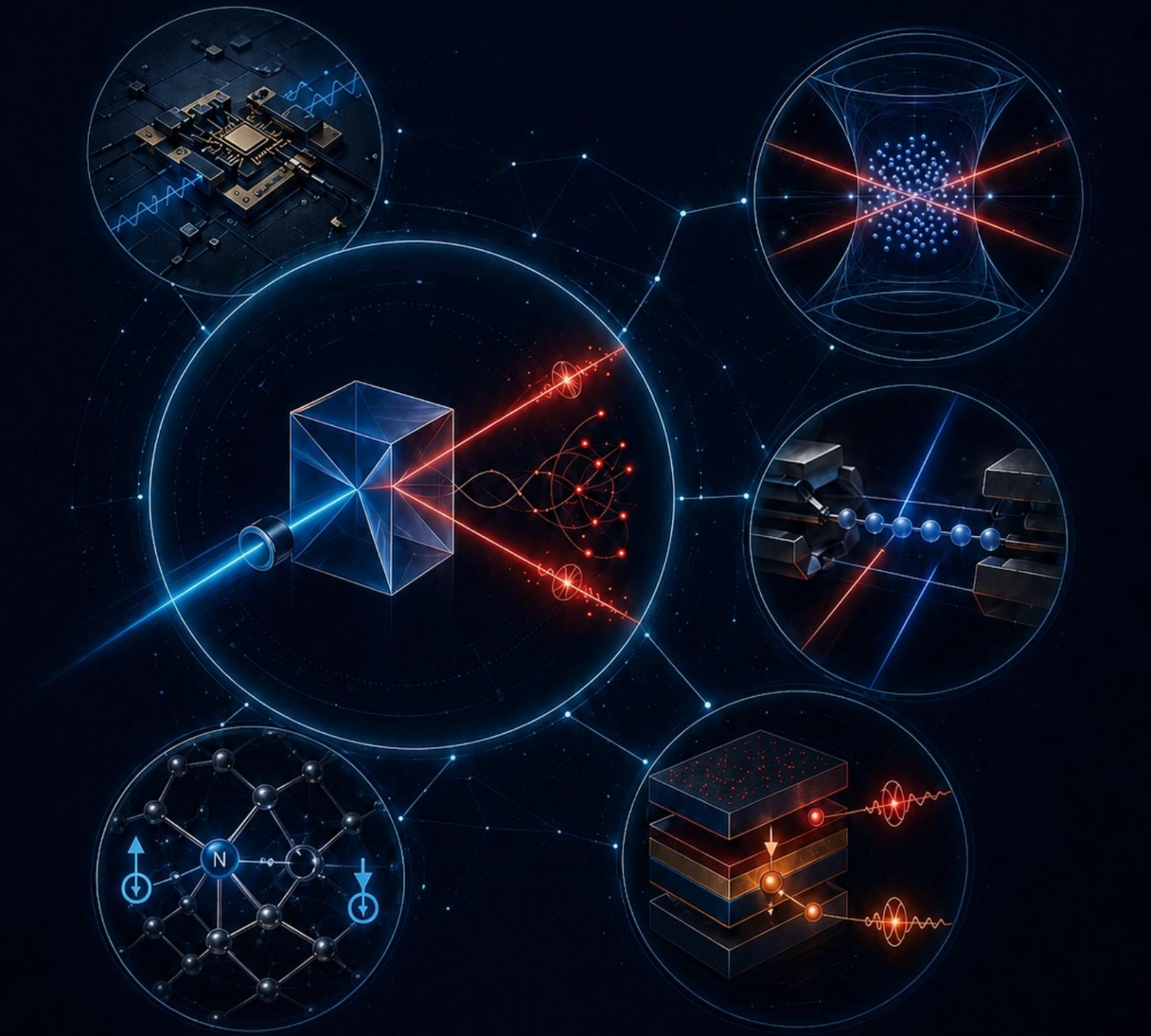
KUANTUM BİLİŞİMİ



MSc Ahmet Nail TAŞTAN, MSc Hilal ÖZTEMEL, MSc Yetiş ÜNAL, MSc Zehra ŞİMŞEK

Editör: Dr. Öğr. Üyesi Serkan Aydın

ÖNSÖZ

"Einstein, spooky action konusu olan Bell belirsizliğinde / Bell eşitsizliklerinde yanıldı.

Sizler de kuantum fenomenlerini anlatırken yanılabilirsiniz.
Üzülmeyin, hep beraber düzelterek öğreneceğiz."

Bu kitap, Kuantum Bilişimi doktora dersi kapsamında, dersi alan öğrencilerin edindikleri bilgileri yeniden değerlendirerek, literatür desteğiyle geliştirdikleri bölümlerden oluşmaktadır.

Editörden

Bu kitap, 2026 yılının Şubat ayından itibaren Marmara Üniversitesi'nde verilmeye başlanan “Kuantum Bilişimi” dersi için doktora öğrencileri tarafından hazırlanmıştır.

Kitapta bahse geçen temel kavramlar aşağıda özetlenmektedir.

Süperpozisyon ilkesi; parçacığın (elektron ve fotonların) kuantum özelliklerine göre aynı anda hem 1 hem de 0 (bilişim sistemlerinde bu şekilde ifade ediyoruz) olarak nitelendirilebilecek durumda olmasıdır. Bu, kuantum mekaniğinin temel ilkelerinden biridir.

Heisenberg Belirsizlik İlkesi, kuantum durumunda olan bir parçacığın konumu ve momentumunun aynı anda sonsuz hassasiyetle ölçülemeyeceğini belirten temel ilkedir. Konum daha net ölçüldükçe momentumdaki belirsizlik artar. Bu durum, ölçüm cihazlarının yetersizliğinden değil kuantum mekaniğinin temel yapısından kaynaklanır.

Bell eşitsizliğinin ihlali ise birbirine dolanık parçacıklar nerede olursa olsun, dolanık parçacıklardan biri ölçüldüğünde süperpozisyon durumundan çıkarak korele sonuçlar üretmeleriyle ilgilidir. Bu sonuç, bir parçacık 1 ise diğerinin onun zıttı olacak şekilde 0 olarak korele olabileceği gibi, aynı değeri 1 alacak şekilde korele olması biçiminde de görülebilir.

Aynı değeri alma (pozitif korelasyon): Parçacıklar böyle bir durumdaysa, biri “0” ölçüldüğünde diğeri de mutlaka “0” çıkar; yani aynı sonucu verirler.

Zıt değeri alma (negatif korelasyon): Parçacıklar singlet durumdaysa, biri “0” ise diğeri mutlaka “1” çıkar.

Bilişim sistemlerindeki 0 ve 1 nitelemelerinin kaç fiziksel durumun karşılığı olarak yazılabileceği özellikle vurgulanmalıdır. Öğrencilere anlatırken ve örnek verirken frekans ve polariteye göre dolanık durumları kullanmak yararlı olacaktır. Fazla sayıda dolanıklık örneği karışıklık yaratabilir. Frekans ve polaritenin yanında mod (iletim hattında farklı yollardan gitme), zaman gecikmesi (dolanık parçacıklardan birinin diğerine göre gecikmeli gitmesi) ve parçacıkların açısal momentumunun birbirini nötrlemesi gibi özellikler de örnek olarak ele alınabilir.

Örneğin iki foton, toplam açısal momentumun korunduğu veya her ikisinin de aynı anda hem dikey hem yatay olduğu süperpozisyon/Bell durumlarını alabilir. Ölçüm yapılana kadar belirsizdirler; ancak ölçüm anında, seçilen duruma bağlı olarak, birbirlerine zıt veya aynı değerleri alırlar. Aşağıdaki ifade polariteye göre dolanıklığı göstermektedir. H ve V yerine diğer parçacık dolanıklık özellikleri farklı karakterlerle isimlendirilebilir.

$$\Phi^{+} = 1/\sqrt{2}\ (|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B)$$

Burada Einstein’ın yanıldığı nokta, Nobel ödülüyle bilimsel önemi kabul edilen Bell eşitsizliğinin ihlali konusunun bir teorem olmasıdır; kanun değildir. Teoremler ile bilimsel kanunlar (yasalar) arasındaki temel fark, teoremlerin matematiksel ve mantıksal kanıtı olan ifadeler, kanunların ise doğadaki gözlemlenebilir ve tekrar eden olayların tanımları olmasıdır. Teoremler genellikle matematik gibi soyut alanlarda kanıtlanabilirken, kanunlar deneysel verilere dayanır.

Editör Dr. Serkan Aydın, dersin anlaşılmasında farklı yorumların tartışmaya açılmasının öğretici değer taşıdığı düşüncesiyle aşağıdaki hipotezi bir tartışma notu olarak sunmaktadır:

NOT: Aşağıdaki hipotez editörün kişisel görüşüdür; henüz deneysel veya teorik olarak kanıtlanmamıştır. Okuyucuları tartışmaya teşvik amacıyla sunulmuştur.

“Galaktik ölçekli kütleçekimsel yapılar (özellikle kara delikler), kuantum dolanıklığını sınırlayan bir ‘yerellik sınırı’ oluşturur.”

Bu hipotez, mikro ölçekteki kuantum dolanıklığı ile büyük ölçekli uzay-zaman yapıları arasındaki ilişkinin tartışılmasına yönelik spekülatif bir öneri olarak değerlendirilmelidir. Dolanıklığın uzay-zaman geometrisiyle ilişkisi güncel araştırmaların açık problemlerinden biridir.

Editör tarafından yazılan bu giriş yazısı, bu konuyla ilgilenen çocukların, gençlerin, öğrencilerin ve bilim insanlarının eleştirel düşünmesini, tartışmaya katılmasını ve evreni anlamaya yönelik bilimsel merakını canlı tutmasını amaçlamaktadır. Huzur dilerim. Başarılar.

İÇİNDEKİLER

Kuantum Bilişim: Klasik Temelden Kuantum Paradigmaya 9
1.1 Klasik Hesaplamanın Temeli: Anahtarlama ve Bit 10
1.1.1 Klasik Hesaplama Paradigması 10
1.1.2 İkili Sayı Sistemi ve Elektriksel Temsil 10
1.1.3 Elektriksel Anahtar (Switching) Kavramı 10
1.1.4 Transistör: Elektronik Anahtarlama Elemanı 12
1.1.4.1 BJT (Bipolar Junction Transistor) 12
1.1.4.2 MOSFET (Metal Oxide Semiconductor Field Effect Transistor) 13
1.1.5 Mantık Kapıları (Logic Gates) 14
1.1.6 Transistörlerden Bilgisayara: Hiyerarşik Yapı 15
1.1.7 Yazılım ve Anahtarlama: Bir Sentez 17
1.2 Ardışıl Sayısal Devreler: Latch, Flip-Flop, Yazmaç ve Sayaç 18
1.2.1 Bit: Bilginin En Küçük Birimi 18
1.2.2 Latch Devreleri: Bitin Fiziksel Olarak Saklanması 18
1.2.2.1 SR Latch 18
1.2.2.2 D Latch ve Saat Kontrollü Çalışma 19
1.2.3 Flip-Flop: Senkron Belleğin Temel Elemanı 20
1.2.3.1 D Tipi Flip-Flop (D-FF) 20
1.2.3.2 Zamanlama Parametreleri 20
1.2.4 Yazmaç (Register): Çok Bitli Bilgi Saklama 20
1.2.5 Kaydırmalı Yazmaç (Shift Register) ve Seri Veri Aktarımı 22
1.2.6 Sayaç (Counter): Ardışıl Durum Makinesi 22
1.3 Qubit ve Dolanıklık (Entanglement) 26
1.3.1 Qubit Nedir? Klasik Bitten Kuantum Bite Geçiş 26
1.3.2 Qubitin Geometrik Temsili: Bloch Küresi 26
1.3.3 Süperpozisyon (Superposition) 27
1.3.4 Ölçüm Problemi (Measurement Problem) 28
1.3.5 Dolanıklık (Entanglement) 29
1.3.6 Bell Durumları (Bell States) 29
1.4 Kuantum Algoritmalar, Kriptografik Tehditler ve Donanım Sınırlılıkları 30
1.4.1 Shor Algoritması: Periyot Bulma ile Çarpanlara Ayırma 30
1.4.2 Grover Algoritması: Genlik Yükseltme ile Yapısız Arama 30
1.4.3 RSA ile İlişkisi: Kriptografik Güvenlik Üzerindeki Etki 31
1.4.4 Kuantum Aydınlatma (Quantum Illumination): Algılamada Kuantum Korelasyonları 31
1.4.5 Günümüzün Sınırlamaları: Hata Toleransı ve NISQ Rejimi 31
1.4.6 Simülasyon Örnekleri: Python ve Qiskit Uygulamaları 31
1.4.6.1 Grover Algoritması - NumPy Simülasyonu 32
1.4.6.2 Grover Algoritması - Qiskit Devresi 32
1.4.6.3 Shor Algoritması - Klasik Periyot Bulma Simülasyonu 33
1.5 Bölüm Özeti ve Bir Sonraki Bölüme Geçiş 34
Kuantum Kapıları, Dolanıklık ve Kuantum Devreleri 35
2.1 Lojik Kapılar, İkili Aritmetik ve Evrensel Hesaplama 35
2.1.1 Bit: Bilginin Atomik Birimi 35
2.1.2 İkili (Binary) Sayı Sistemi ve Taban Dönüşümü 35
2.1.3 İşaret Biti ve İkiye Tümleme (Two's Complement) 36
2.1.4 Taşıma (Carry) Biti ve Aritmetik Taşıma 37
2.1.5 Mantık Kapısı Kavramı ve Boole İşlem Modeli 38
2.1.6 Temel Mantık Kapıları 38
2.1.6.1 AND Kapısı 38
2.1.6.2 OR Kapısı 39

2.1.6.3 NOT Kapısı (Inverter - Tersleyici) 39
2.1.6.4 NAND Kapısı 39
2.1.7 Evrensel Kapı Kavramı 40
2.1.8 NAND ile Evrensel Kapı Sentezi 40
2.1.8.1 NAND → NOT 40
2.1.8.2 NAND → AND 41
2.1.8.3 NAND → OR 41
2.1.8.4 NAND → NOR 41
2.1.8.5 NAND → XOR (Minimum Devre) 41
2.1.9 AND ve NOT Kapıları ile Diğer Kapıların Sentezi 41
2.1.10 AND + NOT → NAND 41
2.1.10.1 AND + NOT → OR 42
2.1.10.2 AND + NOT → NOR 42
2.1.10.3 AND + NOT → XOR - SOP Formu 42
2.2 Kuantum Hesaplama Temelleri 42
2.2.1 Kuantum Hesaplama Nedir? 42
2.2.2 Bit ve Qubit: Temel Bilgi Birimlerinin Karşılaştırılması 43
2.2.3 Süperpozisyon İlkesi 44
2.2.3.1 Fiziksel Temel: Elektronun Çok Durumlu Varlığı 44
2.2.3.2 Matematiksel Gösterim ve Olasılık Yorumu 44
2.2.3.3 Schrödinger'in Kedisi Analojisi 45
2.2.4 Qubit Gösterimi: Bloch Küresi 45
2.2.5 Kuantum Paralelliği 46
2.2.6 Kuantum Bilgisayarlar Neden Güçlüdür? 47
2.3 Kuantum Kapısı ve Dolanıklık (Entanglement) 48
2.3.1 Temel tek qubit kapıları 49
2.3.1.1 X kapısı 49
2.3.1.2 H kapısı (Hadamard) 49
2.3.2 Kuantum Kapıları: Vektörden Hesaplamaya İlk Adım 50
2.3.3 Tek qubitli kuantum durumu ve üniter evrim. 51
2.3.4 Bloch Küresi 51
2.3.5 Tek qubit kapılarının matris gösterimleri 54
2.3.6 Tipik iki qubitlik kapı 56
2.4 Kuantum Donanımı (Qubit Teknolojileri) 61
2.4.1 Giriş 61
2.4.2 Ion Trap Qubit (İyon Tuzaklı Qubitler) 61
2.4.3 Superconducting Qubit (Süperiletken Qubitler) 62
2.4.4 Photon Qubit (Foton Qubitler) 63
2.4.5 IBM Quantum Composer 64
Kuantum Anahtar Dağıtımı (QKD) Sistemlerinin Mimari Yapısı, Çalışma Prensibi ve Güvenlik Analizi 65
3.1 Kuantum Anahtar Dağıtımı: Temel Kavramlar ve Sistem Mimarisi 65
3.1.1 Kuantum Haberleşme Nedir? 65
3.1.2 RSA ile QKD Farkı Nedir? 65
3.1.3 Neden 'Kuantum RSA' Değil, Kuantum Anahtar Dağıtımı? 66
3.1.4 Tek Foton Neden Kullanılır? 67
3.1.5 Polarizasyon ve Faz Neden Tercih Edilir? 67
3.1.6 Sistemin Genel Blok Yapısı 68
3.1.6.1 Verici (Alice) 68
3.1.6.2 Kuantum İletim Hattı 69
3.1.6.3 Alıcı (Bob) 69
3.1.6.4 Klasik Kontrol ve Zamanlama Altyapısı 69

3.2 Kuantum Anahtar Dağıtımı (QKD) 70
3.2.1 Sistem Mimarisi, Verici-Alıcı Tasarımı ve Zaman Damgalı Saldırı Tespiti 70
3.2.1.1 Giriş ve Motivasyon 70
3.2.2 QKD Genel Sistem Mimarisi 71
3.2.2.1 İki Paralel Kanal Yapısı 71
3.2.2.2 Sistem Bileşenlerine Genel Bakış 71
3.2.3 Verici Taraf (Ali / Transmitter): Kapsamlı Analiz 72
3.2.3.1 Tek Foton Kaynağı (TFK): Neden Tek Foton? 72
3.2.3.2 Fotonun Hazırlanması ve Polarizasyon ile Kuantum Durum Kodlama 73
3.2.3.2.1 BB84 Protokolü: İki Konjuge Baz 73
3.2.3.2.2 Durum Hazırlama Devresi: HWP ve PBS 74
3.2.3.3 Dolanıklık (Entanglement): Hangi Aşamada ve Nasıl Oluşur? 75
3.2.4 FPGA'nın Verici Taraftaki Rolü, Zaman Damgası Mantığı ve Çökme Analizi 76
3.2.4.1 FPGA Verici Tarafta Ne Yapar? 76
3.2.4.2 Neden FPGA Ölçüm Yapmaz? - Fiziksel Zorunluluk 76
3.2.4.3 Zaman Damgası Mantığı: T_1 Fotona Değil, Tetik Olayına Atanır 77
3.2.4.4 Neden Bu Aşamada Dalga Fonksiyonu Çökmez? 77
3.2.4.4.1 Hazırlama ile Ölçümün Matematiksel Karşılaştırması 77
3.2.4.4.2 Foton Yaşam Döngüsü ve Çökme Anı 78
3.2.4.4.3 Dekoherans Riski ve Yönetimi 78
3.2.4.5 Verici Taraf Tam Sistem Akışı 78
3.2.5 Dinleyici Tehdit Modeli: Eve'nin Saldırı Senaryosu 79
3.2.5.1 Man-in-the-Middle (MITM) Saldırısı 79
3.2.5.2 Dolanıklık Korelasyonlarının Saldırı Tespitindeki Rolü 80
3.2.6 Alıcı Taraf (Buse / Bob): Ölçüm ve Anahtar Üretimi 80
3.2.6.1 Polarizasyon Dedektör Sistemi 80
3.2.6.2 Anomali Tespit Algoritması 80
3.2.6.3 RSA Anahtar Oluşturma Süreci 80
3.2.7 Güvenlik Analizi 81
3.2.7.1 Kanıtlanabilir Güvenlik Temeli 81
3.2.7.2 Pratik Saldırı Vektörleri 81
3.2.8 Matematiksel Ek: Temel İlişkiler 82
3.2.8.1 Bell Durumu ve Dolanıklık Ölçütü 82
3.2.8.2 QBER Hesabı 82
3.2.8.3 Zaman Damgası Hassasiyet Sınırı 82
3.2.9 Bölüm Özeti ve Bir Sonraki Bölüme Geçiş 82
3.3 İLETİM HATTI, ALICI TARAF VE ÖLÇÜM SÜRECİ 83
3.3.1 Giriş ve Motivasyon 83
3.3.2 Fotonun Optik Kanal Üzerinden İletilmesi 83
3.3.3 İletim Süresi ve Beklenen Zaman Penceresi 84
3.3.4 Alıcı Tarafta Dedektörlerin Rolü 84
3.3.5 Foton Algılandığında Elektriksel Sinyal Oluşması 85
3.3.6 Ölçüm Anında Kuantum Durumunun Belirlenmesi 85
3.4 Entanglement Tabanlı Sistemlerde Korelasyon 86
3.4.1 Prepare-and-Measure Sistemleri 86
3.4.2 Gönderim Zamanı ile Algılama Zamanının Karşılaştırılması 86
3.5 GÜVENLİK, SALDIRI TESPİTİ VE ŞEKLİN YORUMU 87
3.5.1 Araya Biri Girerse Ne Olur? 87
3.5.2 Ölçüm Neden Sistemi Bozar? 88
3.5.3 Erken Çökme, Bozulma ve Hata Oranı Artışı 88
3.5.4 Zaman Damgaları Neden Önemlidir? 89
3.5.5 Beklenen Zaman Penceresi Dışına Çıkma Ne Gösterir? 90

3.5.6 Hangi Durumda Alarm Verilir?....90
3.5.7 Eşik Değeri Mantığı....91
3.5.8 Alice–Bob Hattının ve Saldırı Tespiti Yaklaşımının Şekil Üzerinde Açıklanması....92
3.5.9 Sistem Nasıl Uyarı Üretir? - Uçtan Uca Akış....93
3.6 Sonuç: Bu Yapı Neden Güvenlidir ve Saldırıyı Nasıl Fark Eder?....95
Kuantum Haberleşmede Güvenlik Sınırları ve Kuantum Anahtar Dağıtım Protokolleri....97
4.1 Klasik İletişim Altyapısının Güvenlik Sınırları ve Kuantum Haberleşmeye Geçiş Motivasyonu97
4.1.1 Fiber Optik Altyapısı: Çalışma İlkeleri ve Donanım....97
4.1.1.1 SFP Modülleri: Altyapının Kritik Bileşeni....97
4.1.1.2 Ağ Mimarisi: Erişimden Omurgaya....98
4.1.2 Fiziksel Katmanda Dinleme Zafiyeti....98
4.1.2.1 Yaygın Bir Yanılgı....98
4.1.2.2 Başlıca Fiziksel Dinleme Yöntemleri....98
4.1.2.3 Dinleme Şemasının Görsel Analizi....100
4.1.2.4 Tespit Yöntemleri ve Sınırlılıkları....100
4.1.3 Altyapı Güvenliğine Yönelik Jeopolitik Tehditler....101
4.1.3.1 Denizaltı Kablo Ağlarının Stratejik Konumu....101
4.1.3.2 Son Dönem Sabotaj Olayları....102
4.1.3.3 Yazılım Egemenliği: Görünmez Tehdit....103
4.1.4 Klasik Kriptografinin Hesaplama Sınırları....103
4.1.4.1 Güvenlik Paradigmasının Yapısal Kırılganlığı....103
4.1.4.2 Kuantum Algoritmalarının Kriptografiye Etkisi....103
4.1.4.3 Üç Paradigmanın Karşılaştırılması....105
4.1.5 Kuantum Haberleşmeye Geçiş Motivasyonu....106
4.1.5.1 Güvenlik Paradigmasının Temelden Değişimi....106
4.1.5.2 Mevcut Altyapının Dönüşümü....106
4.1.5.3 Jeopolitik ve Stratejik Zorunluluk....107
4.2 Kopyalanamama Teoremi (No-Cloning Theorem)....107
4.2.1 Teoremin Tarihsel Arka Planı....107
4.2.2 Teoremin Matematiksel İspatı....108
4.2.3 Kriptografi Açısından Önemi....108
4.3 Ölçüm Bozunumu (Measurement Disturbance)....109
4.3.1 Heisenberg Belirsizlik İlkesi....109
4.3.2 Kuantum Ölçümün Doğası....109
4.3.3 Dinlemenin Fiziksel İzi....109
4.4 Alice, Bob ve Eve....110
4.4.1 Kriptografik Karakter Modeli....110
4.4.2 Klasik Kriptografiden Kuantum Kriptografiye....110
4.5 Kuantum Anahtar Dağıtımına Giriş (QKD)....110
4.5.1 QKD'nin Temel Felsefesi....110
4.5.2 Bilgi-Kuramsal Güvenlik....111
4.5.3 QKD Protokol Ailesi....111
4.6 BB84 Protokolü ve Kuantum Anahtar Dağıtımının Kriptografik Analizi....112
4.6.1 Giriş: Kuantum Kriptografinin Doğuşu....112
4.6.2 BB84 Protokolü: Adım Adım Operasyonel Akış ve Teknik Analiz....112
4.6.2.1 Kuantum İletim Aşaması (Fiziksel Katman)....112
4.6.2.2 Klasik Veri İşleme Aşaması (Protokol Katmanı)....113
4.6.2.3 Hata Tahmini ve QBER Hesabı....113
4.6.2.4 Hata Düzeltme ve Gizlilik Güçlendirme....114
4.6.3 Güvenlik Kontrolü ve Eve Etkisi Analizi....114
4.6.3.1 Klonlamama Teoremi ve Pasif Dinleme İmkânsızlığı....114
4.6.3.2 Intercept-Resend Saldırısı....114

4.6.3.3 Hata Tanımlama ve Eşik Değeri....115
4.6.4 Anahtar Oluşturma Süreci....115
4.6.4.1 Bilgi Uzlaştırma....115
4.6.4.2 Gizlilik Güçlendirme....115
4.6.5 BB84 Örnek Akış Tablosu....115
4.7 E91 Protokolü: Dolanıklığın Gücü, Bell Eşitsizlikleri ve Cihaz Bağımsız Güvenlik....116
4.7.1 Önceki Protokollerin Ötesinde: Neden E91?....116
4.7.2 Charlie ve Kaynak Sorunu....116
4.7.3 Bell Eşitsizliği ve CHSH Testi....117
4.7.3.1 Einstein–Podolsky–Rosen Paradoksu....117
4.7.3.2 Bell'in Orijinal Eşitsizliği....117
4.7.3.3 CHSH Parametresi S....117
4.7.3.4 CHSH'nin E91'de Kullanımı....118
4.7.4 E91 Protokolü Adım Adım....118
4.7.4.1 Kullanılan Kuantum Durumu....118
4.7.4.2 Protokol Akışı....118
4.7.5 Dolanık Foton Üretimi....119
4.7.5.1 Kendiliğinden Parametrik Aşağı Dönüşüm (SPDC)....120
4.7.5.2 Dört-Dalga Karışımı (FWM)....120
4.7.5.3 Dolanıklık Kalitesinin Ölçümü....120
4.7.6 Gerçek Uygulamalar....121
4.7.6.1 Boşluksuz Bell Deneyleri....121
4.7.6.2 Micius Uydusu....121
4.7.6.3 DI-QKD ve MDI-QKD....121
4.7.7 Güvenlik Analizi....122
NIST Standartları ve Kuantum Sonrası Kriptografi: Kurumsal Çerçeve, Tehdit Analizi ve Standardizasyon Süreci....123
5.1 Giriş....123
5.2 NIST'in Kurumsal Kimliği, Yasal Çerçevesi ve Yayın Hiyerarşisi....123
5.2.1 Tarihsel Gelişim ve Yasal Dayanak....123
5.2.2 NIST Yayın Türleri ve Hiyerarşisi....124
5.3 NIST Siber Güvenlik Çerçevesi (CSF) 2.0....124
5.3.1 Çerçeve Mimarisi ve Temel Bileşenleri....124
5.3.2 CSF Core Fonksiyonları....125
5.4 Akademik Çalışma ile Standart Araştırması Arasındaki Temel Farklar....126
5.5 Kuantum Bilgisayarların Kriptografik Tehdit Analizi....127
5.5.1 Shor Algoritması: Asimetrik Kriptografinin Teorik Çöküşü....127
5.5.2 Grover Algoritması: Simetrik Kriptografiye Karekök Etkisi....128
5.5.3 "Şimdi Topla, Sonra Çöz" (Harvest-Now, Decrypt-Later) Tehdidi....128
5.6 NIST Kuantum Sonrası Kriptografi Standardizasyon Süreci....129
5.6.1 Değerl. Kriterleri: Güvenlik, Performans ve Esneklik....130
5.7 Seçilen NIST PQC Standartları: Matematiksel Temeller ve Kapsam....130
5.7.1 FIPS 203 - ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)....131
5.7.2 FIPS 204 - ML-DSA (Module-Lattice-Based Digital Signature Algorithm)....131
5.7.3 FIPS 205 - SLH-DSA (Stateless Hash-Based Digital Signature Algorithm)....131
5.7.4 FIPS 206 - FN-DSA / FALCON (Taslak)....132
5.8 NIST PQC Güvenlik Seviyeleri Çerçevesi....132
5.9 Geçiş Stratejileri, Uluslararası Uyum ve Diğer NIST Çalışmaları....132
5.9.1 Hibrit Kriptografi Yaklaşımı....132
5.9.2 Uluslararası Standardlaşma Uyumu....133
5.9.3 Kuantum Anahtar Dağıtımı (QKD) ile İlişkisi....133
5.10 Eleştirel Değerlendirme: NIST PQC Sürecinin Sınırlılıkları....133

Kuantum Algoritmalar 134
6.1 Giriş: Kuantum Avantajının Gerçek Kaynağı 134
6.2 Oracle: Problemi Devreye Gömen Kara Kutu 135
6.3 Deutsch–Jozsa Algoritması 135
6.3.1 Problem Tanımı ve Klasik Maliyet 135
6.3.2 Kuantum Çözümü ve Devre Yapısı 135
6.4 Simon Algoritması 136
6.4.1 Gizli Yapı Problemi 136
6.4.2 Ölçüm Cevap Değil, Denklem Üretir 137
6.5 Grover Algoritması 137
6.5.1 Yapılandırılmamış Arama ve Klasik Alt Sınır 137
6.5.2 Oracle ve Diffuser: İki Temel Operatör 137
6.5.3 Geometrik Yorum 137
6.6 Kuantum Fourier Dönüşümü (QFT) 138
6.6.1 QFT Nedir? 138
6.6.2 Devre Yapısı ve Rolü 139
6.7 Kuantum Faz Tahmini (QPE) 139
6.7.1 Temel Fikir: Fazı Sayıya Çevirmek 139
6.7.2 QPE Çalışma Mekanizması 140
6.8 Shor Algoritması 140
6.8.1 Faktörizasyonun Periyot Bulmaya İndirgenmesi 140
6.8.2 QFT ve QPE'nin Rolü 141
6.8.3 Kriptografik Etkisi 141
6.9 Kavramsal Harita: Algoritmaları Birbirine Bağlamak 142
Kuantum Kapıları ve Kuantum Hesaplamanın Temelleri 145
7.1 Kuantum Kapılarına Giriş 145
7.1.1 IBM Quantum Composer Arayüzü 145
7.1.2 Tek Kübitlik Kapılar 146
7.1.2.1 Pauli Kapıları (X, Y, Z) 146
7.1.2.2 Hadamard Kapısı (H) 146
7.1.2.3 Faz Kapıları: S ve T 148
7.1.2.4 Parametreli Döndürme Kapıları (RX, RY, RZ) 151
7.1.3 Çok Kübitlik Kapılar 153
7.1.3.1 CNOT (Kontrollü-NOT) Kapısı 153
7.1.3.2 Toffoli Kapısı (CCNOT) 154
7.1.3.3 Identity (I) Kapısı 154
7.1.3.4 Bariyer (Barrier) 155
7.1.3.5 Genel Tek Kübit Kapısı (U) 155
7.2 CNOT ve Pauli Kapıları ile Klasik Lojik Devrelerin Oluşturulması 156
7.2.1 Toffoli Kapısı ile AND İşlemi 156
7.2.2 CNOT ve Toffoli ile OR İşlemi 156
7.2.3 XOR ile CNOT İşlemi 156
7.2.4 Lojik Kapıların Doğruluk Tabloları ve Kuantum Devreleri 157
7.2.4.1 NOT → Pauli-X Kapısı 157
7.2.4.2 AND → Toffoli (CCNOT) Kapısı 157
7.2.4.3 OR → De Morgan Yaklaşımı (X + Toffoli + X) 158
7.2.4.4 XOR → CNOT Kapısı 158
7.3 Kuantum Ölçümü (Measurement) 160
7.3.1 Ölçümün Devre İçindeki Konumu 161
7.3.2 Çok Sayıda Tekrar (Shots) ve İstatistiksel Sonuçlar 161
7.4 Bell Durumları ve Kuantum Dolanıklık 162
7.4.1 Bell Durumlarının Oluşturulması 162

7.4.2 Dolanıklığın Ölçümle Çözülmesi (Bell Korelasyonları) 162
7.4.3 Bell Eşitsizliğinin Deneysel Doğrulanması 163
7.5 Dekoherans (Zaman Gecikmesi) ve Kuantum Hatalar 164
7.5.1 T1 ve T2 Süreleri 164
7.5.2 Gerçek Donanımda Test Etme 164
7.5.3 Gerçek Donanımdaki Hata Kaynakları 164
7.5.4 Fiziksel ve Mantıksal Kübit 164
7.5.5 Simülatörlerle Test 165
7.6 Kuantum Hesaplama Gücü ve Üstünlük 165
7.6.1 Üstel Durum Uzayı: 2^n Kübit 165
7.6.2 Kuantum Paralelizmi 165
7.6.3 Neden Dekoheransa Rağmen Klasik Bilgisayarların Yapamadığını Yapabiliyoruz? 166
7.6.4 Kuantum Üstünlüğü Perspektifi 166
7.6.5 Zaman Karmaşıklığında Fark 166
7.7 Kuantum Bilgisayarların Basit İşlemlerde Zorlanması 166
7.7.1 Neden Basit İşlemlerde Zorlanır? 167
7.7.2 Kuantum Avantajının Olduğu ve Olmadığı Alanlar 167
7.7.3 Klasik ve Kuantum Bilgisayarların Üstün Olduğu Alanlar 167
7.8 Kuantum Algılama (Quantum Sensing) 168
7.9 X Kapısı ile Hadamard Kapısı Karşılaştırması 168
7.10 Süperpozisyon ile Dolanıklık Karşılaştırması 168
7.11 RZ Kapısı Neden Ölçüm Histogramını Değiştirmez? 169
7.12 CNOT Kapısında Kontrol ve Hedef Mantığı 170
7.13 Bell Durumu Nasıl Oluşturulur? 171
7.14 Tek Kübitten Çok Kübite Geçişte Matris Boyutu ve Tensör Çarpımı 171
7.15 Kuantum Register ve Klasik Register Ayrımı 172
7.16 Reset ile Measurement Farkı 173
7.17 Faz Kavramı: Görünmez Ama Etkili 174
7.17.1 Faz Nedir? 174
7.17.2 Faz Neden Ölçümde Doğrudan Görünmez? 174
7.17.3 Faz Neden Yine de Kritiktir? 174
7.18 IBM Composer'dan Gerçek Kuantum Donanımında Çalıştırma 175
Kuantum Şifreleme 176
8.1 Klasik Şifreleme Yöntemleri 177
8.1.1 Simetrik (Gizli Anahtar) Şifreleme Sistemi 177
8.1.2 Asimetrik (Açık Anahtar) Şifreleme Sistemi 178
8.2 Kuantum Şifreleme Algoritmaları 180
8.2.1 Kuantum Anahtar Dağıtımı (QKD) 181
8.2.2 BB84 Protokolü 183
8.2.3 E91 Protokolü 186
8.3 Kuantum Rastgele Sayı Üretimi 189
8.4 Güvenlik Analizi ve Saldırı Tespiti 191
8.4.1 Anahtarın Değiştirildiğinin Tespiti 191
Kuantum Haberleşmesi ve İnternet Siber Güvenliği 194
9.1 Giriş 194
9.2 Tarihsel Arka Plan 194
9.3 Kuantum Haberleşmesinin Fiziksel Temelleri 195
9.3.1 Qubit ve Süperpozisyon 195
9.3.2 Kuantum Dolanıklığı 195
9.3.3 No-Cloning Teoremi: Güvenliğin Fiziksel Temeli 196
9.4 Kuantum Kanalları, Gürültü ve İletim Kapasitesi 197
9.5 Kuantum Tekrarlayıcılar ve Ağ Mimarileri 197

9.6 Küresel Projeler, Uydu Tabanlı Haberleşme ve Türkiye 199
9.6.1 Küresel Konumlanma 199
9.6.2 Uydu Tabanlı QKD ve Micius 199
9.6.3 Türkiye'nin Stratejik Konumu 200
9.7 Siber Güvenlik: Kuantum Teknolojisinin Çift Yönlü Etkisi 201
9.7.1 Savunma Boyutu: QKD ve PQC 201
9.7.2 Saldırı Boyutu: Shor Algoritması ve Grover'ın Etkisi 201
9.8 Harvest Now, Decrypt Later: Bugünün Tehdit Modeli 202
9.9 BB84 Protokolü ve QKD Güvenlik Analizi 203
9.9.1 BB84'ün Adım Adım İşleyişi 203
9.9.2 Güvenlik Kanıtı ve QBER Eşiği 204
9.9.3 QKD Performansı ve Temel Sınırlar 204
9.10 QKD'ye Yönelik Saldırılar ve Katmanlı Tehdit Modeli 205
9.10.1 Foton Sayısı Bölme (PNS) Saldırısı 205
9.10.2 Kör Gözlem (Blinding) Saldırısı 206
9.10.3 Trojan-Horse ve Zamanlama Yan Kanal Saldırıları 207
9.10.4 Katmanlı Tehdit Modeli 207
9.11 QKD, PQC ve Hibrit Yaklaşımlar: Karşılaştırmalı Değerlendirme 208
9.11.1 PQC Geçişinde Siber Güvenlik Riskleri 209
9.12 Standartlaşma, Politika ve Jeopolitik Boyut 209
9.13 Açık Araştırma Problemleri ve Kuantum İnternet Yol Haritası 210
9.13.1 Açık Araştırma Problemleri 210
9.13.2 Kuantum İnternet Yol Haritası (2025–2040+) 210
Kuantum Haberleşme Uygulamaları ve Sistem Mimarileri 213
10.1 Giriş: Uygulamadan Mimariye 213
10.2 Fotonik Bilgi Taşıyıcıları ve Kodlama Serbestlik Dereceleri 213
10.3 Fiber Altyapısı, Klasik Servis Kanalları ve EDFA 215
10.4 BB84 QKD Uçtan Uca Sistem Mimarisi ve Senkronizasyon 216
10.5 Kuantum Tekrarlayıcılar, Bellek ve Dolanıklık Değişimi 217
10.6 Katmanlı Sistem Mimarisi 217
10.7 Uygulama Alanları ve Mimari Seçimler 218
10.8 Mühendislik ve Güvenlik Değerlendirmesi 219
Kapanış 220
Kaynakça 221

BÖLÜM 1

Kuantum Bilişim: Klasik Temelden Kuantum Paradigmaya

Bu bölüm, modern bilişim teknolojisinin fiziksel ve kavramsal temellerini klasik hesaplamadan kuantum paradigmaya uzanan bütüncül bir çerçeve içinde ele almaktadır. Beşinci bölümde ele alınacak NIST standartları ve kuantum sonrası kriptografi (PQC) bağlamında ortaya konan kriptografik tehditler, bu bölümde hem klasik hem de kuantum hesaplamanın temel ilkeleriyle birlikte derinleştirilmektedir.

Bölüm dört ana kısımdan oluşmaktadır. İlk kısım (1.1), dijital bilgisayarların fiziksel ve mantıksal temellerini oluşturan anahtarlama ilkesini, ikili sayı sistemini, transistör teknolojisini ve mantık kapılarını sistematik biçimde ortaya koymaktadır. İkinci kısım (1.2), ardışıl sayısal devrelerin - latch, flip-flop, yazmaç ve sayaç yapılarının - hiyerarşik yapısını incelemektedir. Üçüncü kısım (1.3), klasik bitten kuantum bite (qubit) geçişi, süperpozisyon ilkesini, ölçüm problemini ve dolanıklık kavramını matematiksel titizlikle ele almaktadır. Dördüncü kısım (1.4) ise Shor ve Grover algoritmalarının hesaplama avantajlarını, kriptografik güvenlik üzerindeki etkilerini ve günümüz kuantum donanımının NISQ rejimindeki sınırlılıklarını somut simülasyon örnekleriyle tartışmaktadır.

1.1 Klasik Hesaplamanın Temeli: Anahtarlama ve Bit

Bu kısımda, modern dijital bilgisayarların fiziksel ve mantıksal temellerini oluşturan anahtarlama (switching) ilkesi sistematik biçimde incelenecektir. İkili sayı sisteminin fiziksel donanımla bu denli örtüşmesi tesadüf değil; aksine, donanım tasarımının dayandığı iki kararlı fiziksel durum ilkesinin kaçınılmaz sonucudur (Harris ve Harris, 2021).

1.1.1 Klasik Hesaplama Paradigması

Klasik hesaplama, bilgiyi Boole cebri ilkeleri çerçevesinde ikili sembollerle temsil eden ve deterministik mantık işlemleri yoluyla işleyen hesaplama paradigmasıdır. Klasik bir bilgisayar, donanım katmanından yazılım katmanına uzanan çok düzeyli bir soyutlama hiyerarşisi üzerine inşa edilmiştir. Bu yapının bütününü mümkün kılan temel fiziksel unsur ise anahtarlama ilkesidir (Tanenbaum ve Austin, 2013).

1.1.2 İkili Sayı Sistemi ve Elektriksel Temsil

Bilgisayarların veriyi ikili sistemle temsil etmesi, matematiksel bir tercihten çok mühendislik gerçekliğinin bir yansımasıdır. Elektronik devreler güvenilir biçimde yalnızca iki kararlı fiziksel durumu sürdürebilmektedir. Bu iki durumun sırasıyla 1 ve 0 sembollerine eşlenmesi, Tablo 1.1'de özetlendiği gibi, hesaplamanın fiziksel ortamla buluştuğu temel noktayı oluşturur (Mano ve Ciletti, 2017).

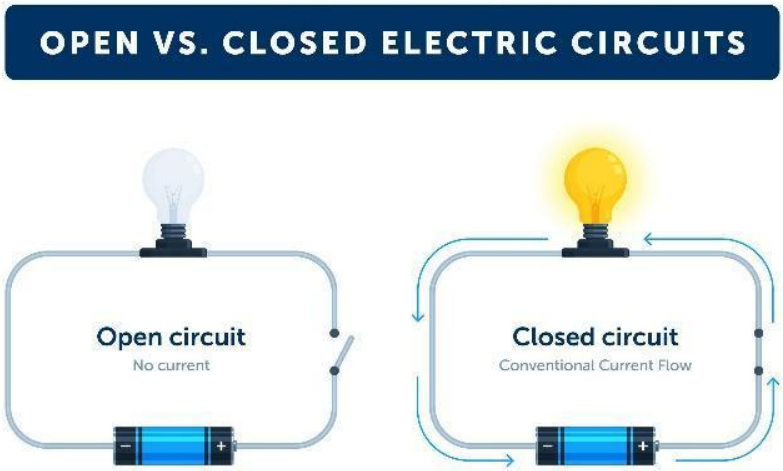
Tablo 1.1. Binary sistemde sembol-fiziksel durum eşleştirmesi.

Değer	Fiziksel Karşılığı
0	Düşük voltaj / kapalı devre
1	Yüksek voltaj / açık devre

n bitlik klasik bir sistem, bu n bit kombinasyonlarından yalnızca tek bir konfigürasyonu aynı anda temsil edebilmektedir. Her bit, gerçekte bir elektrik durumudur: voltaj var ya da yok.

1.1.3 Elektriksel Anahtar (Switching) Kavramı

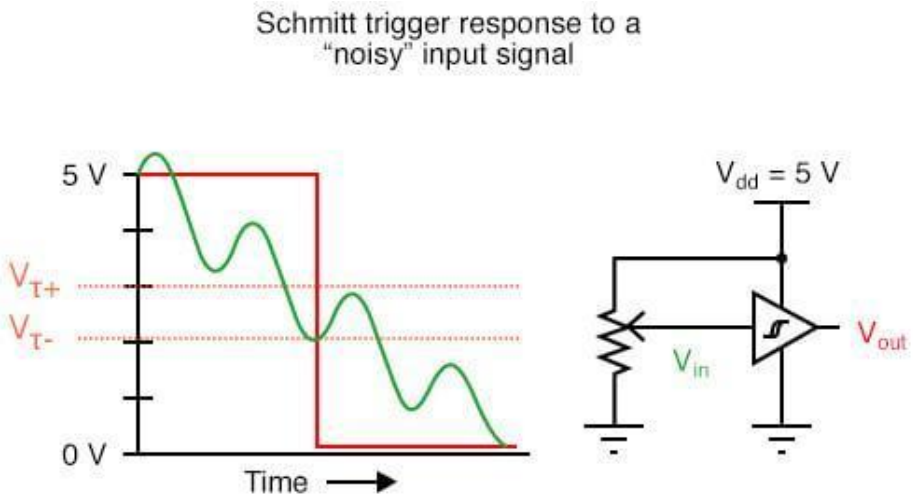
Dijital elektroniğin temel çalışma ilkesi, yalnızca iki kararlı durum arasında geçiş yapan anahtarlama mekanizmasına dayanmaktadır. Şekil 1.1'de gösterilen elektriksel anahtar sembolünde iki durumun - açık ve kapalı - fiziksel karşılıkları sunulmaktadır. Söz konusu tasarım tercihinin üç temel mühendislik avantajı bulunmaktadır: gürültüye dayanıklılık, hata toleransı ve ölçeklenebilirlik (Weste ve Harris, 2015).



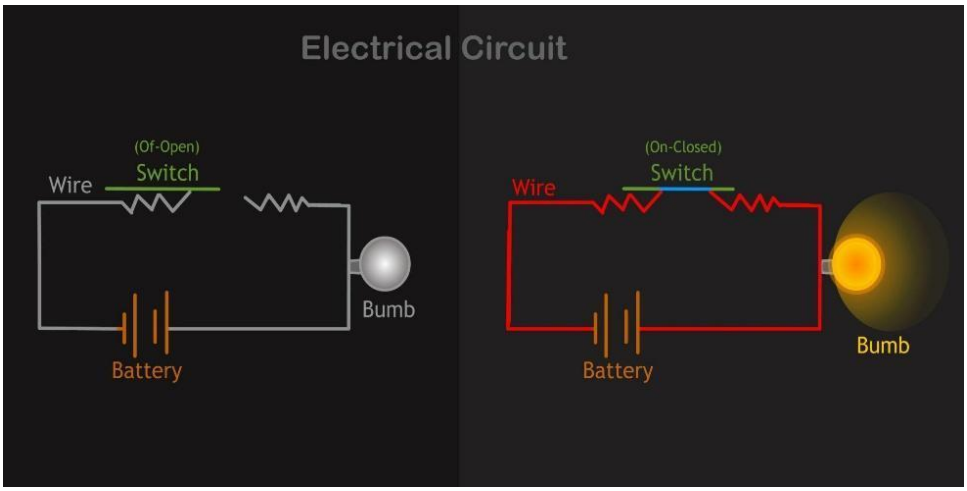
Şekil 1.1. Elektriksel anahtar sembolü ve açık/kapalı durum gösterimi (Harris ve Harris, 2021'den uyarlanmıştır).

Şekil 1.1'de basit bir anahtarlama devresinde akımın varlığı ve yokluğunun 1-0 temsiline nasıl karşılık geldiği gösterilmektedir. Dijital sistemlerin analog sistemlere kıyasla temel avantajı Şekil 1.3'te görselleştirilmiştir: analog sinyal gürültü nedeniyle bozulurken, dijital sinyal voltaj eşiği sayesinde kararlılığını korur. Bu eşikleme mekanizması Şekil 1.4'te detaylandırılmaktadır.

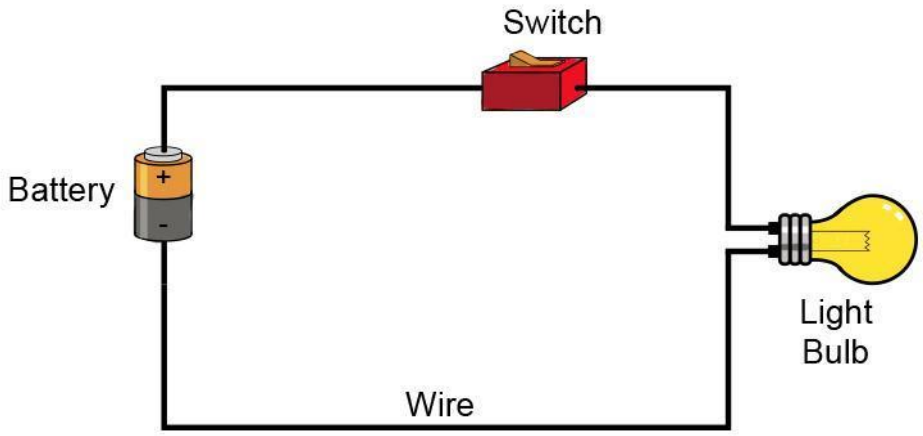
Bu yapı Şekil 1.2'de gösterilmektedir.



Şekil 1.2. Basit anahtarlama devresi: akımın varlığı ve yokluğu üzerinden 1-0 temsili (Harris ve Harris, 2021'den uyarlanmıştır).



Şekil 1.3. Analog sinyal bozulmasına karşı dijital sinyalin kararlı durum avantajı (Weste ve Harris, 2015'ten uyarlanmıştır).



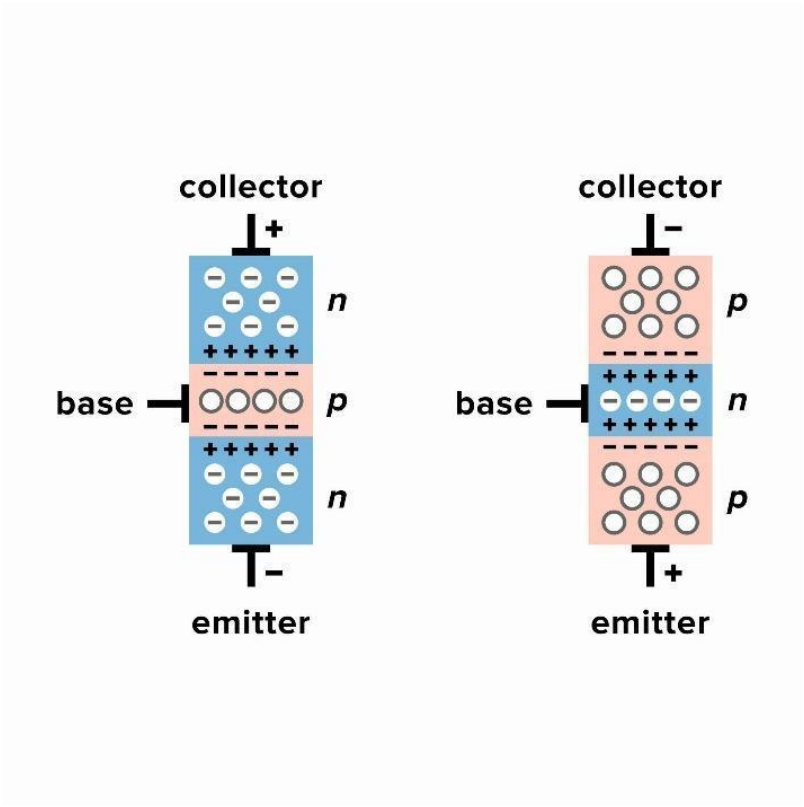
Şekil 1.4. Dijital lojik düzeylerinin voltaj eşiği yorumlama modeli (Weste ve Harris, 2015'ten uyarlanmıştır).

1.1.4 Transistör: Elektronik Anahtarlama Elemanı

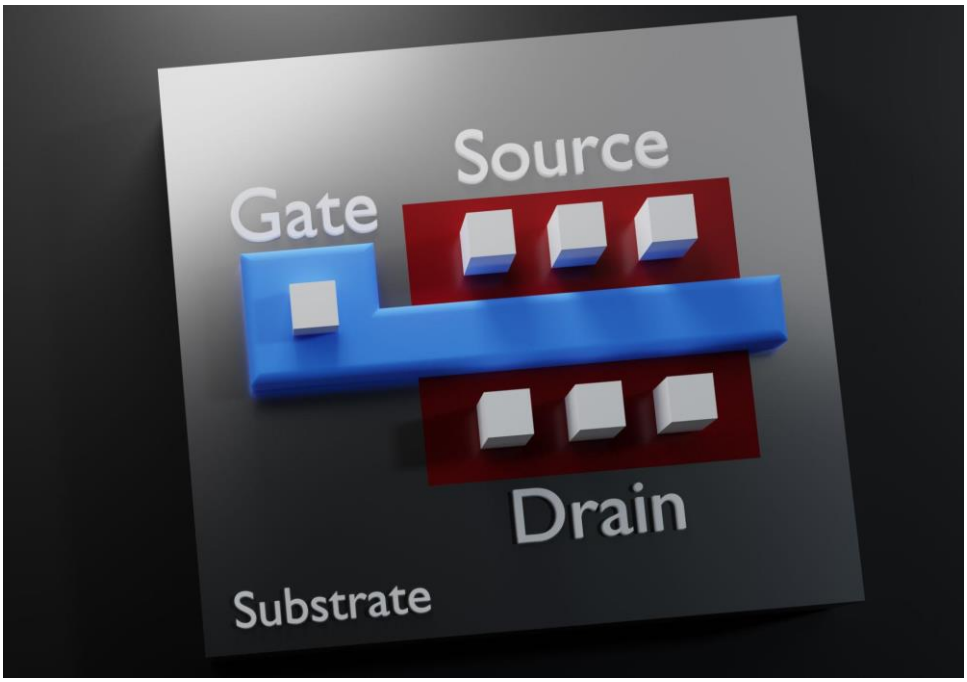
Mekanik anahtarların milisaniye mertebesindeki hızları, modern hesaplama ihtiyaçlarını karşılamaktan uzaktır. 1947 yılında Bell Laboratuvarları'nda Bardeen, Brattain ve Shockley tarafından icat edilen transistör, modern bilişim teknolojisinin temel taşı haline gelmiştir (Sedra ve Smith, 2020).

1.1.4.1 BJT (Bipolar Junction Transistor)

BJT, akım kontrolüyle çalışan bir transistör türüdür. Şekil 1.5'te BJT'nin fiziksel yapısı gösterilmektedir; emitter, base ve collector terminalleri arasındaki akım kontrol mekanizması bu şekilde görselleştirilmiştir. Şekil 1.6'da ise BJT'nin devre sembolü ve taban akımına bağlı çalışma bölgeleri sunulmaktadır (Sedra ve Smith, 2020).



Şekil 1.5. BJT (NPN tipi) yapısı: emitter, base ve collector terminalleri ile akım kontrol mekanizması (Sedra ve Smith, 2020'den uyarlanmıştır).

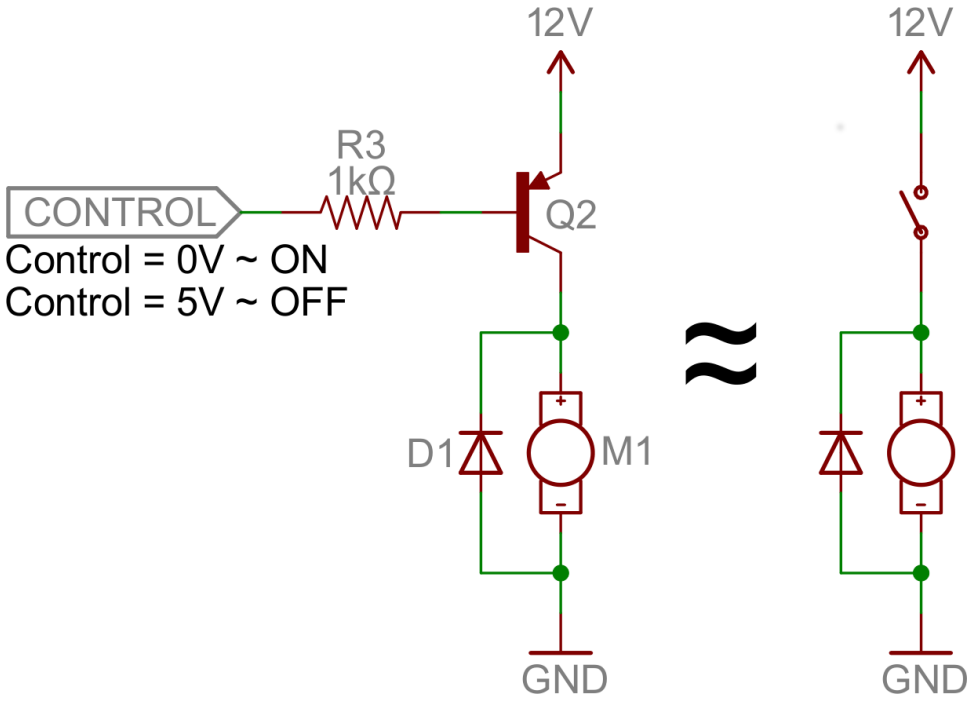


Şekil 1.6. BJT devre sembolü ve anahtarlama karakteristiği: taban akımına bağlı çalışma bölgeleri (Sedra ve Smith, 2020'den uyarlanmıştır).

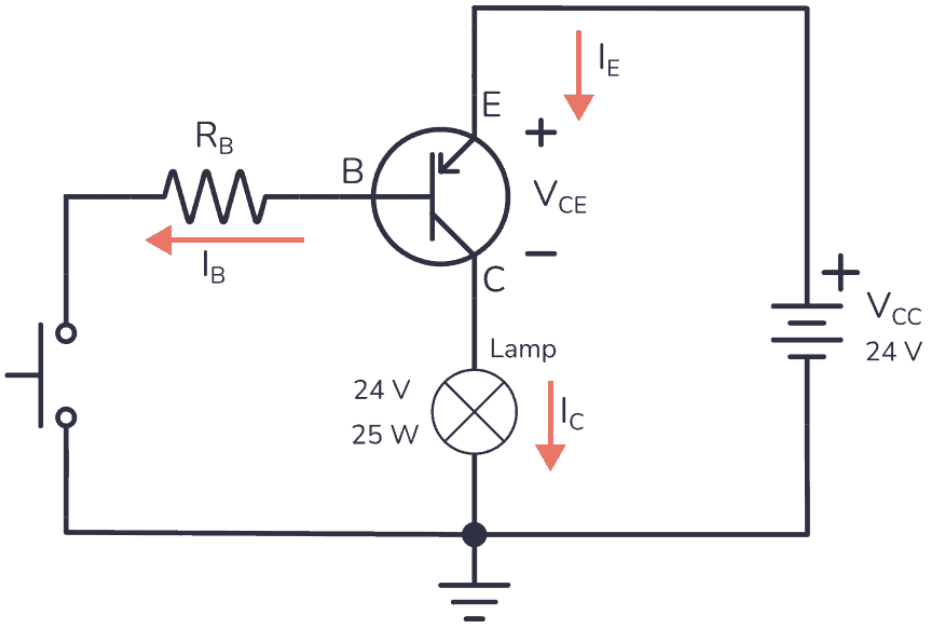
1.1.4.2 MOSFET (Metal Oxide Semiconductor Field Effect Transistor)

MOSFET, voltaj kontrolüyle çalışan ve modern dijital devrelerin neredeyse tamamında tercih edilen transistör türüdür. Şekil 1.7'de MOSFET'in fiziksel yapısı - gate, source, drain terminalleri ve oksit tabakası - gösterilmektedir. Gate-source gerilimi eşik değerini aştığında iletken kanal oluşur; bu

mekanizmanın voltaj-akım karakteristiği Şekil 1.8'de üç çalışma bölgesi (kesim, doğrusal ve doyum) üzerinden sunulmaktadır (Weste ve Harris, 2015).



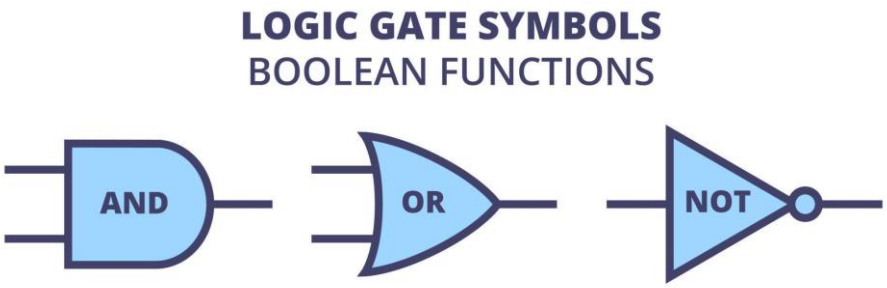
Şekil 1.7. MOSFET (n-kanal, arttırma tipi) yapısı: gate, source, drain ve oksit tabakası (Weste ve Harris, 2015'ten uyarlanmıştır).



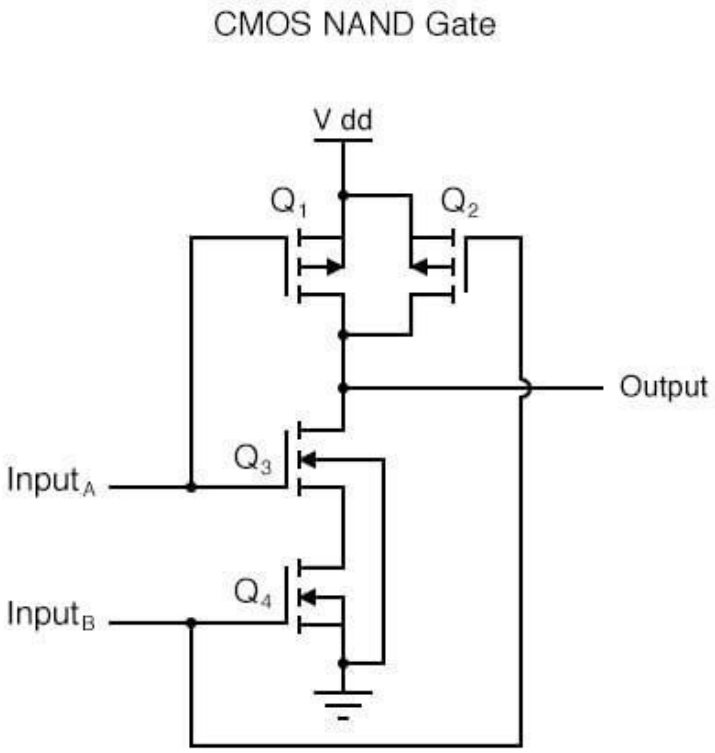
Şekil 1.8. MOSFET'in voltaj-akım karakteristiği ve üç çalışma bölgesi: kesim, doğrusal ve doyum (Weste ve Harris, 2015'ten uyarlanmıştır).

1.1.5 Mantık Kapıları (Logic Gates)

Birden fazla transistörün belirli bağlantı düzenlemesiyle bir araya getirilmesiyle Boole mantığını uygulayan mantık kapıları oluşmaktadır. Şekil 1.9'da AND, OR, NOT, NAND ve NOR kapılarının standart sembolik gösterimleri ve doğruluk tabloları verilmektedir. Şekil 1.10'da ise NAND kapısının CMOS teknolojisiyle transistör düzeyinde nasıl gerçekleştirildiği gösterilmektedir (Mano ve Ciletti, 2017).



Şekil 1.9. Temel mantık kapıları: AND, OR, NOT, NAND ve NOR; semboller ve doğruluk tabloları (Mano ve Ciletti, 2017'den uyarlanmıştır).

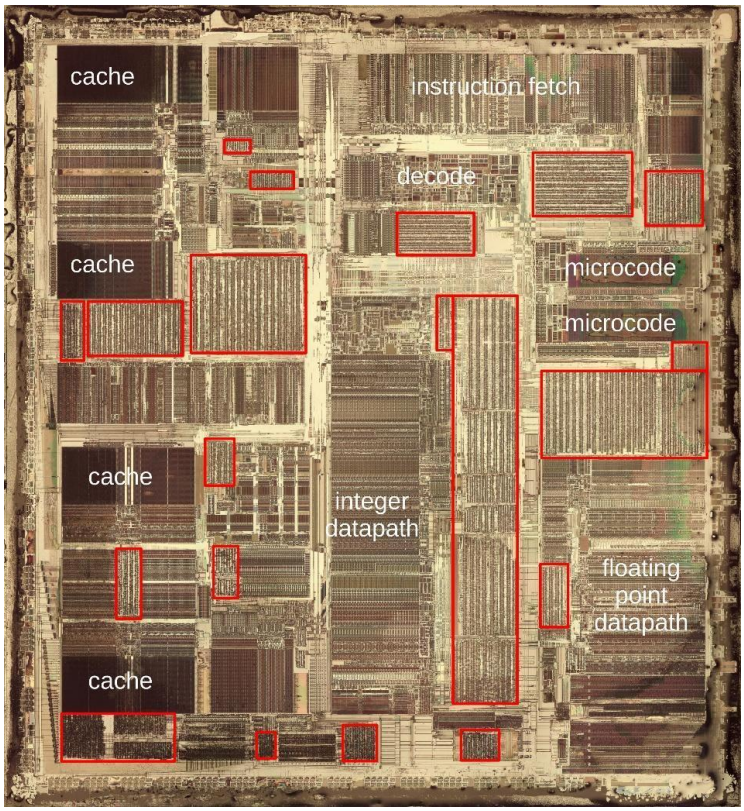


Şekil 1.10. NAND kapısının transistör düzeyinde CMOS gerçekleştirimi (Weste ve Harris, 2015'ten uyarlanmıştır).

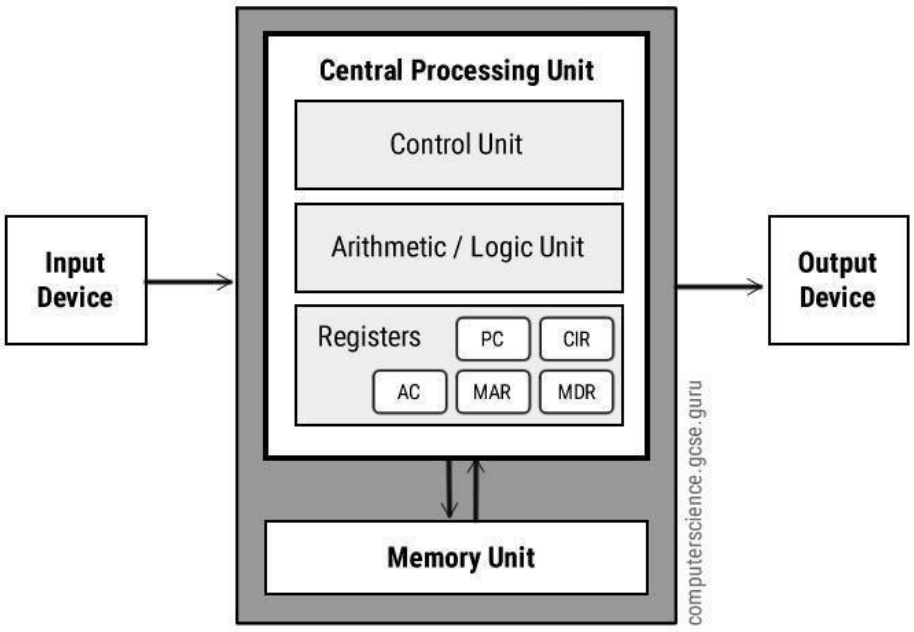
NAND Evrenselliği: Tüm bilgisayarlar yalnızca NAND kapısından inşa edilebilir. Herhangi bir Boole ifadesi, yalnızca NAND kapılarının kombinasyonuyla ifade edilebilmektedir (Harris ve Harris, 2021).

1.1.6 Transistörlerden Bilgisayara: Hiyerarşik Yapı

Bir işlemcinin transistörlerden başlayarak nasıl oluşturulduğu Şekil 1.11'de katmanlı soyutlama yapısı olarak gösterilmektedir. Bu hiyerarşi: Transistör → Mantık Kapısı → Kombinasyonel/Sıralı Devreler → ALU → CPU Core biçiminde ilerler. Şekil 1.12'de tipik bir CPU mimarisinin blok diyagramı - ALU, kontrol birimi, yazmaçlar ve önbellek bileşenleriyle birlikte - sunulmaktadır (Harris ve Harris, 2021).



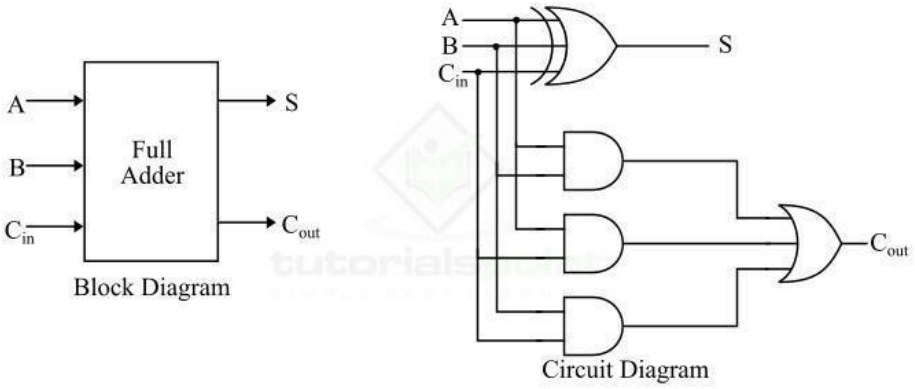
Şekil 1.11. İşlemci hiyerarşisi: transistörden CPU'ya uzanan katmanlı soyutlama yapısı (Harris ve Harris, 2021'den uyarlanmıştır).



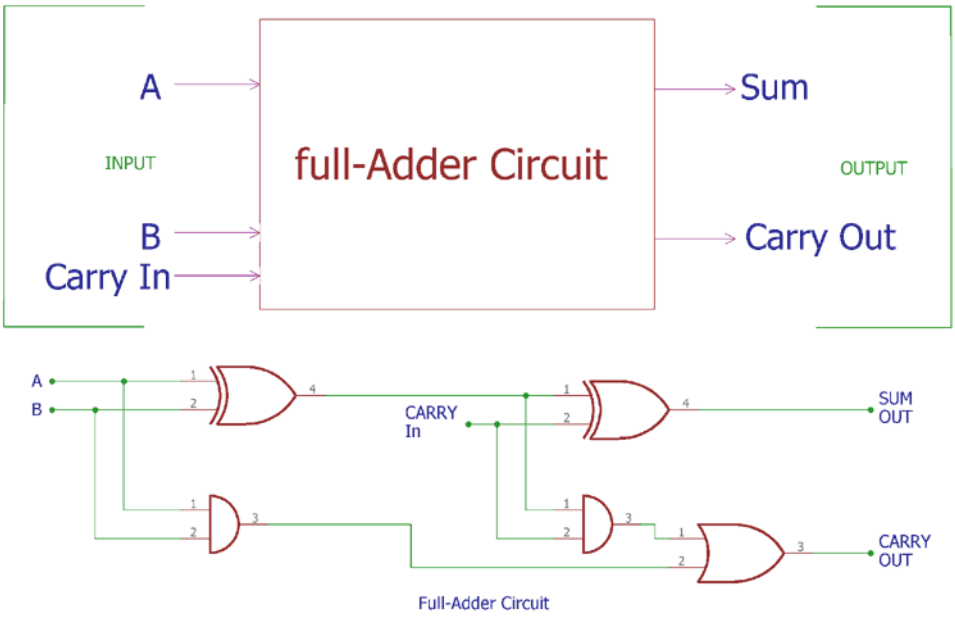
Şekil 1.12. Tipik bir CPU mimarisinin blok diyagramı: ALU, kontrol birimi, yazmaçlar ve önbellek (Harris ve Harris, 2021'den uyarlanmıştır).

Şekil 1.13'te modern bir işlemci çipinin silikon wafer üzerindeki yapısı görülmektedir. Transistör sayısındaki tarihsel büyüme ise Moore Yasası olarak bilinmekte ve Şekil 1.14'te grafiksel olarak sunulmaktadır. Gordon Moore, 1965 yılında entegre devre başına düşen transistör sayısının yaklaşık her iki yılda bir iki katına çıkacağını öngörmüştür (Weste ve Harris, 2015).

Bu yapı Şekil 1.13'te gösterilmektedir.



Şekil 1.13. Modern işlemci çipinin silikon wafer üzerindeki yapısı ve transistör yoğunluğu (Weste ve Harris, 2015'ten uyarlanmıştır).



Şekil 1.14. Entegre devre teknolojisinin transistör yoğunluğundaki tarihsel gelişimi - Moore Yasası (Weste ve Harris, 2015'ten uyarlanmıştır).

1.1.7 Yazılım ve Anahtarlama: Bir Sentez

Bir programda yer alan if (a > b) gibi koşullu bir ifade çalıştırıldığında, fiziksel düzeyde bit dizileri çıkarma devresi aracılığıyla işlenir; işaret bitine göre mantık kapıları çıktı üretir ve program akışı yönlenir. Yani yazılım, transistörlerin kontrollü açma-kapama örüntülerinin soyut bir organizasyonudur (Tanenbaum ve Austin, 2013).

1.2 Ardışıl Sayısal Devreler: Latch, Flip-Flop, Yazmaç ve Sayaç

Sayısal sistemler, bitten başlayarak daha karmaşık yapılara doğru hiyerarşik biçimde inşa edilir: bit → latch → flip-flop → yazmaç → sayaç. Bu inşa sürecinin her aşaması, bir öncekinin sınırlılıklarını giderir (Mano ve Ciletti, 2013).

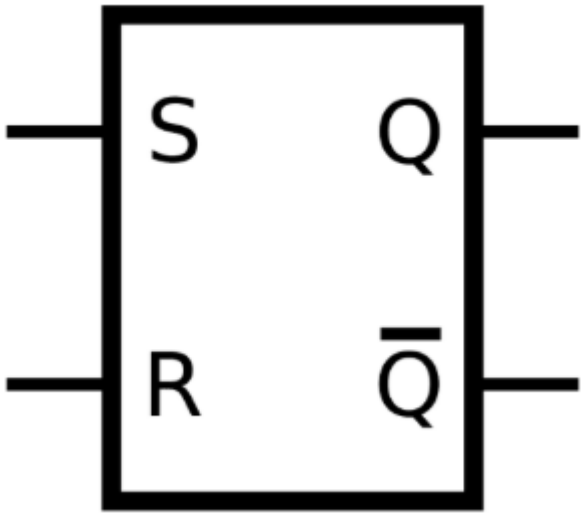
1.2.1 Bit: Bilginin En Küçük Birimi

Bit (binary digit), iki olası durumdan birini temsil eden en küçük bilgi birimidir. Wheeler'ın "it from bit" yaklaşımına göre her fiziksel nicelik, temel anlamını ikili bilgi göstergelerinden almaktadır (Foschini, 2013).

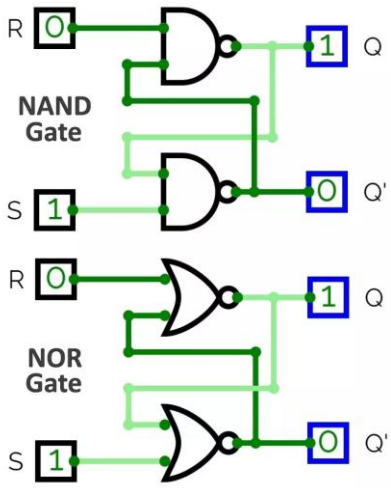
1.2.2 Latch Devreleri: Bitin Fiziksel Olarak Saklanması

1.2.2.1 SR Latch

En basit latch yapısı SR latch'tir. Şekil 1.15'te SR latch'in sembolü - S (Set) ve R (Reset) girişleri ile Q ve $\bar{Q}$ çıkışları - gösterilmektedir. Şekil 1.16'da ise hem NAND hem de NOR kapıları ile gerçekleştirilen SR latch devreleri ve doğruluk tabloları sunulmaktadır. SR latch'in önemli bir kısıtlaması, S ve R girişlerinin eş zamanlı etkinleştirilmesinin belirsiz çıkış durumuna yol açmasıdır; bu sorun D latch ile çözülmüştür (Mano ve Ciletti, 2013).



Şekil 1.15. SR latch sembolü: S (Set) ve R (Reset) girişleri ile Q ve $\bar{Q}$ çıkışları (Mano ve Ciletti, 2013'ten uyarlanmıştır).



SR Latch Truth Table

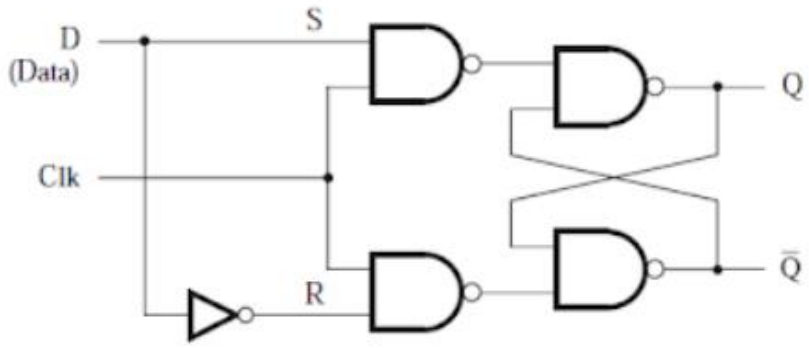
S	R	Q	Q'	State
0	0	Q	Q'	Hold (No Change)
0	1	0	1	Reset
1	0	1	0	Set
1	1	0	0	Invalid (Avoided)

Şekil 1.16. NAND ve NOR kapıları ile gerçekleştirilen SR latch devreleri ve doğruluk tabloları (Mano ve Ciletti, 2013'ten uyarlanmıştır).

1.2.2.2 D Latch ve Saat Kontrollü Çalışma

D latch, tek bir veri girişine sahip olan ve SR latch'teki yasak durumu ortadan kaldıran bir yapıdır. Devreye eklenen saat sinyali, latch'in ne zaman veri kabul edeceğini denetler. Karakteristik denklem (1.1)'de verilmiştir. Şekil 1.17'de D latch'in NAND kapıları ile gerçekleştirilmiş devre yapısı, karakteristik tablosu ve sembol gösterimi sunulmaktadır (Mano ve Ciletti, 2013).

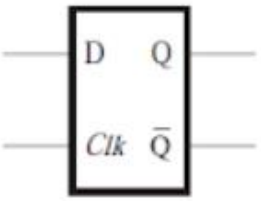
$Clk = 0 \rightarrow Q(t+1) = Q(t);\ Clk = 1 \rightarrow Q(t+1) = D(1.1)$



(a) Circuit

Clk	D	Q(t + 1)
0	x	Q(t)
1	0	0
1	1	1

(b) Characteristic table



(c) Graphical symbol

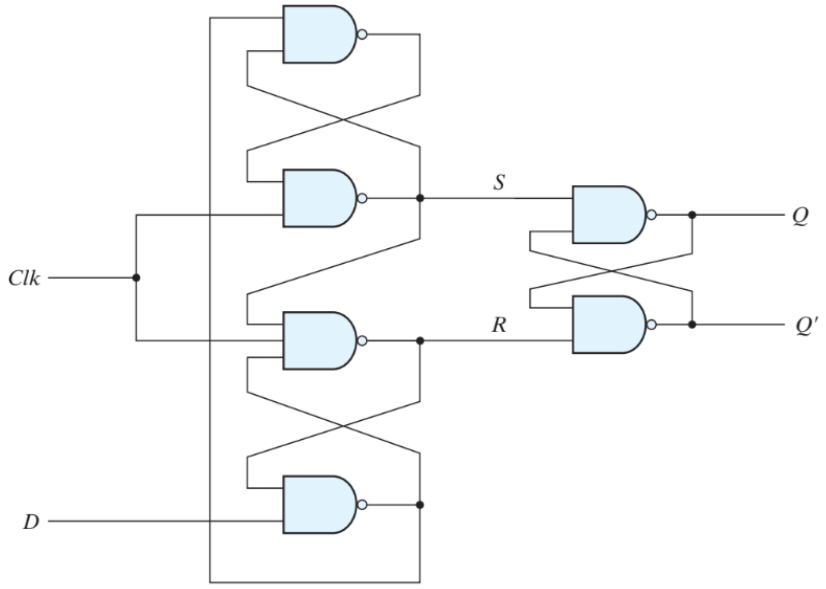
Şekil 1.17. NAND kapıları ile gerçekleştirilmiş kapılı D latch devresi, karakteristik tablosu ve sembol gösterimi (Mano ve Ciletti, 2013, s. 195'ten uyarlanmıştır).

1.2.3 Flip-Flop: Senkron Belleğin Temel Elemanı

1.2.3.1 D Tipi Flip-Flop (D-FF)

Flip-flop, saat sinyalinin yalnızca belirli bir kenar geçişinde durum değiştiren kenar tetiklemeli bir ardışıl devre elemanıdır. D tipi flip-flopun karakteristik denklemi (1.2)'de verilmiştir. Şekil 1.18'de D tipi pozitif kenar tetiklemeli flip-flopun kapı düzeyinde gerçekleştirilmiş devre yapısı gösterilmektedir (Mano ve Ciletti, 2013).

$$Q(t+1) = D \quad (1.2)$$



Şekil 1.18. D tipi pozitif kenar tetiklemeli flip-flopun kapı düzeyinde gerçekleştirilmiş devre yapısı (Mano ve Ciletti, 2013, s. 199'dan uyarlanmıştır).

1.2.3.2 Zamanlama Parametreleri

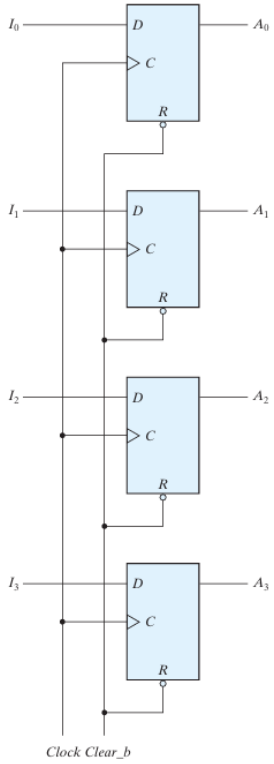
Kenar tetiklemeli flip-flopların doğru çalışabilmesi için giriş verisinin belirli zamanlama kısıtlarını sağlaması gerekmektedir. Tablo 1.2'de D flip-flopun temel zamanlama parametreleri özetlenmektedir. Bu parametreler, bir sayısal sistemin maksimum çalışma frekansını doğrudan belirler (Mano ve Ciletti, 2013).

Tablo 1.2. D flip-flopun temel zamanlama parametreleri.

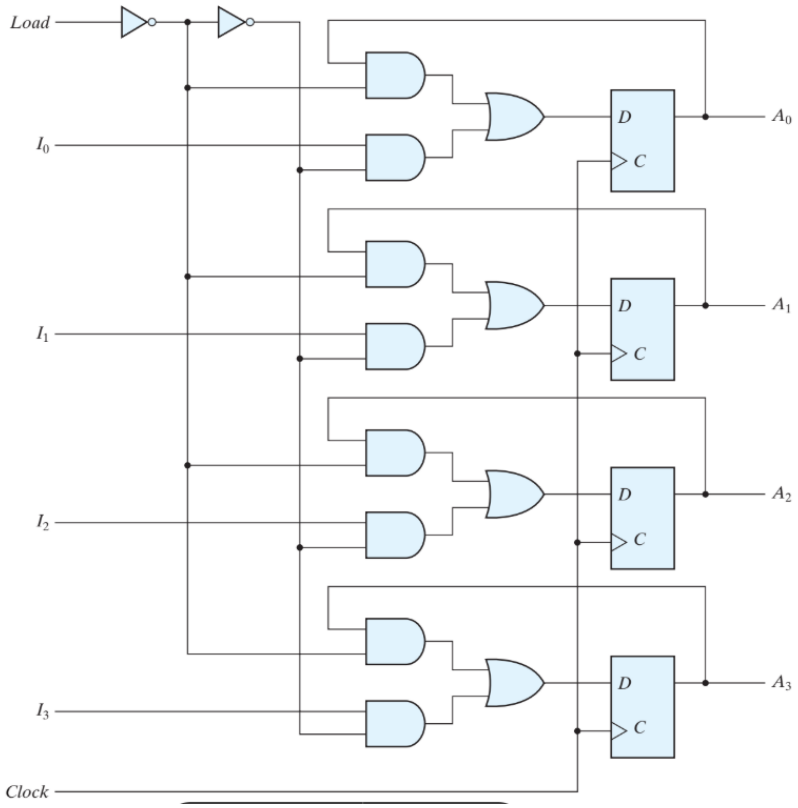
Parametre	Tanım
Kurulum süresi (setup time, tsu)	Saat aktif kenarından önce D girişinin sabit kalması gereken minimum süre
Tutma süresi (hold time, th)	Saat aktif kenarından sonra D girişinin değişmemesi gereken minimum süre
Yayılma gecikmesi (propagation delay, tpd)	Saat kenarından Q çıkışının yeni değerine ulaşması arasında geçen süre

1.2.4 Yazmaç (Register): Çok Bitli Bilgi Saklama

Yazmaç, ortak bir saat sinyaline bağlı birden fazla flip-floptan oluşan bir yapıdır. Şekil 1.19'da dört bitlik bir yazmaç yapısı gösterilmektedir; ortak saat darbesiyle tüm girişler eş zamanlı olarak çıkışlara aktarılır. Şekil 1.20'da ise yükleme denetimi eklenmiş paralel yüklemeli yazmaç yapısı sunulmaktadır (Mano ve Ciletti, 2013).



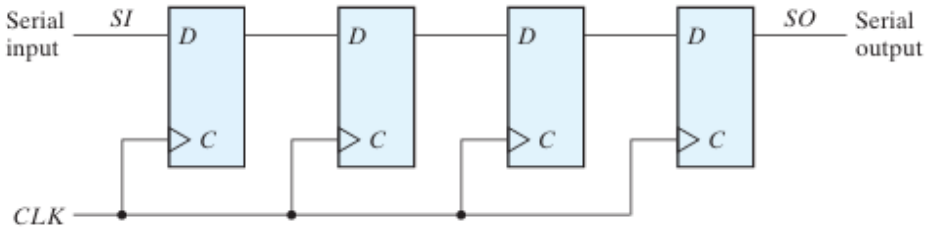
Şekil 1.19. D tipi flip-floplardan oluşturulmuş dört bitlik yazmaç yapısı (Mano ve Ciletti, 2013, s. 256'dan uyarlanmıştır).



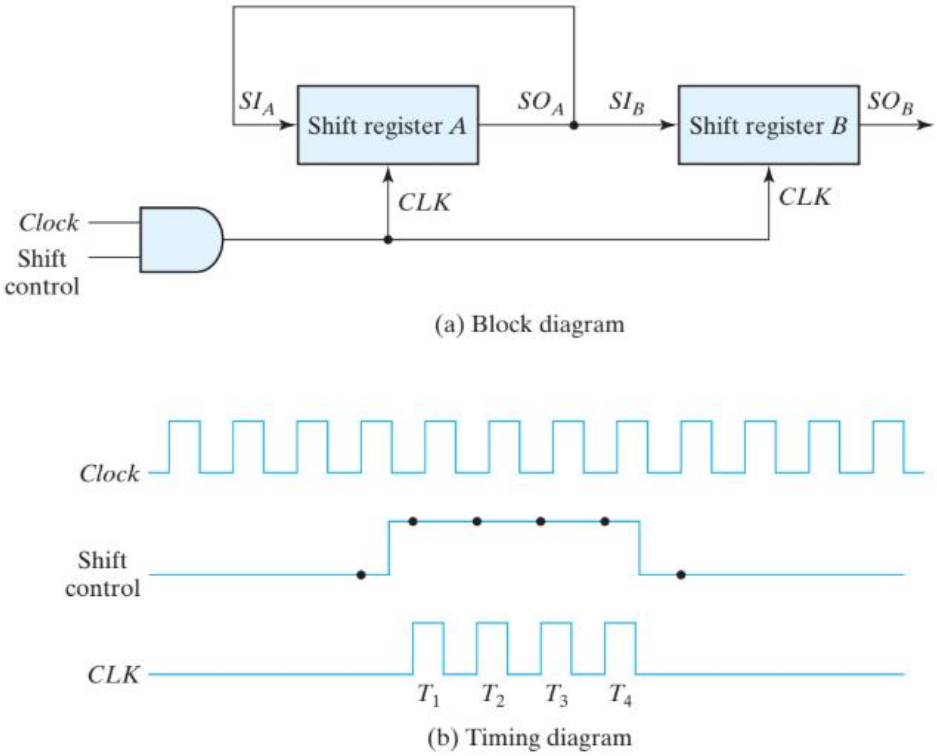
Şekil 1.20. Paralel yüklemeli dört bitlik yazmaç yapısı (Mano ve Ciletti, 2013, s. 256'dan uyarlanmıştır).

1.2.5 Kaydırmalı Yazmaç (Shift Register) ve Seri Veri Aktarımı

Kaydırmalı yazmaç, saklanan bilginin konumunu değiştirebilen bir yazmaç türüdür. Şekil 1.21'de dört bitlik bir kaydırmalı yazmaç yapısı, Şekil 1.22'de ise yazmaç A'dan yazmaç B'ye seri veri aktarımı gösterilmektedir. İki aktarım yönteminin karşılaştırması Tablo 1.3'te sunulmaktadır (Mano ve Ciletti, 2013).



Şekil 1.21. Dört bitlik kaydırmalı yazmaç yapısı (Mano ve Ciletti, 2013, s. 259'dan uyarlanmıştır).



Şekil 1.22. Yazmaç A'dan yazmaç B'ye seri veri aktarımı (Mano ve Ciletti, 2013, s. 260'tan uyarlanmıştır).

Tablo 1.3. Seri ve paralel veri aktarımı yöntemlerinin karşılaştırması.

Özellik	Paralel Aktarım	Seri Aktarım
Aktarım hızı	Tek saat darbesi	n saat darbesi
Donanım hattı	n hat	1 hat
Tipik kullanım	İşlemci içi aktarım	UART, SPI

1.2.6 Sayaç (Counter): Ardışıl Durum Makinesi

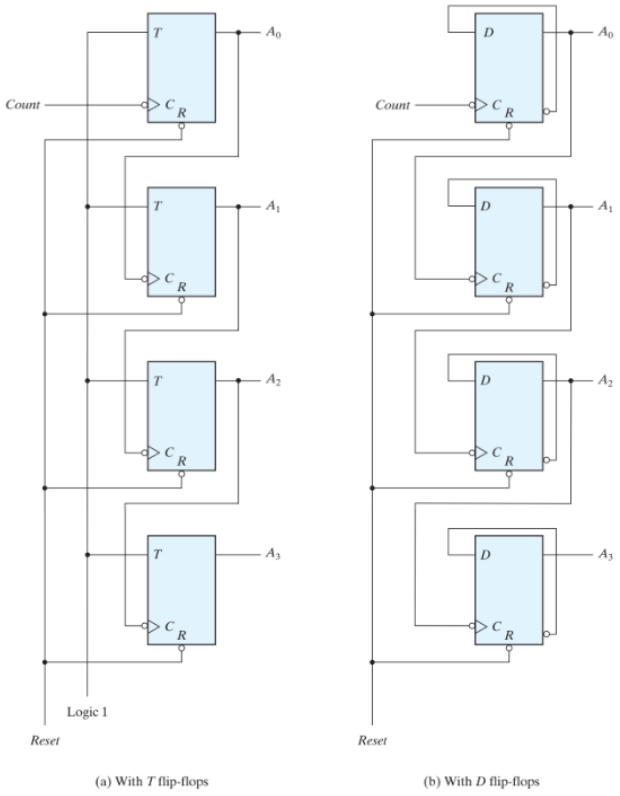
Sayaç, önceden belirlenmiş bir durumlar dizisi boyunca ilerleyen ardışıl devredir. Şekil 1.23'te dört bitlik bir ikili sayacın durum dizisi gösterilmektedir. Asenkron (ripple) tasarımın devre yapısı Şekil

1.24’te, senkron tasarım Şekil 1.25’te ve ileri-geri sayaç Şekil 1.26’da sunulmaktadır. İki yaklaşımın karşılaştırması Tablo 1.4’te özetlenmektedir (Mano ve Ciletti, 2013).

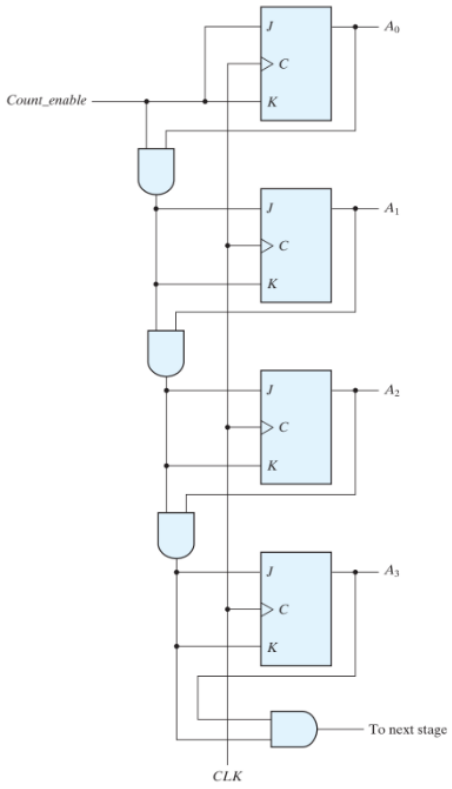
Binary Count Sequence

A_3	A_2	A_1	A_0
0	0	0	0
0	0	0	1
0	0	1	0
0	0	1	1
0	1	0	0
0	1	0	1
0	1	1	0
0	1	1	1
1	0	0	0

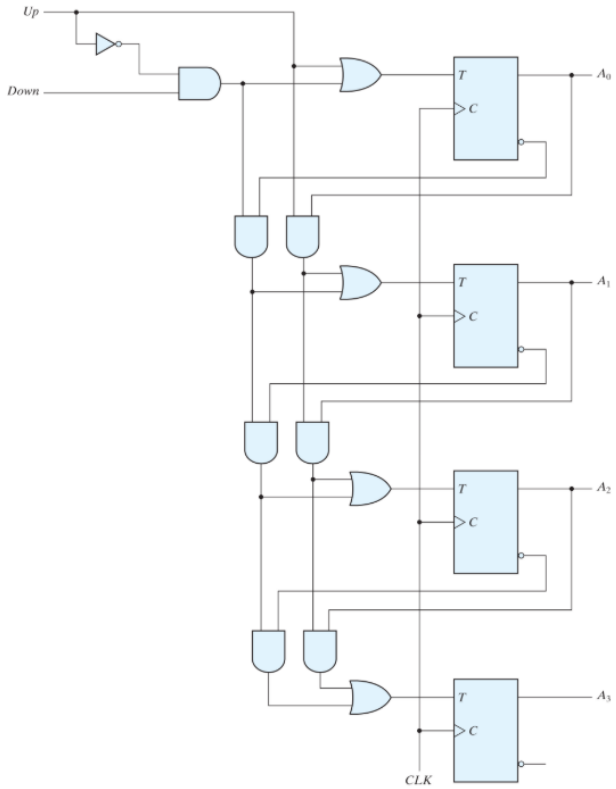
Şekil 1.23. Dört bitlik ikili sayacın durum dizisi (Mano ve Ciletti, 2013, s. 267'den uyarlanmıştır).



Şekil 1.24. Dört bitlik asenkron (ripple) ikili sayaç (Mano ve Ciletti, 2013, s. 266'dan uyarlanmıştır).



Şekil 1.25. Dört bitlik senkron ikili sayaç (Mano ve Ciletti, 2013, s. 273'ten uyarlanmıştır).



Şekil 1.26. Dört bitlik senkron ileri-geri sayaç - Up-Down Counter (Mano ve Ciletti, 2013, s. 274'ten uyarlanmıştır).

Tablo 1.4. Asenkron ve senkron sayaçların karşılaştırmalı özeti.

Özellik	Asenkron (Ripple)	Senkron
Saat yapısı	Zincirleme	Ortak saat
Gecikme	Bit sayısıyla orantılı	Sabit
Hız	Düşük-orta frekans	Yüksek frekans
Tipik kullanım	Frekans bölücü	İşlemci sayacı

1.3 Qubit ve Dolanıklık (Entanglement)

Kuantum hesaplamanın teorik temelini anlayabilmek için klasik bitten kuantum bite geçişi kavramsal düzeyde sağlamlaştırmak gerekmektedir. Bu geçiş; durum uzayının genişlemesini, ölçüm dinamiklerinin dönüşümünü ve dolanıklık korelasyonunun klasik fiziğin sınırlarını aşmasını ifade eder (Rieffel ve Polak, 2011; Bernhardt, 2019).

1.3.1 Qubit Nedir? Klasik Bitten Kuantum Bite Geçiş

Kuantum mekaniği, Schrödinger denkleminin doğrusal yapısı sayesinde süperpozisyon ilkesini mümkün kılmakta ve bitin ötesine geçen qubit (kübit) kavramını doğurmaktadır (Nielsen ve Chuang, 2010). Qubitin en genel saf durumu (1.3) numaralı denklemde verilmiştir; normalizasyon koşulu ise (1.4)'te tanımlanmıştır. Klasik bit ile qubit arasındaki temel farklar Şekil 1.27'de görselleştirilmiş, Tablo 1.5'te ise sistematik biçimde karşılaştırılmıştır.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1.3)$$

$$|\alpha|^2 + |\beta|^2 = 1 \quad (1.4)$$



Şekil 1.27. Klasik bitin iki ayrık durumu (sol) ile qubitin sürekli durum uzayı (sağ) (Rieffel ve Polak, 2011'den uyarlanmıştır).

Tablo 1.5. Klasik bit ve qubitin karşılaştırması.

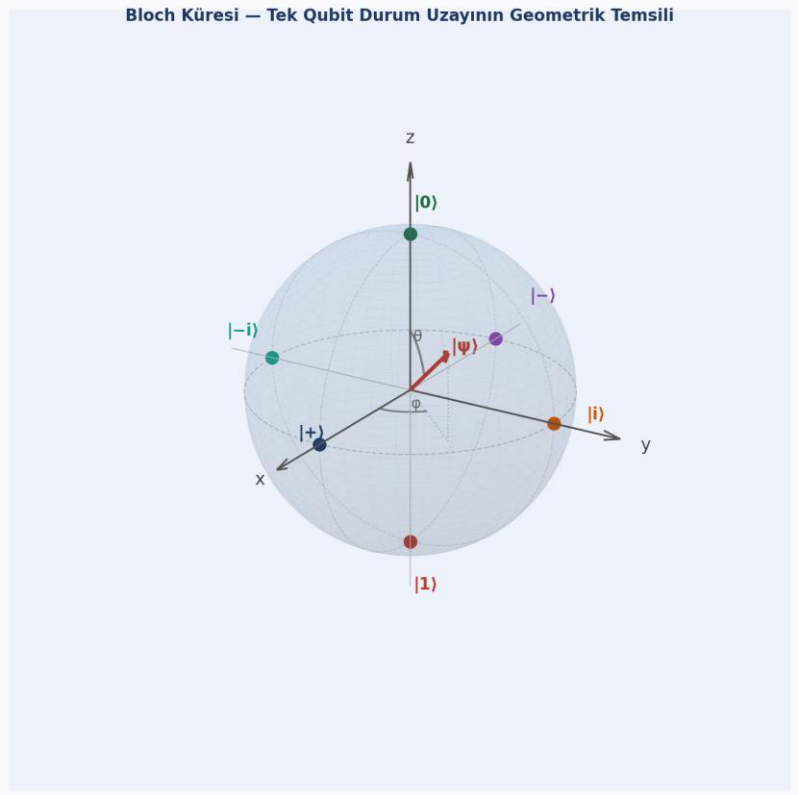
Özellik	Klasik Bit	Qubit
Durum uzayı	{0,1} - ayrık 2 nokta	2B kompleks Hilbert uzayı
Kopyalanabilirlik	Serbestçe kopyalanabilir	Kopyalanamaz (no-cloning)
Ölçüm etkisi	Durumu değiştirmez	Dalga fonksiyonunu çökertir
Korelasyon türü	Yalnızca klasik	Klasik + kuantum (dolanıklık)

1.3.2 Qubitin Geometrik Temsili: Bloch Küresi

Tek bir qubitin durum uzayı, Bloch küresi olarak bilinen birim küre yüzeyindeki noktalara karşılık gelir. Denklem (1.5)'te verilen parametrizasyonla qubit durumu iki açısal parametre ile ifade edilir. Şekil

1.28’de Bloch küresi üzerindeki temel qubit durumlarının konumları -- gösterilmektedir (Kofler, 2025; Bernhardt, 2019). |0⟩ kuzey kutbunda, |1⟩ güney kutbunda, |+⟩ ve |−⟩ ekvatorda

$$|\psi(\theta,\varphi)\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle \quad (1.5)$$



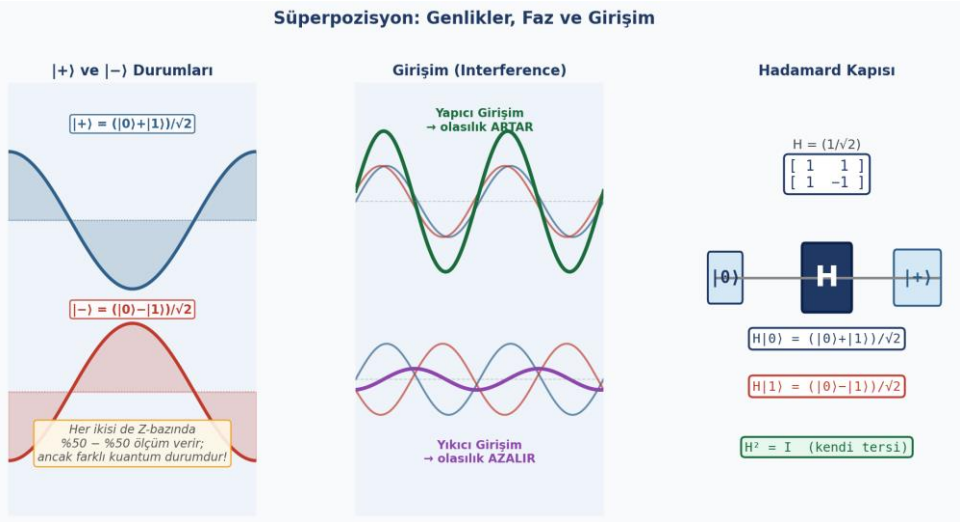
Şekil 1.28. Bloch küresi üzerinde temel qubit durumları (Nielsen ve Chuang, 2010'dan uyarlanmıştır).

1.3.3 Süperpozisyon (Superposition)

Süperpozisyon "qubit aynı anda hem 0 hem 1'dir" şeklinde yorumlanamaz; qubit, ölçümden önce |0⟩ ve |1⟩ temel durumlarının genliklerle ağırlıklandırılmış bir bileşimi olarak tek bir vektörle temsil edilir (Bernhardt, 2019). Hadamard kapısı ile eşit ağırlıklı süperpozisyon üretimi (1.6) ve (1.7) numaralı denklemlerde gösterilmektedir. Bu süreç - olasılık genlikleri, Born kuralına göre ölçüm olasılıkları ve dalga fonksiyonu çökmesi - Şekil 1.29’da görselleştirilmiştir (Allen, 2024).

$$H|0\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle) = |+\rangle \quad (1.6)$$

$$H|1\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle) = |-\rangle \quad (1.7)$$



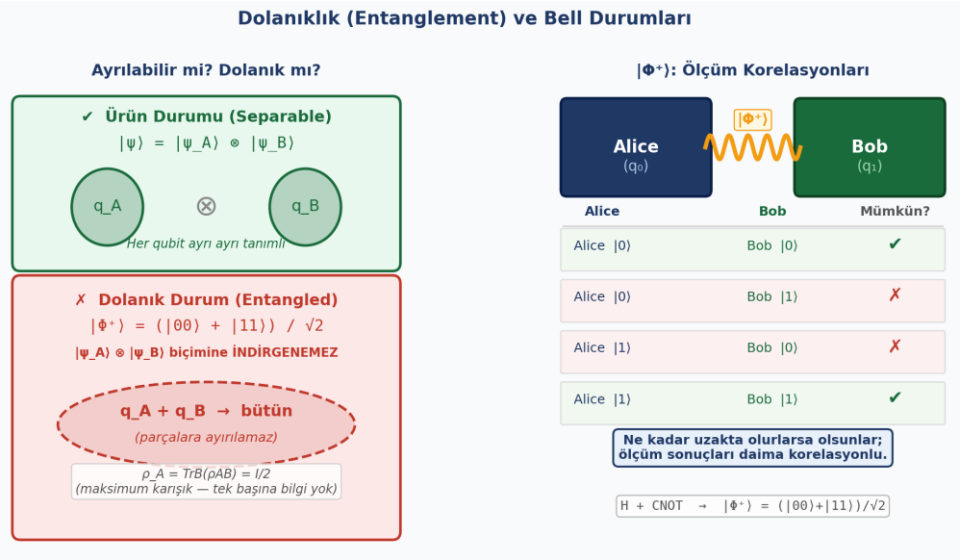
Şekil 1.29. Süperpozisyon: olasılık genlikleri (sol), Born kuralına göre ölçüm olasılıkları (orta) ve dalga fonksiyonu çökmesi (sağ) (Rieffel ve Polak, 2011'den uyarlanmıştır).

Süperpozisyon tek başına hesaplamalı üstünlük sağlamaz; asıl güç girişim (interference) olgusundan doğar. Yapıcı girişim istenen çıktıların genliğini artırırken, yıkıcı girişim istenmeyen çıktıların genliğini sıfıra yaklaştırır (Bernhardt, 2019).

1.3.4 Ölçüm Problemi (Measurement Problem)

Ölçüm sonuçlarının olasılıkları Born kuralı ile belirlenir ve (1.8) numaralı denklemde formüle edilmiştir. Şekil 1.30'da ölçüm sürecinin iki yönü gösterilmektedir: $|+\rangle$ süperpozisyon durumundan Z-bazında ölçümün çöküşü (sol) ve çok sayıda tekrarla ortaya çıkan istatistiksel dağılım (sağ). Ölçümün temele bağımlılığı, kuantum bilgi işlemde temel bir tasarım kararıdır (Kaye vd., 2007; de Wolf, 2023).

$$P(|0\rangle) = |\alpha|^2, \quad P(|1\rangle) = |\beta|^2, \quad |\alpha|^2 + |\beta|^2 = 1 \quad (1.8)$$

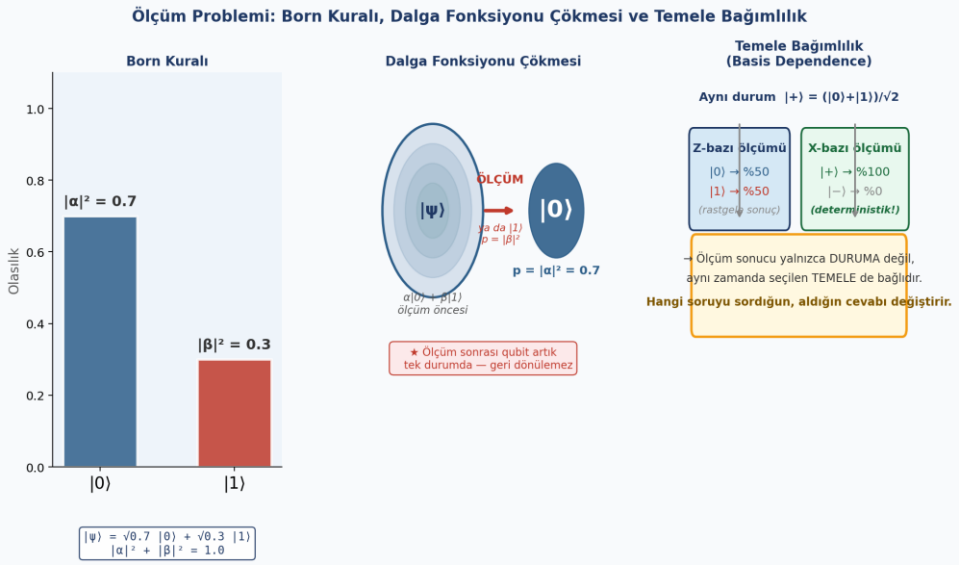


Şekil 1.30. Ölçüm problemi: $|+\rangle$ durumundan Z-bazında ölçümün çöküşü (sol) ve istatistiksel dağılım (sağ) (Kofler, 2025'ten uyarlanmıştır).

1.3.5 Dolanıklık (Entanglement)

İki qubitlik sistemin en genel saf durumu (1.9) numaralı denklemde verilmiştir. Dolanıklık, bazı birleşik kuantum durumlarının alt sistemlerin ayrı ayrı durumlarıyla açıklanamaması olgusudur. Şekil 1.31'de Bell durumu devresi -- gösterilmekte; histogram yalnızca 00 ve 11 çıktılarını yansıtarak dolanıklığın korelasyon yapısını ortaya koymaktadır (Rieffel ve Polak, 2011; Kofler, 2025). H + CNOT ile |00⟩'dan |Φ⁺⟩ üretimi

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \quad |a|^2+|b|^2+|c|^2+|d|^2 = 1 \ (1.9)$$



Şekil 1.31. Bell durumu devresi: H + CNOT ile |00⟩'dan |Φ⁺⟩ = (|00⟩+|11⟩)/√2 üretimi (Nielsen ve Chuang, 2010'dan uyarlanmıştır).

1.3.6 Bell Durumları (Bell States)

Bell durumları, iki qubit için maksimum dolanık saf durumların oluşturduğu ailedir ve (1.10a–d) numaralı denklemlerde tanımlanmıştır. |00⟩ başlangıcından |Φ⁺⟩ üretimi (1.11) ve (1.12) numaralı denklemlerde adım adım gösterilmektedir (Rieffel ve Polak, 2011; Kofler, 2025).

$$|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle) \qquad |\Phi^-\rangle = (1/\sqrt{2})(|00\rangle - |11\rangle) \ (1.10a,b)$$

$$|\Psi^+\rangle = (1/\sqrt{2})(|01\rangle + |10\rangle) \qquad |\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle) \ (1.10c,d)$$

$$(H \otimes I)|00\rangle = (1/\sqrt{2})(|00\rangle + |10\rangle) \ (1.11)$$

$$CNOT \cdot (1/\sqrt{2})(|00\rangle + |10\rangle) = (1/\sqrt{2})(|00\rangle + |11\rangle) = |\Phi^+\rangle \ (1.12)$$

1.4 Kuantum Algoritmalar, Kriptografik Tehditler ve Donanım Sınırlılıkları

Kuantum bilişim, belirli problem sınıflarının hesaplama karmaşıklığını kökten dönüştüren yeni bir paradigmadır. Bu kısımda Shor ve Grover algoritmaları karşılaştırmalı biçimde ele alınmakta; kriptografik etkileri, kuantum aydınlatma ve NISQ sınırlılıkları tartışılmaktadır (Shor, 1997; Grover, 1996).

1.4.1 Shor Algoritması: Periyot Bulma ile Çarpanlara Ayırma

Shor algoritmasının temel fikri, büyük bir tamsayının çarpanlarına ayrılmasını modüler üstel bir fonksiyonun periyodunu bulmaya indirgemektir. QFT, periyodik yapının frekans alanında görünür hale gelmesini sağlar. Tablo 1.6'da N = 15 ve a = 7 için Shor algoritmasının adım adım çalışması gösterilmektedir: periyot r = 4 bulunduğunda gcd($7^2 - 1$, 15) = 3 ve gcd($7^2 + 1$, 15) = 5 sonuçlarıyla 15 = 3 × 5 çarpanlarına ulaşılır (Shor, 1997).

Tablo 1.6. N = 15, a = 7 için Shor algoritması adım adım.

x	7^x mod 15	Açıklama
0	1	Başlangıç
1	7	
2	4	
3	13	
4	1	Periyot: r = 4
5	7	Yineleme başlar

1.4.2 Grover Algoritması: Genlik Yükseltme ile Yapısız Arama

Grover algoritması, N aday arasında doğru cevabı O(√N) karmaşıklıkla bulur. Tablo 1.7'de 4 qubitlik bir Grover simülasyonunun sonuçları sunulmaktadır: yalnızca 3 iterasyonla hedef durumun bulunma olasılığı %96.1'e ulaşmaktadır. İki algoritmanın karşılaştırmalı özeti Tablo 1.8'de verilmiştir (Grover, 1996).

Tablo 1.7. qubitlik Grover simülasyonu sonuçları (hedef: \|1011⟩).

Aşama	P(|1011⟩)	Açıklama
Başlangıç	0.0625	Eşit süperpozisyon
İterasyon 1	0.4727	Genlik yükseltme
İterasyon 2	0.9084	Genlik yükseltme
İterasyon 3	0.9613 (%96.1)	Optimal iterasyon

Tablo 1.8. Shor ve Grover algoritmalarının karşılaştırmalı özeti.

Özellik	Shor	Grover
Hedef problem	Tamsayı çarpanlama	Yapısız arama
Klasik karmaşıklık (n: bit sayısı)	O(exp(n^(1/3)))	O(N)

Özellik	Shor	Grover
Kuantum karmaşıklık	$O(n^3 \log n \log\log n)$	$O(\sqrt{N})$
Hızlanma tipi	Üstel	Karesel
Kriptografik etki	RSA/ECC'yi tehdit eder	Anahtar boyutu etkisi

1.4.3 RSA ile İlişkisi: Kriptografik Güvenlik Üzerindeki Etki

RSA şifrelemesinin güvenliği, büyük bileşik sayıların çarpanlara ayrılmasının pratikte aşılmaz olduğu varsayımına dayanır. Shor algoritması bu varsayımı doğrudan hedef almaktadır. Gidney ve Ekerå (2021), RSA-2048 için yaklaşık 20 milyon gürültülü qubit öngörmüştür; 2025 tarihli bir güncelleme bu tahmini belirli varsayımlar altında bir milyonun altına indirmektedir (Gidney, 2025). "Şimdi topla, sonra çöz" stratejisi, uzun ömürlü veriler için hâlihazırda ciddi bir risk oluşturmaktadır (NIST, 2024).

1.4.4 Kuantum Aydınlatma (Quantum Illumination): Algılamada Kuantum Korelasyonları

Lloyd (2008) tarafından formüle edilen kuantum aydınlatma yaklaşımında, kaynakta üretilen iki korelasyonlu moddan biri hedefe gönderilirken diğeri yerelde tutulur. Yakın vadede beklenen sonuç, belirli algılama rejimlerinde niş üstünlükler sağlayan hibrit çözümlerdir (Barzanjeh vd., 2015; Karsa vd., 2024).

1.4.5 Günümüzün Sınırlamaları: Hata Toleransı ve NISQ Rejimi

Qubitler dekoheranstan kolayca bozulur; pratik bir kuantum bilgisayar hataları bastırabilen mantıksal qubitler gerektirmektedir. Hata toleranslı hesaplama için gereken bileşenler Tablo 1.9'da özetlenmektedir. Google'ın 2025 sonuçları yüzey kodlarında mantıksal hata oranının bastırılabildiğini göstermekle birlikte, büyük ölçekli faydalı hesaplamaya henüz geçilmemiştir (Acharya vd., 2025; Preskill, 2018; Newman ve Satzinger, 2024).

Tablo 1.9. Hata toleranslı kuantum hesaplama için gereken bileşenler.

Gereksinim	Açıklama
Düşük kapı hata oranı	Her mantıksal kapının yeterince güvenilir olması
Güvenilir ölçüm	Ölçüm hatalarının devre sonuçlarını bozmaması
Hata düzeltme kodları	Yüzey kodu veya benzeri protokollerle hataların bastırılması
Gerçek zamanlı klasik denetim	Hataların anlık tespit ve düzeltme döngüsü
Mantıksal qubit üretimi	Birden fazla fiziksel qubitten tek bir hata toleranslı mantıksal qubit

1.4.6 Simülasyon Örnekleri: Python ve Qiskit Uygulamaları

Kapsam sınırlılığı notu: Aşağıdaki kod örnekleri yalnızca eğitim amaçlıdır; algoritmik mantığı küçük ölçekli sistemlerde görünür kılmayı hedefler. Örnekler büyük ölçekli hata toleranslı kuantum hesaplamayı taklit etmez; gerçek donanımda gürültü, dekoherans ve kapı hataları nedeniyle sonuçlar ideal simülasyonlardan sapma gösterecektir. NumPy örnekleri durum vektörü üzerinde çalışır ve qubit sayısı arttıkça bellek gereksinimi üstel olarak büyür. Qiskit örnekleri AerSimulator ile gürültüsüz ideal simülasyon ortamında yürütülmektedir.

1.4.6.1 Grover Algoritması - NumPy Simülasyonu

Kod 1.1. Grover algoritması - NumPy durum vektörü simülasyonu. Bu kod yalnızca ideal durum vektörü evrimi üzerinde çalışır; gerçek kuantum donanımındaki gürültü ve dekoherans etkileri modellenmemektedir.

```
import numpy as np

def grover_algorithm(n_qubits: int, target_state: int) -> np.ndarray:
 N = 2 ** n_qubits
 state = np.ones(N, dtype=float) / np.sqrt(N)
 optimal_iterations = int(np.round(np.pi / 4 * np.sqrt(N)))
 for _ in range(optimal_iterations):
 state[target_state] *= -1 # oracle: faz işareti
 mean = np.mean(state)
 state = 2 * mean - state # diffusion operatörü
 return np.abs(state) ** 2

probs = grover_algorithm(n_qubits=4, target_state=11)
# Çıktı: Hedef |1011> bulma olasılığı: 0.9613
```

1.4.6.2 Grover Algoritması - Qiskit Devresi

Kod 1.2. Grover algoritması - 2 qubitlik Qiskit devresi (hedef: |11⟩). Bu minimal örnek, oracle için CZ; diffusion için H-X-CZ-X-H sıralamasını kullanır. Daha büyük sistemlerde oracle ve diffusion operatörlerinin genelleştirilmiş tasarımı gereklidir.

```
from qiskit import QuantumCircuit, transpile
from qiskit_aer import AerSimulator

qc = QuantumCircuit(2, 2)
qc.h([0, 1]); qc.barrier()
qc.cz(0, 1); qc.barrier()
qc.h([0, 1]); qc.x([0, 1]); qc.cz(0, 1); qc.x([0, 1]); qc.h([0, 1])
qc.barrier(); qc.measure([0, 1], [0, 1])

sim = AerSimulator()
result = sim.run(transpile(qc, sim), shots=1024).result()
# Çıktı: {'11': 1024} - ideal simülatörde tüm atışlarda hedef durum
```

1.4.6.3 Shor Algoritması - Klasik Periyot Bulma Simülasyonu

Kod 1.3. Shor algoritması - klasik periyot bulma simülasyonu. Bu kod kuantum devresi içermez; yalnızca Shor'un cebirsel mantığını (periyot bulma → çarpan elde etme) klasik Python akışıyla göstermektedir. Gerçek Shor uygulaması QFT tabanlı kuantum devresi gerektirir.

```
from math import gcd
import numpy as np

def shor_algorithm(N):
 np.random.seed(42)
 for _ in range(10):
 a = np.random.randint(2, N)
 g = gcd(a, N)
 if g != 1: return (g, N // g)
 r = 1
 while pow(a, r, N) != 1: r += 1
 if r % 2 != 0: continue
 x = pow(a, r // 2, N)
 if x == N - 1: continue
 f1, f2 = gcd(x+1, N), gcd(x-1, N)
 if 1 < f1 < N: return (f1, f2)
 return None

# Çıktı: 15->(5,3) | 21->(3,7) | 35->(5,7) | 77->(11,7)
```

1.5 Bölüm Özeti ve Bir Sonraki Bölüme Geçiş

Bu bölümde modern bilişim teknolojisinin fiziksel ve kavramsal temelleri, klasik hesaplamadan kuantum paradigmaya uzanan bütüncül bir çerçeve içinde ele alınmıştır.

İlk kısımda (1.1), ikili sayı sistemi ve elektriksel temsil (Tablo 1.1), anahtarlama mekanizması (Şekil 1.1–1.4), transistör teknolojisi (Şekil 1.5–1.8), mantık kapıları (Şekil 1.9–1.10) ve işlemci hiyerarşisi (Şekil 1.11–1.14) sistematik biçimde ortaya konulmuştur.

İkinci kısımda (1.2), latch devreleri (Şekil 1.15–1.17), flip-flop yapısı (Şekil 1.18, Tablo 1.2), yazmaçlar (Şekil 1.19–1.22, Tablo 1.3) ve sayaçlar (Şekil 1.23–1.26, Tablo 1.4) bitten sayaca uzanan hiyerarşi içinde incelenmiştir.

Üçüncü kısımda (1.3), qubit kavramı (Şekil 1.27, Tablo 1.5), Bloch küresi (Şekil 1.28), süperpozisyon (Şekil 1.29), ölçüm problemi (Şekil 1.30) ve dolanıklık ile Bell durumları (Şekil 1.31) ele alınmıştır.

Dördüncü kısımda (1.4), Shor algoritması (Tablo 1.6), Grover algoritması (Tablo 1.7–1.8), kriptografik etkiler, kuantum aydınlatma ve NISQ sınırlılıkları (Tablo 1.9) somut simülasyon örnekleriyle (Kod 1.1–1.3) tartışılmıştır.

Bir sonraki bölümde (Bölüm 2), kuantum kapı modeli ve devre tasarımı sistematik biçimde ele alınacaktır. Bu bölümde tanıtılan Hadamard, CNOT ve kontrollü kapıların devre düzeyinde gerçekleştirimi incelenerek Shor ve Grover algoritmalarının fiilen uygulanabilir devre yapıları olarak nasıl kurgulandığı gösterilecektir.

BÖLÜM 2

Kuantum Kapıları, Dolanıklık ve Kuantum Devreleri

Bu bölümde, kuantum hesaplamanın temel işlem birimleri olan kuantum kapıları incelenmektedir. Özellikle Hadamard ve CNOT kapıları üzerinden süperpozisyon ve dolanıklık kavramlarının nasıl oluşturulduğu açıklanmakta, ayrıca kuantum devrelerinin çalışma mantığı ele alınmaktadır. Böylece kuantum algoritmalarının temelini oluşturan kapı tabanlı hesaplama yaklaşımı kavramsal olarak ortaya konulmaktadır.

2.1 Lojik Kapılar, İkili Aritmetik ve Evrensel Hesaplama

2.1.1 Bit: Bilginin Atomik Birimi

Klasik hesaplama kuramının en temel soyutlama birimi olan bit (binary digit - ikili basamak), yalnızca iki ayrık durumdan (0 ve 1) birini alabilen bir enformasyon ölçütüdür. Bilgi kuramı açısından, eş olasılıklı iki durumlu bir sistemde bir bitin taşıdığı bilgi miktarı Shannon entropisi ile tanımlanır (Shannon, 1948). Bu bağlamda Denklem (2.1)'de gösterildiği üzere, iki eş olasılıklı durum için entropi değeri 1 bit olmaktadır.

$H = log_2(2) = 1$ *(Shannon, C. E. 1948) (2.1)*

Bu iki durumlu yapı, soyut matematiksel düzeyde Boole mantığının temellerini oluştururken, fiziksel sistemlerde farklı ve kararlı durumlara karşılık gelecek biçimde gerçeklenir.

Bilgisayar biliminin operasyonel gücü, tam olarak bu noktadaki **eşikleme (thresholding)** ve **ayrıklaştırma (discretization)** mekanizmalarında yatar. Fiziksel dünyadaki sürekli ve gürültülü süreçler, bu mekanizmalar aracılığıyla iki kararlı ve yalıtılmış mantıksal sınıfa indirgenir. Dolayısıyla bit, yalnızca fiziksel bir sinyalin taşıyıcısı değil; karmaşık bilgi işleme süreçlerini iki değerli mantık sistemi üzerinden güvenilir ve ölçeklenebilir kılan ontolojik bir soyutlama aracıdır.

Fiziksel gerçekleştirim bağlamında bu soyutlama, mantıksal 0 ve 1 değerlerini belirli bir gerilim eşiğiyle temsil eden anahtarlama elemanları aracılığıyla somutlaşır. Modern CMOS (Complementary Metal-Oxide-Semiconductor) teknolojisinde bu referans eşik, tipik olarak besleme geriliminin yarısı VDD/2 civarında belirlenir; bu eşiğin altındaki gerilim seviyeleri mantıksal 0, üzerindekiler ise mantıksal 1 olarak yorumlanır. (Mano, M. M., ve Ciletti, M. D. 2013)

Bu iki mantıksal seviye arasında bırakılan ve gürültü marjı (noise margin) olarak adlandırılan tolerans bandı, termal gürültü ve sinyal dalgalanmalarına karşı sistemin deterministik kararlılığını güvence altına alır. Aritmetik işlemler, karar yapıları ve kontrol akışı gibi tüm hesaplama süreçleri, donanım seviyesindeki bu hata toleranslı ikili temsil üzerine inşa edilir. (Mano, M. M., ve Ciletti, M. D. 2013)

2.1.2 İkili (Binary) Sayı Sistemi ve Taban Dönüşümü

İnsanların günlük kullanımında baskın olan sayı sistemi onluk (decimal) sistemdir; buna karşılık dijital bilgisayarlar ikili sayı sistemi (binary number system) ile çalışır. İkili sistem, tabanı 2 olan bir konumsal sayı sistemidir. Bu sistemde her basamak yalnızca 0 ya da 1 olabilir ve her basamağın ağırlığı, sağdan sola doğru 2'nin artan kuvvetleriyle belirlenir. (Mano, M. M., ve Ciletti, M. D. 2013)

Herhangi bir negatif olmayan tamsayı N, ikili sistemde basamak değerlerinin toplamı biçiminde ifade edilir. Bu gösterimin genel matematiksel formu Denklem (2.2)'de verilmiştir (Mano ve Ciletti, 2013).

$$N = b_{n-1} \cdot 2^{n-1} + b_{n-2} \cdot 2^{n-2} + \ldots + b_1 \cdot 2^1 + b_0 \cdot 2^0 \quad (2.2)$$

$$b_i \in \{0, 1\},\ i = 0, 1, \ldots, n-1$$

Burada b_0 **en düşük anlamlı bit (Least Significant Bit, LSB)** ve b_{n-1} **en yüksek anlamlı bit (Most Significant Bit, MSB)** olarak adlandırılmaktadır. Bu iki bit konumu, sayısal işlem sırasındaki taşıma (carry) ve işaret (sign) bilgisinin barındırıldığı kritik noktalardır.

Genel biçimde, n basamaklı bir ikili sayının onluk karşılığı şöyle hesaplanır: Buna karşılık, n basamaklı bir ikili sayının onluk karşılığı, her bitin kendi konumsal ağırlığı ile çarpılıp toplanmasıyla elde edilir. Bu dönüşümün genel ifadesi Denklem (2.3)'de gösterilmektedir (Mano ve Ciletti, 2013).

$$\sum_{i=0}^{n-1} b_i \cdot 2^i \quad (2.3)$$

Örnek hesaplamalar:

$$0011_2 = 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 3_{10}$$

$$1111_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 15_{10}$$

Tablo 2.1. 4-bit işaretsiz tamsayıların ikili ve ondalık gösterimleri

İkili (4-bit)	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$	Ondalık Değer
0000	0	0	0	0	0
0001	0	0	0	1	1
0011	0	0	1	1	3
0101	0	1	0	1	5
0111	0	1	1	1	7
1000	1	0	0	0	8
1111	1	1	1	1	15

Bu örnekler, bilgisayarların sayısal veriyi temelde nasıl kodladığını göstermektedir (bkz. Tablo 2.1). Kullanıcı arayüzü düzeyinde onluk gösterimle karşılaşılsa da, işlemci, bellek ve veri yolu gibi donanım bileşenleri açısından gerçek işlem alanı ikili düzlemdir.

İkili sistemin tercih edilmesinin sebebi yalnızca kuramsal sadelik değildir; fiziksel devrelerin iki kararlı durum arasında güvenilir biçimde çalışabilmesi, ikili temsili mühendislik açısından da son derece elverişli kılar. Bu nedenle klasik hesaplama, hem mantıksal hem de fiziksel bakımdan **ikili ayrıklık** üzerine kuruludur.

2.1.3 İşaret Biti ve İkiye Tümleme (Two's Complement)

Gerçek hesaplama ortamlarında yalnızca doğal sayılar değil, negatif tamsayılar da temsil edilmek zorundadır. Negatif sayıların ikili sistemde temsili, donanım aritmetiğinin en kritik tasarım kararlarından birini oluşturur. Günümüz mimarilerinin büyük çoğunluğunda benimsenen ikiye tümleme (two's complement) gösterimi, toplamsal ters işlemin (additive inverse) hesaplanmasına ve toplama/çıkarma devrelerinin aynı donanım üzerinde verimle gerçekleştirilmesine olanak tanımaktadır. (Mano, M. M., ve Ciletti, M. D. 2013)

n-bitlik ikiye tümleme kodlamasında MSB, işaret biti (sign bit) görevini üstlenir; 0 pozitifi, 1 ise negatifi temsil eder. Bu gösterimde bir sayının değerinin nasıl hesaplandığı Denklem (2.4)'te tanımlanmaktadır (Mano ve Ciletti, 2013).

$$N = -b_{n-1} \cdot 2^{n-1} + b_{n-2} \cdot 2^{n-2} + \cdots + b_1 \cdot 2^1 + b_0 \cdot 2^0 \quad (2.4)$$

4-bit örnekleri üzerinden değerlendirildiğinde:

- $0111_2 = +7$ (pozitif maksimum)
- $1000_2 = -8$ (negatif minimum)
- $1111_2 = -1$

Bu sayede $[-2^{n-1}, 2^{n-1} - 1]$ aralığında, simetrik olmayan ancak matematiksel açıdan tutarlı bir temsil elde edilmiş olur. Bu **asimetri** - negatif tarafın bir birim daha geniş olması - ikiye tümleme kodlamasının yapısal bir özelliğidir ve tamsayı taşması (integer overflow) analizi sırasında göz önünde bulundurulması gereken önemli bir unsur olarak karşımıza çıkmaktadır.

2.1.4 Taşıma (Carry) Biti ve Aritmetik Taşıma

Klasik işlemcilerin temel işlevlerinden biri aritmetik işlemleri yürütmektir. İkili aritmetikte toplama işlemi, onluk sistemdekine benzer biçimde sütun bazında gerçekleştirilir. İki n-bitlik sayının ikili toplamı, n+1 bite ihtiyaç duyabilir. n. bitten (MSB) dışarıya taşınan bu ekstra bit **taşıma biti (carry bit, C_{out})** olarak tanımlanır ve toplayıcı devreler tarafından ayrı bir sinyal hattında tutulur.

İkili toplamada temel kurallar şunlardır:

1. $0 + 0 = 0$
2. $0 + 1 = 1$
3. $1 + 0 = 1$
4. $1 + 1 = 10_2$ (taşıma: carry = 1, toplam biti = 0)

Son kural özel önem taşır: sonuç tek bitlik alana sığmaz; sağdaki 0 toplam biti olurken soldaki 1 bir üst basamağa taşınır. Bu taşınan bit, carry bit olarak adlandırılır. Taşıma mekanizmasının bu davranışı Denklem (2.5)'te verilen örnek üzerinden açıkça görülmektedir.

$$1111_2 + 0001_2 = 1\ 0000_2 \quad (2.5)$$

Denklem (2.5)'te, 4-bitlik iki sayının toplamı sonucunda solda fazladan bir bit oluştuğu görülmektedir. Eğer işlem sabit genişlikli bir donanım üzerinde yürütülüyorsa, bu fazladan bit ayrı olarak değerlendirilir. Bu noktada yalnızca carry değil, taşma (overflow) kavramı da önem kazanır.

İşaretli ve İşaretsiz Taşıma Farkı

İşaretsiz aritmetikte carry biti doğrudan taşmayı gösterir. İşaretli (ikiye tümleme) aritmetikte ise taşma, MSB'ye giren carry (C_{in}) ile çıkan carry (C_{out}) arasındaki XOR işleminin 1 üretmesi durumunda mevcuttur:

$$Overflow = C_{in} \oplus C_{out}$$

İşaretli ve İşaretsiz Taşıma Farkı

Bu ayrım, derleyici optimizasyon teknikleri ve güvenlik-kritik gömülü sistemler açısından son derece önem taşımaktadır.

Ripple-carry adder gibi basit toplayıcı mimarilerinde taşıma biti, LSB'den MSB'ye bit bit yayılır ve bu yayılım gecikmesi (carry propagation delay), büyük bit genişliklerinde (64-bit, 128-bit) performans darboğazı oluşturabilir. Carry-lookahead ve prefix adder (Kogge-Stone, Han-Carlson) gibi ileri mimari yaklaşımlar bu yayılımı paralel olarak çözerek O(log n) gecikmeyle işlem yapabilmektedir. (Mano, M. M., ve Ciletti, M. D. 2013)

2.1.5 Mantık Kapısı Kavramı ve Boole İşlem Modeli

Klasik hesaplamanın temel operasyonel birimi **mantık kapısı (logic gate)**dır. Mantık kapıları, bir veya daha fazla bit girdisini Boole fonksiyonları çerçevesinde işleyerek bit çıktıları üretir; Boole cebiri operatörlerinin fiziksel elektronikte gerçekleştirimi olarak da tanımlanabilir.

Boole cebiri, iki değerli bir mantık sistemi olarak klasik devre tasarımının matematiksel temelini oluşturur. Dijital devrelerde hesaplama, özünde Boole fonksiyonlarının fiziksel olarak gerçekleştirilmesidir. İşlemciler, kaydediciler, sayaçlar, çoklayıcılar, toplayıcılar ve bellek birimleri gibi yüksek seviyeli bileşenler, alt düzeyde mantık kapılarının sistematik bileşimlerinden oluşur. (Mano, M. M., ve Ciletti, M. D. 2013)

Matematiksel olarak bir lojik kapı, giriş kümesinden çıkış kümesine tanımlı bir fonksiyon olarak modellenebilir. Bu genel gösterim Denklem (2.6)'te verilmiştir.

$$f : \{0,1\}^n \rightarrow \{0,1\} \quad (n : \text{giriş sayısı, fan-in}) \quad (2.6)$$

Denklem (2.6)'te nnn, giriş sayısını yani fan-in değerini temsil etmektedir. Bu nedenle mantık kapıları yalnızca basit eğitimsel örnekler değil; aynı zamanda tüm klasik hesaplama mimarisinin en düşük soyutlama düzeyindeki kurucu öğeleridir.

2.1.6 Temel Mantık Kapıları

2.1.6.1 AND Kapısı

AND kapısı, Boole çarpımını (lojik çarpma) hesaplar. Tüm girişler 1 olduğunda ve yalnızca bu durumda çıkış 1 üretilir. Bu kapının cebirsel gösterimi Denklem (2.7)'de verilmiştir (Mano ve Ciletti, 2013).

$$Y = A \cdot B \quad (AND) \quad (2.7)$$

Bu karşılaştırma Tablo 2.2'de özetlenmektedir.

Tablo 2.2. AND kapısının doğruluk tablosu

A	B	Y = A · B
0	0	0
0	**1**	0
1	0	0
1	**1**	**1**

2.1.6.2 OR Kapısı

OR kapısı, Boole toplamını hesaplar. En az bir giriş 1 olduğunda çıkış 1 üretilir. Bu temel cebirsel gösterim Denklem (2.8)'de sunulmaktadır (Mano ve Ciletti, 2013).

$Y = A + B$ (OR) (2.8)

Bu karşılaştırma Tablo 2.3'te özetlenmektedir.

Tablo 2.3. OR kapısının doğruluk tablosu

A	B	Y = A + B
0	0	0
0	**1**	**1**
1	0	**1**
1	**1**	**1**

OR kapısı, mantıksal olarak NAND-NAND bileşimi aracılığıyla gerçekleştirilebilir. Bu eşdeğerlik Denklem (2.9)'de gösterilmektedir.

$A + B = \neg(\neg A \cdot \neg B)$ (2.9)

Bu dönüşüm, tüm AND/OR/NOT mantığını yalnızca NAND yapı taşları üzerine inşa etmenin teorik altyapısını oluşturmaktadır.

2.1.6.3 NOT Kapısı (Inverter - Tersleyici)

NOT kapısı (inverter/tersleyici), tek girişli bir kapı olup Boole tümleyenini hesaplar. Girişin mantıksal zıddını üretir. Girişin mantıksal zıddını üretir. Bu işlemin cebirsel gösterimi Denklem (2.10)'te verilmiştir (Mano ve Ciletti, 2013).

$Y = \bar{A}$ (NOT) (2.10)

Bu karşılaştırma Tablo 2.4'te özetlenmektedir.

Tablo 2.4. NOT kapısının doğruluk tablosu

A	Y = Ā
0	**1**
1	0

2.1.6.4 NAND Kapısı

NAND (Not AND) kapısı, AND kapısının çıkışını tersleyen bileşik bir kapıdır. Çıkış, tüm girişler 1 olduğunda ve yalnızca bu durumda 0 üretir; tüm diğer giriş kombinasyonlarında çıkış 1'dir. Bu kapının Boole ifadesi Denklem (2.11)'te verilmiştir (Mano ve Ciletti, 2013).

$Y = \neg(A \cdot B)$ (NAND) (2.11)

Bu karşılaştırma Tablo 2.5'te özetlenmektedir.

Tablo 2.5. NAND kapısının doğruluk tablosu

A	B	Y = ¬(A · B)
0	0	**1**

A	B	Y = ¬(A · B)
0	**1**	**1**
1	0	**1**
1	**1**	0

2.1.7 Evrensel Kapı Kavramı

Bir lojik kapı ailesi, herhangi bir Boole fonksiyonunu yalnızca o ailedeki kapıları kullanarak gerçekleştirebildiğinde fonksiyonel olarak tam (functionally complete) ya da evrensel (universal) olarak nitelendirilmektedir. Post'un 1941 tarihli yetkinlik teoremi, bir lojik sistemin fonksiyonel tamlığının gerekli ve yeterli koşullarını formel olarak tanımlamaktadır. (Mano, M. M., ve Ciletti, M. D. 2013)

Post'un Fonksiyonel Tamlık Teoremi (1941)

Bir fonksiyon kümesi $\{f_1, f_2, \ldots, f_n\}$, Post'un beş sınıfından (T_0, T_1, S, M, L) en az birini barındırmıyorsa ve yalnızca bu durumda fonksiyonel olarak tamdır. Bu sınıflar sırasıyla: 0-koruyucu, 1-koruyucu, kendine-dual, monoton ve doğrusal (lineer) fonksiyonları kapsamaktadır. NAND, bu beş sınıfın hiçbirine ait olmadığından evrenseldir.

Evrensellik kavramı, donanım tasarımında derin pratik sonuçlar doğurmaktadır. Yalnızca tek tip bir kapıya ihtiyaç duyulması, üretim sürecini basitleştirmekte, test otomasyonunu kolaylaştırmakta ve özelleştirilmiş entegre devrelerin (ASIC) verimli biçimde tasarlanmasını mümkün kılmaktadır.

2.1.8 NAND ile Evrensel Kapı Sentezi

NAND kapısının evrenselliği teorik bir sonuç olmaktan öte, aşağıdaki kapı dönüşümleriyle somut biçimde gösterilebilmektedir. Her bir dönüşüm, De Morgan teoreminden ve Boole cebirinin temel özdeşliklerinden türetilmektedir.

Bu karşılaştırma Tablo 2.6'da özetlenmektedir.

Tablo 2.6. NAND kapısıyla temel lojik kapıların sentezi

Hedef Kapı	NAND Sentezi	Boole İfadesi / Açıklama
NOT	NAND(A, A)	¬A = NAND(A,A) - Her iki giriş kısa devre yapılır; tek NAND kapısı yeterlidir.
AND	NOT(NAND(A,B))	A·B = ¬NAND(A,B) - İki NAND kapısı gereklidir.
OR	NAND(¬A, ¬B)	A+B = ¬(¬A · ¬B) = NAND(¬A,¬B) - De Morgan dönüşümü; üç NAND kapısı.
NOR	NOT(OR(A,B))	¬(A+B) - Dört NAND kapısı ile gerçekleştirilir.
XOR	NAND kombinasyonu	`A⊕B = NAND(NAND(A,s), NAND(B,s)), s=NAND(A,B)` - Minimum dört NAND kapısı.

2.1.8.1 NAND → NOT2.1.8.1 NAND → NOT

NAND kapısının her iki girişi aynı sinyale bağlandığında tersleme işlemi elde edilmektedir. Bu durum Denklem (2.12)'de gösterildiği üzere, *A* sinyalinin kendiyle NAND işlemine sokulmasıyla doğrudan ¬ *A* sonucunu üretmektedir.

$$Y = \neg(A \cdot A) = \neg A \text{ (2.12)}$$

Dolayısıyla Denklem (2.12), özel bir inverter devresine ihtiyaç duyulmaksızın NOT işlevinin tek bir NAND kapısıyla gerçekleştirilebildiğini göstermektedir.

2.1.8.2 NAND → AND2.1.8.2 NAND → AND

AND işlevi, önce NAND ile ¬(A·B) üretilip ardından bu sonucun tekrar terslenmesiyle elde edilmektedir. Bu dönüşüm Denklem (2.13)'de ifade edilmiştir.

$$Y = \neg(\neg(A \cdot B)) = A \cdot B \text{ (2.13)}$$

Burada Denklem (2.13), çift tersleme özdeşliği kullanılarak AND kapısının **iki NAND** kapısıyla sentezlenebildiğini göstermektedir.

2.1.8.3 NAND → OR2.1.8.3 NAND → OR

OR işlemi, De Morgan teoremi kullanılarak yalnızca NAND kapılarıyla da kurulabilmektedir. Bu eşdeğerlik Denklem (2.14)'te verilmiştir.

$$Y = \neg(\neg A \cdot \neg B) = A + B \text{ [De Morgan] (2.14)}$$

Denklem (2.14)'te görüldüğü üzere, önce girişler terslenmekte, ardından bu terslenmiş değerler NAND kapısına uygulanarak OR işlevi elde edilmektedir.

2.1.8.4 NAND → NOR2.1.8.4 NAND → NOR

$$Y = \neg(A + B) \text{ (2.15)}$$

1.8.3'teki OR devresinin çıkışına yalnızca bir NAND(x,x) tersleyici eklenir. **4 NAND kapısı** ile gerçekleştirilir.

2.1.8.5 NAND → XOR (Minimum Devre)2.1.8.5 NAND → XOR (Minimum Devre)

s = NAND(A, B), p = NAND(A, s), q = NAND(B, s), Y = NAND(p, q)

$$A \oplus B = NAND(NAND(A,s), NAND(B,s)),\ s = NAND(A,B) \text{ (2.16)}$$

Denklem (2.16), XOR işlevinin dört NAND kapısıyla nasıl sentezlendiğini ve ortak s sinyalinin üç farklı noktada kullanılarak devre yapısının nasıl optimize edildiğini göstermektedir. G1 paylaşılan s = NAND(A,B) hesaplar; G2 = NAND(A,s); G3 = NAND(B,s); G4 = NAND(G2,G3) ile A⊕B elde edilir. s sinyali üç kapı tarafından ortak kullanılarak kapı sayısı minimize edilmiştir. 4'ten az NAND kullanılarak XOR üretmek mümkün değildir; bu teorik minimumdur.(Mano, M. M., ve Ciletti, M. D. 2013) 4 NAND kapısı (kanıtlanmış minimum).

2.1.9 AND ve NOT Kapıları ile Diğer Kapıların Sentezi

2.1.10 AND + NOT → NAND2.1.10 AND + NOT → NAND

$$Y = \neg(A \cdot B) \text{ (2.17)}$$

Denklem (2.17)'da gösterildiği üzere, AND çıkışının doğrudan terslenişiyle NAND tanımı karşılanır. **1 AND + 1 NOT** kapısı kullanılır.

2.1.10.1 AND + NOT → OR2.1.10.1 AND + NOT → OR

$$A + B = \neg(\neg A \cdot \neg B) \text{ [De Morgan] (2.18)}$$

Denklem (2.18)'de verildiği gibi, iki NOT ile A ve B terslenip AND'a beslenir; AND çıkışı üçüncü NOT ile ters çevrilince OR elde edilir. **1 AND + 3 NOT** kapısı gereklidir.

2.1.10.2 AND + NOT → NOR2.1.10.2 AND + NOT → NOR

$$\neg(A+B) = \neg(\neg(\neg A \cdot \neg B)) \text{ (2.19)}$$

Denklem (2.19)'te ifade edilen yapıya göre, (2.18)'deki OR devresine bir NOT kapısı daha eklenerek NOR işlevi elde edilir. 1 AND + 4 NOT kapısı gereklidir.

2.1.10.3 AND + NOT → XOR - SOP Formu2.1.10.3 AND + NOT → XOR - SOP Formu

$$A \oplus B = (A \cdot \bar{B}) + (\bar{A} \cdot B) \text{ (2.20)}$$

Denklem (2.20)'te gösterildiği üzere, üst dalda A ve NOT(B) → AND → $A \cdot \bar{B}$, alt dalda ise NOT(A) ve B → AND → $\bar{A} \cdot B$ elde edilir. İki dalın OR'ı: $(A \cdot \bar{B}) + (\bar{A} \cdot B) = A \oplus B$. OR, De Morgan ile AND+NOT kullanılarak gerçekleştirilir (2.18 numaralı denklemdeki yapı). Bu, SOP (Sum of Products - Çarpımlar Toplamı) formunun doğrudan gerçekleştirimidir. (Mano, M. M., ve Ciletti, M. D. 2013) 2 AND + 5 NOT kapısı gereklidir.

Klasik bilgisayarlarda tüm hesaplama, bu lojik kapıların - her biri deterministik ve geri döndürülemez (irreversible) bir Boole işlevi uygulayan - kombinasyonu ve sıralı bileşimleriyle gerçekleştirilmektedir (Mano, M. M., ve Ciletti, M. D. 2013).

Kuantum bilgisayarlarda ise klasik kapıların yerini kuantum kapıları (quantum gates) almaktadır. Kuantum kapıları, klasik karşıtlarından farklı olarak terslenebilir (reversible) ve üniter (unitary) dönüşümler uygulamaktadır; bu durum hem hesaplama modelini hem de evrensel kapı setinin tanımını kökten değiştirmektedir. Bu farklar, bir sonraki bölümde ayrıntılı biçimde ele alınacaktır. (Shannon, C. E. 1948) (Mano, M. M., ve Ciletti, M. D. 2013)

2.2 Kuantum Hesaplama Temelleri

Bu bölümde, önceki bölümde incelenen klasik hesaplama paradigmasından hareketle kuantum hesaplamanın temel kavramları ele alınacaktır. Klasik bilgisayarların deterministik ve ikili yapısının yerini, olasılıksal ve süperpozisyon temelli bir hesaplama modeline bırakan kuantum bilgisayarlar; günümüzde şifreleme, ilaç tasarımı, optimizasyon ve yapay zeka gibi alanlarda çığır açıcı potansiyel sunmaktadır. Bu bölümün amacı, kuantum hesaplamanın matematiksel ve fiziksel altyapısını sistematik biçimde ortaya koymak; bit ile qubit arasındaki köklü farkları, süperpozisyon ve kuantum paralellik ilkelerini akademik bir çerçevede açıklamaktır.

2.2.1 Kuantum Hesaplama Nedir?

Kuantum hesaplama (quantum computing), bilginin işlenmesinde klasik Boole mantığı yerine kuantum mekaniğinin ilkelerini - süperpozisyon, dolanıklık (entanglement) ve girişim (interference) - temel alan bir hesaplama paradigmasıdır. 1980'li yıllarda Richard Feynman ve David Deutsch tarafından teorik temelleri atılan bu alan, "kuantum sistemleri en iyi yine kuantum bir bilgisayar simüle edebilir" önermesine dayanmaktadır (Feynman, 1982).

Klasik bilgisayarlar, mantık kapılarından oluşan deterministik devrelerle bit dizileri üzerinde işlem yapar. Buna karşılık kuantum bilgisayarlar, qubit adı verilen kuantum bilgi birimleri üzerinde üniter (tersinir) dönüşümler uygular. Bu yapı, belirli problem sınıfları için hesaplamalı karmaşıklığı köklü

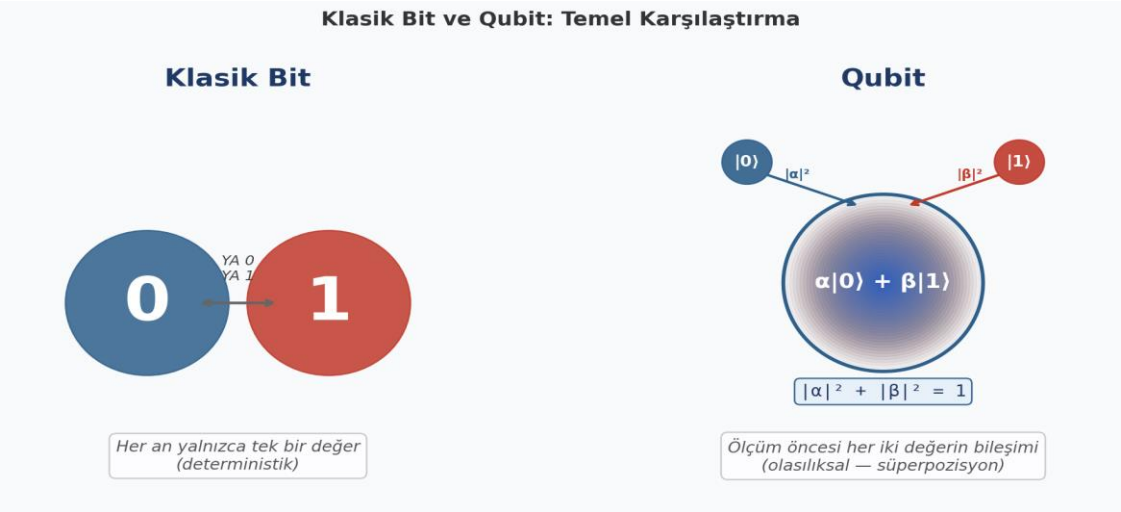
biçimde azaltma potansiyeline sahiptir. Shor'un (1994) asal çarpanlara ayırma algoritması ve Grover'un (1996) arama algoritması, kuantum üstünlüğünün (quantum advantage) somut matematiksel kanıtları olarak kabul edilmektedir.

Kuantum hesaplama, yalnızca daha hızlı bir bilgisayar değil; farklı bir hesaplama modeli olarak konumlandırılmalıdır. Nitekim her problem türü için kuantum bilgisayarlar avantajlı değildir; ancak yapısal olarak üstel arama uzayı gerektiren problemlerde - kriptografi, optimizasyon, moleküler simülasyon gibi - klasik sınırların ötesine geçme kapasitesi taşımaktadır (Aaronson, 2013).

2.2.2 Bit ve Qubit: Temel Bilgi Birimlerinin Karşılaştırılması

Klasik hesaplamanın temel bilgi birimi olan bit (binary digit), herhangi bir anda yalnızca iki ayrık değerden birini alabilmektedir: 0 ya da 1. Bu ikili yapı, transistör bazlı fiziksel gerçekleştirim ile birebir örtüşmekte; düşük gerilim 0, yüksek gerilim ise 1 olarak kodlanmaktadır. Dolayısıyla klasik bir n-bitlik sistem, söz konusu n bit kombinasyonlarından yalnızca tek bir konfigürasyonu aynı anda temsil edebilir.

Qubit (quantum bit), kuantum mekaniğinin iki durumlu bir sistemi üzerine inşa edilmiş bilgi birimidir. Fiziksel olarak bir qubit; elektronun spin durumu (yukarı/aşağı), fotonun polarizasyonu (yatay/dikey) ya da süper iletken devredeki akım yönü gibi iki ayırt edilebilir kuantum durumuyla gerçekleştirilebilir. Temel fark şudur: bir qubit, ölçüm yapılmadan önce her iki temel durumun doğrusal birleşiminde bulunabilmektedir, yani klasik anlamda "bir değer almak" yerine olasılıksal bir durum uzayında var olmaktadır. Şekil 2.1'de bu temel fark görsel olarak özetlenmektedir.



Şekil 2.1. Klasik bit (deterministik, tek değer) ve qubitin (olasılıksal, süperpozisyon) karşılaştırmalı gösterimi.

Tablo 2.7'de bit ve qubit arasındaki temel farklılıklar karşılaştırmalı biçimde özetlenmektedir.

Tablo 2.7. Klasik bit ve qubit arasındaki temel karşılaştırma.

Özellik	Klasik Bit	Qubit
Temel değerler	0 veya 1	|0⟩ veya |1⟩ (veya bileşimi)
Fiziksel gerçekleştirim	Transistör voltaj seviyeleri	Elektron spini, foton,
Ölçüm öncesi durum	Kesin (deterministik)	Süperpozisyon (olasılıksal)
Ölçüm sonrası durum	Değişmez	Dalga fonksiyonu çöker (collapse)

Özellik	Klasik Bit	Qubit
n birimlik sistem	2^n durumdan yalnızca biri	2^n durumun eş zamanlı süperpozisyonu
İşlem tersinirliği	Tersinmez (NAND, AND…)	Tersinir (üniter matrisler)

2.2.3 Süperpozisyon İlkesi

2.2.3.1 Fiziksel Temel: Elektronun Çok Durumlu Varlığı

Kuantum mekaniğinin en köklü ilkelerinden biri, bir kuantum sisteminin ölçülmediği sürece birden fazla özelbiçim (eigenstate) üzerinde eş zamanlı olarak var olabilmesidir. Bu olgu, günlük sezgilerle bağdaşmayan ancak defalarca deneysel olarak doğrulanmış bir fizik gerçeğidir. Bir elektronu düşündüğümüzde, ölçüm yapılmadan önce bu elektron "yukarı spin" ($|0\rangle$) ve "aşağı spin" ($|1\rangle$) durumlarının matematiksel bir bileşimi halindedir - bu iki durumdan biri değil, ikisinin birlikte var olduğu bir "bulut"tur.

Young'ın çift yarık deneyi bu ilkenin en çarpıcı deneysel kanıtıdır. Bir elektron her iki yarıktan geçer gibi davranarak perde üzerinde girişim deseni oluşturur; oysa ölçüm yapıldığında - yani "hangi yarıktan geçti?" sorusu sorulduğunda - girişim deseni yok olur ve elektron tek bir konuma "yerleşir." Ölçüm eylemi, süperpozisyon durumunu sonlandırır ve sistemi tek bir özelbiçime zorlar; bu süreç dalga fonksiyonu çökmesi (wave function collapse) olarak adlandırılmaktadır (Dirac, 1930).

2.2.3.2 Matematiksel Gösterim ve Olasılık Yorumu

Kuantum mekaniğinde bir qubitin durumu, Dirac bra-ket notasyonuyla ifade edilmektedir. Herhangi bir qubit durumu $|\psi\rangle$, iki temel durum $|0\rangle$ ve $|1\rangle$ üzerinde aşağıdaki doğrusal birleşim olarak yazılır:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2.21)$$

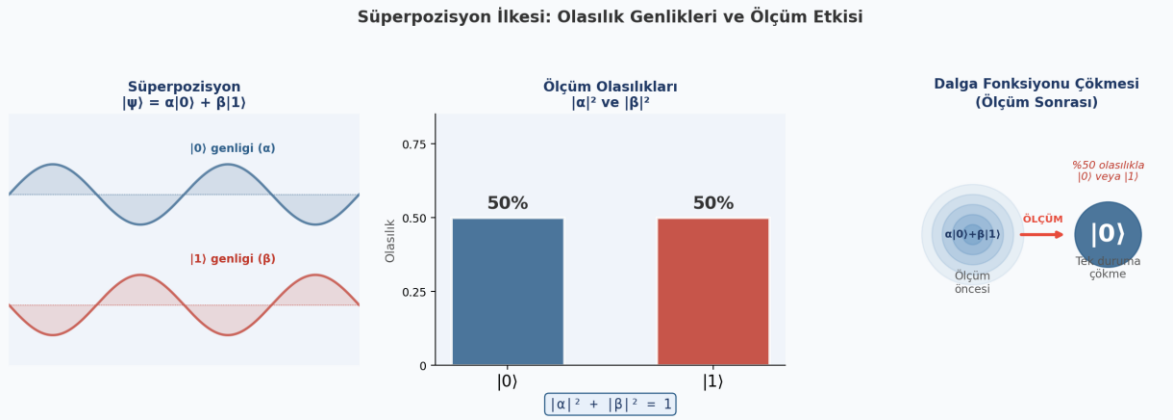
Burada α ve β karmaşık sayılardır; kuantum bilgisayar literatüründe olasılık genlikleri (probability amplitudes) olarak adlandırılmaktadır (Nielsen ve Chuang, 2010). Bu genliklerin karmaşık sayı olması, girişim (interference) olgusunu - yani qubit durumlarının birbirini pekiştirip zayıflatmasını - matematiksel olarak mümkün kılar. (2.21) numaralı denklemde sistem bir kez ölçüldüğünde $|0\rangle$ sonucunun elde edilme olasılığı $|\alpha|^2$, $|1\rangle$ sonucunun elde edilme olasılığı ise $|\beta|^2$'dir. Olasılıkların 1'e eşit olması zorunluluğundan normalizasyon koşulu şu şekilde türetilir:

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2.22)$$

(2.22) denklemi somutlaştırmak gerekirse, eşit süperpozisyon durumu olan $|+\rangle$ aşağıdaki biçimde ifade edilir:

$$|+\rangle = (1/\sqrt{2})|0\rangle + (1/\sqrt{2})|1\rangle \quad (2.23)$$

(2.23) numaralı denklemde $|\alpha|^2 = |\beta|^2 = 1/2$ olduğundan, ölçüm yapıldığında 0 veya 1 sonucu %50 olasılıkla elde edilmektedir. Şekil 2.2'de süperpozisyon ilkesi; olasılık genlikleri, ölçüm olasılıkları ve dalga fonksiyonu çökmesi boyutlarıyla görsel olarak özetlenmektedir.



Şekil 2.2. Süperpozisyon ilkesi: (soldan sağa) α|0⟩ ve β|1⟩ bileşenlerinin genlikleri, ölçüm olasılıkları ve dalga fonksiyonu çökmesi.

2.2.3.3 Schrödinger'in Kedisi Analojisi

Süperpozisyon ilkesinin en bilinen örneklerinden biri, Erwin Schrödinger tarafından 1935 yılında ortaya konulan kedi düşünce deneyidir. Bu analojiye göre kapalı bir kutu içindeki sistem, ölçüm yapılıncaya kadar klasik anlamda tek bir duruma indirgenmiş değildir. Başka bir ifadeyle, sistem ölçüm öncesinde olası durumların doğrusal birleşimi ile temsil edilmektedir. Kutu açılıp gözlem yapıldığında ise sistem belirli bir sonuca karşılık gelen tek bir duruma indirgenir. Bu düşünce deneyi, kuantum süperpozisyonunun doğrudan klasik sezgilerle açıklanmasının güç olduğunu, ancak ölçüm sonucunda belirli bir durumun elde edildiğini vurgulamak için kullanılmaktadır. Gerçek qubit sistemleri de benzer şekilde, ölçüm öncesinde |0⟩|0\rangle|0⟩ ve |1⟩|1\rangle|1⟩ durumlarının doğrusal birleşimi halinde bulunur; ölçüm sonrasında ise bu temel durumlardan birine indirgenir.

2.2.4 Qubit Gösterimi: Bloch Küresi

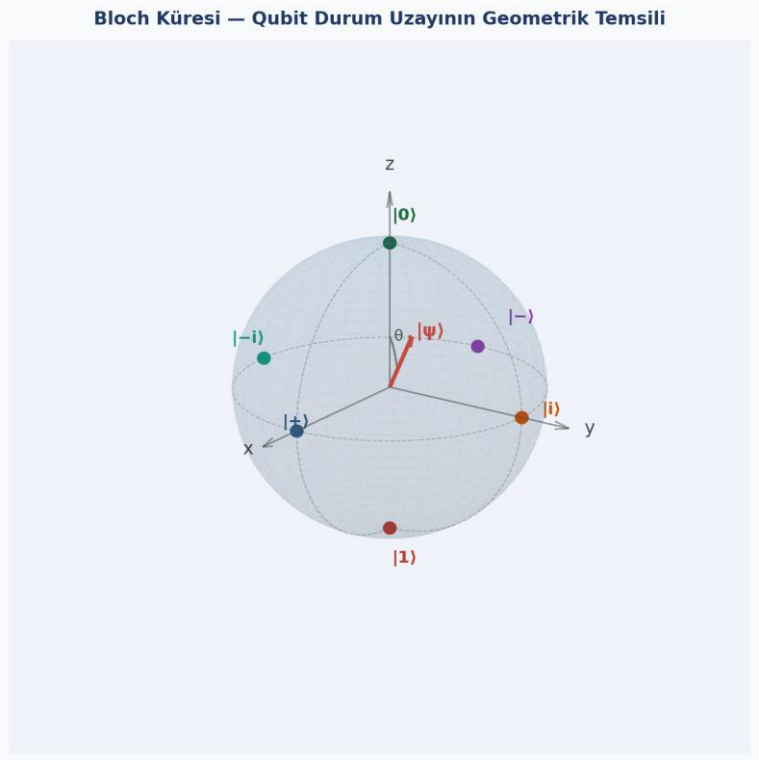
(2.21) numaralı denklemde α ve β karmaşık sayılardır. Normalizasyon koşulu (2.22) ve global fazın fiziksel anlamsızlığı göz önünde bulundurulduğunda, qubit durumu gerçekte yalnızca iki bağımsız gerçel parametre (θ ve φ) ile tam olarak tanımlanabilmektedir:

$$\alpha = \cos(\theta/2),\ \beta = e^{i\varphi} \cdot \sin(\theta/2) \quad (2.24)$$

Bu parametrizasyonla qubit durumu (2.21) numaralı denklem, (2.25) numaralı biçimi alır:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi} \sin(\theta/2)|1\rangle \quad (2.25)$$

Burada $\theta \in [0, \pi]$ açısı z ekseninden olan sapıklığı; $\varphi \in [0, 2\pi)$ açısı ise xy düzlemindeki dönüşü temsil etmektedir. (2.24) ve (2.25) numaralı denklemlerdeki parametrizasyon, her saf (pure) qubit durumunun yarıçapı 1 olan bir küre - Bloch küresi - üzerindeki benzersiz bir noktayla eşleştirilebileceğini ortaya koymaktadır. Şekil 2.3'te Bloch küresi ve temel qubit durumlarının geometrik konumları gösterilmektedir.



Şekil 2.3. Bloch küresi: |0⟩ (kuzey kutbu), |1⟩ (güney kutbu), |+⟩, |−⟩, |i⟩, |−i⟩ ekvator durumları ve genel |ψ⟩ durum vektörü.

Kuantum kapıları, Bloch küresi üzerinde belirli rotasyon ve yansıma işlemleri olarak geometrik biçimde yorumlanabilmektedir. Örneğin Hadamard (H) kapısı, kuzey kutbundaki |0⟩ vektörünü ekvator düzlemine indirerek |+⟩ durumunu üretir - yani z ekseninden x eksenine 90° döndürme işlemidir. Pauli-X kapısı ise vektörü kuzey kutbundan güney kutbuna taşır: |0⟩ → |1⟩ dönüşümü, geometrik olarak x ekseni etrafında 180° dönüme karşılık gelir (Nielsen ve Chuang, 2010).

2.2.5 Kuantum Paralelliği

Kuantum hesaplamanın klasik hesaplamaya kıyasla en önemli üstünlüklerinden biri, kuantum paralellik (quantum parallelism) olgusudur. Bu kavramı anlamak için önce çok-qubitlik sistemlerin matematiksel yapısına değinmek gerekmektedir.

İki qubitin birleşik sistemi, her bir qubitin durum uzayının tensör çarpımı ile tanımlanır. Genel durumda 2 qubitlik bir sistem aşağıdaki süperpozisyonu ifade edebilir:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \quad (2.26)$$

Bu örüntü n quibit'e genelleştirildiğinde, n-qubitlik bir sistemin 2^n temel durum üzerinde eş zamanlı süperpozisyon oluşturabildiği görülür:

$$|\psi_n\rangle = \Sigma(x=0 \rightarrow 2^{n-1})\ \alpha_x|x\rangle, \quad \Sigma|\alpha_x|^2 = 1 \quad (2.27)$$

İşte kuantum paralelliğinin özü tam da burada yatmaktadır: n klasik bit, 2^n olası konfigürasyondan yalnızca birini herhangi bir anda temsil edebilirken, n qubit aynı anda tüm 2^n konfigürasyonun süperpozisyonunda bulunabilmektedir. Şekil 2.4'te bu fark, 3-bitlik/qubitlik örnek sistem üzerinden somutlaştırılmaktadır.



Şekil 2.4. Kuantum paralelliği: klasik 3-bit sistemde yalnızca 1 durum aktif iken (solda), 3-qubitlik sistemde $2^3 = 8$ durum eş zamanlı süperpozisyon içindedir (sağda).

Ancak bu noktada kritik bir uyarı gereklidir: 2^n sonucun tamamı yalnızca ölçüm yapılmadan önce süperpozisyon içinde "gizli" biçimde mevcuttur. Ölçüm yapıldığında sistem tek bir sonuca çöker. Dolayısıyla kuantum paralelliği, yalnızca bu sonuçları akıllıca "seçen" ve amplitüd girişimi üzerine kurulu algoritmalar tasarlandığında anlam kazanmaktadır.

Tablo 2.8'de klasik bit ve qubit sistemlerinin durum uzayı kapasitesi, farklı sistem büyüklükleri üzerinden karşılaştırmalı biçimde gösterilmektedir.

Tablo 2.8. Klasik bit ve qubit sistemlerinin durum uzayı kapasitesi karşılaştırması.

Sistem Büyüklüğü	Klasik bit (aynı anda 1 durum)	Qubit (eş zamanlı süperpozisyon)
n = 1	$2^1 = 2$ durumdan biri	$2^1 = 2$ eş zamanlı durum
n = 2	$2^2 = 4$ durumdan biri	$2^2 = 4$ eş zamanlı durum
n = 10	$2^{10} = 1.024$ durumdan biri	$2^{10} = 1.024$ eş zamanlı durum
n = 50	$2^{50} \approx 10^{15}$ (birer birer)	$2^{50} \approx 10^{15}$ (eş zamanlı)
n = 300	2^{300} > evrendeki atom sayısı	2^{300} eş zamanlı süperpozisyon

2.2.6 Kuantum Bilgisayarlar Neden Güçlüdür?

Kuantum bilgisayarların gücü, salt işlem hızından kaynaklanmamaktadır. Temel üstünlük, belirli problem sınıflarında hesaplama karmaşıklığının farklı bir büyüme eğrisiyle artmasından gelmektedir. Bu üstünlüğün üç temel kaynağı analitik biçimde incelenebilir.

Birinci kaynak, süperpozisyon temelli paralel işlemdir. (2.27) numaralı denklemde formüle edilen kuantum paralelliği sayesinde, n qubite sahip bir sistem tek bir işlem adımında 2^n farklı girişi eş zamanlı olarak işleyebilir. Buna karşılık klasik bir bilgisayarın aynı işlemi yapabilmesi için 2^n paralel işlemci gerektirmesi ya da ardışık hesaplama yapması gerekmektedir (Aaronson, 2013).

İkinci kaynak, kuantum girişimidir (quantum interference). Kuantum algoritmaları, olasılık genliklerini manipüle ederek doğru yanıtların genliğini artıran, yanlış yanıtlarınkini ise azaltan girişim örüntüleri yaratır. Grover'un (1996) algoritması, bu mekanizmayı yapılandırılmamış bir veritabanı aramasında O(√N) adımla çözüm üretecek biçimde kullanmaktadır; klasik en iyi yöntem ise O(N) adım gerektirmektedir.

Üçüncü kaynak, kuantum dolanıklığıdır (quantum entanglement). Dolanık qubit çiftlerinde, bir qubitin ölçüm sonucu diğerinin durumunu anlık olarak belirlemektedir. Bu özellik, kuantum hata düzeltme kodlarından kuantum kriptografisine uzanan geniş bir uygulama yelpazesinin temel taşını oluşturmaktadır (Nielsen ve Chuang, 2010).

Tablo 2.9'da seçilmiş problemler için kuantum ve klasik algoritmaların hesaplama karmaşıklıkları karşılaştırmalı olarak sunulmaktadır.

Bu karşılaştırma Tablo 2.9'da özetlenmektedir.

Tablo 2.9. Seçilmiş problemlerde kuantum ve klasik algoritmaların karmaşıklık karşılaştırması (* belirli koşullar altında).

Problem	Klasik bit (aynı anda 1 durum)	Qubit (eş zamanlı süperpozisyon)	Hızlanma
Yapılandırılmamış arama	O(N)	O(√N) - Grover (1996)	Karekök
Tamsayı çarpanlara ayırma	O(exp(n^{1/3}))	O(n³) - Shor (1994)	Üstel
Lineer denklem sistemleri	O(Ns)	O(log N) - HHL	Üstel
Moleküler simülasyon	O(exp(N))	O(poly(N)) - VQE	Üstel

2.3 Kuantum Kapısı ve Dolanıklık (Entanglement)

Kuantum kapısı (quantum gate ya da kuantum mantık kapısı), kuantum bilgisayarların en temel yapı taşlarından biridir. "A classical logic circuit is a set of gate operations on bits and is the unit of computation." [Klasik bir mantık devresi, bitler üzerinde gerçekleştirilen bir dizi kapı işleminden oluşur ve hesaplama birimidir.] (Numata, 2024, s. 3). Klasik bilgisayarlarda mantık kapıları (AND, OR, NOT, XOR vb.) bit'ler üzerinde çalışır ve her bit yalnızca 0 ya da 1 değerini alır. Kuantum bilgisayarlarda ise işlemler qubit üzerinde yapılır. Qubit, ölçülmeden önce 0 ve 1 durumlarının bir birleşimi halinde bulunabilir; bu özelliğe süperpozisyon denir. Klasik devrelerle benzer biçimde, "Inputs are on the left, outputs are on the right, and operations are represented by symbols between them."[Girişler solda, çıkışlar sağda ve işlemler aralarındaki sembollerle temsil edilmektedir.](Numata, 2024, s. 3).

2.3.1 Temel tek qubit kapıları

2.3.1.1 X kapısı



Şekil 2.5. X kapısı (Numata, 2024, s. 6)

Şekil 2.5'te ifade edilen X kapısı, klasik bilgisayardaki NOT işlemi gibi düşünülebilir: |0⟩ durumunu |1⟩'e, |1⟩ durumunu da |0⟩'a çevirir. Bu nedenle "bit flip" (bit çevirme) olarak da anılır (Numata, 2024).

2.3.1.2 H kapısı (Hadamard)



Şekil 2.6. H kapısı (Numata, 2024, s. 6)

Şekil 2.6'da ifade edilen H (Hadamard) kapısı, |0⟩ durumunu alıp qubiti eşit süperpozisyon durumuna taşır. Yani H kapısı |0⟩'a uygulandığında, qubit 0 ve 1 sonuçlarını eşit olasılıkla verecek bir duruma gelir (Numata, 2024). Bu durum çok yaygın olduğu için özel bir sembolle gösterilir Şekil 2.7'de ifade edilmiştir:

$$|+\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Şekil 2.7. Eşit süperpozisyon durumu denklemi

Benzer şekilde, |0⟩ ile |1⟩'in "işareti farklı" olan başka bir eşit süperpozisyon daha vardır ve Şekil 2.8'de gösterilmiştir:

Bu yapı Şekil 2.8'de gösterilmektedir.

$$|-\rangle \equiv \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Şekil 2.8. Eşit süperpozisyon durumu denklemi

|+⟩ ve |−⟩ durumlarında **ölçüm olasılıkları** (0 gelme/1 gelme ihtimali) benzer görünse de, devre içinde ilerleyen kapılarla birlikte davranışları farklılaşabilir. Ayrıca |−⟩ durumunu oluşturmanın pratik yolu da şu şekilde verilir: önce **X** ile |1⟩ elde edilir, ardından **H** uygulanır (Numata, 2024).

2.3.2 Kuantum Kapıları: Vektörden Hesaplamaya İlk Adım

Kuantum bilgisayarlarda bit yerine qubit kullanılır. Qubit matematiksel olarak bir vektördür. |0⟩ ve |1⟩ ise bu vektörün alabileceği iki temel değerdir. Qubit'i Vektör Olarak Düşünün Şekil 2.9'da gösterilen sadece vektörlerdir. x ve y ekseni gibi. |0⟩ yukarı bakıyor, |1⟩ yana bakıyor. Birbirine dik, birbirinden bağımsızdır ve şekil 3.2.1 deki gibidir.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Şekil 2.9. Qubit'i Vektör (Numata, 2024, s. 6)

Örneğin Şekil 2.10'daki X kapısı matrisi şu biçimde okunmalıdır:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$



$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

Şekil 2.10. X kapısı matrisi (Numata, 2024, s. 6)

Şekil 2.10'daki X kapısı matrisinin köşegenine bakınca sıfırlar var, köşegen dışında ise birler. Bu yapı matris çarpımında vektörün elemanlarını yer değiştirir. En alttaki işlemde bunu görebiliyoruz. X matrisi |0⟩ vektörüyle çarpılıyor. Üst eleman için 0×1 + 1×0 hesaplanıyor, sonuç 0. Alt eleman için 1×1 + 0×0 hesaplanıyor, sonuç 1. Yani |0⟩ olan vektör |1⟩'e dönüşüyor. Bu da tam olarak |1⟩. Ortadaki ok diyagramı bunu görsel olarak özetliyor. |0⟩ girişten giriyor, X kutusundan geçiyor, çıkışta |1⟩ çıkıyor. Matematikteki işlemin devre gösterimi budur.

2.3.3 Tek qubitli kuantum durumu ve üniter evrim.

Bir qubit durumu, |0⟩ ve |1⟩ temel durumlarının doğrusal birleşimi şeklinde gösterilebilmektedir. Bu genel durum Denklem (2.28)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2.28)$$

ifadesiyle tanımlanmakta olup α ve β katsayılarının 3.3.2

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2.29)$$

koşulunu sağladığı bilinmektedir (Numata, 2024).

Qubit durumları üzerindeki dönüşümler üniter operatörler aracılığıyla gerçekleştirilmektedir. U operatörünün uygulanmasıyla |ψ⟩ durumunun |ψ'⟩ durumuna evrildiği 3.3.3

$$|\psi'\rangle = U|\psi\rangle \quad (2.30)$$

görülmektedir. Üniter operatörlerin 3.3.4

$$U\dagger U = UU\dagger = I \quad (2.31)$$

koşulunu sağladığı, dolayısıyla $U\dagger = U^{-1}$ olduğu ifade edilmektedir (Numata, 2024).

Bu yapının en önemli sonucu, kuantum işlemlerinin tersine çevrilebilir olmasıdır. U operatörü uygulandıktan sonra U^{-1} uygulanması durumunda 3.3.5

$$U^{-1}U|\psi\rangle = |\psi\rangle \quad (2.32)$$

sistemin başlangıç durumuna geri döndüğü görülmektedir (Numata, 2024).

2.3.4 Bloch Küresi

|ψ⟩ = α|0⟩ + β|1⟩ ifadesinde α ve β karmaşık sayılardı. Bu karmaşık sayılar $|\alpha|^2 + |\beta|^2 = 1$ koşulunu sağladığından, trigonometrik özdeşlikler kullanılarak qubit durumu yeniden yazılabilmektedir. α ve β karmaşık sayıları 3.4.1

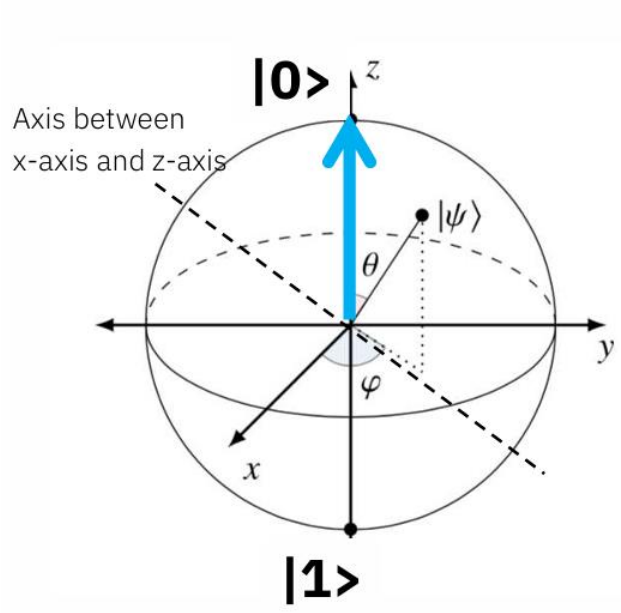
$$\alpha = \cos(\theta/2),\ \beta = e\text{^}(i\varphi)\ \sin(\theta/2) \quad (2.33)$$

formül ile tanımlandığında genel qubit durumu 3.4.2 formül

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e\text{^}(i\varphi)\ \sin(\theta/2)|1\rangle \quad (2.34)$$

biçiminde ifade edilmektedir (Numata, 2024). Bu gösterimde θ ve φ olmak üzere yalnızca iki açı parametresi bulunmaktadır.

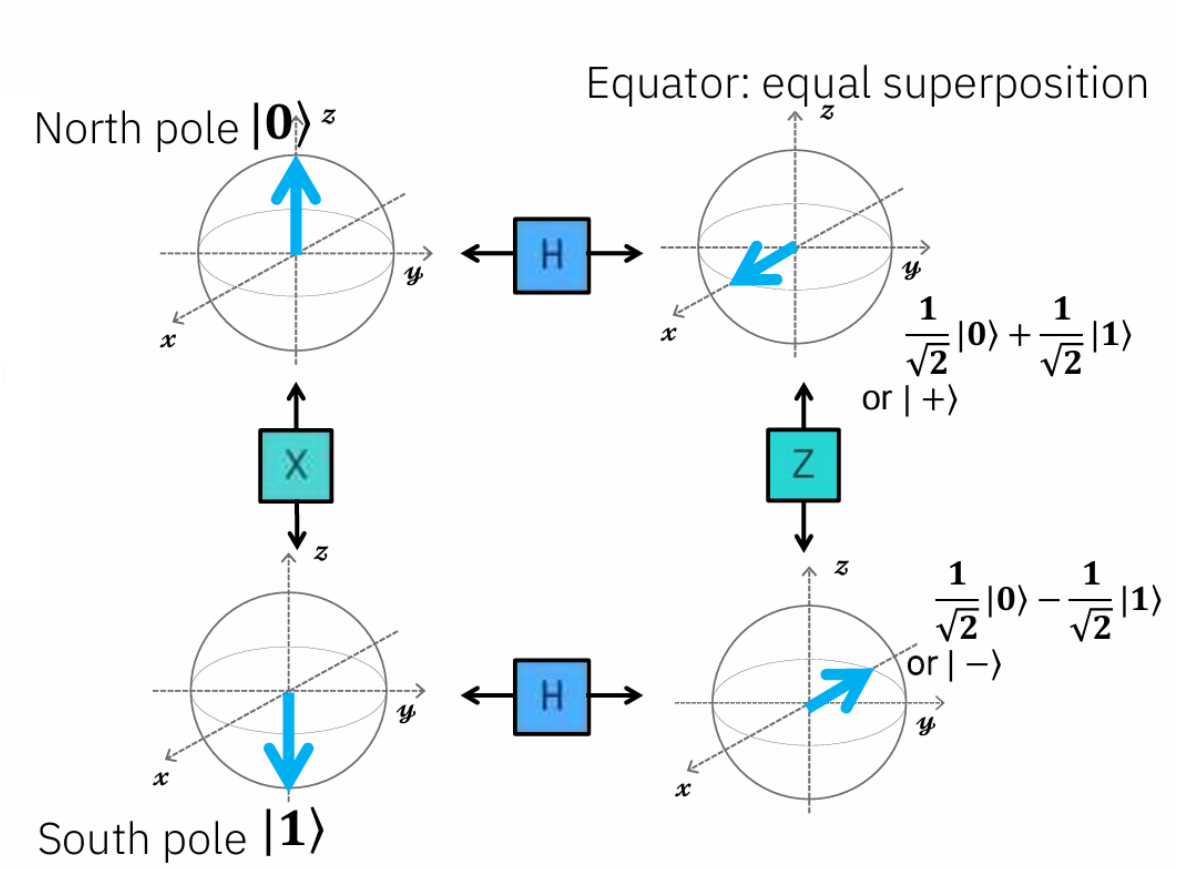
Bu parameterizasyonun önemi, sağdaki şekilde görülmektedir. Her qubit durumu bir birim küre üzerindeki bir noktaya karşılık gelmektedir. Buna Bloch küresi adı verilmektedir. Şekil 2.11'de kürenin kuzey kutbunda |0⟩, güney kutbunda ise |1⟩ durumu yer almaktadır. θ açısı z ekseninden olan sapıklığı, φ açısı ise xy düzlemindeki dönüşü temsil etmektedir. Böylece sonsuz olası qubit durumunun tamamı bu kürenin yüzeyi üzerinde gösterilebilmektedir (Numata, 2024).



Şekil 2.11. Bloch küresi (Numata, 2024, s. 9)

Şekil 2.11'de bloch küresi, saf bir kuantum durumunun yarıçapı 1 olan bir kürenin merkezinden yüzeyine uzanan bir vektörle temsil edildiğini göstermektedir. Kuzey kutbunda |0⟩, güney kutbunda |1⟩ yer almaktadır. θ açısı z ekseninden olan sapıklığı, φ açısı ise xy düzlemindeki dönüşü ifade etmektedir.

Bu yapı Şekil 2.12'de gösterilmektedir.



Şekil 2.12. Bloch küresi (Numata, 2024, s. 9)

|0⟩ durumu kuzey kutbunda, yani z ekseninin yukarısında konumlanmaktadır. X kapısı uygulandığında vektör güney kutbuna dönmekte ve durum |1⟩ olmaktadır. X kapısı Bloch küresi üzerinde z ekseni etrafında 180° döndürme işlemine karşılık gelmektedir.

|0⟩ durumuna Hadamard (H) kapısı uygulandığında vektör kuzey kutbundan ekvator düzlemine inmektedir. Elde edilen durum Denklem (2.35)

$$1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle = |+\rangle \quad (2.35)$$

olarak ifade edilmektedir. Bu eşit süperpozisyon durumudur.

|1⟩ durumuna H kapısı uygulandığında vektör yine ekvator düzlemine gelmekte, ancak bu kez ters yönde konumlanmaktadır. Elde edilen durum Denklem (2.36)

$$1/\sqrt{2}\,|0\rangle - 1/\sqrt{2}\,|1\rangle = |-\rangle \quad (2.36)$$

olarak ifade edilmektedir.

|+⟩ durumuna Z kapısı uygulandığında vektör ekvator düzleminde ters yöne dönmekte ve durum |−⟩ olmaktadır.

2.3.5 Tek qubit kapılarının matris gösterimleri

Tek-qubit kuantum kapıları matris gösterimleriyle tanımlanmaktadır. En temel kapılar Pauli kapıları olarak bilinmekte olup X, Y ve Z olmak üzere üç tanedir ve sırasıyla Denklem (2.37), (2.38) ve (2.39)'te ifade edilmektedir (Nielsen ve Chuang, 2010).

$$X \equiv [[0, 1], [1, 0]] \quad (2.37)$$

$$Y \equiv [[0, -i], [i, 0]] \quad (2.38)$$

$$Z \equiv [[1, 0], [0, -1]] \quad (2.39)$$

Önceki bölümlerde ele alınan X kapısı bu kapılar arasında yer almaktadır. Bir diğer önemli kapı, eşit süperpozisyon durumu oluşturmak için kullanılan Hadamard kapısıdır ve Denklem (2.40)'te ifade edilmiştir.

$$H = (1/\sqrt{2}) \cdot [[1, 1], [1, -1]] \quad (2.40)$$

S ve T kapıları ise faz kapıları olarak sınıflandırılmakta ve sırasıyla $\pi/2$ ve $\pi/4$ faz dönüşümü gerçekleştirmektedir ve Denklem (2.41) ve (2.42)'da ifade edilmektedir.

$$S = [[1, 0], [0, i]] \quad (2.41)$$

$$T = [[1, 0], [0, \exp(i\pi/4)]] \quad (2.42)$$

Son olarak rotasyon kapıları, Bloch küresi üzerinde belirli bir θ açısı kadar dönüşüm gerçekleştirmektedir. X, Y ve Z eksenlerindeki rotasyonlar sırasıyla $R_x(\theta)$, R_y(θ) ve R_z(θ) olarak tanımlanmaktadır ve sırasıyla Denklem (2.43), (2.44) ve (2.45)'da ifade edilmektedir.

$$R_x(\theta) = [[\cos \theta/2, -i \sin \theta/2], [-i \sin \theta/2, \cos \theta/2]] \quad (2.43)$$

$$R_y(\theta) = [[\cos \theta/2, -\sin \theta/2], [\sin \theta/2, \cos \theta/2]] \quad (2.44)$$

$$R_z(\theta) = [[e\text{^}(-i\theta/2), 0], [0, e\text{^}(i\theta/2)]] \quad (2.45)$$

Bu kapıların tamamı üniter matrislerdir ve dolayısıyla (2.31) numaralı koşulu sağlamaktadır (Numata, 2024).

Süperpozisyon, bir qubit durumunun $|0\rangle$ ve $|1\rangle$ temel durumlarının aynı anda bir arada bulunduğu bileşik bir durum olarak ifade edilmesidir. Bu durum (2.28) numaralı denklemde gösterildiği üzere Denklem (2.46)'da ifade edilmiştir.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = (\alpha, \beta)^T \quad (2.46)$$

şeklinde yazılmakta ve $|\alpha|^2 + |\beta|^2 = 1$ koşulunu sağlamaktadır. α ve β katsayılarının ikisi de sıfırdan farklı olduğunda qubit durumunun hem $|0\rangle$ hem de $|1\rangle$ bileşenlerini aynı anda içerdiği görülmektedir. Halk arasında bir qubitin "aynı anda hem 0 hem de 1 olabildiği" şeklinde ifade edilen bu kavramın matematiksel karşılığı süperpozisyon ilkesidir (Numata, 2024).

Ölçüm, süperpozisyon durumundaki bir qubitin gözlemlenmesi sonucunda $|0\rangle$ veya $|1\rangle$ temel durumlarından birine zorla çökmesi işlemidir. (2.46) numaralı denklemde ifade edilen $\alpha|0\rangle + \beta|1\rangle$ durumunda α ve β katsayıları olasılık genlikleri olarak adlandırılmaktadır. Ölçüm sonucunda $|0\rangle$ elde edilme olasılığı $|\alpha|^2$, $|1\rangle$ elde edilme olasılığı ise $|\beta|^2$ olmaktadır. Bu iki olasılığın toplamının (2.29) numaralı koşul gereği 1'e eşit olduğu görülmektedir (Numata, 2024).

Bunu somutlaştırmak için iki örnek verilebilir. Birinci örnekte qubit durumu Denklem (2.47)'de verilmektedir.

$$\sqrt{2}/2\ |0\rangle + \sqrt{2}/2\ |1\rangle \quad (2.47)$$

Burada $|\alpha|^2 = |\beta|^2 = 1/2$ olduğundan $|0\rangle$ ve $|1\rangle$ elde edilme olasılıkları eşittir. İkinci örnekte ise durum Denklem (2.48)'de ifade edilmiştir.

$$\sqrt{3}/2\ |0\rangle - 1/2\ i\ |1\rangle \quad (2.48)$$

Burada $|\alpha|^2 = 3/4$ olduğundan ölçüm sonucunda %75 olasılıkla $|0\rangle$ elde edilmektedir (Numata, 2024).

Standart baz ölçümlerinde iki ölçüm operatörü tanımlanmaktadır. M_0 operatörü $|0\rangle$ durumunu, M_1 operatörü ise $|1\rangle$ durumunu ölçmek için kullanılmaktadır. (2.49) ve (2.50) numaralı denklemde ifade edilmektedir.

$$M_0 = |0\rangle\langle 0| = [[1, 0], [0, 0]] \quad (2.49)$$

$$M_1 = |1\rangle\langle 1| = [[0, 0], [0, 1]] \quad (2.50)$$

(2.46) numaralı denklemde verilen $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ durumu için ölçüm sonuçlarının olasılıkları $\langle\psi|M^\dagger M|\psi\rangle$ ifadesiyle hesaplanmaktadır. Buna göre 0 gözlemlenme olasılığı (2.51) numaralı denklemde

$$p_0 = \langle\psi|M_0^\dagger M_0|\psi\rangle = |\alpha|^2 \quad (2.51)$$

1 gözlemlenme olasılığı ise

$$p_1 = \langle\psi|M_1^\dagger M_1|\psi\rangle = |\beta|^2 \quad (2.52)$$

(2.52) numaralı denklemde elde edilmektedir. Bu sonuç bir önceki slayttaki olasılık genliği tanımıyla örtüşmektedir. Ölçüm gerçekleştikten sonra sistem artık süperpozisyon durumunda kalmamaktadır. Ölçüm sonrasındaki kuantum durumları normalize edilerek

$$M_0|\psi\rangle / \sqrt{p_0} = \alpha/|\alpha|\ |0\rangle \cong |0\rangle \quad (2.53)$$

$$M_1|\psi\rangle / \sqrt{p_1} = \beta/|\beta|\ |1\rangle \cong |1\rangle \quad (2.54)$$

(2.53) ve (2.54) numaralı denklemlerde ifade edilmektedir. Yani ölçüm sonrasında sistem ya tam olarak $|0\rangle$ ya da tam olarak $|1\rangle$ durumuna çökmektedir (Numata, 2024).

$|\psi\rangle$ ve $|\varphi\rangle$ birim vektörler olarak temsil edilen iki kuantum durumu ele alındığında, aralarında $|\alpha| = 1$ koşulunu sağlayan, yani birim çember üzerinde yer alan bir $\alpha = e^{(i\theta)}$ karmaşık sayısı bulunuyorsa

$$|\varphi\rangle = \alpha|\psi\rangle \quad (2.55)$$

bu iki durum global faz farkıyla ayrıldığı söylenmektedir ve (2.55) numaralı denklem ile ifade edilmektedir. Burada α global faz olarak adlandırılmaktadır. Global faz farkına sahip iki durum fiziksel olarak eşdeğer kabul edilmektedir. Bunun nedeni, (2.51) ve (2.52) numaralı denklemlerde ifade edilen ölçüm olasılıklarının her iki durum için de aynı sonucu vermesidir.

$$\langle\varphi|M_j\dagger M_j|\varphi\rangle = \alpha^*\alpha\,\langle\psi|M_j\dagger M_j|\psi\rangle = \langle\psi|M_j\dagger M_j|\psi\rangle \quad (2.56)$$

Denklem (2.56)'de $\alpha^*\alpha = |\alpha|^2 = 1$ olduğundan ölçüm sonuçları değişmemektedir. Bu durumu somutlaştırmak için iki örnek verilebilir. $|+\rangle$ ve $|-\rangle$ durumları birbirinden farklı kuantum durumlarıdır, çünkü aralarındaki fark global faz değil işaret farkından kaynaklanmaktadır. Öte yandan $|-\rangle$ ve $-|-\rangle$ durumları yalnızca $-1 = e^{(i\pi)}$ global fazıyla ayrılmaktadır ve dolayısıyla fiziksel olarak aynı durum olarak kabul edilmektedir (Numata, 2024). Tablo 2.10'da kuantum kapılarının özet tablosu yer almaktadır.

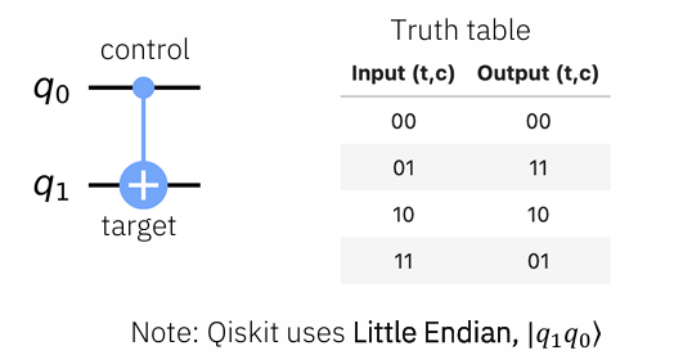
Tablo 2.10. Kuantum kapıları özet tablosu

Kapı	Sembol	Ne yapar?	Klasik karşılığı	Kaç qubit etkiler?
Pauli-X	X	Qubit'i tersine çevirir 0'ı 1, 1'i 0 yapar (0 → 1, 1 → 0)	NOT kapısı	1
Pauli-Z	Z	Fazı (phase) tersine çevirir. $\|0\rangle$ aynı kalır, $\|1\rangle \rightarrow -\|1\rangle$	"işaret/faz çevirme" (klasikte direkt karşılığı yok)	1
Pauli-Y	Y	Hem bit flip hem phase flip yapar	Klasikte tam karşılığı yok.	1
Hadamard	H	Süperpozisyon yaratır: $\|0\rangle \rightarrow (\|0\rangle+\|1\rangle)/\sqrt{2}$, $\|1\rangle$ $\rightarrow (\|0\rangle-\|1\rangle)/\sqrt{2}$ Bir qubiti kesin bir durumdan (0 veya 1) alıp %50 ihtimalle 0, %50 ihtimalle 1 olduğu "süperpozisyon" haline sokar.	Klasikte tam karşılığı yok.	1
CNOT	CX	Kontrol qubit 1 ise hedef qubiti ters çevirir. İki qubit arasında etkileşim kurar. Eğer ilk qubit 1 ise, ikinci qubiti ters çevirir. Kuantum dolanıklık (entanglement) oluşturmak için temel taştır.	Controlled-NOT (XOR)	2
SWAP	SWAP	İki qubit'in yerini değiştirir	değiş tokuş	2
Toffoli	CCX	2 kontrol 1 ise hedefi ters çevirir	Controlled-Controlled-NOT	3

2.3.6 Tipik iki qubitlik kapı

İki-qubit kapıları ise iki qubit arasında koşullu işlemler gerçekleştirmektedir. Bu kapıların en temel örneği CNOT kapısıdır. CNOT kapısı, kontrol qubitinin durumu $|1\rangle$ olduğunda hedef qubit üzerinde

(2.37) numaralı denklemde tanımlanan X kapısını uygulayan koşullu bir kapıdır (Numata, 2024) (Nielsen ve Chuang, 2010).



Şekil 2.13. Devre şeması ve doğruluk tablosu (Numata, 2024, s.15).

Şekil 2.13'te gösterilen devre şemasında q_0 kontrol qubitini, q_1 ise hedef qubitini temsil etmektedir. Doğruluk tablosuna bakıldığında kontrol qubitinin 0 olduğu durumlarda hedef qubitin değişmediği, kontrol qubitinin 1 olduğu durumlarda ise hedef qubitin terslendiği görülmektedir. Qiskit'in Little Endian gösterimi kullandığı ve qubit sıralamasını $|q_1 q_0\rangle$ şeklinde ifade ettiği belirtilmektedir.

İki-qubit sistemler 4 boyutlu durum vektörleriyle temsil edildiğinden CNOT kapısının matrisi de 4×4 boyutundadır. Hangi qubitin kontrol hangisinin hedef olduğuna bağlı olarak iki farklı matris gösterimi bulunmaktadır. (2.57) ve (2.58) denklemlerde ifade edilmiştir.

CNOT (kontrol birinci qubit, hedef ikinci qubit) = [[1, 0, 0, 0], [0, 1, 0, 0], [0, 0, 0, 1], [0, 0, 1, 0]] (2.57)

CNOT (kontrol ikinci qubit, hedef birinci qubit) = [[1, 0, 0, 0], [0, 0, 0, 1], [0, 0, 1, 0], [0, 1, 0, 0]] (2.58)

Farklı kaynak, simülatör ve makalelerin qubit sıralamasını farklı biçimlerde ele aldığı belirtilmektedir. Qiskit'te (2.57) numaralı matrisin yukarıdaki devre şemasına karşılık geldiği ifade edilmektedir (Numata, 2024).

Tek bir qubitin süperpozisyonu (2.46) numaralı denklemde ifade edildiği üzere iki temel durum olan $|0\rangle$ ve $|1\rangle$ üzerinde tanımlıdır. Qubit sayısı arttıkça sistemin süperpozisyon içerebileceği durum sayısı da üstel olarak artmaktadır.

(2.59) numaralı denklemde ifade edilen iki-qubit bir sistem, iki qubitin tensör çarpımıyla oluşturulan $2^2 = 4$ temel durum üzerinde süperpozisyon oluşturabilmektedir.

$$|0\rangle\otimes|0\rangle,\ |1\rangle\otimes|0\rangle,\ |0\rangle\otimes|1\rangle,\ |1\rangle\otimes|1\rangle \quad (2.59)$$

Bu örüntü genel olarak n-qubit sistemlere genelleştirildiğinde, sistemin 2^n temel durum üzerinde süperpozisyon oluşturabildiği görülmektedir. (2.60) numaralı denklemde ifade edilmiştir.

$$|0\rangle_{n-1}\otimes\cdots\otimes|0\rangle_0,\ |0\rangle_{n-1}\otimes\cdots\otimes|1\rangle_0,\ \cdots,\ |1\rangle_{n-1}\otimes\cdots\otimes|1\rangle_0 \quad (2.60)$$

Bu özellik kuantum bilgisayarların klasik bilgisayarlara kıyasla belirli problemlerde üstel hız kazanımı sağlamasının temel nedenidir. n klasik bit yalnızca 2^n durumdan birini temsil edebilirken, n qubit aynı anda tüm 2^n durumun süperpozisyonunda bulunabilmektedir (Numata, 2024).

Çok-qubit sistemlerin matematiksel gösteriminde tensör çarpımı kullanılmaktadır. (2.59) numaralı denklemde yer alan ⊗ sembolü bu işlemi ifade etmektedir. Tensör çarpımının somut bir örneği olarak iki $|0\rangle$ durumunun birleşimi ele alındığında (2.61) numaralı denklemdeki

$$|0\rangle \otimes |0\rangle \equiv |0\rangle|0\rangle = (1,0)^T \otimes (1,0)^T = (1,0,0,0)^T = |00\rangle \quad (2.61)$$

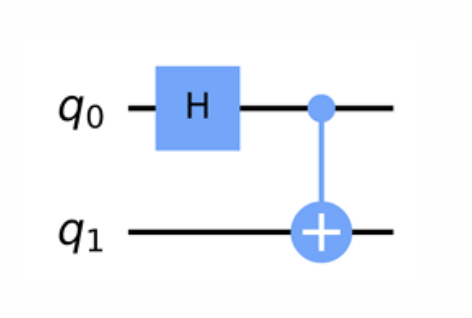
sonucu elde edilmektedir. Görüldüğü üzere iki ayrı 2 boyutlu vektörün tensör çarpımı 4 boyutlu bir vektör oluşturmaktadır. Bu durum (2.57) ve (2.58) numaralı denklemlerde verilen CNOT matrisinin neden 4×4 boyutunda olduğunu açıklamaktadır.

Genel durumda m boyutlu bir vektörle n boyutlu bir vektörün tensör çarpımı m×n boyutlu bir vektör üretmektedir. (2.62) numaralı denklemde ifade edilmiştir.

$$(\alpha_1, \cdots, \alpha_m)^T \otimes (\beta_1, \cdots, \beta_n)^T = (\alpha_1\beta_1, \cdots, \alpha_1\beta_n, \cdots, \alpha_m\beta_n)^T \quad (2.62)$$

Sonuç vektörünün her elemanı, birinci vektörün bir elemanı ile ikinci vektörün tüm elemanlarının çarpımından oluşmaktadır (Numata, 2024).

Dolanık durum, iki qubitten oluşan bir $|\psi\rangle_AB$ sisteminin ayrı ayrı qubit durumlarının tensör çarpımı olarak yazılamadığı durumdur. Bu özellik dolanıklığı süperpozisyondan ayıran temel niteliktir (Numata, 2024).



Şekil 2.14. Devre şeması (Numata, 2024, s.18).

Şekil 2.14'teki devre bu durumu somutlaştırmaktadır. Başlangıç durumu $|0\rangle\otimes|0\rangle = |00\rangle$ olarak alınmaktadır. İlk adımda q_0 üzerine H kapısı, q_1 üzerine ise kimlik operatörü I uygulanmaktadır.

$$|00\rangle \rightarrow (H\otimes I) \rightarrow 1/\sqrt{2}\,(|0\rangle + |1\rangle) \otimes |0\rangle = 1/\sqrt{2}\,(|00\rangle + |10\rangle) \quad (2.63)$$

İkinci adımda bu duruma (2.57) numaralı denklemde tanımlanan CNOT kapısı uygulanmaktadır.

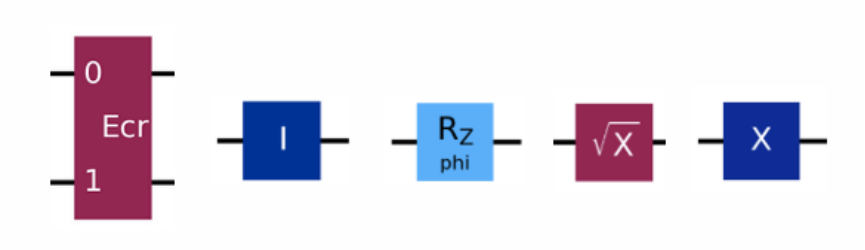
$$1/\sqrt{2}\,(|00\rangle + |10\rangle) \rightarrow (CNOT) \rightarrow 1/\sqrt{2}\,(|00\rangle + |11\rangle) \quad (2.64)$$

(2.64) numaralı denklemde elde edilen $|\psi\rangle_AB = 1/\sqrt{2}\,(|00\rangle + |11\rangle)$ bir birim vektördür. Ancak bu durum ayrışabilir değildir, yani

$$1/\sqrt{2}\,(|00\rangle + |11\rangle) \neq (a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) \quad (2.65)$$

(2.65) numaralı denklemdeki eşitsizliği her a_0, a_1, b_0, b_1 değeri için geçerlidir. Bu, iki qubitin birbirinden bağımsız olarak tanımlanamayacağı anlamına gelmektedir. Bir qubitin ölçüm sonucu diğerini anlık olarak belirlemektedir (Numata, 2024).

Gerçek kuantum donanımı üzerinde yalnızca sınırlı sayıda kapı doğrudan çalıştırılabilmektedir. Bu kapılar kümesine baz kapı kümesi adı verilmektedir.



Şekil 2.15. IBM Quantum Eagle işlemcisinin baz kapı kümesi {ECR, ID, RZ, SX, X} kapılar (Numata, 2024, s.19).

Şekil 2.15'te IBM Quantum Eagle işlemcisinin baz kapı kümesi {ECR, ID, RZ, SX, X} kapılarından oluşmakta olup bu kapıların devre sembolleri sırasıyla gösterilmektedir. ECR kapısı iki girişli bordo renkte, ID kapısı koyu mavi renkte, R_z kapısı φ parametresiyle açık mavi renkte, SX kapısı mor renkte ve X kapısı mavi renkte temsil edilmektedir (Numata, 2024).

Bu kümede yer alan kapıların bir kısmı daha önce tanımlanmıştır. (2.37) numaralı denklemde verilen X kapısı ve (2.45) numaralı denklemde verilen R_z(θ) kapısı bu kümenin birer elemanıdır. ID ise kimlik operatörüdür, qubit durumunu değiştirmeden bırakan birim matristir.

Kümeye özgü iki kapı ise ECR ve SX kapılarıdır. ECR (Echoed Cross Resonance) iki-qubit bir kapıdır ve (2.57) numaralı denklemdeki CNOT kapısının yerini fiziksel donanımda almaktadır. (2.66) numaralı denklemde ifade edilmektedir.

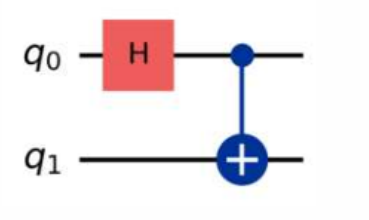
$$\mathrm{ECR} = 1/\sqrt{2} \cdot [[0,0,1,i],[0,0,i,1],[1,-i,0,0],[-i,1,0,0]] \quad (2.66)$$

(2.67) numaralı denklemde SX ise X kapısının kareköküdür ve iki kez uygulandığında X kapısını üretmektedir.

$$\mathrm{SX} = 1/2 \cdot [[1+i,\ 1-i],[1-i,\ 1+i]] \quad (2.67)$$

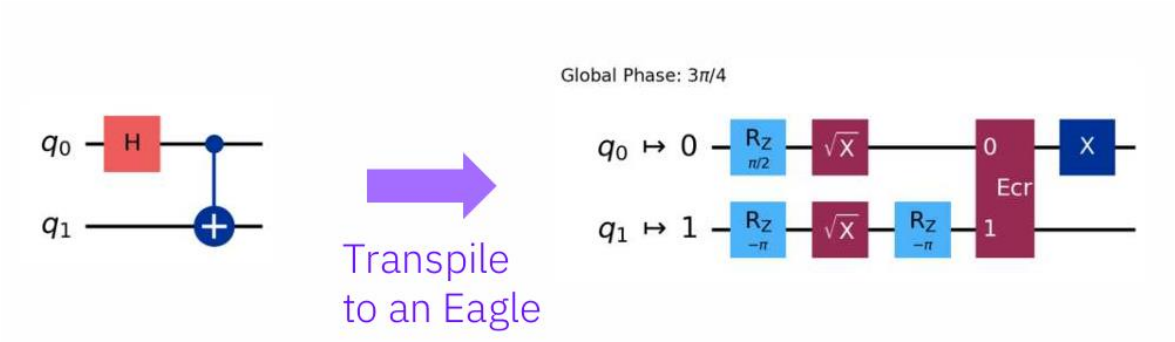
Yazılımda kullanılan H, CNOT gibi kapılar donanımda çalıştırılmadan önce bu baz kapı kümesine derlenmektedir (Numata, 2024).

Baz kapı kümesine dahil olmayan kapılar donanımda doğrudan çalıştırılamamakta, bunun yerine baz kapılara derlenmektedir. Bu işlem transpilasyon olarak adlandırılmaktadır (Numata, 2024).



Şekil 2.16. Devre şeması (Numata, 2024, s.20).

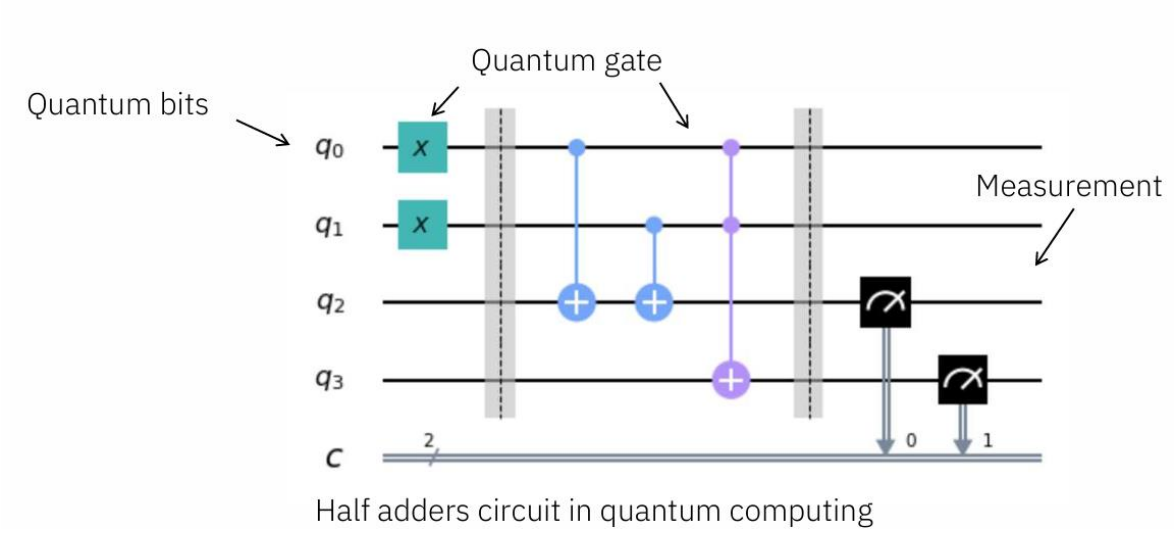
Şekil 2.16'daki (2.64) numaralı denklemde ele alınan dolanık durum devresi yer almaktadır. Bu devre q_0 üzerinde H kapısı ve ardından CNOT kapısından oluşmaktadır.



Şekil 2.17. Transpilasyon (Numata, 2024, s.20).

Şekil 2.17'deki transpilasyon adımından sonra sağ taraftaki devre elde edilmektedir. Derlenen devrede q_0 hattında sırasıyla R_z(π/2), SX, ECR'nin 0 girişi ve X kapıları yer almakta; q_1 hattında ise R_z(−π), SX, R_z(−π) ve ECR'nin 1 girişi kapıları bulunmaktadır. Devrenin üzerinde 3π/4 değerinde bir global faz belirtilmektedir. (2.56) numaralı denklemde ifade edildiği üzere global faz ölçüm sonuçlarını etkilemediğinden bu fark fiziksel olarak anlamlı değildir (Numata, 2024).

Kuantum kapıları, qubit'in durumunu değiştiren ve dönüştüren işlemler olarak düşünülebilir. Kuantum kapılarının çoğu tersinirdir (reversible); yani çıktıdan yola çıkarak giriş durumuna geri dönmek mümkündür. Bu nedenle AND gibi klasik anlamda tersinir olmayan işlemler kuantum devrelerinde doğrudan değil, Toffoli gibi tersinir kapılar yardımıyla gerçekleştirilir. Matematiksel olarak kuantum kapıları üniter matrisler ile temsil edilir.



Şekil 2.18. Kuantum Devre Gösterimi ile Yarım Toplayıcı (Half Adder)(Numata, 2024)

Şekil 2.18'de gösterildiği gibi bu çizim, kuantum bilgisayarda çalışan basit bir devreyi anlatır. Kuantum devresi, klasik devre gibi "kablolar ve üzerlerine konan işlemler" şeklinde düşünülebilir. Şekildeki q0, q1, q2 ve q3 yatay çizgileri, her biri birer qubit hattını temsil eder. İşlemler soldan sağa doğru uygulanır; yani soldaki kapılar önce, sağdakiler sonra çalışır. Devrede görülen X kutuları, klasik bilgisayardaki NOT işlemine benzer; X kapısı bulunduğu hattaki qubit'i ters çevirir (0 ise 1 yapar, 1 ise 0 yapar). Şekilde q0 ve q1 üzerinde X kapısı bulunması, girişleri istenen değere getirmek için yapılmış

bir hazırlık adımı olarak düşünülebilir. Şekildeki ● (dolu nokta) ve ⊕ (artı işareti) birlikte görüldüğünde bu, kontrollü bir işlemi ifade eder: ● kontrol qubitini, ⊕ ise hedef qubitini gösterir. Kontrol edilen hat 1 durumundaysa hedef hatta X (tersleme) uygulanır; kontrol 0 ise hedef hat değişmeden kalır. Bu yapıya CNOT (Controlled-NOT) denir. Şekil 2.18'de mavi bölgede iki adet CNOT vardır: biri q0'ı kontrol edip q2'yi etkiler, diğeri q1'i kontrol edip yine q2'yi etkiler; böylece q2 hattında toplam (sum) biti üretilir. Mor bölgede ise iki tane ● ve bir tane ⊕ bulunur; bu yapı Toffoli (CCNOT) kapısıdır ve iki kontrol aynı anda 1 olduğunda hedef qubit'i tersleyerek q3 hattında elde (carry) bilgisini üretir. Devrenin en sağındaki ölçüm sembolleri q2 ve q3 hatlarında oluşan sonuçların okunmasını sağlar; sonuçta q2 toplamı (sum), q3 ise eldeyi (carry) verir.

Bu kuantum işlemler farklı fiziksel teknolojilerle gerçekleştirilebilir. Süperiletken qubitler, iyon tuzakları ve fotonik sistemler bunların başında gelmektedir.

2.4 Kuantum Donanımı (Qubit Teknolojileri)

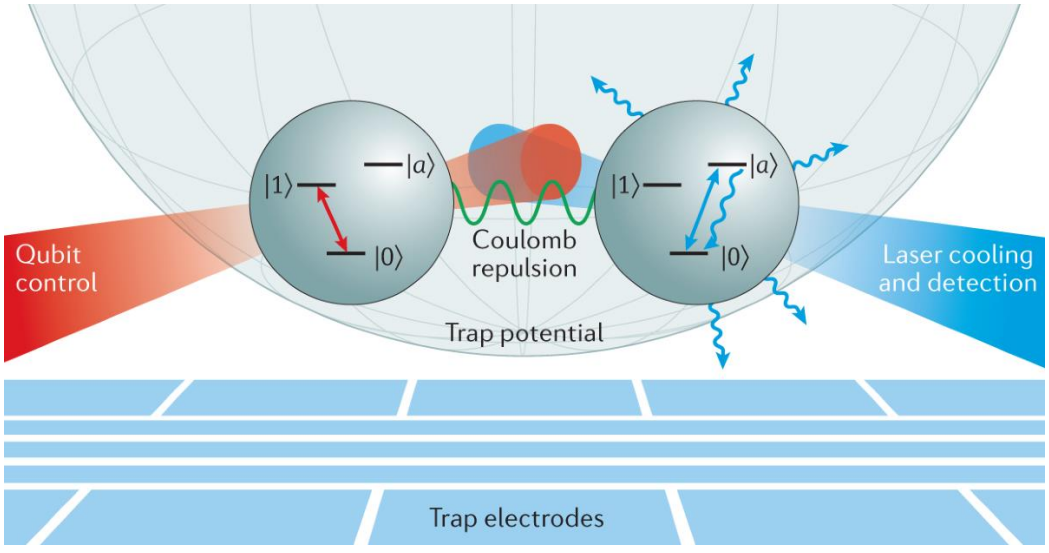
2.4.1 Giriş

Klasik bilgisayarlar bilgiyi bit adı verilen 0 ve 1 değerleriyle temsil ederken, kuantum bilgisayarlar bilgiyi qubit ile temsil eder. Qubitler aynı anda birden fazla durumda bulunabilir ve bu özellik süperpozisyon olarak adlandırılır. Ayrıca iki veya daha fazla qubit arasında dolanıklık (entanglement) oluşabilir ve bu durum kuantum bilgisayarların paralel işlem gücünü artırır (Nielsen ve Chuang, 2010).

Kuantum bilgisayarların fiziksel olarak gerçekleştirilebilmesi için farklı donanım teknolojileri geliştirilmiştir. Bunlar arasında en yaygın olanları ion trap qubit, superconducting qubit ve photon qubit teknolojileridir (Monroe ve Kim, 2013). İyon tuzaklı qubit sisteminin genel yapısı ve çalışma prensibi Şekil 2.19'da gösterilmektedir.

2.4.2 Ion Trap Qubit (İyon Tuzaklı Qubitler)

Ion Trap teknolojisi kuantum bilgisayar alanında en erken geliştirilen yöntemlerden biridir. Bu yöntemde yüklü atomlar (iyonlar) elektromanyetik alanlar kullanılarak bir tuzak içerisinde tutulur ve lazer ışınları ile kontrol edilir. (Monroe ve Kim, 2013).



Şekil 2.19. İyon Tuzaklı Qubit Sisteminin Çalışma Prensibi

Çalışma Prensibi

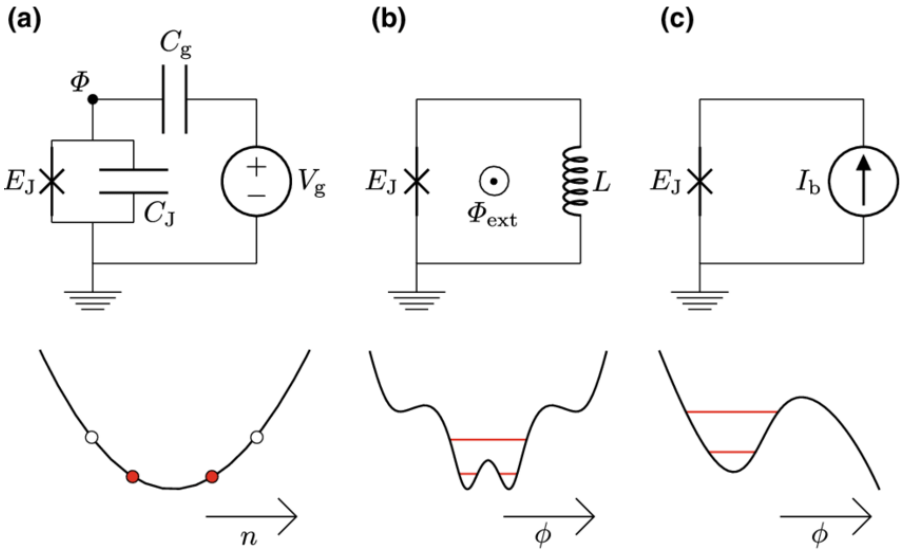
- İyonlar elektromanyetik tuzak içerisinde sabitlenir.
- Lazer ışınları ile iyonların enerji seviyeleri kontrol edilir.
- Bu enerji seviyeleri **0 ve 1 kuantum durumlarını temsil eder.**
- Lazer darbeleri ile entanglement (dolanıklık) oluşturulur.

Ion trap teknolojisi özellikle **hassas kuantum deneylerinde ve araştırma laboratuvarlarında** kullanılmaktadır.

2.4.3 Superconducting Qubit (Süperiletken Qubitler)

Süperiletken qubitler günümüzde en yaygın kullanılan kuantum donanım teknolojilerinden biridir. Bu sistemlerde qubitler süperiletken devreler kullanılarak oluşturulur. Süperiletken devrelerde bulunan Josephson junction yapısı kuantum davranışı mümkün hale getirir (Devoret ve Schoelkopf, 2013).

Süperiletken qubitler günümüzde en yaygın kullanılan kuantum bilgisayar teknolojilerinden biridir. Google, IBM ve Rigetti gibi şirketler bu teknolojiyi kullanmaktadır. Süperiletken qubit devre yapıları ve enerji potansiyel diyagramları Şekil 2.20'da gösterilmektedir.



Şekil 2.20. Süperiletken Qubit Türleri ve Enerji Potansiyel Diyagramları

Çalışma Prensibi

Bu teknolojide qubitler süperiletken devreler üzerinde oluşturulur. Devrelerde bulunan Josephson Junction adı verilen yapı kuantum davranışı sağlar.

Josephson Junction:

İki süperiletken malzeme arasında çok ince bir yalıtkan tabaka bulunur.

Bu yapı sayesinde kuantum enerji seviyeleri oluşturulur.

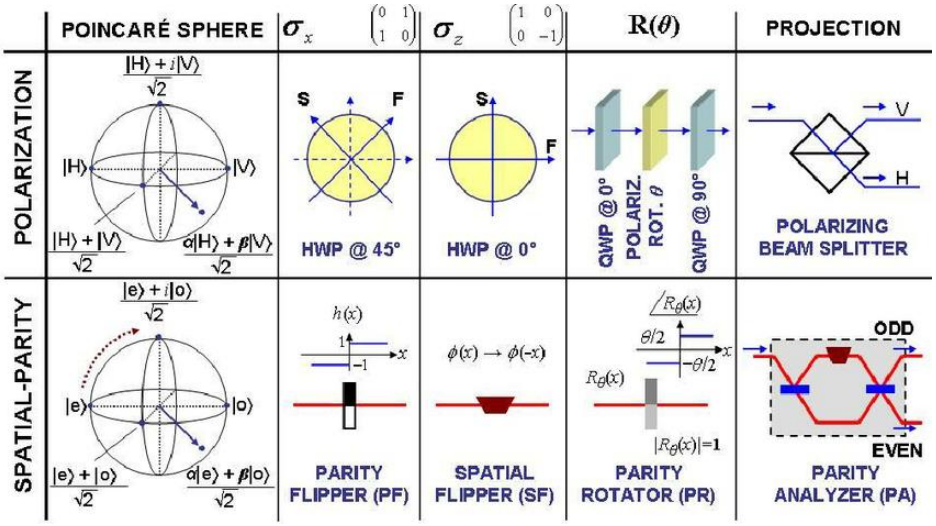
Özellikleri

- Mikrodalga sinyaller ile kontrol edilir
- Çok düşük sıcaklıkta çalışır (~10 mK)
- Çok hızlı kuantum kapıları

IBM Quantum sistemleri bu teknoloji ile geliştirilmiştir.

2.4.4 Photon Qubit (Foton Qubitler)

Photon qubit teknolojisinde bilgi ışık parçacıkları olan fotonlar kullanılarak temsil edilir. Foton qubitleri genellikle fotonların polarizasyon, faz veya yol bilgisi kullanılarak oluşturulur (O'Brien, Furusawa, ve Vučković, 2009). Foton qubitlerinde polarizasyon durumlarının gösterimi ve Poincaré küresi Şekil 2.21'de gösterilmektedir.



Şekil 2.21. Foton Qubitlerinde Polarizasyon ve Poincare Küresi

Çalışma Prensibi

Foton qubitleri genellikle şu özelliklerle temsil edilir:

- Polarizasyon
- Faz
- Yol bilgisi

Örnek:

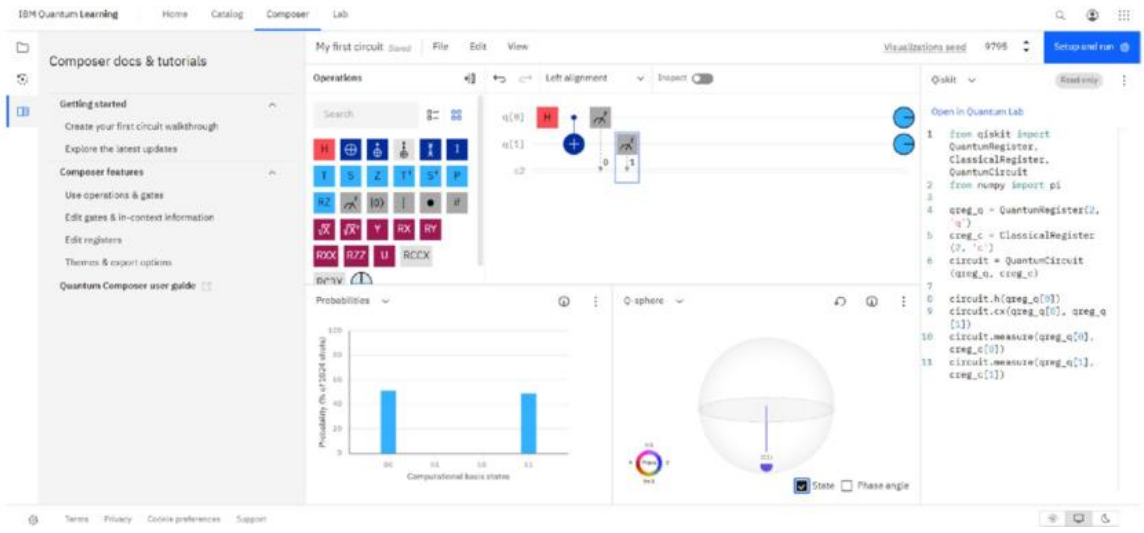
Polarizasyon	Qubit
Dikey	0
Yatay	1

Photon qubit teknolojisi özellikle **kuantum haberleşme ve kuantum kriptografi** alanında kullanılmaktadır.

2.4.5 IBM Quantum Composer

Kuantum bilgisayar donanımları oldukça karmaşık ve maliyetli sistemlerdir. Bu nedenle araştırmacılar ve öğrenciler için bulut tabanlı kuantum bilgisayar platformları geliştirilmiştir. Bu platformlardan biri IBM Quantum Experience sistemidir. Bu platform üzerinden kullanıcılar kuantum devreleri tasarlayabilir ve gerçek kuantum bilgisayarlar üzerinde deneyler gerçekleştirebilir (IBM Quantum, 2024). IBM Quantum Composer arayüzü ve kuantum devre tasarım ortamı Şekil 2.22'de gösterilmektedir.

Platform adresi: IBM Quantum Platform.



Şekil 2.22. IBM Quantum Composer Arayüzü

BÖLÜM 3

Kuantum Anahtar Dağıtımı (QKD) Sistemlerinin Mimari Yapısı, Çalışma Prensibi ve Güvenlik Analizi

Bu bölümde, kuantum haberleşme sistemlerinin temelini oluşturan **Kuantum Anahtar Dağıtımı (QKD)** yapısı incelenmektedir. Özellikle verici (sender), iletim hattı ve alıcı (receiver) bileşenleri üzerinden fotonların nasıl üretildiği, iletildiği ve ölçüldüğü açıklanmakta; ayrıca kuantum durumlarının nasıl okunarak bilgiye dönüştürüldüğü ele alınmaktadır. Bunun yanı sıra, entanglement ve prepare-and-measure yaklaşımları çerçevesinde sistemin çalışma mantığı ve zaman senkronizasyonunun rolü değerlendirilmektedir. Böylece kuantum iletişim süreçlerinin temelini oluşturan fiziksel ve sistemsel yapı kavramsal olarak ortaya konulmaktadır.

3.1 Kuantum Anahtar Dağıtımı: Temel Kavramlar ve Sistem Mimarisi

3.1.1 Kuantum Haberleşme Nedir?

İletişim teknolojilerinin tarihsel gelişimi incelendiğinde, güvenli bilgi aktarımı probleminin her dönemde merkezî bir öneme sahip olduğu görülmektedir. Klasik kriptografik yöntemler, bilginin korunmasını matematiksel güçlüğe dayandırmıştır; ancak bu yaklaşım, hesaplama gücündeki artışla birlikte yapısal kırılganlıklar barındırmaktadır. Kuantum haberleşme, bu kırılganlığa köklü bir yanıt niteliği taşımakta ve güvenliğin temelini matematikten fiziğe taşımaktadır.

Kuantum haberleşme; bilginin klasik bit yerine kuantum bit (qubit) aracılığıyla iletildiği ve kuantum mekaniğinin temel ilkelerinin -süperpozisyon, dolanıklık ve ölçüm geri dönümsüzlüğü- güvenli iletişim amacıyla kullanıldığı bir iletişim paradigmasıdır (Gisin vd., 2002). Bu paradigmada bilgi, kuantum durumlarının üzerine kodlanmakta; söz konusu durumların ölçülmesi ise kaçınılmaz biçimde dalga fonksiyonunun çökmesine -dolayısıyla bilginin bütünlüğünün bozulmasına- yol açmaktadır.

Kuantum haberleşmenin güvenlik mantığının temel taşlarından birini kopyalanamama teoremi (no-cloning theorem) oluşturmaktadır. Bu teorem, bilinmeyen bir kuantum durumunun herhangi bir fiziksel işlemle mükemmel biçimde çoğaltılamayacağını ileri sürmektedir (Wootters ve Zurek, 1982). Klasik haberleşmede bir mesaj kopyalanabilir, depolanabilir ve araya girilerek okunabilir; bu durum pasif dinleme saldırılarını fiziksel olarak mümkün kılmaktadır. Kuantum sistemlerinde ise aynı işlem hem bilgiyi tahrip eder hem de saldırganın varlığını açığa çıkarır. Dolayısıyla kuantum haberleşme, güvenliği yalnızca hesapsal engellere değil, doğa yasalarının kendisine dayandıran özgün bir yapı sunmaktadır.

Bu yapı içinde en belirgin uygulama alanı, iki taraf arasında gizli bir kriptografik anahtar oluşturulmasıdır. Söz konusu süreç -Kuantum Anahtar Dağıtımı (Quantum Key Distribution, QKD)- kuantum haberleşmenin hem teorik hem de pratik açıdan en olgun dalını temsil etmektedir. Bir QKD protokolünde gönderici ve alıcı, kuantum kanalı üzerinden bit bilgisi alışverişi yapar; dinleme girişimi ise kaçınılmaz olarak ölçülebilir hata örüntüleri bırakır ve tespit edilebilir hale gelir (Gisin vd., 2002).

3.1.2 RSA ile QKD Farkı Nedir?

Modern kriptografinin köşe taşlarından biri olan RSA algoritması, güvenliğini büyük asal sayıların çarpanlara ayrılmasının hesapsal güçlüğüne dayandırmaktadır (Rivest vd., 1978). Bu yaklaşımda sistem, potansiyel bir saldırganın mevcut hesaplama kaynaklarıyla söz konusu işlemi makul bir sürede gerçekleştiremeyeceği varsayımı üzerine inşa edilmiştir. Ne var ki bu güvenlik güvencesi koşullu bir

nitelik taşımakta; hesaplama paradigmalarındaki dönüşümle birlikte yapısal kırılganlıklar gün yüzüne çıkmaktadır.

Bu kırılganlık 1994 yılında dramatik biçimde somutlaşmıştır. Peter Shor, kuantum hesaplama modeli üzerinde çalışan bir algoritmayı teorik olarak tanımlamış ve bu algoritmanın büyük tam sayıları asal çarpanlarına polinomsal zamanda ayırabildiğini göstermiştir (Shor, 1994). Bu gelişme, RSA başta olmak üzere hesapsal güçlüğe dayanan tüm asimetrik kriptosistemler üzerinde varoluşsal bir tehdit oluşturmaktadır: yeterli sayıda kararlı qubite sahip bir kuantum bilgisayar, bu sistemlerin güvenlik temelini doğrudan çökertme kapasitesine ulaşabilir.

QKD ise bu tehdidi farklı bir düzlemden yanıtlamaktadır. RSA, 'kırmak hesapsal olarak zordur' öncülüne yaslanırken; QKD, 'kırmak fiziksel iz bırakır' ilkesine dayanmaktadır. İki yaklaşım arasındaki bu asimetri yalnızca teknik bir ayrıntı değil, güvenlik anlayışındaki köklü bir felsefi farklılığın yansımasıdır. RSA'nın güvenliği hesaplama gücüne karşı kırılgan iken, QKD'nin güvenliği kuantum fiziğinin yasalarına dayanmakta ve bu yasaların geçerliliği sürdükçe zaman içinde aşınmamaktadır (Gisin vd., 2002).

Scarani vd. (2009) bu ayrımı teorik açıdan netleştirmektedir: QKD protokollerinin güvenliği bilgi-teorik kanıtlara dayandırılabilir; yani saldırganın hesaplama gücü ne olursa olsun -klasik ya da kuantum- ihlal olasılığı herhangi bir öngörülebilir kaynakla arttırılamaz. RSA için böyle bir güvence söz konusu değildir.

3.1.3 Neden 'Kuantum RSA' Değil, Kuantum Anahtar Dağıtımı?

Kuantum kriptografi tartışmalarında sıkça rastlanan bir kavram karışıklığı, QKD'nin mevcut açık anahtar altyapısının kuantum versiyonu ya da 'kuantum RSA' olarak konumlandırılmasıdır. Bu algı hem terminolojik hem de işlevsel açıdan yanıltıcıdır.

QKD, bir şifreleme algoritması değildir. Sistematik olarak tanımlamak gerekirse: QKD, iki tarafın güvenli bir biçimde rastgele bir bit dizisi üzerinde mutabık kalmasını sağlayan bir anahtar dağıtım protokolüdür (Gisin vd., 2002). Protokolün çıktısı -paylaşılan gizli anahtar- daha sonra simetrik şifreleme algoritmalarıyla ya da bilgi-teorik olarak güvenli tek kullanımlık şifreleme (one-time pad) yöntemiyle birlikte kullanılır. Dolayısıyla QKD, mevcut kriptografik katmanı ikame etmek yerine onun anahtar yönetim bileşenini kuantum fiziğiyle donatmaktadır.

RSA, veri şifreleme, sayısal imza ve kimlik doğrulama gibi geniş bir işlev yelpazesini kapsayan bir kriptosistemdir; QKD ise yalnızca anahtar oluşturma ve dağıtma işleviyle sınırlıdır. Bu işlevsel ayrım, iki sistemin rakip değil tamamlayıcı nitelikte olduğunu ortaya koymaktadır. Nitekim gerçek dünya QKD uygulamalarında kuantum kanalı üzerinden üretilen anahtar, klasik şifreleme altyapısının bir girdisi olarak konumlandırılmaktadır (Scarani vd., 2009).

Öte yandan, Bennett ve Brassard (1984) tarafından ortaya konan BB84 protokolü -QKD'nin ilk ve en temel örneği- bu yapıyı açıkça yansıtmaktadır: protokol bir şifreleme şeması sunmaz; iki tarafın eşit uzunlukta gizli bir bit dizisine güvenle ulaşmasını sağlar. Şifreleme işlemi bu dizinin nasıl kullanılacağına ilişkin bir karar olup protokolün dışında kalır.

3.1.4 Tek Foton Neden Kullanılır?

Kuantum bilgisinin fiziksel taşıyıcısı olarak tek fotonun seçilmesi, kuantum mekaniğinin temel ilkelerinden doğrudan türemektedir. Bu tercihin ardında iki temel gerekçe yatmaktadır: bölünemezlik ve kopyalanamama.

Bir fotonun bölünemez enerji paketi (kuantum) niteliği taşıması, bilginin parçalanamaz bir kuantum birimine kodlanmasını mümkün kılar. Buna karşılık, birden fazla fotona sahip bir ışık darbesi kullanıldığında, potansiyel bir saldırgan darbenin bir bölümünü ayırarak ölçüm yapabilir ve alıcının elindeki bilgiyi etkilemeden bilgiye erişme imkânı bulabilir (Gisin vd., 2002). Bu saldırı türü foton sayısı bölme saldırısı (photon number splitting attack) olarak adlandırılmakta ve çok fotonlu sistemlerin temel güvenlik açığını oluşturmaktadır.

Tek foton, kopyalanamama teoremiyle (Wootters ve Zurek, 1982) birlikte değerlendirildiğinde, sisteme önemli bir güvenlik garantisi sağlamaktadır: bilinmeyen bir kuantum durumu -dolayısıyla üzerine kodlanmış bit bilgisi- mükemmel biçimde kopyalanamaz. Bir saldırgan fotonu ölçmek zorundaysa bu eylem dalga fonksiyonunu çökertir; fotonun durumunu değiştirir ve gönderici ile alıcı arasındaki hata oranını ölçülebilir biçimde yükseltir. Bu durum, aktif dinlemenin izlenebilir kılınmasını fiziksel zorunluluk haline getirmektedir (Gisin vd., 2002).

Pratik uygulamalarda ideal tek foton kaynaklarının üretimindeki teknik güçlükler nedeniyle zayıflatılmış lazer darbeleri yaygın biçimde kullanılmaktadır. Bu yaklaşım, ortalama foton sayısını birden çok küçük tutarak -genellikle 0,1 foton/darbe düzeyinde- çok fotonlu darbelerden kaynaklanan güvenlik açığını minimize etmeye çalışır. Söz konusu pratik kısıtlar, BB84 protokolünün gerçek dünya uygulamaları için kapsamlı güvenlik analizlerini gerekli kılmış ve protokolün önemli ölçüde geliştirilmesine zemin hazırlamıştır (Scarani vd., 2009).

3.1.5 Polarizasyon ve Faz Neden Tercih Edilir?

Foton üzerine kuantum bilgisi kodlamak için çeşitli fiziksel serbestlik dereceleri kullanılabilir. Uygulamada öne çıkan iki temel yöntem, polarizasyon tabanlı kodlama ve faz tabanlı kodlamadır. Her iki yaklaşım da BB84 protokolünün fiziksel gerçekleştirim biçimlerine karşılık gelmekte ve farklı pratik avantajlar sunmaktadır.

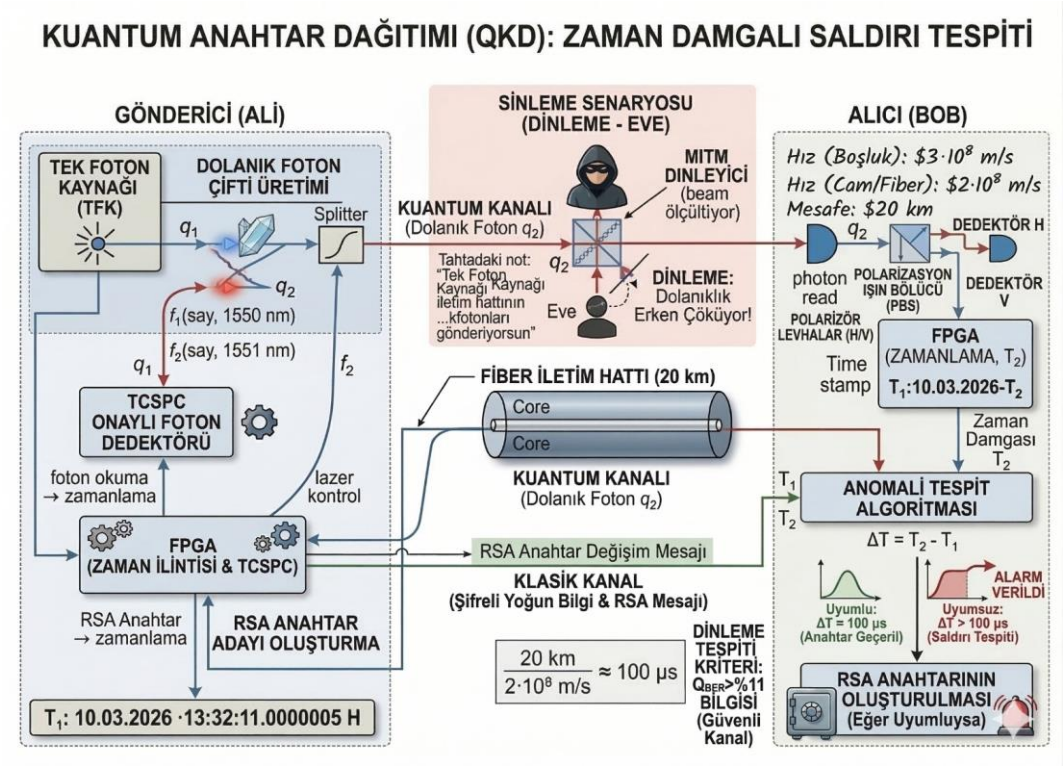
Polarizasyon tabanlı kodlamada, fotonun elektrik alan titreşim yönü bilgi taşıyıcısı olarak kullanılmaktadır. BB84 protokolü, iki farklı taban seti tanımlamıştır: dikdörtgen taban (yatay/dikey: 0°/90°) ve çapraz taban (45°/135°). Gönderici, her bit için rastgele bir taban seçerek fotonunu hazırlar; alıcı ise bağımsız olarak rastgele bir taban seçer ve ölçüm yapar. Taban seçimlerinin yalnızca eşleştiği ölçümler ham anahtar oluşturmak üzere tutulur (Bennett ve Brassard, 1984). Bu tasarımın kilit özelliği, yanlış taban seçimiyle yapılan ölçümün kesin bit bilgisi yerine rastgele bir sonuç üretmesidir; bu durum dinleyici için belirsizliği zorunlu kılmaktadır.

Faz tabanlı kodlama ise referans foton ve bilgi fotonu arasındaki faz farkını bilgi birimi olarak kullanmaktadır. Bu yaklaşım genellikle Mach-Zehnder interferometre düzenekleriyle gerçekleştirilir ve fiber optik sistemlerde önemli pratik avantajlar sunar: polarizasyon, optik fiberde çeşitli fiziksel etkenler (sıcaklık dalgalanmaları, mekanik gerilimler, fiber döngüleri) nedeniyle bozulmaya uğrayabilir. Faz tabanlı sistemlerde bu tür dış etkenlerden kaynaklanan istikrarsızlıklar daha kolay yönetilmektedir (Gisin vd., 2002).

Her iki kodlama yaklaşımında da temel ilke özdeştir: kuantum mekaniğinin doğrusal olmayan ölçüm özelliği, yanlış taban ya da referans seçimiyle yapılan ölçümün bilgi içermemesini -yalnızca gürültü üretmesini- garanti altına alır. Bu garanti, dinleme girişiminin hata oranı üzerinde kaçınılmaz bir iz bırakmasının fiziksel temelidir.

3.1.6 Sistemin Genel Blok Yapısı

Bir QKD sisteminin mimari çerçevesi dört temel bileşen üzerinden tanımlanabilir. Bu bileşenler birbirinden bağımsız işlev blokları olarak değil, tümleşik bir güvenlik altyapısı olarak ele alınmalıdır. Sistemin genel işleyişi Şekil 3.1'de özetlenmektedir. Görselde gönderici (Ali) bloğunda tek foton kaynağı, TCSPC dedektörü ve FPGA zamanlama birimleri; iletim katmanında 20 km fiber optik kuantum kanalı ve klasik kanal; alıcı (Bob) bloğunda polarizasyon ışın bölücü, dedektörler ve anomali tespit algoritması yer almaktadır. Dinleme senaryosunda (Eve) dolanıklık çöküşünün tetiklediği QBER artışı ve zaman damgası uyumsuzluğu ($\Delta T > 100$ μs) saldırı tespitinin fiziksel temeli olarak gösterilmektedir.



Şekil 3.1. QKD sisteminin zaman damgalı saldırı tespiti mimarisi: gönderici (Ali), kuantum/klasik kanallar, dinleme senaryosu (Eve) ve alıcı (Bob) blokları

3.1.6.1 Verici (Alice)

Verici bloğu, sistem sürecinin başlatıcısı ve kuantum bilgisinin üreticisi konumundadır. Bu blokta rastgele bir bit dizisi üretilir; ardından seçilen kodlama protokolüne uygun biçimde -polarizasyon ya da faz- foton durumları hazırlanır. Her bit için taban seçimi rastgele gerçekleşir ve bu seçim gizli tutulur. Hazırlanan foton durumları kuantum kanalına aktarılır. Karar verme sürecinin kalitesi, sistem güvenliğini doğrudan etkileyen kritik bir faktördür; bu nedenle yüksek kaliteli rastgele sayı üretimi -tercihen kuantum rastgele sayı üreteci- temel gereksinim olarak öne çıkmaktadır (Gisin vd., 2002).

3.1.6.2 Kuantum İletim Hattı

İletim hattı, fotonların gönderici ile alıcı arasında fiziksel olarak taşındığı katmanı temsil eder. Uygulamada iki temel ortam kullanılmaktadır: tek modlu optik fiber ve serbest uzay optik bağlantısı. Fiber optik sistemler, yerleşik telekomünikasyon altyapısıyla uyumluluk açısından avantaj sunarken; serbest uzay sistemleri, uydular aracılığıyla uzun mesafeli iletim imkânı sağlamaktadır (Gisin vd., 2002).

Bu katmanın temel kısıtlayıcıları foton kaybı ve gürültüdür. Foton kaybı, iletim mesafesiyle üstel biçimde artmakta ve alınabilecek foton sayısını sınırlamaktadır. Gürültü kaynakları ise hem ortam koşullarından (termal fotonlar, polarizasyon saçınımı) hem de dedektör özelliklerinden (kara akım, zamanlama titreşimi) kaynaklanmaktadır. Kuantum bit hata oranı (QBER), bu katmanın performans kalitesini özetleyen temel ölçüt olarak kullanılmakta; QBER'in belirli bir eşiği -tipik olarak %11- aşması, güvenli anahtar üretimini olanaksız kılmaktadır (Scarani vd., 2009).

3.1.6.3 Alıcı (Bob)

Alıcı bloğu, kuantum kanalından gelen fotonları ölçerek bit değerlerine dönüştürür. Her foton için rastgele bir taban seçilir ve ölçüm gerçekleştirilir. Ölçüm sonuçları kayıt altına alınır; ancak bu aşamada hangi sonuçların geçerli olduğu henüz belli değildir. Geçerlilik tespiti, bir sonraki aşamada klasik iletişim kanalı aracılığıyla göndericiyle taban bilgilerinin karşılaştırılmasıyla yapılır. Eşleşmeyen taban seçimlerinden elde edilen ölçümler atılır; eşleşenler ham anahtar olarak saklanır (Bennett ve Brassard, 1984).

3.1.6.4 Klasik Kontrol ve Zamanlama Altyapısı

QKD sistemlerinin görünmeyen ama vazgeçilmez bileşeni, klasik iletişim katmanı üzerinde yürütülen kontrol protokolleridir. Bu katmanda gerçekleştirilen başlıca işlemler şunlardır: taban mutabakatı, hata oranı tahmini, hata düzeltme (information reconciliation) ve gizlilik güçlendirme (privacy amplification).

Gizlilik güçlendirme, özellikle kritik bir işlemdir: ham anahtardaki olası bilgi sızıntısını -potansiyel bir dinleyicinin ham anahtar üzerindeki kısmi bilgisini- istatistiksel olarak bastırmak amacıyla anahtar kısaltılır ve sıkıştırılır. Bu işlem sonucunda daha kısa ama bilgi-teorik olarak güvenli bir nihai anahtar elde edilir (Scarani vd., 2009).

Bu katmanın kritik bir güvenlik gereksinimi, doğrulanmış (authenticated) olmasıdır. Klasik kanalın şifrelenmesi zorunlu değildir; ancak tarafların kimliklerinin doğrulanması bir ön koşuldur. Doğrulama mekanizması bulunmadığında, sistem ortadaki adam (man-in-the-middle) saldırısına açık hale gelir: saldırgan hem göndericiyle hem de alıcıyla bağımsız QKD oturumları kurarak tüm anahtar değişimini şeffaf biçimde kontrol edebilir. Bu nedenle kimlik doğrulama, güvenli bir başlangıç paylaşık gizli değer gerektirmekte; bu durum önyükleme (bootstrapping) problemi olarak tanımlanmaktadır (Scarani vd., 2009).

3.2 Kuantum Anahtar Dağıtımı (QKD)

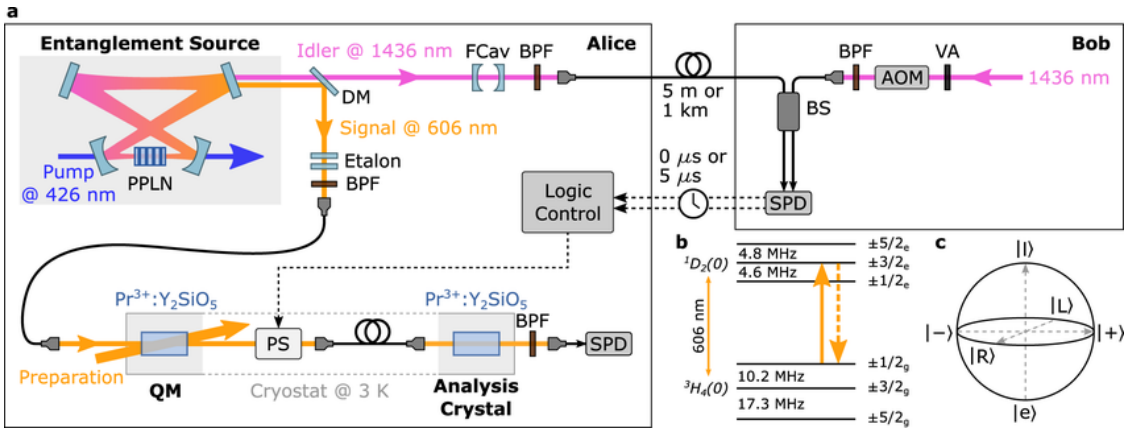
3.2.1 Sistem Mimarisi, Verici-Alıcı Tasarımı ve Zaman Damgalı Saldırı Tespiti

3.2.1.1 Giriş ve Motivasyon

Günümüz şifreleme altyapısının büyük bölümü, RSA gibi asimetrik algoritmalara dayanmaktadır. Bu algoritmaların güvenliği, büyük tam sayıları asal çarpanlarına ayırmanın (integer factorization) klasik bilgisayarlar için pratikte çözülemez bir problem olduğu varsayımına yaslanır. Ancak Shor algoritmasının yeterli ölçekteki bir kuantum bilgisayarda çalıştırılabilir hale gelmesi, bu varsayımı temelinden ortadan kaldıracaktır (Shor, 1994). Üstelik "şimdi topla, sonra çöz" (harvest now, decrypt later) stratejisi, saldırganların bugün şifrelenmiş trafiği depolayıp gelecekteki kuantum bilgisayarlarla çözebileceğini ima eder; bu da tehdidi yalnızca geleceğe ait bir sorun olmaktan çıkarır.

Kuantum Anahtar Dağıtımı (Quantum Key Distribution, QKD), bu tehdide hesaplama güçlüğü yerine doğrudan fizik yasalarını güvenlik temeli olarak kullanarak yanıt verir. QKD'de gizliliğin garantisi şudur: herhangi bir dinleme girişimi, iletilen fotonun kuantum durumunu kaçınılmaz biçimde bozar ve bu bozulma ölçülebilir bir hata oranı artışı olarak ortaya çıkar. Dolayısıyla QKD, bilgi-teorik güvenlik (information-theoretic security) sunan tek anahtar dağıtım paradigmasıdır (Gisin ve ark., 2002).

Bu bölümde incelenen sistem, dolanık foton çifti tabanlı bir QKD mimarisini kapsamlı biçimde ele almaktadır. Sistemin genel mimarisi Şekil 3.2'de gösterilmektedir: Gönderici (Ali) tarafında Tek Foton Kaynağı (TFK) ve SPDC kristali ile üretilen dolanık foton çifti (q_1, q_2), bir Splitter üzerinden iki kola ayrılır. q_2 fotonu yaklaşık 20 km'lik fiber kuantum kanalı üzerinden alıcıya (Buse) iletilirken, FPGA foton üretim olayının T_1 zaman damgasını kaydeder. Klasik kanal, şifreli yoğun bilgi ve RSA anahtar değişim mesajlarını taşır. Bölümün ilerleyen kısımlarında bu mimarinin tüm bileşenleri sırasıyla incelenmektedir.



Şekil 3.2. Kuantum Anahtar Dağıtımı Tam Sistem Mimarisi. Gönderici Ali tarafında TFK ve SPDC kristali dolanık foton çifti (q_1, q_2) üretir; q_2 fiber kuantum kanalıyla alıcı Buse'ye iletilir. FPGA, T_1 zaman damgasını foton üretim tetik olayına atar. Dinleyici Eve'nin varlığı, QBER > %11 ve ΔT > 100 μs koşullarıyla tespit edilir.

Bölüm şu sırayı izlemektedir: 3.2.2'de sistemin iki paralel kanal yapısı ve bileşenlerine genel bakış sunulmaktadır. 3.2.3'te verici tarafın (Ali) mimarisi sekiz kritik soru ekseninde ayrıntılandırılmaktadır; bu kısım bölümün çekirdeğini oluşturmaktadır. 3.2.4'te FPGA'nın zaman damgalama mantığı ve çökme analizi, 3.2.5'te dinleyici tehdit modeli, 3.2.6'da alıcı taraf mimarisi, 3.2.7'de güvenlik analizi ve 3.2.8'de matematiksel ek sunulmaktadır.

3.2.2 QKD Genel Sistem Mimarisi

3.2.2.1 İki Paralel Kanal Yapısı

Sistemin temel mimarisi iki paralel iletim kanalına dayanmaktadır. Kuantum kanal (quantum channel), dolanık foton çiftinin q_2 kolunu fiber optik hat üzerinden alıcıya ulaştırır. Bu kanalda herhangi bir sinyal amplifikasyonu uygulanamaz; zira kuantum hatasız kopyalama (no-cloning theorem) gereğince bir fotonu kopyalayıp güçlendirmek, fotonun kuantum durumunu zorunlu olarak bozacaktır. Klasik kanal (classical channel) ise şifreli yoğun bilgi ve RSA anahtar değişim mesajlarını konvansiyonel elektromanyetik yolla taşır.

Sistem tasarımında iki referans hız değeri kritik öneme sahiptir. Boşlukta ışık hızı $c \approx 3{,}0 \times 10^8$ m/s iken, fiber/cam ortamındaki etkin hız kırılma indisi $n \approx 1{,}5$ nedeniyle daha düşük kalır:

$$v_{\text{fiber}} = c / n = 3{,}0 \times 10^8 / 1{,}5 = 2{,}0 \times 10^8 \text{ m/s} \quad (3.1)$$

Bu hız değerinden hareketle, 20 km'lik fiber kanalda beklenen foton iletim gecikmesi şöyle hesaplanır:

$$\Delta t_{\text{fiber}} = 20 \times 10^3 \text{ m} / 2{,}0 \times 10^8 \text{ m/s} = 100 \ \mu\text{s} \quad (3.2)$$

(3.1) ve (3.2) numaralı denklemlerde elde edilen 100 μs referans gecikmesi, saldırı tespit algoritmasının temel karşılaştırma noktasını oluşturmaktadır. Eğer ölçülen $\Delta T = T_2 - T_1$ bu değeri aşarsa, araya giren bir dinleyicinin ek gecikme yarattığına dair istatistiksel kanıt elde edilir.

3.2.2.2 Sistem Bileşenlerine Genel Bakış

Sistemin bütününü oluşturan yedi temel bileşen Tablo 3.1'de özetlenmektedir. Her bileşenin konumu, görevi ve ürettiği çıktı açık biçimde verilmektedir; ilerleyen alt bölümlerde bu bileşenler tek tek derinlemesine ele alınacaktır.

Tablo 3.1. QKD sistem bileşenleri, konumları, görevleri ve ürettikleri çıktılar.

Bileşen	Konum	Görev	Çıktı
TFK / BBO Kristal	Gönderici (Ali)	SPDC ile dolanık foton çifti üretimi	q_1, q_2 foton çifti
Splitter (PBS)	Gönderici	Fotonları f_1 ve f_2 kollarına ayırma	CW (f_1) ve ACW (f_2) kolları
TCSPC Dedektör	Gönderici - yerel	q_1 tespiti: tetik sinyali üretimi	Elektronik tetik → FPGA
FPGA (Gönderici)	Gönderici	T_1 zaman damgası, HWP kontrol, RSA	T_1 damgası, baz bilgisi, RSA mesajı
Fiber İletim Hattı	`Kanal (~ 20 km)`	q_2 fotonunun Buse'ye iletimi	Fiber çıkışı: q_2
Pol. Dedektör	Alıcı (Buse)	q_2 ölçümü, baz seçimi	Bit değeri + T_2
FPGA (Alıcı)	Alıcı	T_2 damgası, ΔT hesabı, anomali tespiti	Alarm veya RSA anahtarı

3.2.3 Verici Taraf (Ali / Transmitter): Kapsamlı Analiz

Bu bölümün odak sorusu şudur: Gönderici tarafında foton nasıl hazırlanıyor ve nasıl zaman referansına bağlanıyor? Yanıt, birbiriyle bağlantılı sekiz alt soruya verilen yanıtların bütününden oluşmaktadır: (1) Neden tek foton kullanılır? (2) SPDC süreci nedir? (3) Foton nasıl hazırlanır? (4) Polarizasyon ile kuantum durum kodlama nasıl yapılır? (5) Dolanıklık hangi aşamada oluşur? (6) FPGA verici tarafta ne yapar? (7) Zaman damgası mantığı nedir? (8) Bu aşamada neden dalga fonksiyonu çökmez?

3.2.3.1 Tek Foton Kaynağı (TFK): Neden Tek Foton?

Klasik optik haberleşmede lazer ışını, eş fazlı (coherent) çok sayıda foton içeren bir dalga paketi olarak kullanılır. Bu durum, kanalı izleyen bir saldırganın yeterli foton örneği toplayarak bilgiyi sessizce kopyalamasına imkân tanır. QKD'nin güvenlik ilkesi tam bu noktada devreye girer: kopyalanamazlık teoremi (no-cloning theorem, Wootters ve Zurek, 1982) şöyle ifade edilir:

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \text{her } |\psi\rangle \text{ için mümkün değildir.} \quad (3.3)$$

(3.3) denklemi şunu ifade eder: bilinmeyen bir |ψ⟩ kuantum durumunu kopyalayacak üniter bir U operatörü mevcut değildir. Dolayısıyla bilgi tek bir fotona kodlandığında, saldırganın kopyalama girişimi fotonun ölçülmesini, dolayısıyla kuantum durumunun çökmesini zorunlu kılar ve bu çökme sistemde tespit edilebilir bir gürültü izi bırakır (Scarani ve ark., 2009).

Gerçek tek foton kaynakları (kuantum noktaları, NV-merkez defektleri vb.) kriojenik koşullar gerektirdiğinden bu sistemde Spontan Parametrik Aşağı Dönüşüm (Spontaneous Parametric Down-Conversion, SPDC) tercih edilmektedir. Yaklaşık 405 nm UV pompa lazeri, BBO (Beta Baryum Borat, β-BaB_2O_4) kristaline yöneltilir. Kristaldeki ikinci mertebe doğrusal olmayan elektrik duyarlılığı χ^{-2} sayesinde tek bir pompa fotonu, enerjisi ve momentumu korunarak iki alt-foton üretir:

$$\hbar\omega_p = \hbar\omega_q_1 + \hbar\omega_q_2 \text{ (enerji korunumu)} \quad \textbf{(3.4)}$$

$$\hbar\bar{k}_p = \hbar\bar{k}_q_1 + \hbar\bar{k}_q_2 \text{ (momentum korunumu / faz eşleşmesi)} \quad (3.5)$$

(3.4) ve (3.5) denklemlerinde görüldüğü üzere çıkan foton çifti enerji ve momentum bakımından eş güdümlüdür. Tip-II SPDC konfigürasyonunda iki foton birbirine dik polarizasyonlara sahiptir ve polarizasyon serbestlik derecesinde dolanık bir Bell durumu oluştururlar (Kwiat ve ark., 1995). Bu durum bir sonraki alt bölümde ayrıntılı ele alınmaktadır.

Önemli Not: SPDC olasılıksal bir süreçtir. Tipik dönüşüm verimliliği ~10^{-5}– 10^{-7} çift / pompa fotonu düzeyindedir. Bu nedenle yerel koldaki TCSPC dedektörü, q_1 fotonunu tespit ederek "çift üretim olayı gerçekleşti" sinyalini FPGA'ya iletir. Yalnızca bu doğrulanmış olaylar için T_1 zaman damgası kaydedilir.

3.2.3.2 Fotonun Hazırlanması ve Polarizasyon ile Kuantum Durum Kodlama

3.2.3.2.1 BB84 Protokolü: İki Konjuge Baz

Fotonun kuantum bilgiyi taşıyabilmesi için belirli bir polarizasyon durumuna hazırlanması gerekir. Bu işlem BB84 protokolü (Bennett ve Brassard, 1984) çerçevesinde yapılır. Protokol, güvenliğini iki birbiriyle konjuge (conjugate / eşlenik) ölçüm bazının kullanımına borçludur. Z-bazında yatay polarizasyon |H⟩ = |0⟩_Z ve dikey polarizasyon |V⟩ = |1⟩_Z olarak atanır. X-bazında ise:

$$|+45°\rangle = |0\rangle_x = (|H\rangle + |V\rangle) / \sqrt{2} \quad \textbf{(3.6)}$$

$$|-45°\rangle = |1\rangle_x = (|H\rangle - |V\rangle) / \sqrt{2} \quad (3.7)$$

(3.6) ve (3.7) denklemleri, X-bazı durumlarının Z-bazı durumlarının eşit ağırlıklı süperpozisyonu olduğunu göstermektedir. Z-bazı ile X-bazı Bloch küresi üzerinde birbirine dik yönlere karşılık gelir; bu Heisenberg belirsizlik ilkesi gereğince eşzamanlı kesin ölçüme olanak vermez. Dinleyici doğru bazı bilemediği için yanlış baz seçildiğinde ölçüm rastgele sonuç verir ve sistemde istatistiksel iz bırakır (Shor ve Preskill, 2000).

3.2.3.2.2 Durum Hazırlama Devresi: HWP ve PBS

Fotonun polarizasyon durumu, yarım dalga levhası (Half-Wave Plate, HWP) ve polarizasyon ışın bölücü (Polarizing Beam Splitter, PBS) kombinasyonuyla belirlenir. HWP, döndürme açısı θ ile fotonun polarizasyon yönünü döndürür; PBS ise fotonu seçilen baza göre iki kola ayrıştırır. FPGA, rastgele sayı üreticisinden gelen baz kararına göre θ değerini anlık olarak ayarlar. Dört BB84 durumuna karşılık gelen HWP açıları ve qubit karşılıkları Tablo 3.2'de verilmektedir.

Tablo 3.2. BB84 protokolünde HWP açısı, foton polarizasyon durumu ve qubit karşılığı. θ = 22,5° ayarı X-bazını seçer (Bennett ve Brassard, 1984).

HWP Açısı (θ)	Foton Durumu	Qubit Karşılığı	Baz
0°	|H⟩ - Yatay polarizasyon	|0⟩z (Z-bazı bit-0)	Z
0°	|V⟩ - Dikey polarizasyon	|1⟩z (Z-bazı bit-1)	Z
22,5°	|+45°⟩ - Diyagonal	$\|0\rangle_x = (\|0\rangle+\|1\rangle)/\sqrt{2}$	X
22,5°	|−45°⟩ - Anti-diyagonal	$\|1\rangle_x = (\|0\rangle-\|1\rangle)/\sqrt{2}$	X

Tablo 3.2'deki dönüşümün matematiksel ifadesi şudur: HWP ve PBS, fotonun durum vektörüne üniter bir operatör uygular.

$$|\psi_{çıkış}\rangle = U^{HWP} \cdot U^{PBs} \cdot |\psi_{giriş}\rangle \quad \textbf{(3.8)}$$

(3.8)'de görüldüğü üzere HWP'nin etkisi $U_{HWP} = exp(i\cdot\theta\cdot\sigma_y)$ şeklinde yazılabilir. Bu operatör üniterdir (U†U = I) ve normu korur; dolayısıyla fotonun kuantum bilgisi bozulmadan iletilir. Dalga fonksiyonunun çökmesi yalnızca Bob'un dedektöründe gerçekleşecektir; bu meseleye 4.4.4 alt bölümünde ayrıntılı dönülecektir.

3.2.3.3 Dolanıklık (Entanglement): Hangi Aşamada ve Nasıl Oluşur?

Dolanıklık, sistemde aktif olarak "üretilen" ayrı bir adım değildir; BBO kristalindeki SPDC etkileşimi sırasında foton çifti üretim anında kendiliğinden oluşur. Tip-II SPDC konfigürasyonunda çıkan iki foton birbirine dik polarizasyonlara sahiptir ve polarizasyon serbestlik derecesinde $|\Phi^+\rangle$ Bell durumunu oluştururlar (Kwiat ve ark., 1995):

$$|\Phi^+\rangle = 1/\sqrt{2} \cdot (|H\rangle_1 |V\rangle_2 + |V\rangle_1 |H\rangle_2) \quad \textbf{(3.9)}$$

(3.9) denklemi şunu ifade eder: iki fotondan herhangi birinin polarizasyonu ölçülmeden önce sistemin tanımlı bir polarizasyon değeri yoktur; yalnızca birleşik sistemin belirli bir dolanıklık yapısı mevcuttur. Bu, aşağıdaki operasyonel sonucu doğurur: bir dinleyici q_2 fotonunu ölçtüğünde, korelasyon istatistikleri bozulur ve bu bozulma alıcı tarafında tespit edilebilir. Dolanıklığın sistem genelindeki yaşam döngüsü Tablo 3.3'te özetlenmektedir.

Aşama	**Fiziksel İşlem**	**Dolanıklık Durumu**
Pompa öncesi	UV lazer fotonu kristale girmeden önce	Yok - tek foton durumu
SPDC etkileşimi	χ^{-2} etkileşimi: 1 pompa → q_1 + q_2	Bu anda oluşur: $\|\Phi^+\rangle$
Splitter sonrası	q_1 yerel kol, q_2 kuantum kanalı	Korunur - fotonlar ayrılır

Aşama	Fiziksel İşlem	Dolanıklık Durumu
Normal iletim	q_2 fiber kanalda ilerler	Korunur - ölçüm yok
Eve müdahalesi	Eve q_2'yi durdurur ve ölçer	Bozulur - Bell ihlali kaybolur

Tablo 3.3. Dolanıklığın sistemdeki oluşma aşaması ve yaşam döngüsü. Dolanıklık SPDC etkileşimi anında meydana gelir ve herhangi bir ölçüm yapılmadığı sürece korunur.

> ***Schmidt ayrışımı perspektifinden bakıldığında, $\|\Phi^+\rangle$ durumunun iki sıfır dışı Schmidt katsayısı ($\lambda_1 = \lambda_2 = 1/\sqrt{2}$) mevcuttur. Tek sıfır dışı katsayısı olsaydı durum ürün (product) formuna ayrışabilir, dolayısıyla dolanık sayılmazdı. İki eşit katsayı, maksimal dolanıklığa ve Von Neumann entropisi S(ρ_A) = 1 ebit değerine karşılık gelir. Bu değer dolanıklık kalitesinin ölçütüdür.***

3.2.4 FPGA'nın Verici Taraftaki Rolü, Zaman Damgası Mantığı ve Çökme Analizi

3.2.4.1 FPGA Verici Tarafta Ne Yapar?

Alan-programlanabilir kapı dizisi (Field-Programmable Gate Array, FPGA), verici tarafta dört görevi üstlenir. Tablo 3.3, bu görevleri ve her birinin kuantum kanalıyla etkileşim içerip içermediğini göstermektedir.

Tablo 3.4. FPGA'nın verici taraftaki dört görevi ve kuantum kanalıyla etkileşim analizi. Hiçbir görev q_2 fotonunu doğrudan ölçmez veya etkiler.

FPGA Görevi	Açıklama	Kuantum Etkileşimi?
Lazer tetikleme	Pompa lazerinin atım zamanlamasını kontrol eder	Hayır - klasik elektronik
$T_ı$ zaman damgası	$q_ı$ tetik sinyalini alır; pikosaniye hassasiyetle damgalar	Hayır - klasik elektronik sinyal
HWP baz seçimi	Rastgele baz kararına göre θ açısını kontrol eder	Dolaylı - üniter optik
RSA senkronu	Anahtar adayını klasik kanal üzerinden iletir	Hayır - klasik şifreleme

3.2.4.2 Neden FPGA Ölçüm Yapmaz? - Fiziksel Zorunluluk

FPGA'nın q_2 fotonunu ölçmemesi bir tasarım tercihi değil, fiziksel bir zorunluluktur. Kuantum mekaniğinin ölçüm postülatı şunu öngörür: bir {M_m} ölçüm operatörleri kümesiyle $|\psi\rangle$ durumu ölçüldüğünde m sonucu şu olasılıkla ortaya çıkar:

$$P(m) = \langle\psi| M^T_m M_m |\psi\rangle \quad \textbf{(3.10)}$$

ve sistem şu biçimde güncellenir:

$$|\psi\rangle \longrightarrow M_m |\psi\rangle / \sqrt{P(m)} \quad \textbf{(3.11)}$$

(3.10) ve (3.11) denklemlerinde görüldüğü üzere bu güncelleme geri döndürülemezdir ve projeksiyon nedeniyle bilgi silinir. Eğer FPGA q_2 fotonunu ölçseydi üç kritik sonuç kaçınılmaz olurdu:

- Fotonun polarizasyon durumu $|\psi_polarize\rangle \rightarrow |H\rangle$ veya $|V\rangle$ biçiminde çökerdi ve Bob'a iletilmesi gereken kuantum bilgi yok edilirdi.
- q_1-q_2 dolanıklığı bozulurdu. Ali'nin kendi sisteminde yaptığı ölçüm (3.9)'daki Bell durumunu çökertir, sistem güvenlik kanıtları geçersiz kalırdı.
- Bob boş veya yanlış durumda bir foton alırdı; güvenli anahtar üretimi mümkün olmazdı.

Bu üç neden, FPGA'nın neden yalnızca q_1 fotonunun TCSPC dedektöründe oluşturduğu klasik elektronik tetik sinyalini işlediğini açıklamaktadır. Bu sinyal fotonun kuantum durumuna hiçbir şekilde dokunmaz; yalnızca "foton üretim olayı gerçekleşti" bilgisini taşır.

3.2.4.3 Zaman Damgası Mantığı: T_1 Fotona Değil, Tetik Olayına Atanır

Sistemin güvenlik zincirinin en kritik kavramsal ayrımı şudur: T_1 zaman damgası, fotonun kendisine değil foton üretim/tetik olayına atanır. Bu ayrımın üç fiziksel gerekçesi mevcuttur:

- Foton bir kuantum nesnedir. Zaman-enerji belirsizliği $\Delta E \cdot \Delta t \geq \hbar/2$ gereğince fotonun kesin varoluş zamanı tanımlanamaz.
- Fotonu doğrudan "damgalamak" bir ölçüm aygıtının temas etmesini gerektirir. Bu temas Born kuralı gereğince (3.11) fotonun kuantum durumunu çökerterek polarizasyon bilgisini yok eder.
- Çözüm: q_1 fotonunun TCSPC dedektöründe yarattığı elektronik tetik sinyali foton üretim süreciyle eşzamanlıdır; ancak q_2 fotonunun kuantum durumuna dokunmaz.

T_1 Zaman Damgası Örneği: T_1 = 10.03.2026 · 13:32:11,000 000 5 H
Bu damga, q_1 fotonunun TCSPC dedektörüne çarptığı elektronik olay zamanını temsil eder. q_2 fotonu bu anda henüz fiber kanaldadır ve kuantum durumu korunmaktadır. FPGA'nın ~10 ps hassasiyeti, fiber kanalın ~100 µs gecikme bütçesinin yanında ihmal edilebilir düzeydedir.
Beklenen Gecikme: 20 km / ($2{,}0 \times 10^8$ m/s) = 100 µs - (3.2) denkleminden

3.2.4.4 Neden Bu Aşamada Dalga Fonksiyonu Çökmez?

3.2.4.4.1 Hazırlama ile Ölçümün Matematiksel Karşılaştırması

Dalga fonksiyonu çökmesi, kuantum mekaniğinin ölçüm postülatının geri döndürülemez bir projeksiyon işlemi içermesinden kaynaklanır. Buna karşın verici taraftaki foton hazırlama, durum

vektörüne üniter operatörler uygulamaktan ibarettir. İki işlem arasındaki fark Tablo 3.4'te karşılaştırmalı olarak sunulmaktadır.

Tablo 3.5. Hazırlama, ölçüm ve FPGA tetik kaydının matematiksel karşılaştırması. Yalnızca kuantum ölçüm işlemi çökmeye yol açar.

İşlem Türü	Matematiksel Yapı	Norm	Geri Dönüşüm	Çökme
Foton hazırlama (HWP)	U|ψ⟩, üniter U†U = I	Korunur	Mümkün	HAYIR
Kuantum ölçüm	M_m|ψ⟩/√P(m), projektör	Bozulur	İmkânsız	EVET
FPGA tetik kaydı	Klasik elektronik sinyal	-	-	HAYIR

3.2.4.4.2 Foton Yaşam Döngüsü ve Çökme Anı

Verici taraftan alıcı tarafına uzanan fotonun tüm yaşam döngüsü üç evreden oluşmaktadır; bu evrelerin tamamında çökmenin gerçekleşip gerçekleşmediği ve T damgalarının nasıl atandığı aşağıda verilmektedir:

- Hazırlık evresi (Ali): SPDC ile üretim → HWP/PBS ile üniter dönüşüm (3.8) → fiber kanala giriş. Tüm işlemler üniter; Tablo 3.4'e göre çökme yok. T_1 damgası bu evrede, q_1 tetik sinyali aracılığıyla atanır.
- İletim evresi (fiber kanal, ~100 μs): q_2 fotonu ~20 km fiber boyunca yayılır. Kasıtlı ölçüm yoktur; dalga fonksiyonu koheransını koruyarak ilerler. Dekoherans riski yönetimi 4.4.5'te ele alınmaktadır.
- Ölçüm evresi (Buse/Bob): Alıcının PBS dedektörü q_2 fotonunu absorbe eder → (3.11) Born kuralı projeksiyonu gerçekleşir → durum çöker. T_2 damgası bu anda atanır.

Özet: Verici tarafta OLAN işlemler: foton üretimi, dolanıklık oluşumu (3.9), üniter polarizasyon hazırlama (3.8), T_1 tetik damgası.
Özet: Verici tarafta OLMAYAN işlemler: q_2 ölçümü, dalga fonksiyonu çökmesi, dolanıklık bozulması, T_1'in fotona atanması.

3.2.4.4.3 Dekoherans Riski ve Yönetimi

Fotonun fiber kanalda ilerlerken koheransını kaybetme riski üç kaynaktan beslenir: polarizasyon modu dağılımı (PMD), Rayleigh saçılması ve fiber içi birefringence (çift kırınım). Bu riskler iki strateji ile yönetilmektedir. Birincisi, f_1 ve f_2 frekanslarının yakın dalga boylarında (örn. 1550 nm ve 1551 nm) tasarlanması sağlanır; böylece her iki foton fiber içi kayıplardan benzer biçimde etkilenir ve zaman korelasyonu ölçümlerinin güvenilirliği artar. İkincisi, fiber kanal boyu ~20 km ile sınırlı tutularak dekoherans etkilerinin kritik eşiğin altında kalması hedeflenir.

3.2.4.5 Verici Taraf Tam Sistem Akışı

4.3.1'den 4.4.4'e kadar aktarılan tüm bileşenlerin işleyişi aşağıdaki adım dizisinde bütünleşik olarak görülmektedir. Bu akış, Şekil 3.1'deki tam sistem diyagramında da izlenebilir:

- UV pompa lazeri FPGA tetikiyle ateşlenir; lazer fotonları BBO kristaline gönderilir.

- SPDC etkileşimi (3.4) ve (3.5) korunumu altında q_1-q_2 çiftini üretir; fotonlar (3.9)'daki $|\Phi^+\rangle$ Bell durumunda dolanık olarak kristalden çıkar.
- Splitter, q_1'i yerel TCSPC dedektörüne, q_2'yi fiber kuantum kanalına yönlendirir.
- TCSPC dedektörü q_1'i algılar, klasik elektronik tetik sinyali FPGA'ya iletilir.
- FPGA tetik sinyalini T_1 zaman damgasıyla işaretler (örn. T_1 = 10.03.2026 · 13:32:11,000 000 5 H).
- Eşzamanlı olarak FPGA, rastgele baz kararını HWP'ye iletir; HWP üniter dönüşümle (3.8) q_2'nin polarizasyon durumunu hazırlar.
- q_2 fotonu ~100 μs gecikme süresinde fiber kanalı kat ederek alıcıya ulaşır. Bu süre boyunca dalga fonksiyonu çökmez (Tablo 3.4).
- FPGA, T_1 damgasını ve RSA anahtar adayını klasik kanal üzerinden Buse'ye gönderir.

3.2.5 Dinleyici Tehdit Modeli: Eve'nin Saldırı Senaryosu

3.2.5.1 Man-in-the-Middle (MITM) Saldırısı

Şekil 3.2'deki dinleyici (Eve) senaryosunda saldırgan, fiber kanalın bir noktasında q_2 fotonunu durdurur, ölçüm yapar ve ardından bir vekil foton gönderir. Bu saldırı iki bağımsız mekanizma tarafından tespit edilir.

Birinci mekanizma zaman anomalisidir. (3.2) denkleminden elde edilen 100 μs referans gecikmesine ek olarak, Eve'nin ölçüm-yeniden gönderim (intercept-resend) döngüsü kaçınılmaz biçimde ek gecikme yaratır:

$$\Delta T_gözlenen = T_2 - T_1 > 100\ \mu s \Rightarrow Saldırı\ tespiti \quad (3.12)$$

İkinci mekanizma QBER yükselmesidir. Eve doğru bazı bilemediği için rastgele baz seçecektir. BB84 analizine göre her fotona müdahale eden Eve %25 ek hata yaratır; yaklaşık %11 QBER eşiği asimptotik analizlerde kullanılan tipik güvenlik sınırı olarak ele alınmıştır:

$$QBER_{toplam} = QBER_0 + f_Eve / 4 \quad (3.13)$$

f_Eve = 1 (tüm fotona müdahale) durumunda (3.13) ile QBER_Eve = 0,25 elde edilir. QBER_toplam > 0,11 koşulu sağlandığında sistem alarmı tetikler ve anahtar reddedilir.

3.2.5.2 Dolanıklık Korelasyonlarının Saldırı Tespitindeki Rolü

(3.9)'daki Bell durumunun dolanık olması ek bir güvenlik katmanı sağlar. Eve'nin q_2 fotonunu ölçmesi dolanıklık korelasyonunu yok eder. Bu etki, q_1 ve q_2 ölçüm sonuçları arasındaki korelasyon katsayısının Bell eşitsizliği sınırının altına düşmesiyle istatistiksel olarak tespit edilir (Aspect ve ark., 1982):

$$|E(a,b) + E(a,b') + E(a',b) - E(a',b')| \leq 2 \text{ (Bell sınırı)} \quad (3.14)$$

Dolanık foton çiftleri (3.14)'ü ihlal ederek bu sınırı aşar. Eve müdahalesi bu ihlali ortadan kaldırır ve korelasyon istatistiklerinde iz bırakır. Bu iki mekanizma - (3.12) ve (3.13) - birbirinden bağımsız olduğundan, ikisinin de aynı anda geçilmesi güvenlik kanıtını önemli ölçüde güçlendirir.

3.2.6 Alıcı Taraf (Buse / Bob): Ölçüm ve Anahtar Üretimi

3.2.6.1 Polarizasyon Dedektör Sistemi

Alıcı tarafta gelen q_2 fotonu, polarizör levhalar (H/V) veya yarım dalga levhasından geçirilir; ardından PBS, fotonu iki kola ayrıştırır. Dedektör H veya V kolunda foton algıladığında hem ölçüm sonucu hem de T_2 zaman damgası belirlenir. Bu ölçüm anı, Tablo 3.4'te de görüldüğü üzere dalga fonksiyonunun çöktüğü tek andır.

BB84 protokolünde Buse baz seçimini rastgele yapar. Yalnızca Ali ile aynı bazı seçtiği fotonlar - tüm iletimlerin yaklaşık yarısı - ham anahtar bit'lerine dönüştürülür. Farklı baz seçilen fotonlar, baz uzlaştırma (basis reconciliation) aşamasında klasik kanal üzerinden elenir.

3.2.6.2 Anomali Tespit Algoritması

Buse'nin FPGA'sı, q_2 dedektöründen gelen tetik sinyaline T_2 damgasını atar. Ardından Ali'nin klasik kanal üzerinden ilettiği T_1 değeriyle $\Delta T = T_2 - T_1$ hesaplanır. Tablo 3.5, anomali tespit algoritmasının karar matrisini sunmaktadır.

Tablo 3.6. Anomali tespit algoritmasının karar matrisi. ΔT referans değeri (3.2) denkleminden, QBER eşiği ise (3.13) analizinden elde edilmektedir.

ΔT Koşulu	**Fiziksel Yorum**	**Karar**
$\Delta T \approx 100$ μs (±tolerans)	Normal fiber gecikmesi: (3.20) ile uyumlu - saldırı yok	✓ Uyumlu: RSA anahtarı oluşturulur
$\Delta T > 100$ μs	Eve ek gecikme yarattı - (3.12) ihlali	✗ Alarm: Anahtar reddedilir
$\Delta T \ll 100$ μs	Fiziksel olarak imkânsız - sahte sinyal şüphesi	✗ Alarm: Protokol yeniden başlatılır
QBER > %11	Eve müdahalesi veya kanal gürültüsü - (3.13) ihlali	✗ Alarm: Gizlilik güçlendirme

3.2.6.3 RSA Anahtar Oluşturma Süreci

ΔT tolerans sınırları içindeyse ve QBER < %11 ise sistem RSA anahtar adayını kesinleştirir. Bu süreç dört aşamadan oluşmaktadır:

- Ham anahtar: Eşleşen baz ölçümlerinden ham bit dizisi elde edilir.

- Hata düzeltme (error correction): Cascade veya LDPC protokolleri ile klasik kanal üzerinden hata giderimi yapılır.
- Gizlilik güçlendirme (privacy amplification): Eve'nin olası kısmi bilgisini ortadan kaldırmak için evrensel hash fonksiyonu uygulanır.
- RSA oturum anahtarı: Güvenli ham materyal, şifreli klasik haberleşme için oturum anahtarına dönüştürülür.

3.2.7 Güvenlik Analizi

3.2.7.1 Kanıtlanabilir Güvenlik Temeli

QKD güvenliğinin formal kanıtı iki ilkeye dayanır. Mayers (2001) tarafından geliştirilen kanıt, Eve'nin elinde bulunan bilgi miktarının gizlilik güçlendirme aşamasından sonra istenen herhangi bir ε değerinin altına indirilebileceğini göstermektedir. Shor ve Preskill (2000) ise BB84'ün güvenliğini kuantum hata düzeltme teorisi çerçevesinde ispat etmiştir. Asimptotik güvenli anahtar hızı şöyle ifade edilir:

$$R_s \geq q \cdot [\, 1 - f(e)\, H(e) - H(e)\,] \qquad (3.15)$$

(3.15)'te q = 1/2 olasılık faktörünü, f(e) hata düzeltme verimliliğini (tipik ~1,16), e = QBER ve H(e) = −e $\log_2$(e) − (1−e) $\log_2$(1−e) ikili entropi fonksiyonunu temsil etmektedir. e < 0,11 için R_s > 0 olup pozitif güvenli anahtar üretimi mümkündür.

3.2.7.2 Pratik Saldırı Vektörleri

Teorik güvenlik kanıtlarının pratik sistemlerde geçerliliğini koruyabilmesi için çeşitli saldırı vektörlerinin sistem tasarımında dikkate alınması gerekmektedir. Tablo 3.6, bu vektörleri ve sistemin her birine karşı aldığı önlemleri özetlemektedir.

Bu karşılaştırma Tablo 3.7'de özetlenmektedir.

Tablo 3.7. Pratik QKD saldırı vektörleri ve sistemin karşı önlemleri.

Saldırı Türü	Mekanizma	Sistemin Karşı Önlemi
Intercept-Resend	Eve q_2'yi ölçüp vekil foton gönderir	QBER (3.13) ve ΔT (3.12) alarmı
Photon Number Splitting	Çok fotonlu pulslardan birini ayırma	TFK: gerçek tek foton - PNS imkânsız
Trojan Horse	Ali'ye ışık göndererek baz bilgisi okuma	Optik izolator + güç monitörü
Detector Blinding	Buse dedektörünü kör hale getirme	TCSPC foton sayım doğrulaması
Zaman Yan Kanalı	Timing yan kanalı saldırısı	ps hassasiyeti + zaman randomizasyonu

3.2.8 Matematiksel Ek: Temel İlişkiler

3.2.8.1 Bell Durumu ve Dolanıklık Ölçütü

(3.9)'da verilen $|\Phi^+\rangle$ durumunun dolanık olduğu Schmidt ayrışımıyla gösterilebilir. Bir iki-parçacık saf durum $|\psi\rangle = \Sigma_i \lambda_i |a_i\rangle|b_i\rangle$ biçiminde yazılabilir; Schmidt sayısı > 1 ise dolanıktır. $|\Phi^+\rangle$ için iki eşit Schmidt katsayısı mevcuttur ($\lambda_1 = \lambda_2 = 1/\sqrt{2}$), dolayısıyla durum kesinlikle dolanıktır. Von Neumann entropisi:

$$S(\rho_A) = -Tr(\rho_A \log_2 \rho_A) = 1 \text{ ebit} \quad \textbf{(3.16)}$$

(3.16) sonucu, foton çiftinin maksimal dolanıklık derecesinde olduğunu, yani iki foton arasındaki kuantum korelasyonunun olası en yüksek değerde bulunduğunu ifade etmektedir.

3.2.8.2 QBER Hesabı

Kuantum Bit Hata Oranı (QBER), ham anahtar aşamasında saptanan hatalı bit sayısının toplam bit sayısına oranıdır. Dinleme olmaksızın yalnızca kanal gürültüsünden kaynaklanan temel QBER, dedektör karanlık sayım oranı d, kanal iletim verimliliği η ve optik yanlış hizalanma hatası e_opt parametrelerine bağlıdır:

$$QBER_0 = (e_{opt} \cdot \eta + d) / (\eta + 2d) \quad \textbf{(3.17)}$$

Eve müdahalesi bu değere (3.13) uyarınca eklenir. f_Eve = 1 durumunda QBER_Eve = 0,25 ve toplam QBER, asimptotik güvenlik analizlerinde kullanılan yaklaşık %11 eşiğini genellikle aşmaktadır.

3.2.8.3 Zaman Damgası Hassasiyet Sınırı

T_1 zaman damgasının fiziksel hassasiyet sınırı zaman-enerji belirsizlik ilişkisinden kaynaklanır:

$$\Delta E \cdot \Delta t \geq \hbar / 2 \quad \textbf{(3.18)}$$

1550 nm telekomünikasyon fotonları için tipik koherans süresi ~1 ns düzeyindedir; bu, FPGA'nın ~10 ps hassasiyetinin çok üzerindedir. Dolayısıyla T_1 damgasının hassasiyet sınırını belirleyen (3.18) değil; TCSPC dedektörünün elektronik gürültüsü ve FPGA'nın dahili saat çözünürlüğüdür.

3.2.9 Bölüm Özeti ve Bir Sonraki Bölüme Geçiş

Bu bölümde dolanık foton çifti tabanlı bir QKD sisteminin verici taraftan alıcı tarafına uzanan tam mimarisi incelenmiştir. Öne çıkan temel bulgular şunlardır:

- SPDC kristali, (3.22) ve (3.23) enerji-momentum korunumu altında Tip-II konfigürasyonunda (3.9)'daki $|\Phi^+\rangle$ Bell durumunda dolanık q_1-q_2 çiftini üretir. Dolanıklık kristal içinde kendiliğinden oluşur (Tablo 3.3) ve herhangi bir ölçüm yapılmadığı sürece korunur.

- BB84 polarizasyon kodlama (3.24)-(3.25), HWP ve PBS üzerinden (3.8)'deki üniter operasyonlarla gerçekleştirilir. Tablo 3.4'te gösterildiği üzere bu işlem boyunca dalga fonksiyonu çökmez.

- FPGA, T_1 zaman damgasını fotonun kendisine değil foton üretim/tetik olayına atar (bkz. 4.4.3). Foton bir kuantum nesne olarak (3.18) belirsizlik ilkesine tabidir; doğrudan damgalamak mümkün değildir.

- (3.12)'deki $\Delta T > 100$ μs anomalisi ve (3.13)'teki QBER > %11 koşulu, dinleyici tespitinin iki bağımsız ölçütünü oluşturmaktadır (Tablo 3.5).

- (3.15)'teki güvenli anahtar hızı formülü, e < %11 için pozitif anahtar üretiminin mümkün olduğunu göstermektedir.

Bir sonraki bölümde QKD sisteminin ölçeklenebilirlik sorunları ve kuantum tekrarlayıcı (quantum repeater) mimarileri ele alınacaktır. Fiber tabanlı QKD'nin pratik menzil sınırı günümüzde ~100–200 km düzeyindedir; bu sınırı aşmak için dolanıklık saflaştırma (entanglement purification) ve kuantum bellek (quantum memory) bileşenleri incelenecektir.

3.3 İLETİM HATTI, ALICI TARAF VE ÖLÇÜM SÜRECİ

3.3.1 Giriş ve Motivasyon

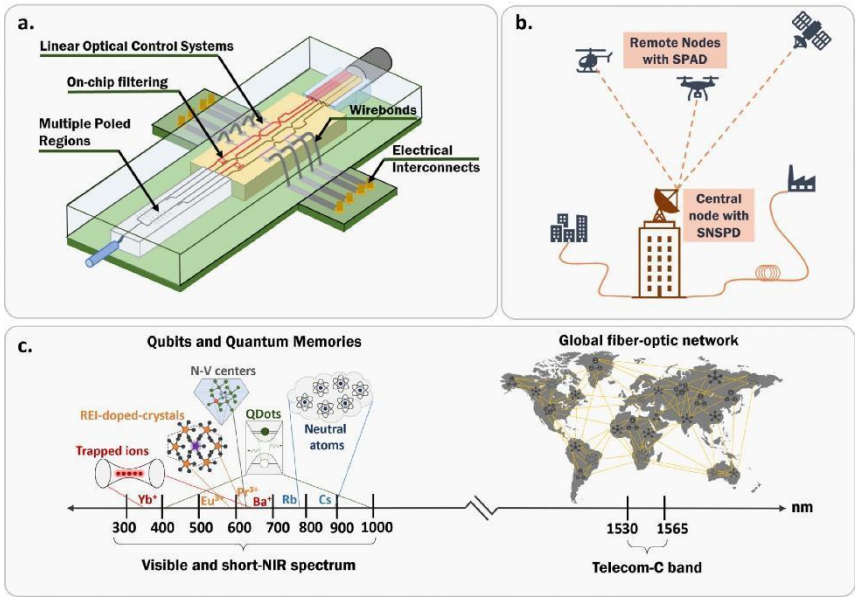
Kuantum haberleşme sistemlerinde bilgi genellikle fotonlar aracılığıyla taşınır. Gönderici tarafından hazırlanan kuantum durumları bir iletişim kanalı üzerinden alıcıya iletilir. Bu iletişim kanalı çoğunlukla optik fiber kablolar veya serbest uzay optik iletişimi şeklinde olabilir. Alıcı tarafta bulunan özel dedektörler gelen fotonları algılar ve kuantum durumunun ölçülmesini sağlar. Ölçüm işlemi gerçekleştiği anda fotonun kuantum durumu belirlenir. Bu durum kuantum mekaniğinin temel özelliklerinden biri olan ölçüm sonrası durumun belirlenmesi prensibine dayanır (Nielsen ve Chuang, 2010).

Bu süreç kuantum haberleşme ve kuantum kriptografi sistemlerinin temel çalışma prensibini oluşturur (Gisin, Ribordy, Tittel, ve Zbinden, 2002).

3.3.2 Fotonun Optik Kanal Üzerinden İletilmesi

Kuantum haberleşme sistemlerinde bilgi taşıyıcı olarak genellikle tek fotonlar kullanılır. Gönderici tarafından hazırlanan fotonlar optik bir kanal aracılığıyla alıcıya gönderilir. Bu kanal çoğunlukla fiber optik kablolardan oluşur. Fiber optik kablolar ışığın düşük kayıpla iletilmesini sağladığı için kuantum iletişim sistemlerinde yaygın olarak tercih edilir (Gisin vd., 2002). Fotonların optik iletişim kanalı üzerinden gönderici ve alıcı arasında iletilme süreci Şekil 3.1'de gösterilmektedir.

Bu yapı Şekil 3.3'te gösterilmektedir.



Şekil 3.3. Fotonların optik kanal üzerinden gönderici ve alıcı arasında iletilmesi

Fotonlar optik kanal boyunca ilerlerken ortam koşulları nedeniyle bazı kayıplar oluşabilir. Bu nedenle kuantum haberleşme sistemlerinde çok hassas algılama yöntemleri kullanılmaktadır.

3.3.3 İletim Süresi ve Beklenen Zaman Penceresi

Bir foton gönderildiğinde alıcıya ulaşması için belirli bir süre gerekir. Bu süre kullanılan iletişim kanalının uzunluğuna ve ışığın ortam içindeki yayılma hızına bağlıdır. Bu nedenle kuantum iletişim sistemleri belirli bir **zaman penceresi (time window)** kullanarak çalışır.

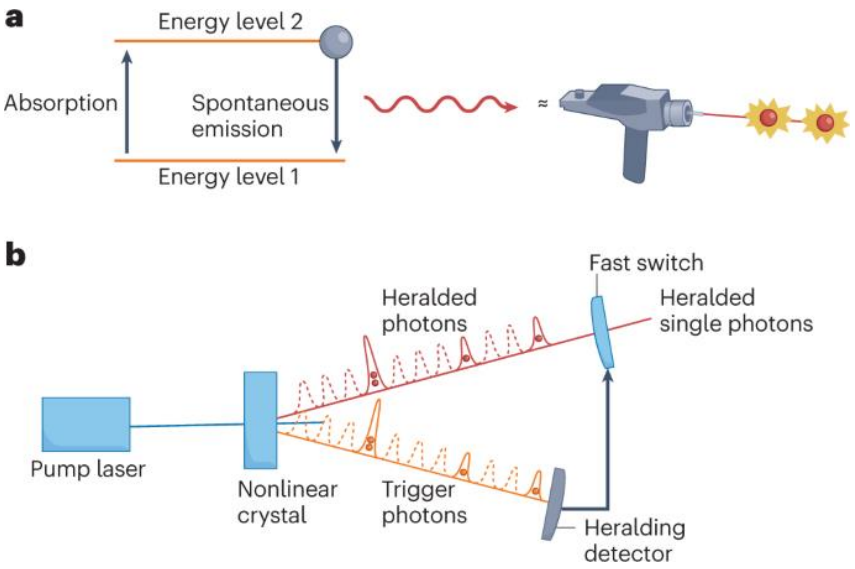
Gönderici fotonu gönderdiğinde gönderim zamanı kaydedilir. Alıcı taraf yalnızca beklenen zaman aralığında gelen sinyalleri dikkate alır. Bu yöntem sayesinde:

- yanlış sinyaller azaltılır
- ortam gürültüsü filtrelenir
- sistem güvenilirliği artırılır

Bu zaman eşleştirme yöntemi kuantum anahtar dağıtım sistemlerinde önemli bir rol oynamaktadır (Bennett ve Brassard, 1984).

3.3.4 Alıcı Tarafta Dedektörlerin Rolü

Alıcı tarafında bulunan dedektörler gelen fotonları algılar. Bu dedektörler çok düşük enerji seviyelerindeki tek bir fotonu bile algılayabilecek hassasiyete sahiptir. Kuantum iletişim sistemlerinde genellikle tek foton dedektörleri kullanılmaktadır. Tek foton dedektörünün çalışma prensibi ve algılama sistemi Şekil 3.4'te gösterilmektedir.



Şekil 3.4. Tek foton algılama sistemi

Foton dedektöre ulaştığında dedektör içinde elektriksel bir sinyal oluşur. Bu sinyal sistem tarafından kaydedilir ve analiz edilir (Hadfield, 2009).

3.3.5 Foton Algılandığında Elektriksel Sinyal Oluşması

Bir foton dedektör tarafından algılandığında elektronik devrede kısa süreli bir elektriksel darbe oluşur. Bu darbe genellikle **klik (click)** olarak adlandırılır.

Bu süreç şu şekilde gerçekleşir:

- Foton dedektöre ulaşır.
- Dedektör içinde elektriksel yük taşıyıcıları oluşur.
- Elektronik devre kısa süreli bir akım üretir.
- Sistem bu sinyali algılama olayı olarak kaydeder.

Bu olayın zamanı yüksek hassasiyetli elektronik sistemler tarafından kaydedilir. Bu zaman etiketleme yöntemi kuantum iletişim sistemlerinin senkronizasyonunda önemli bir rol oynar.

3.3.6 Ölçüm Anında Kuantum Durumunun Belirlenmesi

Kuantum sistemlerinde ölçüm işlemi gerçekleştiği anda sistemin durumu belirlenir. Ölçümden önce bir foton aynı anda birden fazla durumda bulunabilir. Ancak ölçüm yapıldığında sistem belirli bir değere çöker. Bu durum kuantum mekaniğinde dalga fonksiyonunun çökmesi olarak adlandırılır (Nielsen ve Chuang, 2010).

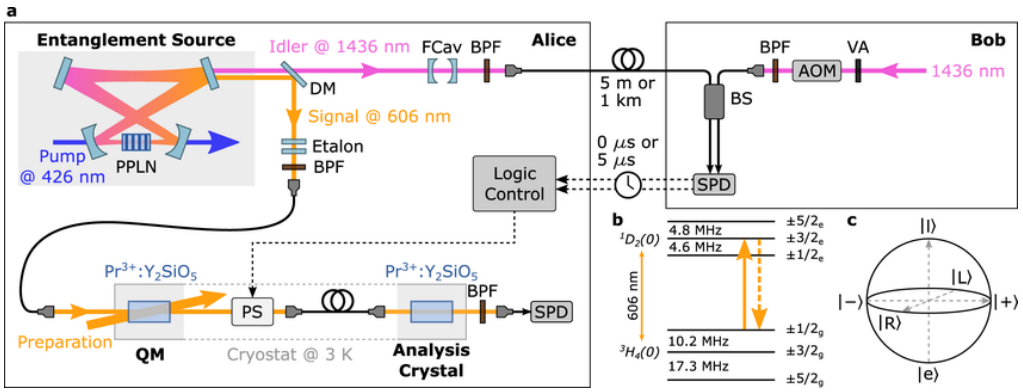
Örneğin polarizasyon tabanlı bir sistemde ölçüm sonucu şu şekilde olabilir:

Polarizasyon	Qubit
Dikey	0
Yatay	1

Bu işlem kuantum iletişim protokollerinde bilgiyi okumak için kullanılır.

3.4 Entanglement Tabanlı Sistemlerde Korelasyon

Bazı kuantum iletişim sistemlerinde dolaşık foton çiftleri kullanılır. Bu durumda iki foton birbirine kuantum seviyesinde bağlıdır. Bu fotonlar farklı konumlarda ölçülse bile sonuçları arasında güçlü bir ilişki bulunur. Dolaşık foton çiftleri kullanılarak gerçekleştirilen kuantum iletişim sistemi Şekil 3.5'te gösterilmektedir.



Şekil 3.5. Dolaşık foton çiftleri ile kuantum iletişim sistemi

Bu özellik sayesinde iki taraf arasında güvenli bilgi paylaşımı yapılabilir. Dolanıklık özelliği kuantum kriptografi ve kuantum iletişim sistemlerinin güvenlik mekanizmasının temelini oluşturur (Ekert, 1991).

3.4.1 Prepare-and-Measure Sistemleri

Kuantum iletişim sistemlerinde kullanılan bir diğer yöntem **prepare-and-measure** yaklaşımıdır. Bu yöntemde gönderici fotonun kuantum durumunu önceden hazırlar ve alıcı bu durumu ölçerek bilgiyi elde eder.

Gönderici fotonun polarizasyonunu belirler ve alıcı bu polarizasyonu ölçerek gönderilen bilgiyi belirler. Bu yaklaşım özellikle BB84 kuantum anahtar dağıtım protokolünde kullanılmaktadır (Bennett ve Brassard, 1984).

3.4.2 Gönderim Zamanı ile Algılama Zamanının Karşılaştırılması

Sistem güvenliğinin sağlanması için gönderim zamanı ile algılama zamanı karşılaştırılır. Eğer algılanan sinyal beklenen zaman aralığında gelmişse doğru sinyal olarak kabul edilir. Beklenen zaman penceresi dışında gelen sinyaller genellikle gürültü veya hatalı sinyal olarak değerlendirilir.

Bu yöntem sistem güvenilirliğini artırmak için kullanılan önemli bir tekniktir ve kuantum iletişim sistemlerinin doğru çalışmasını sağlar.

3.5 GÜVENLİK, SALDIRI TESPİTİ VE ŞEKLİN YORUMU

Kuantum anahtar dağıtımının (Quantum Key Distribution, QKD) güvenlik temeli, klasik kriptografideki hesapsal karmaşıklık varsayımlarından kökten ayrılmaktadır. Klasik şifreleme algoritmaları, RSA veya AES gibi, güvencelerini belirli matematiksel problemlerin çözümünün hesapsal açıdan güçlüğüne dayandırır. Kuantum bilgisayarların olgunlaşmasıyla bu güvence zayıflayabilir. QKD ise güvencesini **kuantum mekaniğinin temel ilkelerinden** türetir; bu ilkeler herhangi bir teknolojik ilerlemeyle aşılamaz (Gisin ve ark., 2002).

Bu bölümde, bir QKD kanalında araya giren bir saldırganın **fiziksel olarak kaçınılmaz** izler bıraktığı matematiksel ve fiziksel gerekçeleriyle gösterilmekte; sistemin bu izleri nasıl tespit ettiği ve alarm ürettiği adım adım açıklanmaktadır.

3.5.1 Araya Biri Girerse Ne Olur?

Kuantum kanalı üzerinde gerçekleştirilen gizli dinleme girişimini gerçekleştiren tarafa geleneksel kriptografi literatüründe Eve (İng. eavesdropper - gizlice dinleyen) adı verilir. Eve, Alice'in Bob'a gönderdiği kuantum bitleri (qubitleri) yakalamaya ve içeriği öğrenmeye çalışır.

Klasik bir iletişim kanalında bu mümkündür: sinyal kopyalanır, analiz edilir ve yeniden iletilir; Bob tarafında herhangi bir bozulma gözlemlenmez. Kuantum mekaniğinde ise durum köklü biçimde farklıdır.

Temel İlke: Kuantum Durumları Kopyalanamaz - Klonlama Yasak Teoremi
Klonlama Yasak Teoremi (No-Cloning Theorem)
Bilinmeyen bir kuantum durumunu $\|\psi\rangle$ değiştirmeksizin kopyalamak fiziksel olarak imkânsızdır. Wootters ve Zurek (1982) ile Dieks (1982) tarafından bağımsız olarak kanıtlanan bu teorem, kuantum mekaniğinin doğrusal (lineer) yapısının bir sonucudur.
Biçimsel ifade: Hiçbir üniter operatör U, $\|\psi\rangle\|0\rangle \rightarrow \|\psi\rangle\|\psi\rangle$ dönüşümünü her $\|\psi\rangle$ için gerçekleştiremez.

Bu teoremin pratik sonucu şudur: Eve, qubiti ölçmeksizin kopyalayamaz. Ölçüm yapması ise qubiti çöktürür (wavefunction collapse) ve kuantum durumu geri döndürülemez biçimde değişir. Sonrasında Eve, değiştirilmiş bu qubiti Bob'a iletmek zorunda kalır. Bu noktada iki senaryo mümkündür:

- Eve doğru tabanı seçerse: qubiti ölçer, doğru değeri öğrenir, aynı durumu yeniden hazırlayarak Bob'a iletir. Bu durumda Bob'un ölçümünde hata oluşmaz ve Eve bu spesifik bit için tespiti atlatır.
- Eve yanlış tabanı seçerse: ölçüm qubiti bozar, yeniden hazırlanan qubit Alice'in gönderdiğinden farklıdır ve Bob %50 olasılıkla hatalı sonuç alır. Bu hata, sistemin QBER analizinde ortaya çıkar.

BB84 protokolünde rastgele taban seçimi yapıldığından (iki olası taban: {+, ×}), Eve'in doğru tabanı seçme olasılığı yalnızca 1/2'dir. Dolayısıyla her qubit için Eve'in sisteme hata ekleme olasılığı:

$$P(\text{hata} \mid \text{Eve ölçtü}) = P(\text{yanlış taban}) \times P(\text{hata} \mid \text{yanlış taban}) = 1/2 \times 1/2 = 1/4 \quad (3.19)$$

Bu, tüm qubitler üzerinde Eve tam kapsamlı bir intercept-resend saldırısı uyguladığında beklenen kuantum bit hata oranının (QBER) yaklaşık %25 olacağı anlamına gelir.

3.5.2 Ölçüm Neden Sistemi Bozar?

Kuantum mekaniğinin merkezinde yer alan ölçüm sorunu (measurement problem), klasik mantıkla çelişen bir olgu sunar: bir sistemi ölçmek, onu kaçınılmaz biçimde etkiler. Bu etki, ölçüm aletinin hassasiyetiyle değil, **kuantum mekaniğinin matematiksel yapısıyla** belirlenir.

Bir qubit, ölçülmeden önce genel olarak süperpozisyon halindedir:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,\ |\alpha|^2 + |\beta|^2 = 1 \quad (3.20)$$

Burada α ve β karmaşık genlik katsayılarıdır. Ölçüm yapıldığında dalga fonksiyonu çöker (Copenhagen yorumuna göre):

$$|\psi\rangle \longrightarrow |0\rangle \text{ ile olasılık } |\alpha|^2, \text{ ya da } |1\rangle \text{ ile olasılık } |\beta|^2 \quad (3.21)$$

Ölçüm sonrası süperpozisyon bilgisi tamamen yok olur. Sistemin ölçümden önceki durumu yeniden oluşturulamaz. Bu geri döndürülemezlik (irreversibility), Eve'in izini kapatmasını olanaksız kılar (Nielsen ve Chuang, 2010).

Heisenberg Belirsizlik İlkesi ve Konjuge Tabanlar
BB84 protokolünde kullanılan iki polarizasyon tabanı ({0°, 90°} ve {45°, 135°}) birbirine göre konjuge (tamamlayıcı) tabanlardır. Bir qubiti konjuge tabanda ölçmek, özgün taban bilgisini tamamen rastgeleleştirir - bu, Heisenberg belirsizlik ilkesinin doğrudan bir sonucudur:
$\Delta J_x \cdot \Delta J_z \geq \hbar/2$
Bu özellik, Eve'in her iki taban kanalını eş zamanlı ve hatasız ölçmesini doğası gereği imkânsız kılar (Bennett ve Brassard, 1984).

Fiziğin bu kısıtları, güvenliği matematiksel karmaşıklık varsayımı yerine **doğa yasası** üzerine oturtur. Bu ayrım, QKD'yi teorik olarak **koşulsuz güvenli (information-theoretically secure)** kılar; yani sınırsız hesaplama gücüne sahip bir saldırgan bile kanalı gizlice dinleyemez (Lo ve ark., 2014).

3.5.3 Erken Çökme, Bozulma ve Hata Oranı Artışı

Kuantum iletişim sistemleri gerçek dünya koşullarında çalışırken kanal gürültüsü, fiber optik kayıp, foton soğurulması ve termal etkilere maruz kalır. Bu nedenle sıfır hata oranı hiçbir zaman beklenmez; sistem **beklenen (arkaplan) hata oranına** sahip bir temel çizgide çalışır.

Saldırı tespiti, bu temel çizginin **istatistiksel olarak anlamlı biçimde aşılıp aşılmadığının** sürekli izlenmesine dayanır.

Kuantum Bit Hata Oranı (QBER) Tanımı:

$$QBER = N_{hatalı} / N_{toplam} \quad (3.22)$$

Burada Nhatalı, yanlış ölçülen qubit sayısını; Ntoplam, simetrik taban seçimi yapılan ve karşılaştırmaya dahil edilen qubit sayısını gösterir.

Hata oranı kaynaklarına göre ayrımı şu şekilde yapılabilir:

Bu karşılaştırma Tablo 3.8'de özetlenmektedir.

Tablo 3.8. QBER değerlerine göre hata kaynağı sınıflandırması

Hata Kaynağı	Beklenen QBER Aralığı	Olası Açıklama
Kanal gürültüsü	< %2–3	**Normal - fiber kalitesi veya optik hizalama sorunu**
Dedektör karanlık sayımı	< %1–2	**Normal - arka plan foton gürültüsü**
Kısmi Eve müdahalesi	%3–11	**UYARI - istatistiksel anomali, araştır**
Tam intercept-resend	~%25	**ALARM - yüksek güven ile aktif saldırı**
Photon number splitting (PNS)	Düşük ama zamanlama anomalisi	**ALARM - gelişmiş saldırı, zamanlama analizi gerekli**

"Erken çökme" ifadesi, istatistiksel yeterli örnek büyüklüğüne ulaşılmadan hata oranının güven aralığının üst sınırını aşmasını tanımlar. Bu durum, kanalda anlık yüksek yoğunluklu bir girişimin varlığını gösterebilir ve daha uzun örnekleme süreleri beklenmeksizin derhal incelenmelidir.

3.5.4 Zaman Damgaları Neden Önemlidir?

QKD sistemlerinde zaman damgası (timestamp), her fotonun ya da foton grubunun belirli bir donanım saatine (genellikle GPS-disiplinli ya da atom saatine senkronize) bağlı kesin gönderim ve alım zamanlarının kaydedilmesidir. Bu kayıtlar yalnızca senkronizasyon amacıyla değil; **istatistiksel saldırı imzalarının belirlenmesi** için de kritik öneme sahiptir.

Alice ve Bob arasındaki fiziksel mesafe ve kanal özellikleri bilindiğinden, iki nokta arasındaki foton geçiş süresi (iletim gecikmesi) deterministik olarak tahmin edilebilir:

$$\Delta t_{beklenen} = d / v_{grup} \quad (3.23)$$

Burada d fiber uzunluğunu, v_{grup} ise fotonun fiber içindeki grup hızını gösterir (tipik olarak $c/n \approx 2\times10^8$ m/s, $n \approx 1.5$ fiber kırılma indisi). Alice ve Bob, bu beklenen gecikme penceresinin dışına çıkan gönderim-alım çiftlerini anormal olarak işaretler.

Zaman damgalarının tespit ettiği saldırı imzaları:

- Klasik intercept-resend: Eve qubiti ölçer ve yeniden hazırlar. Yeniden hazırlama süresi (typik olarak nanosaniye mertebesinde) beklenen iletim süresine ek gecikme ekler; $\Delta t > \Delta t_{beklenen}$ anomalisi oluşur.
- Photon Number Splitting (PNS) saldırısı: Eve zayıf koherent foton demetlerinden fazladan fotonu saklar, ileride analiz etmek üzere gönderimi geciktirir. Anlık gecikme profili değişir.
- Trojan-horse saldırısı: Eve, Alice'in cihazına ışık gönderir ve yansımaları inceler. Bu girişim, çift yönlü zamanlama profilinde ve foton sayım istatistiklerinde anormallik olarak gözüklür.
- Toplu gecikme (delay-line) saldırısı: Eve, fotonları geciktirip saklarken kopyasını incelemeye çalışır. Akumulatif zaman sapması istatistiksel olarak birikir ve tespit edilir.

3.5.5 Beklenen Zaman Penceresi Dışına Çıkma Ne Gösterir?

Alice ve Bob, kuantum kanalını sürekli kalibrasyon ölçümleriyle karakterize eder. Bu süreç sonunda her iletim için bir **kabul penceresi (acceptance window)** tanımlanır. Bu pencere, beklenen ortalama gecikme ($\mu_{\Delta t}$) ve bu gecikmedeki standart sapma ($\sigma_{\Delta t}$) cinsinden ifade edilir:

$$[\mu_{\Delta t} - k \cdot \sigma_{\Delta t}, \mu_{\Delta t} + k \cdot \sigma_{\Delta t}] \text{ (k: eşik katsayısı, tipik k = 3) (3.24)}$$

k = 3 seçildiğinde normal dağılıma göre pencere dışına çıkma olasılığı yaklaşık %0.27'dir (3σ kuralı). Bu pragmatik bir seçimdir; k büyütülürse yanlış alarm oranı düşer ama gerçek saldırıyı gözden kaçırma riski artar (kaçırganlık - missed detection oranı).

Pencere dışına çıkmanın olası yorumları:

- Tek foton - tesadüfi: Kanal gürültüsü veya dedektör jitter'ı nedeniyle tekil bir olay pencere dışına çıkabilir. Birkaç ardışık normal ölçüm sonrasında bu olay geçici anomali olarak sınıflandırılır.
- Belirli bir zaman bloğunda kümeli sapmalar: Birden fazla fotonun ardışık biçimde pencere dışına çıkması, sistematik bir müdahaleye işaret eder; bu durum alarm eşiğini tetikler.
- Asimetrik sapma (hep geç gelen): Fotonların sistematik olarak beklenen pencereden geç gelmesi, gecikme ekleyen bir araya girmeye (delay injection) işaret eder.

3.5.6 Hangi Durumda Alarm Verilir?

QKD sisteminin güvenlik katmanı, iki bağımsız metriği sürekli izler: **QBER** (hata oranı) ve **zamanlama anomali skoru**. Bu iki metrik, birbirini doğrulayan çift kanallı bir tespit mekanizması oluşturur.

Bu karşılaştırma Tablo 3.9'da özetlenmektedir.

Tablo 3.9. Çift metrikli alarm karar matrisi

Durum	QBER	Zamanlama Anomalisi	Sistem Kararı
Normal işleyiş	< %3	Yok	**Normal - anahtar dağıtımına DEVAM**
Kanal bozulması	%3–7	Kısmen var	**UYARI - insan denetimi, hat kalitesini kontrol et**
Kısmi Eve müdahalesi	%7–15	Var (asimetrik)	**UYARI - gizlilik yükseltme protokolü başlat**
Tam intercept-resend	> %15	Var (gecikmeli)	**ALARM - oturumu KES, yeni kanal kur**
PNS / gelişmiş saldırı	Düşük–orta	Belirgin gecikme	**ALARM - bant genişliğini kısıt, protokol yenile**
Dedektör kör etme (blinding)	Düşük	Anormal sayım oranı	**ALARM - donanım güvenlik denetimi başlat (Lydersen ve ark., 2010)**

Alarm kararı, yalnızca anlık ölçüme değil, belirli bir blok boyutu (Nblok qubit) üzerinden hesaplanan istatistiklere dayanır. Tipik uygulamalarda Nblok = 10^3, 10^4 mertebesinde seçilir; bu, hem istatistiksel güvenilirlik hem de gerçek zamanlı tepki hızı arasındaki dengeyi sağlar.

3.5.7 Eşik Değeri Mantığı

Eşik değerinin (threshold) belirlenmesi, iki hata türü arasındaki mühendislik dengesidir:

- **Yanlış alarm (False Positive - Tip I Hata):** Gerçekte saldırı olmadığı halde sistemin alarm vermesi. Bu durum, gereksiz oturum kesintilerine ve anahtar üretim verimliliğinin düşmesine yol açar.
- **Gözden kaçırma (False Negative - Tip II Hata):** Gerçekte saldırı olduğu halde sistemin alarm üretmemesi. Bu, güvenlik ihlalinin fark edilmeden sürmesi anlamına gelir; çok daha kritik bir başarısızlıktır.

Neyman-Pearson çerçevesinde bu denge, **sabit yanlış alarm oranı (CFAR - Constant False Alarm Rate)** altında tespit gücünün (power) maksimize edilmesiyle yönetilir. QKD sistemlerinde QBER eşiği için tipik seçim:

$$Q_{eşik} = Q_{temel} + z_{1-\alpha} \cdot \sqrt{(Q_{temel}(1-Q_{temel})/N_{blok})} \quad (3.25)$$

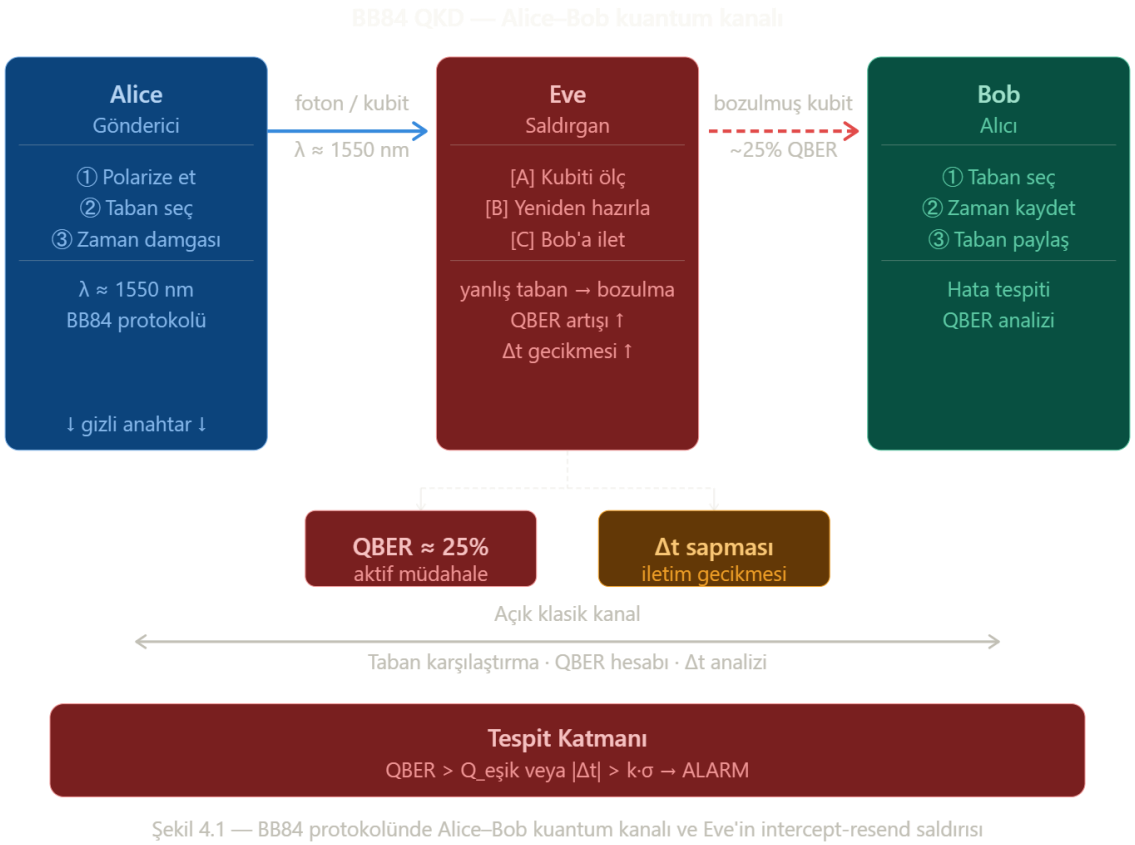
Burada Q_{temel} kalibrasyon aşamasında ölçülen arkaplan hata oranı, $z_{1-\alpha}$ ise z-puanı ($\alpha = 0.001$ için $z \approx 3.09$), N_{blok} ise blok büyüklüğüdür. Bu formül, istatistiksel olarak yetersiz veriyle (küçük N) aşırı duyarlılığı ve büyük N ile geç tepkiyi dengeler (Scarani ve ark., 2009).

Gizlilik Yükseltme (Privacy Amplification) ile Eşiğin İlişkisi
Gizlilik yükseltme (Shor ve Preskill, 2000), Eve'in edinmiş olabileceği bilginin üst sınırı bilinemeden ham anahtar üzerinden güvenli bir alt anahtar türetme yöntemidir. QBER eşiği, bu yöntemin ne zaman devreye gireceğini belirler:
QBER < Qeşik → Gizlilik yükseltme yeterli, anahtar dağıtımına devam.
QBER ≥ Qeşik → Eve'in bilgi edinimi telafi edilemez - oturum güvensiz, yeni kanal gerekli.

3.5.8 Alice–Bob Hattının ve Saldırı Tespiti Yaklaşımının Şekil Üzerinde Açıklanması

Aşağıdaki şema, BB84 tabanlı bir QKD sisteminin üst düzey mimari görünümünü ve Eve'in araya girme senaryosundaki veri akışını özetlemektedir.

Bu yapı Şekil 3.6'da gösterilmektedir.



Şekil 3.6. BB84 protokolünde Alice–Bob kuantum kanalı ve Eve'in intercept-resend saldırısının sistem üzerindeki etkileri

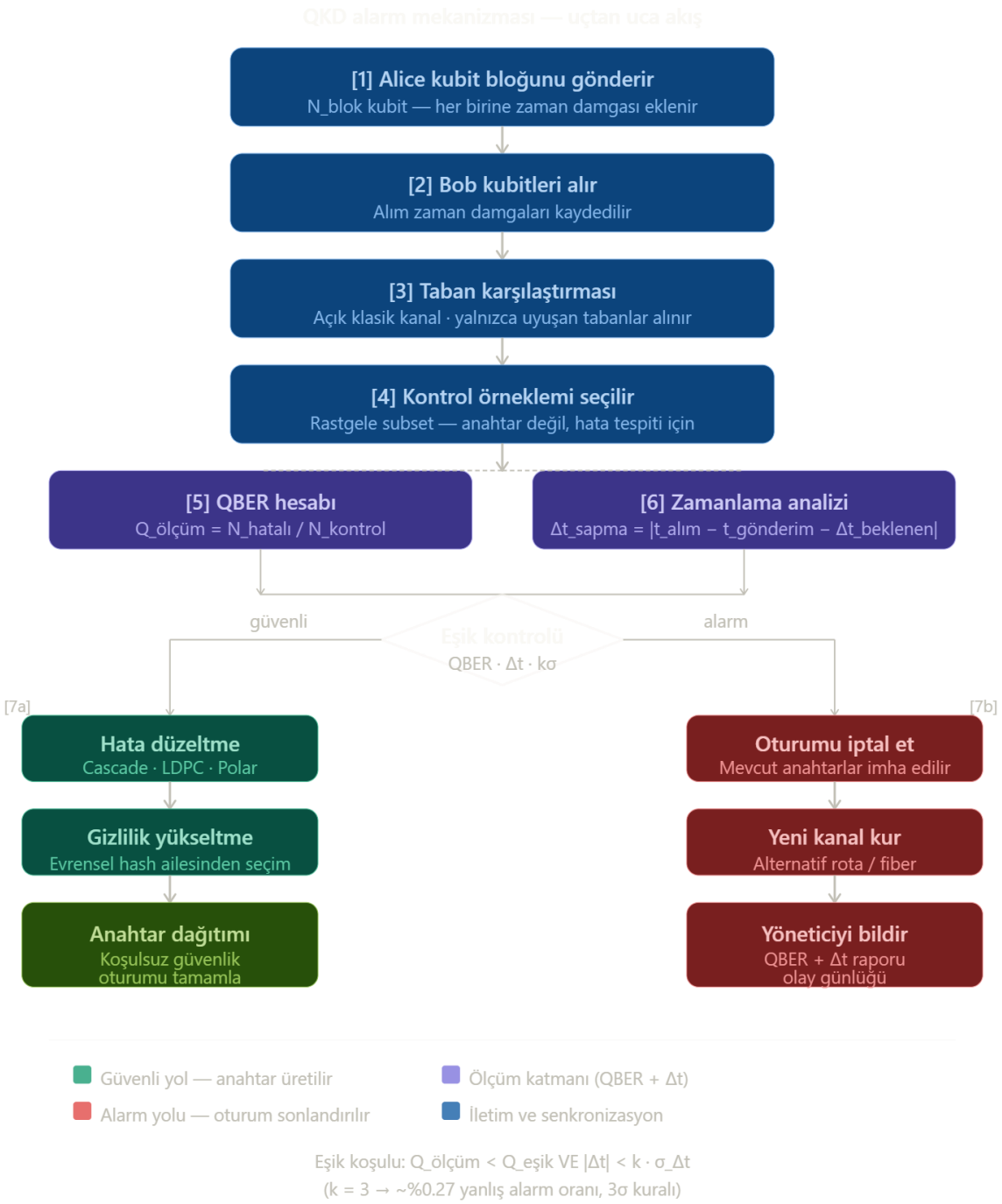
Şekildeki her bileşenin işlevi:

- Alice (Gönderen): Rastgele taban seçerek qubitleri polarize eder ve her qubite hassas bir donanım zaman damgası ekler. Gönderilen ham bit dizisi gizlidir.

- Kuantum Kanal (fiber optik / serbest uzay): Qubitleri taşır; Eve dahil herhangi bir fiziksel girişime açık. Kanal, klasik kriptografik güvence sağlamaz; güvenlik fizik yasalarından gelir.
- Eve (Opsiyonel - Saldırgan): Qubiti yakalar (A), kendi seçtiği tabanda ölçer (B), ardından ölçüm sonucuna uygun yeni bir qubit hazırlayıp Bob'a iletir (C). Yanlış taban seçimi → QBER artışı. Yeniden hazırlama gecikmesi → Δt anomalisi.
- Bob (Alıcı): Qubiti kendi rastgele seçtiği tabanda ölçer ve zaman damgasını kaydeder. Alice ile bu ölçüm zamanını ve taban seçimini açık klasik kanal üzerinden paylaşır.
- Klasik Kanal (Açık): Taban karşılaştırması, hata oranı hesabı ve zaman damgası analizi için kullanılır. Bu kanal kimlik doğrulamalı olmalıdır (tipik olarak hash tabanlı MAC ile); aksi takdirde man-in-the-middle saldırısına açık kalır.
- Tespit Katmanı: Alice ve Bob'un istatistiksel analiz birimi. QBER ve zamanlama metriklerini birlikte değerlendirerek karar üretir.

3.5.9 Sistem Nasıl Uyarı Üretir? - Uçtan Uca Akış

QKD sisteminin alarm mekanizması, aşağıdaki ardışık adımlarla çalışır. Bu akış, hem teorik güvenlik kanıtlarının hem de fiziksel kanal ölçümlerinin birleşimi olan **çok katmanlı bir savunma mimarisini** oluşturur:



Adım 7a'daki güvenli yolda devreye giren **hata düzeltme (error correction)** - tipik olarak Cascade, LDPC veya Polar kodlar - ve ardından uygulanan **gizlilik yükseltme (privacy amplification)** - evrensel hash fonksiyonları ailesinden rastgele seçim - birlikte, Eve'in sahip olabileceği sınırlı bilgiyi kriptografik olarak sıfıra indirgeyerek nihai anahtarın koşulsuz güvenliğini sağlar.

3.6 Sonuç: Bu Yapı Neden Güvenlidir ve Saldırıyı Nasıl Fark Eder?

QKD'nin güvenliği, doğası gereği birbirini destekleyen **üç katmandan** oluşur:

Katman 1 - Fizik Güvencesi (Kanıtlanamaz Sızma Teoremi)
Klonlama yasağı ve Heisenberg belirsizliği, Eve'in qubiti ölçmeksizin kopyalamasını fiziksel olarak olanaksız kılar. Ölçüm yapması ise sistemde kaçınılmaz iz bırakır. Bu, herhangi bir teknolojik ilerlemeyle aşılamaz; matematiksel kanıtı kuantum mekaniğinin aksiyomlarından doğrudan türeyen bir güvencedir.

Katman 2 - İstatistiksel Tespit (QBER + Zamanlama)
Eve'in bıraktığı iz iki bağımsız kanal üzerinden ölçülür: hata oranı artışı (QBER) ve iletim zamanlama anomalileri. İki metriğin eş zamanlı analizine dayalı karar mekanizması, hem tespit gücünü artırır hem de yanlış alarm oranını kontrollü tutar.
Önemli not: Tek bir metrik tek başına yeterli değildir. Gelişmiş saldırılar (PNS, dedektör kör etme) QBER'i düşük tutarak zamanlama anomalisi yaratabilir ya da tersini yapabilir. Çift kanallı analiz bu boşluğu kapatır.

Katman 3 - Bilgi Teorik Düzeltme (Gizlilik Yükseltme)
Sistem, Eve'in ne kadar bilgi edinmiş olabileceğini tam olarak bilemez; ancak QBER üst sınırından bu miktarın üst sınırını hesaplar. Gizlilik yükseltme aşaması, Eve'in maksimum edinebileceği bilgi miktarına karşı güvenli bir anahtar uzunluğu türeterek çıkış anahtarını koşulsuz güvenli kılar. Bu güvence, Shor ve Preskill (2000) kanıtıyla formel olarak gösterilmiştir.

Bu üç katmanın birleşimi, QKD'ye **koşulsuz (information-theoretic) güvenlik** sağlar; yani güvenlik, Eve'in hesaplama kaynaklarından bağımsız ve kuantum mekaniğinin geçerliliği süresince matematiksel olarak garanti altındadır. Klasik şifrelemenin sunduğu hesapsal güvenlikten farklı olarak, kuantum hesaplama çağında dahi bu güvence çökmez.

✓ Sistem başarıyla tespit ve yanıt verir çünkü:
Eve fizik yasaları gereği iz bırakmak zorundadır,
Bu iz iki bağımsız metrikle eş zamanlı ölçülür,
İstatistiksel karar mekanizması, eşiği aşan her olayda alarm üretir,
Alarm öncesinde edinilmiş bilgi, gizlilik yükseltme ile kriptografik olarak imha edilir.

BÖLÜM 4

Kuantum Haberleşmede Güvenlik Sınırları ve Kuantum Anahtar Dağıtım Protokolleri

4.1 Klasik İletişim Altyapısının Güvenlik Sınırları ve Kuantum Haberleşmeye Geçiş Motivasyonu

4.1.1 Fiber Optik Altyapısı: Çalışma İlkeleri ve Donanım

Günümüz telekomünikasyon ağlarının omurgasını oluşturan fiber optik kablolar, ışığın cam ya da plastik çekirdek içinde toplam iç yansıma ilkesiyle iletildiği yüksek kapasiteli iletim ortamlarıdır. Bakır altyapının aksine, elektromanyetik parazite karşı bağışıklıkları ve düşük zayıflama katsayıları bu kabloları uzun mesafeli yüksek bant genişliği uygulamaları için vazgeçilmez kılmaktadır (Agrawal, 2019). Bir ülkenin büyük şehirlerini birbirine bağlayan omurga hatlarında saniyede 10 ila 100 gigabit arasında değişen hızlar artık standart kabul görmektedir.

4.1.1.1 SFP Modülleri: Altyapının Kritik Bileşeni

Telekom santrallerinde fiber optik hattı ağ ekipmanına bağlayan SFP (Small Form-factor Pluggable) modülleri, modern iletişim altyapısının en kritik donanım bileşenlerinden birini oluşturur. Her SFP modülü bir lazer verici alt sistemi (TOSA (Transmitter Optical Sub-Assembly)) ile bir fotodetektör alıcı biriminden (ROSA (Receiver Optical Sub-Assembly)) oluşur; bu ikili yapı elektriksel sinyallerin optik sinyallere ve geri dönüştürülmesi işlemini gerçekleştirir (FS.com, 2023). SFP modülleri 850 nm, 1310 nm, 1490 nm ve 1550 nm gibi farklı çalışma dalga boylarında; 550 metre ile 160 kilometre arasında değişen mesafe aralıklarında ve 1 Gbps'den 100 Gbps'e uzanan hız kademelerinde üretilmektedir.

Bu modüllerin sıcak takılabilir (hot-swappable) tasarımı, ağ kesintisi yaratmadan değiştirilmelerini sağlar; ancak beraberinde önemli bir lojistik sorunu da getirir: kullanım ömrünün sona erdiği modüllerin yerinde yenileri bulunmazsa, o santranın bağlı olduğu tüm il veya bölgeyle iletişim kopabilir. Kritik altyapıda yedek modül envanteri bulundurmak, dolayısıyla salt teknik bir gereklilik değil stratejik bir güvenlik önlemidir. Tablo 4.1, başlıca SFP ailesi üyelerini ve tipik kullanım alanlarını özetlemektedir.

Tablo 4.1. SFP ailesi: sınıflandırma, teknik özellikler ve kullanım alanları

Modül / Hız	Dalga Boyu	Maks. Mesafe	Ortam	Tipik Kullanım
SFP - 1 Gbps	850 / 1310 / 1550 nm	≤ 160 km	MM + SM	Metro ağ, telekom santrali omurgası
SFP+ - 10 Gbps	850 / 1310 nm	≤10 km (LR) / 80 km (ZR)	MM + SM	Veri merkezi, il santrali bağlantısı
SFP28 - 25 Gbps	850 / 1310 nm	≤ 10 km	MM + SM	5G fronthaul, yüksek yoğunluklu DC
QSFP28 - 100 Gbps	850 / 1310 nm	≤10 km (LR4) / 40 km (ER4)	SM	Ulusal omurga, uluslararası hat
BiDi SFP - 1 Gbps	1310 / 1490 nm	≤ 60 km	SM (tek)	Fiber tasarruflu FTTH ve PON

Modül / Hız	Dalga Boyu	Maks. Mesafe	Ortam	Tipik Kullanım
SFP-Cu - 1 Gbps	Elektriksel (RJ-45)	≤ 100 m	Cat5e/6	Kısa mesafe erişim katmanı, konfigürasyon

Kaynak: Wolontek (2025); L-P Resources (2026); FS.com (2023) verilerinden sentezlenmiştir.

4.1.1.2 Ağ Mimarisi: Erişimden Omurgaya

Modern ulusal bir fiber ağı, üç hiyerarşik katmandan oluşur. Erişim katmanı, son kullanıcıyı veya kurumsal ağı mahalle dağıtım noktalarına taşır ve genellikle 1 Gbps kapasiteli bağlantılar sunar. Toplamlama katmanı bu dağıtım noktalarını il santrallerine bağlar; omurga katmanı ise büyük şehirler ile uluslararası bağlantı noktaları arasındaki yüksek kapasiteli ana hatları yönetir. Her katmanda farklı SFP modül tipleri kullanılmakta; bu da ağı modüler ve ölçeklenebilir kılmaktadır (L-P Resources, 2026).

Omurga düğümleri konumundaki büyük santral cihazları yalnızca pasif bir fiber bağlantı noktası değildir: içlerinde işlemciler, RAM modülleri ve bellek kartları barındıran, program çalıştırabilen ve ağ yönetimi gerçekleştirebilen entegre sistemlerdir. Bu donanımların yönetim arayüzlerine erişim, örneğin 10BASE-T gibi düşük hızlı bir SFP modülüyle konfigürasyon bağlantısı kurulması, saha mühendisleri için rutin bir işlem olmakla birlikte, bu erişim kanallarının güvensiz bırakılması önemli bir saldırı yüzeyi oluşturur.

4.1.2 Fiziksel Katmanda Dinleme Zafiyeti

4.1.2.1 Yaygın Bir Yanılgı

Fiber optik ağların doğası gereği güvenli olduğu inancı, telekomünikasyon sektöründe köklü biçimde yerleşmiş bir yanılgıdır. Bu kanı kısmen haklıdır: fiber, bakır kabloya kıyasla elektromanyetik dinlemeye karşı çok daha dirençlidir. Ne var ki 'fiber kırılamaz' söylemi, fiziksel katmandaki gerçek zafiyetleri örtbas etmekte ve sistem yöneticilerini yanlış bir güven algısına sürüklemektedir.

Spurny ve ark. (2022), fiziksel katman bileşenlerinin güvenlik risklerini deneysel olarak ölçen çalışmalarında bu gerçeği kapsamlı biçimde belgelemektedir: hem tek modlu hem çok modlu fiberlerde gizli dinleme vakalarına somut kanıtlar mevcuttur. Kritik bulgularından biri, optik dağıtım ağına bölücü eklenmesinin tüm WDM kanallarının, yani tüm spektrumun, kopyalanmasına olanak tanıdığıdır. Öte yandan bu müdahale, rutin ağ izleme sistemleri tarafından fark edilmeyebilmektedir; sinyalin yalnızca küçük bir fraksiyonunu yakalamak, aktif hattı kesintiye uğratmaksızın tam veri erişimi sağlamaya yetmektedir. Bu bulgular, 'fiber ağlar güvenlidir' kabulünü temelden sarsmaktadır.

4.1.2.2 Başlıca Fiziksel Dinleme Yöntemleri

Makro bükme yöntemi: Fiber kablo, ışığın çekirdek-kaplama sınırını aşarak dışarı sızacağı kritik açıya getirilir. Sızdıran ışık, kablonun yanına yerleştirilen bir fotodetektörle yakalanır. İşlem saniyeler içinde tamamlanır, ağ trafiğinde herhangi bir kesinti yaratmaz ve tipik olarak 0,5 ila 3 dB arasında bir kayba yol açar.

Splitter (bölücü) ekleme yöntemi: Kablo yaklaşık 30 saniye gibi kısa bir süre için kesilerek araya 1:2 ya da 1:N optik bölücü eklenir. Sinyalin bir kolu meşru alıcıya, öbürü dinleme istasyonuna yönlendirilir. Oluşan kayıp 3–4 dB'dir; bu değer kablo eskimesi ya da konektör kirliliğiyle açıklanabilir ve yöneticilerin eşik değerlerinin altında kalabilir (Spurny ve ark., 2022).

Konik daraltma (taper) yöntemi: Fiber çapı kimyasal aşındırma ya da mekanik işlemle 25 μm'ye kadar daraltılır. Bu işlem mod alanını genişleterek ışığın fiberden kaçmasına yol açar. Bradley ve ark. (2024), standart tek modlu fiberde bu yöntemle ≤1 dB kayıpla ≥−20 dB bilgi ekstraksiyon verimliliği elde edildiğini deneysel olarak kanıtlamıştır; yani meşru hat neredeyse hiç zarar görmezken saldırgan tam veri akışına erişir. Önemli bir pratik sınırlama olarak belirtmek gerekir: bu yöntem, UV lazer ve kontrollü laboratuvar koşulları gerektirdiğinden sahada anlık uygulanması güçtür; daha çok altyapıya uzun vadeli erişimi olan aktörler için geçerlidir.

Bragg ızgarası (FBG) yöntemi: Ultraviole lazerle fiber çekirdeğinin kırma indisi periyodik biçimde değiştirilir ve belirli bir dalga boyunu seçici olarak yansıtan bir ızgara oluşturulur. Yansıyan sinyal ikinci bir fiberle toplanır. Bu yöntem standart OTDR test ekipmanlarıyla neredeyse tespit edilemez ve en sofistike saldırı türü olarak kabul edilir (Si ve ark., 2018).

Bu saldırı vektörlerinin başlıca özellikleri Tablo 4.2'de özetlenmiştir.

Tablo 4.2. Fiber optik dinleme yöntemleri: teknik özellikler ve risk analizi

Dinleme Yöntemi	***Tipik Kayıp***	***Tespit Güçlüğü (0-10)***	***Tespit Riski***	***Veri Erişimi***	***Teknik Seviye***
Makro Bükme	5.0.5 –3 dB	*6/10*	*Orta*	*Orta*	*Düşük*
Splitter Ekleme	*3–4 dB*	*7/10*	*Çok Zor*	*Tam*	*Orta*
Konik Daraltma	*≤1 dB*	*9/10*	*Neredeyse Yok*	*Tam*	*Yüksek*
Bragg Izgarası (FBG)	*≤0.5 dB*	*10/10*	*Yok*	*Kısmi/Tam**	*Yüksek*
WDM Çapraz Kanal	*Değişken dB*	*3/10*	*Orta*	*Kısmi*	*Orta*

*Kaynak: Spurny ve ark. (2022); Bradley ve ark. (2024); Si ve ark. (2018) verilerinden sentezlenmiştir. Tespit güçlüğü indeksi (0–10): Spurny ve ark. (2022) ölçüm verileri, Bradley ve ark. (2024) OTDR sonuçları ve Si ve ark. (2018) nitel değerlendirmeleri temel alınarak yazarlar tarafından birleştirilmiştir; yüksek değer tespit güçlüğünün arttığını gösterir. * FBG (Bragg Izgarası): WDM sistemlerinde yalnızca hedef dalga boyu yakalanır; tek kanallı sistemlerde erişim tamdır.*

Tablo 4.2'deki veriler, saldırı yöntemleri arasındaki kritik ilişkiyi açıkça ortaya koymaktadır: en düşük sinyal kaybına, dolayısıyla en düşük tespit riskine, yol açan yöntemler, aynı zamanda en yüksek veri erişim oranını sunmaktadır. Bu ters orantı, klasik fiber altyapısının güvenliği değil işlevselliği esas alarak tasarlandığının en somut göstergesidir.

4.1.2.3 Dinleme Şemasının Görsel Analizi



Şekil 4.1. Fiber optik hatta splitter ile gizli dinleme mekanizması

Not: Şekil, 1:2 optik bölücü ekleme senaryosunu şematik olarak göstermektedir. Meşru hat kesintisiz çalışmaya devam ederken, saldırgan tam veri akışına erişir; gözlemlenen kayıp yalnızca 3–4 dB'dir.

Şekil 4.1'de görselleştirilen saldırı senaryosu teknik olarak son derece basittir: deneyimli bir teknisyen bu müdahaleyi 30 dakika ile 1 saat arasında gerçekleştirebilmekte, ağ operatörleri ise meşru hatta herhangi bir kesinti gözlemlemediğinden şüphe duymamaktadır (Si ve ark., 2018). Asıl tehlike burada yatmaktadır: klasik fiber altyapı, kendisini gözetleyen bir gözü tespit etme mekanizmasından yoksundur.

4.1.2.4 Tespit Yöntemleri ve Sınırlılıkları

Fiber optik altyapıda fiziksel dinlemeye karşı geliştirilen başlıca tespit aracı OTDR'dir (Optical Time-Domain Reflectometry; Optik Zaman-Alan Yansıma Ölçümü). Fiber boyunca kısa ışık darbeleri göndererek geri saçılan sinyali analiz eden OTDR, kırılmalar, ek noktaları veya makro bükme gibi anomalileri milimetre hassasiyetiyle belirleyebilir. Bradley ve ark. (2024), konik daraltma uygulanmış fiberlerde OTDR izlerinin yalnızca ≤0.5 dB değişim gösterdiğini saptamıştır; bu değer, rutin muayene eşiklerinin altında kalabilmektedir.

Optik güç izleme, polarizasyon analizi ve sürekli sinyal gözlemi diğer tespit yaklaşımlarını oluşturur. Spurny ve ark. (2022), optomekânik anahtarların yalıtım kaybının 1 dB'nin altında, çapraz konuşma (crosstalk) değerinin ise 70 dB'nin üzerinde olduğunu doğrulayarak bu bileşenlere yönelik saldırıların ağırlıklı olarak hizmet kesintisi değil tespit edilemezlik üzerine kurulu olduğunu ortaya koymuştur. Sonuç olarak, klasik fiber altyapısında dinlemenin tespit edilmesi teknik açıdan mümkündür; ancak bu tespitin güvenilir biçimde gerçekleşmesi için sürekli otomatik izleme sistemlerinin devrede olması ve referans ölçümlerin düzenli olarak güncellenmesi gerekmektedir. Tek seferlik bakım muayeneleri, uzun vadeli gizli müdahaleleri yakalamakta yetersiz kalmaktadır.

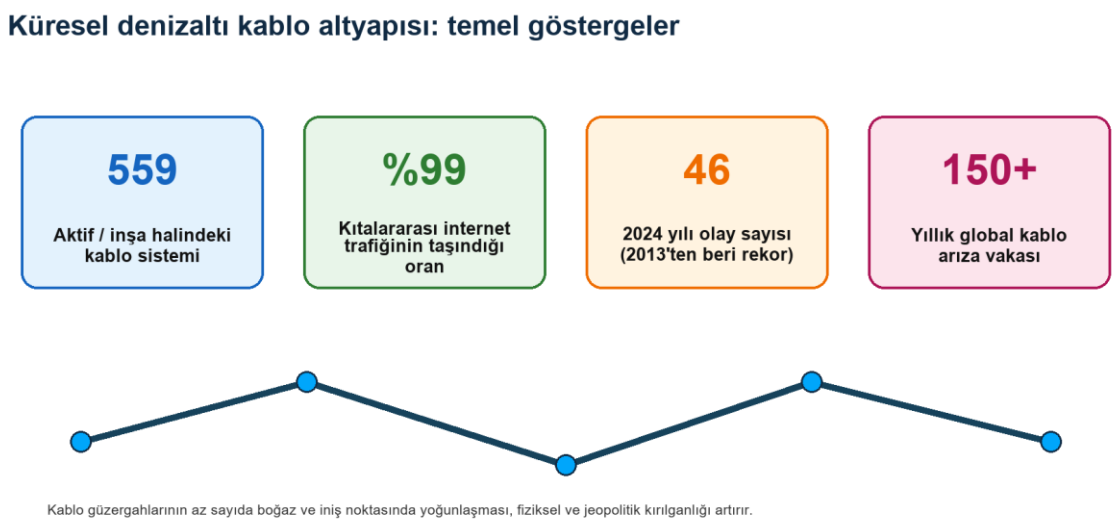
Gerçek dünya saldırı senaryolarında kritik risk penceresi çoğunlukla ilk kurulum ya da bakım aşamasında açılır. Kablo döşeme, splitter ekleme ve cihaz yapılandırmasının yoğun biçimde yürütüldüğü bu dönemde altyapıya müdahale en kolaydır. Üçüncü taraf firmaların devreye girdiği büyük kurulum projelerinde ya da yabancı kaynaklı ekipmanın kullanıldığı durumlarda bu risk katlanmaktadır. Optik güç ölçer ile sürekli izleme ve bağımsız denetim bu açığı kapatabilecek temel önlemler arasındadır.

4.1.3 Altyapı Güvenliğine Yönelik Jeopolitik Tehditler

4.1.3.1 Denizaltı Kablo Ağlarının Stratejik Konumu

Fiber optik altyapının en kırılgan ve aynı zamanda en stratejik kesimi, kıtaları birbirine bağlayan denizaltı kablolarıdır. 2024 yılı itibarıyla dünya genelinde 559 aktif ya da inşaat halindeki kablo sistemi bulunmakta; bu kablolar kıtalararası internet trafiğinin yüzde doksan dokuzunu ve yıllık 10 trilyon doları aşan finansal işlem hacmini taşımaktadır (Global Taiwan Institute, 2025). Herhangi bir denizaltı kablosunun hasar görmesi bireysel kullanıcılarla sınırlı kalmaz; ulusal ekonomileri, askeri komuta sistemlerini ve kritik devlet altyapılarını doğrudan etkiler.

Bu yapı Şekil 4.2'de gösterilmektedir.



Şekil 4.2. Küresel denizaltı kablo altyapısı: temel göstergeler

Kaynak: Insikt Group (2025); Global Taiwan Institute (2025); The Week (2026) verilerinden derlenmiştir.

Insikt Group'un (2025) kapsamlı değerlendirmesine göre, denizaltı kablo ekosistemindeki üç yapısal zayıflık (ağ fazlalığının yetersizliği, kablo güzergâhlarının çeşitlendirilememiş olması ve küresel onarım kapasitesinin kısıtlılığı) ciddi bir kesinti riskini kalıcı hale getirmektedir. Carnegie Endowment (2024), bu bağlamda çarpıcı bir uyarıda bulunmaktadır: birden fazla denizaltı kablosuna koordineli bir saldırı, küresel internet bağlantısı üzerinde felaket boyutlarında sonuçlar doğurabilir.

4.1.3.2 Son Dönem Sabotaj Olayları

Şüpheli sabotaj vakalarının sayısı, 2022 yılından bu yana dramatik biçimde artmıştır. SubTel Forum verilerine göre 2024'te raporlanan 46 olay, platformun 2013'ten bu yana tuttuğu kayıtlarda görülen en yüksek değeri temsil etmektedir; bu rakam 2023'teki 15 olayla kıyaslandığında trendin kaygı verici bir ivme kazandığı açıkça görülmektedir (Insikt Group, 2025).

Tablo 4.3. 2023–2025 döneminde öne çıkan denizaltı kablo olayları

Tarih	Kablo / Bölge	Olası Aktör	Etki	Sonuç
Şub. 2023	Tayvan, Matsu Adaları (2 kablo)	Çin balıkçı ve kargo gemisi (kasıtlı şüphesi kuvvetli)	50 gün kısıtlı erişim; kapasitenin %5'ine düşüş	NCC altyapıyı 'kritik' ilan etti (2024)
Eki. 2023	Balticconnector (Baltık Denizi)	Çin bayraklı gemi; çıpa hasarı iddiası	Doğalgaz + internet altyapısı zarar gördü	AB ve NATO soruşturması
Mar. 2024	Kızıldeniz Koridoru (4 kablo)	Houthi tehdidi nedeniyle gemi güzergah değişiklikleri; çıpa hasarı şüphesi	Hindistan, Afrika, Orta Doğu etkilendi	Google ve Meta yeniden rotalama
Kas. 2024	C-Lion1 Fin.–Alm. + BCS İsv.–Lit.	Yi Peng 3 gemisi (Rus limanından çıktı)	Litvanya bant genişliğinin ~%20'si	NATO 'Baltic Sentry' misyonu
Oca. 2025	Tayvan - Uluslararası hat	4 ayrı olay 2 ayda; model örüntüsü	Finansal işlemler yeniden yönlendirildi	MODA 10 kabloyu koruma altına aldı

Tablo 4.3'teki olaylar üç ortak örüntüyü paylaşmaktadır: saldırılar kriz dönemlerinde ya da jeopolitik gerilimin tırmandığı anlarda yoğunlaşmakta; olağan deniz trafiği kablolar üzerinde 'kaza' kılığına bürünmüş müdahaleleri gizlemek için kullanılmakta; hasar sonrası onarım süreci haftalar ya da aylarca sürebilmekte, bu da kalıcı bağlantı sorunlarına yol açmaktadır. NATO, bu tehdit ortamına yanıt olarak 2023 yılında Brüksel'de Kritik Deniz Altı Altyapı Koordinasyon Hücresi'ni kurmuş; 'Baltic Sentry' misyonuyla bölgedeki denizaltı kablo güvenliğini bir savunma önceliği haline getirmiştir (Jackson School, 2025).

4.1.3.3 Yazılım Egemenliği: Görünmez Tehdit

Fiziksel güvenliğin ötesinde, telekom santrallerinde kullanılan yazılımın menşei de kritik bir güvenlik boyutu oluşturmaktadır. Yabancı kaynaklı yazılım ya da ürün yazılımı (firmware) içeren santral donanımları, teorik olarak üretici firmanın uzaktan müdahalesine, devre dışı bırakma komutlarına ya da arka kapı erişimine açık olabilir. Bu risk, özellikle savaş veya kriz dönemlerinde stratejik sonuçlar doğurabilir: düşman ya da rakip ülkenin yazılımını kullanan altyapılar, kritik bir anda iletişimi kesen bir 'kill switch' işlevi görme potansiyeli taşır.

Avrupa Birliği'nin NIS2 Direktifi (2022), bu gerekçeyle telekomünikasyon ağlarını 'birincil siber saldırı hedefleri' olarak tanımlamış ve üye devletleri denizaltı kabloları da dahil olmak üzere kritik iletişim altyapılarına özgü siber güvenlik stratejileri geliştirmeye zorlamaktadır (Carnegie Endowment, 2024). Fransa'nın 2024'te Alcatel Submarine Networks'ü millileştirme kararı, bu stratejik hassasiyetin somut bir yansımasıdır (HEC Paris, 2024).

4.1.4 Klasik Kriptografinin Hesaplama Sınırları

4.1.4.1 Güvenlik Paradigmasının Yapısal Kırılganlığı

Klasik kriptografi, güvenliğini belirli matematiksel problemlerin hesaplama açısından çözümsüzlüğüne yaslar. RSA algoritması büyük tamsayıların asal çarpanlarına ayrıştırılmasının pratikte mümkün olmadığı varsayımına, Eliptik Eğri Kriptografisi (ECC) ise ayrık logaritma problemine dayanır. Bu varsayımlar bugünkü teknoloji için geçerliliğini korumaktadır. Ancak bu güvenlik modeli yapısal bir zafiyet barındırır: 'hesaplama açısından zor' ifadesi mutlak değil göreli bir nitelendirmedir; bugün zor olan, yarın donanım ve algoritma gelişmeleriyle aşılabilir hale gelebilir (ETSI, 2015).

Bu güvensizliğin somut bir boyutu, 'şimdi sakla, sonra çöz' (harvest now, decrypt later; HNDL) saldırısıdır. Bu senaryoda bir saldırgan bugün şifreli trafiği kaydedip kuantum bilgisayarlar olgunlaştığında deşifre eder. Askeri iletişimler, tıbbi kayıtlar ve diplomatik yazışmalar gibi uzun vadeli gizlilik gerektiren veriler, bu tehdide zaten bugünden maruz kalmaktadır; çünkü kaydedilen veri gelecekte kırılabilecektir (Renner ve Wolf, 2023).

4.1.4.2 Kuantum Algoritmalarının Kriptografiye Etkisi

TEMEL MATEMATİKSEL İFADELER	
Formül Adı	**Matematiksel Gösterim**
Optik Güç Kaybı *Sinyal gücü dB ölçümü*	***L (dB) = −10 · log10 (Pçıkış / Pgiriş)***
Shor Algoritması *Açık anahtar kriptografi tehdidi*	Klasik: O (exp (n1/3)) → Shor: O (n3)

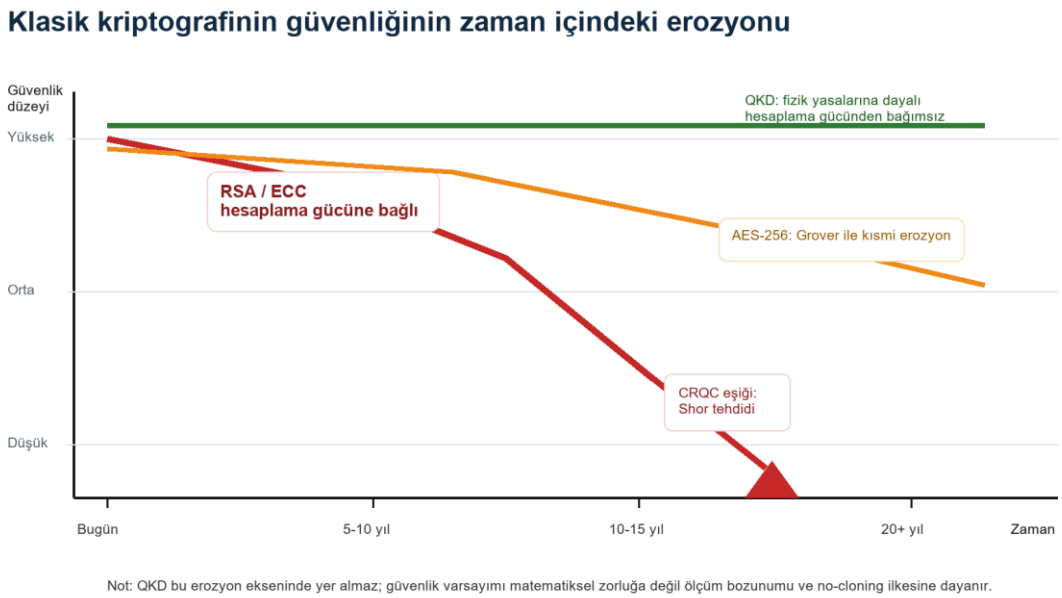
TEMEL MATEMATİKSEL İFADELER	
Grover Algoritması *Simetrik şifre güvenlik düşüşü*	AES-k → 2k/2 sorgu ≡ AES-256 → AES-128 eşdeğeri
QKD Bilgi Güvenliği *Bilgi-teorik ispat*	$I(\text{saldırgan} ; \text{anahtar}) = 0 \ \forall$ *hesaplama gücü*

Not: n = anahtar bit uzunluğu. RSA-2048 için n = 2048; klasik kırma O(exp(2048^(1/3))) ≈ O(exp(12.7)) iken Shor algoritması bunu O(2048³) ≈ O(8.6 × 10⁹) işleme indirir; günümüz kuantum donanımıyla ölçeklenebilir.

Peter Shor'un 1994'te önerdiği ve adını taşıyan algoritma, büyük tamsayıları polinom zamanda asal çarpanlarına ayırabilmektedir. Klasik bilgisayarların bu işlem için üstel süre gerektirdiği düşünüldüğünde, Shor algoritması RSA ve ECC tabanlı tüm açık anahtarlı kriptografi sistemlerini pratik olarak anlamsız kılar. Scrivano'nun (2025) kapsamlı karşılaştırmalı analizine göre, 2048 bitlik bir RSA anahtarı, bugün için son derece güçlü kabul edilmektedir, yeterli qubit kapasitesine sahip bir kuantum bilgisayar tarafından saniyeler içinde kırılabilir.

Lov Grover'ın 1996'da geliştirdiği algoritma ise simetrik şifreleme sistemlerini hedef almaktadır. Yapılandırılmamış arama problemlerini karesel hızlanmayla çözen bu algoritma, AES-256'nın etkin güvenlik düzeyini yaklaşık 128 bit eşdeğerine indirir. ETSI (2015), bu bulgu doğrultusunda simetrik şifreleme için anahtar uzunluğunun iki katına çıkarılmasını önerir; bu sayede Grover tehdidi azaltılabilir. Oysa Shor tehdidi matematiksel yapı gereği temel kırılmayı temsil ettiğinden, anahtar uzunluğunu artırmak RSA ve ECC için yeterli değildir; bu şemalar bütünüyle değiştirilmelidir.

Bu yapı Şekil 4.3'te gösterilmektedir.



Şekil 4.3. Klasik Kriptografinin Güvenliğinin Zaman İçindeki Erozyonu

Not: QKD güvenliği bu eksende yer almaz; fizik yasalarına dayandığından hesaplama gücündeki ilerlemeyle aşınamaz.

4.1.4.3 Üç Paradigmanın Karşılaştırılması

Klasik kriptografinin ötesinde iki ana çözüm yolu öne çıkmaktadır. Kuantum Sonrası Kriptografi (PQC), kuantum bilgisayarlara dirençli olduğu öngörülen yeni matematiksel problemlere dayalı algoritmalar geliştirir. NIST, 2024 yılında CRYSTALS-Kyber ve Dilithium gibi algoritmaları standart olarak onaylamıştır. Kuantum Anahtar Dağıtımı (QKD) ise güvenliğini matematiksel bir varsayıma değil, kuantum fiziğinin temel yasalarına (ölçüm bozunumu ve no-cloning teoremi) dayandırır. ETSI'nin bu konudaki değerlendirmesi açık ve güçlüdür: QKD, sınırsız hesaplama kaynağına sahip bir saldırgana karşı dahi bilgi-teorik olarak güvenli olduğu ispat edilmiş tek anahtar dağıtım mekanizmasıdır (ETSI, 2015).

Bu karşılaştırma Tablo 4.4'te özetlenmektedir.

Tablo 4.4. Klasik kriptografi, QKD ve PQC: kapsamlı karşılaştırma

Kriter	Klasik Kriptografi (RSA / ECC)	Kuantum Anahtar Dağıtımı (QKD)	Kuantum Sonrası Kriptografi (PQC)
Güvenlik temeli	Hesaplama karmaşıklığı (matematiksel problem)	Kuantum fiziğinin yasaları (ölçüm bozunumu / no-cloning)	Hesaplama karmaşıklığı (kuantuma dirençli problem)
RSA-2048 kırılması	Klasik bilgisayar için pratik değil	İlgisiz - RSA kullanmaz; foton tabanlı anahtar	Tasarımı gereği kuantuma karşı dirençli
Shor algoritması riski	TAM KIRILIYOR - polinom zamanda çözüm	ETKİSİZ - güvenlik hesaplamaya dayanmıyor	DİRENÇLİ - kuantum zor problemler seçildi
Grover algoritması riski	AES-256 → AES-128 eşdeğerine düşer	ETKİSİZ	SINIRLI - anahtar uzatma yeterli
'Şimdi sakla sonra çöz'	MEVCUT - bugünkü veri gelecekte kırılabilir	YOK - dinleme tespit edilince anahtar iptal edilir	DÜŞÜK - matematiksel varsayıma bağlı
Eavesdropper tespiti	YOK - pasif dinleme görünmez	GARANTİLİ - ölçüm durumu bozar, hata artar	YOK - klasikle aynı fiziksel katman

Kriter	Klasik Kriptografi (RSA / ECC)	Kuantum Anahtar Dağıtımı (QKD)	Kuantum Sonrası Kriptografi (PQC)
Mevcut olgunluk	Çok Yüksek (50+ yıllık altyapı)	Orta (ilk ticari dağıtımlar aktif)	Yüksek (NIST 2024 standartları)

Kaynak: ETSI (2015); Scrivano (2025); Kish ve Pieprzyk (2025); Frontiers in Physics (2024) verilerinden sentezlenmiştir. Kırmızı hücreler kritik zafiyetleri, yeşil hücreler güvenlik üstünlüklerini göstermektedir.

4.1.5 Kuantum Haberleşmeye Geçiş Motivasyonu

4.1.5.1 Güvenlik Paradigmasının Temelden Değişimi

Önceki bölümlerde ortaya konan tehdit tablosu, tek bir temel sonucu işaret etmektedir: klasik iletişim güvenliği hem fiziksel hem de kriptografik katmanlarda yapısal kırılganlıklar barındırmaktadır. Fiziksel katmanda bir saldırgan, fiber hattını kesmeksizin kopyalayabilir; kriptografik katmanda ise bugünkü şifreli veriler gelecekte çözülebilir. Bu iki kırılganlık birleştiğinde, güvenli iletişim ancak her iki zafiyeti de aynı anda kapatan yeni bir paradigmayla mümkün olabilir.

Kuantum haberleşme bu paradigmayı üç temel ilke üzerine inşa eder. Birincisi, fizik yasaları dinlemeyi kaçınılmaz biçimde ifşa eder: kuantum anahtar dağıtımında bilgi fotonların kuantum durumları aracılığıyla aktarılır. Bir fotonu ölçmek, kuantum mekaniğinin ölçüm sonrası durum çöküşü ilkesi gereği o fotonun durumunu geri dönüşümsüz biçimde değiştirir; bu bozunma saldırganın (dinleyicinin) varlığını kaçınılmaz biçimde ortaya çıkarır. İkincisi, kopyalama fiziksel olarak olanaksızdır: no-cloning teoremi, bilinmeyen bir kuantum durumunun birebir kopyasının üretilemeyeceğini kanıtlar; bu, klasik bitlerin aksine fotonların mükemmel biçimde kopyalanamayacağı anlamına gelir. Üçüncüsü, güvenlik hesaplama gücüne değil doğaya dayanır: ETSI'nin (2015) ifadesiyle, QKD sonsuz hesaplama kaynağına sahip bir saldırgana karşı bile güvenliğini korur; çünkü bu güvenlik matematiksel varsayımlara değil fiziğin temel yasalarına yaslanır.

4.1.5.2 Mevcut Altyapının Dönüşümü

Kuantum anahtar dağıtımının yaygınlaşması, telekom altyapısında köklü bir dönüşümü zorunlu kılacaktır. Günümüzün SFP modülleri ve klasik optik alıcı-vericiler, foton düzeyinde iletişim gerektiren QKD sistemlerine uyum sağlamak için yeniden tasarlanmış bileşenlerle değiştirilecektir. Kish ve Pieprzyk (2025), bu geçişin önündeki temel teknik engeli açıkça tanımlar: kuantum yükselteçlerin (quantum repeaters) henüz olgunlaşmamış olması nedeniyle günümüz QKD sistemleri 100–200 km mesafeyle sınırlıdır.

Mevcut fiber altyapısının QKD için yeniden kullanılması mümkün olmakla birlikte, önemli bir teknik kısıtlama göz önünde bulundurulmalıdır: tek modlu fiber üzerinde klasik optik sinyaller ile kuantum sinyaller (tekil fotonlar) eş zamanlı iletildiğinde, klasik sinyallerin uyarılmış Raman saçılımı (SRS) gürültüsü foton tabanlı kuantum kanalını baskılayabilir. Pratik çözüm, iki kanalı farklı spektral bantlara ayırmaktır. Yaygın kullanılan bir yapılandırmada klasik yüksek hızlı trafik C-bandında (1530–1565 nm) taşınırken kuantum sinyalleri O-bandında (1260–1360 nm) ya da L-bandında (1565–1625 nm) iletilir;

böylece SRS etkisinin yoğunlaştığı bölgeden kaçınılır. Alternatif olarak ayrı bir fiber çifti tahsis edilebilir. Her iki yaklaşım da geçiş maliyetini artırır; ancak mevcut kablo güzergahlarının ve kanallarının büyük bölümü fiziksel olarak yeniden değerlendirilebilir niteliktedir (ETSI, 2015; Kish ve Pieprzyk, 2025).

Geçişi hızlandıran bir diğer etken hibrit güvenlik mimarilerinin uygulanabilirliğidir: QKD ile üretilen kuantum anahtarlar, mevcut AES gibi simetrik şifreleme sistemlerini beslemek için kullanılabilir. Bu sayede klasik altyapının büyük bölümü değiştirilmeksizin güvenlik düzeyi kuantum temeline taşınabilir (ETSI, 2015).

Kuantum yükselteç teknolojisindeki son gelişmeler, mesafe sınırının önümüzdeki on yılda aşılacağına işaret etmektedir. 2025 yılı sonlarında Stuttgart Üniversitesi, iki farklı kuantum noktasından gelen fotonlar arasında kuantum ışınımı gerçekleştirerek ölçeklenebilir kuantum yükselteçlere giden yolda kritik bir adım attı (Strobel ve ark., Nature Communications, 2025). Aynı dönemde Chicago Üniversitesi, telekomünikasyon dalga boyunda çalışan yeni nesil spin-foton arayüzleri geliştirerek kuantum bağlantı mesafesini 200 kat uzatabilecek bir platform sundu. Bu alandaki en çarpıcı ilerleme ise Şubat 2026'da gerçekleşti: Çin Bilim ve Teknoloji Üniversitesi'nden Pan Jianwei liderliğindeki ekip, ölçeklenebilir kuantum yükselteçler için gereken bellek-bellek dolanıklığını ilk kez başarıyla göstererek bu temeli kullanarak 100 km ötesinde aygıt-bağımsız kuantum anahtar dağıtımı (DI-QKD) gerçekleştirdi; sonuçlar Nature ve Science dergilerinde yayımlandı. Bu gelişme, kuantum yükselteç araştırmacılarının uzun süredir beklediği fizibilite kanıtını oluşturmaktadır.

4.1.5.3 Jeopolitik ve Stratejik Zorunluluk

Bölüm 3.1.3.2'de belgelenen denizaltı kablo sabotajları ve saldırıları, kuantum iletişiminin yalnızca bir teknoloji yükseltmesi olmadığını; ulusal güvenlik açısından stratejik bir zorunluluk haline geldiğini göstermektedir. Fiber hattına fiziksel müdahale her zaman mümkün olacaktır. Ancak kriptografik katman kuantum güvenli hale getirildiğinde, bir saldırgan fiberi başarıyla dinlemiş olsa bile elinde anlamsız veriler kalır: no-cloning teoremi fotonu kopyalamayı, ölçüm bozunumu ise gizlice dinlemeyi fiziğin yasaları düzeyinde engeller.

Bu gerekçeyle küresel ölçekte yoğun bir kuantum altyapı yatırımı başlamıştır: Çin ülke geneline yayılan bir kuantum iletişim ağı kurmuş; Avrupa Birliği, üye ülkeleri kapsayan EuroQCI (European Quantum Communication Infrastructure) girişimini hayata geçirmiş; ABD ise Ulusal Kuantum Girişimi Yasası kapsamında araştırma ve geliştirme fonlamasını artırmıştır. NATO, kritik altyapı güvenliğini birincil savunma önceliği olarak tanımlamış ve bu çerçevede üye ülkeleri kuantum güvenli iletişim teknolojilerine yatırım yapmaya yönlendirmiştir (ETSI, 2015).

Bu tartışma, bir sonraki bölümde ele alınan no-cloning teoremi ve ölçüm bozunumu ilkelerinin neden kuantum anahtar dağıtımının fiziksel temelini oluşturduğunu açık hale getirmektedir.

4.2 Kopyalanamama Teoremi (No-Cloning Theorem)

4.2.1 Teoremin Tarihsel Arka Planı

Klasik bilgi işlemede herhangi bir veri, ilkesel olarak sonsuz sayıda kopyalanabilir. Bir metin dosyası, bir müzik parçası veya bir şifreleme anahtarı birebir çoğaltılabilir ve bu kopya orijinalinden ayırt edilemez. Kuantum mekaniğinde ise durum kökten farklıdır. 1982 yılında Wootters ve Zurek, bilinmeyen bir kuantum durumunun tam bir kopyasının üretilemeyeceğini matematiksel olarak kanıtlamıştır (Wootters ve Zurek, 1982). Aynı yıl, bağımsız olarak Dieks de benzer bir sonuca ulaşmıştır (Dieks, 1982).

Bu teorem, kuantum bilgi kuramının en temel ilkelerinden birini oluşturmakta ve kuantum kriptografinin güvenlik temelini sağlamaktadır.

Teoremin keşfi, aslında Nick Herbert'ın ışıktan hızlı iletişim ("superluminal communication") önerisini çürütme girişiminden doğmuştur. Herbert, EPR (Einstein-Podolsky-Rosen) dolaşıklığını kullanarak ışıktan hızlı sinyal göndermenin mümkün olduğunu ileri sürmüştü. Wootters ve Zurek bu önerinin neden işlemeyeceğini gösterirken kopyalanamama teoremine ulaşmıştır. Böylece, görelişin temel bir ilkesini (superluminal iletişim yasağı) kuantum mekaniğiyle uzlaştıran bu teorem, aynı zamanda yepyeni bir alanın kapılarını açmıştır.

4.2.2 Teoremin Matematiksel İspatı

Kopyalanamama teoreminin kanıtı, kuantum mekaniğinin lineer yapısına dayanır. Varsayımsal olarak, bilinmeyen herhangi bir kuantum durumunu kopyalayabilen bir üniter operatör U bulunduğu kabul edilsin. Bu durumda kopyalama işlemi Denklem (4.1) ile gösterilebilir (Nielsen ve Chuang, 2010).

$$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle \quad \textbf{(4.1)}$$

Aynı operatör iki farklı durum için de geçerli kabul edildiğinde, üniterliğin korunumu iç çarpımlar üzerinde Denklem (4.2)'yi zorunlu kılar.

$$\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle^2 \quad \textbf{(4.2)}$$

Denklem (4.2) yalnızca $\langle\psi|\varphi\rangle = 0$ veya $\langle\psi|\varphi\rangle = 1$ durumlarında sağlanır. Başka bir deyişle, evrensel bir kopyalama makinesi yalnızca birbirine dik ya da özdeş durumlarda çalışabilir; bilinmeyen genel bir kuantum durumunun mükemmel kopyasının üretilmesi fiziksel olarak mümkün değildir (Wootters ve Zurek, 1982; Dieks, 1982).

4.2.3 Kriptografi Açısından Önemi

Kopyalanamama teoremi, kuantum kriptografinin güvenlik teminatının merkezinde yer alır. Klasik kriptografide bir dinleyici (Eve), iletişim kanalı üzerinden geçen bitleri fark edilmeden kopyalayabilir. Oysa kuantum kriptografide bilgi, kuantum durumları (genellikle tek fotonların polarizasyon durumları) üzerinde kodlanmıştır. Kopyalanamama teoremi gereği, Eve bu fotonların tam bir kopyasını alamaz (Gisin vd., 2002). Bilgiyi elde etmek için ölçüm yapması gerekir; ancak bu ölçüm kuantum durumunu kaçınılmaz olarak bozar. Dolayısıyla dinleme girişimi, iletişim kuran taraflar tarafından tespit edilebilir hale gelir.

Bu durum, klasik kriptografi ile kuantum kriptografi arasındaki paradigma farkını vurgular. Klasik kriptografik protokollerin güvenliği, belirli matematiksel problemlerin hesaplama güçlüğüne (örneğin büyük sayıların çarpanlarına ayrılması; bkz. Rivest vd., 1978) dayanmaktadır. Kuantum kriptografi ise güvenliğini fizik yasalarından, özellikle kopyalanamama teoreminden ve ölçüm bozunumundan almaktadır (Scarani vd., 2009).

4.3 Ölçüm Bozunumu (Measurement Disturbance)

4.3.1 Heisenberg Belirsizlik İlkesi

Kuantum mekaniğinin en temel ilkelerinden biri, Werner Heisenberg tarafından 1927 yılında formüle edilen belirsizlik ilkesidir (Heisenberg, 1927). Bu ilke, birbirini tamamlayan (konjuge) fiziksel büyüklüklerin eşzamanlı olarak keyfi hassasiyetle belirlenemeyeceğini ifade eder. Örneğin, bir parçacığın konumu ne kadar kesin ölçülürse, momentum değeri o kadar belirsiz hale gelir ve bunun tersi de geçerlidir.

Kuantum kriptografi bağlamında belirsizlik ilkesi, farklı ölçüm tabanlarının birbirini tamamlayıcı (konjuge) olması anlamına gelir. BB84 protokolünde kullanılan dikdoğrusal (+) ve çapraz (×) polarizasyon tabanları, konjuge tabanlardır. Bir fotonun dikdoğrusal tabanda kesin olarak bilinen polarizasyonu, çapraz tabanda tamamen rasgele bir sonuç verir (Nielsen ve Chuang, 2010). Bu özellik, dinleyicinin doğru tabanı tahmin edemediği her durumda hata üretmesine yol açar.

4.3.2 Kuantum Ölçümün Doğası

Klasik fizikte ölçüm, sistemi ilkesel olarak bozmadan gerçekleştirilebilir. Bir termometreyi bir suya daldırdığımızda suyun sıcaklığını ihmal edilebilir ölçüde etkileriz. Oysa kuantum mekaniğinde ölçüm, sistemin durumunu temel düzeyde değiştirir. Süperpozisyon durumundaki bir kuantum sistemi ölçüldüğünde, ölçüm sonucuna karşılık gelen özduruma çöker ve süperpozisyon bilgisi geri dönülemez biçimde kaybolur (Nielsen ve Chuang, 2010).

Bu durumu somutlaştırmak için şu örneği düşünelim: Alice, 45° polarizasyonlu (çapraz tabanda $|+\rangle$ durumunda) bir foton göndersin. Eğer Eve bu fotonu dikdoğrusal tabanda ($\{|0\rangle, |1\rangle\}$) ölçerse, %50 olasılıkla $|0\rangle$ (yatay) veya $|1\rangle$ (dikey) sonucunu elde edecektir. Ölçüm sonrasında fotonun durumu artık orijinal 45° değil, ölçüm sonucuna göre 0° veya 90° olacaktır. Eve bu fotonu Bob'a ilettiğinde, Bob doğru tabanı kullansa bile yanlış sonuç elde edebilecektir. Bu hata, dinlemenin fiziksel bir izidir (Gisin vd., 2002).

4.3.3 Dinlemenin Fiziksel İzi

Ölçüm bozunumu, kuantum kriptografinin güvenlik garantisinin ikinci temel direğidir. Kopyalanamama teoremi, Eve'in bilgiyi kopyalamasını engeller; ölçüm bozunumu ise Eve'in bilgiyi elde etme girişiminin kaçınılmaz olarak izler bırakmasını sağlar. Bu iki ilke birlikte, kuantum anahtar dağıtımının koşulsuz güvenliğini garanti eder (Scarani vd., 2009).

Somut olarak, Eve'in en basit saldırı stratejisi olan "yakala ve tekrar gönder" (intercept-resend) saldırısında, Eve her fotonu yakalar, rasgele bir tabanda ölçer ve ölçüm sonucuna göre yeni bir foton üretip Bob'a gönderir. Eve, tabanları rasgele seçtiği için durumların yarısında yanlış taban kullanacak ve bu bitlerin dörtte birinde hata oluşacaktır. Dolayısıyla bu saldırı yöntemi, tüm bitlerin yaklaşık %25'lik bir hata oranı (Quantum Bit Error Rate, QBER) üretir. Alice ve Bob, anahtarın bir kısmını karşılaştırarak bu hata oranını tespit edebilir (Bennett ve Brassard, 1984).

4.4 Alice, Bob ve Eve

4.4.1 Kriptografik Karakter Modeli

Kriptografi literatüründe iletişim protokollerini açıklamak için geleneksel olarak karakter isimleri kullanılır. Bu gelenek, soyut matematik ve mühendislik kavramlarını somutlaştırarak anlaşılırlığı artırır. En yaygın üç karakter şunlardır:

Alice: İletişimi başlatan taraftır. Kuantum kriptografide fotonları hazırlayan ve gönderen kişidir. Protokolün gönderici (transmitter) tarafını temsil eder.

Bob: İletişimin alıcı tarafıdır. Kuantum kriptografide fotonları alan ve ölçen kişidir. Protokolün alıcı (receiver) tarafını temsil eder.

Eve: İngilizce "eavesdropper" (dinleyici/gizli dinleyici) kelimesinden türetilmiş bir isimdir. Kanalı dinleyen, bilgi elde etmeye çalışan saldırganı temsil eder. Eve'in kapasitesi, analiz edilen güvenlik modeline göre değişir; en güçlü varsayımda Eve, fizik yasalarının izin verdiği her türlü teknolojiye sahiptir (Scarani vd., 2009).

4.4.2 Klasik Kriptografiden Kuantum Kriptografiye

Klasik kriptografide Alice ve Bob'un temel sorunu, güvenli bir anahtar paylaşımı gerçekleştirmektir. Açık anahtar kriptografisi (Rivest vd., 1978) bu sorunu hesaplama karmaşıklığına dayanarak çözer: Büyük sayıları çarpanlarına ayırmak hesaplama açısından son derece zordur ve RSA gibi algoritmalardaki güvenlik bu zorluğa dayanır. Ancak bu güvenlik koşulsuz değildir; yeterli hesaplama gücüne sahip bir saldırgan (veya gelecekte bir kuantum bilgisayar) bu sistemleri kırabilir.

Shannon (1949), mükemmel gizliliğin (perfect secrecy) ancak anahtarın mesaj kadar uzun olduğu durumda elde edilebileceğini göstermiştir. Bu koşulu sağlayan tek kriptografik sistem, tek kullanımlık şifre defteridir (one-time pad). Ancak bu sistemin pratik bir sorunu vardır: uzun anahtarların güvenli biçimde dağıtılması gerekir. Kuantum anahtar dağıtımı (QKD), fizik yasalarının garantisi altında güvenli anahtar dağıtımı yaparak bu sorunu çözer ve tek kullanımlık şifre defterinin pratik uygulanabilirliğini mümkün kılar (Gisin vd., 2002).

Kuantum kriptografide Alice ve Bob arasındaki iletişim iki kanal üzerinden gerçekleşir. Birincisi, fotonların gönderildiği kuantum kanalıdır. Bu kanal, Eve'in fiziksel erişimine açık olabilir; ancak ölçüm bozunumu sayesinde dinleme tespit edilebilir. İkincisi, Alice ve Bob'un taban karşılaştırması ve hata analizi yaptığı klasik kanalıdır (açık bir kanalda yapılır). Bu kanalın gizli olmaması sorun teşkil etmez; yalnızca kimlik doğrulaması (authentication) yapılması yeterlidir (Bennett ve Brassard, 1984).

4.5 Kuantum Anahtar Dağıtımına Giriş (QKD)

4.5.1 QKD'nin Temel Felsefesi

Kuantum anahtar dağıtımı (Quantum Key Distribution, QKD), iki tarafın ortak bir gizli anahtar oluşturmasını sağlayan bir protokol ailesidir. QKD'nin amacı doğrudan mesaj göndermek değildir; amaç, güvenli bir şifreleme anahtarı oluşturmaktır. Bu anahtar daha sonra klasik şifreleme yöntemleriyle (tercihen tek kullanımlık şifre defteriyle) birlikte kullanılır (Gisin vd., 2002).

QKD'nin devrimsel yönü, güvenliğinin hesaplama karmaşıklığına değil, kuantum mekaniğinin temel yasalarına dayanmasıdır. Eğer kuantum mekaniği doğruysa, QKD koşulsuz güvenlidir (information-theoretic security). Bu, gelecekteki herhangi bir teknolojik gelişmenin -kuantum bilgisayarlar dâhil- QKD'nin güvenliğini tehdit edemeyeceği anlamına gelir (Scarani vd., 2009).

4.5.2 Bilgi-Kuramsal Güvenlik

Güvenlik kavramı kriptografide iki farklı düzeyde tanımlanır. Birincisi, hesaplama güvenliği (computational security): güvenlik, belirli bir matematiksel problemin çözülmesinin pratik olarak mümkün olmamasına dayanır. RSA ve Diffie-Hellman bu kategoridedir. İkincisi, bilgi-kuramsal güvenlik (information-theoretic security): Eve, sınırsız hesaplama gücüne sahip olsa bile bilgiyi elde edemez. Shannon'ın (1949) tanımladığı mükemmel gizlilik bu kategoridedir.

QKD, ikinci kategori olan bilgi-kuramsal güvenlik sağlar. QKD'nin güvenlik kanıtı, kopyalanamama teoremi ve ölçüm bozunumunun birleşiminden türetilir. Eve'in kanal üzerinden elde edebileceği bilgi miktarı, fizik yasaları tarafından sınırlanmıştır. Alice ve Bob, hata oranını analiz ederek Eve'in elde edebileceği maksimum bilgiyi hesaplayabilir ve gizlilik yükselticisi (privacy amplification) teknikleriyle bu bilgiyi ihmal edilebilir düzeye indirebilir (Gisin vd., 2002).

4.5.3 QKD Protokol Ailesi

QKD alanında çeşitli protokoller geliştirilmiştir. Tarihsel olarak ilk ve en temel protokol, Bennett ve Brassard (1984) tarafından önerilen BB84'tür. Ekert (1991) tarafından önerilen E91 protokolü, Bell eşitsizliğine dayanan dolanıklık tabanlı bir yaklaşım sunar. B92 protokolü ise BB84'ün sadeleştirilmiş bir versiyonudur ve iki kuantum durumu kullanır. Gisin vd. (2002) bu protokollerin kapsamlı bir karşılaştırmasını sunmuştur. BB84, hem tarihsel önemi hem de pratik uygulanabilirliği nedeniyle en yaygın kullanılan QKD protokolüdür ve bir sonraki bölümde ayrıntılı olarak incelenecektir.

4.6 BB84 Protokolü ve Kuantum Anahtar Dağıtımının Kriptografik Analizi

4.6.1 Giriş: Kuantum Kriptografinin Doğuşu

1984 yılında Charles Bennett ve Gilles Brassard tarafından önerilen BB84 protokolü, kuantum anahtar dağıtımının (QKD) ilk ve en temel protokolüdür (Bennett ve Brassard, 1984). Klasik kriptografinin aksine BB84, güvenliğini matematiksel problemlerin (çarpanlara ayırma vb.) zorluğuna değil, kuantum mekaniğinin temel yasalarına dayandırır. Bennett ve Brassard, bu protokolün "koşulsuz güvenli" (unconditionally secure) bir haberleşme kanalı sunduğunu belirtir (Bennett ve Brassard, 1984).

4.6.2 BB84 Protokolü: Adım Adım Operasyonel Akış ve Teknik Analiz

BB84 protokolü, kuantum mekaniğinin "Gözlemcinin Etkisi" ve "Klonlamama Teoremi" (No-Cloning Theorem) yasalarını kullanarak, iki taraf (Alice ve Bob) arasında güvenli bir simetrik anahtar oluşturulmasını sağlar. Süreç, fiziksel bir kuantum kanalı ile klasik bir haberleşme kanalının eş zamanlı kullanımını gerektirir.

4.6.2.1 Kuantum İletim Aşaması (Fiziksel Katman)

Kuantum iletimi, bilginin tekil fotonlar üzerine kodlandığı ve kanal (fiber veya serbest uzay) üzerinden gönderildiği aşamadır.

Alice'in kuantum hazırlığı ve kodlama adımında önce rastgele bir bit dizisi a ∈ {0,1}^n, ardından bu bitleri temsil edecek rastgele bir baz dizisi b ∈ {+,×}^n üretilir. Nielsen ve Chuang (2010), bu iki bazın eşlenik olduğunu; bir bazda tam bilginin diğer bazda belirsiz hale geldiğini vurgulamaktadır.

Rektilinear baz (+) için 0 → |H⟩ (yatay) ve 1 → |V⟩ (dikey); diyagonal baz (×) için ise 0 → |D⟩ (+45°) ve 1 → |A⟩ (−45°) eşlemesi kullanılır.

Bu eşleşmenin sifting aşamasındaki etkisi Tablo 4.5'te örneklenmiştir.

Tablo 4.5. BB84'te baz eşleşmesi ve elenmiş anahtarın oluşumu

Aşama	**1**	**2**	**3**	**4**	**5**
Alice Baz	+	×	×	×	+
Bob Baz	+	+	+	×	×
Eşleşme	✔	✘	✘	✔	✘
Elenen Bitler	✔	-	-	✔	-
Sadece eşleşenler tutulur	Sadece eşleşenler tutulur	Sadece eşleşenler tutulur	Sadece eşleşenler tutulur	Sadece eşleşenler tutulur	Sadece eşleşenler tutulur

Alice, her bir biti seçtiği baza göre bir foton durumuna dönüştürür. Bu aşamada fotonların tekil olması kritiktir; zira zayıflatılmış lazer darbeleri kullanıldığında birden fazla fotonun gönderilmesi PNS saldırılarına zemin hazırlayabilir.

Bob'un ölçüm stratejisi Alice'in baz seçiminden tamamen bağımsızdır. Bob, gelen her foton için rastgele bir baz seçer; doğru baz seçildiğinde biti doğru olarak elde eder, yanlış baz seçildiğinde ise sonuç 0 ile 1 arasında eşit olasılıkla dağılır ve orijinal durum geri dönüşsüz biçimde bozulur (Pirandola vd., 2020).

4.6.2.2 Klasik Veri İşleme Aşaması (Protokol Katmanı)

Kuantum iletimi bittikten sonra, taraflar klasik kanal üzerinden ham veriyi işleyerek nihai anahtara ulaşır.

Alice ve Bob, klasik (ancak kimliği doğrulanmış) bir kanal üzerinden birbirlerine sadece kullandıkları baz listelerini (b ve b′) gönderirler.

Alice ve Bob, bazların uyuşmadığı tüm pozisyonları eler. İstatistiksel olarak başlangıçtaki bit dizisinin yaklaşık yarısı atılır ve geriye kalan dizi "elenmiş anahtar" (sifted key) olarak adlandırılır.

BB84'ün tüm işlem adımları Tablo 4.6'da özetlenmiştir.

Tablo 4.6. BB84 operasyonel adımlarının özeti

Adım	İşlem Tipi	Paylaşılan Veri	Amaç
İletim	Kuantum	Polarize Fotonlar	Qubit transferi
Sifting	Klasik	Baz İsimleri (+, x)	Uyumsuz ölçümleri ayıklama
Tahmin	Klasik	Bit Değerlerinin %5-10'u	Dinleyici (Eve) tespiti
Düzeltme	Klasik	Parite Bitleri	Kanal gürültüsünü giderme
Hashleme	Algoritmik	Hiçbiri	Eve'in bilgisini sıfırlama

4.6.2.3 Hata Tahmini ve QBER Hesabı

Gerçek dünyadaki hiçbir kanal mükemmel değildir. Fiberdeki sönümleme, dedektör gürültüsü veya bir dinleyicinin (Eve) varlığı hatalara neden olur.

Alice ve Bob, elenmiş anahtarın rastgele seçilen küçük bir alt kümesini açıkça karşılaştırarak kuantum bit hata oranını hesaplar. QBER, Denklem (4.3)'de gösterildiği gibi test edilen bitler içindeki hatalı bit oranı olarak tanımlanır.

$$QBER = N_{hata} / N_{test} \quad (4.3)$$

QBER değeri belirli bir eşik değerini aştığında sistemde dinleme ya da aşırı kanal gürültüsü bulunduğu kabul edilir. Uygulamada sıklıkla kullanılan yaklaşık %11 eşiği asimptotik güvenlik analizleri için verilen tipik bir sınırdır; sonlu anahtar uzunluklarında kabul edilebilir eşik, güvenlik parametresi ε, örnekleme oranı ve hata düzeltme verimliliğine bağlı olarak farklılaşabilir (Gisin vd., 2002; Shor ve Preskill, 2000).

4.6.2.4 Hata Düzeltme ve Gizlilik Güçlendirme

Eğer hata oranı kabul edilebilir düzeydeyse, karşılaştırılmayan bitler üzerinden şu işlemler yapılır:

Bilgi uzlaştırma aşamasında Cascade, Winnow veya LDPC tabanlı yöntemlerle Alice ve Bob'un elindeki diziler eşitlenir. Ardından gizlilik güçlendirme uygulanarak Eve'in elde etmiş olabileceği kısmi bilgi evrensel hash fonksiyonları yardımıyla ihmal edilebilir düzeye indirilir (Wilde, 2013).

Bu son işlem adımlarının güvenlik bağlamı Tablo 4.7'de özetlenmiştir.

Tablo 4.7. BB84'te güvenlik ve işleme parametrelerinin özeti

Aşama	Temel Risk / Amaç	Kullanılan Teknik	Kritik Sınır
Kuantum Kanalı	Intercept-Resend Saldırısı	No-Cloning ve Ölçüm Etkisi	QBER < %11
Reconciliation	İletim Hatalarını Giderme	Cascade / LDPC Kodları	Minimum sızıntı
Privacy Amplif.	Eve'in Kısmi Bilgisini Yok Etme	Universal Hashing	Koşulsuz Güvenlik

4.6.3 Güvenlik Kontrolü ve Eve Etkisi Analizi

BB84 protokolünün güvenliği kuantum mekaniğinin fiziksel yasalarına dayanır; özellikle no-cloning teoremi ve ölçüm bozunumu ilkesi bu güvenliğin temelini oluşturur (Bennett ve Brassard, 1984).

4.6.3.1 Klonlamama Teoremi ve Pasif Dinleme İmkânsızlığı

Klasik iletişimde bir sinyal, aradaki bir dinleyici tarafından kopyalanıp aslına zarar vermeden okunabilir. Ancak kuantum dünyasında, "bilinmeyen bir kuantum durumunun (qubit) mükemmel bir kopyasını oluşturmak imkânsızdır" (Wilde, 2013). Bu durum, bir dinleyicinin (Eve) fotonu kopyalayıp Alice'e çaktırmadan Bob'a gönderemeyeceği anlamına gelir.

4.6.3.2 Intercept-Resend Saldırısı

Eve'in uygulayabileceği en temel saldırı stratejisi, Alice'ten gelen fotonu ölçmek ve elde ettiği sonuca göre yeni bir foton üretip Bob'a iletmektir. Ancak bu süreçte Eve ciddi bir istatistiksel riskle karşı karşıyadır:

Eve, fotonun hangi bazda hazırlandığını bilmediği için rastgele bir baz seçmek zorundadır. Doğru baz seçme olasılığı %50'dir; yanlış baz seçildiğinde ise kuantum durumunun çökmesi ölçülebilir hata üretir (Gisin vd., 2002).

4.6.3.3 Hata Tanımlama ve Eşik Değeri

Eve'in müdahalesi, Alice ve Bob'un bazları uyuşsa bile Bob'un yanlış sonuç almasına neden olur. En basit yakala-tekrar gönder (intercept-resend) senaryosunda Eve her fotona müdahale ederse Bob'un hata alma olasılığı yaklaşık %25 olur. Daha karmaşık kolektif veya koherent saldırılar için QBER analizi ayrıca güvenlik kanıtı ve saldırı modeline göre değerlendirilmelidir.

Bu nedenle BB84'te güvenlik, yalnızca teorik bir varsayım değil; Alice ve Bob tarafından hesaplanan QBER değeri üzerinden pratik olarak sınanabilen istatistiksel bir özelliktir.

4.6.4 Anahtar Oluşturma Süreci

Güvenlik kontrolünden geçen "Elenmiş Anahtar" (Sifted Key) henüz doğrudan kriptografik amaçlarla kullanılamaz. Bu aşamada uygulanan post-processing adımları, anahtarı mükemmel hale getirir.

4.6.4.1 Bilgi Uzlaştırma

Alice ve Bob'un ellerindeki diziler, kuantum kanalındaki gürültü nedeniyle küçük farklılıklar içerebilir. Bu hataları gidermek için klasik hata düzeltme protokolleri kullanılır:

Cascade protokolü etkileşimli parite kontrolleriyle hataları düzeltirken, LDPC tabanlı yaklaşımlar daha yüksek verim ve daha düşük sızıntı avantajı sunar.

4.6.4.2 Gizlilik Güçlendirme

E91 Protokolü: Dolanıklığın Gücü

"God does not play dice with the universe."

4.6.5 BB84 Örnek Akış Tablosu

Protokolün sekiz bitlik örnek bir kesiti Tablo 4.8'de verilmiştir. Tablo, Alice ve Bob'un baz seçimleri uyuştuğunda hangi bitlerin elenmiş anahtara girdiğini somut biçimde göstermektedir.

Tablo 4.8. BB84 protokolünün sekiz bitlik örnek akışı

Adım	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Alice'in Rastgele Biti	0	1	0	1	1	0	0	1
Alice'in Bazı	⊕	⊗	⊕	⊕	⊗	⊗	⊕	⊗
Fotonun Durumu	→	↗	→	↑	↗	↖	→	↗
Bob'un Baz Seçimi	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊕
Bob'un Ölçümü	0	0/1	1/0	1	1	0	0	0/1

Adım	1	2	3	4	5	6	7	8
Baz Uyumu (Sifting)	EVET	HAYIR	HAYIR	EVET	EVET	EVET	EVET	HAYIR
Sifted Key	0	-	-	1	1	0	0	-

4.7 E91 Protokolü: Dolanıklığın Gücü, Bell Eşitsizlikleri ve Cihaz Bağımsız Güvenlik

4.7.1 Önceki Protokollerin Ötesinde: Neden E91?

BB84 ve B92'de güvenliğin temeli, hazırlama cihazlarının gizliliğine dayanır. Bu durum, yan kanal saldırıları ve dedektör kör etme gibi pratik güvenlik açıklarına zemin hazırlar (Gisin vd., 2002).

Ekert (1991) tamamen farklı bir yaklaşım önerdi: güvenliği Bell eşitsizliklerinin kuantum ihlalinden türetmek. Bu yaklaşımda herhangi bir gizli dinleyicinin varlığı, ölçüm korelasyonlarını bozarak CHSH parametresinin klasik sınırın altına düşmesine yol açar ve dinleyici tespit edilir.

BB84/B92 güvenliği ağırlıklı olarak hazırlama gizliliği ve no-cloning ilkesi üzerinden kurarken, E91 güvenliği Bell eşitsizliklerinin kuantum ihlalinden türetir. Bu ayrım, protokolün cihaz bağımsız güvenliğe açılan kapı olmasını sağlamaktadır (Ekert, 1991).

4.7.2 Charlie ve Kaynak Sorunu

Charlie, EPR çiftleri üretir ve her çiftin bir fotonunu Alice'e, diğerini Bob'a gönderir. Kritik nokta şudur: protokol Charlie'ye herhangi bir güven gerektirmez. Alice ve Bob, CHSH testi yoluyla dolanıklığı istatistiksel olarak doğrularlar (Ekert, 1991).

Charlie'nin güvenilirlik durumu protokolün davranışını doğrudan etkiler. Bu olası senaryolar Tablo 4.9'da özetlenmiştir.

Tablo 4.9. Charlie'nin güven durumuna göre protokol davranışı

Senaryo	Durum	Protokol Davranışı
Senaryo 1	Charlie tamamen güvenilir	CHSH gereksizdir; protokol çalışır
Senaryo 2	Charlie güvenilmez ama meşru kaynak	CHSH ihlali dolanıklığı doğrular
Senaryo 3	Charlie = Eve (tam düşman kaynak)	Dolanıklık yok → CHSH ihlali yok → iptal

Senaryo 3, cihaz bağımsız QKD (DI-QKD) araştırmalarının temel motivasyonunu oluşturur (Gisin vd., 2002).

4.7.3 Bell Eşitsizliği ve CHSH Testi

4.7.3.1 Einstein–Podolsky–Rosen Paradoksu

Einstein ve arkadaşları (1935) kuantum mekaniğinin tamamlanmamış bir teori olduğunu öne sürdü. Argümanları, uzak parçacıklar arasındaki korelasyonların yerel gizli değişkenler (LHV) ile açıklanabileceğine dayanıyordu. Bell (1964) bu görüşü deneysel olarak test edilebilir hale getirdi.

4.7.3.2 Bell'in Orijinal Eşitsizliği

Korelasyon fonksiyonu. ±1 sonuç veren ölçüm operatörleri A(a) ve B(b) için iki-taraf korelasyonu aşağıdaki gibi tanımlanır:

$$E(a, b) = \langle A(a) \cdot B(b) \rangle \tag{4.4}$$

Bell (1964), Denklem (4.4) ile tanımlanan korelasyonlar için LHV teorilerinin bir üst sınırı aşamayacağını kanıtladı:

$$|E(a,b) - E(a,b')| + |E(a',b) + E(a',b')| \leq 2 \tag{4.5}$$

4.7.3.3 CHSH Parametresi S

Clauser ve arkadaşları (1969) dört yönelim çifti için korelasyonları Denklem (4.6)'teki S parametresinde birleştirdi:

$$S = E(a,b) - E(a,b') + E(a',b) + E(a',b') \tag{4.6}$$

Denklem (4.5)'nin CHSH biçimi, Denklem (4.7)'te verilen klasik sınırı ortaya koyar:

$$|S| \leq 2 \tag{4.7}$$

Kuantum mekaniği ise Denklem (4.7)'teki klasik sınırı aşabilir. Tsirelson (1980) maksimum kuantum değerini, Denklem (4.8)'te gösterildiği üzere belirledi:

$$|S| \leq 2\sqrt{2} \approx 2.828 \tag{4.8}$$

Singlet durumu için korelasyon E(a,b) = −cos(θ_ab) biçimindedir. 22.5° aralıklı yönelimler seçildiğinde CHSH parametresi 2√2 değerine ulaşır ve böylece kuantum mekaniksel sınır elde edilir.

4.7.3.4 CHSH'nin E91'de Kullanımı

Ekert'in (1991) tasarımında Alice ve Bob üçer yönelim seçeneği kullanır. Bu ölçüm ayarları Tablo 4.10'da verilmiştir.

Tablo 4.10. E91 protokolünde ölçüm yönelim seçenekleri

Taraf	5.1 Yönelim	5.2 Yönelim	5.3 Yönelim
Alice	$a_1 = 0°$	$a_2 = 45°$	$a_3 = 90°$
Bob	$b_1 = 22.5°$	$b_2 = 67.5°$	$b_3 = 112.5°$

|S| > 2 olduğunda Bell ihlalinin gözlendiği ve dolanıklığın varlığının doğrulandığı kabul edilir; |S| ≤ 2 durumunda ise korelasyonlar yerel gizli değişken modeliyle açıklanabilir ve protokol iptal edilir.

4.7.4 E91 Protokolü Adım Adım

4.7.4.1 Kullanılan Kuantum Durumu

E91'de Charlie foton çiftlerini singlet durumunda hazırlar (Ekert, 1991), Denklem (4.9):

$$|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle) \quad \textbf{(4.9)}$$

$|\Psi^-\rangle$ iki kritik özelliğe sahiptir. Birincisi, tam anticorrelation özelliğidir; aynı yönelimde ölçüldüklerinde her zaman zıt sonuç verirler. İkincisi, döndürme değişmezliğidir; her referans çerçevesinde aynı formda kalır.

4.7.4.2 Protokol Akışı

Charlie, SPDC yöntemiyle Denklem (4.9)'daki $|\Psi^-\rangle$ durumunda foton çiftleri üretir (Kwiat vd., 1995). Her çiftten bir foton Alice'e, diğeri Bob'a iletilir.

Alice ve Bob, Tablo 4.10'daki yönelimlerden birini bağımsız rastgele seçerek ±1 sonuçlu polarizasyon ölçümü yapar. Rastgelelik bir QRNG ile sağlanmalıdır.

Alice ve Bob, doğrulanmış açık kanal üzerinden yalnızca yönelimlerini açıklar, sonuçlarını açıklamaz. Bu karşılaştırma, ölçümlerin anahtar grubuna mu yoksa CHSH grubuna mı girdiğini belirler.

CHSH grubundaki ölçüm çiftlerinden korelasyon fonksiyonları hesaplanır (Clauser vd., 1969), Denklem (4.10):

$$E(a_i, b_j) = (N^{++} + N^{--} - N^{+-} - N^{-+}) / N_toplam \quad (4.10)$$

S parametresi, Denklem (4.11)'de gösterildiği üzere bu korelasyonlardan elde edilir:

$$S = E(a_1,b_1) - E(a_1,b_2) + E(a_2,b_1) + E(a_2,b_2) \quad (4.11)$$

Denklem (4.7)'teki klasik sınırın, Denklem (4.11) ile hesaplanan S değeri tarafından istatistiksel olarak anlamlı biçimde aşıldığı doğrulanırsa protokol devam eder.

Yönelimlerin örtüştüğü Q grubundaki ölçümler ham anahtar bitlerini oluşturur. Denklem (4.9)'daki singlet'in anticorrelation özelliği nedeniyle Bob bitleri terse çevirerek Alice ile aynı diziyi elde eder. Hata düzeltme ve gizlilik yükseltmesi ardından nihai anahtar çıkarılır (Gisin vd., 2002).

Bu karşılaştırma Tablo 4.11'de özetlenmektedir.

Tablo 4.11. E91 protokolü: adım adım özet

Adım	Taraf	İşlem
1	Charlie	SPDC ile $\|\Psi^-\rangle$ (Dkl. 4.6) dolanık foton çiftleri üretir
2	Charlie → Alice, Bob	Her çiftten birer foton iki tarafa gönderilir
3	Alice ve Bob	Bağımsız rastgele yönelim seçimi (Tablo 3.2) ve ölçüm
4	Açık kanal	Yalnızca yönelimler açıklanır
5	Alice ve Bob	S (Dkl. 4.8) hesaplanır; $\|S\| > 2$ (Dkl. 4.4) doğrulanır
6	Alice ve Bob	Eşleşen yönelimlerden ham anahtar çıkarılır
7	Alice ve Bob	Hata düzeltme + gizlilik yükseltmesi → nihai anahtar

4.7.5 Dolanık Foton Üretimi

E91'in fiziksel gerçekleştiriminin kalbi, Denklem (4.9)'daki $|\Psi^-\rangle$ durumunun deneysel olarak üretilmesidir (Kwiat vd., 1995; Gisin vd., 2002).

4.7.5.1 Kendiliğinden Parametrik Aşağı Dönüşüm (SPDC)

SPDC, dolanık foton çiftlerinin üretiminde bugün en yaygın kullanılan yöntemdir (Kwiat vd., 1995). Doğrusal olmayan bir BBO kristalinde pompa fotonu iki alt-frekanslı fotona dönüşür; bu dönüşüm enerji korunumu (Denklem 4.12) ve momentum korunumu (Denklem 4.13) koşullarına tabidir:

$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_i \tag{4.12}$$

$$\hbar k_p = \hbar k_s + \hbar k_i \tag{4.13}$$

Burada p pompa, s sinyal, i boşta fotonlarını gösterir. Denklem (4.13)'daki faz eşleşmesi koşulunun sağlanması, dolanıklık görünürlüğü açısından kritiktir.

Fotonlar dik polarizasyonlarda üretilir ve iki konik ışın demetinin kesişiminde Denklem (4.9)'daki Bell durumu doğrudan elde edilir (Kwiat vd., 1995):

$$|\Psi\pm\rangle = (1/\sqrt{2})(|HV\rangle \pm |VH\rangle) \tag{4.14}$$

4.7.5.2 Dört-Dalga Karışımı (FWM)

Silikon nitrür ya da silika fiber tabanlı sistemlerde dört-dalga karışımı mekanizması kullanılır:

$$\omega_{p1} + \omega_{p2} = \omega_s + \omega_i \tag{4.15}$$

Denklem (4.15)'deki FWM, mevcut fiber altyapısıyla entegrasyon açısından avantajlıdır, ancak Raman saçılmasından kaynaklanan arka plan gürültüsü bir dezavantaj oluşturur.

4.7.5.3 Dolanıklık Kalitesinin Ölçümü

Üretilen çiftlerin kalitesini değerlendirmede kullanılan temel metrikler Tablo 4.12'de sunulmuştur.

Tablo 4.12. Dolanık foton kaynakları için kalite metrikleri

Metrik	Tanım/Formül	Eşik / Açıklama
Görünürlük (V)	`V = (C_max − C_min)/(C_max + C_min)`	V > 0.71 (Dkl. 4.4 ihlali için gerekli)
CAR oranı	Koinsidans / Rastgele koinsidans	Çift üretim verimi; >100 iyi

Metrik	Tanım/Formül	Eşik / Açıklama
Yoğunluk matrisi tomografisi	ρ tam durum karakterizasyonu	Tüm Bell durumları analiz edilir
Concurrence C(ρ)	C ∈ (Nielsen ve Chuang, 2010)	C = 1 maksimum dolanıklık

Çoklu çift emisyonu, dedektör verimsizliği ve optik yol kayıpları görünürlüğü düşürerek QBER'i artırabilir; bu da CHSH parametresinin kuantum sınırından uzaklaşmasına neden olur (Gisin vd., 2002).

4.7.6 Gerçek Uygulamalar

4.7.6.1 Boşluksuz Bell Deneyleri

Bell eşitsizliğinin gerçek anlamda ihlal edildiğini kanıtlamak, Tablo 4.13'te özetlenen iki tarihsel boşluğun kapatılmasını gerektirmiştir.

Tablo 4.13. Bell testi boşlukları ve kritik deneyler

Boşluk Türü	Gereksinim	Kritik Deney
Yerellik boşluğu	400 m ayrık foton çiftleri	Weihs vd. (1998) - Innsbruck
Dedektör verimliliği boşluğu	%97+ verimli dedektörler	Rowe vd. (2001) - iyon tuzakları
Her ikisi birden	5.1.3 km - elektron spin çiftleri	Hensen vd. (2015) - Delft

Hensen ve arkadaşları (2015), Tablo 4.13'teki her iki boşluğu aynı anda kapatan ilk boşluksuz Bell deneyini gerçekleştirdi. Elde edilen S değeri Denklem (4.7)'teki klasik sınırı 2,42 standart sapmayla aşmaktadır.

4.7.6.2 Micius Uydusu

Yin ve arkadaşları (2017) 1203 km mesafede yer-uydu dolanıklık dağıtımı gerçekleştirdi ve S = 2.37 ± 0.09 değerini ölçerek Denklem (4.7)'teki sınırı açıkça ihlal etti. Pan ve arkadaşları (2020) ise iki yer istasyonu arasında 1120 km mesafede uydu köprüsü üzerinden dolanık QKD demonstrasyonu yaptı.

4.7.6.3 DI-QKD ve MDI-QKD

Nadlinger ve arkadaşları (2022), Bell teoremi ile sertifikalanan ilk DI-QKD demonstrasyonunu gerçekleştirdi. Güvenlik doğrudan Denklem (4.6) ile ölçülen S parametresine dayanmaktadır. Lo ve arkadaşları (2012) ise dedektör güvensizliğini tam olarak bertaraf eden MDI-QKD protokolünü önerdi.

Güncel protokol karşılaştırması Tablo 4.14'te sunulmuştur.

Tablo 4.14. QKD protokollerinin karşılaştırması

Protokol	Anahtar Hızı	Cihaz Bağımsızlık	Olgunluk
BB84 (standart)	~10 Mbit/s (100 km)	Hayır	Yüksek (ticari)
MDI-QKD (Lo vd., 2012)	~kbit/s (100 km)	Kısmen	Orta
E91 / Bell tabanlı	~kbit/s, Mbit/s	Evet (kanal)	Orta
DI-QKD (Nadlinger vd., 2022)	~bit/s	Tam	Araştırma

4.7.7 Güvenlik Analizi

E91'in güvenlik kanıtı üç katmanlı bir yapıya sahiptir: no-signaling prensibi, Denklem (4.11) ile hesaplanan CHSH testi ve entanglement'ın monogamy özelliği (Gisin vd., 2002). Tablo 4.15 başlıca saldırı tiplerini ve E91'in bu saldırılara karşı yanıtını özetlemektedir.

Tablo 4.15. E91 protokolüne yönelik saldırı modelleri

Saldırı Türü	Mekanizma	E91 Karşı Yanıtı
Intercept-Resend	Eve fotonu ölçer, yenisini gönderir	S (Dkl. 4.8) düşer; tespit edilir
Entangle-Measure	Eve üçüncü fotonla dolanıklık kurar	Monogamy → korelasyonlar bozulur
Yan kanal (Trojan-horse)	Eve cihaza sinyaller gönderir	DI-QKD bu saldırıya karşı dirençlidir
PNS saldırısı	Çok-çift emisyonundan yararlanma	Düşük pompa gücü veya DI-QKD ile azaltılır

Özetle E91, güvenliği doğrudan dolanıklığın istatistiksel imzasından türettiği için BB84'e kıyasla daha güçlü bir doğrulama çerçevesi sunar; bununla birlikte düşük anahtar hızı ve deneysel karmaşıklık gibi pratik sınırlılıklar halen araştırma gündeminde yer almaktadır.

BÖLÜM 5

NIST Standartları ve Kuantum Sonrası Kriptografi: Kurumsal Çerçeve, Tehdit Analizi ve Standardizasyon Süreci

5.1 Giriş

Dijital dünyanın hızla genişleyen ekosisteminde kriptografik güvenlik, bilgi altyapısının temel direğini oluşturmaktadır. Günümüzde internet trafiğinin şifrelenmesinden finansal işlemlerin kimlik doğrulamasına, devlet belgelerinin imzalanmasından sağlık kayıtlarının korunmasına uzanan geniş bir yelpazede sayısız kritik işlev, RSA, Elliptic Curve Cryptography (ECC) ve Diffie-Hellman protokolleri gibi matematiksel güçlüğe dayalı asimetrik kriptosistemler üzerine inşa edilmiştir. Bu sistemlerin güvenlik garantileri, büyük tamsayıları asal çarpanlarına ayırmanın ya da ayrık logaritma problemini çözmenin hesaplamalı açıdan son derece güç olduğu temel varsayımına dayanmaktadır (Rivest vd., 1978; ElGamal, 1985).

Bu köklü güvenlik paradigması, teorik fizik ve bilgisayar biliminin kesişiminden doğan kuantum bilişim alanındaki gelişmelerle ciddi bir tehdit altına girmiştir. Peter Shor'un 1994 yılında ortaya koyduğu polinom zamanlı kuantum algoritması (Shor, 1994) ve Lov Grover'ın 1996 yılında geliştirdiği kuantum arama algoritması (Grover, 1996), mevcut kriptografik standartların temel matematiksel varsayımlarını sırasıyla yıkıcı ve aşındırıcı biçimde hedef almaktadır. Bu olgular kriptografi camiasını yeni bir paradigma değişimine zorlamış; kuantum bilgisayarlara karşı dirençli kriptografik sistemlerin araştırılması ve standartlaştırılması, on yılı aşkın bir süreye yayılan küresel bir çabanın konusu haline gelmiştir.

Bu bölüm, söz konusu dönüşümün merkezinde yer alan National Institute of Standards and Technology (NIST)'in kurumsal kimliğini, standart belirleme metodolojisini ve Kuantum Sonrası Kriptografi (Post-Quantum Cryptography, PQC) standartlaştırma sürecini kapsamlı biçimde incelemeyi amaçlamaktadır. Bölüm boyunca NIST'in hangi yasal yetki ve metodolojik ilkelerle faaliyet gösterdiği; kuantum tehdidinin kriptografik boyutlarının neler olduğu ve teorik tehdidin pratik tehlikeye ne zaman dönüşeceği; NIST PQC standardizasyon sürecinin nasıl yürütüldüğü ile hangi algoritmaların nihai standartlar olarak seçildiği; ve son olarak bu standartların evrensel güvenlik mimarisine nasıl entegre edilmesi gerektiği ele alınacaktır.

5.2 NIST'in Kurumsal Kimliği, Yasal Çerçevesi ve Yayın Hiyerarşisi

5.2.1 Tarihsel Gelişim ve Yasal Dayanak

National Institute of Standards and Technology (NIST), 1901 yılında "National Bureau of Standards" (NBS) adıyla kurulan ve 1988 yılında Omnibus Trade and Competitiveness Act ile yeniden yapılandırılarak bugünkü adını alan federal bir araştırma ve standartlar kurumudur (U.S. House of Representatives, 2024). ABD Ticaret Bakanlığı'na (Department of Commerce) bağlı bu kurum, 15 U.S.C. § 271 maddesinde düzenlenen NIST Yasası çerçevesinde "ölçüm bilimini, standartları ve teknolojiyi geliştirerek ABD yenilikçiliğini ve endüstriyel rekabet gücünü artırmak, ekonomik güvenliği güçlendirmek ve yaşam kalitesini yükseltmek" misyonuyla faaliyet göstermektedir (NIST, 2023a). Yaklaşık 3.400 çalışanı ve yıllık 1,5 milyar USD'yi aşan bütçesiyle NIST, küresel ölçekte standart belirleme alanında en etkili kurumlardan biri konumundadır.

NIST'in düzenleyici olmayan (non-regulatory) bir kurum olduğu kritik bir ayrımı ifade etmektedir. NIST, yasal bağlayıcılığı olan düzenlemeler (regulations) yayınlamaz; bunun yerine teknik standartlar, kılavuzlar ve referans çerçeveleri geliştirir. Bu standartlar, diğer düzenleyici kurumlar ya da Federal Bilgi Güvenliği Modernizasyon Kanunu (Federal Information Security Modernization Act - FISMA) gibi federal yasalar aracılığıyla bağlayıcı hale gelebilir. Örneğin FISMA kapsamında federal kurumlar, NIST SP 800-53'teki güvenlik kontrollerine uyum sağlamakla yükümlüdür (NIST, 2020a). Özel sektör için ise NIST standartları gönüllülük esaslı olmakla birlikte, finans, enerji ve sağlık sektörlerinde düzenleyici kurumlar tarafından "en iyi uygulama" referansı olarak giderek daha fazla kullanılmaktadır (U.S. Congress, 2018).

5.2.2 NIST Yayın Türleri ve Hiyerarşisi

NIST'in kriptografi ve siber güvenlik alanındaki yayınları, farklı bağlayıcılık düzeylerine sahip hiyerarşik bir yapı içinde düzenlenmektedir. Bu hiyerarşiyi kavramak, akademik ve pratik değerlendirmeler için temel bir gerekliliktir. Tablo 5.1'de NIST'in siber güvenlik yayın türleri ve hiyerarşisi özetlenmektedir.

Tablo 5.1. NIST Siber Güvenlik Yayın Türleri ve Hiyerarşisi

Yayın Turu	Amac	Hedef Kitle	Bağlayıcılık	Ornek
FIPS (Federal Inf. Proc. Std.)	Federal sistemler icin zorunlu teknik standartlar	ABD Federal kurumlar ve yukleniciler	Federal kurumlar icin ZORUNLU (FISMA)	FIPS 140-3 (Kriptografik Modüller), FIPS 203 (ML-KEM)
NIST SP 800 Serisi (Special Publication)	Bilgi guvenligi konularinda ayrintili kilavuz	Federal kurumlar, ozel sektor, kamu	Tavsiye; FISMA kapsaminda referans alinir	SP 800-53 (Güvenlik Kontrolleri), SP 800-171 (CUI)
NISTIR (Interagency Report)	Araştırma bulgulari, on çalışma, sektor analizleri	Araştırmacı ve teknik uzmanlar	Bilgilendirme amacli; baglayici degil	NISTIR 8105 (PQC On Raporu), NISTIR 8413 (PQC 3. Tur)
NIST CSF (Cybersecurity Framework)	Kurumsal siber güvenlik programlari icin ust duzey çerçeve	Tum sektorler ve olcekler	Gonulluluk esasli; kritik altyapi icin tesvik edilir	CSF 2.0 (Govern, Identify, Protect, Detect, Respond, Recover)
NIST SP 1800 Serisi (Cybersecurity Practice Guide)	Pratik uygulama senaryolari ve referans mimariler	Güvenlik pratisyenleri ve mimarlar	Tavsiye niteliginde uygulama rehberi	SP 1800-38 (PQC Geçiş Rehberi)

Not. FIPS: Federal Information Processing Standard; SP: Special Publication; NISTIR: NIST Interagency Report; CSF: Cybersecurity Framework; FISMA: Federal Information Security Modernization Act; CUI: Controlled Unclassified Information. NIST (2006, 2020a, 2020b, 2024a) temel alınarak yazarlar tarafından derlenmiştir.

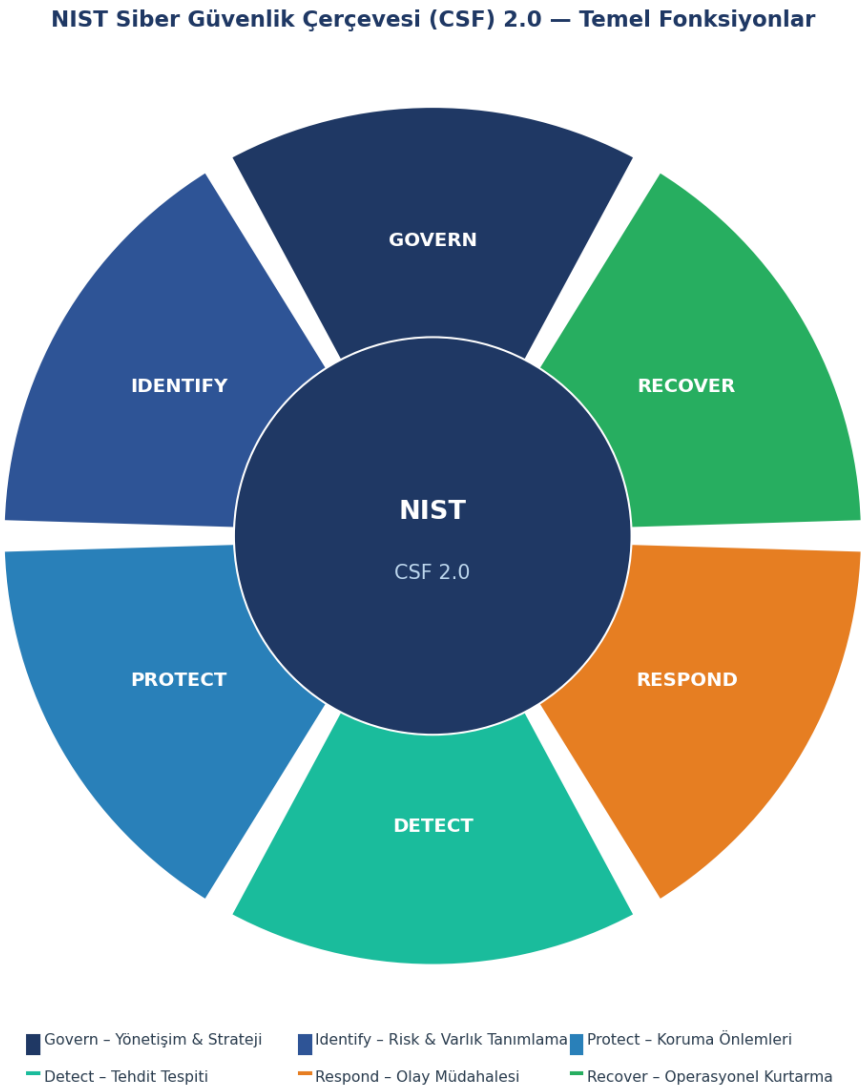
5.3 NIST Siber Güvenlik Çerçevesi (CSF) 2.0

5.3.1 Çerçeve Mimarisi ve Temel Bileşenleri

NIST Siber Güvenlik Çerçevesi (Cybersecurity Framework, CSF) 2.0, Şubat 2024'te yayımlanan ve kurumların siber güvenlik risklerini yönetmelerine yardımcı olmak üzere tasarlanmış kapsamlı bir rehber sistemdir (NIST, 2024a). Çerçeve, kuruluşun büyüklüğünden, sektöründen veya teknolojik olgunluk seviyesinden bağımsız olarak uygulanabilecek şekilde tasarlanmıştır. CSF 2.0, orijinal 2014 sürümüne kıyasla önemli bir yenilik barındırmaktadır: tedarik zinciri risk yönetimini ve yönetişim fonksiyonunu ön

plana çıkaran altıncı fonksiyon olan "Govern"'ın eklenmesi, çerçevenin toplam yönetişim perspektifini derinleştirmiştir (NIST, 2024a).

CSF 2.0 üç ana bileşenden oluşmaktadır. Birinci bileşen olan CSF Çekirdeği (Core), Fonksiyonlar, Kategoriler ve Alt Kategorilerden oluşan hiyerarşik bir yapıdır ve sektör ile teknoloji tarafsız tutularak kuruluşlara kendi bağlamlarına uyum esnekliği tanınmıştır. İkinci bileşen olan Organizasyonel Profiller, kuruluşun mevcut veya hedef siber güvenlik duruşunu Çekirdek çıktıları üzerinden tanımlamasını sağlar. Üçüncü bileşen Katmanlar (Tiers) ise risk yönetimi uygulamalarının titizliğini "Kısmi" (Tier 1)'den "Uyarlanabilir" (Tier 4)'a uzanan bir skalada karakterize eder (NIST, 2024a). Bu altı temel fonksiyonun birbirleriyle ilişkisi Şekil 5.1'de gösterilmektedir.



Şekil 5.1. NIST Siber Güvenlik Çerçevesi (CSF) 2.0 - Alti Temel Fonksiyon. Çerçeve, merkezi yönetişim (Govern) fonksiyonu etrafinda duzenlenmis alti birbirine bagli bilesendir. NIST (2024a) temel alınarak hazirlanmiştir.

5.3.2 CSF Core Fonksiyonları

CSF Core, siber güvenlik çıktılarını altı temel fonksiyon altında düzenlemektedir. Bu fonksiyonlar uygulama önceliğini değil, kurumsal güvenlik olgunluğunu temsil eden sürekli döngüsel süreçleri ifade etmektedir (NIST, 2024a). Bu fonksiyonlar, alt kategorileri ve örnek kontrolleriyle birlikte Tablo 5.2'de sunulmaktadır.

Tablo 5.2. NIST CSF 2.0 Fonksiyonları, Alt Kategorileri ve Ornek Kontroller

Fonksiyon	Amac	Temel Alt Kategoriler	Ornek SP 800-53 Kontrolleri
GOVERN (GV) [YENİ - 2024]	Risk yönetimi stratejisi oluşturma, iletme ve izleme	Kurumsal baglam, risk toleransi, politika, tedarik zinciri	PM-9 (Risk Yön. Stratejisi), SA-12 (Tedarik Zinciri)
IDENTIFY (ID)	Sistem varliklari ve risklerin tanimlanmasi	Varlik yönetimi, risk değerlendirme, iyilestirme	CM-8 (Varlik Envanteri), RA-3 (Risk Değerlendirme)
PROTECT (PR)	Kritik hizmetlerin korunmasi icin onlemler	Kimlik yönetimi, veri güvenligi, platform güvenligi	AC-2 (Hesap Yönetimi), SC-28 (Veri Sifrelemesi)
DETECT (DE)	Olayların ve anomalilerin zamaninda tespiti	Sürekli izleme, anomali tespiti, olay analizi	AU-6 (Denetim Analizi), SI-4 (Sistem Izleme)
RESPOND (RS)	Tespit edilen olaylara müdahale	Müdahale planlama, iletisim, etki sinirlama	IR-4 (Olay Islem), IR-6 (Olay Raporlama)
RECOVER (RC)	Etkilenen sistem ve operasyonlarin yeniden kurulmasi	Kurtarma planlama, altyapi onarimi, iletisim	CP-10 (Bilgi Sistemi Kurtarma), IR-8 (Olay Plani)

Not. SP: Special Publication. NIST (2020a, 2024a) temel alınarak yazarlar tarafından derlenmiştir.

CSF fonksiyonları birbirinden bağımsız değil, sürekli etkileşim halindedir: Govern aşamasında belirlenen risk toleransı tüm diğer fonksiyonların bağlamını şekillendirir; Identify'da tanımlanan varlıklar Protect'te korunur; Detect'teki erken uyarılar Respond ve Recover süreçlerini besler. NIST, özellikle CSF'nin yalnızca geleneksel BT ortamlarına değil; Nesnelerin İnterneti (IoT), operasyonel teknoloji (OT), bulut sistemleri ve yapay zekâ platformlarına da uygulanabileceğini vurgulamaktadır (NIST, 2024a). Bu kapsamlı yaklaşım, CSF'yi PQC geçiş planlaması için de önemli bir referans çerçevesi haline getirmektedir.

5.4 Akademik Çalışma ile Standart Araştırması Arasındaki Temel Farklar

Bir kriptografik algoritmanın akademik literatürde kabul görmesi ile NIST standardı olarak belgelenmesi arasında nitelik ve süre bakımından son derece önemli farklar bulunmaktadır. Akademik bir çalışma özgünlük ve yayınlanabilirlik kriterlerini karşılamayı önceliklendirirken, standart araştırması gerçek dünyada güvenilir, doğrulanmış ve uzun vadede savunulabilir teknolojiler üretmeyi hedeflemektedir (Chen vd., 2016). Bu ayrımın doktora araştırmacısı için kavranması, hem araştırma problemlerinin doğru konumlandırılması hem de sonuçların doğru yorumlanması açısından kritik önem taşımaktadır. Tablo 5.3'te bu iki yaklaşım arasındaki temel farklar karşılaştırmalı olarak sunulmaktadır.

Tablo 5.3. Akademik Çalışma ile NIST Standart Araştırması Karşılaştırması

Kriter	Akademik Çalışma	NIST Standart Araştırması
Birincil Hedef	Yeni yontem onerisi, teorik katki	Gercek dunya kullanimina hazir, guvenli teknoloji
Dogrulama	Simulasyon ve teorik kanit yeterli	Kapsamlı kriptanaliz, uygulama testi, peering
Sure	Tipik olarak 1-3 yil	Genellikle 8-15 yil
Kapsam	Belirli bir problem veya senaryo	Evrensel kullanimda tum tehdit senaryolari
Güvenlik Kanıtı	Reduksiyon kanıtı yeterli	Formal güvenlik kanıtı + aktif kriptanaliz
Donanım Gerekliliği	Yazilim prototipi yeterli	ARM, x86-64, IoT cihazlar, donanım hizlandirici
Topluluk Katılımı	Hakemli değerlendirme (peer review)	Kuresel kriptografi toplulugunun aktif katılımı

Kriter	Akademik Çalışma	NIST Standart Araştırması
Sonuc	Yayın, patent, tez	Resmi FIPS/SP yayını; kuresel referans

Not. Chen vd. (2016) ve NIST (2016) temel alınarak yazarlar tarafından derlenmiştir.

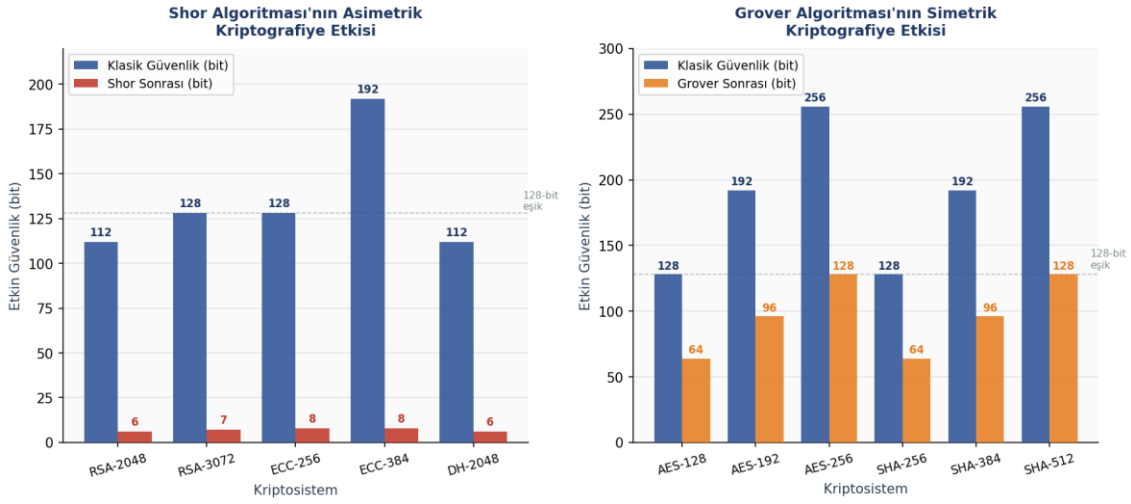
5.5 Kuantum Bilgisayarların Kriptografik Tehdit Analizi

5.5.1 Shor Algoritması: Asimetrik Kriptografinin Teorik Çöküşü

Peter Shor'un 1994 yılında Bell Laboratories'de geliştirdiği polinom zamanlı kuantum algoritması, kriptografi tarihinin en önemli teorik kırılma noktalarından birini temsil etmektedir (Shor, 1994). Algoritma, iki temel matematiksel problemi polinom zamanda çözebilmektedir: (1) tam sayı asal çarpanlarına ayırma ve (2) ayrık logaritma problemi. Bu iki problem, sırasıyla RSA kriptosisteminin ve Diffie-Hellman / ECC protokollerinin güvenlik temelini oluşturmaktadır.

Karmaşıklık kuramsal açıdan değerlendirildiğinde: n-bit bir sayının klasik en iyi bilinen algoritma olan General Number Field Sieve (GNFS) ile çarpanlarına ayrılması O(exp((64/9)^{1/3} · n^{1/3} · (log n)^{2/3})) karmaşıklığına sahipken, Shor algoritması aynı problemi yalnızca O(n^2 · log n · log log n) kuantum kapı işlemiyle çözmektedir (Shor, 1997). Bu asimptotik fark, 2048-bit RSA anahtarının kırılması için gereken zamanı klasik yöntemlerle "evrenin ömrü" mertebesinden güçlü bir kuantum bilgisayarda saatler mertebesine indirir.

Pratik gerçekleşme koşulları açısından: 2048-bit RSA için Shor algoritmasının yaklaşık 4.000 mantıksal qubite ihtiyaç duyduğu hesaplanmıştır (Roetteler vd., 2017). Hata düzeltmeli (fault-tolerant) fiziksek gerçekleşme için ise bu ihtiyaç milyonlarca fiziksel qubite karşılık gelmekte olup günümüz teknolojisi bu eşiğin henüz çok gerisindedir. 2024 itibarıyla en büyük mevcut sistemler 1.000-2.000 fiziksel qubit aralığındadır; ancak bu sistemler gürültülü, hata-düzeltme kapasitesinden yoksun NISQ (Noisy Intermediate-Scale Quantum) cihazlarıdır (National Academies, 2019). Shor ve Grover algoritmalarının kriptografik güvenlik üzerindeki etkisi Şekil 5.2'de karşılaştırmalı olarak gösterilmektedir.



Şekil 5.2. Shor ve Grover Algoritmalarının Kriptografik Güvenliğe Etkisi. Sol panel: Shor algoritması RSA ve ECC'nin güvenliğini neredeyse tamamen ortadan kaldirmaktadir. Sag panel: Grover algoritması simetrik sifrelemenin etkin güvenliğini yarim oraninda azaltmakta, ancak AES-256 kabul edilebilir düzeyde güvenli kalmaktadir. Shor (1997), Grover (1996) temel alınarak yazarlar tarafından uretilmiştir.

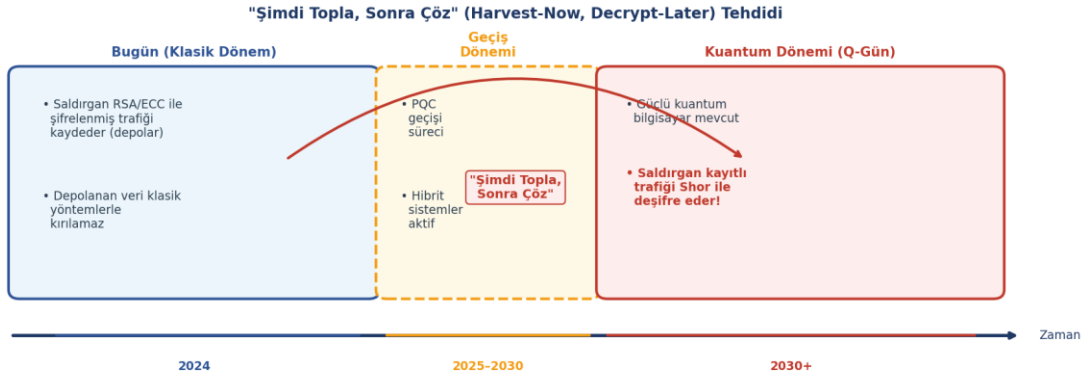
5.5.2 Grover Algoritması: Simetrik Kriptografiye Karekök Etkisi

Lov Grover'ın 1996 yılında geliştirdiği kuantum arama algoritması, N elemanlı sırasız bir veritabanında arama problemini O(√N) karmaşıklığında çözebilmektedir (Grover, 1996). Simetrik kriptografi bağlamındaki pratik etkisi, güvenlik parametresini etkin olarak yarıya indirmektir: AES-128 için 128-bit güvenlik seviyesi 64-bit eşdeğerine düşerken, AES-256 128-bit etkin güvenlik seviyesini korumaktadır. NIST, bu nedenle kuantum çağında en az 128-bit etkin güvenlik garantisi için minimum AES-256 ve SHA-384 kullanımını önermektedir (NIST, 2016).

Grover'ın etkisinin Shor'a kıyasla daha hafif değerlendirilmesinin temel nedeni, simetrik şifre ve karma fonksiyonlarının basit parametre artışıyla bu tehdide yanıt verebilmesidir. Bununla birlikte, paralel Grover saldırılarının teorik hız kazanımı tek kuantum bilgisayar senaryosunun çok altında kaldığına dair önemli analitik bulgular mevcuttur (Banegas ve Bernstein, 2017). Karma fonksiyonları ve HMAC protokollerinde Grover etkisinin güvenlik analizine dahil edilmesi, doktora düzeyinde araştırmalar için kritik bir metodolojik gerekliliktir.

5.5.3 "Şimdi Topla, Sonra Çöz" (Harvest-Now, Decrypt-Later) Tehdidi

Kuantum tehdidin pratikte şu an fiilen başlamış olduğunu gösteren en önemli argüman, "Harvest-Now, Decrypt-Later" (HNDL) stratejisidir. Bu saldırı modelinde tehdit aktörleri, güçlü bir kuantum bilgisayara sahip olmaksızın şu anda TLS, IPsec veya benzeri protokollerle şifrelenmiş ağ trafiğini depolamakta; ileride kuantum kapasitesi elde ettiklerinde bu arşivi Shor algoritmasıyla deşifre etmeyi planlamaktadır (Bernstein ve Lange, 2017). Bu strateji, özellikle gizlilik ömrü uzun veriler - devlet güvenlik belgeleri, sağlık kayıtları, finansal sözleşmeler, fikrî mülkiyet arşivleri - için acil bir tehdit oluşturmaktadır. Bu tehdit modelinin çalışma mantığı Şekil 5.3'te şematik olarak gösterilmektedir.

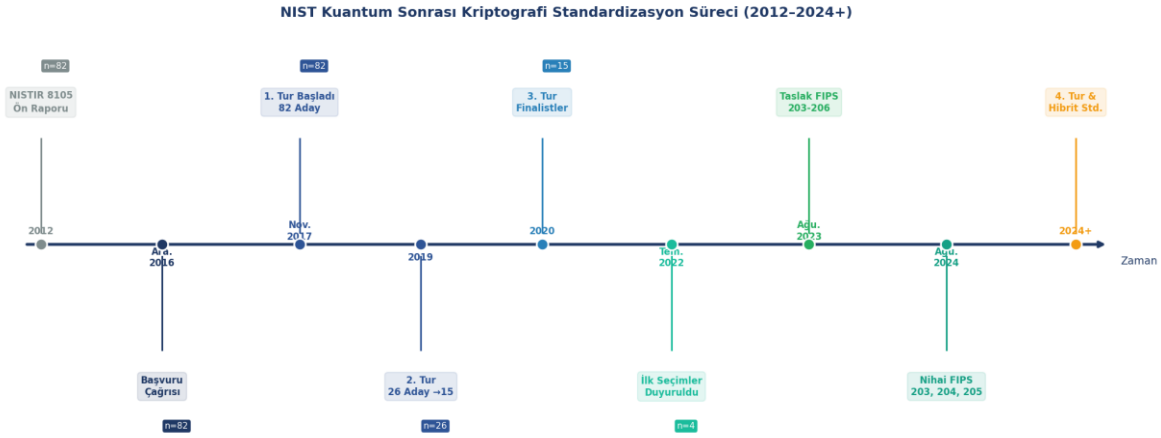


Şekil 5.3. "Şimdi Topla, Sonra Çöz" (Harvest-Now, Decrypt-Later) Tehdit Modeli. Bugün sağlanan gizlilik garantileri, kuantum bilgisayarların olgunlasmasiyla geriye donuk olarak tehdit altina girebilir. Bernstein ve Lange (2017) temel alınarak yazarlar tarafından hazirlanmiştir.

Bu tehdidin zaman hassasiyeti, PQC geçişini salt teorik bir "gelecek" meselesi olmaktan çıkarmaktadır. NSA, ABD Ulusal Güvenlik Ajansı olarak 2015 yılında yayımladığı duyuruda bu tehdide dikkat çekmiş; ardından NIST PQC süreci başlatılmıştır. Akademik araştırma açısından da bu durum, güvenlik kanıtlarının "kuantum saldırılar dahil" olarak tasarlanmasını zorunlu kılmaktadır.

5.6 NIST Kuantum Sonrası Kriptografi Standardizasyon Süreci

NIST, kuantum sonrası kriptografik standartlara duyulan ihtiyacı 2012 yılından itibaren resmi raporlarında vurgulayarak 2016 yılında NISTIR 8105 kapsamındaki ön değerlendirme sürecini tamamlamıştır (Chen vd., 2016). 2 Aralık 2016 tarihinde Federal Register'de yayımlanan başvuru çağrısıyla açılan PQC standardizasyon süreci, sekiz yıla yayılan, 25'ten fazla ülkeden araştırmacının katıldığı ve kriptografi tarihinin en kapsamlı açık değerlendirme süreçlerinden biri olarak kayıtlara geçmiştir (NIST, 2016; Moody vd., 2020). Sürecin zaman çizelgesi Şekil 5.4'te, aşamaları ve çıktıları ise Tablo 5.4'te sunulmaktadır.



Şekil 5.4. NIST PQC Standardizasyon Süreci Zaman Çizelgesi (2012–2024+). Süreç; aday sayısının 82'den nihai standartlara indirildigi alti aşamamdan olusmaktadir. NIST (2022b), Alagic vd. (2022) temel alınarak yazarlar tarafından hazirlanmiştir.

Tablo 5.4. NIST PQC Standardizasyon Sürecinin Aşamaları ve Çıktıları

Aşama	Donem	Temel Faaliyetler	Aday Sayisi	Kilit Cikti
Hazırlık (NISTIR 8105)	2012–2016	Kuantum tehdit analizi, kripto toplulugu istisaresi, degerl. kriterleri	-	NISTIR 8105: PQC ihtiyaci tescillendi
Basvuru & 0. Aşama	Ara. 2016	Uluslararası basvuru cagri; güvenlik, performans ve algoritma kriterleri	82 basvuru	Değerl. çerçevesi ve metodolojisi oluşturuldu
1.1 Tur	Kas. 2017–Oca. 2019	Topluluk kriptanalizi, güvenlik analizi, performans degerlendirilmesi	69 → 26	NISTIR 8240: 1. Tur durum raporu
1.2 Tur	2019–2020	Derinlemesine güvenlik analizi, uygulama testi, standartlasma kriterleri	26 → 15	NISTIR 8309: Alternatif adaylar belirlendi
1.3 Tur	2020–2022	Finalistler (4) ve alternatif adaylar (5); topluluk yorumlari, calistaylar	15 → 7	NISTIR 8413: 4 finalist, 4. tura taşındı
Standart Yayını	2022–2024	Taslak FIPS 203/204/205/206 yayını; kamu yorum donemi; nihai duzenleme	4 finalist	FIPS 203, 204, 205 (Agustos 2024)
1.4 Tur &Sonrası	2024+	Kod tabanlı adaylar (BIKE, McEliece, HQC); hibrit sistemler standartlasma	Devam	Ek standartlar bekleniyor

Not. NIST (2016), Moody vd. (2020) ve Alagic vd. (2022) temel alınarak yazarlar tarafından derlenmiştir.

5.6.1 Değerl. Kriterleri: Güvenlik, Performans ve Esneklik

NIST, aday algoritmaları değerlendirirken üç temel kriter bütününü uygulamıştır (NIST, 2016):

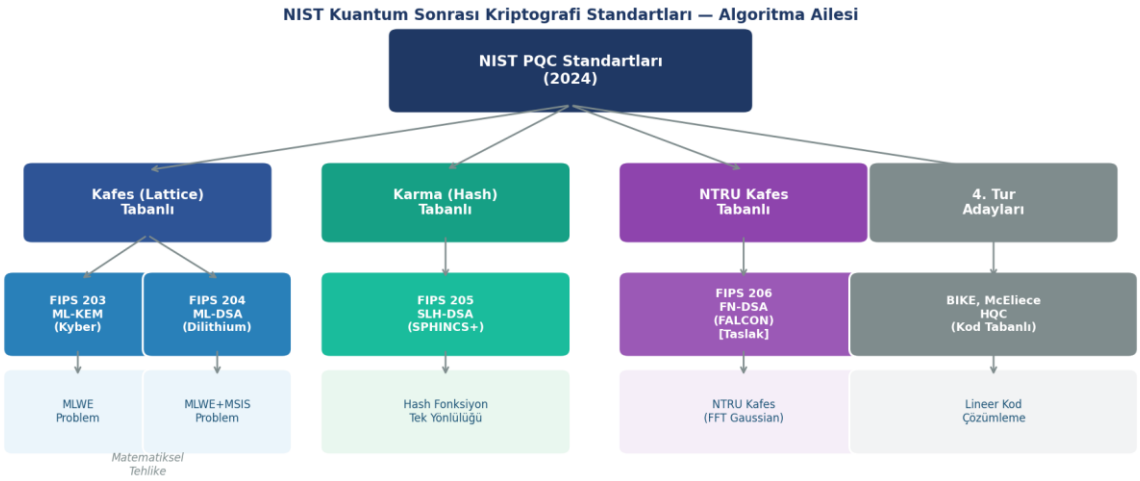
Güvenlik: Klasik ve kuantum saldırılarına karşı kanıtlanabilir güvenlik; kaba kuvvet, yapısal saldırılar, yan kanal saldırıları ve uygulama tabanlı saldırılar dahil bilinen tüm tehdit vektörlerine karşı direnç. Güvenlik seviyesi, AES ve SHA ailesiyle kalibrasyon yapılarak 1-5 arası ölçekte tanımlanmıştır.

Performans: Anahtar boyutları, imza/kapsül boyutları; x86-64, ARM, RISC-V ve IoT platformlarında anahtar üretimi, şifreleme/deşifreleme ve imzalama/doğrulama hızları. Hem yazılım hem donanım uygulamaları değerlendirilmiştir.

Algoritma ve Uygulama Özellikleri: Basitlik, mevcut protokollerle (TLS, IKE, 1.509) uyumluluk, paralelleştirilebilirlik, bellek gereksinimleri ve yan kanal saldırılarına karşı savunulabilirlik. Durum bilgisi gerektirmeme (statelessness) özelliği de avantaj olarak değerlendirilmiştir.

5.7 Seçilen NIST PQC Standartları: Matematiksel Temeller ve Kapsam

Sekiz yıllık ve küresel katılımlı değerlendirme sürecinin sonucunda NIST, Ağustos 2024 itibarıyla üç nihai FIPS standardı yayımlamış; dördüncü standart taslak aşamasında kalmıştır (NIST, 2024b; 2024c; 2024d). Bu standartlar birbirini tamamlayan iki temel işlev kategorisini karşılamaktadır: anahtar kapsülleme (KEM) ve dijital imza. Standartların dayandığı matematiksel aileler Şekil 5.5'te, karşılaştırmalı analizi ise Tablo 5.5'te sunulmaktadır.



Şekil 5.5. NIST PQC Standartları Algoritma Ailesi ve Matematiksel Temeller. Standartlar; kafes tabanlı (lattice), karma (hash) tabanlı ve NTRU kafes tabanlı olmak uzere uc matematiksel aileye dayanmakta olup bu dağıtım tek bir yapiya bagimlilik riskini azaltmaktadir. NIST (2024b, 2024c, 2024d) temel alınarak hazirlanmiştir.

Tablo 5.5. NIST Kuantum Sonrası Kriptografi Standartları - Karşılaştırmalı Analiz

FIPS	Algoritma (Kaynak)	Matematiksel Temel	Is. Amacı	Param. Setleri	Durum
FIPS 203	ML-KEM (CRYSTALS-Kyber)	Module Lattice / MLWE (Module Learning With Errors)	Anahtar Kapsulleme (KEM)	ML-KEM-512 (Sv.1) ML-KEM-768 (Sv.3)	NIHAI Agu. 2024

FIPS	Algoritma (Kaynak)	Matematiksel Temel	Is. Amacı	Param. Setleri	Durum
				ML-KEM-1024 (Sv.5)	
FIPS 204	ML-DSA (CRYSTALS-Dilithium)	Module Lattice / MLWE+MSIS (Fiat-Shamir with Aborts)	Dijital Imza	ML-DSA-44 (Sv.2) ML-DSA-65 (Sv.3) ML-DSA-87 (Sv.5)	NIHAI Agu. 2024
FIPS 205	SLH-DSA (SPHINCS+)	Hash-Based Signatures (SHA-256 / SHAKE-256, stateless)	Dijital Imza	12 parametre seti (hiz vs. kucuk imza dengesi)	NIHAI Agu. 2024
FIPS 206	FN-DSA (FALCON)	NTRU Kafes / Fast Fourier Lattice (Gaussian Sampling)	Dijital Imza	FALCON-512 (Sv.1) FALCON-1024 (Sv.5)	TASLAK 2024

Not. MLWE: Module Learning With Errors; MSIS: Module Short Integer Solution; Sv.: Güvenlik Seviyesi. NIST (2024b, 2024c, 2024d), Bos vd. (2018), Ducas vd. (2018), Bernstein vd. (2019), Fouque vd. (2020) temel alınarak yazarlar tarafından derlenmiştir.

5.7.1 FIPS 203 - ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)

FIPS 203, CRYSTALS-Kyber algoritmasının standartlaştırılmış biçimi olan ML-KEM'i tanımlamaktadır (NIST, 2024b). Güvenliği, Module Learning With Errors (MLWE) problemine dayanan bir güvenlik indirgeme kanıtına sahiptir. Problem şu biçimde ifade edilebilir: A matrisi ve b = As + e vektörü verildiğinde (s küçük gizli vektör, e küçük hata terimi), s'yi bulmak hem klasik hem de bilinen tüm kuantum algoritmalar için hesaplamalı açıdan güçtür (Peikert, 2016).

ML-KEM'in kritik tasarım özellikleri şöyledir: (1) Güvenlik kanıtı, standart model ("random oracle olmaksızın") değil, rastgele oracle modelinde kurulmuştur; (2) İndirgenemez rastgelelik (indistinguishability) özelliği IND-CCA2 saldırılarına karşı güvenliği garanti eder; (3) Üç parametre seti (512/768/1024) farklı güvenlik-performans dengesi sunar. Algoritma, TLS 1.3, SSH ve IPsec protokollerinde ECDH'nın yerini alması amacıyla tasarlanmıştır.

5.7.2 FIPS 204 - ML-DSA (Module-Lattice-Based Digital Signature Algorithm)

FIPS 204, CRYSTALS-Dilithium'dan türetilen ML-DSA'yı standartlaştırmaktadır (NIST, 2024c). Güvenlik kanıtı MLWE ve MSIS (Module Short Integer Solution) problemlerine indirgenmiştir. "Fiat-Shamir with Aborts" paradigmasına dayanan bu tasarım, ret-kabul örneklemesi (rejection sampling) kullanarak imzaların gizli anahtar bilgisini sızdırmamasını garanti etmektedir (Ducas vd., 2018). ML-DSA, deterministik imza üretimini destekleyerek ECDSA'nın nonce yeniden kullanımı güvenlik açığını (Sony PlayStation 3 saldırısı gibi) yapısal olarak ortadan kaldırmaktadır.

5.7.3 FIPS 205 - SLH-DSA (Stateless Hash-Based Digital Signature Algorithm)

FIPS 205, SPHINCS+'dan türetilen SLH-DSA'yı tanımlamaktadır (NIST, 2024d). Temel farklılığı, güvenliğinin yapısal kriptografik problemlere değil yalnızca hash fonksiyonlarının (SHA-256, SHAKE-256) tek yönlülüğüne ve çarpışma direncine dayanmasıdır (Bernstein vd., 2019). Bu özellik SLH-DSA'ya köklü bir uzun vadeli güvenlik garantisi kazandırır: kafes problemlerine yönelik henüz bilinmeyen kriptanalitik saldırılar geliştirilse dahi SLH-DSA güvenliğini koruyacaktır. Kompromis olarak büyük imza boyutları (SLH-DSA-128s'de 7.856 bayt) ve yavaş imzalama hızı kabul edilmiştir. Buna karşın,

yalnızca 32 baytlık genel anahtar boyutu ve durum bilgisi gerektirmeyen tasarımı, kök CA (Certificate Authority) ve uzun ömürlü belge imzalama için ideal kılmaktadır.

5.7.4 FIPS 206 - FN-DSA / FALCON (Taslak)

FIPS 206, NTRU kafes yapısına dayanan FALCON'dan türetilen FN-DSA'yı tanımlamaktadır. FALCON'ın ML-DSA'ya göre en belirgin avantajı, kompakt imza boyutudur (FALCON-512'de ~666 bayt). Bu verimlilik, Hızlı Fourier Dönüşümü (FFT) üzerinde Gaussian örnekleme ile sağlanmakta olup güvenli uygulaması hassas bir mühendislik gerektirmektedir (Fouque vd., 2020). Yan kanal saldırılarına karşı Gaussian örneklemenin sabit zamanda gerçekleştirilmesi zorunluluğu, FIPS 206'nın nihai yayınını diğer standartlara kıyasla gecikmesine yol açmıştır.

5.8 NIST PQC Güvenlik Seviyeleri Çerçevesi

NIST, PQC sürecinde güvenlik düzeylerini simetrik kriptografinin referans noktaları üzerinden tanımlamıştır. Bu beş katmanlı çerçeve, farklı uygulama gereksinimlerinde algoritma seçimini standart bir zemine oturtmakta ve üretim maliyeti ile güvenlik garantisi arasındaki dengeyi optimize etmeye imkân tanımaktadır (NIST, 2016). Bu çerçevenin güvenlik seviyeleri ve algoritma eşleştirmesi Tablo 5.6'da sunulmaktadır.

Tablo 5.6. NIST PQC Güvenlik Seviyeleri Çerçevesi ve Algoritma Eşleştirmesi

Guv. Sev.	Tanim (Referans Problem)	Klasik Esdeger	ML-KEM Par. Seti	ML-DSA Par. Seti	SLH-DSA Ornek
Seviye 1	AES-128 tam arama kadar zorlu hesaplama	128-bit	ML-KEM-512	ML-DSA-44	SLH-DSA-SHA2-128s
Seviye 2	SHA-256/SHA3-256 carpisma bulma kadar zorlu	~128-192-bit	-	-	SLH-DSA-SHA2-128f
Seviye 3	AES-192 tam arama kadar zorlu hesaplama	192-bit	ML-KEM-768	ML-DSA-65	SLH-DSA-SHA2-192s
Seviye 4	SHA-384/SHA3-384 carpisma bulma kadar zorlu	~192-256-bit	-	-	SLH-DSA-SHA2-192f
Seviye 5	AES-256 tam arama kadar zorlu hesaplama	256-bit	ML-KEM-1024	ML-DSA-87	SLH-DSA-SHA2-256s

Not. NIST (2016, 2022b) temel alınarak yazarlar tarafından derlenmiştir. Güvenlik seviyeleri, ilgili referans problemi için klasik en iyi bilinen algoritmaya dayali hesaplamal güclukle kalibre edilmiştir. SLH-DSA: Stateless Hash-Based DSA; "s" yavaş-kücük imza, "f" hızlı parametrelerini belirtmektedir.

Pratik uygulama bağlamında bu seviyelendirme kritik önem taşır. Kısa vadeli gizlilik yeterli olan IoT ve gömülü sistemlerde Seviye 1 tercih edilirken, uzun vadeli gizlilik gerektiren devlet belgeleri ve finansal arşivler için Seviye 5 önerilmektedir. Kritik altyapı ve PKI (Public Key Infrastructure) uygulamaları için NIST, en az Seviye 3'ü tavsiye etmektedir (Barker vd., 2020).

5.9 Geçiş Stratejileri, Uluslararası Uyum ve Diğer NIST Çalışmaları

5.9.1 Hibrit Kriptografi Yaklaşımı

NIST ve akademik konsensüs, geçiş döneminde hibrit kriptografi yaklaşımını öncelikli strateji olarak benimsemektedir. Bu modelde TLS veya diğer protokollerde hem klasik (ECDH) hem de kuantum sonrası (ML-KEM) anahtar değişimi mekanizması eş zamanlı olarak çalıştırılır; kombinasyonun

güvenliği her iki algoritmanın da kırılamamasına bağlıdır (Stebila ve Mosca, 2016). Bu yaklaşım, özellikle PQC algoritmalarında henüz keşfedilmemiş güvenlik açıklarına karşı bir sigorta işlevi görmektedir. NIST SP 1800-38 ve IETF'nin RFC 9370 belgesi bu geçiş metodolojisini ayrıntılı biçimde tanımlamaktadır.

5.9.2 Uluslararası Standardlaşma Uyumu

NIST PQC süreci, küresel ölçekte belirleyici bir referans işlevi kazanmıştır. ISO/IEC JTC 1/SC 27 çalışma grubu, NIST standartlarıyla uyumlu uluslararası standartlar geliştirmekte; ETSI Quantum Safe Cryptography çalışma grubu Avrupa perspektifinden göç rehberleri yayımlamaktadır (ETSI, 2020). Almanya'nın BSI ve Fransa'nın ANSSI ajansı, büyük ölçüde NIST PQC tercihlerini benimseyen ulusal PQC tavsiyeleri yayımlamıştır (BSI, 2021). Japonya CRYPTREC projesi ve Kore KISA da benzer sonuçlara ulaşmıştır.

Öte yandan Çin, SM2/SM9/SM4 ulusal kriptografi standartlarını sürdürmekte ve kendi PQC çalışmalarını yürütmektedir. Rusya'nın GOST sistemi de bağımsız bir yol izlemektedir. Bu çoğulcu tablo, küresel birlikte çalışabilirlik açısından uzun vadeli bir standartlaşma zorunluluğunu gündeme getirmektedir (National Academies, 2019).

5.9.3 Kuantum Anahtar Dağıtımı (QKD) ile İlişkisi

NIST, QKD'yi geleneksel ağ güvenlik katmanlarının tamamını ikame eden bir çözüm olarak değil, PQC ile birlikte katmanlı bir güvenlik mimarisinin bir bileşeni olarak konumlandırmaktadır (NISTIR 8240, 2019). QKD fizik yasalarına dayalı teorik güvenlik sağlarken, güncel QKD sistemleri yan kanal saldırılarına, kimlik doğrulama açıklarına ve mesafe kısıtlarına karşı hâlâ savunmasızdır. Bu nedenle PQC, QKD'ye kıyasla daha geniş uygulama yelpazesine sahip ve standartlaşma açısından daha olgun bir yaklaşım sunmaktadır.

5.10 Eleştirel Değerlendirme: NIST PQC Sürecinin Sınırlılıkları

Nesnel bir akademik perspektiften değerlendirildiğinde, NIST PQC standardizasyon sürecinin belirli sınırlılıkları kabul edilmelidir. Birincisi, seçilen dört standartın üçünün (ML-KEM, ML-DSA, FN-DSA) kafes problemlerine dayandığı görülmektedir. Bu homojenlik, henüz bilinmeyen bir kafes saldırısının eş zamanlı üç standardı tehlikeye atması senaryosunu olası kılmaktadır; bu riski azaltmak için hash tabanlı SLH-DSA'nın dahil edilmesi önemli bir tasarım kararı olmuştur (Bernstein ve Lange, 2017).

İkincisi ve en dramatik biçimde örnekleyen vakası, SIKE (Supersingular Isogeny Key Encapsulation) algoritmasıdır. 2022 yılında üç turda hayatta kalan bu aday, beklenmedik derecede verimli bir klasik saldırıyla (Castryck ve Decru, 2022) kırılmıştır. Castryck ve Decru'nun EUROCRYPT 2023'te sunulan saldırısı, tek bir kişisel bilgisayarda 62 dakikada SIKE'ı çözmüş; yedi yıllık toplu kriptanaliz çabasının gözden kaçırdığı bir geometrik zafiyeti ortaya koymuştur. Bu olay, akademik kriptografi araştırmaları için kritik bir uyarı niteliği taşımaktadır: Aday sayısının azlığı ve özelleşmiş matematiksel yapılar, uzun süreli taramayı bile yanıltabilir.

Üçüncüsü, sürecin ABD merkezli kurumsal yapısı ve ticari çıkar potansiyelidir. Ancak tam şeffaf değerlendirme metodolojisi, tüm kaynak kodların ve şartnamelerin kamuoyuyla paylaşılması ve uluslararası topluluk katılımı bu endişeyi önemli ölçüde azaltmaktadır. Son olarak, performans açısından PQC algoritmalarının anahtar ve imza boyutları klasik algoritmalarla kıyaslandığında anlamlı ölçüde büyüktür; bu durum bant genişliği kısıtlı protokoller ve kaynak sınırlı cihazlar için geçiş maliyetlerini artırmaktadır.

BÖLÜM 6

Kuantum Algoritmalar

Faz, Girişim ve Hesaplamanın Yeni Dili

6.1 Giriş: Kuantum Avantajının Gerçek Kaynağı

Kuantum algoritmalar üzerine yazılmış popüler anlatılarda sıkça tekrarlanan bir yanlış, hesaplama avantajının yalnızca "aynı anda birden fazla ihtimali denemek" yeteneğinden kaynaklandığı iddiasıdır. Bu açıklama yaygın olmakla birlikte temelden eksiktir (Nielsen ve Chuang, 2010). Süperpozisyon, qubit sistemlerin olasılık genliklerini aynı anda birden fazla hesapsal duruma dağıtabilmesi anlamına gelir; fakat bu özellik tek başına algoritmik bir avantaj sağlamaz. Herhangi bir gözlem yapıldığında, yani ölçüm gerçekleştiğinde, sistemin bu geniş süperpozisyonu çöker ve elimizde yalnızca tek bir klasik sonuç kalır.

Kuantum avantajının gerçek motoru şudur: genlikler yalnızca pozitif değil, negatif ve karmaşık değerler de taşıyabilir. Bu nedenle doğru cevabın genliğini yapıcı girişimle büyütmek, yanlış cevapların genliğini ise yıkıcı girişimle söndürmek mümkündür (Nielsen ve Chuang, 2010, s. 248). Ölçüm öncesinde gerçekleştirilen bu kasıtlı genlik manipülasyonu, doğru sonucun son ölçümde yüksek olasılıkla görünmesini sağlar. Klasik olasılıklar yalnızca pozitif ve toplamsal davranırken, kuantum genlikleri birbirini hem güçlendirebilir hem de yok edebilir. Bu fark, kuantum ve klasik hesaplama sınıfları arasındaki en köklü ayrımı oluşturur.

Bu bölümde incelenen tüm algoritmalar - Deutsch–Jozsa, Simon, Grover, Kuantum Fourier Dönüşümü (QFT), Kuantum Faz Tahmini (QPE) ve Shor - bu ortak ilkenin farklı problem yapılarına uygulanmasıdır (Cleve vd., 1998). Her biri, oracle'ın sisteme bıraktığı faz izlerini işleyerek ölçüm öncesinde bilgiyi öne çıkarır; doğrudan değer okumak yerine global yapıyı ya da gizli simetriyi yakalayarak çözüme ulaşır. Bölümde ele alınan algoritmaların karmaşıklık karşılaştırması Tablo 6.1'de özetlenmektedir.

AKILDA TUT Kuantum avantajı, olasılık taşımaktan değil, bu olasılıkların fazlarını kasıtlı biçimde işleyerek yıkıcı ve yapıcı girişim kurmaktan doğar.

Tablo 6.1. Bölümde ele alınan algoritmaların klasik ve kuantum karmaşıklık karşılaştırması (Nielsen ve Chuang, 2010; Shor, 1994; Grover, 1996).

Algoritma	Klasik	Kuantum	Avantaj Türü
Deutsch-Jozsa	O(2^(n-1))	O(1)	Üstel
Simon	O(2^n)	O(n)	Üstel
Grover	O(N)	O(√N)	Karesel
QFT	O(N log N)	O(n^2) kapı	Üstel (kapı)
QPE	N/A	O(n^2)	Olanaklı kılar
Shor	O(e^(n^(1/3)))	O(n^3)	Üstel

6.2 Oracle: Problemi Devreye Gömen Kara Kutu

Bu bölümdeki birçok algoritmada, çözülmesi gereken problem devre içine doğrudan yazılmaz. Bunun yerine oracle adı verilen bir kara kutu mekanizması kullanılır (Nielsen ve Chuang, 2010, s. 255). Oracle, matematiksel açıdan bir üniter dönüşümdür; işlevsel açıdan ise problemin kurallarını ya da çözülmek istenen fonksiyonu kuantum devreye gömen bir yapıdır. Kullanıcı açısından oracle'ın iç yapısı bilinmez; yalnızca ona sorgu gönderilebilir.

Oracle'ı sezgisel olarak anlamanın en iyi yolu, onun klasik anlamda "cevap döndürmediğini" kavramaktır. Oracle sorgulanan duruma doğrudan bir değer atamaz; onun yerine sisteme belirli bir faz izi bırakır - bu mekanizma faz geri tepme (phase kickback) olarak bilinir (Cleve vd., 1998). Bu faz izi, algoritmanın sonraki adımlarında anlamlı girişim desenlerine dönüşür. Başka bir ifadeyle, oracle bir cevap vermez; ancak doğru cevabın ileride öne çıkmasını mümkün kılan koşulları hazırlar.

Sorgu karmaşıklığı perspektifinden bakıldığında, bir algoritmanın verimliliği büyük ölçüde oracle'a kaç kez sormak zorunda kaldığıyla ölçülür (Buhrman ve de Wolf, 2002). Deutsch–Jozsa ve Simon algoritmaları bu sayıyı dramatik biçimde azaltır; Grover ise karesel bir iyileşme sağlar.

6.3 Deutsch–Jozsa Algoritması

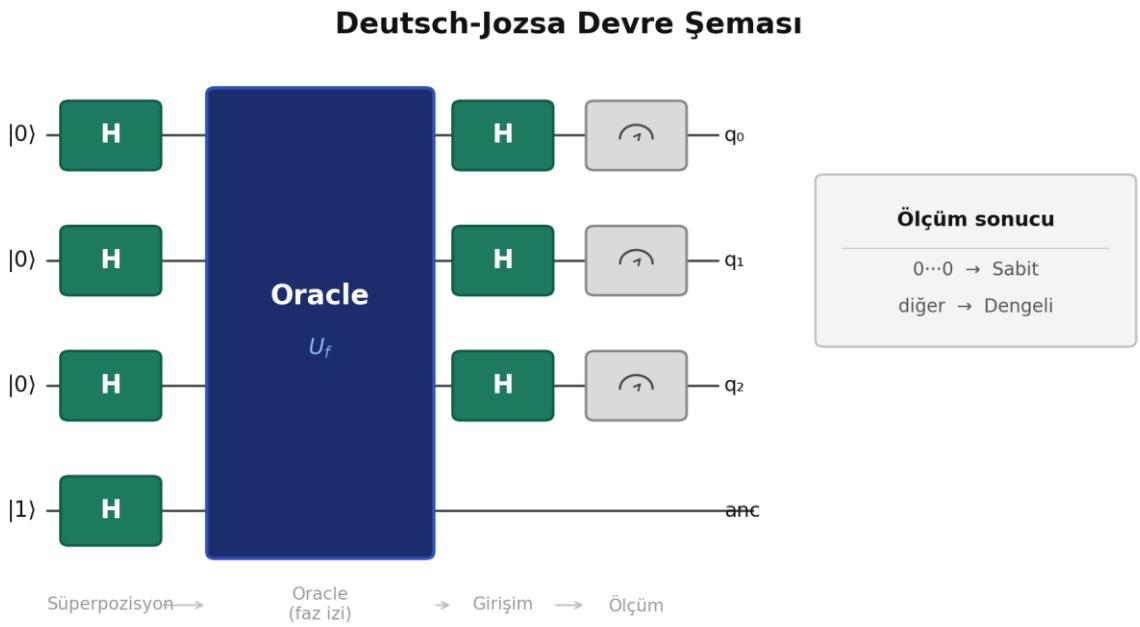
6.3.1 Problem Tanımı ve Klasik Maliyet

Deutsch–Jozsa algoritması, kuantum sorgu karmaşıklığında net bir avantajın ilk formel olarak gösterildiği örnektir (Deutsch ve Jozsa, 1992). Problem şu koşulla başlar: bir kara kutu fonksiyon $f: \{0,1\}^n \rightarrow \{0,1\}$ verilmiştir ve bu fonksiyonun iki özellikten birini taşıdığı garanti edilmiştir. Ya fonksiyon sabittir - yani her girdi için aynı çıktıyı üretir - ya da dengelidir - yani girdilerin tam yarısında 0, yarısında 1 üretir. Görev, fonksiyonun bu iki sınıftan hangisine ait olduğunu belirlemektir.

Klasik deterministik bir algoritma için en kötü durum analizi şu sonucu verir: n-bitlik girdi uzayı üzerinde kesin bir karar vermek $2^{n-1} + 1$ sorgu gerektirebilir (Cleve vd., 1998). Bunun nedeni şudur: n/2 adet aynı çıktı görmek, fonksiyonun sabit olduğunu kanıtlamaz; dengeli fonksiyonun henüz test edilmemiş kısmına denk gelmiş de olabilir.

6.3.2 Kuantum Çözümü ve Devre Yapısı

Kuantum versiyonu tek oracle sorgusunda kesin karar verir (Deutsch ve Jozsa, 1992). Şekil 6.1'de gösterilen devrenin yapısı üç temel katmandan oluşur: (1) Hadamard kapıları ile süperpozisyon hazırlık katmanı, (2) oracle sorgulama - faz geri tepme mekanizmasıyla sonuç faza taşınır, (3) ikinci Hadamard katmanı ile girişim oluşturma ve son ölçüm. Fonksiyon sabit ise tüm bileşenler yapıcı girişimle $|0\ldots0\rangle$ durumuna toplanır; dengeli ise yıkıcı girişimle $|0\ldots0\rangle$ tamamen söndürülür.



Şekil 6.1. Deutsch–Jozsa devre şeması. Giriş qubitleri ve yardımcı qubit süperpozisyona alınır; oracle faz izini bırakır; ikinci Hadamard katmanı girişim oluşturur (Deutsch ve Jozsa, 1992; Nielsen ve Chuang, 2010).

Algoritmanın Özü
Deutsch–Jozsa her noktadaki fonksiyon değerini ayrı ayrı öğrenmez. Bunun yerine, fonksiyonun tüm girdi uzayı üzerindeki simetrisini faz ve girişim yoluyla tek bir sorguda görünür kılar. Bu, yerel örnekler toplamak değil; global yapıyı ölçmektir (Deutsch ve Jozsa, 1992).

AKILDA TUT Deutsch–Jozsa: Fonksiyon değerlerini tek tek sormaz; fonksiyonun global simetrisini tek sorguda ayırt eder.

6.4 Simon Algoritması

6.4.1 Gizli Yapı Problemi

Simon algoritması, Deutsch–Jozsa'nın ötesine geçerek daha zengin bir yapısal problemi ele alır (Simon, 1997). Problem şu şekilde tanımlanır: f: $\{0,1\}^n \rightarrow \{0,1\}^n$ fonksiyonu bilinmeyen bir $s \in \{0,1\}^n$ dizisine göre iki-bire (two-to-one) eşlemedir. İki farklı giriş x ve y için f(x) = f(y) koşulu, yalnızca ve yalnızca $x \oplus y = s$ olduğunda sağlanır; burada $\oplus$ XOR işlemini gösterir. Amaç bu gizli s dizisini bulmaktır.

Klasik bir algoritmanın bu problemi çözmesi için en kötü durumda Ω(2^{n/2}) sorgu gerekir (Simon, 1997). Simon algoritması ise bunu O(n) kuantum sorgu ve ardından yapılan klasik Gauss eleme adımlarıyla çözer. Bu, kuantum hesaplamanın klasik hesaplamaya göre üstel kazanç sağladığı ilk örneklerden biridir ve Shor algoritmasının geliştirilmesine önemli bir ilham kaynağı olmuştur (Shor, 1994).

6.4.2 Ölçüm Cevap Değil, Denklem Üretir

Simon algoritmasının en kritik özelliği, her kuantum çalıştırmanın doğrudan s değerini vermemesidir (Simon, 1997). Bunun yerine her çalıştırma, s hakkında bir doğrusal kısıt üretir. Devre uygulandıktan ve ölçüm yapıldıktan sonra elde edilen y vektörü, $y \cdot s = 0 \pmod 2$ koşulunu sağlar. Algoritma yaklaşık n kez çalıştırıldıkça n bağımsız doğrusal kısıt biriktirilir; ardından klasik Gauss eleme yöntemiyle s belirlenir (Nielsen ve Chuang, 2010, s. 260).

Bu tasarım ilkesi, kuantum hesaplamada alışılmadık ama son derece güçlü bir düşünce biçimini temsil eder: ölçüm bir sonuç değil, çözüme götüren bir denklem üreticisidir. Anlam tek ölçümde değil, biriken kısıtların toplamında doğar (Cleve vd., 1998).

Simon ile Shor Arasındaki Köprü
Simon algoritması tarihsel açıdan da büyük önem taşır: Shor'un faktörizasyon algoritmasında kullanılan periyot bulma yaklaşımının zihinsel öncülüdür (Shor, 1994). Her iki algoritma da gizli grup yapısını ortaya çıkarmak için kuantum girişiminden yararlanır ve ardından gelen klasik bir adımla sonucu tamamlar (Nielsen ve Chuang, 2010).

AKILDA TUT Simon algoritması gizli stringi doğrudan ölçmez; her çalıştırma, gizli stringi çözmek için gereken doğrusal bir kısıt üretir.

6.5 Grover Algoritması

6.5.1 Yapılandırılmamış Arama ve Klasik Alt Sınır

Grover algoritması, yapılandırılmamış arama problemleri için tasarlanmıştır (Grover, 1996). N elemanlı bir aday kümesinde herhangi bir yapı ya da sıralama garantisi olmaksızın, klasik bir algoritmanın en kötü durumda $\Theta(N)$ sorgu yapması kaçınılmazdır. Grover bu maliyeti $O(\sqrt{N})$ sorgusuna indirir - bu karesel bir iyileştirmedir ve Bennett vd. (1997) tarafından asimptotik açıdan optimal olduğu kanıtlanmıştır: hiçbir kuantum algoritması yapılandırılmamış aramayı $O(\sqrt{N})$'dan daha az sorguda çözemez.

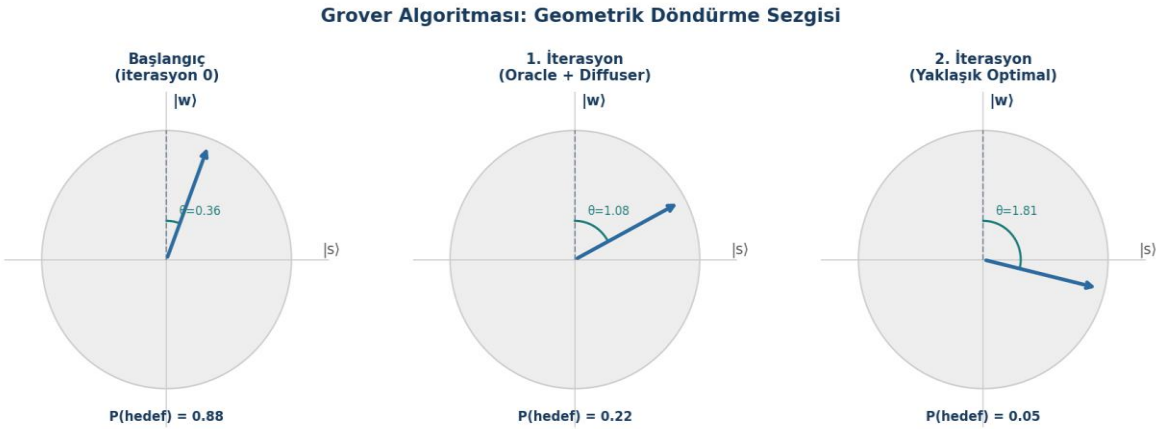
6.5.2 Oracle ve Diffuser: İki Temel Operatör

Grover iterasyonu iki temel bileşenden oluşur (Grover, 1996). Oracle, hedef durumun fazını ters çevirerek onu işaretler: $U_w|x\rangle = -|x\rangle$ ($x = w$ için). Diffuser ise tüm genlikleri ortalama değer etrafında yansıtır - bu işlem genlik amplifikasyonu (amplitude amplification) olarak bilinir (Brassard vd., 2002). Oracle'ın negatife döndürdüğü hedef genlik, yansıma sonucunda ortalamanın üstüne fırlatılır; böylece her iterasyonda hedef durumun ölçüm olasılığı artar.

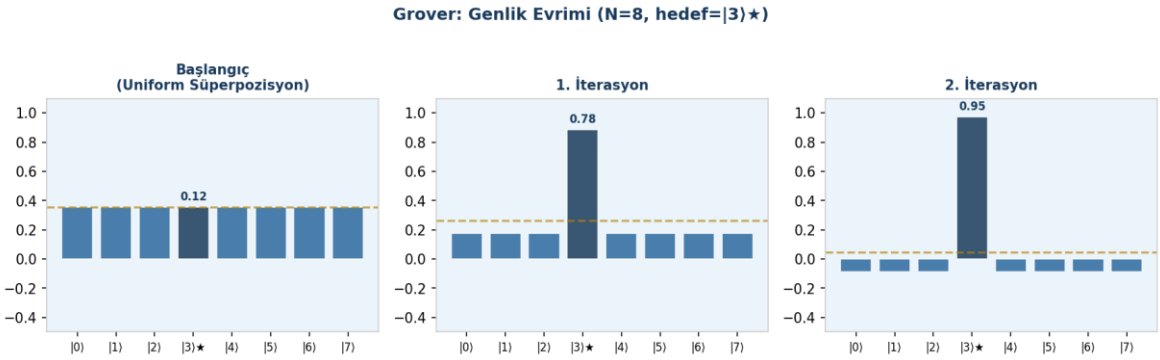
6.5.3 Geometrik Yorum

Grover'ın en sezgisel açıklaması geometrik bir yorum üzerine kuruludur (Nielsen ve Chuang, 2010, s. 278). Şekil 6.2'de gösterildiği üzere, durum vektörü hedef durumu ve hedef-dışı durumların altuzayı tarafından tanımlanan iki boyutlu düzlemde döner. Her Grover iterasyonu vektörü sabit bir 2θ açısı kadar hedefe yaklaştırır; burada $\sin(\theta) = 1/\sqrt{N}$'dir. Optimal iterasyon sayısı $\lfloor \pi\sqrt{N}/4 \rfloor$ civarındadır (Grover,

1996). Şekil 6.3'te N=8 örneği üzerinden gösterildiği gibi, bu sayıyı aştığında vektör hedefi geçer ve başarı olasılığı düşmeye başlar.



Şekil 6.2. Grover geometrik döndürme. Her iterasyon durum vektörünü hedef yönüne (|w⟩) yaklaştırır; başarı olasılığı kademeli olarak artar (Nielsen ve Chuang, 2010).



Şekil 6.3. Grover genlik evrimi (N=8). Hedef durum |3⟩'ün genliği her iterasyonda büyürken diğer durumların genliği azalır (Grover, 1996).

Karesel mi, Üstel mi?
Grover'ın sağladığı karesel hızlanma bazı uygulamalar için son derece değerlidir: kriptografik brute-force saldırılarını 2ⁿ'den 2^(n/2)'ye indirger (Bernstein, 2010). Bununla birlikte üstel hızlanma değildir; Shor'un üstel hızlanmasından nitelik olarak farklıdır (Nielsen ve Chuang, 2010, s. 276).

AKILDA TUT Oracle hedefi fazda işaretler, diffuser bu işareti genlik artışına dönüştürür. Başarı, iterasyonları doğru sayıda yapmaktan gelir.

6.6 Kuantum Fourier Dönüşümü (QFT)

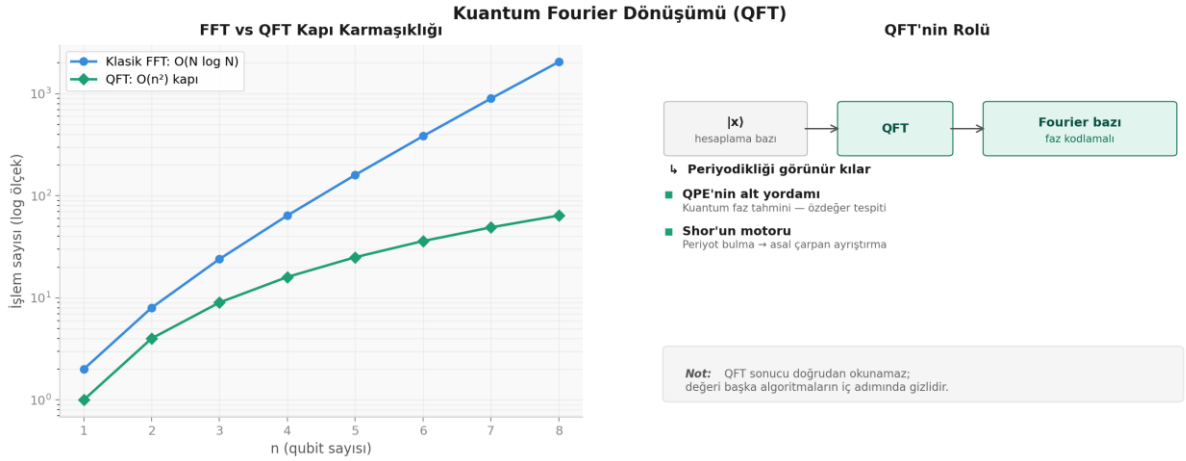
6.6.1 QFT Nedir?

Kuantum Fourier Dönüşümü (QFT), kuantum hesaplamadaki en temel alt yordamlardan biridir (Coppersmith, 2002). Fonksiyonel açıdan QFT şunu gerçekleştirir: hesaplama bazındaki bir kuantum durumu |x⟩'yi, Fourier bileşenlerinin genlik olarak kodlandığı başka bir baza dönüştürür. Bu dönüşüm matematiksel olarak klasik Ayrık Fourier Dönüşümü ile aynı haritayı tanımlar; fakat işlemi tamamen kuantum durum içinde gerçekleştirir (Nielsen ve Chuang, 2010, s. 217).

Klasik FFT, N noktalı bir sinyali O(N log N) işlemle dönüştürür ve sonuçları açıkça okunabilir katsayılar olarak çıktı verir. QFT ise $N = 2^n$ boyutlu bir kuantum durumu üzerinde yalnızca $O(n^2)$ kapıyla aynı dönüşümü gerçekleştirir (Coppersmith, 2002). Ancak kritik bir kısıt vardır: QFT sonucunu doğrudan okuyamazsınız. Ölçüm yalnızca tek bir bileşeni ortaya çıkarır; dönüşümün geri kalanı kaybolur (Nielsen ve Chuang, 2010, s. 220).

6.6.2 Devre Yapısı ve Rolü

QFT devresi, Hadamard kapıları ve controlled-phase (CP) rotasyon kapılarından oluşur; n qubitlik bir sistem için toplam kapı sayısı n(n+1)/2 olup $O(n^2)$ karmaşıklığa karşılık gelir (Nielsen ve Chuang, 2010, s. 219). Şekil 6.4'te gösterildiği üzere, QFT'nin gerçek değeri bir algoritma zinciri içinde faz bilgisini başka bir yapıya erişilebilir kılmasında yatar: QPE'de bilinmeyen fazı ölçülebilir ikili sayıya çevirir; Shor'da modüler üslemenin periyodunu görünür kılar (Kitaev, 1995; Shor, 1994).



Şekil 6.4. QFT karmaşıklık karşılaştırması ve algoritma zincirindeki rolü. Sol: Klasik FFT ile QFT kapı karmaşıklığı (Coppersmith, 2002). Sağ: QFT'nin QPE ve Shor içindeki konumu (Nielsen ve Chuang, 2010).

AKILDA TUT QFT faz yapısını görünür hale getirir - kendi başına sonuç üretmez, başka algoritmaların çalışmasına zemin hazırlar.

6.7 Kuantum Faz Tahmini (QPE)

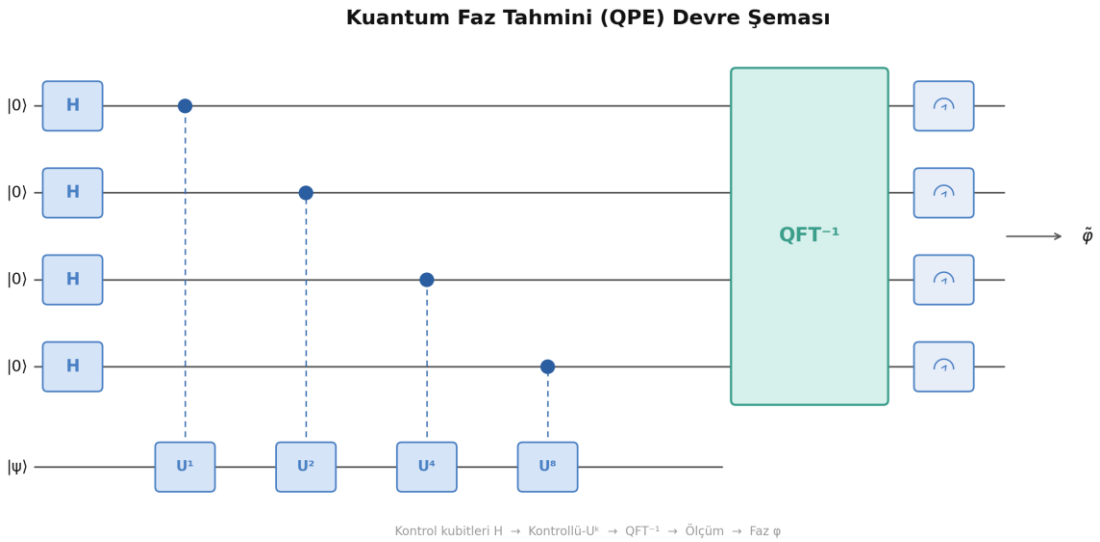
6.7.1 Temel Fikir: Fazı Sayıya Çevirmek

Kuantum Faz Tahmini (QPE), kuantum algoritma mimarisinin en merkezi yapı taşlarından biridir (Kitaev, 1995). Temel hedefi şudur: bir üniter operatör U verildiğinde, onun bilinmeyen bir özgenleme $|\psi\rangle$ üzerindeki özdeğer fazı ϕ'yi tahmin et; öyle ki $U|\psi\rangle = e^{2\pi i\phi}|\psi\rangle$. Özdeğer fazları, kuantum kimyada moleküler enerji seviyeleri (Aspuru-Guzik vd., 2005), kriptografide periyot bilgisi (Shor, 1994) ve lineer denklem sistemlerinin çözümünde (Harrow vd., 2009) temel büyüklüklere karşılık gelir; QPE bu soyut fazı okunabilir nicel çıktıya dönüştürerek geniş bir uygulama alanı sunar.

6.7.2 QPE Çalışma Mekanizması

Şekil 6.5'te şematik olarak gösterilen QPE, t adet kontrol qubit ve |ψ⟩ durumunu tutan hedef register ile başlar (Nielsen ve Chuang, 2010, s. 221). Kontrol qubitler Hadamard ile süperpozisyona alınır. Ardından kontrollü-U, kontrollü-U², kontrollü-U⁴,..., kontrollü-U^{2^{t-1}} sırasıyla uygulanır. Bu işlem, faz bilgisini faz geri tepme (phase kickback) yoluyla kontrol register'ına bit bit yayar. İnverse QFT uygulandığında, bu bilgi hesaplama bazına dönüştürülür ve φ'nin t-bit hassasiyetinde tahmini elde edilir. Hassasiyet, kullanılan kontrol qubit sayısı t arttıkça iyileşir (Cleve vd., 1998).

Bu yapı Şekil 6.5'te gösterilmektedir.



Şekil 6.5. QPE devre şeması. Kontrol qubitleri Hadamard'dan geçer; kontrollü-U^k operatörleri faz bilgisini yayar; QFT^{-1} faz bilgisini okunabilir ikili sayıya çevirir (Kitaev, 1995; Nielsen ve Chuang, 2010).

AKILDA TUT QPE fazı sayıya çevirir: QFT fazı görünür kılar; QPE onu bit düzeyinde okunabilir nicel bilgiye dönüştürür.

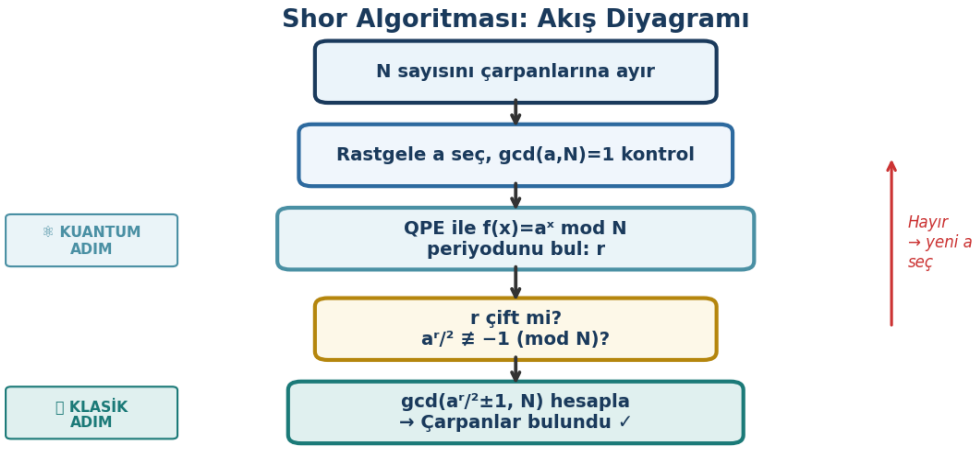
6.8 Shor Algoritması

6.8.1 Faktörizasyonun Periyot Bulmaya İndirgenmesi

Shor algoritması, kuantum hesaplamanın tarihsel dönüm noktalarından biridir (Shor, 1994). Yüzeysel bakışta büyük sayıları asal çarpanlarına ayıran bir algoritma olarak tanımlanır; fakat Shor'un kuantum kısmı faktörleri doğrudan aramaz. Bunun yerine, asal çarpanlara ayırma problemini daha temel bir probleme indirger: modüler üsleme fonksiyonunun periyodunu bulmak (Nielsen ve Chuang, 2010, s. 232). N ile aralarında asal rastgele bir a seçilir; ardından $f(x) = a^x \bmod N$ fonksiyonunun periyodu r, QPE aracılığıyla bulunur. r çift ve $a^{r/2} \not\equiv -1 \pmod N$ ise, $\gcd(a^{r/2}\pm 1, N)$ ifadeleri N'nin gerçek çarpanlarını verir (Shor, 1994).

6.8.2 QFT ve QPE'nin Rolü

Shor'un kuantum kısmında QFT kritik bir role sahiptir (Kitaev, 1995). Modüler üslemenin periyodunu bulmak için fonksiyon değerleri süperpozisyon içinde hazırlanır ve bu yapıya QFT uygulanır; QFT çıktısı periyot bilgisini taşıyan tepe değerlerini üretir. Bu yapı QPE'nin özel bir uygulamasıdır. Bu nedenle Nielsen ve Chuang (2010, s. 234) Shor'u QFT ve QPE'nin güçlü bir uygulama örneği olarak nitelendirmektedir. Şekil 6.6'daki akış diyagramında görüldüğü üzere, kuantum adım (periyot bulma) ve klasik sayı kuramı adımları (GCD hesaplama) birlikte çalışarak faktörizasyonu tamamlar.



Şekil 6.6. Shor algoritması akış diyagramı. Kuantum adım (QPE ile periyot bulma) ve klasik adım (GCD ile çarpan hesaplama) birlikte çalışır (Shor, 1994; Nielsen ve Chuang, 2010).

6.8.3 Kriptografik Etkisi

RSA şifrelemesi, büyük sayıları çarpanlarına ayırmanın klasik bilgisayar için hesaplamalı olarak zor olduğu varsayımına dayanır; ECC ise ayrık logaritma probleminin zorluğuna dayanır (Rivest vd., 1978). Shor algoritması her iki problemi de polinom zamanda çözebildiğinden bu şifreleme sistemlerini teorik olarak kırar (Shor, 1994). Ancak teorik tehdit ile bugünkü pratik tehdit arasında önemli bir fark mevcuttur: gerçek anlamda büyük sayıları çarpanlarına ayırabilmek için binlerce hata-düzeltmeli mantıksal qubit gerekmektedir (Preskill, 2018). Bu durum post-kuantum kriptografi (PQC) standardizasyonunu hızlandırmış; NIST (2024) ilk PQC standartlarını yayımlamıştır.

Bu karşılaştırma Tablo 6.2'de özetlenmektedir.

Tablo 6.2. RSA ve ECC'ye yönelik kuantum tehdidi ile Grover'ın karesel kazanımının karşılaştırması (Shor, 1994; Grover, 1996; Rivest vd., 1978).

Problem	Klasik En İyi	Kuantum	Etki
Büyük tam sayı çarpanlara ayırma (RSA)	O(exp((log N)^{1/3}))	O((log N)^3)	RSA kırılabilir
Ayrık logaritma (ECC)	O(exp(√n))	O(n^3)	ECC kırılabilir
Yapılandırılmamış arama (Grover)	O(N)	O(√N)	Karesel kazanım

AKILDA TUT Shor faktör aramaz; periyot arar. Bu ayrım anlaşıldığında QFT ve QPE'nin neden bu algoritmada yer aldığı da anlaşılır.

6.9 Kavramsal Harita: Algoritmaları Birbirine Bağlamak

Bu bölümde ele alınan algoritmalar bağımsız teknikler değil; ortak bir temel sezginin farklı problem yapılarına uygulanmasıdır (Cleve vd., 1998). Bu sezgi şudur: kuantum hesaplama doğrudan cevap aramaz; doğru cevabın genliğini ölçüm öncesinde öne çıkarmak için faz ve girişimi kullanır (Nielsen ve Chuang, 2010, s. 248).

Deutsch–Jozsa bu ilkenin en sade örneğidir: tek bir oracle sorgusunda global fonksiyon yapısını ayırt eder (Deutsch ve Jozsa, 1992). Simon daha zengin bir gizli yapıyı lineer kısıtlar toplayarak ortaya çıkarır ve Shor'a zihinsel köprü kurar (Simon, 1997). Grover, yapılandırılmamış aramada oracle'ın faz işaretlemesini diffuser ile genlik büyütmeye dönüştürerek karesel kazanım sağlar (Grover, 1996). QFT, kuantum durum içindeki periyodik faz yapısını okunabilir temsilere çeviren temel alt yordamdır; QPE bu dönüşümü kullanarak özdeğer fazını nicel çıktıya taşır (Kitaev, 1995; Coppersmith, 2002). Shor ise QPE'nin faz ölçüm kapasitesini sayı kuramıyla birleştirerek faktörizasyona uygular (Shor, 1994).

Anlatırken her geçişe bir köprü cümlesi eklemek kavramsal akışı güçlendirir (Nielsen ve Chuang, 2010). Deutsch–Jozsa'dan Simon'a: "global ayrımdan gizli yapıya geçiyoruz". Simon'dan Grover'a: "promise problemden genel aramaya geçiyoruz". Grover'dan QFT'ye: "genlik büyütmeden fazı açıkça işleyen yapılara geçiyoruz". QPE'den Shor'a: "faz ölçümünü faktörizasyona uyguluyoruz".

Bölümün Özeti
Kuantum algoritmalar farklı problem yapılarını hedefler; ancak hepsinin kalbi aynıdır: oracle'ın bıraktığı faz izleri, girişim mekanizmasıyla doğru cevabın genliğine dönüştürülür (Nielsen ve Chuang, 2010; Cleve vd., 1998).

BÖLÜME AİT SUNUM SLAYTINA ERİŞİM İÇİN QR KOD



BÖLÜM 7

Kuantum Kapıları ve Kuantum Hesaplamanın Temelleri

7.1 Kuantum Kapılarına Giriş

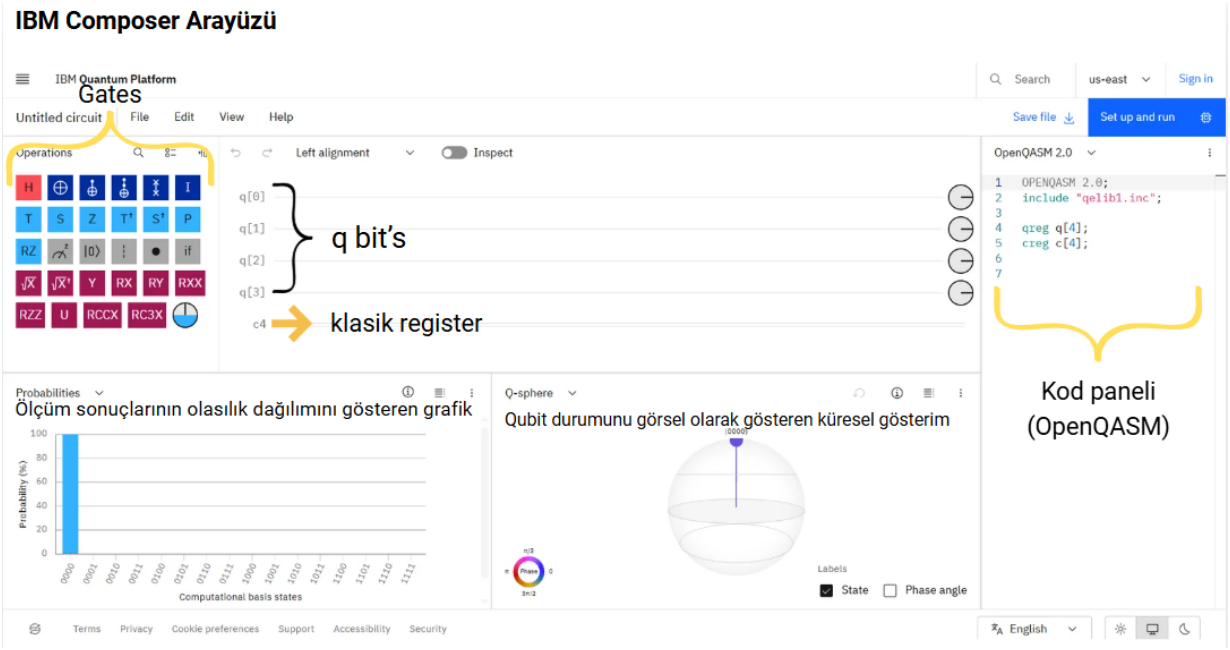
Klasik bilgisayarlarda bilgi, 0 veya 1 değerini alan bitlerle temsil edilir. Kuantum bilgisayarlarda ise bilginin temel birimi kübit (qubit) olup, $|0\rangle$ ve $|1\rangle$ durumlarının herhangi bir doğrusal bileşimi olarak bulunabilir. Matematiksel olarak bir kübitin durumu $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ biçiminde ifade edilir; burada α ve β karmaşık sayılardır ve $|\alpha|^2 + |\beta|^2 = 1$ normalizasyon koşulunu sağlar (Nielsen ve Chuang, 2010).

Kuantum kapıları, kübitlerin durumları üzerine etki eden üniter dönüşümlerdir. Klasik lojik kapılarından farklı olarak, tüm kuantum kapıları tersine çevrilebilir (reversible) olmalıdır; yani girdiden çıktıya olduğu gibi çıktıdan girdiye de geri dönülebilir. Bu özellik, kuantum mekaniğinin üniter evriminden kaynaklanır (Rieffel ve Polak, 2011).

7.1.1 IBM Quantum Composer Arayüzü

Bu bölümdeki kuantum devreleri görselleştirmek için IBM Quantum Composer kullanılmaktadır. Composer, kuantum kapılarını sürükle-bırak yöntemiyle bir devre üzerine yerleştirmeye olanak tanıyan görsel bir araçtır. Arayüzün temel bileşenleri şunlardır (Şekil 7.1):

- Kuantum telleri (q[0], q[1], …): Kübitlerin yer aldığı tek çizgili yataylardır; kapılar bu tellere uygulanır.
- Klasik register (c): Ölçüm sonuçlarının yazıldığı çift çizgili kayıtçıdır; yalnızca 0 veya 1 değeri tutar.
- Kapı paleti (Operations): H, X, Y, Z, S, T, RX, RY, RZ, CNOT, Toffoli, ölçüm, reset gibi kapıların bulunduğu menüdür.
- OpenQASM kod paneli: Devreye eklenen kapıların metinsel karşılığını (örn. h q[0]; cx q[0],q[1];) gösteren koddur.
- Olasılık (Probabilities) grafiği: Ölçüm sonuçlarının olasılık dağılımını histogram olarak gösterir.
- Q-sphere: Kübit durumunu küresel bir gösterimle (durum ve faz açısı dâhil) görselleştirir.



Şekil 7.1. IBM Quantum Composer arayüzünün genel görünümü (kaynak: sunum s. 2).

7.1.2 Tek Kübitlik Kapılar

7.1.2.1 Pauli Kapıları (X, Y, Z)

Pauli kapıları, kuantum hesaplamanın en temel yapı taşlarıdır ve Bloch küresi üzerinde rotasyonlara karşılık gelir (Nielsen ve Chuang, 2010).

Pauli-X Kapısı (NOT Kapısı): Klasik NOT kapısının kuantum karşılığıdır. $|0\rangle$ durumunu $|1\rangle$ durumuna, $|1\rangle$ durumunu da $|0\rangle$ durumuna dönüştürür. Matris gösterimi: X = [[0,1],[1,0]]. Bloch küresi üzerinde x ekseni etrafında π radyanlık bir rotasyona karşılık gelir (Şekil 7.2).

Pauli-Y Kapısı: Y = [[0, −i],[i, 0]]. Hem faz değişikliği hem de bit çevirme işlemi uygular. Bloch küresi üzerinde y ekseni etrafında π radyanlık rotasyona karşılık gelir.

Pauli-Z Kapısı (Faz Kapısı): Z = [[1,0],[0,−1]]. Hesaplama tabanındaki durumları değiştirmez ancak $|1\rangle$ durumuna −1 fazı ekler. Yani $Z|0\rangle = |0\rangle$ ve $Z|1\rangle = -|1\rangle$. Ölçüm olasılıklarını değiştirmez, yalnızca göreli fazı etkiler (Mermin, 2007).

7.1.2.2 Hadamard Kapısı (H)

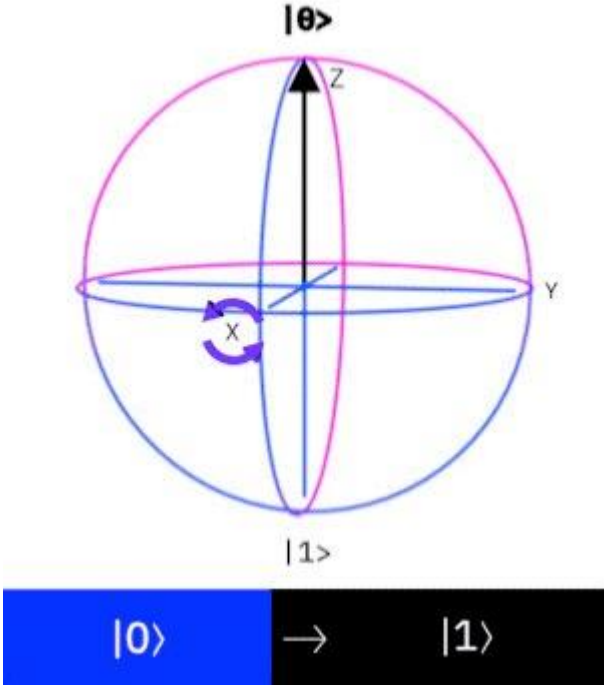
Hadamard kapısı, süperpozisyon oluşturmak için en sık kullanılan tek kübitlik kapıdır. Matris gösterimi $H = (1/\sqrt{2})[[1,1],[1,-1]]$ şeklindedir. $H|0\rangle = (|0\rangle+|1\rangle)/\sqrt{2}$ ve $H|1\rangle = (|0\rangle-|1\rangle)/\sqrt{2}$ dönüşümlerini gerçekleştirir. Bir kübiti kesin bir hesaplama taban durumundan, her iki ölçüm sonuçlarının eşit olasılıkla görüleceği bir süperpozisyona taşır (Şekil 7.3) (Nielsen ve Chuang, 2010).

Hadamard kapısının Pauli kapılarıyla önemli bir ilişkisi vardır: HXH = Z ve HZH = X. Bu eşitlik, Hadamard kapısının X ve Z tabanları arasında geçiş sağladığını gösterir.

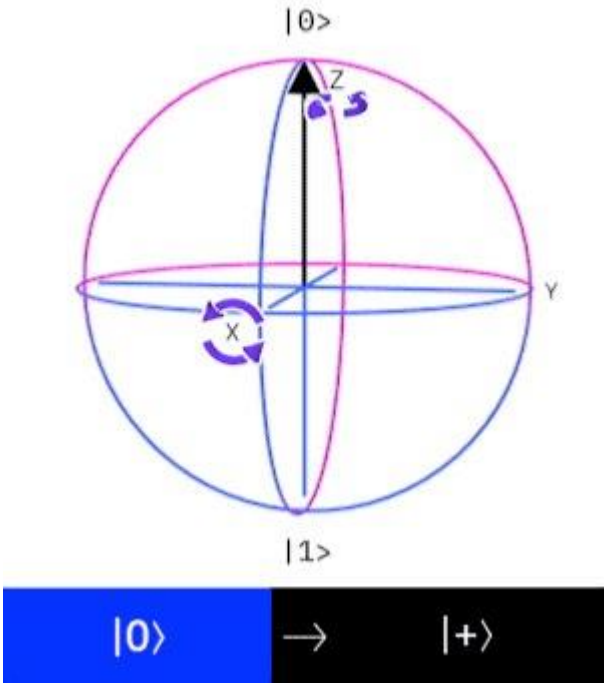
Tablo 7.1'de temel tek kübitlik kapılar matris, etki ve Bloch rotasyonu açısından özetlenmektedir.

Tablo 7.1. Temel tek kübitlik kapıların matris, etki ve Bloch rotasyonu özeti.

Kapı	Matris	Etki	Bloch Rotasyonu
X	[[0,1],[1,0]]	$\|0\rangle \leftrightarrow \|1\rangle$	x ekseni, π rad
Y	[[0,−i],[i,0]]	Bit+Faz çevirme	y ekseni, π rad
Z	[[1,0],[0,−1]]	$\|1\rangle \rightarrow -\|1\rangle$	z ekseni, π rad
H	$(1/\sqrt{2})$[[1,1],[1,−1]]	Süperpozisyon	x+z ekseni, π rad



Şekil 7.2. Pauli kapıları; X (NOT) Bloch küresi ve matris uygulaması, Y ve Z kapıları Bloch gösterimi (kaynak: sunum s. 3-4, 37-38).



Şekil 7.3. Hadamard kapısı; Bloch küresinde süperpozisyona geçiş ve |+⟩, |−⟩ durumları (kaynak: sunum s. 14, 19).

7.1.2.3 Faz Kapıları: S ve T

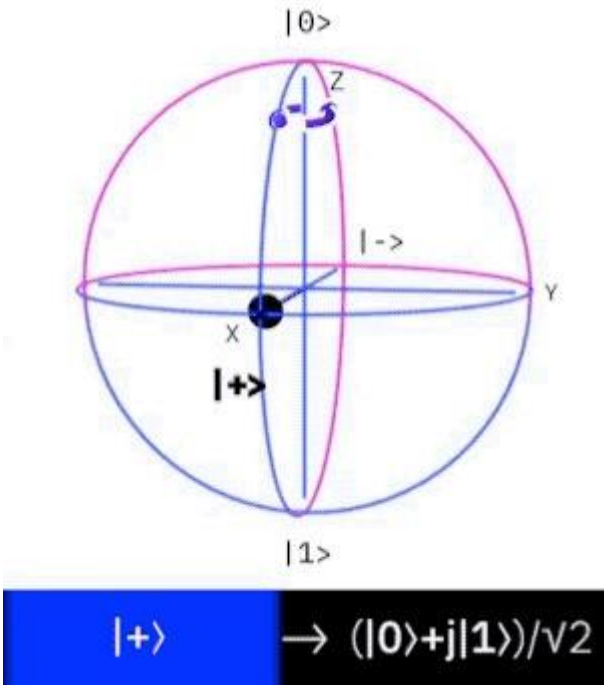
S kapısı, |1⟩ durumuna π/2 (yani i çarpanı) faz ekleyen kapıdır ve Z kapısının kareköküdür: $S^2 = Z$. Matris gösterimi S = [[1, 0],[0, i]] şeklindedir. Bit değiştirmez, yalnızca |1⟩ bileşenine 90° (π/2) faz ekler; Bloch küresinde z ekseni etrafında π/2'lik dönüşe karşılık gelir. RZ ile ilişkisi global faz farkıyla eşdeğerdir: S = e^(iπ/4)·RZ(π/2).

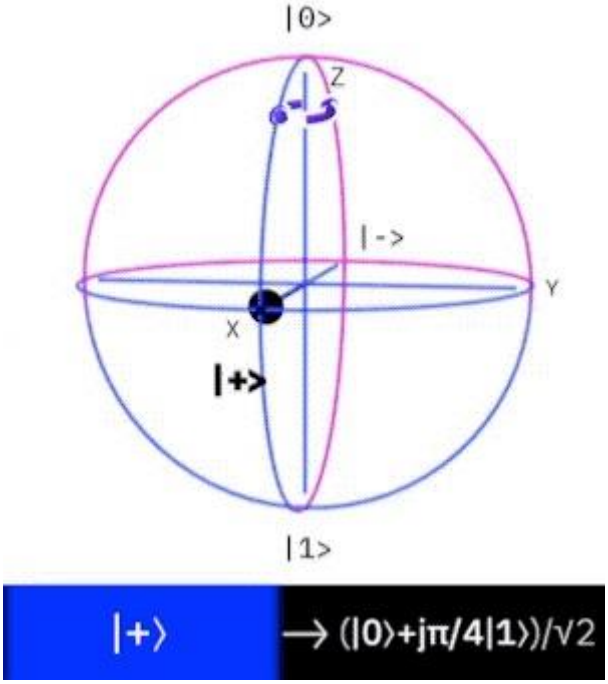
T kapısı, |1⟩ durumuna π/4 faz ekleyen kapıdır ve S kapısının kareköküdür: $T^2 = S$. Matris gösterimi T = [[1, 0],[0, e^(iπ/4)]] şeklindedir. Bloch küresinde z ekseni etrafında π/4'lük dönüştür. "π/8 kapısı" olarak da anılır.

Bu kapıların tersleri (Hermitik eşlenikleri) S† ve T† şeklinde gösterilir; sırasıyla −π/2 ve −π/4 faz ekler ve S†·S = I, T†·T = I koşulunu sağlar.

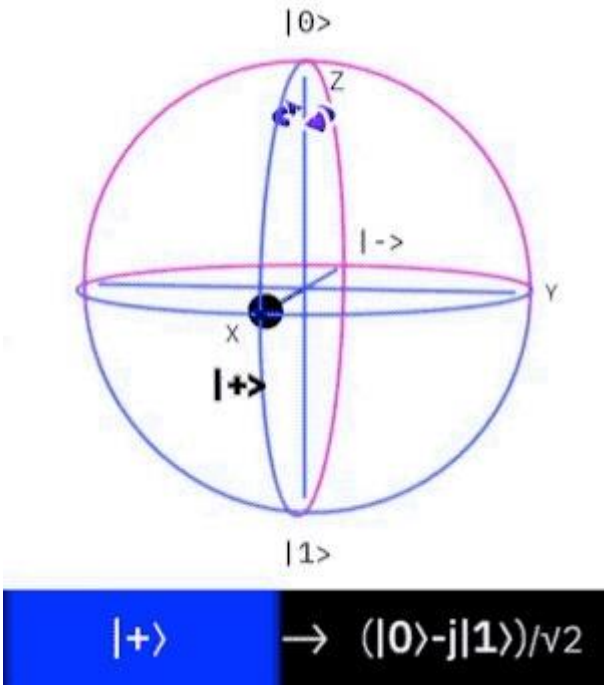
Faz hiyerarşisi: Bu kapılar bir karekök zinciri oluşturur: $T^2 = S$, $S^2 = Z$, $Z^2 = I$; dolayısıyla $T^4 = Z$ ve $T^8 = I$. Açısal olarak T (π/4) → S (π/2) → Z (π) → I (2π) her adımda ikiye katlanır (Şekil 7.4).

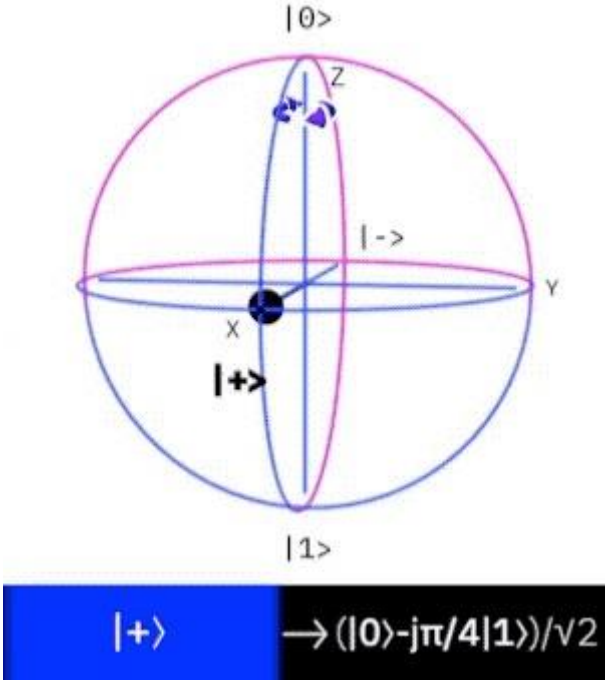
Evrensellik açısından önemi: Clifford kapıları (H, S, CNOT) tek başına evrensel değildir; Gottesman–Knill teoremine göre yalnızca Clifford kapılarından oluşan devreler klasik bilgisayarda verimli olarak simüle edilebilir (Gottesman, 1998). T kapısı Clifford grubunun dışındadır ve eklendiğinde {H, T, CNOT} kümesi evrensel hâle gelir; Solovay–Kitaev teoremine göre bu küme herhangi bir üniter dönüşümü keyfi hassasiyetle yaklaşık olarak gerçekleştirebilir (Nielsen ve Chuang, 2010). Hata toleranslı hesaplamada T kapısı, magic state distillation gerektirdiği için en maliyetli kapıdır; bu nedenle devre optimizasyonunda "T-sayısı" (T-count) temel maliyet ölçütüdür (Nielsen ve Chuang, 2010).



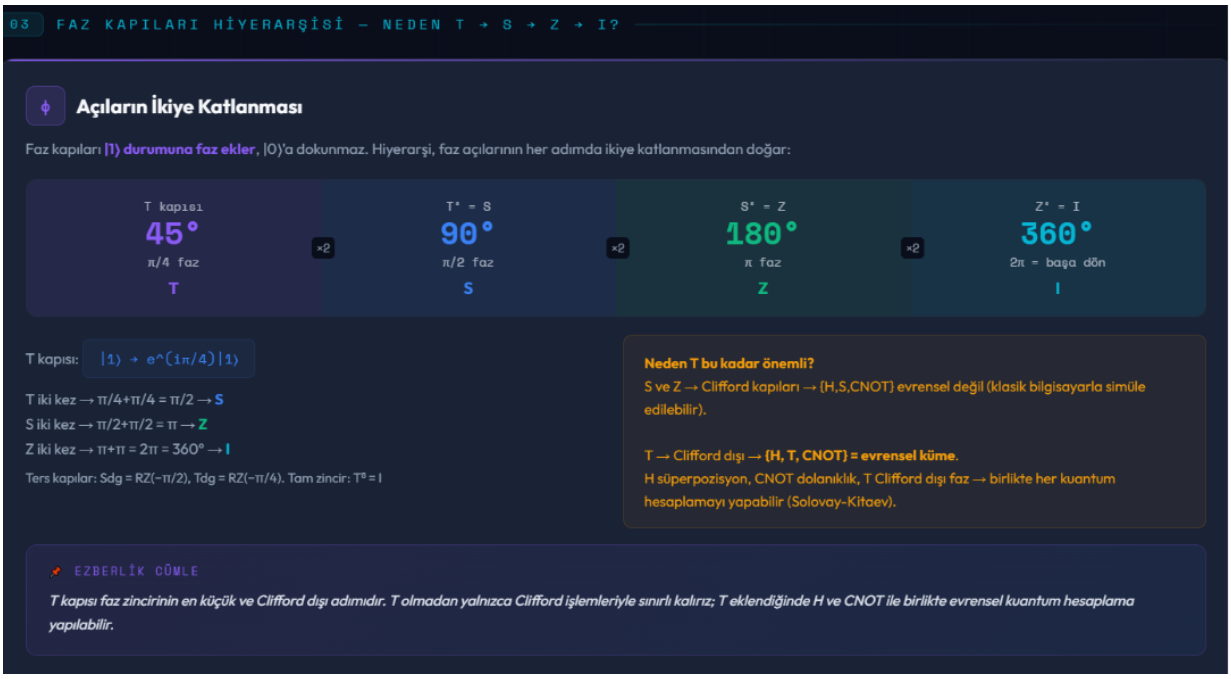


S Kapısı T Kapısı





SDG Kapısı TDG Kapısı



Şekil 7.4. Faz kapıları S, S†, T, T† Bloch gösterimleri ve T→S→Z→I faz hiyerarşisi (kaynak: sunum s. 39-43).

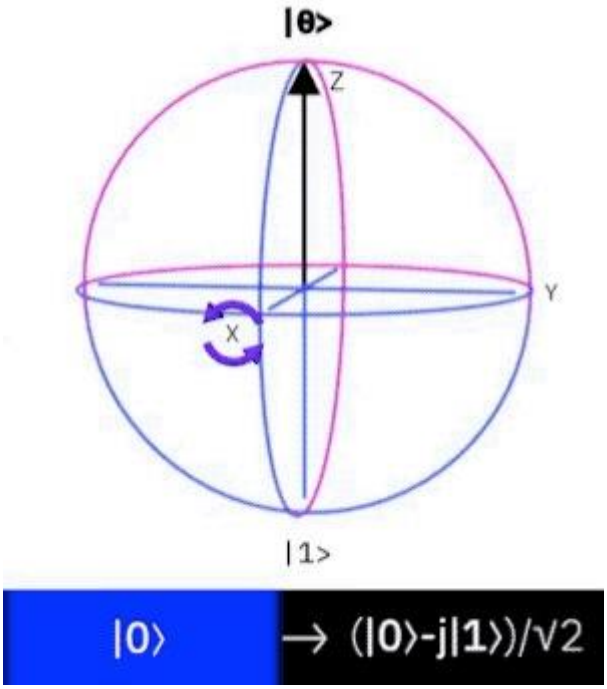
7.1.2.4 Parametreli Döndürme Kapıları (RX, RY, RZ)

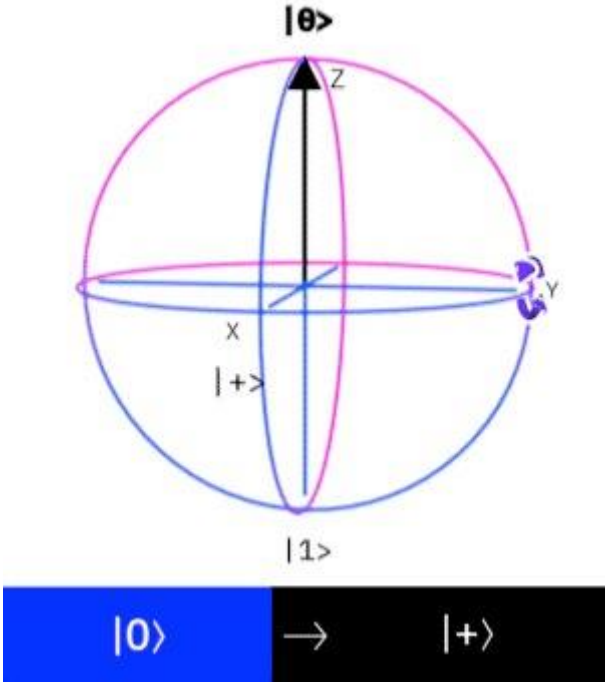
Pauli kapıları (X, Y, Z) Bloch küresi üzerinde sabit π radyanlık (180°) rotasyonlar uygularken, parametreli döndürme kapıları keyfi bir θ açısı kadar dönüş sağlar. RX(θ), RY(θ) ve RZ(θ) kapıları kübiti sırasıyla x, y ve z ekseni etrafında θ radyan döndürür (Nielsen ve Chuang, 2010). θ = π verildiğinde bu kapılar global faz farkı dışında ilgili Pauli kapısına indirgenir.

Bloch küresi bir dünya küresine benzetilirse RX doğu–batı, RY kuzey–güney, RZ ise yerinde (eksen etrafında) dönmeye karşılık gelir. Bu üç rotasyonun birleşimiyle küre üzerindeki herhangi bir noktaya ulaşılabilir (Şekil 7.5).

Kritik bir ayrım vardır: RX ve RY kapıları kübitin kutupsal konumunu (|0⟩ ve |1⟩ bileşenlerinin ağırlıklarını) değiştirdiğinden ölçüm olasılıklarını etkileyebilir. RZ ise köşegen bir matris olduğundan yalnızca göreli fazı değiştirir ve tek başına histogramı değiştirmez (bkz. Bölüm 7.11).

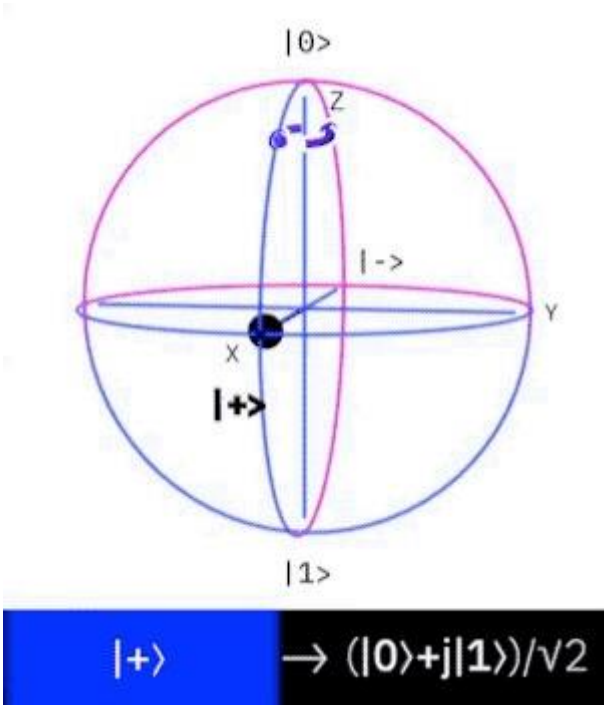
Yaygın kullanılan birçok kapı RZ'nin özel durumudur: RZ(π) = Z, RZ(π/2) = S, RZ(−π/2) = S†, RZ(π/4) = T, RZ(−π/4) = T† (global faz farkıyla).





RX Kapısı RY Kapısı

RZ Kapısı



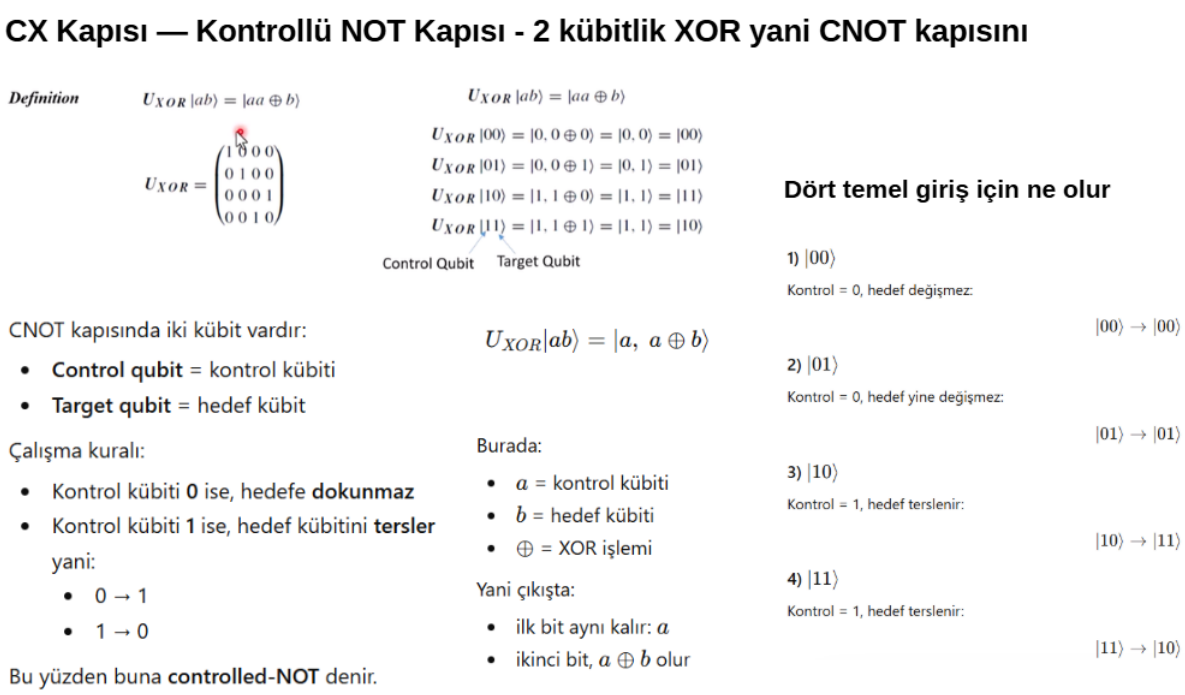
Şekil 7.5. Parametreli döndürme kapıları RX, RY, RZ; Bloch küreleri ve histogram örnekleri (kaynak: sunum s. 32, 34-36).

7.1.3 Çok Kübitlik Kapılar

7.1.3.1 CNOT (Kontrollü-NOT) Kapısı

CNOT kapısı, iki kübitlik en temel kapıdır ve kuantum hesaplamanın olmazsa olmazıdır. Bir kontrol kübiti ve bir hedef kübitten oluşur. Kontrol kübiti |1⟩ durumundaysa hedef kübitin durumunu çevirir, |0⟩ durumundaysa hedef kübiti değiştirmez. Dönüşüm tablosu: |00⟩ → |00⟩, |01⟩ → |01⟩, |10⟩ → |11⟩, |11⟩ → |10⟩ (Şekil 7.6) (Nielsen ve Chuang, 2010).

CNOT kapısı, doğrudan klasik XOR işlemine karşılık gelir: hedef kübitin çıkışı, kontrol ve hedef kübitlerin XOR'ıdır. Bu özellik, klasik lojik kapıların kuantum eşdeğerlerini oluşturmak için temel yapı taşı olarak kullanılır.



Şekil 7.6. CNOT kapısı; dört temel giriş dönüşümü ve 4×4 matris gösterimi (kaynak: sunum s. 46-47).

7.1.3.2 Toffoli Kapısı (CCNOT)

Toffoli kapısı, iki kontrol kübiti ve bir hedef kübitten oluşur. Her iki kontrol kübiti de |1⟩ durumundaysa hedef kübitin durumunu çevirir. Bu kapı, tersine çevrilebilir hesaplamanın evrensel kapısıdır; yani herhangi bir klasik Boolean fonksiyonu yalnızca Toffoli kapıları kullanılarak gerçekleştirilebilir (Nielsen ve Chuang, 2010).

7.1.3.3 Identity (I) Kapısı

Identity kapısı, kübitin durumunu hiçbir şekilde değiştirmeyen kapıdır: I = [[1, 0],[0, 1]]. Herhangi bir durum vektörüyle çarpıldığında sonuç aynı vektördür: I|ψ⟩ = |ψ⟩. Süperpozisyon dâhil her durumu olduğu gibi bırakır. Devrede bir zaman aralığı boyunca boş işlem (idle) göstermek veya devre zamanlamasını hizalamak amacıyla kullanılır. Bu matris, X kapısının üniterlik ispatında da karşımıza çıkmıştır: XX = I (Şekil 7.7).



Şekil 7.7. Identity (I) kapısının Composer gösterimi (kaynak: sunum s. 29-31).

7.1.3.4 Bariyer (Barrier)

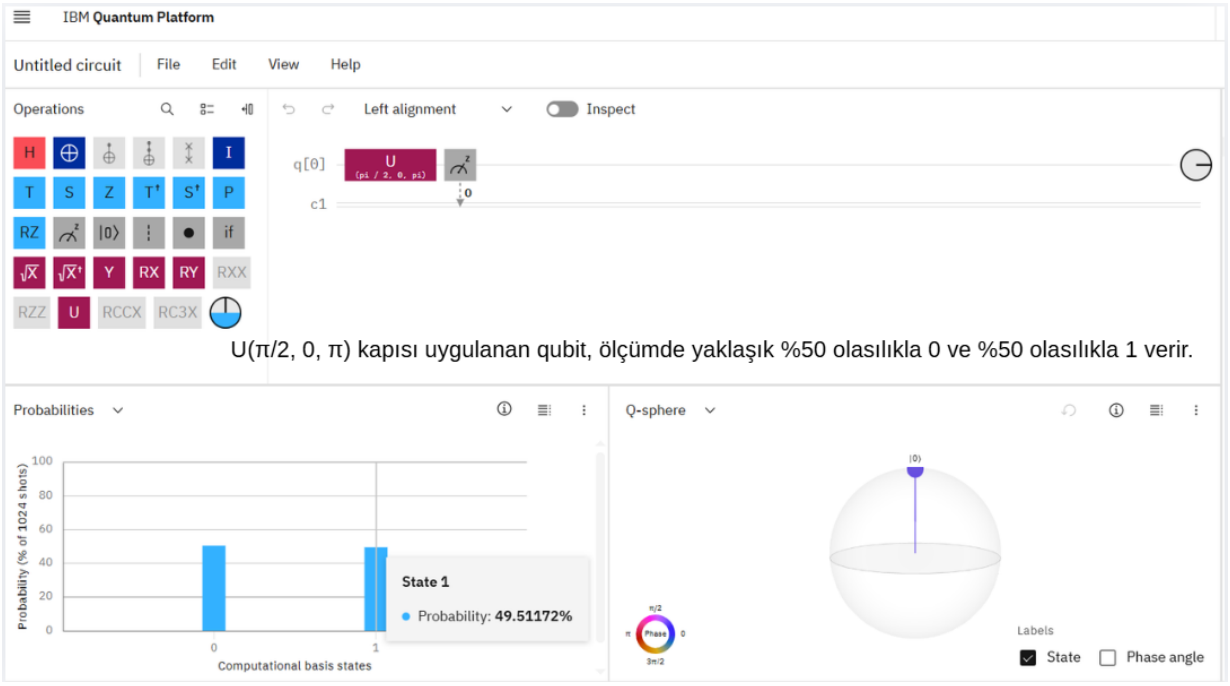
Bariyer bir kapı değildir; kübite herhangi bir fiziksel işlem uygulamaz ve durumunu değiştirmez. İki işlevi vardır: (i) devredeki farklı adımları görsel olarak ayırarak okunabilirliği artırmak, (ii) derleyici (transpiler) optimizasyonunu sınırlamak; bariyerin iki tarafındaki kapıların birleştirilmesini veya yeniden sıralanmasını engellemek. Identity kapısından temel farkı, Identity'nin devrede gerçek (etkisi olmasa da) bir kuantum işlemi olarak yer alması, bariyerin ise bir işlem değil yalnızca derleyici ve görsel düzeyde bir ayırıcı olmasıdır (Şekil 7.8).



Şekil 7.8. Bariyer (Barrier) sembolünün devre üzerindeki gösterimi (kaynak: sunum s. 26).

7.1.3.5 Genel Tek Kübit Kapısı (U)

U kapısı, tek bir kübite uygulanabilecek herhangi bir üniter dönüşümü tek başına tanımlayabilen üç parametreli genel kapıdır: U(θ, φ, λ). Burada θ Bloch küresindeki kutupsal açıyı, φ uygulama öncesi z-ekseni dönüşünü, λ ise uygulama sonrası z-ekseni dönüşünü temsil eder. Bu üç açının uygun değerleriyle X, Y, Z, H, S ve T dâhil tüm tek kübitlik kapılar U kapısının özel durumları olarak ifade edilebilir: örneğin X = U(π, 0, π), H = U(π/2, 0, π), Z = U(0, 0, π), S = U(0, 0, π/2), T = U(0, 0, π/4) (Şekil 7.9) (Nielsen ve Chuang, 2010).



Şekil 7.9. Genel U(θ, φ, λ) kapısı sembolü ve U(π/2, 0, π) histogram örneği (kaynak: sunum s. 44-45).

7.2 CNOT ve Pauli Kapıları ile Klasik Lojik Devrelerin Oluşturulması

Kuantum kapılarının tersine çevrilebilir doğası nedeniyle, klasik AND ve OR gibi geri dönüşsüz kapılar doğrudan uygulanamaz. Ancak yardımcı (ancilla) kübitler kullanılarak bu kapıların tersine çevrilebilir karşılıkları oluşturulabilir (Rieffel ve Polak, 2011).

7.2.1 Toffoli Kapısı ile AND İşlemi

AND kapısı, Toffoli (CCNOT) kapısı kullanılarak doğrudan gerçekleştirilebilir. İki giriş kübiti |a⟩ ve |b⟩ kontrol kübitleri olarak, |0⟩ durumuna hazırlanmış bir yardımcı kübit ise hedef kübit olarak kullanılır. Toffoli kapısı uygulandığında, hedef kübitin durumu a AND b sonucunu verir: |a, b, 0⟩ → |a, b, a∧b⟩. Yalnızca a=1 ve b=1 olduğunda hedef kübit |1⟩ olur (Nielsen ve Chuang, 2010).

7.2.2 CNOT ve Toffoli ile OR İşlemi

OR kapısı, De Morgan yasasından yararlanılarak oluşturulur: a OR b = NOT(NOT(a) AND NOT(b)). Uygulama adımları: (i) Her iki giriş kübitine Pauli-X (NOT) kapısı uygulanır, (ii) Toffoli kapısı ile AND işlemi yapılır, (iii) Sonuç kübitine Pauli-X uygulanarak NOT alınır, (iv) Giriş kübitlerine tekrar Pauli-X uygulanarak orijinal değerleri geri yüklenir. Böylece |a, b, 0⟩ → |a, b, a∨b⟩ dönüşümü elde edilir (Nielsen ve Chuang, 2010).

7.2.3 XOR ile CNOT İşlemi

XOR, kuantum devrelerde en basit şekilde gerçekleştirilen klasik lojik işlevdir. Tek bir CNOT kapısı doğrudan XOR işlemini verir: kontrol kübiti |a⟩ olduğunda, hedef kübit |b⟩ durumundan |a⊕b⟩ durumuna dönüşür. Bu, CNOT kapısının doğal davranışıdır.

Tablo 7.2'de klasik lojik işlevlerin kuantum devre gerçeklemeleri özetlenmektedir.

Tablo 7.2. Klasik lojik işlevlerin kuantum devre gerçeklemeleri.

Lojik İşlev	Kuantum Gerçekleme	Dönüşüm	Gerekli Kapılar
AND	Toffoli	|a,b,0⟩→|a,b,a∧b⟩	1 Toffoli

Lojik İşlev	Kuantum Gerçekleme	Dönüşüm	Gerekli Kapılar
OR	X + Toffoli + X	$\|a,b,0\rangle \rightarrow \|a,b,a \vee b\rangle$	5 Pauli-X + 1 Toffoli
XOR	CNOT	$\|a,b\rangle \rightarrow \|a,a \oplus b\rangle$	1 CNOT
NOT	Pauli-X	$\|a\rangle \rightarrow \|\neg a\rangle$	1 Pauli-X

7.2.4 Lojik Kapıların Doğruluk Tabloları ve Kuantum Devreleri

Aşağıdaki tablolar, klasik lojik kapıların kuantum kapılarıyla gerçeklenmesini kübit düzeyinde gösterir; ilgili IBM Composer devre görselleri Şekil 7.10'da verilmiştir (slayt sunumundaki 49–56. sayfalardan derlenmiştir).

7.2.4.1 NOT → Pauli-X Kapısı

Klasik NOT kapısı bir bitin değerini tersine çevirir (0→1, 1→0). Kuantum karşılığı Pauli-X kapısıdır ve hesaplama tabanı durumları arasında geçiş yapar: $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$. Matris gösterimi X = [[0,1],[1,0]] olup Bloch küresinde x ekseni etrafında π radyanlık (180°) bir dönüşe karşılık gelir.

Tablo 7.3'te NOT işleminin Pauli-X kapısıyla doğruluk dönüşümü gösterilmektedir.

Tablo 7.3. NOT işleminin Pauli-X kapısıyla doğruluk dönüşümü.

Giriş $\|q\rangle$	Çıkış $X\|q\rangle$
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$

7.2.4.2 AND → Toffoli (CCNOT) Kapısı

AND kapısı iki giriş alır ve her ikisi de 1 ise çıkış 1 olur. Kuantum bilgisayarlarda AND işlemi Toffoli (CCNOT = Controlled-Controlled-NOT) kapısı ile gerçekleştirilir. Bu kapı üç kübit üzerinde çalışır: q_0 (Kontrol 1 / Giriş A), q_1 (Kontrol 2 / Giriş B) ve q_2 (Hedef / Çıkış; başlangıçta $|0\rangle$ olmalı). Her iki kontrol kübiti de $|1\rangle$ ise hedef kübit terslenir; başlangıçta $q_2 = |0\rangle$ olduğunda sonuç tam olarak AND mantığını verir.

Tablo 7.4'te AND işleminin Toffoli kapısıyla gerçekleştirilmesi gösterilmektedir.

Tablo 7.4. AND işleminin Toffoli kapısıyla gerçekleştirilmesi.

q_0 (A)	q_1 (B)	q_2 Giriş	q_2 Çıkış
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$

Önemli: Toffoli kapısı evrensel bir klasik kapıdır; yalnızca Toffoli kullanılarak tüm klasik mantık devreleri inşa edilebilir. Üstelik tersinir (reversible) olduğu için kuantum hesaplamanın üniterlik gereksinimini karşılar.

7.2.4.3 OR → De Morgan Yaklaşımı (X + Toffoli + X)

OR kapısının doğrudan bir kuantum karşılığı yoktur; De Morgan yasası kullanılarak NOT ve AND kapılarından türetilir: A OR B = NOT(NOT(A) AND NOT(B)). Kuantum devre adımları aşağıdaki gibidir:

Adım 1: q_0 ve q_1 kübitlerinin her birine Pauli-X (NOT) uygulanır.

Adım 2: Toffoli kapısı uygulanır (q_0, q_1 kontrol; q_2 hedef). Bu aşamada q_2, NOT(A) AND NOT(B) değerini taşır.

Adım 3: q_2'ye Pauli-X uygulanır → q_2 = NOT(NOT(A) AND NOT(B)) = A OR B.

Adım 4 (opsiyonel): q_0 ve q_1 orijinal değerlerine döndürmek için tekrar Pauli-X uygulanır (uncomputation).

Sonuç: 3 Pauli-X + 1 Toffoli kapısıyla OR işlemi gerçekleştirilmiş olur. Aşağıdaki tablo q_2 çıkış kübitinin (A OR B) değerini gösterir.

Tablo 7.5'te OR işleminin De Morgan yaklaşımıyla gerçekleştirilmesi gösterilmektedir.

Tablo 7.5. OR işleminin De Morgan yaklaşımıyla gerçekleştirilmesi.

q_0 (A)	q_1 (B)	q_2 Çıkış (A OR B)
|0⟩	|0⟩	|0⟩
|0⟩	|1⟩	|1⟩
|1⟩	|0⟩	|1⟩
|1⟩	|1⟩	|1⟩

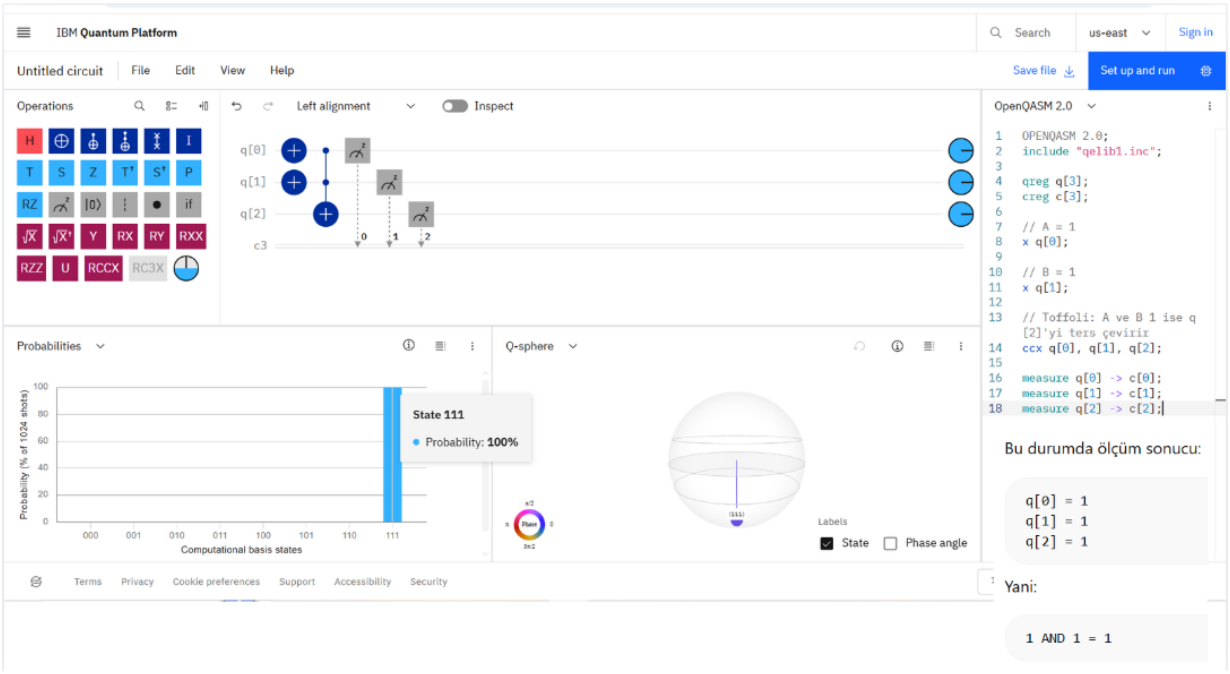
7.2.4.4 XOR → CNOT Kapısı

XOR (exclusive-OR) kapısı, kuantumda en doğal karşılığı bulan kapıdır. CNOT kapısı tam olarak XOR işlemi yapar: kontrol kübiti |1⟩ ise hedef kübitin değerini çevirir, |0⟩ ise dokunmaz. Hedef kübit B değeriyle başlatıldığında çıkış A ⊕ B olur.

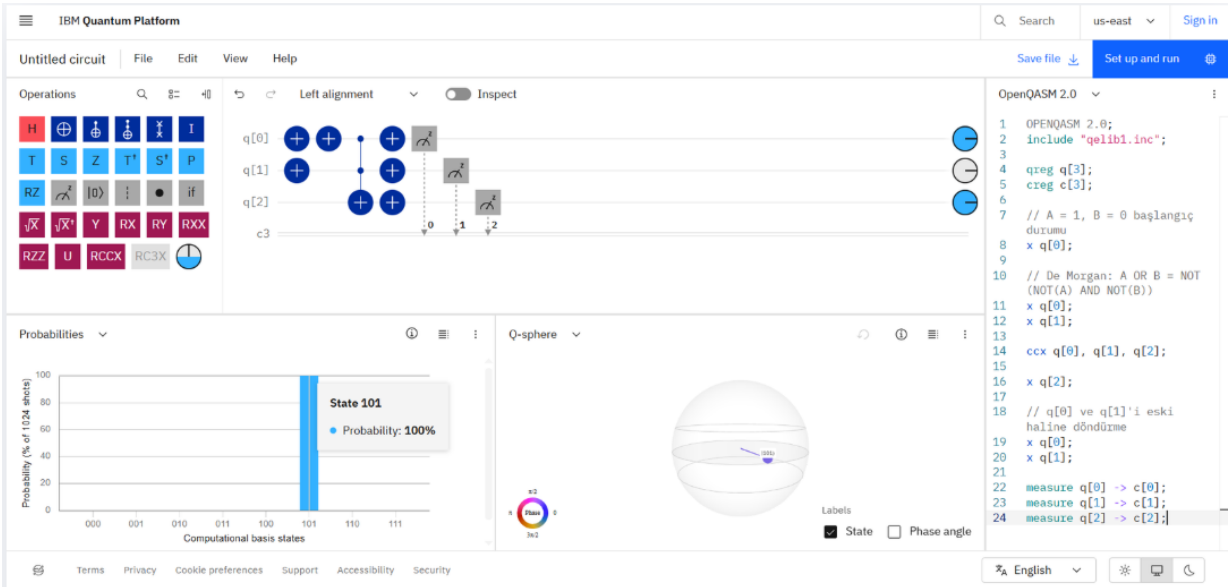
Tablo 7.6'da XOR işleminin CNOT kapısıyla gerçekleştirilmesi gösterilmektedir.

Tablo 7.6. XOR işleminin CNOT kapısıyla gerçekleştirilmesi.

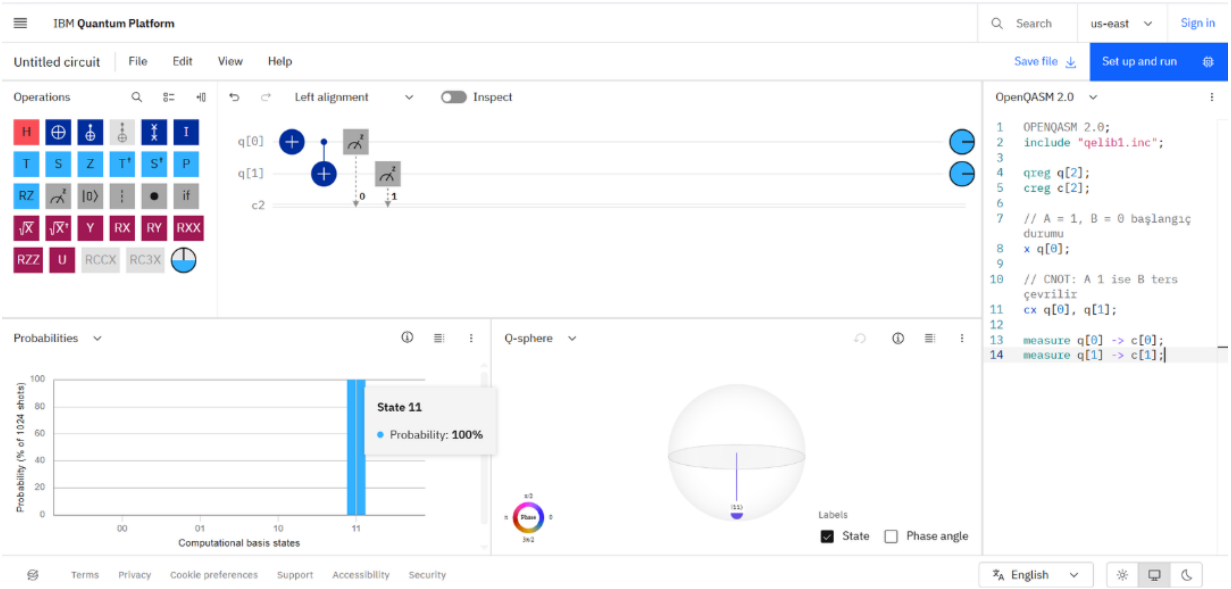
q_0 (A)	q_1 Giriş (B)	q_1 Çıkış (A ⊕ B)
|0⟩	|0⟩	|0⟩
|0⟩	|1⟩	|1⟩
|1⟩	|0⟩	|1⟩
|1⟩	|1⟩	|0⟩


IBM Quantum Platform
Search
us-east
Sign in
Untitled circuit
File
Edit
View
Help
Save file
Set up and run
Operations
Left alignment
Inspect
OpenQASM 2.0
1 OPENQASM 2.0;
2 include "qelib1.inc";
3
4 qreg q[3];
5 creg c[3];
6
7 // A = 1
8 x q[0];
9
10 // B = 1
11 x q[1];
12
13 // Toffoli: A ve B 1 ise q [2]'yi ters çevirir
14 ccx q[0], q[1], q[2];
15
16 measure q[0] -> c[0];
17 measure q[1] -> c[1];
18 measure q[2] -> c[2];
Probabilities
Q-sphere
State 111
Probability: 100%
Computational basis states
Labels
State
Phase angle
Terms
Privacy
Cookie preferences
Support
Accessibility
Security
Bu durumda ölçüm sonucu:
q[0] = 1
q[1] = 1
q[2] = 1
Yani:
1 AND 1 = 1


IBM Quantum Platform
Search
us-east
Sign in
Untitled circuit
File
Edit
View
Help
Save file
Set up and run
Operations
Left alignment
Inspect
OpenQASM 2.0
1 OPENQASM 2.0;
2 include "qelib1.inc";
3
4 qreg q[3];
5 creg c[3];
6
7 // q[0] = A kontrol qubit
8 // q[1] = B kontrol qubit
9 // q[2] = hedef qubit / çıktı
10
11 ccx q[0], q[1], q[2];
12
13 measure q[0] -> c[0];
14 measure q[1] -> c[1];
15 measure q[2] -> c[2];
q[0]=0 ve q[1]=0 olduğu için Toffoli kapısı çalışmaz. q[2] değişmeden 0 kalır. Bu yüzden ölçüm sonucu 000 çıkar.
Probabilities
Q-sphere
State 000
Probability: 100%
Computational basis states
Labels
State
Phase angle
Terms
Privacy
Cookie preferences
Support
Accessibility
Security
English



Başta x q[0]; uygulanarak A değeri 1 yapılır, B ise 0 kalır. De Morgan dönüşümü sonunda q[2] çıkış qubiti 1 olur. Yani devre 1 OR 0 = 1 sonucunu verir.



q[0] kontrol qubiti A'dır, q[1] hedef qubit B'dir. A=1 olduğu için CNOT kapısı q[1]'i 0'dan 1'e çevirir. Bu yüzden sonuç 11 olur; çıkış değeri A ⊕ B = 1'dir.

Şekil 7.10. Klasik lojik kapıların IBM Composer devre örnekleri; AND, OR ve XOR (kaynak: sunum s. 50-56).

7.3 Kuantum Ölçümü (Measurement)

Kuantum ölçümü, bir kübitin süperpozisyon durumundan kesin bir klasik değere (0 veya 1) çökmesini sağlayan işlemdir. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ durumundaki bir kübit ölçüldüğünde, $|\alpha|^2$ olasılıkla $|0\rangle$ ve $|\beta|^2$ olasılıkla $|1\rangle$ sonucu elde edilir. Ölçüm işlemi geri dönüşsüzdür; ölçüm sonrasında süperpozisyon yok olur ve kübit ölçülen duruma çöker. Bu, kuantum mekaniğinin Born kuralı olarak bilinir (Şekil 7.11) (Nielsen ve Chuang, 2010).

7.3.1 Ölçümün Devre İçindeki Konumu

Ölçümün devrenin neresine yerleştirildiği, hesaplamanın sonucunu temelden etkiler. Devre ortasında yapılan ölçüm (mid-circuit measurement), kübiti klasik bir değere çökertir ve o kübit üzerindeki tüm kuantum bilgi (süperpozisyon, dolanıklık) kaybolur. Bu nedenle kuantum algoritmalarında ölçüm genellikle devrenin en sonuna konulur; ancak bazı algoritmalar (teleportasyon, kuantum hata düzeltme) devrenin ortasında biçimleştirme amacıyla ölçüm kullanır (Rieffel ve Polak, 2011).

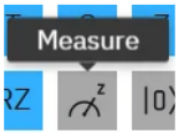
7.3.2 Çok Sayıda Tekrar (Shots) ve İstatistiksel Sonuçlar

Kuantum hesaplamanın olasılıksal doğası nedeniyle, bir kuantum devresinin tek bir çalıştırılması (shot) yalnızca tek bir örneklem sağlar. İstatistiksel olarak anlamlı sonuçlar elde etmek için devre çok sayıda tekrarlanır; örneğin 1000 veya 8192 kez. Bu tekrarlar sonucunda oluşan histogram, her olası sonucun görülme sıklığını gösterir.

Bir Bell durumu devresi 1000 kez çalıştırıldığında, ideal simülatörde yaklaşık 500 kez |00⟩ ve 500 kez |11⟩ sonucu görülür. Gerçek donanımda ise gürültü ve dekoherans nedeniyle az sayıda |01⟩ ve |10⟩ sonucu da ortaya çıkabilir; ancak baskın sonuçlar beklenen |00⟩ ve |11⟩ durumları olur (hata oranı kullanılan donanıma göre değişir). İşte "bazı hatalar olsa da çoğunlukla cevabı 1'dir" ifadesinin anlamı budur: olasılık dağılımı beklenen sonuca yoğunlaşmıştır.

Ölçüm Kapısı — Measurement Gate

Composer'daki gösterimi



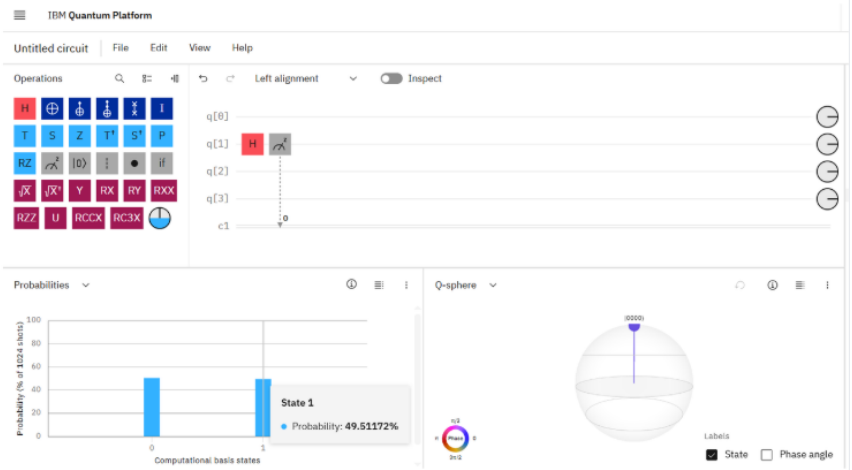
Olasılıklar nereden geliyor?

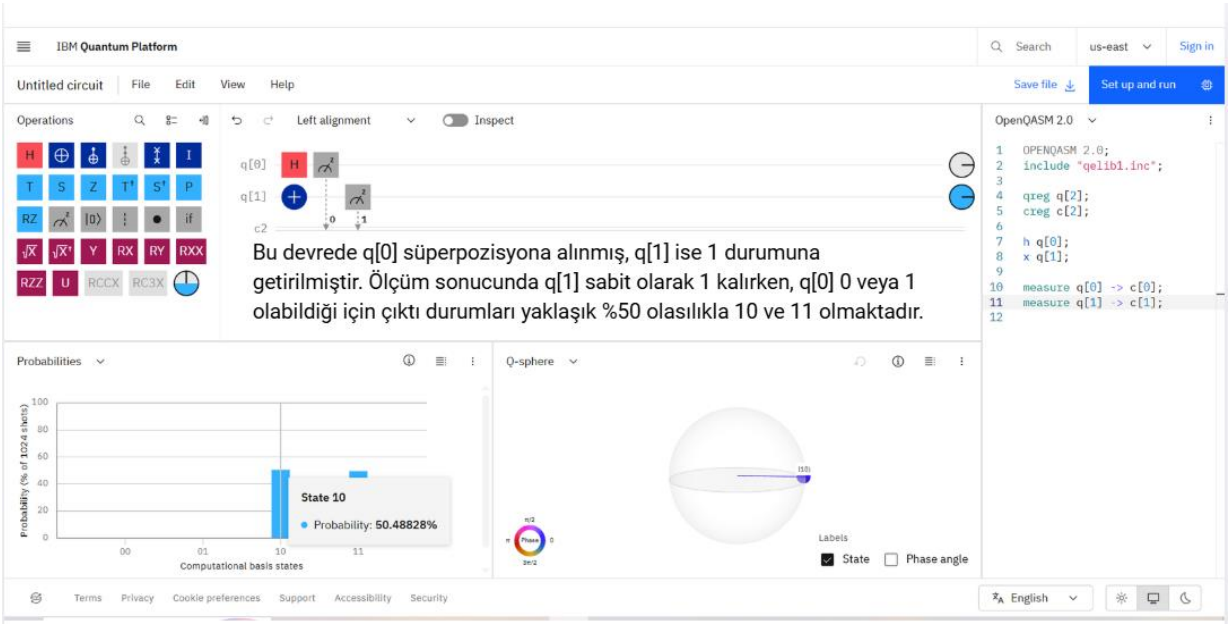
Qubitin durumu |ψ⟩ = α|0⟩ + β|1⟩ ise:

- 0 gelme olasılığı = |α|²
- 1 gelme olasılığı = |β|²

Örnek: Hadamard sonrası qubit (1/√2)|0⟩ + (1/√2)|1⟩ durumunda. Ölçersen:

- %50 ihtimalle 0
- %50 ihtimalle 1





Şekil 7.11. Ölçüm (Measurement) kapısı, Composer gösterimi ve süperpozisyon ölçümünde %50-%50 histogram (kaynak: sunum s. 22-25).

7.4 Bell Durumları ve Kuantum Dolanıklık

Kuantum dolanıklık (entanglement), iki veya daha fazla kübitin birbirine bağımlı hale geldiği ve tek tek kübitlerin durumlarının bağımsız olarak tanımlanamadığı bir olgudur. Bu, klasik fiziğin hiçbir karşılığı olmayan, tamamen kuantum mekaniksel bir özelliktir. Einstein, Podolsky ve Rosen (EPR) bu durumu 1935'te "uzaktan ürkütücü eylem" (spooky action at a distance) olarak nitelendirmiştir. 1964'te John Bell, yerel gizli değişkenlerle açıklanabilecek korelasyonların üst sınırını belirleyen Bell eşitsizliklerini türetmiş ve kuantum mekaniğinin bu sınırları aştığını göstermiştir (Bell, 1964).

7.4.1 Bell Durumlarının Oluşturulması

Bell durumları, maksimal dolanıklı iki kübitlik durumlardır. En bilinen Bell durumu $|\Phi^+\rangle = (|00\rangle+|11\rangle)/\sqrt{2}$ olup, bir Hadamard kapısı ve ardından bir CNOT kapısı ile oluşturulur (Nielsen ve Chuang, 2010):

Adım 1: $|00\rangle$ durumundan başla.

Adım 2: İlk kübite Hadamard kapısı uygula → $(|0\rangle+|1\rangle)/\sqrt{2} \otimes |0\rangle = (|00\rangle+|10\rangle)/\sqrt{2}$.

Adım 3: CNOT uygula (ilk kübit kontrol) → $(|00\rangle+|11\rangle)/\sqrt{2} = |\Phi^+\rangle$.

Bu durumda, ilk kübit ölçüldüğünde 0 bulunursa ikinci kübit kesinlikle 0, 1 bulunursa ikinci kübit kesinlikle 1 olur. Bu korelasyon, kübitlerin arasındaki mesafeden bağımsızdır (Şekil 7.12).

7.4.2 Dolanıklığın Ölçümle Çözülmesi (Bell Korelasyonları)

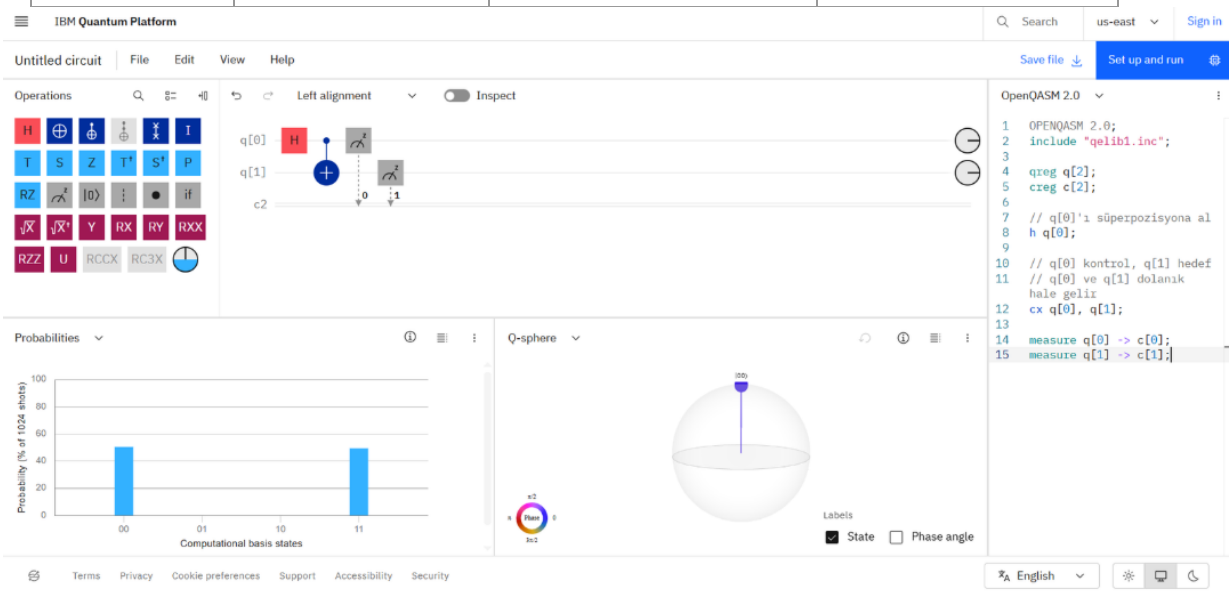
Dolanıklı bir çiftteki kübitlerin ölçüm yoluyla kesin değerlerine çökertilmesi, Bell korelasyonlarının doğrudan gözlemlenmesi anlamına gelir. $|\Phi^+\rangle = (|00\rangle+|11\rangle)/\sqrt{2}$ durumunda, hiçbir kübitin tek başına kesin bir değeri yoktur; yalnızca aralarındaki korelasyon belirlidir. Ölçüm yapıldığında, süperpozisyon çöker ve hem kontrol hem hedef kübit aynı anda kesin değerlerine ulaşır (Mermin, 2007).

Dört Bell durumu ve oluşturma devreleri aşağıdaki gibidir:

Tablo 7.7'de Bell durumlarının dalga fonksiyonu, devre ve ölçüm sonuçları özetlenmektedir.

Tablo 7.7. Bell durumlarının dalga fonksiyonu, devre ve ölçüm sonuçları.

Bell Durumu	Dalga Fonksiyonu	Devre	Ölçüm Sonucu
$\|\Phi^+\rangle$	$(\|00\rangle+\|11\rangle)/\sqrt{2}$	H → CNOT	00 veya 11 (%50-%50)
$\|\Phi^-\rangle$	$(\|00\rangle-\|11\rangle)/\sqrt{2}$	X→H → CNOT	00 veya 11 (%50-%50)
$\|\Psi^+\rangle$	$(\|01\rangle+\|10\rangle)/\sqrt{2}$	H → CNOT → X(q1)	01 veya 10 (%50-%50)
$\|\Psi^-\rangle$	$(\|01\rangle-\|10\rangle)/\sqrt{2}$	X→H → CNOT → X(q1)	01 veya 10 (%50-%50)



Hadamard kapısı q[0]'ı 0 ve 1 olasılığına sokar. CNOT kapısı q[0] ile q[1] arasında bağlantı kurar. Bu yüzden ölçümde sonuçlar ya 00 ya da 11 çıkar. Yani iki qubit dolanık hale gelir.

Şekil 7.12. Bell durumu; H→CNOT devresi ve 00/11 ölçüm histogramı (kaynak: sunum s. 58-60).

7.4.3 Bell Eşitsizliğinin Deneysel Doğrulanması

1964'te John Bell, yerel gerçekçilik (lokalite ve gizli değişkenler) varsayımı altında iki parçacık arasındaki korelasyonların aşamayacağı bir üst sınır türetmiştir (Bell, 1964). Kuantum mekaniği bu eşitsizliğin dolanık parçacıklarda ihlal edileceğini öngörür. Bu öngörü deneysel olarak defalarca doğrulanmıştır: Aspect ve arkadaşlarının 1982 deneyleri (Aspect, Dalibard ve Roger, 1982) ve boşluk-içermeyen (loophole-free) testler arasında yer alan Hensen ve arkadaşlarının 2015 deneyi (Hensen ve diğ., 2015) bunların başlıcalarıdır. Bu alandaki çalışmalar nedeniyle Alain Aspect, John F. Clauser ve Anton Zeilinger 2022 Nobel Fizik Ödülü'ne layık görülmüştür.

Yerel gerçekçilik varsayımı iki bileşene dayanır: (i) gerçekçilik; her parçacığın ölçümden önce belirli bir değeri vardır; (ii) yerellik; bir parçacığın ölçümü, uzaktaki diğer parçacığı anlık olarak etkileyemez. Bu varsayımlar doğru olsaydı, iki parçacık arasındaki korelasyonlar Bell eşitsizliğinin belirlediği sınırı aşamazdı. Kuantum mekaniği ise dolanık parçacıkların bu sınırı aştığını öngörür ve deneyler bunu doğrulamıştır (Bell, 1964).

Süperpozisyon ile dolanıklık ilişkisi: Bell testinin çalışması doğrudan süperpozisyona dayanır. Dolanıklık oluşturmak için önce kübitlerin Hadamard kapısıyla süperpozisyona getirilmesi gerekir; süperpozisyon olmadan dolanıklık oluşturulamaz. Ölçüm anında süperpozisyon çöker ve dolanıklık sona erer. Eğer parçacıklar yalnızca kesin 0 veya 1 değerlerinde olsaydı, ölçüm sonuçları klasik olasılık kurallarına uyar ve Bell eşitsizliği ihlal edilemezdi (slayt 65-66).

7.5 Dekoherans (Zaman Gecikmesi) ve Kuantum Hatalar

Dekoherans, bir kuantum sisteminin çevresiyle istenmeyen etkileşimi sonucu kuantum bilgisini kaybetmesi sürecidir. Bir kübitin süperpozisyon ve dolanıklık gibi kuantum özelliklerini koruyabildiği süreye koherans süresi denir. Günümüz süperiletken kübitleri için bu süre tipik olarak mikrosaniyeler mertebesindedir; ancak bazı platformlarda (iyon tuzağı, nötr atom) saniyeler mertebesine ulaşabilir (Preskill, 2018).

7.5.1 T1 ve T2 Süreleri

T1 (Enerji gevşemesi): Kübitin |1⟩ uyarılmış durumundan |0⟩ taban durumuna düşme süresidir. T1 süresi dolduğunda kübit kesinlikle |0⟩ durumuna çöker.

T2 (Faz koheransı): Kübitin süperpozisyon durumundaki göreli faz bilgisini kaybetme süresidir. T2 ≤ 2×T1 ilişkisi her zaman geçerlidir. Faz bilgisi kaybolduğunda süperpozisyon klasik bir karışıma dönüşür ve kuantum avantajı kaybolur (Nielsen ve Chuang, 2010).

7.5.2 Gerçek Donanımda Test Etme

Dekoheransın etkisini doğrudan test etmek için, bilinen bir kuantum devresi (örneğin Bell durumu) gerçek kuantum donanımı üzerinde çok sayıda (örn. 1000 shot) çalıştırılır ve sonuçlar teorik beklentiyle karşılaştırılır. İdeal sonuçta sadece |00⟩ ve |11⟩ görülmesi gerekirken, gerçek donanımda görülen |01⟩ ve |10⟩ oranları dekoherans ve kapı hatalarının birleşik etkisini yansıtır. Bu yöntemle donanıma zarar vermeden gürültü profili çıkarılabilir.

İşte "zaman gecikmesini donanıma zarar vermeden test eder, 1000 kere yapar, bazı hatalar olsa da çoğunlukla cevabı 1'dir" ifadesinin teknik karşılığı budur: devre 1000 shot çalıştırılır, baskın sonuç beklenen değerdir, az sayıdaki sapma hatalardan kaynaklanır ve bu süreçte donanım fiziksel olarak hasar görmez.

7.5.3 Gerçek Donanımdaki Hata Kaynakları

Gerçek kuantum donanımında (IBM Quantum, Google vb.) başlıca üç hata kaynağı bulunur (slayt 68):

- Kapı hataları (Gate Errors): Her kuantum kapısı yaklaşık %0,01–%1 hata oranına sahiptir; kapılar ideal üniter dönüşümlerden sapma gösterir.
- Ölçüm hataları (Readout Errors): Kübit aslında |1⟩ durumundayken dedektör bazen yanlışlıkla 0 okuyabilir veya tam tersi olabilir.
- Evre-yitimi (Decoherence): Kübit, hesaplama sırasında çevresel gürültüden dolayı bilgi kaybedebilir; T_1 (enerji gevşemesi) ve T_2 (faz tutarlılığı) süreleriyle ölçülür.

Sonuç olarak, 1000 shotluk ideal olarak 1000 kez |1⟩ beklenen bir devrede, gerçek donanımda yaklaşık 950–990 kez |1⟩, 10–50 kez |0⟩ görülebilir. Çoğunluk oylamasıyla doğru cevap belirlenir.

7.5.4 Fiziksel ve Mantıksal Kübit

Fiziksel kübit, gerçek donanımda (süperiletken devreler, iyon tuzakları vb.) bulunan temel birimdir. Süperpozisyon ve dolanıklık özelliklerine sahiptir ancak gürültü, sıcaklık ve çevresel etkileşim nedeniyle çok kırılgandır ve kolayca dekoheransa uğrar. Mantıksal (logical) kübit ise tek bir fiziksel kübit değildir; birden fazla fiziksel kübit kullanılarak kuantum hata düzeltme (Quantum Error Correction) teknikleriyle oluşturulur. Amaç hataları tespit edip düzeltmek ve daha güvenilir hesaplama sağlamaktır. Örneğin yüzey

kodu (surface code) gibi yöntemlerde tek bir mantıksal kübit için onlarca hatta yüzlerce fiziksel kübit gerekebilir (Fowler ve diğ., 2012).

Tablo 7.8'de fiziksel ve mantıksal kübitler karşılaştırılmaktadır.

Tablo 7.8. Fiziksel ve mantıksal kübitlerin karşılaştırması.

Özellik	Fiziksel Kübit	Mantıksal Kübit
Yapı	Tek kübit	Birçok kübitin birleşimi
Hata oranı	Yüksek	Çok daha düşük
Stabilite	Düşük	Yüksek
Kullanım	Donanım seviyesi	Gerçek hesaplama seviyesi

Basit benzetme: Fiziksel kübit tek bir hassas ampul gibidir; mantıksal kübit ise birçok ampul ve yedekleme sistemi gibidir; biri bozulsa bile ışık devam eder. Günümüz kuantum bilgisayarları (IBM, Google) çoğunlukla fiziksel kübit seviyesinde çalışmakta olup, büyük ve güvenilir hesaplama için mantıksal kübitler gereklidir.

Not: Fiziksel ve mantıksal kübit karşılaştırması (kaynak: sunum s. 62-64).

7.5.5 Simülatörlerle Test

Kuantum devreleri, klasik bilgisayarlarda çalışan ve kuantum davranışını matematiksel olarak taklit eden simülatörler üzerinde de test edilebilir. Simülatörlerin avantajları: donanım gürültüsünün bulunmaması (ideal sonuçlar), kuyruk bekleme süresinin olmaması ve dekoherans probleminin yer almamasıdır. IBM Qiskit Aer, Google Cirq ve QuTiP bu amaçla kullanılan başlıca araçlardır. Ancak temel bir sınırlama vardır: n kübitlik bir sistemi simüle etmek için 2^n karmaşık sayı saklanması gerektiğinden simülatörler kübit sayısı arttıkça üstel olarak yavaşlar; bu nedenle yaklaşık 40–50 kübitin üzerinde klasik simülasyon pratik olarak imkânsızlaşır (Preskill, 2018).

7.6 Kuantum Hesaplama Gücü ve Üstünlük

7.6.1 Üstel Durum Uzayı: 2^n Kübit

Kuantum bilgisayarlarının gücü, kübit sayısıyla üstel olarak büyüyen durum uzayından gelir. n kübitlik bir sistem, 2^n boyutlu bir Hilbert uzayında bulunur. Bu, n kübitin aynı anda 2^n farklı durumun süperpozisyonunda olabileceği anlamına gelir (Nielsen ve Chuang, 2010).

20 kübit: 2^{20} = 1.048.576 durum. Yaklaşık 1 milyon farklı değer üzerinde paralel işlem potansiyeli. Klasik bir bilgisayar bu durumları tek tek işlerken, 20 kübitlik bir kuantum sistemi tüm bu durumları aynı anda taşır.

128 kübit: $2^{128} \approx 3{,}4 \times 10^{38}$ durum. Bu sayı, gözlemlenebilir evrendeki atom sayısından ($\sim 10^{80}$) küçük olmasına rağmen, klasik bilgisayarlar için temsil edilemeyecek kadar büyüktür. Tüm dünyadaki klasik bellek, 128 kübitlik bir kuantum sisteminin tam durum vektörünü depolayamaz.

7.6.2 Kuantum Paralelizmi

Kuantum paralelizmi, süperpozisyon sayesinde bir kuantum fonksiyonunun tüm giriş değerlerine "aynı anda" uygulanabilmesidir. n kübite Hadamard kapıları uygulayarak 2^n farklı girişin eşit ağırlıklı süperpozisyonu oluşturulur ve ardından uygulanan üniter dönüşüm tüm bu durumlar üzerinde aynı anda etki eder. Ancak burada kritik bir nokta vardır: süperpozisyondaki bilgiye doğrudan erişilemez. Ölçüm,

2^n olası sonuçtan yalnızca birini verir. Kuantum algoritmalarının zekice kısmı, girişimle (interference) doğru cevabın olasılığını artırırken yanlış cevapların olasılığını azaltmasıdır (Rieffel ve Polak, 2011).

7.6.3 Neden Dekoheransa Rağmen Klasik Bilgisayarların Yapamadığını Yapabiliyoruz?

Bu soru, kuantum hesaplamanın en derin soruşturmasıdır. Cevap birkaç katmandan oluşur:

1) Üstel durum uzayı: n kübit, 2^n boyutlu bir uzayda çalışır. Klasik n bitlik bir sistem sadece n bitlik bilgi taşırken, n kübitlik bir kuantum sistemi 2^n karmaşık genlik taşır. Bu, hesaplama kapasitesinde üstel bir atılım sağlar.

2) Kuantum girişimi (interference): Algoritmalar, doğru cevabın genliklerini yapıcı girişimle büyütürken yanlış cevapların genliklerini yıkıcı girişimle söndürür. Grover'ın arama algoritması ve Shor'un çarpanlara ayırma algoritması bu prensibin başarılı uygulamalarıdır (Grover, 1996; Shor, 1994).

3) Kuantum hata düzeltme: Dekoherans sorunu, kuantum hata düzeltme kodları ile aşılabilir. Birden fazla fiziksel kübit kullanarak tek bir mantıksal kübitin bilgisini korumak mümkündür. Eşik teoremi (threshold theorem), kapı hata oranı belirli bir eşiğin altında kaldığı sürece rastgele uzun hesaplamaların güvenilir biçimde yürütülebileceğini garanti eder (Nielsen ve Chuang, 2010).

4) Algoritma tasarımı: Kuantum algoritmaları, dekoherans süresi içinde tamamlanacak kadar verimli tasarlanır. Devre derinliği (gate depth) minimize edilir ve koherans penceresi içinde işlem bitirilir.

7.6.4 Kuantum Üstünlüğü Perspektifi

Kuantum üstünlüğü (quantum supremacy), bir kuantum bilgisayarın belirli bir problemi klasik bilgisayarların pratikte ulaşamayacağı bir hızda çözmesidir. Google'ın Sycamore işlemcisi 53 kübitle, belirli bir örnekleme (sampling) probleminde klasik süper bilgisayarların 10.000 yılda yapacağı hesaplamayı 200 saniyede yaptığını iddia etmiştir (Arute vd., 2019). IBM bu iddianın abartılı olduğunu ileri sürmüş olsa da, sonuç kuantum üstünlüğünün boyutunu göstermektedir.

7.6.5 Zaman Karmaşıklığında Fark

Aşağıdaki tablo, belirli problemlerde klasik ve kuantum algoritmaların zaman karmaşıklığını karşılaştırır (slayt 72):

Tablo 7.9'da seçilmiş problemlerde klasik ve kuantum zaman karmaşıklığı karşılaştırılmaktadır.

Tablo 7.9. Seçilmiş problemlerde klasik ve kuantum zaman karmaşıklığı.

Problem	Klasik Karmaşıklık	Kuantum Karmaşıklık
Sırasız arama (N eleman)	O(N)	$O(\sqrt{N})$ – Grover
Tam sayı çarpanlarına ayırma	Alt-üstel (GNFS)	$O(n^3)$ – Shor
Kuantum simülasyonu	$O(2^n)$ – Üstel	O(poly(n)) – Polinom

Grover algoritması karesel (quadratic), Shor algoritması ise üstel hızlanma sağlar. Bu farklar, belirli problem sınıflarında kuantum bilgisayarların neden devrim niteliğinde olduğunu açıklar.

7.7 Kuantum Bilgisayarların Basit İşlemlerde Zorlanması

Kuantum bilgisayarlarının her türlü problemde klasik bilgisayarlardan üstün olduğu algısı yanlıştır. Kuantum avantajı, yalnızca belirli problem sınıflarında ortaya çıkar; pek çok günlük ve basit işlemde kuantum bilgisayarları klasik sistemlerden çok daha yavaş ve verimsizdir (Preskill, 2018).

7.7.1 Neden Basit İşlemlerde Zorlanır?

Yüksek hazırlık maliyeti (overhead): Bir kübiti başlatmak, süperpozisyona sokmak ve ölçmek, klasik bir bitin 0 veya 1 olarak ayarlanmasından çok daha karmaşık ve yavaştır. Basit bir toplama işlemi için bu ek yük, elde edilen herhangi bir hızlanmayı tamamen ortadan kaldırır.

Ölçümün olasılıksal doğası: Klasik bir bilgisayar 2+2=4 sonucunu tek adımda ve kesin olarak verir. Kuantum bilgisayar ise tek bir ölçümde yanlış sonuç üretebilir; kesinlik için çok sayıda tekrar gerekir. Basit işlemler için bu, büyük bir dezavantajdır.

Sıralı işlem zorlukları: Kuantum paralelizmi, doğası gereği paralel yapıda çalışır. Sıralı karar verme süreçleri (if-else zincirleri, döngüler) kuantum devrelerinde doğal değildir ve ek kapı maliyeti getirir.

Soğutma ve izolasyon: Süperiletken kübitler, mutlak sıfırın yakınında, ultra-vakum ortamında çalışır. Bu koşulları sağlamak, basit bir hesaplama için orantısız kaynak tüketimi anlamına gelir.

7.7.2 Kuantum Avantajının Olduğu ve Olmadığı Alanlar

Tablo 7.10'da kuantum avantajının problem türlerine göre dağılımı özetlenmektedir.

Tablo 7.10. Kuantum avantajının problem türlerine göre dağılımı.

Problem Türü	Kuantum Avantajı	Açıklama
Asal çarpanlara ayırma	Üstel hızlanma	Shor algoritması (1994)
Sıralanmamış arama	Karekök hızlanma	Grover algoritması (1996)
Kuantum simülasyonu	Üstel hızlanma	Molekül/malzeme modelleme
Basit aritmetik (+, ×)	Avantaj yok	Klasik CPU çok daha hızlı
Veritabanı sorgusu (indeksli)	Avantaj yok	Klasik indeksleme O(1)
Kelime işleme, web	Avantaj yok	Sıralı iş, klasik uygun

7.7.3 Klasik ve Kuantum Bilgisayarların Üstün Olduğu Alanlar

Aşağıdaki tablo, hangi tür işlemlerde klasik, hangilerinde kuantum bilgisayarların daha iyi olduğunu özetler (slayt 74):

Tablo 7.11'de klasik ve kuantum bilgisayarların üstün olduğu işlem alanları özetlenmektedir.

Tablo 7.11. Klasik ve kuantum bilgisayarların üstün olduğu işlem alanları.

Klasik Bilgisayar Daha İyi	Kuantum Bilgisayar Daha İyi
Günlük aritmetik (toplama, çarpma)	Çarpanlarına ayırma (Shor)
Metin işleme, web gezinme	Sırasız veritabanı araması (Grover)
Veritabanı sorguları (SQL)	Molekül ve malzeme simülasyonu
Dosya sıkıştırma, video kodlama	Optimizasyon (QAOA)
Genel amaçlı programlama	Kriptografi kırma (RSA, ECC)

Sonuç: Kuantum bilgisayarlar, üstel karmaşıklığa sahip belirli problemlerde devrim niteliğinde hız kazanımı sağlar. Ancak basit, sıralı ve kesin sonuç gerektiren görevlerde klasik bilgisayarlar üstündür. Gelecekte hibrit yaklaşımların (klasik + kuantum) baskın olması beklenmektedir.

7.8 Kuantum Algılama (Quantum Sensing)

Kuantum algılama, kuantum mekaniksel özellikleri (süperpozisyon, dolanıklık, sıkışma) kullanarak fiziksel büyüklüklerin (manyetik alan, yerçekimi, zaman, sıcaklık) ölçüm hassasiyetini klasik sınırların ötesine taşıyan teknolojidir. Bu alan, kuantum bilgisayarlardan önce teknolojik olgunluğa ulaşabilecek ilk kuantum uygulaması olarak görülmektedir (Degen, Reinhard ve Cappellaro, 2017).

Kuantum algılamanın zaman ölçümündeki uygulaması, atom saatlerinde somutlaşır. Atom saatleri, atomların kuantum enerji geçişlerinin son derece kararlı frekansını kullanarak zamanı çok yüksek hassasiyette ölçebilir. GPS uydularındaki sezyum ve rubidyum atom saatleri bu prensiple çalışır.

7.9 X Kapısı ile Hadamard Kapısı Karşılaştırması

X kapısı ve Hadamard kapısı, tek kübitlik kapılar arasında en sık karıştırılan iki kapıdır. İkisi de 2×2 üniter matrislerle temsil edilir; ancak kübit üzerindeki etkileri birbirinden temelden farklıdır. X kapısı, klasik NOT işleminin kuantum karşılığıdır ve kübiti hesaplama tabanında deterministik olarak çevirir: $|0\rangle \rightarrow |1\rangle$, $|1\rangle \rightarrow |0\rangle$. Sonuç her zaman kesin bir taban durumudur. Hadamard kapısı ise bir taban durumunu süperpozisyona taşır: $H|0\rangle = (|0\rangle+|1\rangle)/\sqrt{2}$. Ölçüm yapıldığında her iki sonuç da eşit olasılıkla elde edilir (Nielsen ve Chuang, 2010).

Tablo 7.12'de Pauli-X ve Hadamard kapıları karşılaştırılmaktadır.

Tablo 7.12. Pauli-X ve Hadamard kapılarının karşılaştırması.

Özellik	Pauli-X Kapısı	Hadamard Kapısı	Temel Fark
Matris	[[0,1],[1,0]]	$(1/\sqrt{2})[[1,1],[1,-1]]$	Farklı üniter dönüşüm
$\|0\rangle$ girdisi	$\|1\rangle$ (kesin)	$(\|0\rangle+\|1\rangle)/\sqrt{2}$	X: çevirir, H: süperpozisyon
$\|1\rangle$ girdisi	$\|0\rangle$ (kesin)	$(\|0\rangle-\|1\rangle)/\sqrt{2}$	X: çevirir, H: süperpozisyon
Ölçüm sonucu	Deterministik	Olasılıksal (%50-%50)	X kesinlik, H belirsizlik üretir
Bloch rotasyonu	x ekseni, π rad	$(x+z)/\sqrt{2}$ ekseni, π rad	Farklı eksen, farklı geometri
Kullanım amacı	Bit çevirme (NOT)	Süperpozisyon oluşturma	X: klasik benzeri, H: kuantum benzeri

Özet: X kapısı "değeri tersle" der; Hadamard kapısı "ikisi de olabilir" der. Bu yüzden kuantum algoritmalarında süperpozisyon gereken yerlerde X değil H kullanılır.

7.10 Süperpozisyon ile Dolanıklık Karşılaştırması

Süperpozisyon ve dolanıklık, kuantum mekaniğinin iki temel ilkesidir; ancak farklı fiziksel olgulara karşılık gelir. Süperpozisyon, tek bir kübitin aynı anda birden fazla durumun doğrusal bileşiminde bulunmasıdır: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Bu özellik tek bir kübit için bile geçerlidir ve Hadamard kapısıyla kolayca oluşturulabilir. Dolanıklık ise en az iki kübit arasında ortaya çıkan, klasik karşılığı olmayan bir korelasyondur. Dolanıklı bir sistemde tek bir kübitin durumu, diğer kübitten bağımsız olarak tanımlanamaz (Nielsen ve Chuang, 2010).

Tablo 7.13'te süperpozisyon ve dolanıklık arasındaki temel farklar özetlenmektedir.

Tablo 7.13. Süperpozisyon ve dolanıklık arasındaki temel farklar.

Özellik	Süperpozisyon	Dolanıklık (Entanglement)
Minimum kübit sayısı	1 kübit yeterlidir	En az 2 kübit gereklidir
Tanım	Bir kübitin |0⟩ ve |1⟩ durumlarının doğrusal bileşiminde bulunması	İki veya daha fazla kübitin ayrıştırılamaz ortak durumda olması
Örnek durum	$\|\psi\rangle = (\|0\rangle+\|1\rangle)/\sqrt{2}$	$\|\Phi^+\rangle = (\|00\rangle+\|11\rangle)/\sqrt{2}$
Nasıl oluşturulur?	Hadamard kapısı (H)	H + CNOT (Bell devresi)
Ölçüm etkisi	Kübit tek bir değere çöker	Bir kübitin ölçümü diğerini de belirler
Klasik benzeri var mı?	Kısmen: yazı-tura benzetmesi (ancak genlik fazlıdır)	Hayır, klasik fizikte karşılığı yoktur

Anahtar cümle: Süperpozisyon tek bir kübitin "birden fazla olasılıkta" olmasıdır; dolanıklık ise iki kübitin kaderlerinin birbirine bağlanmasıdır. Dolanıklık süperpozisyonu gerektirir, ancak süperpozisyon tek başına dolanıklık değildir.

Soru: Kuantum kapıları tersinir (reversible) olduğu hâlde, ölçüm neden geri alınamaz?

Cevap: Kuantum kapıları üniter matrislerle temsil edilir. Üniter matrisin tersi her zaman vardır ($U^\dagger U = I$); dolayısıyla kapının etkisi ters kapı uygulanarak geri alınabilir. Örneğin X kapısını iki kez uygulamak kübitin orijinal durumunu geri verir: $XX = I$ (Nielsen ve Chuang, 2010).

Ölçüm ise üniter bir işlem değildir. Ölçüm, kübitin durumunu $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ süperpozisyonundan ya $|0\rangle$ ya da $|1\rangle$ durumuna çökertir (wave function collapse). Bu süreçte α ve β genlik bilgisi geri dönüşümsüz olarak kaybolur. Ölçüm sonrasında elde edilen tek bilgi, sonucun 0 mı yoksa 1 mi olduğudur; orijinal α ve β değerlerini geri çıkarmak fiziksel olarak imkânsızdır (Mermin, 2007).

Matematiksel olarak, ölçüm bir projeksiyon işlemidir ve projeksiyon matrisleri ($P_0 = |0\rangle\langle 0|$, $P_1 = |1\rangle\langle 1|$) üniter değildir; $P^2 = P$ özelliğini sağlarlar, $P^\dagger P \neq I$'dır. Bu nedenle bilgi kaybı kaçınılmazdır.

Tablo 7.14'te kuantum kapısı ve ölçüm işlemi karşılaştırılmaktadır.

Tablo 7.14. Kuantum kapısı ve ölçüm işleminin karşılaştırması.

Özellik	Kuantum Kapısı	Ölçüm
Matematiksel temsil	Üniter matris ($U^\dagger U = I$)	Projeksiyon ($P^2 = P$, üniter değil)
Tersinir mi?	Evet, ters kapı uygulanabilir	Hayır, genlik bilgisi kaybolur
Bilgi kaybı	Yok (tüm bilgi korunur)	Var (α, β geri elde edilemez)
Çıktı	Kuantum durumu (süperpozisyon mümkün)	Klasik bit (0 veya 1)

7.11 RZ Kapısı Neden Ölçüm Histogramını Değiştirmez?

RZ(θ) kapısı, Bloch küresi üzerinde z ekseni etrafında θ açısıyla rotasyon yapar. Matris gösterimi RZ(θ) = [[e^(−iθ/2), 0],[0, e^(iθ/2)]] şeklindedir. Bu matris köşegen olduğundan |0⟩ ve |1⟩ durumlarının olasılıklarını değiştirmez; yalnızca aralarındaki göreli fazı (relative phase) değiştirir (Nielsen ve Chuang, 2010).

Tek cümlelik güçlü açıklama: RZ kapısı, |0⟩ ve |1⟩ genliklerinin büyüklüklerini değil açılarını döndürür; ölçüm olasılığı |α|² ve |β|² yalnızca büyüklüğe bağlı olduğundan histogram değişmez.

Bunu somutlaştırmak gerekirse: |ψ⟩ = (|0⟩+|1⟩)/√2 durumuna RZ(π/4) uygulandığında, |0⟩ bileşeni e^(−iπ/8), |1⟩ bileşeni e^(iπ/8) fazı kazanır. Her iki bileşenin büyüklüğü hâlâ 1/√2'dir; dolayısıyla ölçümde |0⟩ ve |1⟩ görülme olasılıkları yine %50-%50 kalır. Ancak faz bilgisi tamamen gerçek bir etkiye sahiptir: RZ'den sonra uygulanan Hadamard veya başka kapılar, fazdan etkilenerek farklı girişim desenleri oluşturur ve sonraki ölçüm sonuçlarını değiştirir (Mermin, 2007).

7.12 CNOT Kapısında Kontrol ve Hedef Mantığı

CNOT kapısı, iki kübitlik en temel kontrollü kapıdır. Öğrencilerin en sık karıştırdığı nokta, hangi kübitin kontrol, hangisinin hedef olduğudur. Kuralı tek cümlede özetlemek gerekirse:

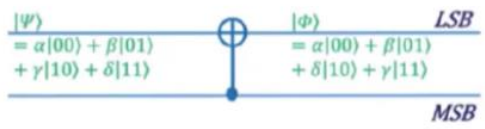
Kural: Kontrol kübiti |1⟩ ise hedef kübitin durumu tersine çevrilir; kontrol |0⟩ ise hiçbir şey olmaz.

Devre çizimlerinde kontrol kübiti genellikle dolu nokta (●) ile, hedef kübiti ise ⊕ sembolü ile gösterilir. 4×4 matris gösteriminde CNOT = [[1,0,0,0],[0,1,0,0],[0,0,0,1],[0,0,1,0]] şeklindedir; burada üçüncü ve dördüncü satırların yer değiştirmesi, kontrol=|1⟩ durumunda hedefin çevrilmesine karşılık gelir (Şekil 7.13) (Nielsen ve Chuang, 2010).

Tablo 7.15'te CNOT kapısında kontrol ve hedef dönüşümü gösterilmektedir.

Tablo 7.15. CNOT kapısında kontrol ve hedef dönüşüm tablosu.

Kontrol (q_0)	Hedef (q_1) — Önce	Hedef (q_1) — Sonra	Açıklama
|0⟩	|0⟩	|0⟩	Kontrol 0 → hedef değişmez
|0⟩	|1⟩	|1⟩	Kontrol 0 → hedef değişmez
|1⟩	|0⟩	|1⟩	Kontrol 1 → hedef TERSLENİR
|1⟩	|1⟩	|0⟩	Kontrol 1 → hedef TERSLENİR



CNOT =

"İlk bite bak, eğer 1 ise ikinci biti tersle."

Sağ alttaki devrede:

- üst çizgide daire içi artı işareti: **target**
- alt çizgide dolu nokta: **control**

Bu sembol şunu söyler:

> Alttaki bit 1 ise, üstteki biti çevir.

Ama dikkat: bazı kitaplarda üst çizgi control, alt çizgi target olabilir.
Burada görselde hangi çizginin hangi kübit olduğu ayrıca belirtilmiş.

Akılda kalıcı örnek

Klasik mantık gibi düşün:

- kontrol = anahtar
- target = lamba

Anahtar 0 ise lamba olduğu gibi kalır.
Anahtar 1 ise lambanın durumu değişir.

Şekil 7.13. CNOT kontrol (●) ve hedef (⊕) sembollerinin devre gösterimi (kaynak: sunum s. 48).

Önemli not: Kontrol kübiti CNOT işlemi sırasında hiçbir zaman değişmez; yalnızca hedef kübiti etkilenir. Kontrol kübiti bir "koşul", hedef kübiti ise o koşula bağlı olarak hareket eden "aktör" olarak düşünülebilir.

7.13 Bell Durumu Nasıl Oluşturulur?

Bell durumu oluşturmak, kuantum devre tasarımının en temel yapı taşlarından biridir. Üç adımlık formül, sözlü sınavlarda en sık sorulan konulardan biridir (Nielsen ve Chuang, 2010):

Adım 1 → Başlangıç: $|00\rangle$ (her iki kübit $|0\rangle$ durumunda).

Adım 2 → Hadamard (H): İlk kübite H kapısı uygula → $(|0\rangle+|1\rangle)/\sqrt{2} \otimes |0\rangle = (|00\rangle+|10\rangle)/\sqrt{2}$. İlk kübit artık süperpozisyonda.

Adım 3 → CNOT: İlk kübit kontrol, ikinci kübit hedef → $(|00\rangle+|11\rangle)/\sqrt{2} = |\Phi^+\rangle$. Artık kübitlerin kaderi birbirine bağlı.

Ezber formülü: H → CNOT → Dolanıklık. Bu üç kelime Bell devresinin tamamını özetler. H süperpozisyon yaratır, CNOT bu süperpozisyonu iki kübite yayarak dolanıklık oluşturur.

7.14 Tek Kübitten Çok Kübite Geçişte Matris Boyutu ve Tensör Çarpımı

Kuantum mekaniğinde çok parçacıklı sistemlerin durum uzayı, tek parçacık durum uzaylarının tensör çarpımı (tensor product, ⊗) ile elde edilir. Bu matematiksel yapı, boyutun kübit sayısıyla üstel olarak artmasına neden olur (Nielsen ve Chuang, 2010).

Tablo 7.16'da kübit sayısına göre durum vektörü ve kapı matrisi boyutları verilmektedir.

Tablo 7.16. Kübit sayısına göre durum vektörü ve kapı matrisi boyutları.

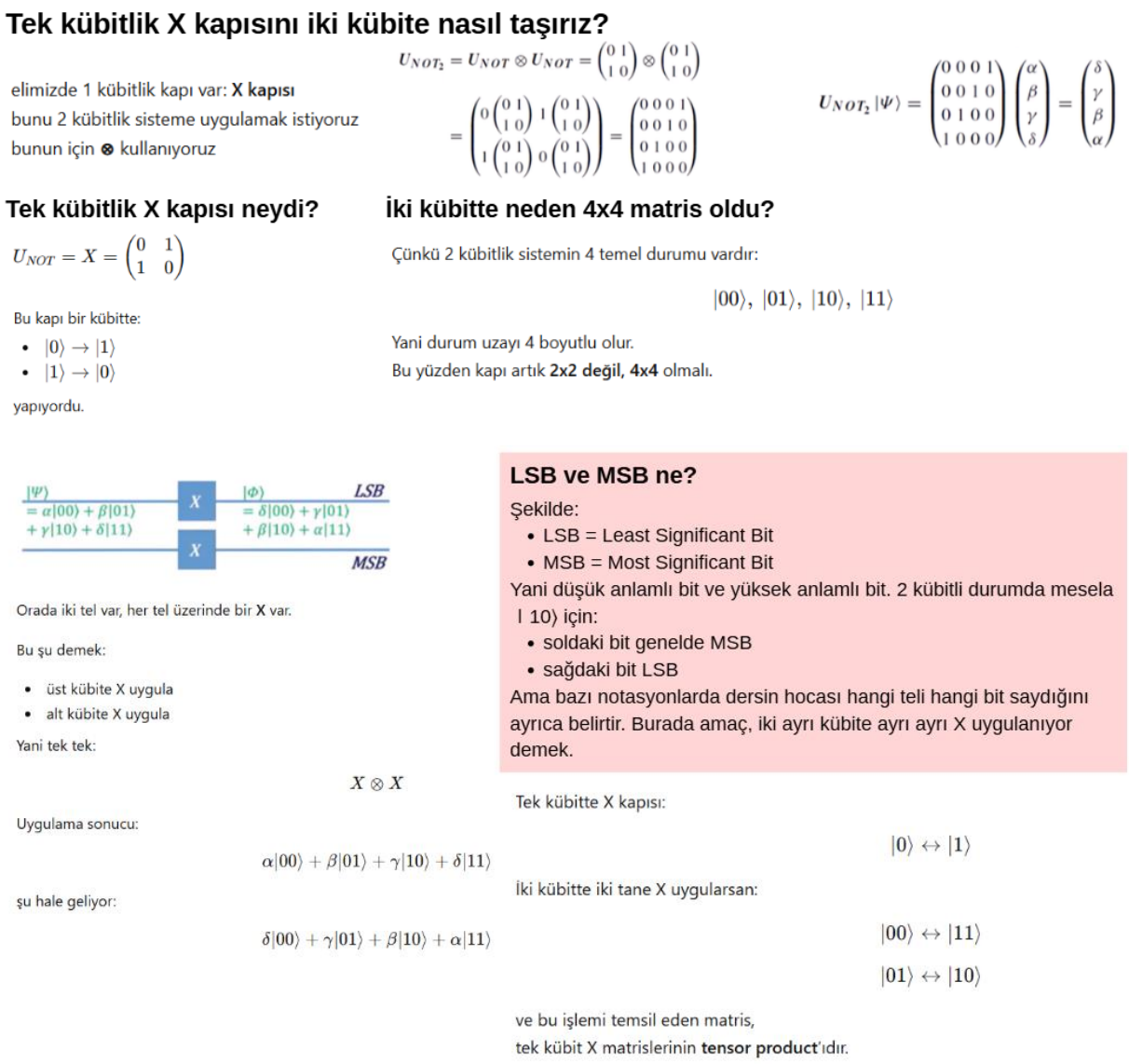
Kübit Sayısı	Olası Durum Sayısı	Durum Vektörü Boyutu	Kapı Matris Boyutu
1	$2^1 = 2$ ($\|0\rangle$, $\|1\rangle$)	2×1	2×2
2	$2^2 = 4$ ($\|00\rangle$, $\|01\rangle$, $\|10\rangle$, $\|11\rangle$)	4×1	4×4
3	$2^3 = 8$	8×1	8×8
n	2^n	$2^n \times 1$	$2^n \times 2^n$

Vurucu özet: 1 kübit = 2 durum → 2×2 matris. 2 kübit = 4 durum → 4×4 matris. Her eklenen kübit, durum sayısını ve matris boyutunu ikiye katlar. Bunun nedeni tensör çarpımıdır: iki kübitin ortak durum uzayı, tek tek kübit uzaylarının çarpımı ($2 \times 2 = 4$) olarak inşa edilir.

Örnek; tek kübitlik X kapısının iki kübite taşınması: İki ayrı kübitin her birine X uygulamak istediğimizde, kapı tensör çarpımı ile birleştirilir: X⊗X. Tek kübitlik X = [[0,1],[1,0]] iken, X⊗X dört boyutlu (4×4) bir matris olur ve her iki kübitin bitini birden çevirir: $|00\rangle\rightarrow|11\rangle$, $|01\rangle\rightarrow|10\rangle$, $|10\rangle\rightarrow|01\rangle$, $|11\rangle\rightarrow|00\rangle$ (slayt 9-13).

Genel iki kübit durumu $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ vektör biçiminde ($\alpha, \beta, \gamma, \delta$) olarak yazılır. X⊗X uygulandığında katsayılar ters sıraya geçer: çıkış ($\delta, \gamma, \beta, \alpha$) olur; yani $|\varphi\rangle = \delta|00\rangle + \gamma|01\rangle + \beta|10\rangle + \alpha|11\rangle$. Bunun nedeni kapının baz durumlarını çevirmesidir (Şekil 7.14).

LSB ve MSB: İki kübitlik bir gösterimde (örneğin $|10\rangle$) soldaki bit genellikle MSB (Most Significant Bit / en yüksek anlamlı bit), sağdaki bit ise LSB (Least Significant Bit / en düşük anlamlı bit) olarak adlandırılır. Bu adlandırma, devre çizimlerinde hangi telin hangi kübite karşılık geldiğini belirtmek için kullanılır; bazı kaynaklar sıralamayı tersine alabildiğinden notasyon her zaman ayrıca belirtilmelidir.



Şekil 7.14. Tek kübitlik X kapısının tensör çarpımıyla iki kübite taşınması ve LSB/MSB gösterimi (kaynak: sunum s. 9-13).

7.15 Kuantum Register ve Klasik Register Ayrımı

Kuantum devrelerde iki tür kayıtçı (register) bulunur. Bu ayrım, kuantum bilgi ile klasik bilginin devre içinde nasıl taşındığını ve saklandığını anlamak için temeldir (Nielsen ve Chuang, 2010).

Tablo 7.17'de kuantum register ile klasik register ayrımı özetlenmektedir.

Tablo 7.17. Kuantum register ile klasik register ayrımı.

Özellik	Kuantum Register	Klasik Register
İçeriği	Kübitler (kuantum durumu taşır)	Klasik bitler (0 veya 1)
Süperpozisyon	Olabilir	Olamaz, her zaman kesin değer
Dolanıklık	Diğer kübitlerle dolanık olabilir	Mümkün değil
Kapı uygulanır mı?	Evet (H, X, CNOT vb.)	Hayır, yalnızca okuma/yazma
Ne zaman değer alır?	Ölçüm yapılana kadar belirsiz	Ölçüm sonucu yazıldığında kesinleşir
Devre çiziminde gösterimi	Tek çizgi (———)	Çift çizgi (═══)

Tek cümle: Kuantum register kübitin kuantum bilgisini (süperpozisyon, faz, dolanıklık) taşır; klasik register ise ölçümden sonra elde edilen kesin sonucu (0 veya 1) depolar

Composer'da kuantum telleri (q[0], q[1]...) ve klasik register (c) birlikte kullanılır (kaynak: sunum s. 2, 24).

7.16 Reset ile Measurement Farkı

Reset ve measurement (ölçüm) işlemleri, kübitin durumunu değiştirmeleri açısından benzer görünse de amaçları ve etkileri birbirinden temelden farklıdır (Rieffel ve Polak, 2011).

Tablo 7.18'de measurement ve reset işlemleri karşılaştırılmaktadır.

Tablo 7.18. Measurement ve reset işlemlerinin karşılaştırması.

Özellik	Measurement (Ölçüm)	Reset (Sıfırlama)
Amaç	Kübitin durumunu öğrenmek	Kübiti zorla |0⟩ yapmak
Klasik çıktı var mı?	Evet, sonuç klasik registere yazılır	Hayır, klasik registere bilgi yazılmaz
Sonraki durum	Ölçüm sonucuna göre |0⟩ veya |1⟩	Her zaman |0⟩
Süperpozisyon korunur mu?	Hayır, çöker	Hayır, zorla |0⟩ yapılır
Kullanım senaryosu	Hesaplama sonucunu okuma	Kübiti yeniden kullanıma hazırlama, devre ortasında temiz kübit elde etme
Tersinir mi?	Hayır	Hayır

Özet: Measurement sonucu öğrenir ve klasik registere yazar; reset sonucu öğrenmeden kübiti zorla |0⟩ yapar. İkisi de süperpozisyonu bozar ve tersinir değildir (Şekil 7.15).

Reset
|0⟩

Reset kapısı, qubitin **o anki durumu ne olursa olsun onu zorla |0⟩ durumuna getirir.** Qubit |1⟩ durumundaysa → |0⟩ yapar Qubit süperpozisyondaysa → |0⟩ yapar Qubit zaten |0⟩ ise → |0⟩ kalır. Yani her durumda sonuç |0⟩ olur.

Ölçüm sonucu 0 veya 1 gelir, biz kontrol edemeyiz. Ama Reset her zaman 0 verir, rastgelelik yoktur.
Ölçüm → "bak bakalım ne çıkacak"
Reset → "ne olursa olsun sıfırla"

Ne zaman kullanılır?

- Devre ortasında bir qubiti yeniden kullanmak istediğinde (mid-circuit reset)
- Qubit sayısı sınırlıysa, aynı qubiti sıfırlayıp tekrar işlem yapmak için
- Başlangıç durumunu garantilemek istediğinde





Şekil 7.15. Reset kapısı; X→Reset→ölçüm devresi ve sonucun her zaman 0 çıkması (kaynak: sunum s. 27-28).

7.17 Faz Kavramı: Görünmez Ama Etkili

Faz (phase), kuantum hesaplamada en sık yanlış anlaşılan kavramlardan biridir. Öğrencilerin çoğu, "faz ölçümde görünmüyorsa ne işe yarar?" sorusunu sorar. Bu bölüm, faz kavramını sezgisel bir biçimde açıklamayı amaçlamaktadır.

7.17.1 Faz Nedir?

Bir kübitin durumu $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ olarak yazıldığında, α ve β karmaşık sayılardır. Her karmaşık sayı bir büyüklük ve bir açıdan oluşur: $\alpha = |\alpha|\cdot e^{(i\varphi)}$. İşte bu açı ($\varphi$), fazı temsil eder. $|0\rangle$ ve $|1\rangle$ bileşenleri arasındaki faz farkına "göreli faz" (relative phase) denir (Nielsen ve Chuang, 2010).

7.17.2 Faz Neden Ölçümde Doğrudan Görünmez?

Born kuralına göre ölçüm olasılıkları $|\alpha|^2$ ve $|\beta|^2$ ile belirlenir. Büyüklüğün karesi alındığında açı bilgisi (faz) kaybolur: $|e^{(i\varphi)}|^2 = 1$. Bu nedenle Z, S, T veya RZ gibi yalnızca faz değiştiren kapılar tek başına histogramı etkilemez.

7.17.3 Faz Neden Yine de Kritiktir?

Faz, sonraki kapılar tarafından görülür ve girişim (interference) desenlerini belirler. Kuantum algoritmaları; Deutsch-Jozsa, Grover, Shor; tamamıyla faz manipülasyonu üzerine kuruludur. Bu algoritmalarda faz kapıları ile Hadamard kapısının birlikte kullanılması, doğru cevabın genliğini büyütürken yanlış cevapların genliğini söndürür (Rieffel ve Polak, 2011).

Somut örnek: H → Z → H devresini düşünün. İlk H, $|0\rangle$ durumunu $(|0\rangle+|1\rangle)/\sqrt{2}$ süperpozisyonuna taşır. Z kapısı, $|1\rangle$ bileşenine -1 fazı ekleyerek durumu $(|0\rangle-|1\rangle)/\sqrt{2}$ yapar. Bu aşamada ölçüm yapılsaydı hâlâ %50-%50 sonuç görülürdü; faz "görünmez" gibidir. Ancak ikinci H kapısı uygulandığında, $H\cdot(|0\rangle-|1\rangle)/\sqrt{2} = |1\rangle$ sonucunu verir. Artık ölçümde kesinlikle $|1\rangle$ çıkar. Faz, ikinci Hadamard kapısı aracılığıyla ölçüm sonucunu tamamen belirlemiştir (Mermin, 2007).

Faz tek başına ölçümde görünmez; ama sonraki kapılara "hangi yöne döneceğini" söyler. Kuantum algoritmaların tüm gücü, bu görünmez fazı kontrol etmekten gelir.

Hadamard kapısı; süperpozisyon, |+⟩ ve |−⟩ faz farkı üzerinden yorumlanır (kaynak: sunum s. 15-21).

7.18 IBM Composer'dan Gerçek Kuantum Donanımında Çalıştırma

IBM Quantum Composer'da tasarlanan bir devre, yalnızca simülatörde değil gerçek kuantum donanımında da çalıştırılabilir. Devre, IBM Quantum Platform üzerinden uzaktaki bir kuantum bilgisayarına (örneğin ibm_kingston) iş (job) olarak gönderilir; sonuçlar tamamlandığında ölçüm dağılımı olarak geri alınır (slayt 75-78).

Tipik bir iş kaydında şu bilgiler yer alır: işin durumu (Completed), oluşturulma ve tamamlanma zamanı, toplam tamamlanma süresi, kullanılan kuantum bilgisayarı, bölge (region) ve giriş seçenekleri (örneğin init_qubits: true). Sonuçlar, klasik register "c" için ölçüm sonuçları (measurement outcomes) ve bit-bit sonuçlar (bit-by-bit outcomes) biçiminde sunulur; her olası çıktının frekansı bir histogramda gösterilir.

IBM Composer'dan gerçek donanıma iş gönderme süreci, iş (workload) durumu ve sonuç ekranları üzerinden izlenebilir (kaynak: sunum s. 75-78).

BÖLÜME AİT SUNUM SLAYTINA ERİŞİM İÇİN QR KOD

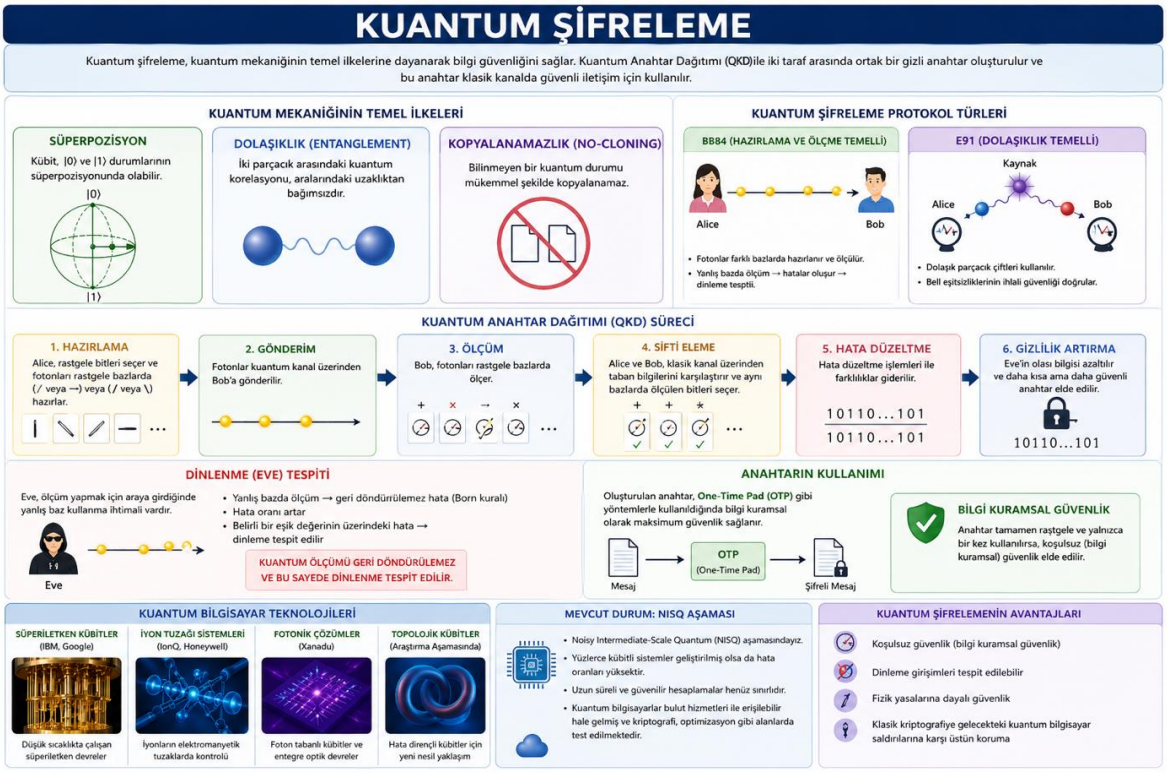
BÖLÜM 8

Kuantum Şifreleme

Kuantum şifreleme, bilgi güvenliğini klasik matematiksel yöntemlerden ziyade doğrudan kuantum mekaniğinin temel ilkelerine dayandıran yaklaşımları ifade etmektedir (Bennett ve Brassard, 2014). Bu sistemlerin temelinde süperpozisyon, dolanıklık ve kopyalanamazlık (no-cloning) ilkesi yer almaktadır (Ekert, 1991). Bu yaklaşımın en yaygın uygulama alanı Kuantum Anahtar Dağıtımı (QKD) olup, iki taraf arasında foton tabanlı bir kuantum kanal üzerinden ortak bir gizli anahtar oluşturulmasını sağlar. Oluşturulan bu anahtar, daha sonra klasik iletişim kanalı üzerinden gerçekleştirilen hata düzeltme ve gizlilik artırma süreçlerinden geçirilerek güvenli ve kullanılabilir hale getirilir. Hazırlama ve ölçme temelli protokollerin en bilinen örneği BB84 iken, dolanıklık temelli yaklaşım E91 protokolü ile temsil edilmektedir. Elde edilen anahtarın One-Time Pad (OTP) gibi yöntemlerle kullanılması durumunda, bilgi kuramsal açıdan maksimum güvenlik sağlanabilmektedir (Bennett ve Brassard, 2014).

Kuantum şifreleme sistemlerinin güvenliği, Hilbert uzayında tanımlanan kuantum durumlarının ölçüm kurallarına dayanmaktadır. Ölçüm işlemi yanlış bir bazda gerçekleştirildiğinde Born kuralı gereği geri döndürülemez hatalar oluşmakta ve bu durum izinsiz dinleme girişimlerinin tespit edilmesini mümkün kılmaktadır. Dolanıklık tabanlı protokollerde ise güvenlik, ölçüm sonuçları arasındaki korelasyonların Bell eşitsizliklerini ihlal edip etmediği üzerinden değerlendirilmektedir. Bu yönüyle kuantum şifreleme yalnızca teorik bir güvenlik yaklaşımı değil, aynı zamanda deneysel olarak doğrulanabilir bir sistemdir.

Bu yapı Şekil 8.1'de gösterilmektedir.



Şekil 8.1. Kuantum Şifreleme

Bu bağlamda kuantum bilgisayarların mevcut gelişim seviyesi de önemli bir rol oynamaktadır. Günümüzde süperiletken qubitler (IBM ve Google), iyon tuzağı tabanlı sistemler (IonQ ve Honeywell), fotonik çözümler (Xanadu) ve topolojik qubit yaklaşımları üzerine yoğun çalışmalar yürütülmektedir (Bayram ve Ilgaz Çağlayan, 2024). Ancak mevcut kuantum bilgisayarlar, NISQ (Noisy Intermediate-Scale Quantum) olarak adlandırılan aşamada yer almaktadır. Her ne kadar yüzlerce qubite sahip sistemler geliştirilmiş olsa da, hata oranlarının yüksek olması nedeniyle uzun süreli ve güvenilir hesaplamalar henüz sınırlıdır (Preskill, 2018). Buna rağmen kuantum bilgisayarlar artık yalnızca araştırma laboratuvarları ile sınırlı kalmayıp, bulut tabanlı hizmetler aracılığıyla erişilebilir hale gelmiş ve kriptografi ile optimizasyon gibi alanlarda aktif olarak test edilmeye başlanmıştır.

8.1 Klasik Şifreleme Yöntemleri

8.1.1 Simetrik (Gizli Anahtar) Şifreleme Sistemi

1970'li yıllarda açık anahtarlı şifreleme yöntemlerinin ortaya çıkışına kadar tüm kriptografik sistemler, günümüzde **gizli anahtar (simetrik) şifreleme** olarak adlandırılan farklı bir prensibe dayanarak çalışmaktaydı. Bu sistemlerde, gönderici mesajını şifrelemek için bir anahtar kullanırken, alıcının da aynı anahtar yardımıyla mesajı çözmesi gerekmektedir. Başka bir ifadeyle, şifreleme ve şifre çözme işlemlerinde kullanılan anahtar ortaktır ve her iki taraf tarafından da önceden paylaşılmış olmalıdır. Bu yöntemin en basit ve aynı zamanda en güçlü örneklerinden biri Vernam şifresidir (Vernam, 1926).

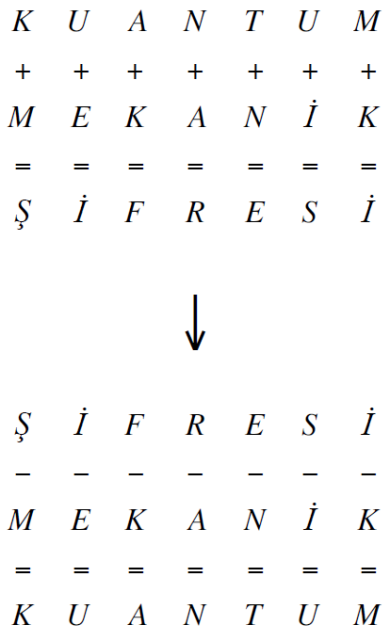
Bu sistemde gönderici ve alıcı, uzunluğu n bit olan ortak bir gizli anahtar dizisini paylaşır. Gönderici, mesajını bu anahtar ile birleştirerek şifrelerken, alıcı aynı anahtarı kullanarak şifreli mesajı çözmektedir. Vernam şifresinin en önemli özelliği, anahtarın tamamen gizli kalması durumunda **kanıtlanabilir güvenlik** sağlamasıdır. Her ne kadar iletişim kanalı üzerinden gerçekleştirilen dış müdahaleler (gürültü veya dinleme girişimleri) mümkün olsa da, gönderici ve alıcı bu tür anormallikleri tespit edebilir ve iletişimin güvenliğini değerlendirebilir. Ayrıca, herhangi bir dinleme stratejisi karşısında, uygun yöntemler kullanılarak bilgi sızıntısı istenildiği kadar azaltılabilmektedir (Nielsen ve Chuang, 2000).

Buna karşılık, günümüzde yaygın olarak kullanılan açık anahtarlı şifreleme sistemlerinin güvenliği, belirli matematiksel problemlerin çözüm zorluğuna dayanmaktadır. Örneğin büyük sayıların asal çarpanlara ayrılması problemi klasik bilgisayarlar için zor kabul edilirken, kuantum bilgisayarlar üzerinde çalışan Shor algoritması ile bu problem etkin bir şekilde çözülebilmektedir (Shor, 1995). Bu durum, klasik kriptografik sistemlerin gelecekteki güvenliği açısından önemli bir risk oluşturmaktadır.

Gizli anahtar şifreleme sistemlerinin en büyük zorluklarından biri ise anahtarın güvenli bir şekilde dağıtılmasıdır. Özellikle Vernam şifresinde, anahtar uzunluğunun en az mesaj uzunluğu kadar olması ve aynı anahtarın tekrar kullanılmaması gerekmektedir. Bu durum, pratik uygulamalarda oldukça uzun anahtar dizilerinin oluşturulmasını zorunlu kılmakta ve sistemin kullanımını sınırlamaktadır. Ayrıca anahtarların kullanım öncesinde güvenli bir şekilde saklanması ve kullanım sonrasında imha edilmesi gerekmektedir. Klasik bilginin kolaylıkla kopyalanabilir olması da güvenlik açısından ek bir risk oluşturmaktadır.

Tüm bu sınırlamalara rağmen, Vernam şifresi gibi gizli anahtar şifreleme yöntemleri, özellikle güvenli anahtar paylaşımının mümkün olduğu ortamlarda, kanıtlanabilir güvenlik sağlamaları nedeniyle günümüzde de kullanılmaya devam etmektedir (Nielsen ve Chuang, 2000). Simetrik şifreleme sistemlerinin genel yapısı Şekil 2'de gösterilmektedir.

Bu yapı Şekil 8.2'de gösterilmektedir.



Şekil 8.2. Herkesin erişimine açık kanalda gizli anahtar şifreleme yöntemi, Vernam şifresi

8.1.2 Asimetrik (Açık Anahtar) Şifreleme Sistemi

Bu şifreleme yaklaşımı, şifreleme ve şifre çözme işlemlerinde farklı anahtarların kullanılması prensibine dayanır. Açık anahtarlı kriptografinin temelleri ilk kez Stanford Üniversitesi'nden Whitfield Diffie ve Martin Hellman tarafından 1976 yılında ortaya konmuştur (Diffie ve Hellman, 1976). Bu yaklaşımın ilk pratik uygulaması ise Massachusetts Institute of Technology'de Ronald Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiştir (Rivest, Shamir, ve Adleman, 1978). Bu üç araştırmacının isimlerinin baş harflerinden oluşan RSA algoritması, günümüzde de yaygın olarak kullanılan temel açık anahtarlı şifreleme yöntemlerinden biridir.

Açık anahtar şifreleme sistemlerinde alıcı, kendisine gönderilecek mesajları güvenli şekilde alabilmek için gizli tuttuğu bir **özel anahtar (private key)** belirler. Bu özel anahtardan türetilen **açık anahtar (public key)** ise herkesle paylaşılabilir. Gönderici, mesajını bu açık anahtarı kullanarak şifreler ve yalnızca ilgili alıcının sahip olduğu özel anahtar ile çözülebilecek şekilde iletir. Bu yapı, herkesin mesaj gönderebildiği ancak yalnızca yetkili kişinin mesajı okuyabildiği bir posta kutusu sistemine benzetilebilir. Günümüzde internet güvenliğinin büyük bir kısmı bu tür açık anahtarlı sistemlere dayanmaktadır.

Açık anahtarlı şifreleme yöntemlerinin güvenliği, matematiksel olarak zor problemlere dayalıdır. Bu sistemlerde genellikle **tek yönlü fonksiyonlar** kullanılır. Bu fonksiyonlarda ileri yönde hesaplama kolayken, tersine işlem oldukça zordur. Örneğin iki sayının çarpımını hesaplamak kısa sürede mümkünken, elde edilen büyük bir sayıyı asal çarpanlarına ayırmak çok daha karmaşık ve zaman alıcıdır. RSA algoritmasının güvenliği de büyük sayıların asal çarpanlara ayrılmasının zorluğuna dayanmaktadır.

Ancak bu yaklaşım bazı temel belirsizlikler içermektedir. Özellikle asal çarpanlara ayırma probleminin gerçekten zor olup olmadığı matematiksel olarak kesin biçimde kanıtlanmış değildir (Nielsen ve Chuang, 2000). Günümüzde bu işlemi hızlı şekilde gerçekleştiren klasik bir algoritma

bulunmasa da, gelecekte geliştirilebilecek yeni yöntemler mevcut sistemlerin güvenliğini tehdit edebilir. Bu durum, açık anahtarlı şifreleme sistemlerinin güvenliğinin belirli varsayımlara dayandığını göstermektedir.

Bu belirsizlikler nedeniyle, özellikle yüksek güvenlik gerektiren uygulamalarda bu tür sistemler potansiyel riskler barındırmaktadır. Örneğin matematikte yapılacak önemli bir keşif, mevcut kriptografik altyapıları aniden geçersiz hale getirebilir ve ekonomik sistemler üzerinde ciddi etkiler oluşturabilir. Bu tür riskleri azaltmak amacıyla, güvenliği matematiksel varsayımlardan bağımsız olan **simetrik şifreleme yöntemleri** bazı durumlarda daha güvenilir bir alternatif olarak değerlendirilmektedir.

Örnek: RSA Şifreleme (Le Bellac, 2006)

AES

Alıcı iki asal sayı seçer, p ve q. N = p.q olarak tanımlanır ve bir c sayısı (p q- 1) çarpımıyla hiçbir ortak bölene sahip değildir. Mod(p q- 1) in c ye bölümüyle d hesaplanır.−1)(−1)(

$$c.d \equiv 1 mod (p-1)(q-1) \quad (8.1)$$

Güvensiz bir yolla, alıcı *N* ve *c* sayılarını göndericiye yollar (p ve q yu ayrı ayrı değil!). Gönderici alıcıya bir $a < N$ sayısıyla temsil edilmek zorunda olan şifrelenmiş bir mesaj yollamak ister (Mesaj çok uzunsa, gönderici onu alt mesajlara bölebilir). Sonra

$$b \equiv a^c c mod N \quad (8.2)$$

yi hesaplar. Alıcıya *b* yi yollar, her zaman güvensiz bir yolla, çünkü yalnızca *N*,*b* ve *c* yi bilen bir bilgi hırsızı orjinal mesajı a yı çıkaramaz. Alıcı mesajı aldığında

$$b^d mod N = a \quad (8.3)$$

yı hesaplar. Sonucun kesin olarak a olduğu gerçeği, yani göndericinin ilk mesajı sayı teorisinin bir sonucudur. Özetlersek *N*,*b* ve *c* sayıları herkesin erişimine açık bir yolla, güvensiz bir şekilde yollanılır.

Alıcının seçtiği sayısal değerler p = 3 ve q = 7 olsun. N=p.q =3.7 = 21 ve (p -1)(q -1) =(3 -1).(7 -1) = 12 olur. c = 5 sayısının 12 ile hiçbir ortak böleni yoktur ve mod12 çarpımına göre tersi d = 5 tir. Çünkü 5X 5 = 24 +1. Alıcı N = 21 ve c = 5 sayılarını göndericiye yollar. Gönderici ise a = 4 seçer ve (8.2) yi kullanarak

$$4^5 = 1024 = 21x48 + 16 \quad (8.4)$$

$$4^5 \equiv 16 mod 21 \quad (8.5)$$

hesabını yapar ve (8.5) ifadesinden *b* yi 16 olarak hesaplar ve alıcıya yollar. Alıcı *b* mesajını aldıktan sonra (8.3) ifadesini kullanarak a yı bulur:

$$b^5 = 16^5 = 49932x21 + 4 \quad (8.6)$$

$$16^5 \equiv 4mod21. \quad (8.7)$$

Böylece a = 4 orjinal mesajını keşfeder. Diğer bir örneğimiz şöyle olsun: Alıcı p = 2 ve q = 5 i seçsin. N=p.q =2.5 = 10 ve (p −1)(q -1) (2 −1).(5−1) = 4 olur. c = 3 sayısının 4 ile hiçbir ortak böleni yoktur ve mod 4 çarpımına göre tersi d = 3 tür. Çünkü 3X 3 = 8 + 1. Alıcı N = 10 ve c = 3 sayılarını göndericiye yollar. Gönderici ise a = 6 seçer ve (8.2) yi kullanarak

$$6^3 = 10x21 + 6 \quad (8.8)$$

$$6^3 \equiv 6mod(10) \quad (8.9)$$

hesaplarını yapar. (8.9) ifadesinden b = 6 bulur ve bu sonucu alıcıya iletir. Alıcı ise (8.3) ifadesini kullanarak a yı bulur:

$$b^5 = 6^5 = 777x10 + 6 \quad (8.10)$$

$$6^5 \equiv 6mod10. \quad (8.11)$$

Böylece a = 6 orjinal mesajını elde eder.

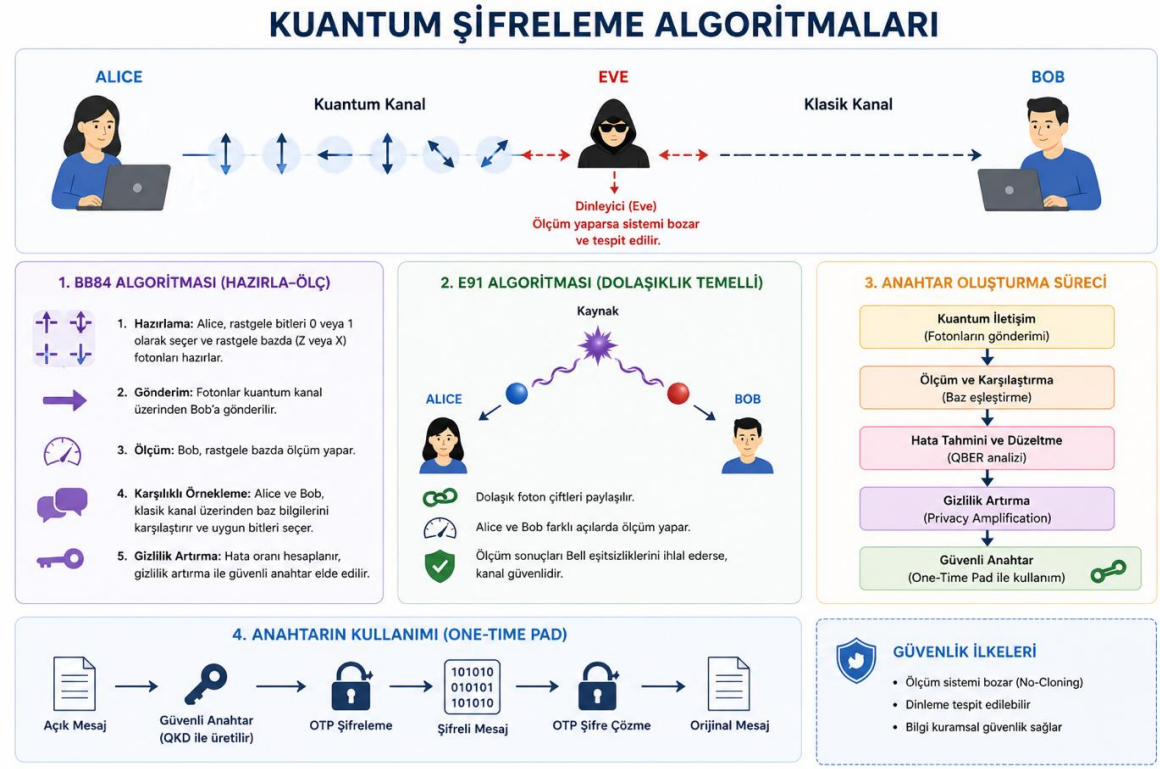
8.2 Kuantum Şifreleme Algoritmaları

Kuantum şifreleme, kuantum mekaniğinin ölçüm sırasında sistemi bozma özelliği ile kopyalanamazlık (no-cloning) ilkesini kullanarak, bilgi kuramsal açıdan güvenli anahtar üretimi ve iletimini mümkün kılan protokolleri kapsar. Pratik uygulamalarda güvenli iletişim, üretilen bu anahtarın One-Time Pad (OTP) gibi yöntemlerle kullanılmasıyla sağlanır. Hazırla-ölç (prepare-and-measure) yaklaşımının en bilinen örneği olan BB84 protokolü, farklı ölçüm bazlarında yapılan karşılıklı örnekleme ve hata oranı analizleri sayesinde olası bir dinleyicinin (Eve) varlığını tespit edebilir ve ardından gizlilik artırma (privacy amplification) süreçleri ile güvenli bir anahtar uzlaşımı gerçekleştirir (Bennett ve Brassard, 2014). Buna karşılık, dolanıklık temelli E91 protokolü güvenliğini Bell eşitsizliklerinin (örneğin CHSH testi) ihlal edilmesine dayandırarak, özellikle kaynağın güvenilir olmadığı senaryolarda daha sağlam bir yaklaşım sunar (Ekert, 1991).

Gerçek dünya uygulamalarında ise ideal koşullar yerine daha karmaşık ve kusurlu sistemler söz konusudur. Bu nedenle çok fotonlu zayıf koherent kaynaklar, Decoy-State yöntemi ile kontrol altına alınır; dedektör kaynaklı güvenlik açıkları Measurement-Device-Independent QKD (MDI-QKD) ile azaltılır; ayrıca Continuous-Variable (CV) tabanlı yaklaşımlar kullanılarak fiber ve serbest uzay iletişim kanallarında verimlilik artırılır. Tüm bu sistemler, sonlu anahtar uzunlukları dikkate alınarak evrensel-birleşik (composable) güvenlik çerçevesinde analiz edilir (Pirandola vd., 2020). Kuantum şifreleme olarak adlandırılan bu yöntemler, post-kuantum kriptografi yaklaşımlarından farklı bir amaca hizmet eder. QKD, anahtar üretimini fiziksel yasalar temelinde gerçekleştirirken; post-kuantum algoritmalar klasik şifreleme sistemlerini kuantum saldırılarına karşı dayanıklı hale getirmeyi hedefler. Bu iki yaklaşım birlikte kullanıldığında uçtan uca daha güçlü bir güvenlik yapısı elde edilir (Pirandola vd., 2020).

Uygulamada elde edilen gizli anahtar oranı; kuantum bit hata oranı (QBER), dedektör verimliliği, kanal kayıpları ve hata düzeltme sırasında ortaya çıkan bilgi sızıntısı gibi parametrelere bağlıdır. Bu nedenle sistem performansının optimize edilmesi için bu metriklerin dikkatli şekilde kontrol edilmesi gerekir. Ayrıca cihaz kaynaklı hataların etkisini azaltmak amacıyla, model tabanlı analizler veya cihazdan bağımsız güvenlik yaklaşımları tercih edilmektedir (Pirandola vd., 2020).

Bu yapı Şekil 8.3'te gösterilmektedir.



Şekil 8.3. Kuantum Şifreleme Algoritmaları

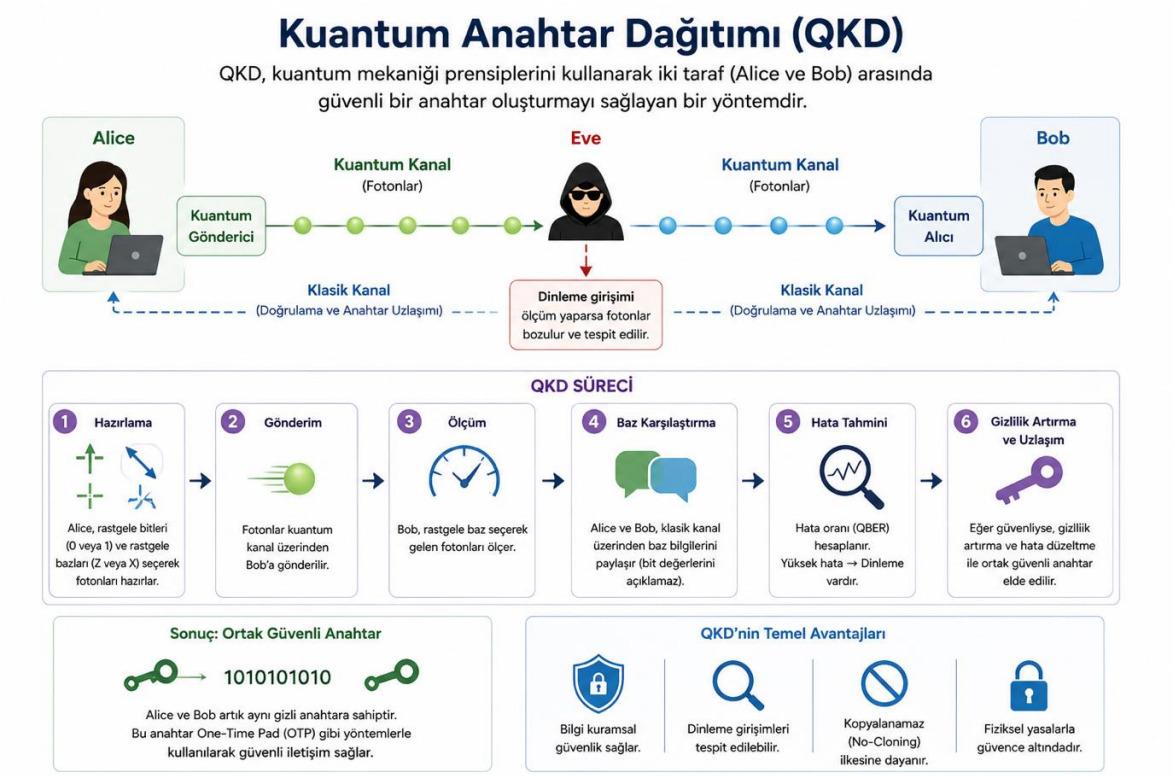
8.2.1 Kuantum Anahtar Dağıtımı (QKD)

Kuantum Anahtar Dağıtımı (Quantum Key Distribution, QKD), kuantum kriptografi alanında geliştirilen ve klasik kriptografik yöntemlere kıyasla daha yüksek güvenlik sağlamayı amaçlayan yenilikçi bir yaklaşımdır. BB84, E91, B92, SARG04, Six-State, Decoy-State BB84, DPS, RRDPS, COW, MDI, TF, DI, CV ve CV-MDI gibi birçok protokol, güvenli anahtar üretimi için bu çerçevede geliştirilmiştir. Geleneksel kriptografik sistemler güvenliklerini, büyük asal sayıların çarpanlara ayrılması gibi matematiksel problemlerin çözüm zorluğuna dayandırmaktadır. Ancak kuantum bilgisayarların gelişimi, bu tür problemlerin daha kısa sürede çözülebilme ihtimalini doğurarak klasik yöntemlerin güvenliğini tehdit etmektedir.

Buna karşılık QKD sistemleri, güvenliğini doğrudan kuantum mekaniğinin temel ilkelerinden almaktadır. Özellikle Heisenberg Belirsizlik İlkesi ve kuantum durumlarının kopyalanamazlığı (no-cloning) bu sistemlerin güvenliğinin temelini oluşturur. Bu prensiplere göre, bir qubit üzerinde yapılan ölçüm işlemi, sistemin durumunu kaçınılmaz olarak değiştirir. Dolayısıyla iletişim hattına müdahale etmeye çalışan bir dinleyici (Eve), farkında olmadan sistemde hatalara neden olur ve bu durum gönderici

(Alice) ile alıcı (Bob) tarafından tespit edilebilir. Bu özellik, QKD'nin en önemli avantajlarından biri olan dinleme tespiti mekanizmasını mümkün kılar.

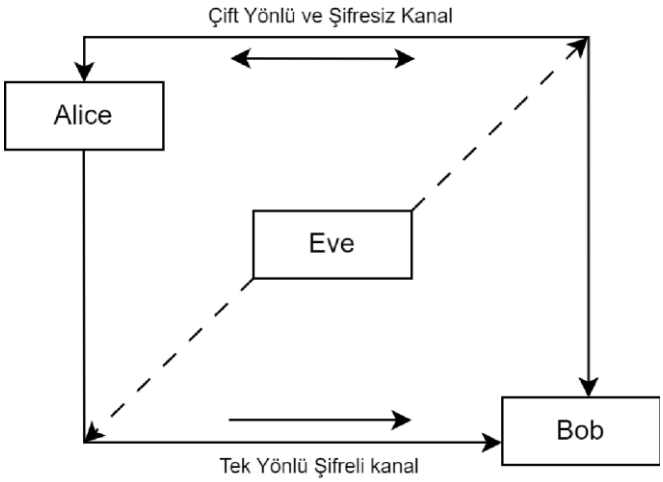
Bu yapı Şekil 8.4'te gösterilmektedir.



Şekil 8.4. Kuantum Anahtar Dağıtımı (QKD)

QKD protokolleri arasında en yaygın olarak bilinenlerden biri BB84 protokolüdür. 1984 yılında Bennett ve Brassard tarafından önerilen bu protokol, kuantum bitlerinin iki farklı bazda tanımlanan dört kuantum durumu kullanılarak kodlanmasına dayanır (Bennett ve Brassard, 2014). Gönderici ve alıcının rastgele baz seçimleri yapması sayesinde, üçüncü bir tarafın doğru bazda ölçüm yapma olasılığı düşer ve bu da saldırıların tespit edilmesini sağlar. Diğer önemli bir protokol olan Ekert91 (E91) ise 1991 yılında Ekert tarafından geliştirilmiş olup, kuantum dolanıklık prensibini temel alır (Ekert, 1991). Bu yaklaşımda güvenlik, ölçüm sonuçları arasındaki korelasyonların Bell eşitsizliklerini ihlal etmesine dayandırılır. Bu nedenle E91 protokolü, özellikle güvenilir olmayan kaynaklara karşı daha güçlü bir güvenlik modeli sunmaktadır.

Bu yapı Şekil 8.5'te gösterilmektedir.



Şekil 8.5. Kuantum İletişim Örneği

Kuantum şifreleme sistemlerinde iletişim genellikle üç temel aktör üzerinden tanımlanır: gönderici (Alice), alıcı (Bob) ve olası dinleyici (Eve). Bu taraflar arasındaki etkileşim ve iletişim süreci genel olarak Şekil 5'de gösterildiği gibi modellenmektedir.

Alice ve Bob arasında kurulan sistemde, kullanılan ölçüm bazları çift yönlü ancak şifresiz bir klasik kanal üzerinden karşılıklı olarak paylaşılmaktadır. Buna karşılık, Alice'in Bob'a ilettiği asıl mesaj tek yönlü ve şifreli bir kanal aracılığıyla gönderilmektedir. Sistemde üçüncü taraf olan Eve'in temel amacı ise, Alice ve Bob fark etmeden bu iletişimi dinlemek ve bilgi elde etmektir. Kuantum şifreleme protokolleri, bu tür yetkisiz erişim girişimlerini tespit edebilmek amacıyla kuantum mekaniğinin bazı temel prensiplerinden yararlanarak çalışmaktadır. Bu prensipler aşağıda özetlenmektedir:

Süperpozisyon İlkesi: Kuantum mekaniğinde, bir sistem birden fazla durumla aynı anda sahip olabilir. Örneğin, bir qubit hem |0⟩ hem de |1⟩ durumlarında bulunabilir. Bir qubitin süperpozisyonu denklem (8.12)'de gösterildiği gibi ifade edilir.

$$\psi = \alpha 0 + \beta 1 \quad (8.12)$$

Burada α ve β kompleks sayılar olup $|\alpha|^2 + |\beta|^2 = 1$ koşulu sağlanır.

Ölçüm İlkesi: Bir kuantum sistem ölçüldüğünde sistem süperpozisyonunu koruyamaz ve belirli bir durum alır. Bir qubitin ölçümü onu |0⟩ ve |1⟩ arasındaki durumlardan birini almaya zorlar.

Dolanıklık İlkesi: İki veya daha fazla kuantum sistem birbiriyle dolanık hale gelebilir bu noktada sistemler birbirlerinden bağımsız olarak ele alınamaz. Dolanıklık, kuantum şifreleme protokollerinin güvenliğinde elzemdir.

8.2.2 BB84 Protokolü

BB84 protokolü, 1984 yılında Charles Bennett ve Gilles Brassard tarafından önerilen ilk kuantum anahtar dağıtımı (QKD) yöntemidir (Bennett ve Brassard, 2014). Bu protokolde, rastgele oluşturulan bit dizilerinden oluşan gizli anahtarın güvenli bir şekilde paylaşılması amacıyla tek fotonlar kullanılmaktadır. Her bir foton, dört olası polarizasyon durumundan biriyle hazırlanmakta ve bu durumlar iki farklı eşlenik baz üzerinden seçilmektedir. Bu bazlardan ilki, dikey ve yatay polarizasyonları içeren doğrusal baz; diğeri

ise çapraz ve karşıt çapraz polarizasyonları kapsayan diyagonal baz olarak tanımlanmaktadır. BB84 protokolünde kullanılan bu kuantum durumları, Dirac notasyonu ile aşağıdaki şekilde ifade edilmektedir:

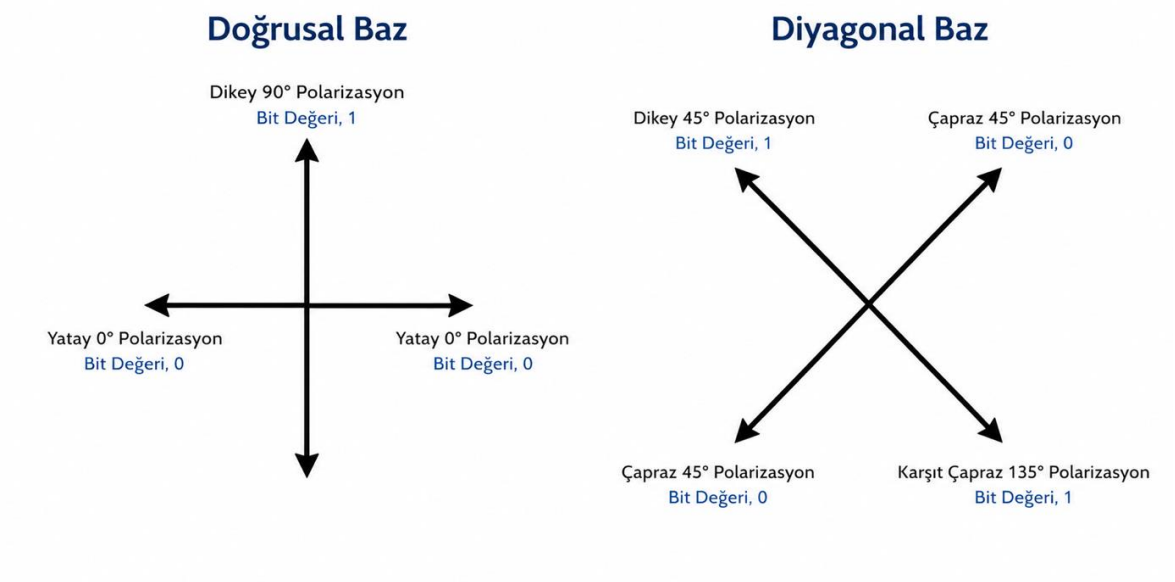
Doğrusal Baz:

$$0 \geq (10), \vee 1 \geq (01) \quad (8.13)$$

Diyagonal Baz:

$$+ = \frac{1}{\sqrt{2}}(11), \vee \rightarrow = \frac{1}{\sqrt{2}}(1-1) \quad (8.14)$$

Bu yapı Şekil 8.6'da gösterilmektedir.



Şekil 8.6. BB84 Protokolü İçin Bazlar ve Bit Değerleri

BB84 protokolünde iletişim örneği:

• Alice, 0 ve 1 bitlerinden oluşan bir bit dizisi seçer. Örneğin, 0, 1, 1, 0, 0, 1, 0, 1 dizisi seçilsin.

• Alice, her bir bit için rastgele bir baz seçer. Doğrusal baz (ör. yatay ve dikey) şeklinde polarize eder. Benzer şekilde diyagonal baz seçimi de 0 ve 1 bitleri, sırasıyla +45◦ ve −45◦ ile şeklinde polarize edilir. Örneğin, ×, +, +, ×, +, ×, +, × bazları seçilsin.

• Alice, her bir bitini seçtiği baz kullanarak kuantum durumuna dönüştürür ve Bob'a gönderir.

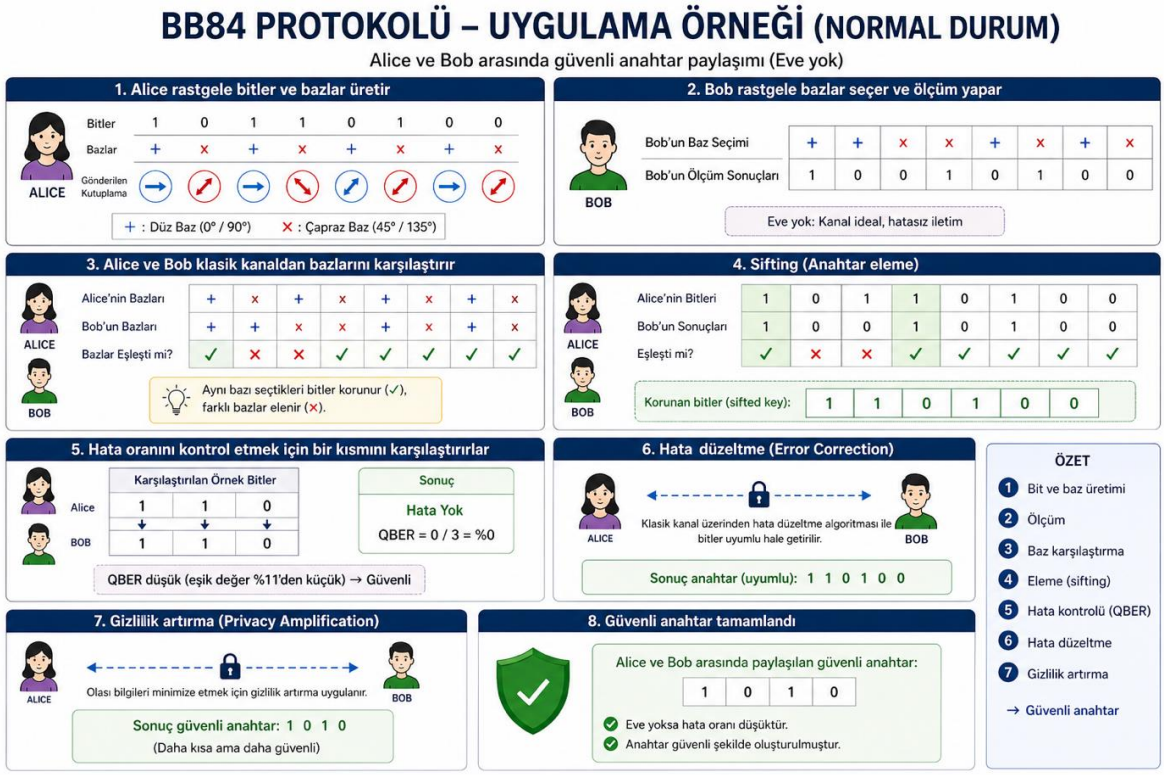
• Bob, Alice'ten gelen her foton için rastgele bir baz seçer. Örneğin, +, +, +, ×, ×, +, ×, × bazları seçsin.

• Bob, seçtiği bazları kullanarak her bir fotonu ölçer ve elde ettiği bit değerlerini kaydeder. Eğer Bob'un seçtiği baz, Alice'in seçtiği baz ile aynıysa doğru bit değeri ölçülmüş olur.

• Alice ve Bob, seçtikleri bazları birbirleriyle paylaşır, bu bilgiyi güvenli bir kanal üzerinden paylaşırlar ve bit değerlerini paylaşmazlar.

• Alice ve Bob, aynı baz kullandıkları bitleri seçer ve bu bitleri güvenli anahtar olarak kullanır.

Bu yapı Şekil 8.7'de gösterilmektedir.



Şekil 8.7. BB84 ÖRNEĞİ

BB84 protokolünde güvenliğin en önemli ölçütlerinden biri, kuantum bit hata oranı (Quantum Bit Error Rate, QBER) olarak bilinen parametredir.

$$QBER = \frac{N_{hata}}{N_{toplam}} \quad (8.15)$$

Bu ifadede Nhata hata sayısını, Ntoplam ise toplam qubit sayısını temsil etmektedir. QBER (Quantum Bit Error Rate), gönderilen ve alıcı tarafından ölçülen qubitler arasındaki uyuşmazlık oranını ifade eder ve bu değerin düşük olması, oluşturulan anahtarın güvenilirliğinin yüksek olduğunu gösterir. QBER'i etkileyen başlıca faktörler arasında kuantum kanalındaki gürültü, kullanılan donanım bileşenlerindeki kusurlar ve olası saldırganların gerçekleştirdiği dinleme girişimleri yer almaktadır.

Literatürde yapılan çalışmalar, QBER değerinin yaklaşık %11 seviyesine kadar olduğu asimptotik analizlerde BB84 protokolünün güvenli kabul edilebileceğini göstermektedir (Watanabe, Matsumoto, ve Uyematsu, 2006). Bununla birlikte, hata oranının %25'in üzerine çıkması durumunda sistem güvenliğinin ciddi şekilde tehlikeye girdiği kabul edilir (Nikolopoulos ve Alber, 2004). Bazı gelişmiş saldırı senaryolarında ise bu kritik eşik daha düşük değerlere, örneğin yaklaşık %17.7 seviyesine kadar indirilebilmektedir (Xu, Qi, ve Lo, 2010). Bu tür yüksek hata oranları, iletişim kanalına müdahale eden bir saldırganın (Eve) qubitlerin önemli bir kısmını dinlediğini veya manipüle ettiğini göstermektedir.

BB84 protokolünde anahtar üretim hızı (key rate), sistemin güvenli bir şekilde ne kadar veri üretebildiğini belirleyen önemli bir performans ölçütüdür. Bu değer, doğrudan hata oranına ve iletişim kanalındaki kayıplar ile gürültü seviyesine bağlı olarak değişmektedir. Güvenli anahtar oranı genellikle aşağıdaki matematiksel ifade ile tanımlanmaktadır:

$$R = Q \cdot [1 - h(e)] \quad (8.16)$$

Burada R güvenli anahtar oranını, Q kuantum bitlerinin başarılı iletim oranını ve e hata oranını temsil eder. h(e) ise Shannon entropisi ile ilişkili bir fonksiyondur ve

$$h(e) = -elog2e - (1-e)log2(1-e) \quad (8.17)$$

şeklinde tanımlanır. Bu formül, hata oranının artmasıyla güvenli anahtar oranının azaldığını gösterir (Sano, Matsumoto, ve Uyematsu, 2010).

8.2.3 E91 Protokolü

E91 protokolü, 1991 yılında Artur Ekert tarafından önerilen ve kuantum mekaniğinin temel ilkelerine dayanan bir kuantum anahtar dağıtım (QKD) yöntemidir (Ekert, 1991). Bu protokol, BB84 gibi daha önce geliştirilen yaklaşımlardan farklı olarak kuantum dolanıklık ve Bell teoremi üzerine kuruludur. E91'de, Alice ve Bob güvenli bir anahtar elde edebilmek için dolaşık foton çiftlerinden yararlanır. Bu çiftler, Bell durumları olarak adlandırılan özel süperpozisyon hallerinde bulunur ve iki parçacık arasında güçlü bir kuantum korelasyonu oluşturur. Bu sayede, taraflar arasındaki ölçüm sonuçları belirli ilişkiler sergiler ve bu ilişkiler güvenlik doğrulaması için kullanılabilir. E91 protokolünde kullanılan dört temel Bell durumu aşağıdaki gibi tanımlanmaktadır:

$$\psi^{+\rangle=\frac{1}{\sqrt{2}}(\mathrm{V}01\rangle+10\rangle)} \quad (8.18)$$

$$\psi^{-\rangle=\frac{1}{\sqrt{2}}(\mathrm{V}01\rangle-10\rangle)} \quad (8.19)$$

$$\phi^{+\rangle=\frac{1}{\sqrt{2}}(\mathrm{V}00\rangle+11\rangle)} \quad (8.20)$$

$$\phi^{-\rangle=\frac{1}{\sqrt{2}}(\mathrm{V}00\rangle-11\rangle)} \quad (8.21)$$

Bu dört Bell durumu, iki qubit arasında kuantum dolanıklığın varlığını ifade eder ve bu durumlar arasındaki fark, qubitlerin birbirleriyle aynı ya da zıt korelasyon göstermesine bağlıdır. E91 protokolünde çoğunlukla |⟩|\psi^{-}\rangle|⟩ durumu tercih edilmekle birlikte, diğer Bell durumları da aynı temel prensiplere dayanarak kullanılabilmektedir. Klasik sistemlerde Bell parametresi SSS en fazla 2 değerini alabilirken, kuantum dolanık sistemlerde bu değer 222\sqrt{2}22'ye kadar ulaşabilmektedir. Bu durum, klasik fizik ile kuantum mekaniği arasındaki temel farkı ortaya koymaktadır. Bell parametresi SSS, aşağıdaki denklem kullanılarak hesaplanmaktadır:ψ−ψ−

$$S = E(\theta A, \theta B) - E(\theta A, \theta' B) + E(\theta' A, \theta B) + E(\theta' A, \theta' B) \quad (8.22)$$

Burada, E $(\theta A,\ \theta B)$ ifadesi, Alice ve Bob'un θA ve θB açılarında yaptıkları ölçümlerin korelasyonlarını temsil eder ve şu şekilde tanımlanır:

$$E(\theta A, \theta B) = P(\theta A, \theta B) - P(\theta A, \theta B) \quad (8.23)$$

P (Alice = Bob| $\theta A,\ \theta B$) Alice ve Bob'un aynı sonucu elde etme olasılığını temsil eder. Kuantum mekaniğine göre, Bell parametresinin S değeri şu aralıkta olacaktır:

$$2 < |S| \leq 2\sqrt{2}. \quad (8.24)$$

E91 protokolünde iletişim adım adım şu şekilde gerçekleşir:

- Alice ve Bob, birbirlerine göndermek üzere kuantum dolanık qubit çiftleri alır. Bu dolanık qubitler genellikle Bell durumundadır. Yani, Alice'in qubiti bir durumda ölçüldüğünde, bob'un qubiti de buna göre anında belirlenir.
- Alice ve Bob, qubitleri hangi tabanda ölçüm yapacaklarını rastgele seçerler:

$$0\rangle = (10), \vee 1\rangle = (01) \quad (8.25)$$

$$+\rangle = \frac{1}{\sqrt{2}}(\vee 0\rangle + 1\rangle), \vee -\rangle = \frac{1}{\sqrt{2}}(\vee 0\rangle - 1\rangle), \quad (8.26)$$

- Alice ve Bob, seçtikleri tabanlarda ölçüm yapar. Eğer Alice ve Bob aynı tabanı seçmişse, qubitlerin ölçüm sonuçları tamamen korele olacaktır; Alice $|0\rangle$ ölçtüğünde Bob kesinlikle $|1\rangle$ ölçecektir. Korelasyon fonksiyonu deneyden toplanan verilerle hesaplanır.
- Alice ve Bob, klasik bir iletişim kanalı üzerinden hangi tabanları kullandıklarını karşılaştırır. Taban seçimlerini paylaştıktan sonra, aynı tabanı seçtikleri ölçümlerden kalanlar anahtar bitlerini oluşturur; farklı tabanlarda ölçülmüş sonuçlar atılır.
- Alice ve Bob, seçilmemiş sonuçlardan yararlanarak S parametresini hesaplayıp protokolün güvenliğini doğrular.
- S değeri uygun aralıkta ise, belirlenmiş ölçüm sonuçlarını birleştirerek bir ham anahtar oluştururlar. Aynı tabanda yapılan ölçümler anahtarı oluşturur; farklı tabanlarda alınan sonuçlar test bitleri olarak kullanılır.
- Hata düzeltme işlemlerinden ardından, Eve'in olası bilgi kazanımını minimuma indirmek ve ham anahtarın güvenliğini artırmak için gizlilik güçlendirme işlemleri uygulanır.

Bilgi kaybı tahmini olarak adlandırılan süreçte, Eve'in elde edebileceği bilgi miktarı; Von Neumann entropisi, karşılıklı bilgi ölçütleri ve Bell eşitsizlikleri gibi matematiksel araçlar kullanılarak değerlendirilir. Bu analizler sayesinde, potansiyel bilgi sızıntısının ne düzeyde olduğu belirlenebilir. Elde edilen ham anahtarın daha güvenli hale getirilmesi için ise evrensel karma (hash) fonksiyonları kullanılarak gizlilik artırımı (privacy amplification) uygulanır.

Örneğin, uzunluğu nnn bit olan bir ham anahtar için Eve'in en fazla mmm bitlik bilgiye sahip olduğu tahmin ediliyorsa, Alice ve Bob kalan n−mn - mn−m bitlik kısmı güvenli anahtar olarak kullanabilirler (Scarani vd., 2009). Bu işlem, anahtar uzunluğunu azaltmakla birlikte güvenlik seviyesini artırır. Matematiksel olarak, evrensel bir karma fonksiyonu h(x)h(x)h(x) aşağıdaki şekilde ifade edilebilir:

$$h(x) = \big(h1(x), h2(x), \ldots, hk(x)\big) \quad (8.27)$$

5. Gizlilik güçlendirme işlemi sonrasında Alice ve Bob güvenli bir son anahtara sahip olurlar. Bu anahtar; tek kullanımlık şifre (OTP) ya da AES/DES gibi simetrik şifreleme algoritmalarında kullanılabilir.

6. Eğer ilk turda yeterince uzun ve güvenli bir anahtar elde edilemezse, Alice ve Bob protokolü tekrar ederler. Bu, kuantum kanalındaki gürültü seviyesine ve hata oranlarına bağlı olarak birden fazla kez gerekebilir. Protokol tekrarlanarak, nihai güvenli anahtar uzunluğu artırılır.

Bu adımların her biri, E91 protokolünün güvenliğini sağlamak için gereklidir. Bu süreçte kullanılan matematiksel araçlar, klasik kriptografinin ötesine geçerek kuantum mekaniğinin prensiplerinden yararlanır ve bu sayede çok daha güçlü bir yapı inşa eder.

BB84 protokolünde olduğu gibi, E91 protokolü için de kuantum bit hata oranı (QBER) tanımlanmaktadır. Ancak BB84'ten farklı olarak, E91'de hata analizi iki dolaşık fotondan elde edilen ölçüm sonuçları arasındaki rastlantısal olaylara dayanmaktadır. Bu bağlamda, toplam rastlantı olasılığı PrastlantıP_{rastlantı}Prastlantı iki bileşene ayrılarak incelenir.

Bunlardan PasılP_{asıl}Pasıl, dolaşık foton çiftlerinden kaynaklanan gerçek rastlantı olasılığını ifade ederken; PsahteP_{sahte}Psahte, ideal olmayan kaynaklar, ortam gürültüsü veya fonon gibi mekanik etkiler sonucu oluşan hatalı sayımlardan kaynaklanan sahte rastlantı olasılığını temsil etmektedir.

$$Prastlantı = Pasıl + Psahte \quad (8.28)$$

ve QBER şöyle ifade edilir (Waks, Zeevi, ve Yamamoto, 2002):

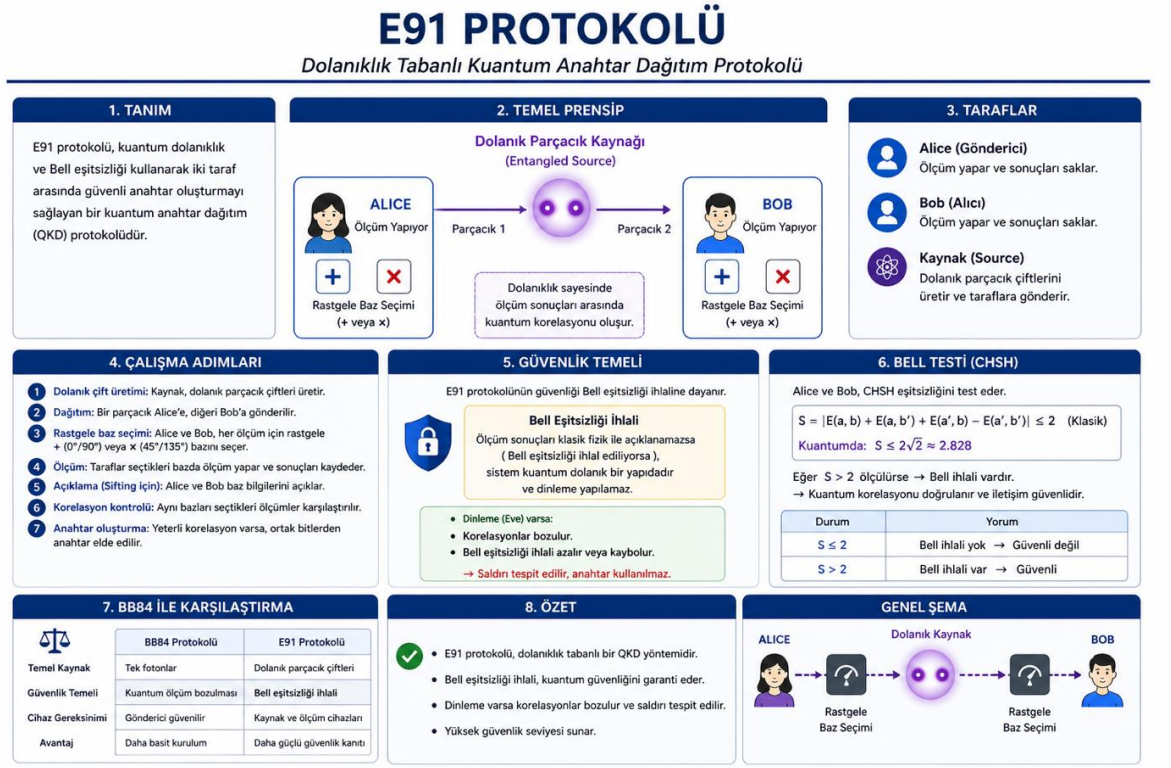
$$QBER = \frac{P\,sahte/2 + \mu Pasıl}{Prastlantı} \quad (8.29)$$

E91 protokolünün bir diğer kritik yönü, güvenli anahtar oluşturma oranıdır (key rate). Bu oran, protokolün güvenli bir şekilde ne kadar veri üretebileceğini belirler ve QBER ile doğrudan ilişkilidir. Matematiksel olarak, güvenli anahtar oluşturma oranı aşağıdaki gibi ifade edilir:

$$R = S \times (1 - 2 \times QBER) \quad (8.30)$$

Burada R güvenli anahtar oranını, S ise Bell eşitsizliğini kullanarak elde edilen verimliliği temsil eder. Bu oran, hata oranının artması durumunda güvenli anahtar oluşturmanın azalacağını gösterir. Ancak, Bell eşitsizliklerinin doğru bir şekilde test edilmesi ve hata oranlarının etkin bir şekilde yönetilmesi, E91 protokolünün güvenli bir şekilde çalışmasını sağlar.

Bu yapı Şekil 8.8'de gösterilmektedir.



Şekil 8.8. E91 Protokolü

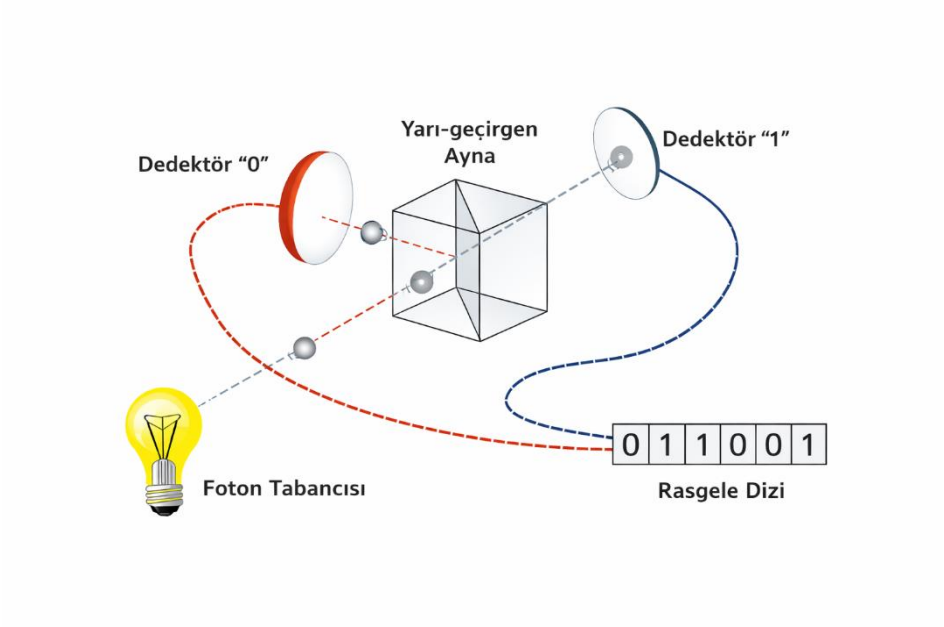
8.3 Kuantum Rastgele Sayı Üretimi

Rastgele sayı üretimi, bilgisayar bilimlerinde en çok araştırılan konulardan biri olup, özellikle kriptografik uygulamalar açısından büyük önem taşımaktadır. Klasik fizik kurallarının deterministik yapısı nedeniyle, klasik yöntemlerle rastgelelik üretimi sınırlı kalmaktadır. Bu kapsamda rastgele sayı üretimi üç temel yaklaşımla gerçekleştirilmektedir: Gerçek Rastgele Sayı Üreteçleri (GRSÜ), Sözde Rastgele Sayı Üreteçleri (SRSÜ) ve bu iki yöntemin birlikte kullanıldığı Hibrit Rastgele Sayı Üreteçleri (HRSÜ).

GRSÜ'ler donanımsal temelli olup fiziksel süreçlerden yararlanarak gerçek rastgelelik üretir. Ancak bu sistemlerin en önemli dezavantajları, düşük hızda çalışmaları ve esnekliklerinin sınırlı olmasıdır. Buna karşılık SRSÜ'ler yazılım tabanlıdır ve deterministik algoritmalar aracılığıyla sözde rastgele sayılar üretir. Bu nedenle daha hızlı ve esnek olmalarına rağmen, gerçek anlamda rastgelelik sağlamazlar. HRSÜ'ler ise her iki yöntemin avantajlarını birleştirerek hem güvenilir hem de daha verimli bir yapı sunmayı amaçlamaktadır. Bununla birlikte, bu üç yaklaşım da klasik fizik prensiplerine dayandığı için temelde deterministik sınırlamalara sahiptir (Bennett ve Brassard, 2014).

Kuantum fiziği tabanlı sistemlerde ise rastgelelik doğrudan fiziksel süreçlerin doğasından kaynaklanmaktadır. Bu nedenle geliştirilen Kuantum Rastgele Sayı Üreteçleri (KRSÜ), gerçek rastgelelik elde etmek için kuantum mekaniğinin olasılıksal yapısından yararlanır. KRSÜ'ler, klasik yöntemlere kıyasla daha yüksek güvenlik ve öngörülemezlik sunar. Bu kapsamda, ticari bir örnek olan "Quantis" cihazının çalışma prensibi Şekil 8'de gösterilmektedir.

Bu yapı Şekil 8.9'da gösterilmektedir.



Şekil 8.9. Ticari bir ürün olan Quantis'in çalışma mantığı (ID Quantique, 2015).

"Quantis" olarak bilinen bu sistemde, fotonlar yarı geçirgen bir aynadan geçirilerek rastgelelik elde edilmektedir. Fotonların bu optik elemanla etkileşimi sırasında hangi yoldan ilerleyecekleri tamamen olasılıksal olup, dış etkenlerden bağımsız şekilde gerçekleşir. Bu sayede ölçülen 0 ve 1 değerleri gerçek anlamda rastgelelik taşır. Sistem, temelde kuantum belirsizlik ilkesine dayanarak çalışmaktadır. Kuantum belirsizliği yalnızca bu yöntemle değil; parçacıkların konumu, momentumu veya elektrik alan gibi farklı fiziksel büyüklüklerin ölçümü yoluyla da rastgele sayı üretiminde kullanılabilmektedir.

Bununla birlikte, yarı geçirgen aynanın ideal olmaması (örneğin %49–%51 gibi dengesiz geçirgenlik oranları) ve foton kaynağının zaman zaman birden fazla foton üretmesi gibi nedenlerden dolayı Kuantum Rastgele Sayı Üreteçleri (KRSÜ) tamamen kusursuz sistemler olarak değerlendirilememektedir (Bennett ve Brassard, 2014). KRSÜ teknolojilerinin hâlen geliştirilme aşamasında olması ve maliyetlerinin yüksekliği göz önünde bulundurularak, bu tez çalışmasında rastgele sayı üretimi için Sözde Rastgele Sayı Üreteçleri (SRSÜ) tercih edilmiştir.

Bu yapı Şekil 8.10'da gösterilmektedir.



Şekil 8.10. Kuantum Rastgele Sayı Üretimi (QRNG)

8.4 Güvenlik Analizi ve Saldırı Tespiti

8.4.1 Anahtarın Değiştirildiğinin Tespiti

Kuantum şifreleme sistemlerinde, aynı polarizasyon bazının ve aynı ölçüm kurallarının kullanıldığı durumlarda, gönderilen ve alıcı tarafından ölçülen bitlerin farklı olması, iletişim hattında bir müdahale olduğunu gösterir. Bu durum genellikle “Man-in-the-Middle” (ortadaki adam) saldırısına işaret eder. İletişimi dinleyen bir saldırgan, gönderici tarafından iletilen fotonları yakalayıp yeniden alıcıya göndermeye çalıştığında, kuantum mekaniğinin kopyalanamazlık ilkesi nedeniyle fotonların kuantum durumunu birebir koruyamaz. Bu da alıcı tarafında farklı ölçüm sonuçlarının ortaya çıkmasına neden olur.



Şekil 8.11. Saldırganın Tespiti (Toyran, 2006).

Sistem güvenliğini test etmek amacıyla, gönderici ve alıcı protokolün son aşamasına geçmeden önce, elde edilen bit dizisinin rastgele seçilen bir alt kümesi üzerinde karşılaştırma yapar. Bu karşılaştırma sırasında hem kullanılan polarizasyon bazları hem de elde edilen bit değerleri incelenir. Eğer tarafların aynı bazda gerçekleştirdiği ölçümler sonucunda bitler arasında uyumsuzluk gözlemlenirse, bu durum iletişim hattında bir dinleme veya müdahale olduğunu gösterir. Şekil 8.11'de de görüldüğü üzere, araya giren bir saldırganın varlığı alıcı tarafında bit hatalarının artmasına neden olmaktadır (Toyran, 2006).

Şekil 8.11'de görüldüğü üzere, soldan sağa doğru incelendiğinde 6. bitte saldırı kaynaklı bir değişim meydana geldiği gözlemlenmektedir. Bu tür hatalar, iletişim hattında bir dinleyicinin (saldırganın) varlığına işaret etmektedir. Test edilen bit sayısı arttıkça, bu tür anormalliklerin tespit edilme olasılığı da önemli ölçüde yükselmektedir.

Gönderici ve alıcı tarafından seçilen NNN bitlik bir test kümesi için, saldırganın tespit edilme olasılığı $1-(3/4)4$ bağıntısı ile ifade edilmektedir. Bu ilişkinin grafiksel gösterimi ise metin içinde ifade edilmektedir (Huang, Wijejesekera, ve Sharma, 2008).

İletişim hattında bir dinleme girişimi tespit edilmesi durumunda, güvenliği sağlamak amacıyla haberleşme süreci derhal sonlandırılır. Buna karşılık, herhangi bir müdahale veya dinleme belirtisi bulunmadığında, iletişim güvenli bir şekilde sürdürülmeye devam eder.

BÖLÜME AİT SUNUM SLAYTINA ERİŞİM İÇİN QR KOD



BÖLÜM 9

Kuantum Haberleşmesi ve İnternet Siber Güvenliği

Kuantum Ağlarından Kuantum İnternete: Geleceğin Güvenli İletişim Altyapısı

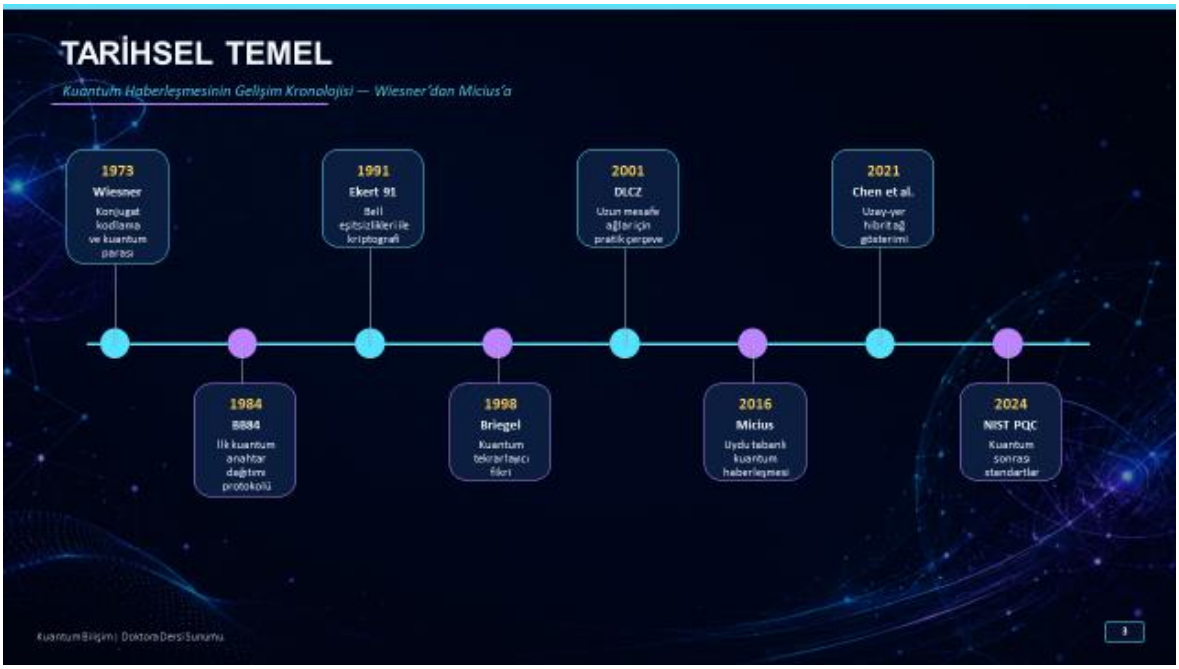
9.1 Giriş

Kuantum haberleşmesi, bilginin iletilme ve korunma biçimini kökten değiştiren bir paradigma dönüşümünü temsil etmektedir. Klasik kriptografi, güvenliğini belirli matematiksel problemlerin hesaplama açısından zorluğu üzerine inşa eder; büyük asal çarpanlara ayırma ya da ayrık logaritma problemlerinin makul sürede çözülememesi bu sistemlerin temelidir. Kuantum haberleşmesi ise güvenliğini bu tür varsayımsal hesaplama zorluklarına değil, doğrudan fiziğin temel yasalarına -ölçümün geri döndürülemezliğine ve kuantum durumlarının kopyalanamamasına- dayandırır. Bu niteliksel fark, özellikle güçlü kuantum bilgisayarların yaklaşmakta olduğu öngörülen dönemde kritik bir anlam kazanmaktadır (Nielsen ve Chuang, 2010; Wilde vd., 2017).

Bu bölüm, kuantum haberleşmesinin fiziksel temellerini, Kuantum Anahtar Dağıtımı (QKD) protokollerini ve bu protokollere yönelik bilinen saldırıları, Harvest Now Decrypt Later (HNDL) tehdit modelini, kuantum sonrası kriptografi (PQC) ile hibrit geçiş stratejilerini ve uluslararası standartlaşma süreçlerini bütüncül bir siber güvenlik perspektifinden ele almaktadır.

9.2 Tarihsel Arka Plan

Kuantum haberleşmesinin kökleri, 1973 yılında Stephen Wiesner'ın konjugat kodlama kavramını ve kuantum parası fikrini geliştirmesine dayanmaktadır. Alanın kriptografik pratiğe dönüşmesi ise Bennett ve Brassard'ın 1984'teki BB84 protokolüyle gerçekleşmiştir (Bennett ve Brassard, 1984). Ekert, 1991'de Bell eşitsizliklerine dayanan E91 protokolüyle dolanıklık temelli QKD'nin kapısını açmış; 1998'de Briegel ve arkadaşları kuantum tekrarlayıcı fikrini ortaya atmıştır (Ekert vd., 1991; Briegel vd., 1998). Uzun mesafe uygulamalar için pratik bir çerçeve 2001'de DLCZ protokolüyle sunulmuş, uydu tabanlı küresel kuantum haberleşmesi ise 2016'da Micius uydusunun fırlatılmasıyla laboratuvardan çıkıp gerçek dünyaya adım atmıştır (Liao vd., 2017; Chen vd., 2021). Bu gelişim sürecinin en güncel halkası, NIST'in 2024 yılında yayımladığı kuantum sonrası kriptografi standartlarıdır (NIST, 2024). Alanın tarihsel dönüm noktaları Şekil 9.1'de kronolojik olarak özetlenmektedir.



Şekil 9.1. Kuantum haberleşmesinin gelişim kronolojisi: Wiesner (1973), BB84 (1984), Ekert (1991), DLCZ (2001), Micius (2016), NIST PQC (2024).

9.3 Kuantum Haberleşmesinin Fiziksel Temelleri

9.3.1 Qubit ve Süperpozisyon

Kuantum bilgisinin temel birimi olan qubit, saf durumunu $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ biçiminde ifade eder; burada $\alpha, \beta \in \mathbb{C}$ ve $|\alpha|^2 + |\beta|^2 = 1$ koşulu sağlanır. Klasik bitin deterministik ikili yapısının aksine, qubit ölçülene kadar her iki temel durumu belirli genliklerle aynı anda barındırabilir. Ölçüm gerçekleştiğinde süperpozisyon çöker ve yalnızca bir sonuç elde edilir; faz bilgisi dolaylı olarak yok olur. Yoğunluk matrisi $\rho = |\psi\rangle\langle\psi|$ formalizmi, karışık durumları ve çevre kaynaklı gürültüyü matematiksel olarak modellemek için kullanılır (Nielsen ve Chuang, 2010; Wilde vd., 2017).

9.3.2 Kuantum Dolanıklığı

İki qubit arasındaki dolanıklık, alt sistemlerin durumlarının birbirinden bağımsız yazılamadığı bir korelasyon biçimidir. En yaygın örnek Bell durumudur: $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Bu durumda Alice hangi bitini ölçürse ölçsün, Bob'un bitinin durumu anında belirlenmekte; ancak bu bağıntı kullanılarak klasik bilgi anında iletilemez - no-signaling ilkesi bunu yasaklar. Bell eşitsizliklerinin deneysel ihlali, yerel gizli değişken teorilerini dışlamış ve E91 protokolünün güvenlik temelini güçlendirmiştir (Nielsen ve Chuang, 2010; Ekert vd., 1991). Alice-Bob dolanıklık kurulumu ve no-signaling ilkesi Şekil 9.2'de şematik olarak gösterilmektedir.



Şekil 9.2. Kuantum dolanıklığı ve no-signaling: Alice ve Bob arasında paylaşılan $|\Phi^+\rangle$ Bell durumu ile sinyal iletiminin olanaksızlığı.

9.3.3 No-Cloning Teoremi: Güvenliğin Fiziksel Temeli

Wootters ve Zurek'in 1982'de ispatlayan no-cloning teoremi, bilinmeyen bir kuantum durumunun mükemmel kopyasının üretilemeyeceğini ortaya koyar (Wootters ve Zurek, 1982). Kanıt, kuantum mekaniğinin doğrusal (lineer) yapısından doğrudan çıkar: Bilinmeyen $|\psi\rangle$ durumunu kopyalayan hiçbir üniter operatör U yoktur. Bu teorem, kuantum haberleşme güvenliğinin fiziksel temelidir. Dinleyici (Eve), kanaldan geçen qubiti gizlice kopyalayamaz; girişimi kaçınılmaz biçimde Kuantum Bit Hata Oranını (QBER) yükseltir ve tespit edilir. Klasik ağlarda sinyali amplifikatörle güçlendirmek mümkünken, kuantum kanalında bu işlem mümkün değildir; bu kısıt, kuantum tekrarlayıcı teknolojisinin geliştirilmesini zorunlu kılmıştır (Bennett ve Brassard, 1984; Briegel vd., 1998). Şekil 9.3, klasik ve kuantum kanal arasındaki bu temel farkı ve Eve'in müdahalesinin QBER üzerindeki yansımasını görsel olarak karşılaştırmaktadır.



Şekil 9.3. No-cloning teoremi ve dinleme tespiti: Klasik kanalda kopyalama mümkünken kuantum kanalda Eve'in müdahalesi kaçınılmaz olarak QBER'e yansır.

9.4 Kuantum Kanalları, Gürültü ve İletim Kapasitesi

Gerçek bir kuantum iletişim kanalında qubit durumu gürültüsüz taşınmaz. Kuantum kanalı matematiksel olarak Tamamen Pozitif İz Koruyan (CPTP) dönüşümler ve Kraus operatör toplamı $\varepsilon(\rho) = \Sigma_i K_i \rho K_i^\dagger$ ile temsil edilir. Temel gürültü mekanizmaları; bit çevirme, faz çevirme, depolarize ve genlik söndürme kanallarıdır. Bu kanalların Kraus operatörleri ve pratik etkileri Tablo 9.1'de ayrıntılı olarak verilmektedir. 200 km optik fiberde iletim verimi $\eta \approx 10^{-4}$ düzeyine düşmekte; Pirandola ve arkadaşlarının (PLOB) teoremi $Q(\eta) \leq -\log_2(1-\eta)$ bağıntısıyla tekrarlayıcısız sistemlerin kapasite üst sınırını kesin olarak belirlemektedir (Pirandola vd., 2017).

Tablo 9.1. Temel kuantum gürültü kanalları, Kraus operatörleri ve pratik etkileri.

Kanal	Fiziksel Mekanizma	Etki
Bit çevirme ($K_0=\sqrt{(1-p)}I$, $K_1=\sqrt{p}X$)	Polarizasyon bozunumu	QBER ≈ p
Faz çevirme ($K_0=\sqrt{(1-p)}I$, $K_1=\sqrt{p}Z$)	Atmosferik türbülans	Faz kaybı
Depolarize ($K_i = \{I,X,Y,Z\}$)	Genel gürültü	QBER = p/2
Genlik söndürme (kayıp modeli γ)	Foton soğrulması / fiber kaybı	$\eta = 1, \gamma$

9.5 Kuantum Tekrarlayıcılar ve Ağ Mimarileri

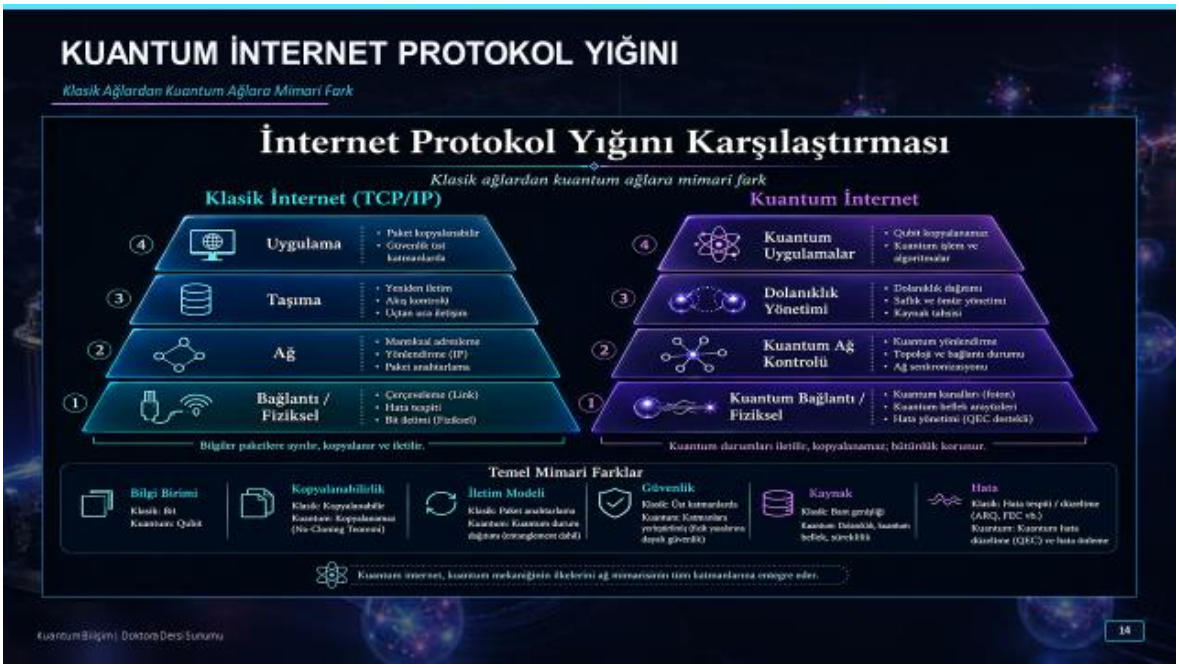
Optik fiberde klasik amplifikasyon no-cloning nedeniyle kullanılamadığından, uzun mesafe kuantum iletişimi kuantum tekrarlayıcılara dayanmaktadır. İdeal bir tekrarlayıcı düğümü; dolanık foton çiftleri üretir, komşu düğümlerle Bell Durum Ölçümü (BSM) yaparak dolanıklığı yayar ve dolanıklık arıtma ile kaliteyi iyileştirir. Tekrarlayıcı mimarileri tarihsel olarak üç kuşakta değerlendirilmektedir: Birinci kuşak dolanıklık arıtma ve klasik iletişime; ikinci kuşak kuantum hata düzeltme entegrasyonuna; üçüncü kuşak ise hata toleranslı mantıksal qubitler üzerine kuruludur (Briegel vd., 1998; Duan vd., 2001; Muralidharan

vd., 2016; Azuma vd., 2023). Şekil 9.4, ideal bir tekrarlayıcı düğümünün çalışma akışını adım adım göstermektedir.



Şekil 9.4. Kuantum tekrarlayıcı çalışma akışı: Dolanıklık üretimi, BSM ve dolanıklık uzatma adımları.

Kuantum İnternet protokol yığını, klasik TCP/IP'den köklü biçimde farklılaşır. Fiziksel katmanda foton iletimi, bağlantı katmanında dolanıklık damıtma, ağ katmanında dolanıklık yönlendirme ve oturum katmanında QKD/teleportasyon protokolleri yer almaktadır. Bu mimarinin standartlaşması ITU-T, ETSI ve IEEE bünyesindeki çalışma gruplarının gündeminin üst sıralarında yer almaya devam etmektedir (Wehner vd., 2018). Klasik ve kuantum ağların katman mimarileri arasındaki temel farklar Şekil 9.5'te karşılaştırmalı olarak sunulmaktadır.



Şekil 9.5. Klasik Internet TCP/IP yığını ile Kuantum İnternet protokol yığınının katman bazında karşılaştırması.

9.6 Küresel Projeler, Uydu Tabanlı Haberleşme ve Türkiye

9.6.1 Küresel Konumlanma

2025 itibarıyla kuantum haberleşmesi alanında küresel bir rekabet sürmektedir. Çin, Micius uydusu ve Beijing-Şanghay omurga fiber QKD hattı (>2.000 km) ile en ileri altyapıyı işletmektedir (Liao vd., 2017; Chen vd., 2021). Avrupa Birliği, Quantum Flagship çerçevesinde EuroQCI ile üye devletleri birbirine bağlayacak kuantum güvenli altyapıyı stratejik hedef olarak benimsemiştir. ABD, NIST PQC standartları ve Ulusal Kuantum İnisiyatifi ile hem yazılım hem donanım katmanında kapasitesini hızla geliştirmektedir (NIST, 2024; CISA, NSA ve NIST, 2023).

9.6.2 Uydu Tabanlı QKD ve Micius

Optik fiber ortamının aksine serbest uzay kanalında atmosferik kayıplar mesafeyle üstel artmaz. LEO (~600 km rakım) uydu-yer istasyonu bağlantısında etkili kanal kaybı, 200 km fiber mesafesiyle rekabet edebilir düzeydedir; bu durum Şekil 9.6'daki kanal karşılaştırma diyagramında açıkça görülmektedir. Micius (墨子) uydusu 2016-2021 arasında beş tarihi deneyi başarıyla tamamlamıştır (Tablo 9.2):

Tablo 9.2. Micius uydusunun beş temel kuantum haberleşme deneyi (2016–2021).

Yıl	Deney	Mesafe	Temel Sonuç	Kaynak
2017	Uydudan-yere QKD	9.200 km	Fiber'e kıyasla milyar kat düşük kayıp	(Liao vd., 2017)
2017	Dolanıklık dağıtımı	9.200 km	Bell eşitsizliği ihlali doğrulandı	(Yin vd., 2017)
2017	Yer-uydu kuantum teleportasyon	~1.400 km	Rekor mesafede teleportasyon	(Ren vd., 2017)
2020	Daylight QKD	9.120 km	Gündüz koşullarında QKD ilk gösterim	(Liao vd., 2017)
2021	Uzay-Yer hibrit ağ	9.600 km	Kıtalar arası bütünleşik kuantum ağı	(Chen vd., 2021)



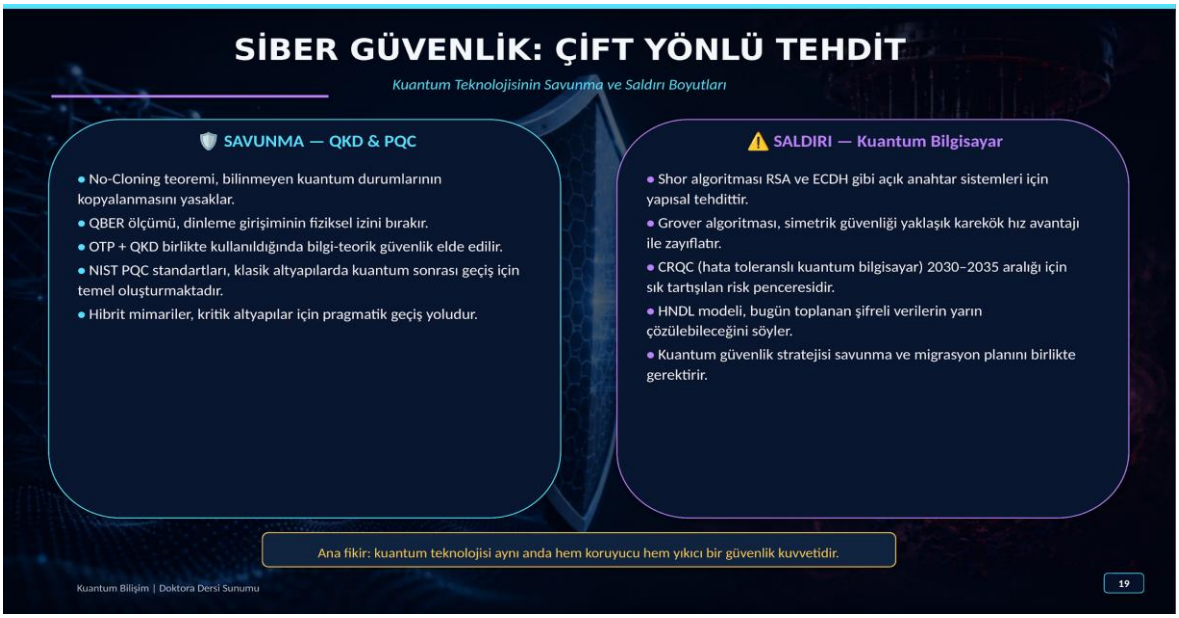
Şekil 9.6. Uydu tabanlı kuantum haberleşme kanal modeli: Fiber QKD ile LEO uydu QKD kanal kayıpları karşılaştırması.

9.6.3 Türkiye'nin Stratejik Konumu

Coğrafi konumu itibarıyla Avrupa ile Asya arasında köprü işlevi üstlenebilecek olan Türkiye, kuantum haberleşmesi alanında kurumsal bir altyapı oluşturma sürecindedir. TÜBİTAK BİLGEM, QKD ürün ve protokol geliştirme Ar-Ge'si sürdürmekte; Ankara-İstanbul güzergâhında pilot QKD hattı çalışmaları yürütülmekte ve QRNG bileşenlerinde yerli üretim kapasitesi geliştirilmektedir. NATO çerçevesinde kuantum güvenli iletişim standartlarına uyum süreci de aktif biçimde izlenmektedir. 2023-2030 Ulusal Kuantum Teknolojileri Strateji ve Eylem Planı, kıtalar arası kuantum ağlara entegrasyonu 2030 hedefi olarak belirlemiştir (TÜBİTAK BİLGEM, 2023).

9.7 Siber Güvenlik: Kuantum Teknolojisinin Çift Yönlü Etkisi

Kuantum teknolojisi, siber güvenlik açısından aynı anda hem koruyucu hem yıkıcı bir güç olarak işlev görmektedir. Bu çift yönlü etki, güvenlik mimarilerinin ve politikalarının yeniden tasarlanmasını kaçınılmaz kılmaktadır; her iki boyut Şekil 9.7'de yan yana özetlenmektedir.



Şekil 9.7. Kuantum teknolojisinin siber güvenliğe çift yönlü etkisi: Savunma (QKD, PQC) ve Saldırı (Shor, Grover) boyutları.

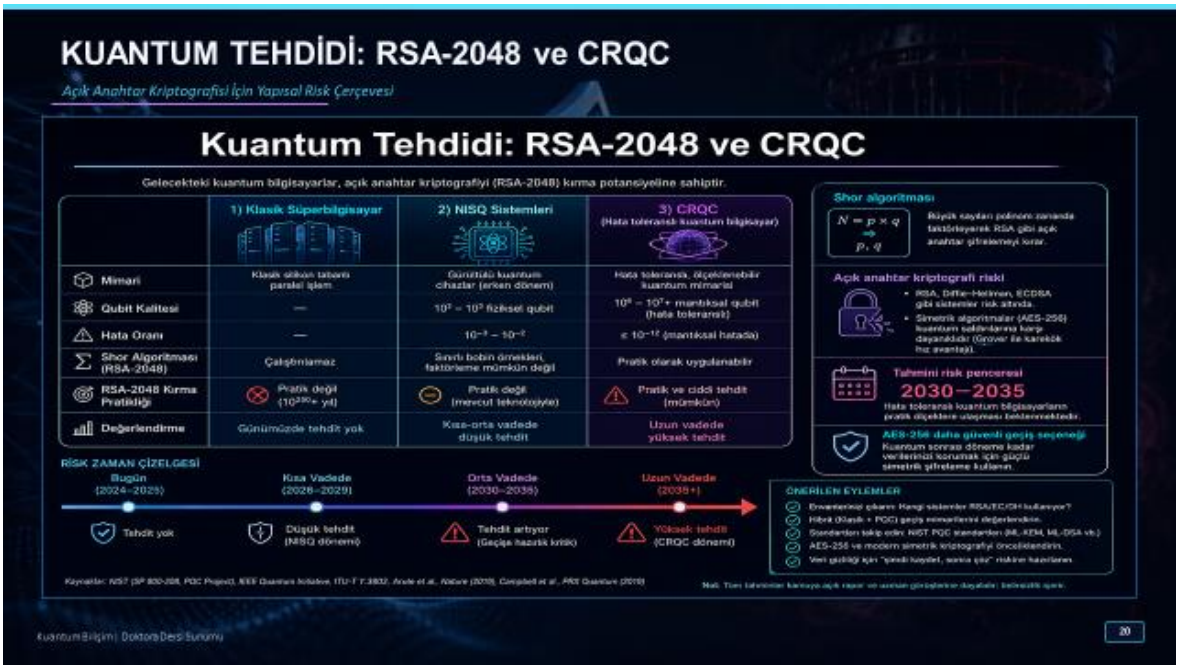
9.7.1 Savunma Boyutu: QKD ve PQC

No-cloning teoremi gereği dinleyici, kanaldan geçen qubiti kopyalayamaz; girişimi kaçınılmaz olarak QBER'i yükseltir ve tespit edilir. Tek kullanımlık şifreleme pedi (OTP) ile QKD birleştirildiğinde, güvenlik herhangi bir hesaplama varsayımına değil fiziğin temel yasalarına dayanır ve bilgi-teorik anlamda mükemmel güvenlik elde edilir (Bennett ve Brassard, 1984; Ekert vd., 1991). NIST'in 2024'te yayımladığı FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) ve FIPS 205 (SLH-DSA) standartları ise klasik ağ altyapılarında kuantum sonrası geçişin referans çerçevesini oluşturmaktadır (NIST, 2024; CISA, NSA ve NIST, 2023).

9.7.2 Saldırı Boyutu: Shor Algoritması ve Grover'ın Etkisi

Shor'un 1994 tarihli algoritması, RSA ve Eliptik Eğri Diffie-Hellman (ECDH) gibi açık anahtar sistemleri için yapısal bir tehdit oluşturmaktadır. Kriptografik Açıdan İlgili Kuantum Bilgisayar (CRQC), binlerce hata toleranslı mantıksal qubit ile donatıldığında RSA-2048'i polinom zamanda kırabilecektir. RSA-2048'in kırılması için gereken kaynaklar; hata oranı, hata düzeltme kodunun verimliliği ve mantıksal qubit sayısına bağlıdır. Mevcut tahminler yüz binlerden milyonlara uzanan fiziksel qubit gerektirdiğine işaret etmektedir (Mosca, 2018). Bu kaynak gereksinimleri ve risk çerçevesi Şekil 9.8'de görsel olarak aktarılmaktadır.

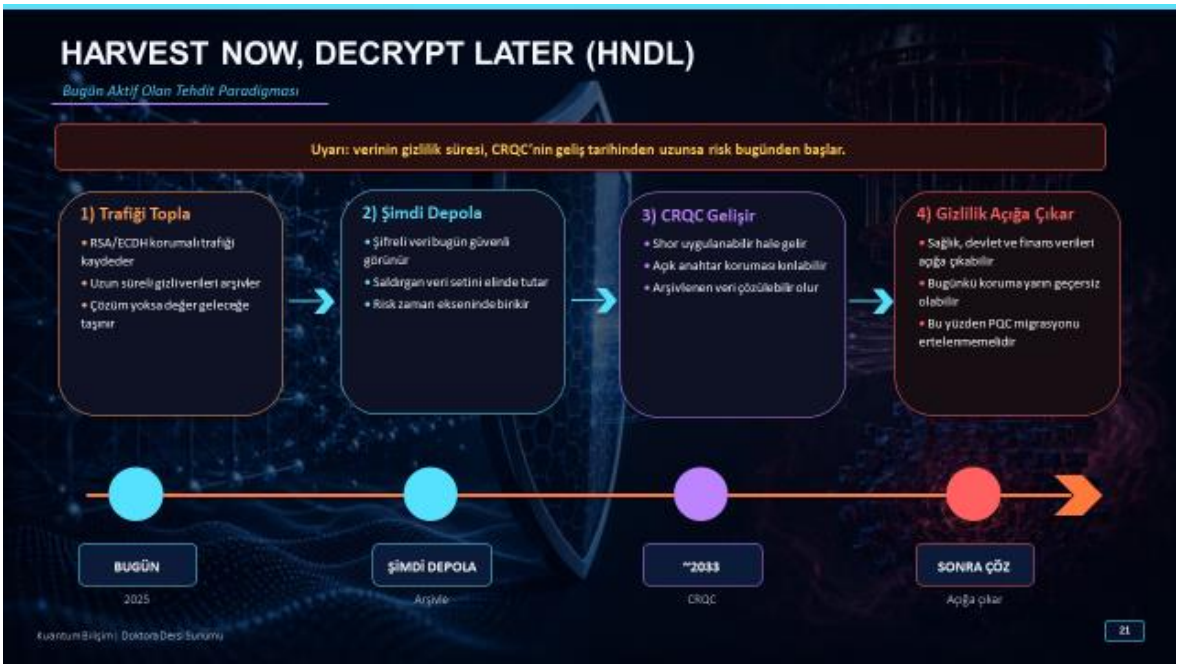
Grover'ın arama algoritması ise simetrik şifreleme sistemlerini karekök hızında etkisiz kılarak AES-128'in etkin güvenliğini 64 bite indirger. Bu nedenle simetrik anahtar uzunluklarının ikiye katlanması - AES-128'den AES-256'ya geçiş- kuantum döneminde standart öneri hâline gelmiştir. Öte yandan simetrik sistemler, Grover etkisini bu şekilde giderilebileceğinden asimetrik sistemler kadar acil bir risk altında değildir (Mosca, 2018).



Şekil 9.8. Kuantum tehdidi: RSA-2048 ve CRQC için gerekli kaynak tahminleri ve risk çerçevesi.

9.8 Harvest Now, Decrypt Later: Bugünün Tehdit Modeli

HNDL (Harvest Now, Decrypt Later - Şimdi Topla, Sonra Çöz) modeli, güncel güvenlik gündeminin en kritik konularından biridir. Bu modelde gelişmiş tehdit aktörleri, bugünkü RSA/ECDH korumalı şifreli trafiği sistemli biçimde kayıt altına almakta ve CRQC erişilebilir olduğunda arşivlediği veriyi çözmeyi planlamaktadır. Modelin temel uyarısı şudur: Bir verinin gizlilik ömrü, CRQC'nin geliş tarihini aşıyorsa risk bugünden başlar (Mosca, 2018; CISA, NSA ve NIST, 2023). Bu dörtlü süreç Şekil 9.9'daki zaman çizelgesinde adım adım gösterilmektedir.



Şekil 9.9. HNDL tehdit modeli zaman çizelgesi: Veri toplama (2025), depolama, CRQC olgunlaşması (~2033) ve şifre çözme aşamaları.

Bu modelin pratik çıkarımları son derece somuttur. Sağlık kayıtları, diplomatik yazışmalar, askeri planlama belgeleri ve finansal veriler gibi 10-30 yıllık gizlilik ömrü beklenen verilerin bugün RSA ile şifrelenmesi gelecekte kabul edilemez bir risk üretmektedir. Mosca'nın 2018 tarihli analizi, PQC'ye geçiş süresinin CRQC bekleme süresinden uzun olması hâlinde bu riskin katlanarak büyüdüğünü kesin biçimde ortaya koymuştur (Mosca, 2018). Dolayısıyla PQC migrasyonu; kritik altyapılar için bir tercih değil, ertelenemeyen bir zorunluluktur.

9.9 BB84 Protokolü ve QKD Güvenlik Analizi

9.9.1 BB84'ün Adım Adım İşleyişi

Bennett ve Brassard'ın 1984'te önerdiği BB84, kuantum anahtar dağıtımının temel referans protokolüdür (Bennett ve Brassard, 1984). Temel fikir, Alice'in rastgele seçilmiş iki baz (Z: {|0⟩, |1⟩} ve X: {|+⟩, |−⟩}) üzerinde bit bilgisini kodlaması ve Bob'un rastgele baz seçerek ölçüm yapmasıdır. Protokol altı aşamada ilerler:

(1) Hazırlık: Alice iki baz (Z ve X) üzerinde rastgele bit dizisi seçer.

(2) Kodlama: Bitleri |0⟩, |1⟩, |+⟩, |−⟩ durumlarına kodlayarak kuantum kanaldan gönderir.

(3) Ölçüm: Bob her foton için rastgele baz seçip ölçüm yapar.

(4) Baz Uzlaşması: Açık klasik kanalda yalnızca kullanılan bazlar karşılaştırılır; bit değerleri kesinlikle paylaşılmaz.

(5) QBER Testi: Uyumlu örneklerin bir alt kümesinde hata oranı hesaplanır; belirlenen eşiği aşarsa oturum iptal edilir.

(6) Anahtar Üretimi: Hata düzeltme (error correction) ve gizlilik güçlendirme (privacy amplification) ile nihai gizli anahtar üretilir. Protokolün bu altı aşamasının akış diyagramı Şekil 9.10’da sunulmaktadır.



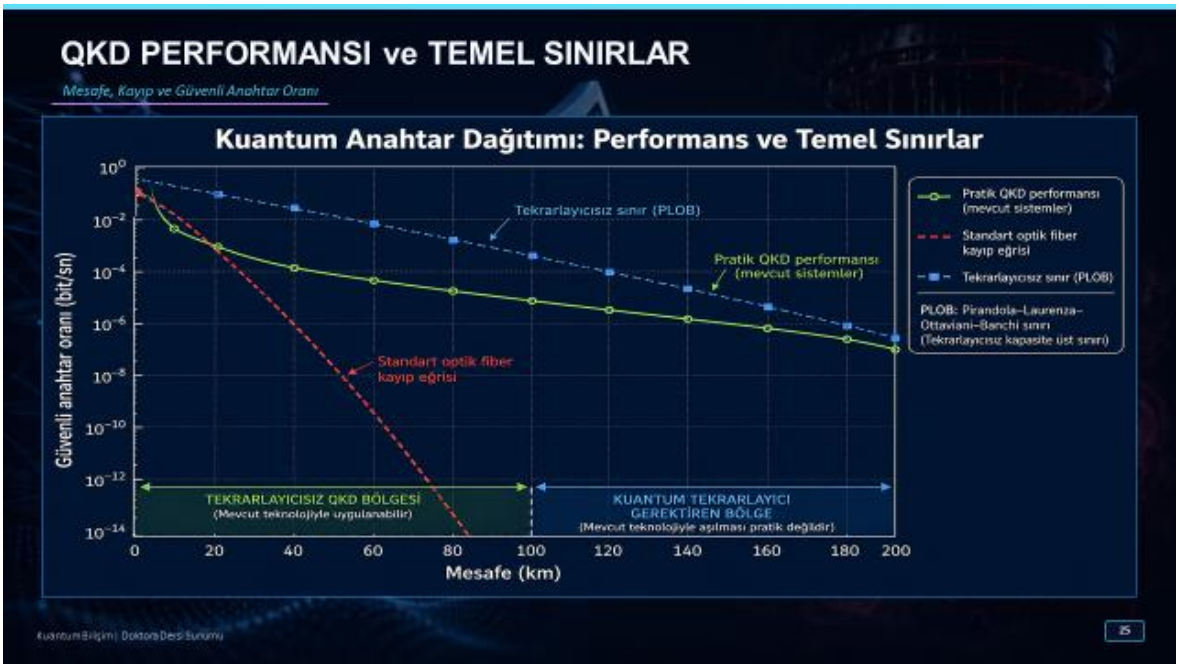
Şekil 9.10. BB84 protokolünün altı aşamalı akış diyagramı: Hazırlık, kodlama, ölçüm, baz uzlaşması, QBER testi ve anahtar üretimi.

9.9.2 Güvenlik Kanıtı ve QBER Eşiği

BB84'ün güvenliği; ölçümün durumu bozması ve baz uyuşmazlığının dinlemeyi istatistiksel olarak görünür kılması ilkelerine dayanır. Eve doğru bazı ancak 1/2 olasılıkla tahmin edebilir; yanlış baz seçiminde QBER'e %25 oranında katkı sağlar. Pratik sistemlerde yaklaşık %11 QBER eşiği asimptotik güvenlik analizlerinde tipik sınır olarak kabul edilmekte; bu değerin üstünde oturum sonlandırılmaktadır. Error correction ve privacy amplification aşamaları, sızıntı bilgiyi hesaplamalı olarak sıfıra indirgeyen post-processing adımlarıdır (Bennett ve Brassard, 1984; Xu vd., 2020).

9.9.3 QKD Performansı ve Temel Sınırlar

QKD sistemlerinin pratik performansı; fiber uzunluğu, foton kaynağı verimi, tek foton dedektörü etkinliği ve karanlık sayım oranına bağlıdır. Günümüz deneysel çalışmalarında 400-500 km optik fiber üzerinde güvenli anahtar üretimi gösterilmiş olmakla birlikte bu mesafelerde anahtar üretim hızı saniyede birkaç bite düşmektedir. PLOB sınırı, tekrarlayıcısız sistemlerin mesafe-kapasite eğrisini kesin olarak belirleyen teorik bir çerçeve sunarken alan ölçümlü ölçüm aygıtı bağımsız QKD (MDI-QKD) ve Twin-Field QKD gibi yeni protokoller bu sınıra yaklaşmayı hedeflemektedir (Pirandola vd., 2017; Lo vd., 2012; Xu vd., 2020). Mesafeye karşı güvenli anahtar üretim hızı ve farklı protokol performansları Şekil 9.11'de karşılaştırmalı olarak gösterilmektedir.



Şekil 9.11. Kuantum anahtar dağıtımı performansı: Mesafeye karşı güvenli anahtar üretim hızı, PLOB sınırı ve farklı protokol karşılaştırması.

Teorik güvence ile pratik sistem gerçekliği arasındaki uçurum, QKD güvenlik analizinin merkezindedir. Teorik kanıtlar gürültüsüz ve kusursuz cihazlar varsayarken gerçek sistemler; detekötr verimsizliği, kaynak kusurları ve arayüz açıkları gibi etkenlerle sınırlanmaktadır. Bu uçurumu kapatmak için Aygıt Bağımsız QKD (DI-QKD) ve ETSI'nin Uygulama Güvenliği Koruma Profili (ETSI, 2023) geliştirilmiştir. Teorik güvence ile pratik sistem gerçekliği arasındaki bu mesafe Şekil 9.12'de görsel olarak ele alınmaktadır.



Şekil 9.12. Kuantum haberleşme güvenliği: Teorik güvence ile pratik sistem gerçekliği arasındaki uçurum ve bu boşluğu kapatan yaklaşımlar.

9.10 QKD'ye Yönelik Saldırılar ve Katmanlı Tehdit Modeli

9.10.1 Foton Sayısı Bölme (PNS) Saldırısı

Zayıf Koherant Atım (WCP) tabanlı QKD sistemleri her atımda zaman zaman birden fazla foton yayar. Saldırgan Eve, fazladan fotonları saklayarak baz uzlaşması açıklandıktan sonra doğru bazda ölçüm yapabilir ve bu yolla QBER'i yükseltmeden -yani herhangi bir iz bırakmadan- gizli anahtar hakkında bilgi edinebilir. Tuzak durum (decoy state) yöntemi bu saldırıya karşı geliştirilmiş başlıca karşı önlemdir: Farklı ortalama foton sayısına sahip ek atımlar gönderilerek Eve'in kanalı manipüle ettiği istatistiksel olarak tespit edilir (Bennett ve Brassard, 1984; Xu vd., 2020). PNS saldırısının adım adım işleyişi Şekil 9.13'te şematik olarak gösterilmektedir.



Şekil 9.13. Foton Sayısı Bölme (PNS) saldırısı: WCP tabanlı sistemlerde Eve'in çok fotonlu atımlardan QBER=0 ile bilgi edinmesi.

9.10.2 Kör Gözlem (Blinding) Saldırısı

Lydersen ve arkadaşlarının 2010'da gösterdiği kör gözlem saldırısı, QKD donanım güvenliği tarihinin dönüm noktalarından biridir (Lydersen vd., 2010). Bu saldırıda Eve, Bob'un tek foton dedektörünü yoğun bir kontrol lazeriyle aydınlatarak dedektörü lineer çalışma moduna zorlar. Lineer modda dedektör, bir enerji eşikleme birimine dönüşür ve Eve tüm bit bilgisine hiçbir QBER izi bırakmadan doğrudan erişebilir. Ticari QKD sistemlerinin donanım katmanındaki bu kritik açık; Aygıt Bağımsız QKD (DI-QKD), Ölçüm Aygıtı Bağımsız QKD (MDI-QKD) ve optik güç izleme gibi karşı önlemlerin geliştirilmesine güçlü motivasyon sağlamıştır (Lo vd., 2012; Nadlinger vd., 2022). Saldırının üç aşamalı işleyişi ve QBER=0 sonucu Şekil 9.14'te adım adım aktarılmaktadır.



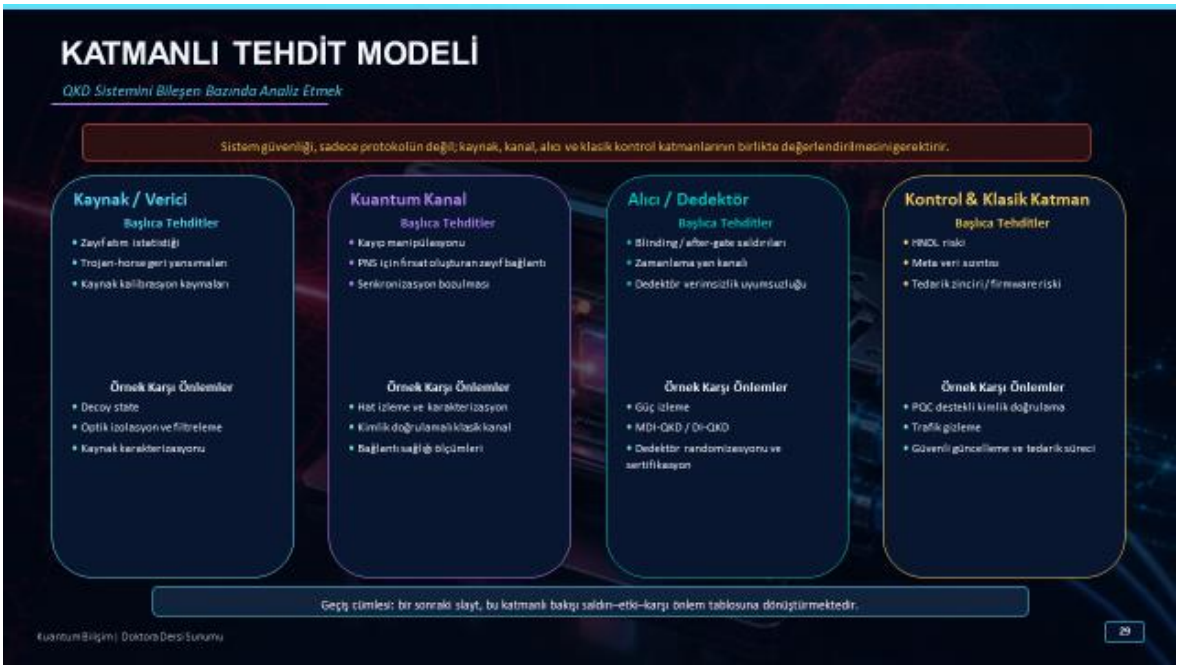
Şekil 9.14. Kör gözlem saldırısı (Makarov, 2010): Dedektörün lineer moda zorlanması, QBER=0 ile tam anahtar elde edilmesi.

9.10.3 Trojan-Horse ve Zamanlama Yan Kanal Saldırıları

Trojan-Horse saldırısı, verici cihazın optik giriş portuna parlak lazer atımları göndererek iç durum bilgisini (baz seçimi, modülatör durumu) geri yansıma ile çıkarmayı hedefler. Optik izolasyon ve WDM filtreler başlıca karşı önlemlerdir (Jain vd., 2014). Zamanlama yan kanal saldırısı ise dedektör gecikmelerindeki küçük farklılıklardan -bu farklar baz ve bit değerine bağlı olabilir- bit bilgisi çıkarmayı amaçlar; rastgele gecikme eklemeleri ve kalibrasyon bu riski azaltır (Qi vd., 2007; Nasedkin vd., 2023).

9.10.4 Katmanlı Tehdit Modeli

QKD güvenliğini yalnızca protokol güvenliğiyle özdeşleştirmek yanıltıcı olur. Gerçek sistemler dört ana katman üzerinden değerlendirilmelidir: Kaynak/verici, kuantum kanal, alıcı/dedektör ve klasik kontrol katmanı. Her katmanın kendine özgü tehdit vektörleri ve karşı önlemleri bulunmaktadır; bu bütünsel yapı Şekil 9.15'te görselleştirilmiş, tüm saldırı vektörlerinin etki ve karşı önlemleri ise Tablo 9.3'te derlenmiştir.



Şekil 9.15. QKD sistemlerinin katmanlı tehdit modeli: Her katmanda başlıca tehditler ve örnek karşı önlemler.

Tablo 9.3. Kapsamlı QKD tehdit matrisi: Saldırı vektörü, etki, karşı önlem ve tespit güçlüğü.

Saldırı Vektörü	Temel Etki	Karşı Önlem	Tespit
PNS saldırısı	Çok fotonlu atımlardan bilgi sızması	Decoy state yöntemi	Orta
Kör gözlem (Blinding)	Dedektörün lineer moda zorlanması	DI-QKD; optik güç izleme	Yüksek
Trojan-Horse	Cihaz içi durum bilgisi sızıntısı	İzolasyon filtresi; WDM; güç sınırı	Orta
Zamanlama yan kanalı	Dedektör gecikmelerinden bit sızıntısı	Rastgele gecikme; kalibrasyon	Orta
DoS / lazer enjeksiyonu	Hizmet reddi; cihaz bozulması	Giriş filtresi; güç koruması	Düşük
Tedarik zinciri arka kapısı	Gizli donanım/firmware manipülasyonu	Sertifikasyon; güvenli tedarik	Yüksek
Meta veri analizi	Trafik deseni yan bilgisi	Padding ve trafik karıştırma	Orta

9.11 QKD, PQC ve Hibrit Yaklaşımlar: Karşılaştırmalı Değerlendirme

Kuantum tehdidine karşı kritik altyapıları korumak için üç temel yaklaşım mevcuttur. Bu yaklaşımların farklı güvenlik temelleri, güçlü yanları ve kısıtları vardır; dolayısıyla kullanım senaryosuna göre doğru seçim ya da kombinasyonun belirlenmesi stratejik bir karar gerektirir. Bu üç yolun ayrıntılı karşılaştırması Tablo 9.4'te sunulmaktadır.

Tablo 9.4. QKD, PQC ve hibrit yaklaşımların karşılaştırmalı analizi.

Yaklaşım	Güvenlik Temeli	Güçlü Yanlar	Sınırlılıklar	Uygun Kullanım
QKD	Fizik yasaları (no-cloning, ölçüm bozulması)	Bilgi kuramsal güvenlik; dinleme iz bırakır	Yüksek donanım maliyeti; mesafe kısıtı; ağ entegrasyonu zor	Metro ağlar; kritik omurga; devlet/savunma

Yaklaşım	Güvenlik Temeli	Güçlü Yanlar	Sınırlılıklar	Uygun Kullanım
PQC	Kuantum dayanımlı matematiksel problemler	Mevcut altyapıya uyumlu; yazılım güncellemesiyle uygulanabilir	Güvenlik varsayımsal; yeni algoritma riskleri; anahtar boyutları artabilir	Genel İnternet; kurumsal VPN/TLS; hızlı migrasyon
Hibrit	PQC + QKD katmanlı savunma	Pratik ve gerçekçi denge; aşamalı geçiş	Mimari karmaşıklık; yönetim ve maliyet planı gerekir	Ulusal ağ omurgaları; kritik altyapılar; uzun dönem

Akademik ve teknik çevrelerdeki uzlaşı şu yöndedir: Kısa vadede PQC migrasyonu acilen zorunludur; seçili, yüksek güvenlik değerli uygulamalarda QKD tamamlayıcı işlev üstlenmektedir. Gerçekçi orta-uzun vade stratejisi ise hibrit mimaridir. CISA-NSA-NIST'in 2023 tarihli ortak rehberi, kritik altyapı operatörleri için bu hibrit yaklaşımı açıkça tavsiye etmektedir (CISA, NSA ve NIST, 2023).

9.11.1 PQC Geçişinde Siber Güvenlik Riskleri

PQC geçişi süreci kendi içinde de kritik siber güvenlik riskleri barındırmaktadır. Kriptografik çeşitlilik kaybı, en önemli risklerden biridir: Tüm sistemlerin aynı anda aynı PQC algoritmasına geçmesi, tek bir algoritmanın kırılması halinde geniş çaplı sistemik bir çöküşe zemin hazırlayabilir. Bunun yanı sıra hibrit TLS/protokol uygulamalarındaki geçiş kodu katmanları, standart güvenlik analizlerinde bulunmayan yan kanal açıklarına kapı aralayabilmektedir. Tedarik zinciri riski de bu süreçte kritik bir kaygıdır: Kütüphane ve ara katman yazılımlarının güncellenmesi sürecinde arka kapı ya da hatalı uygulama riski artış göstermektedir. Son olarak, PQC algoritmalarının anahtar ve imza boyutlarının klasik algoritmalara kıyasla önemli ölçüde büyümesi; ağı tıkayan ek bant genişliği yüküne ve eski donanım/protokollerle uyumsuzluklara yol açabilmektedir (NIST, 2024; CISA, NSA ve NIST, 2023). Bu nedenle PQC migrasyonu, sadece bir algoritma değişikliği olarak değil; baştan sona bir sistem güvenliği değerlendirmesi gerektiren kapsamlı bir mimari dönüşüm olarak ele alınmalıdır.

9.12 Standartlaşma, Politika ve Jeopolitik Boyut

Kuantum haberleşmesi ve PQC standartlaşması, birden fazla uluslararası kuruluşun eş zamanlı ve birbiriyle koordinasyon içindeki çalışmalarıyla ilerlemektedir. Bu kuruluşların güncel standart çıktıları Tablo 9.5'te özetlenmektedir.

Tablo 9.5. Kuantum haberleşmesi ve PQC alanındaki başlıca uluslararası standartlar.

Kuruluş	Standartlar / Çıktılar	Kapsam
ITU-T SG17	Y.3800 serisi; QKD güvenlik mimarisi	Telekom çerçevesi; arayüz ve birlikte işlerlik
ETSI ISG QKD	GS QKD 011 / 014 / 016	Uygulamaya dönük spesifikasyonlar; uygulama güvenliği (ETSI, 2023)
NIST PQC	FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA)	Kuantum sonrası geçiş standardı; 2030'a kadar migrasyon (NIST, 2024)
IEEE P1913	Kuantum ağ protokolleri	Ağ katmanı yönetimi; teknik koordinasyon
NSA CNSA 2.0	RSA/ECDH'den çıkış planı ve migrasyon takvimi	ABD ulusal güvenlik sistemleri



Şekil 9.16. Kuantum haberleşmesi ve PQC standartlaşma ekosistemi: ITU-T, ETSI, NIST, IEEE ve NSA'nın rolleri ile jeopolitik boyut.

Standartlaşma süreci yalnızca teknik bir koordinasyon meselesi değildir; ABD-Çin teknolojik rekabeti, AB'nin stratejik özerklik hedefi ve ihracat kontrolleri standartların biçimlenmesini doğrudan etkilemektedir. Bu bağlamda standartlaşma, güven, teknolojik egemenlik ve ittifak ilişkilerinin somut bir yansımasıdır. Standartlaşma ekosisteminin kurumsal yapısı ve jeopolitik boyutu Şekil 9.16'da görsel olarak özetlenmektedir.

9.13 Açık Araştırma Problemleri ve Kuantum İnternet Yol Haritası

9.13.1 Açık Araştırma Problemleri

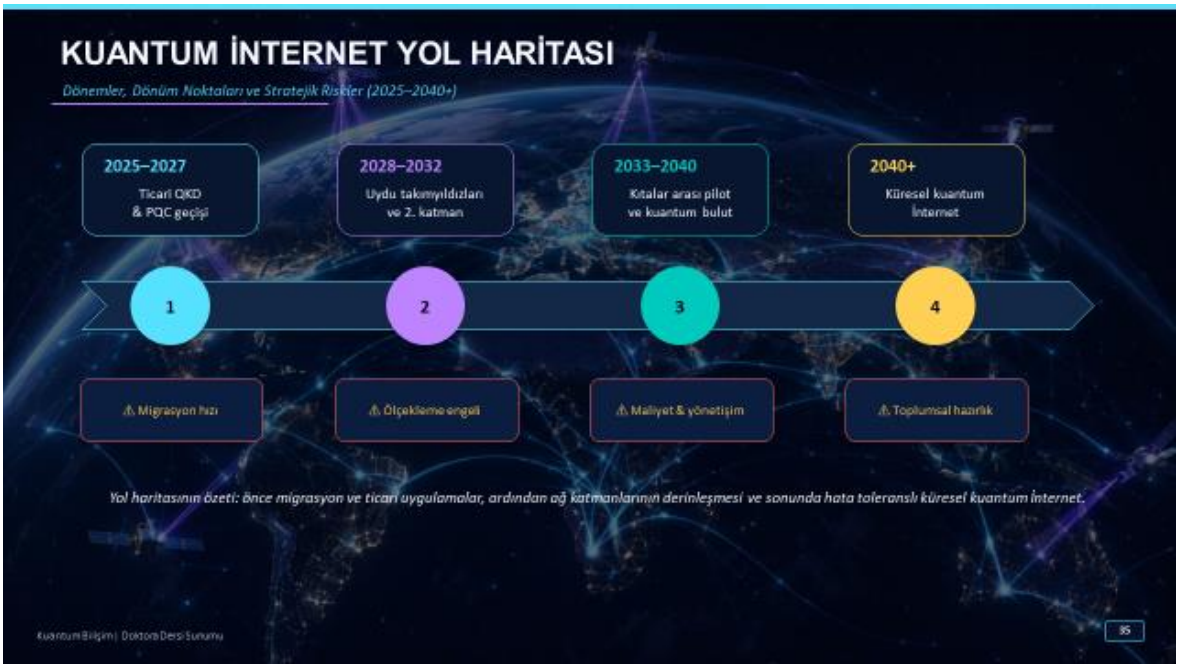
Kuantum haberleşmesi; doktora düzeyinde araştırma fırsatları sunan çok sayıda kritik açık problemle karşı karşıyadır. Bunların başında kuantum bellek geliştirme gelmektedir: Yüksek koherans süresi (T_2), yüksek okuma/yazma verimi ve 1550 nm telekom fotonlarıyla uyumluluğu eş zamanlı sağlayan ölçeklenebilir bir platform henüz mevcut değildir (Azuma vd., 2023). Ağ yönlendirme problemi; dolanıklık kaynak tahsisi, zamanlama senkronizasyonu ve optimal yönlendirme algoritmaları gerektirmekte, bu alanlar klasik ağ kuramından bütünüyle farklı yaklaşımlar talep etmektedir. Fotonik-qubit dönüşümü -1550 nm telekom fotonları ile atomik veya süperiletken düğümler arasında verimli frekans ve mod dönüşümü- kritik darboğaz olmayı sürdürmektedir. Son olarak DI-QKD'nin metro ağ ölçeğine taşınması; dedektör verimliliği, senkronizasyon ve anahtar üretim hızı bakımından somut mühendislik problemleri içermektedir (Nadlinger vd., 2022).

9.13.2 Kuantum İnternet Yol Haritası (2025–2040+)

Wehner, Elkouss ve Hanson'ın çizdiği çerçeve ve güncel sektörel gelişmeler ışığında Kuantum İnternet'in evrimi için dört belirleyici dönem öngörülmektedir (Wehner vd., 2018). Bu dönemlerin odak alanları ve stratejik riskleri Tablo 9.6'da, aynı bilgi kronolojik bir zaman çizelgesi olarak Şekil 9.17'de sunulmaktadır:

Tablo 9.6. Kuantum İnternet gelişim yol haritası: Dönemler, odak alanları ve stratejik riskler.

Dönem	Odak Alanları	Stratejik Risk
2025–2027	Ticari QKD yaygınlaşması; FIPS 203/204/205 geçiş kampanyaları; 1. nesil tekrarlayıcı prototipleri	PQC migrasyon hızı yetersizliği
2028–2032	LEO uydu kuantum takımyıldızları; 2. nesil ağ pilotları; DI-QKD metro demosu	Teknik ölçekleme engelleri
2033–2040	Kıtalar arası pilot Kuantum İnternet; kuantum bulut erişimi; tam PQC migrasyonu tamamlanması	Maliyet ve yönetişim karmaşıklığı
2040+	Dağıtık kör kuantum hesaplama; kuantum sensör ağları; standartlaşmış küresel ekosistem	Toplumsal ve kurumsal hazırlık



Şekil 9.17. Kuantum İnternet yol haritası (2025–2040+): Dönemler, dönüm noktaları ve stratejik riskler.

BÖLÜME AİT SUNUM SLAYTINA ERİŞİM İÇİN QR KOD



BÖLÜM 10

Kuantum Haberleşme Uygulamaları ve Sistem Mimarileri

Fotonik Katmandan Güvenli Kuantum Ağlarına Uçtan Uca Mühendislik Yaklaşımı

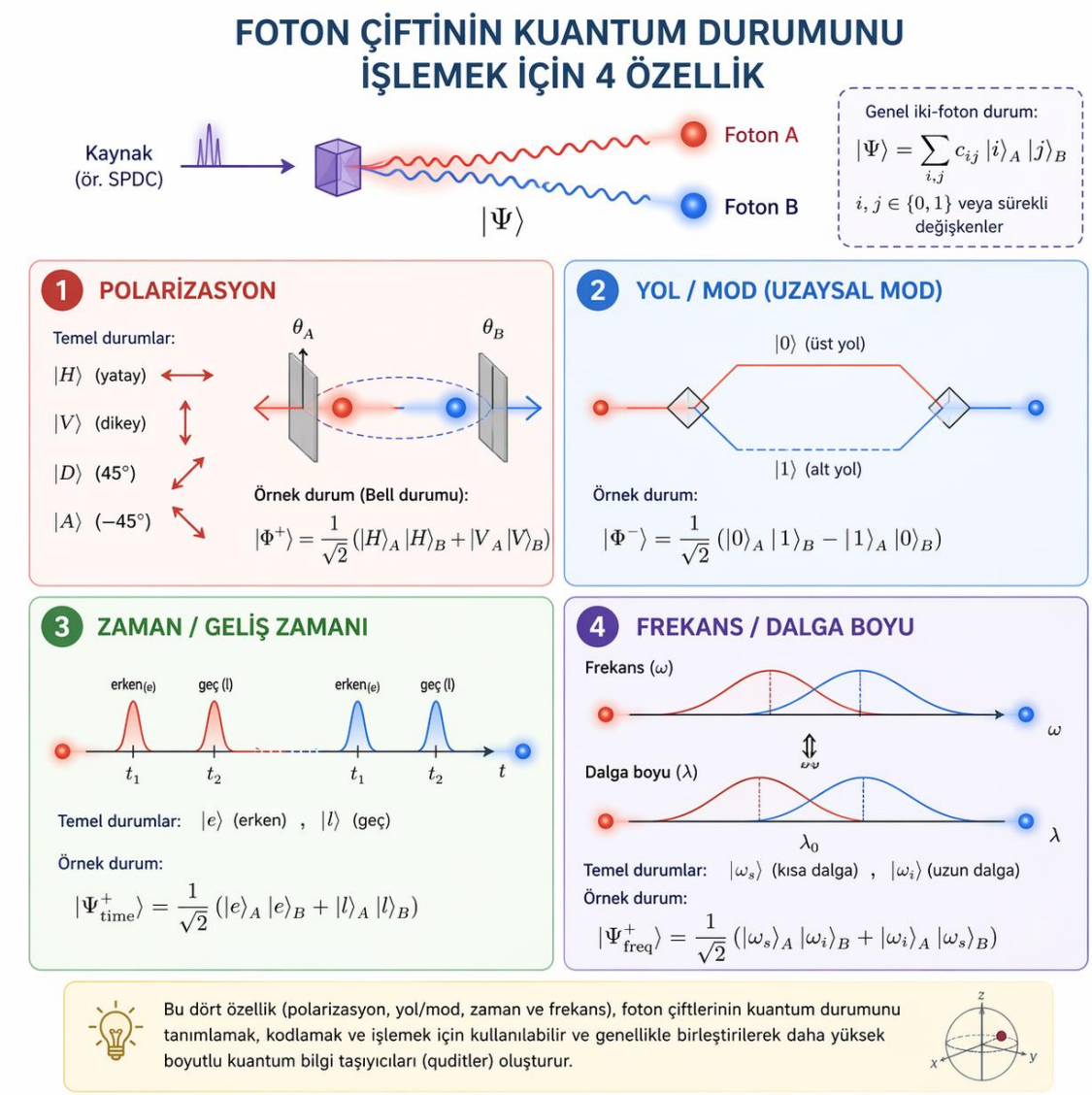
10.1 Giriş: Uygulamadan Mimariye

Kuantum haberleşmesinin laboratuvar deneyinden işletilebilir bir sisteme dönüşmesi, kuantum fiziği ile optik haberleşme, elektronik zamanlama, anahtar yönetimi, ağ denetimi ve siber güvenlik süreçlerinin aynı mimari içinde ele alınmasını gerektirir. Önceki bölümde açıklanan QKD protokolleri ve güvenlik ilkeleri, ancak kaynak, kanal, algılama, klasik son işlem ve uygulama katmanları birlikte tasarlandığında gerçek bir hizmet üretir.

Bu bölüm, kitabın kuramsal çerçevesini sistem düzeyinde tamamlamak amacıyla fotonik kodlama seçeneklerini, fiber altyapısının sınırlarını, BB84 tabanlı bir QKD bağlantısının uçtan uca işleyişini, kuantum tekrarlayıcı mimarisini ve ağ katmanlarını bütüncül biçimde incelemektedir. Şemalarda verilen mesafe, hız ve hata oranları tasarım örneğidir; gerçek sistem boyutlandırması cihaz veri sayfaları, kanal ölçümleri ve uygulanacak güvenlik kanıtına göre yapılmalıdır.

10.2 Fotonik Bilgi Taşıyıcıları ve Kodlama Serbestlik Dereceleri

Fotonik kuantum haberleşmesinde bilgi yalnızca polarizasyona kodlanmak zorunda değildir. Şekil 10.1'de gösterildiği gibi yol ya da uzaysal mod, erken-geç zaman-binleri ve frekans bantları da ayrık kuantum durumları olarak kullanılabilir. Birden fazla serbestlik derecesinin birlikte kullanılması, foton başına taşınan bilgi miktarını artıran yüksek boyutlu qudit kodlamalarına ve hibrit dolanıklık yapılarına olanak verir. Bununla birlikte daha yüksek boyut, kaynak kararlılığı, mod ayrıştırma, faz kilitleme ve dedektör zaman çözünürlüğü üzerinde daha sıkı mühendislik gereksinimleri doğurur (Erhard, Krenn ve Zeilinger, 2020).

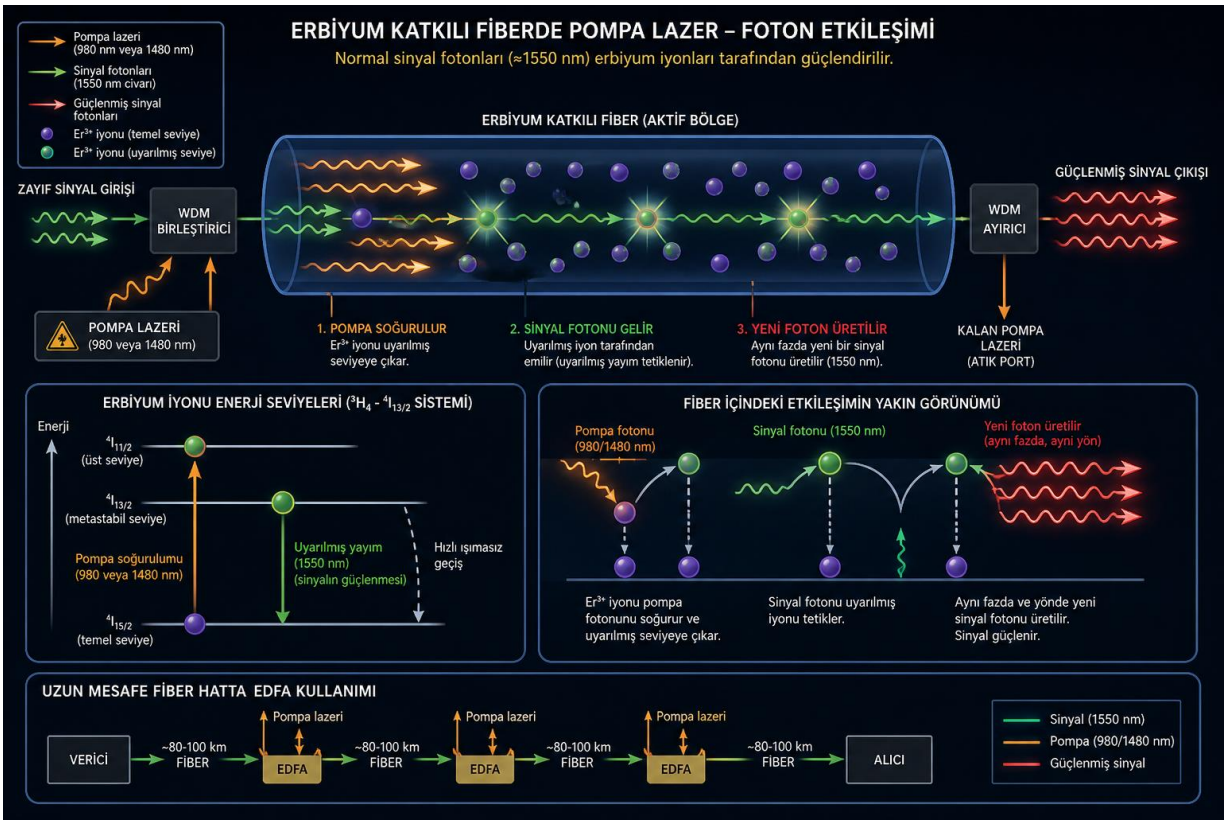


Şekil 10.1. Foton çiftinin kuantum durumunu kodlamak ve işlemek için kullanılan dört temel serbestlik derecesi: polarizasyon, yol/uzaysal mod, zaman-bin ve frekans/dalga boyu. Şematik gösterim yazarlar tarafından hazırlanmıştır.

Kodlama seçimi kanalın fiziksel davranışıyla uyumlu olmalıdır. Polarizasyon serbest uzay ve kısa fiber bağlantılarında yalın bir çözüm sunarken uzun fiberlerde çift-kırılma ve sıcaklık değişimleri aktif izleme gerektirir. Zaman-bin kodlaması fiberde polarizasyon sürüklenmesine daha dayanıklıdır, fakat interferometre kararlılığı ve hassas zaman damgalama ister. Frekans kodlaması WDM altyapısıyla uyumludur; spektral saflık ve filtre izolasyonu belirleyicidir. Yol kodlaması ise entegre fotonik devrelerde doğal olsa da çok modlu yayılım ve bağlantı kayıpları dikkatle yönetilmelidir.

10.3 Fiber Altyapısı, Klasik Servis Kanalları ve EDFA

Klasik fiber omurgalarında 1550 nm bandındaki kayıplar, erbiyum katkılı fiber yükselteçler (EDFA) ile dengelenir. Şekil 10.2, 980 veya 1480 nm pompa lazerinin Er3+ iyonlarını uyararak 1550 nm civarındaki klasik sinyali uyarılmış yayım yoluyla güçlendirmesini göstermektedir (Mears vd., 1987; Agrawal, 2019). Ancak bu mekanizma tek-foton kuantum kanalına uygulanamaz: bilinmeyen kuantum durumunun kusursuz kopyalanması no-cloning teoremiyle yasaktır ve optik yükseltecin eklediği spontan yayım gürültüsü kuantum durumunu bozar. Bu nedenle EDFA, aynı fiberde taşınan klasik veri, saat veya yönetim kanallarında kullanılabilir; kuantum kanalında ise düşük kayıp, spektral filtreleme ve uygun düğüm mimarisi gerekir.



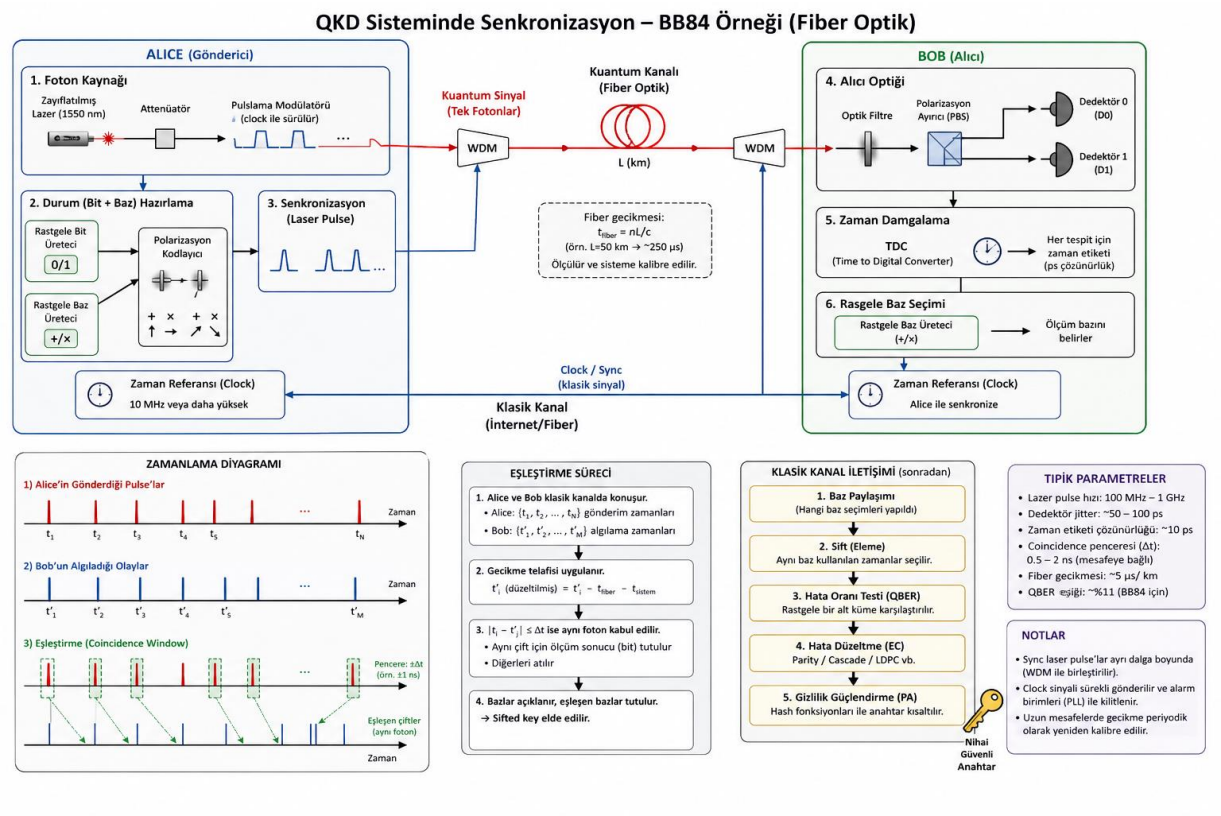
Şekil 10.2. Erbiyum katkılı fiber yükselteçte pompa lazeri, uyarılmış yayım ve uzun mesafe klasik fiber bağlantısındaki EDFA yerleşimi. Kuantum kanalının doğrudan yükseltilmesini değil, klasik optik servis kanalını açıklayan şematik gösterimdir.

Aynı fiber üzerinde klasik ve kuantum kanallarının birlikte işletilmesi maliyet avantajı sağlar, ancak güç bütçeleri birbirinden ayrılmalıdır. Klasik verici gücü, kanal aralığı, yönlülük, filtre bastırması ve fiber uzunluğu; Raman saçılması ile çapraz konuşmanın tek-foton dedektörlerinde oluşturduğu sayım oranını belirler. Uygulamada kuantum kanalı için ayrılmış fiber, geniş spektral ayırım, düşük güçlü klasik kanal, dar bant filtre ve zaman kapılama seçenekleri birlikte değerlendirilir.

Bağlantı bütçesi yalnızca fiber zayıflamasını değil; konektör, ek, WDM, filtre, modülatör ve alıcı optiği kayıplarını da içermelidir. Toplam kanal geçirgenliği düştükçe güvenli anahtar üretim hızı azalır; karanlık sayımlar ve arka plan fotonları QBER içindeki payını artırır. Tekrarlayıcısız kuantum iletişimin temel hız-mesafe sınırları, yalnızca daha güçlü kaynak kullanılarak aşılamaz (Pirandola vd., 2017).

10.4 BB84 QKD Uçtan Uca Sistem Mimarisi ve Senkronizasyon

Uçtan uca bir QKD bağlantısı, yalnızca foton kaynağı ile dedektörden ibaret değildir. Şekil 10.3'teki BB84 örneğinde Alice tarafında lazer, zayıflatıcı, darbe modülatörü, rastgele bit ve baz üretimi ile durum hazırlama; Bob tarafında optik filtre, baz seçimi, tek-foton dedektörleri ve zaman-sayısal dönüştürücü bulunur. Kuantum sinyali ile saat/senkron bilgisinin dalga boyu bölmeli çoğullama ile aynı fiberde taşınması mümkündür; ancak klasik kanalın Raman saçılması ve sızıntısı, kuantum kanalındaki gürültü bütçesine dahil edilmelidir.



Şekil 10.3. Fiber optik BB84 QKD sisteminde Alice ve Bob uçları, kuantum ve klasik kanallar, saat eşzamanlaması, zaman damgalama ve son işlem adımları. Şematik gösterim yazarlar tarafından hazırlanmıştır.

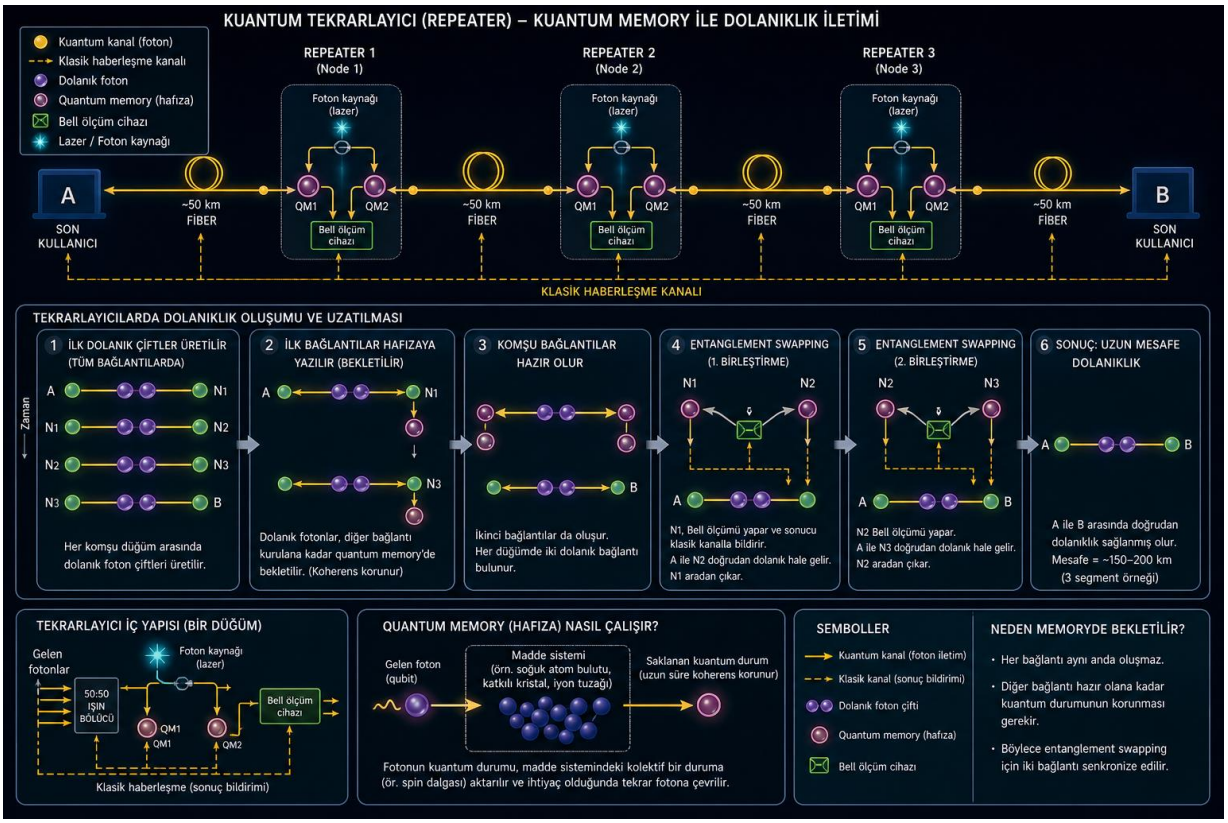
Bob'un zaman damgaları, fiber yayılım gecikmesi ve sistem içi sabit gecikmeler çıkarıldıktan sonra Alice'in gönderim pencereleriyle eşleştirilir. Pencere çok dar seçilirse saat kayması ve dedektör jitter'ı nedeniyle gerçek olaylar kaybedilir; çok geniş seçilirse karanlık sayım ve arka plan olayları kabul edilir. Bu nedenle saat kararlılığı, periyodik gecikme kalibrasyonu ve pikosanisaniye düzeyinde zaman etiketleme, protokol güvenliğinin parçasıdır.

Klasik son işlemde taraflar bazlarını açıklar, farklı bazlardaki olayları eler, örnek bitlerden QBER kestirir, hata düzeltme uygular ve gizlilik güçlendirmesiyle Eve'in olası bilgisini bastırır. İdeal, asimptotik ve tek yönlü son işlem varsayımlarındaki yaklaşık yüzde 11 BB84 eşiği evrensel bir cihaz kabul sınırı değildir; sonlu anahtar etkileri, kaynak kusurları ve yan-kanal modeli hesaba katıldığında işletim eşiği daha düşük seçilir (Shor ve Preskill, 2000; Scarani vd., 2009). Anahtar teslim arayüzleri ve yaşam döngüsü yönetimi de protokol kadar önemlidir (ETSI, 2019).

Kimliği doğrulanmamış klasik kanal, ortadaki adam saldırısına açıktır. Dolayısıyla QKD gizli anahtar üretse bile ilk kimlik doğrulama anahtarı, anahtar yenileme politikası, güvenli depolama, silme, denetim kaydı ve uygulamaya anahtar teslimi ayrı güvenlik kontrolleri olarak tasarlanmalıdır.

10.5 Kuantum Tekrarlayıcılar, Bellek ve Dolanıklık Değişimi

Kuantum tekrarlayıcı, zayıflayan fotonu yükseltmez; uzun hattı daha kısa bağlantılara böler, komşu düğümler arasında dolanıklık üretir ve başarılı bağlantıları kuantum bellekte saklar. Şekil 10.4'te gösterilen Bell-durumu ölçümleri, dolanıklık değişimi yoluyla kısa bağlantıları uçtan uca bir dolanık çifte dönüştürür. Başarı bilgisinin klasik kanaldan iletilmesi ve belleklerin eşzamanlı çalışması zorunludur. Bu yaklaşım klasik tekrarlayıcı mantığından temelden farklıdır ve bellek ömrü, dolanıklık üretim olasılığı, yerel işlem doğruluğu ve çoklu düğüm zamanlaması tarafından sınırlandırılır (Briegel vd., 1998; Sangouard vd., 2011; Wehner vd., 2018).



Şekil 10.4. Kuantum bellekler ve Bell-durumu ölçümleri kullanan çok bölümlü kuantum tekrarlayıcı mimarisi ile dolanıklık değişiminin aşamaları. Şematik gösterim yazarlar tarafından hazırlanmıştır.

Bir tekrarlayıcı zincirinin performansı yalnızca segment uzunluğuyla belirlenmez. Dolanıklık üretiminin olasılıksal olması, farklı segmentlerin aynı anda hazır olmamasına yol açar; bu nedenle kuantum belleğin koherens süresi, en yavaş bağlantının bekleme süresini aşmalıdır. Çok kipli bellek, paralel deneme sayısını artırabilir. Dolanıklık damıtma ve kuantum hata düzeltme daha yüksek son durum sadakati sağlayabilir, ancak ek qubit, kapı ve klasik koordinasyon maliyeti getirir. Günümüz ağlarında güvenilir düğümlü QKD uygulanabilirken, hata-toleranslı uçtan uca kuantum tekrarlayıcılar halen yoğun araştırma ve geliştirme konusudur.

10.6 Katmanlı Sistem Mimarisi

Kuantum haberleşme sistemi, arızayı ve güvenlik sorumluluğunu izole eden katmanlı bir yapıyla yönetilebilir. Tablo 10.1, fiziksel fotonik katmandan uygulamaya kadar temel görevleri ve ölçülmesi gereken başlıca göstergeleri özetlemektedir. Katmanlar arasında açık arayüz tanımı yapılması, farklı üreticilerin birlikte çalışabilirliği ve güvenlik kanıtında kullanılan varsayımların sahadaki cihaz yapılandırmasıyla eşleşmesi açısından kritiktir (ITU-T, 2019).

Tablo 10.1. Kuantum haberleşme sisteminde katmanlar, görevler ve izleme ölçütleri.

Katman	Bileşenler ve temel görev	Başlıca ölçütler
Fiziksel fotonik	Kaynak, modülatör, fiber/serbest uzay, WDM, filtre, dedektör; kuantum durumunu üretir, taşır ve ölçer.	Kayıp, görünürlük, sayım hızı, karanlık sayım, jitter
Bağlantı ve protokol	Durum hazırlama, baz seçimi, zaman eşleme, eleme ve parametre kestirimi işlemlerini yürütür.	QBER, ham/elenmiş/güvenli anahtar hızı, kullanılabilirlik
Anahtar yönetimi	Hata düzeltme, gizlilik güçlendirmesi, anahtar kimliği, depolama, yenileme ve uygulamaya teslimi yönetir.	Anahtar yaşı, tüketim hızı, havuz doluluğu, başarısız teslim
Ağ ve denetim	Yol seçimi, düğüm güven modeli, dalga boyu/zaman kaynağı tahsisi, alarm ve telemetriyi koordine eder.	Uçtan uca gecikme, yol sürekliliği, düğüm güven durumu
Uygulama ve güvenlik	Şifreleme cihazı, VPN, veri merkezi veya görev uygulamasında anahtarı politika doğrultusunda kullanır.	Politika uyumu, denetim izi, anahtar kullanım hatası

Katmanlı yaklaşım güven sınırlarını görünür kılar. Örneğin güvenilir düğümlü bir QKD ağında ara düğüm anahtarı düz metin halinde işleyebilir ve fiziksel olarak korunması gerekir; kuantum tekrarlayıcı ağında hedef, ara düğümün uçtan uca anahtarı öğrenmemesidir. Her iki durumda da klasik yönetim düzlemi kimlik doğrulama, yetkilendirme ve bütünlük koruması gerektirir.

10.7 Uygulama Alanları ve Mimari Seçimler

Uygun mimari, uygulamanın mesafesi, güven modeli, anahtar tüketimi, hizmet sürekliliği ve maliyet hedefleriyle birlikte seçilmelidir. Tablo 10.2, öne çıkan kullanım alanlarını ve bunlara karşılık gelen sistem yaklaşımını karşılaştırmaktadır. QKD'nin veri taşımadığı, şifreleme sistemlerine anahtar sağladığı; dolanıklık dağıtımının ise dağıtık kuantum hesaplama, teleportasyon ve ağ tabanlı algılama gibi daha genel görevleri mümkün kıldığı ayrımı korunmalıdır.

Tablo 10.2. Başlıca kuantum haberleşme uygulamaları ve uygun sistem mimarileri.

Uygulama	Mimari yaklaşım	Değerlendirme
Metro ve veri merkezi bağlantıları	Noktadan noktaya fiber QKD; gerektiğinde aynı fiberde WDM ile klasik servis kanalı.	En olgun kullanım alanıdır; kayıp, birlikte yayılım gürültüsü ve anahtar yönetimi belirleyicidir.
Ulusal omurga ve kritik altyapı	Güvenilir düğümlü QKD ağı, çoklu yol ve merkezî anahtar yönetimi.	Geniş kapsama sağlar; ara düğümlerin fiziksel ve yönetsel güvenliği zorunludur.
Uydu ve serbest uzay	Yer-uydu QKD veya dolanıklık dağıtımı; optik yer istasyonları.	Kıtalar arası erişim sağlar; hava, görüş hattı, takip ve sınırlı temas pencereleri etkiler.
Kuantum internet	Kuantum bellekli tekrarlayıcılar, dolanıklık yönlendirme ve teleportasyon.	Uçtan uca kuantum durum aktarımını hedefler; teknoloji olgunluğu henüz düşüktür.
Dağıtık kuantum hesaplama	Dolanık bağlantılarla modüler işlemciler ve uzaktan kapı işlemleri.	Ölçeklenebilir işlemci fikrini destekler; yüksek sadakat ve düşük gecikme gerektirir.
Saat, algılama ve bilimsel ağlar	Dolanıklık destekli zaman/frekans aktarımı ve dağıtık sensörler.	Temel bilim ve metroloji değeri yüksektir; kalibrasyon ve faz kararlılığı kritiktir.

Kurumsal geçişte tek bir teknolojiye bağımlı tasarım yerine kripto-çevik mimari tercih edilmelidir. QKD fiziksel bağlantı ve özel cihaz gerektirirken kuantum sonrası kriptografi yazılım ve protokol katmanlarında daha geniş ölçeklenebilirlik sunar. Uzun süre gizli kalması gereken yüksek değerli bağlantılarda QKD ile standartlaşmış PQC mekanizmalarının bağımsız veya birleşik anahtar türetme içinde kullanılması, tek hata noktasını azaltan savunma-derinliği yaklaşımı sağlayabilir.

10.8 Mühendislik ve Güvenlik Değerlendirmesi

Bir kuantum haberleşme projesinin kabul testi, yalnızca anahtar üretildiğini göstermemelidir. Optik kayıp ve gürültü bütçesi, QBER ve güvenli anahtar hızı, sonlu anahtar parametreleri, saat sapması, cihaz yeniden başlatma davranışı, anahtar havuzu taşması/boşalması, yedek yol geçişi ve alarm üretimi birlikte doğrulanmalıdır. Laboratuvar performansı ile 7/24 saha kullanılabilirliği ayrı ölçütlerdir.

Güvenlik kanıtının kapsamadığı cihaz davranışları ayrıca sınanmalıdır: dedektör körleme, zaman kaydırma, Trojan-horse ışığı, kaynak yan kanalları, kalibrasyon manipülasyonu ve yazılım tedarik zinciri bunların başlıcalarıdır. Optik izolasyon ve güç izleme, rastgelelik sağlık testleri, güvenli önyükleme, imzalı güncelleme, rol tabanlı erişim ve değişmez denetim kayıtları savunmanın farklı katmanlarını oluşturur.

İşletme modeli de fiziksel mimari kadar önemlidir. Düğüm sahipliği, anahtarın hangi güven bölgesinde açık olarak bulunduğu, arıza durumunda hangi klasik mekanizmaya dönüleceği ve olay kayıtlarının nasıl ilişkilendirileceği önceden tanımlanmalıdır. Standart arayüzler birlikte çalışabilirliği kolaylaştırsa da uygunluk belgesi tek başına uçtan uca güvenlik garantisi değildir; yapılandırma ve operasyon süreçleri sürekli denetlenmelidir.

BÖLÜM 11

Kapanış

Kuantum Bilişimden Kuantum Ağlara

Bu kitap, klasik bilgi ve sayısal sistemlerden başlayarak qubit, süperpozisyon, ölçüm ve dolanıklık kavramlarına; kuantum devreleri, algoritmalar, hata düzeltme, donanım platformları ve güvenli haberleşme uygulamalarına uzanan bütünlüklü bir öğrenme yolu kurmuştur. Bölümler boyunca görüldüğü gibi kuantum üstünlüğü tek bir hızlı algoritmadan değil, fiziksel sistem, kontrol elektroniği, yazılım ve problem modelinin uyumundan doğar.

Kuantum bilgisayarlar bazı hesaplama sınıflarında yeni olanaklar sunarken mevcut kriptografik altyapı için de dönüşüm baskısı yaratmaktadır. Bu nedenle geleceğin güvenliği yalnızca QKD'ye ya da yalnızca kuantum sonrası kriptografiye indirgenemez. En sağlam yaklaşım; veri ömrünü, tehdit modelini, fiziksel bağlantıyı, standartları ve operasyon kapasitesini birlikte değerlendiren kripto-çevik ve katmanlı bir mimaridir.

Kuantum haberleşme sistemleri, kuantum mekaniğinin soyut ilkelerini gerçek dünyanın kayıp, gürültü, gecikme ve güven sınırlarıyla buluşturur. Foton kaynağından uygulamanın anahtar tüketimine kadar her arayüz ölçülebilir ve doğrulanabilir olmalıdır. Bilimsel iddia ile mühendislik varsayımını ayırmak, şematik değerleri bağlama özgü kabul kriterleriyle karıştırmamak ve güvenlik kanıtının cihaz gerçekliğiyle uyumunu sorgulamak, bu alanın temel mesleki sorumluluğudur.

Kuantum teknolojilerinin uzun vadeli etkisi, yalnızca daha güçlü makineler üretmekte değil; hesaplama, iletişim ve güven kavramlarını yeniden birlikte tasarlamakta yatmaktadır. Bu kitabın amacı, okura kesinleşmemiş vaatler yerine sağlam kavramlar, eleştirel değerlendirme alışkanlığı ve yeni gelişmeleri izleyebileceği teknik bir temel kazandırmaktır. Kuantum çağında başarı, fiziğin sınırlarını anlamak kadar bu sınırlar içinde güvenilir, sorumlu ve birlikte çalışabilir sistemler kurabilmeye bağlı olacaktır.

Kaynakça

Aaronson, S. (2013). Quantum computing since Democritus. Cambridge University Press.

Acharya, R., vd. (2025). Quantum error correction below the surface code threshold. Nature, 638, 920–926.

Agrawal, G. P. (2019). Fiber-optic communication systems (5th ed.). Wiley.

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., ve Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process (NISTIR 8413). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8413

Allen, R. (2024). Introduction to quantum computing. Lone Star Analysis.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., ... Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510. https://doi.org/10.1038/s41586-019-1666-5

Aspect, A., Grangier, P., ve Roger, G. (1982). Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell's inequalities. Physical Review Letters, 49(2), 91–94.

Aspuru-Guzik, A., Dutoi, A. D., Love, P. J., ve Head-Gordon, M. (2005). Simulated quantum computation of molecular energies. Science, 309(5741), 1704–1707. https://doi.org/10.1126/science.1113479

Azuma, K., vd. (2023). Quantum repeaters: From quantum networks to the quantum internet. Reviews of Modern Physics, 95(4), 045006.

Banegas, G., ve Bernstein, D. J. (2017). Low-communication parallel quantum multi-target preimage search. In R. Avanzi ve H. Heys (Eds.), Selected Areas in Cryptography: SAC 2017 (Lecture Notes in Computer Science, Vol. 10719, pp. 325–335). Springer. https://doi.org/10.1007/978-3-319-72565-9_16

Barker, E. (2020). Recommendation for key management: Part 1: General (NIST Special Publication 800-57 Part 1 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r5

Barker, E., Chen, L., ve Roginsky, A. (2020). Transitioning to post-quantum cryptography (NIST Special Publication 800-238, Initial Public Draft). National Institute of Standards and Technology.

Barzanjeh, S., Guha, S., Weedbrook, C., Vitali, D., Shapiro, J. H., ve Pirandola, S. (2015). Microwave quantum illumination. Physical Review Letters, 114, 080503.

Bayram, M., ve Ilgaz Çağlayan, E. (2024). Comparative Analysis of BB84 and E91 Quantum Cryptography Protocols. Kocaeli Science Congress 2024 (KOSC-2024), 104-109. doi:https://doi.org/10.5281/zenodo.14316751

Bell, J. S. (1964). On the Einstein Podolsky Rosen paradox. Physics Physique Fizika, 1(3), 195–200. https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195

Bennett, C. H., Bernstein, E., Brassard, G., ve Vazirani, U. (1997). Strengths and weaknesses of quantum computing. SIAM Journal on Computing, 26(5), 1510–1523. https://doi.org/10.1137/S0097539796300933

Bennett, C. H., ve Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (pp. 175–179).

Bennett, C. H., ve Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. Theoretical computer science, 7-11.

Bernhardt, C. (2019). Quantum computing for everyone. MIT Press.

Bernstein, D. J. (2010). Grover vs. McEliece. In N. Sendrier (Ed.), Post-Quantum Cryptography (pp. 73–80). Springer. https://doi.org/10.1007/978-3-642-12929-2_6

Bernstein, D. J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., ve Schwabe, P. (2019). The SPHINCS+ signature framework. In L. Cavallaro, J. Kinder, X. Wang, ve J. Katz (Eds.), Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 2129–2146). ACM. https://doi.org/10.1145/3319535.3363229

Bernstein, D. J., ve Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. https://doi.org/10.1038/nature23461

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., ve Stehle, D. (2018). CRYSTALS–Kyber: A CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 353–367). IEEE. https://doi.org/10.1109/EuroSP.2018.00032

Bradley, T. D., van den Hout, M., Kalla, B., van Vliet, V., Bigot-Astruc, M., Correa, A. A., Sillard, P., Weiner, G., Winzer, P., ve Okonkwo, C. (2024). Fiber eavesdropping using tapers in standard and trench-assisted single-mode fibers. IEEE Photonics Technology Letters, 36(15), 953–956. https://doi.org/10.1109/LPT.2024.3410043

Brassard, G., Høyer, P., Mosca, M., ve Tapp, A. (2002). Quantum amplitude amplification and estimation. In S. J. Lomonaco ve H. E. Brandt (Eds.), Quantum Computation and Information (pp. 53–74). American Mathematical Society. https://doi.org/10.1090/conm/305/05215

Briegel, H.-J., Dür, W., Cirac, J. I. ve Zoller, P. (1998). Quantum repeaters: The role of imperfect local operations in quantum communication. Physical Review Letters, 81(26), 5932-5935.

BSI (Bundesamt für Sicherheit in der Informationstechnik). (2021). Migration to post-quantum cryptography: Recommendations for action (Technical Guideline TR-02102). Federal Office for Information Security. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Quantencomputer-und-Post-Quanten-Kryptografie/quantencomputer_node.html

Buhrman, H., ve de Wolf, R. (2002). Complexity measures and decision tree complexity: A survey. Theoretical Computer Science, 288(1), 21–43. https://doi.org/10.1016/S0304-3975(01)00144-X

Carnegie Endowment for International Peace. (2024, December). Securing Europe's subsea data cables.

Castryck, W., ve Decru, T. (2023). An efficient key recovery attack on SIDH. In C. Hazay ve M. Stam (Eds.), Advances in Cryptology: EUROCRYPT 2023 (Lecture Notes in Computer Science, Vol. 14008, pp. 423–447). Springer. https://doi.org/10.1007/978-3-031-30589-4_15

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., ve Smith-Tone, D. (2016). Report on post-quantum cryptography (NISTIR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

Chen, Y.-A., vd. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature, 589, 214-219.

Clauser, J. F., Horne, M. A., Shimony, A., ve Holt, R. A. (1969). Proposed experiment to test local hidden-variable theories. Physical Review Letters, 23(15), 880–884. https://doi.org/10.1103/PhysRevLett.23.880

Cleve, R., Ekert, A., Macchiavello, C., ve Mosca, M. (1998). Quantum algorithms revisited. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 454(1969), 339–354. https://doi.org/10.1098/rspa.1998.0164

Coppersmith, D. (2002). An approximate Fourier transform useful in quantum factoring (Research Report RC 19642). IBM. https://arxiv.org/abs/quant-ph/0201067

Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA) ve NIST. (2023). Quantum-readiness: Migration to post-quantum cryptography. Joint Cybersecurity Advisory.

Daemen, J., ve Rijmen, V. (2002). The design of Rijndael: AES: The Advanced Encryption Standard. Springer. https://doi.org/10.1007/978-3-662-04722-4

de Wolf, R. (2023). Quantum computing lecture notes. CWI. https://homepages.cwi.nl/~rdewolf/qcnotes.pdf

Degen, C. L., Reinhard, F. ve Cappellaro, P. (2017). Quantum Sensing. Reviews of Modern Physics, 89(3), 035002.

Deutsch, D., ve Jozsa, R. (1992). Rapid solution of problems by quantum computation. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 439(1907), 553–558. https://doi.org/10.1098/rspa.1992.0167

Devoret, M. H., ve Schoelkopf, R. J. (2013). Superconducting circuits for quantum information. Science.

Dieks, D. (1982). Communication by EPR devices. Physics Letters A, 92(6), 271–272. https://doi.org/10.1016/0375-9601(82)90084-6

Diffie, W., ve Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.

Dirac, P. A. M. (1930). The principles of quantum mechanics. Oxford University Press.

Duan, L.-M., Lukin, M. D., Cirac, J. I. ve Zoller, P. (2001). Long-distance quantum communication with atomic ensembles and linear optics. Nature, 414, 413-418.

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., ve Stehle, D. (2018). CRYSTALS-Dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(1), 238–268. https://doi.org/10.13154/tches.v2018.i1.238-268

Einstein, A., Podolsky, B., ve Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? Physical Review, 47(10), 777–780. https://doi.org/10.1103/PhysRev.47.777

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661–663. https://doi.org/10.1103/PhysRevLett.67.661

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4), 469–472. https://doi.org/10.1109/TIT.1985.1057074

Erhard, M., Krenn, M., ve Zeilinger, A. (2020). Advances in high-dimensional quantum entanglement. Nature Reviews Physics, 2, 365-381. https://doi.org/10.1038/s42254-020-0193-5

ETSI (European Telecommunications Standards Institute). (2020). Quantum-safe cryptography: Current state and quantum cryptanalysis of classical encryption schemes (ETSI White Paper No. 8, 2nd ed.). ETSI. https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

European Telecommunications Standards Institute (ETSI). (2019). Quantum key distribution (QKD); Protocol and data format of REST-based key delivery API (ETSI GS QKD 014 V1.1.1). ETSI. https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf

European Telecommunications Standards Institute (ETSI). (2023). QKD implementation security: Protection profile (GS QKD 016). ETSI.

European Telecommunications Standards Institute. (2015). ETSI White Paper No. 8: Quantum safe cryptography and security.

Feynman, R. P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21(6–7), 467–488.

Foschini, L. (2013). Where the "it from bit" come from? arXiv preprint arXiv:1306.0545.

Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., ve Zhang, Z. (2020). Falcon: Fast-Fourier lattice-based compact signatures over NTRU (Version 1.2). NIST PQC Round 3 Submission. https://falcon-sign.info

Fowler, A. G., Mariantoni, M., Martinis, J. M., ve Cleland, A. N. (2012). Surface codes: Towards practical large-scale quantum computation. Physical Review A, 86(3), 032324. https://doi.org/10.1103/PhysRevA.86.032324

Frontiers in Physics. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. Frontiers in Physics, 12, Article 1456491. https://doi.org/10.3389/fphy.2024.1456491

FS.com. (2023). What is inside an SFP module? Understanding TOSA, ROSA, BOSA.

Gidney, C. (2025). How to factor 2048-bit RSA integers with less than a million noisy qubits. arXiv:2505.15917.

Gidney, C., ve Ekerå, M. (2021). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. Quantum, 5, 433.

Gisin, N., Ribordy, G., Tittel, W., ve Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145–195. https://doi.org/10.1103/RevModPhys.74.145

Global Taiwan Institute. (2025, March). Countering China's subsea cable sabotage.

Gottesman, D. (1998). The Heisenberg representation of quantum computers. arXiv:quant-ph/9807006. https://arxiv.org/abs/quant-ph/9807006

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In G. L. Miller (Ed.), Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96) (pp. 212–219). ACM. https://doi.org/10.1145/237814.237866

Gupta, S., Huang, Y., Liu, S., Pei, Y., Gao, Q., Yang, S., Tomm, N., Warburton, R. J., ve Zhong, T. (2025). Dual epitaxial telecom spin-photon interfaces with long-lived coherence. Nature Communications. https://doi.org/10.1038/s41467-025-64780-6

Hadfield, R. H. (2009). Single-photon detectors for optical quantum information applications. Nature Photonics, 3(12), 696–705.

Harris, D. M., ve Harris, S. L. (2021). Digital design and computer architecture (3. baskı). Morgan Kaufmann.

Harrow, A. W., Hassidim, A., ve Lloyd, S. (2009). Quantum algorithm for linear systems of equations. Physical Review Letters, 103(15), Article 150502. https://doi.org/10.1103/PhysRevLett.103.150502

HEC Paris. (2024). AI and sovereignty: The geopolitical power of submarine cables.

Heisenberg, W. (1927). Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Zeitschrift für Physik, 43(3–4), 172–198. https://doi.org/10.1007/BF01397280

Hensen, B., Bernien, H., Dréau, A. E., Reiserer, A., Kalb, N., Blok, M. S., ve Hanson, R. (2015). Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. Nature, 526, 682–686. https://doi.org/10.1038/nature15759

Huang, X., Wijejesekera, S., ve Sharma, D. (2008). Implementation of quantum key distribution in Wi-Fi wireless networks. Proceedings of the 10th International Conference on Advanced Communication Technology.

IBM Quantum. (2024). https://quantum.ibm.com

ID Quantique. (2015). Quantis: True random number generator exploiting quantum physics. http://www.idquantique.com/

Insikt Group / Recorded Future. (2025). Submarine cable security at risk amid geopolitical tensions and limited repair capabilities. Recorded Future.

International Telecommunication Union (ITU-T). (2019). Overview on networks supporting quantum key distribution (Recommendation ITU-T Y.3800). ITU. https://www.itu.int/rec/T-REC-Y.3800-201910-I/en

Jackson School of International Studies, University of Washington. (2025, July). Baltic Sea undersea cable security.

Jain, N., Anisimova, E., Khan, I., Makarov, V., Marquardt, C. ve Leuchs, G. (2014). Trojan-horse attacks threaten the security of practical quantum cryptography. New Journal of Physics, 16, 123030.

Karsa, A., Fletcher, A., Spedalieri, G., ve Pirandola, S. (2024). Quantum illumination and quantum radar: A brief overview. Reports on Progress in Physics, 87, 094001.

Kaye, P., Laflamme, R., ve Mosca, M. (2007). An introduction to quantum computing. Oxford University Press.

Kish, S., ve Pieprzyk, J. (2025). Quantum key distribution. arXiv. https://arxiv.org/abs/2507.23192

Kitaev, A. Y. (1995). Quantum measurements and the Abelian stabilizer problem. arXiv. https://arxiv.org/abs/quant-ph/9511026

Kofler, J. (2025). Quantum information lecture notes. JKU. https://www.jku.at/fileadmin/gruppen/180/2025_Quantum_Information_Lecture_Notes.pdf

Kwiat, P. G., Mattle, K., Weinfurter, H., Zeilinger, A., Sergienko, A. V., ve Shih, Y. (1995). New high-intensity source of polarization-entangled photon pairs. Physical Review Letters, 75(24), 4337–4341. https://doi.org/10.1103/PhysRevLett.75.4337

L-P Resources. (2026, April). SFP in networking: Function, types and applications.

Le Bellac, M. (2006). A short introduction to quantum information and quantum computation. Cambridge University Press.

Liao, S.-K., vd. (2017). Satellite-to-ground quantum key distribution. Nature, 549, 43-47.

Liu, W.-Z., Zhou, Y.-B., Chen, J.-P., Wang, B., Teng, A., Han, X.-W., Liu, G.-C., Zhang, Z.-J., Yang, Y., Liu, F.-G., Xue, C.-H., Yang, B.-W., Yang, J., Zeng, C., Pan, D.-R., Zheng, M.-Y., Zhang, X., Cao, S., Zhen, Y.-Z., Xiao, Y., Li, H., You, L., Ma, X., Zhao, Q., Xu, F., Wang, Y., Wan, Y., Zhang, Q., ve Pan, J.-W. (2026). Long-lived remote ion-ion entanglement for scalable quantum repeaters. Nature. https://doi.org/10.1038/s41586-026-10177-4

Lloyd, S. (2008). Enhanced sensitivity of photodetection via quantum illumination. Science, 321(5895), 1463–1465.

Lo, H.-K., Curty, M. ve Qi, B. (2012). Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), 130503.

Lo, H.-K., Curty, M., ve Qi, B. (2012). Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), 130503. https://doi.org/10.1103/PhysRevLett.108.130503

Lo, H.-K., Curty, M., ve Tamaki, K. (2014). Secure quantum key distribution. Nature Photonics, 8(8), 595–604.

Lo, H.-K., Curty, M., ve Tamaki, K. (2014). Secure quantum key distribution. Nature Photonics, 8, 595–604. https://doi.org/10.1038/nphoton.2014.149

Lu, B.-W., Yang, C.-W., Wang, R.-Q., Gao, B.-F., Zhen, Y.-Z., Wang, Z.-G., Shi, J.-K., Ren, Z.-Q., Hahn, T. A., Tan, E. Y.-Z., Xie, X.-P., Zheng, M.-Y., Jiang, X., Zhang, J., Xu, F., Zhang, Q., Bao, X.-H., ve Pan, J.-W. (2026). Device-independent quantum key distribution over 100 km with single atoms. Science, 391(6785), 592–597. https://doi.org/10.1126/science.aec6243

Lydersen, L., vd. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics, 4, 686–689. https://doi.org/10.1038/nphoton.2010.214

Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. ve Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics, 4, 686-689.

Mano, M. M., ve Ciletti, M. D. (2013). Digital design: With an introduction to the Verilog HDL (5. baskı). Pearson.

Mano, M. M., ve Ciletti, M. D. (2013). Digital Design: With an Introduction to the Verilog HDL, VHDL, and SystemVerilog (5th ed.). Pearson Education.

Mano, M. M., ve Ciletti, M. D. (2017). Digital design: With an introduction to the Verilog HDL, VHDL, and SystemVerilog (6. baskı). Pearson.

Mayers, D. (2001). Unconditional security in quantum cryptography. Journal of the ACM, 48(3), 351–406.

Mayers, D. (2001). Unconditional security in quantum cryptography. Journal of the ACM, 48(3), 351–406. https://doi.org/10.1145/382780.382781

McMahon, D. (2007). Quantum computing explained. Wiley.

Mears, R. J., Reekie, L., Jauncey, I. M., ve Payne, D. N. (1987). Low-noise erbium-doped fibre amplifier operating at 1.54 micrometres. Electronics Letters, 23(19), 1026-1028. https://doi.org/10.1049/el:19870719

Mermin, N. D. (2007). Quantum Computer Science: An Introduction. Cambridge University Press.

Monroe, C., ve Kim, J. (2013). Scaling the Ion Trap Quantum Processor. Science.

Moody, D., Alagic, G., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y.-K., Miller, C., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D., ve Alperin-Sheriff, J. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process (NISTIR 8309). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8309

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security ve Privacy, 16(5), 38-41.

Muralidharan, S., Li, L., Kim, J., Lütkenhaus, N., Lukin, M. D. ve Jiang, L. (2016). Optimal architectures for long distance quantum communication. Scientific Reports, 6, 20463.

Nadlinger, D. P., Drmota, P., Nichol, B. C., Araneda, G., Main, D., Srinivas, R., ve Bancal, J.-D. (2022). Experimental quantum key distribution certified by Bell's theorem. Nature, 607, 682–686. https://doi.org/10.1038/s41586-022-04941-5

Nadlinger, D. P., vd. (2022). Experimental quantum key distribution certified by Bell's theorem. Nature, 607, 682-686.

Nasedkin, B., vd. (2023). Loopholes in the 1500-2100-nm range for QKD systems using InGaAs APDs. Physical Review Applied, 19(5), 054052.

National Academies of Sciences, Engineering, and Medicine. (2019). Quantum computing: Progress and prospects. The National Academies Press. https://doi.org/10.17226/25196

National Institute of Standards and Technology (NIST). (2024). FIPS 203, FIPS 204, FIPS 205: Post-quantum cryptography standards. U.S. Department of Commerce.

National Institute of Standards and Technology. (2006). Minimum security requirements for federal information and information systems (FIPS Publication 200). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.200

National Institute of Standards and Technology. (2016). Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. U.S. Department of Commerce. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

National Institute of Standards and Technology. (2020a). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2020b). Protecting controlled unclassified information in nonfederal systems and organizations (NIST Special Publication 800-171 Rev. 2). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-171r2

National Institute of Standards and Technology. (2022a). PQC standardization process: Announcing four candidates to be standardized, plus fourth round candidates. U.S. Department of Commerce. https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4

National Institute of Standards and Technology. (2022b). Status report on the third round of the NIST post-quantum cryptography standardization process (NISTIR 8413). U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8413

National Institute of Standards and Technology. (2023a). About NIST. U.S. Department of Commerce. https://www.nist.gov/about-nist

National Institute of Standards and Technology. (2024). Post-quantum cryptography standards (FIPS 203, 204, 205). U.S. Department of Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography

National Institute of Standards and Technology. (2024a). Cybersecurity framework 2.0 (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

National Institute of Standards and Technology. (2024b). Module-lattice-based key-encapsulation mechanism standard (FIPS Publication 203). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203

National Institute of Standards and Technology. (2024c). Module-lattice-based digital signature standard (FIPS Publication 204). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204

National Institute of Standards and Technology. (2024d). Stateless hash-based digital signature standard (FIPS Publication 205). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.205

Newman, M., ve Satzinger, K. (2024). Making quantum error correction work. Google Research Blog.

Nielsen, M. A., ve Chuang, I. L. (2010). Quantum computation and quantum information (10th anniversary ed.). Cambridge University Press. https://doi.org/10.1017/CBO9780511976667

Nikolopoulos, G. M., ve Alber, G. (2004). Robustness of the BB84 quantum key distribution protocol against general coherent attacks. Physical Review A, 69(3), 032331.

NIST. (2024). NIST releases first 3 finalized post-quantum encryption standards.

Numata, K. (2024, Nisan 19). Quantum bits, gates, and circuits. IBM Quantum Learning. https://quantum.cloud.ibm.com/learning/en/courses/utility-scale-quantum-computing/bits-gates-and-circuits

O'Brien, J. L., Furusawa, A., ve Vučković, J. (2009). Photonic quantum technologies. Nature Photonics.

Pan, J.-W., Chen, Y.-A., Liu, W.-Y., Zhang, W., Liang, H., Hu, J., ve Peng, C.-Z. (2020). Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature, 582, 501–505. https://doi.org/10.1038/s41586-020-2401-y

Peikert, C. (2016). A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science, 10(4), 283–424. https://doi.org/10.1561/0400000074

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shamsul Shaari, J., Tomamichel, M., Vallone, G., Villoresi, P., Wallden, P., ve Usenko, V. C. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236. https://doi.org/10.1364/AOP.361502

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Ottaviani, C., ve … (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012–1236.

Pirandola, S., Laurenza, R., Ottaviani, C. ve Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. Nature Communications, 8, 15043.

Pompili, M., vd. (2021). Realization of a multinode quantum network of remote solid-state qubits. Science, 372(6539), 259-264.

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, Article 79. https://doi.org/10.22331/q-2018-08-06-79

Qi, B., Fung, C.-H. F., Lo, H.-K. ve Ma, X. (2007). Time-shift attack in practical quantum cryptosystems. Quantum Information and Computation, 7(1-2), 73-82.

Ren, J.-G., vd. (2017). Ground-to-satellite quantum teleportation. Nature, 549, 70-73.

Renner, R., ve Wolf, R. (2023). Quantum advantage in cryptography. AIAA Journal, 61(5), 1895–1910. https://doi.org/10.2514/1.J062267

Rieffel, E. G., ve Polak, W. (2011). Quantum computing: A gentle introduction. MIT Press.

Rivest, R. L., Shamir, A., ve Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126. https://doi.org/10.1145/359340.359342

Roetteler, M., Naehrig, M., Svore, K. M., ve Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. In T. Takagi ve T. Peyrin (Eds.), Advances in Cryptology: ASIACRYPT 2017 (Lecture Notes in Computer Science, Vol. 10625, pp. 241–270). Springer. https://doi.org/10.1007/978-3-319-70697-9_9

Rowe, M. A., Kielpinski, D., Meyer, V., Sackett, C. A., Itano, W. M., Monroe, C., ve Wineland, D. J. (2001). Experimental violation of a Bell's inequality with efficient detection. Nature, 409, 791–794. https://doi.org/10.1038/35057215

Sangouard, N., Simon, C., de Riedmatten, H., ve Gisin, N. (2011). Quantum repeaters based on atomic ensembles and linear optics. Reviews of Modern Physics, 83(1), 33-80. https://doi.org/10.1103/RevModPhys.83.33

Sano, Y., Matsumoto, R., ve Uyematsu, T. (2010). Secure key rate of the BB84 protocol using finite sample bits. Journal of Physics A: Mathematical and Theoretical, 43(49), 495301.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., ve Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301

Scrivano, A. (2025). A comparative study of classical and post-quantum cryptographic algorithms in the era of quantum computing. arXiv. https://arxiv.org/abs/2508.00832

Sedra, A. S., ve Smith, K. C. (2020). Microelectronic circuits (8. baskı). Oxford University Press.

Shannon, C. E. (1948). A Mathematical Theory of Communication. Bell System Technical Journal, 27(3), 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

Shannon, C. E. (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS '94) (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

Shor, P. W., ve Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters, 85(2), 441–444. https://doi.org/10.1103/PhysRevLett.85.441

Si, H., Liu, H., ve Ma, H. (2018). Optical fiber communication network eavesdropping and defensive measures. In Advances in Social Science, Education and Humanities Research (Vol. 130, pp. 307–310). Atlantis Press. https://doi.org/10.2991/ifmeita-17.2018.53

Simon, D. R. (1997). On the power of quantum computation. SIAM Journal on Computing, 26(5), 1474–1483. https://doi.org/10.1137/S0097539796298637

Spurny, V., Munster, P., Tomasov, A., Horvath, T., ve Skaljo, E. (2022). Physical layer components security risks in optical fiber infrastructures. Sensors, 22(2), 588. https://doi.org/10.3390/s22020588

Stebila, D., ve Mosca, M. (2016). Post-quantum key exchange for the Internet and the Open Quantum Safe project. In R. Avanzi ve H. Heys (Eds.), Selected Areas in Cryptography: SAC 2016 (Lecture Notes in Computer Science, Vol. 10532, pp. 14–37). Springer. https://doi.org/10.1007/978-3-319-69453-5_2

Strobel, T., Vyvlecka, M., Neureuther, I., Bauer, T., Schäfer, M., Kazmaier, S., Sharma, N. L., Joos, R., Weber, J. H., Nawrath, C., Nie, W., Bhayani, G., Hopfmann, C., Becher, C., Michler, P., ve Portalupi, S. L. (2025). Telecom-wavelength quantum teleportation using frequency-converted photons from remote quantum dots. Nature Communications, 16, 10027. https://doi.org/10.1038/s41467-025-65912-8

Tanenbaum, A. S., ve Austin, T. (2013). Structured computer organization (6. baskı). Pearson.

The Week. (2026, March). Undersea cables: The invisible battlefield of global geopolitics.

Toyran, M. (2006). Optik ağlarda kuantum kriptografi kullanarak güvenli iletişim. 4. Eleco Uluslararası Elektrik ve Elektronik Mühendisliği Sempozyumu.

Tsirelson, B. S. (1980). Quantum generalizations of Bell's inequality. Letters in Mathematical Physics, 4(2), 93–100. https://doi.org/10.1007/BF00417500

TÜBİTAK BİLGEM. (2023). Ulusal kuantum teknolojileri strateji ve eylem planı 2023-2030. Ankara: TÜBİTAK.

U.S. Congress. (2018). NIST Small Business Cybersecurity Act (Public Law 115-236). https://www.congress.gov/115/plaws/publ236/PLAW-115publ236.htm

U.S. House of Representatives. (2024). 15 U.S.C. § 271: Findings and purposes. United States Code. https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title15-section271

Vernam, G. S. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. Journal of the American Institute of Electrical Engineers, 45, 109–115.

Waks, E., Zeevi, A., ve Yamamoto, Y. (2002). Security of quantum key distribution with entangled photons. Physical Review A, 65(5), 052310.

Watanabe, S., Matsumoto, R., ve Uyematsu, T. (2006). Noise tolerance of the BB84 protocol with random privacy amplification. International Journal of Quantum Information, 4(6), 935–946.

Wehner, S., Elkouss, D. ve Hanson, R. (2018). Quantum internet: A vision for the road ahead. Science, 362(6412), eaam9288.

Weihs, G., Jennewein, T., Simon, C., Weinfurter, H., ve Zeilinger, A. (1998). Violation of Bell's inequality under strict Einstein locality conditions. Physical Review Letters, 81(23), 5039–5043. https://doi.org/10.1103/PhysRevLett.81.5039

Weste, N. H. E., ve Harris, D. M. (2015). CMOS VLSI design: A circuits and systems perspective (4. baskı). Addison-Wesley.

Wilde, M. M. (2013). Quantum information theory. Cambridge University Press.

Wilde, M. M. (2017). Quantum information theory (2. baskı). Cambridge University Press.

Wolontek. (2025). What is an SFP module? Comprehensive guide including fiber optic connector classification.

Wootters, W. K., ve Zurek, W. H. (1982). A single quantum cannot be cloned. Nature, 299(5886), 802–803. https://doi.org/10.1038/299802a0

Xu, F., Ma, X., Zhang, Q., Lo, H.-K. ve Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. Reviews of Modern Physics, 92(2), 025002.

Xu, F., Qi, B., ve Lo, H.-K. (2010). Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. New Journal of Physics, 12(11), 113026.

Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., ve Pan, J.-W. (2017). Satellite-based entanglement distribution over 1200 kilometers. Science, 356(6343), 1140–1144. https://doi.org/10.1126/science.aan3512