Makale Türü: Araştırma Makalesi
Makale Gönderilme Tarihi: 21.10.2024
Kabul Tarihi: 9.12.2024

-

Kuantum Anahtar Dağıtım Protokolleri ve Saldırı Yöntemleri

Quantum Key Distribution Protocols and Attack Methods

Derin Akata

derinakata@gmail.com

0009-0007-1907-6733

Özet

Kriptografi, modern dünyada güvenli iletişim için hayati öneme haizdir. Son yıllardaki teknolojik gelişmeler, günümüz kriptografisini tehdit edebilecek kuantum bilgisayarların yakın gelecekte ortaya çıkabileceğini gösterdi. Bu durumda geleneksel kriptografi metotları güvenli iletişimi sağlamada yeterli olamayacağından, Kuantum Sonrası Kriptografi (KSK) algoritmaları ve Kuantum Anahtar Dağıtım (KAD) sistemleri gibi çözümler öne çıkmaktadır. KAD sistemlerinin güvenliği, geleneksel kriptografik metotların aksine doğa yasalarına dayandığından, teoride tamamen güvenli olsa da teknolojik yetersizlikler nedeniyle pratikte henüz tamamen güvenli değil.

Bu derlemede, KAD sistemlerinin güvenliğini tehdit eden saldırı yöntemlerine kapsamlı bir bakış sunulurken, kriptografinin tarihi, KSK algoritmaları, kuantum mekaniği, KAD protokolleri ve uygulama alanları da incelenmiştir.

Anahtar Kelimeler: *Kuantum, Anahtar Dağıtımı, KAD, Saldırı, Hacking, BB84, B92, E91, SARG04, Kriptografi, Kriptoloji*

Abstract

Cryptography has always been a sensitive topic, but in the modern world, it has become crucial for secure communication. Recent technological advancements indicate that quantum computers, which could undermine today's cryptographic methods, may emerge in the near future. In this case, traditional cryptographic methods may not be sufficient to ensure secure communication, bringing Post-Quantum Cryptography (PQC) algorithms and Quantum Key Distribution (QKD) systems to the forefront. The security of QKD systems is guaranteed by the laws of nature, rather than traditional cryptographic methods. However, while QKD is theoretically completely secure, current technological limitations mean these systems are not yet completely secure in practice.

In this paper, I present a comprehensive literature review and comparative study on QKD hacking strategies while also discussing the history of cryptography, PQC algorithms, quantum mechanics, QKD protocols, and their application areas.

Keywords: *Quantum, Key Distribution, QKD, Attack, Hacking, BB84, B92, E91, SARG04, Cryptography, Cryptology*

1 Giriş-Modern Kriptoloji ve Tehditler

Binlerce yıldır krallar, kraliçeler, generaller ülkelerini ve ordularını yönetmek için iletişimin gücüne güvendi. Bilginin güvenliği bazen bir savaşın sonucunun değişmesine, bazen de bir kraliçenin ölümüne yol açtı. Bilginin saklanırken, iletilirken sadece istenilen kişiler tarafından doğru olarak okunabilmesini sağlama isteği insanlık tarihi kadar eskiye dayanır. Kriptografi, bu isteğin hayata geçirilebilmesini sağlayan sanat ve bilim olarak literatürde yerini aldı[1]. Etimolojik olarak Yunanca krypto's (saklı) ve lo'gos (kelime) kelimelerinin birleştirilmesinden meydana gelen bu sözcük bugün bizlere bilgi çağının kapılarını da araladı[2]. İlk kriptografik teknikler Antik Mısır'da M.Ö 1900'lerde kullanılsa da sistematik olarak M.Ö 100'lerde Jul Sezar tarafından bugün kendi ismiyle anılan harf veya sayıların yer değiştirmesine dayanan şifreleme yöntemiyle yaygınlaştı.

Bilgisayarların icadı ve iletişim ağılarının yaygınlaşmasıyla birlikte kriptografi hayatımızın her alanında yerini aldı. 1970'li yılların başı itibariyle IBM tarafından geliştirilen Data Encryption Standard (DES), ardından 1976'da Diffie–Hellman Anahtar Değişim Algoritması ve 1977'de ortaya çıkan RSA (Rivest–Shamir–Adleman) algoritmasıyla beraber modern kriptografi tarihinde büyük bir atılım gerçekleşti.

Günümüzde kullanılan RSA gibi asimetrik kriptografi algoritmaları yüksek basamaklı asal sayıların çarpanlarına ayrılmasındaki zorluktan ileri gelmektedir. Peter Shor tarafından 1994 yılında yayınlanan ve bugün adıyla anılan Shor Algoritması[3]bizlere asal sayıların çok daha kısa sürede çarpanlarına ayrılabileceğini gösterdi. Bununla birlikte Lov Grover tarafından 1996 yılında yayınlanan makale[4] veritabanı aramalarının kuantum mekaniği sayesinde çok daha hızlı yapılabileceği fark ettirmiştir. Her ne kadar bu algoritmalar, şifreleme algoritmalarının çok hızlı olarak kırılabileceğinin mümkün olduğunu gösterse de kuantum bilgisayarların henüz istenilen yüksek işlem gücü seviyesinde olmamasından dolayı verimli olarak çalışamamaktadırlar. 2023 yılı itibariyle araştırmacılar Shor algoritmasının çok daha az kubit (372) ile çalıştırılabileceğini iddia [5]etmişlerse de Google araştırmacıları tarafından bu durum yalanlanmıştır[6]. Yine de Shor ve Grover algoritmalarıyla beraber açık anahtar

şifrelemesi için geri sayım başladığı yadsınamaz bir gerçektir

1990'lı yılların ortalarıyla beraber hızlanan kuantum bilgisayar geliştirme çalışmaları farklı ticari şirketler ve ülkeler tarafından desteklenmiş, 2019 yılı itibariyle 16 kubitlik dünyanın ilk ticari kuantum bilgisayarı IBM Q System One tanıtılmıştır. Aynı yıl içerisinde Google Yapay Zekâ Departmanı "Sycamore" adında 53 kubitten oluşan yarı iletken tabanlı kuantum işlemciyi tanıttı ve ilk kuantum üstünlüğüne ulaşan bilgisayar oldu[7]. 2020 Aralık itibariyle Çin Bilim ve Teknoloji Üniversitesi'nden (USTC) bir ekip tarafından kuantum üstünlüğüne ulaşan ilk foton tabanlı kuantum bilgisayar geliştirildi[8].

1.1 Kuantum Sonrası Kriptografi

K-Gününün çok da uzak olmadığını düşünen araştırmacılar tarafından 2006 yılında Post Quantum Crypto (PQCrypto) konferanslarıyla AB destekli olarak başlayan Kuantum Sonrası Kriptografi çalışmaları 2013 yılında "Quantum-Safe Cryptography" atölyeleri ve 2015 yılında Amerikan Standartları Enstitüsü (NIST) tarafından düzenlenen ve 140'tan fazla katılımcının dahil olduğu "Cybersecurity in a Post-Quantum World" atölyesi ile ivmelendi.

2016 yılı itibariyle NIST tarafından NISTIR 8105 dokümanının yayınlanması[9] ile Kuantum sonrası kriptografi çalışmalarında standardizasyon için çalışmalar hızlandı. Dokümanda NIST simetrik şifreleme algoritmalarının halen güvenli olduğunu; ancak yüksek bitlerde şifreleme yapılması gerektiğini, asimetrik ve e-imza algoritmalarının ise K-Günü sonrası güvenliğini yitireceğini açıkladı. Bu algoritmalar yerine geçebilecek Kafes Tabanlı Kriptografi, Kod Tabanlı Kriptografi, Çok değişkenli Kriptografi, Hash Tabanlı İmzalar ve diğerleri olmak üzere 5 ana grup belirledi.

Tablo 1-1 Algoritma Karşılaştırmaları

Kriptografik Algoritma	Tipi	Amaç	Geniş Ölçekli Kuantum Bilgisayarın Etkisi
AES	Simetrik Anahtar	Şifreleme	Daha Uzun Anahtar Boyutları Gerekli
SHA-2, SHA-3		Hash Fonksiyonları	Daha Uzun Çıktılar Gerekli
RSA	Açık Anahtar	İmzalar, Anahtar Değişimi	Güvenli Değil
ECDSA, ECDH (Eliptik Eğri)	Açık Anahtar	İmzalar, Anahtar Değişimi	Güvenli Değil
DSA (Finite Field)	Açık Anahtar	İmzalar, Anahtar Değişimi	Güvenli Değil

2016 yılı sonunda açık anahtar ve e-imza kategorilerinde KSK algoritmaları için NIST'in yayınladığı çağrıya[10] tüm dünyadan başvurular yapıldı. Çağrı kapanışı olan 2017 itibariyle toplam 82 aday başvuru yaptı ve bunlardan 69'u minimum gereklilikleri sağlayarak değerlendirmeye alındı.

2018 yılında NIST ilk KSK Standardizasyon konferansını PQCrypto ile beraber düzenledi, konferansta yarışmadaki algoritmalar için görüşmeler sağlandı. Tablo 1-2'de görüldüğü üzere 2019 yılında bu adaylardan 17'si açık anahtar ve 9'u e-imza algoritmaları olmak üzere toplam 26 aday algoritma ikinci tura geçmeye hak kazandı[11].

Tablo 1-2 PQC 1. Tur Kazananları

Algoritma Tipi	Açık Anahtar	E-İmza	Toplam
Kafes tabanlı	9	3	12
Kod Tabanlı	7	-	7
Çok değişkenli	-	4	4
Hash Tabanlı	-	1	1
Diğer	1	1	2
Toplam	17	9	26

2020 yılında ikinci tur sonuçları IR 8309 dokümanı ile açıklanarak 4 açık anahtar, 3 e-imza algoritması asil; 5 açık anahtar ve 3 e-imza algoritması da yedek adaylar olarak belirlendi[12].

Tablo 1-3PQC 3. Tur Seçilenler

ASİL		YEDEK	
Açık Anahtar Şifrelemesi	Dijital İmzalar	Açık Anahtar Şifrelemesi	Dijital İmzalar
Classic McEliece	CRYSTALS/DILITHIUM	BIKE	GeMSS
CRYSTALS-KYBER	FALCON	FrodoKEM	Picnic
NTRU	Rainbow	HQC	SPHINCS+
SABER		NTRU Prime	
		SIKE	

2022 yılıyla beraber üçüncü tur, final sonuçları açıklanarak KSK için algoritma belirleme süreci tamamlandı[13]. Kazanan algoritmaların standardizasyon prosedürleri için çalışmalar halen devam etmektedir.

Tablo 1-4PQC Final Seçilen Algoritmalar

Açık Anahtar Şifrelemesi	Dijital İmzalar
CRYSTALS-KYBER (Kafes Tabanlı)	CRYSTALS-DILITHIUM
	FALCON
	SPHINCS+

2 Kuantum Mekaniği

2.1 Heisenberg Belirsizlik İlkesi

İlk olarak 1927'de Alman fizikçi Werner Heisenberg tarafından ortaya atılan Heisenberg Belirsizlik ilkesine göre aynı anda bir çift eşlenik özellikten biri tam olarak bilenebilir[14]. Başlangıçta bir parçacığın konumu ve momentumundan bahseden Heisenberg, bir parçacığın konumunun ölçümünün, onun eşlenik özelliği olan momentumu bozacağını açıklamıştır. Bu nedenle, her iki özelliği aynı anda kesin olarak bilmek imkansızdır. Kuantum kriptografisinde de bu ilkeden yararlanır; ancak genellikle söz konusu eşlenik özellikler olarak fotonların farklı durumlardaki

polarizasyonunu kullanır.

2.2 No-Cloning Teorem

BB84 protokolünün omurgasını oluşturan teoremdir ve Heisenberg belirsizlik ilkesine dayanır. Klonlanamama ilkesi, bilinmeyen bir kuantum durumu verildiğinde bu durumun kopyalarını üretmenin hiçbir yolu olmadığını belirten kuantum mekaniğinin temel bir özelliğidir. Wootters, Zurek ve Dieks[15] tarafından 1982 yılında keşfedilmiş ve duyurulmuştur. Kuantum hesaplama ve ilgili alanlarda derin etkileri olmuştur. Bu aynı zamanda kuantum durumlarında kodlanmış bilgilerin esasen benzersiz olduğu anlamına gelir.

2.3 Kuantum Dolanıklılık

Kuantum mekaniğine göre birbirlerine yeterli yakınlıkta duran 2 kuantum parçacığı (örn. elektron veya foton) arasında bir bağ oluşmaktadır. Bu bağ dolanıklılık/dolaşıklılık olarak isimlendirilmektedir. Dolanık durumdaki foton veya elektron için uzaklık fark etmeksizin durum ölçümü yaptığımızda diğer foton veya elektron da ilk olarak ölçüm yapılan foton veya elektronun tersi duruma sahip olacaktır. Bu teori Schrödinger tarafından bir düşünce deneyi olan "Schrödinger'in kedisi" olarak gündeme gelmiş, 1930'larda fizikçiler tarafından ortaya atılmıştır. 1935 yılında A. Einstein, B. Podolsky, N. Rosen tarafından EPR paradoksu[16] olarak ortaya çıkartılmış; ancak bu etki gizli bir değişkenin varlığıyla açıklanmaya çalışılmıştı. Schrödinger'in makalesiyle [17] gizli bir değişkenin olmadığı belirtilmiş, bundan etkilenen John Stewart Bell tarafından 1964 yılında Bell teoremi ile düşünce deneyi olarak güçlenmiştir[18]. Stuart Freedman ve John Clauser'in 1972 yılında yaptığı deneyle[19] Bell Eşitsizliğinin fiziksel gösterimi gerçekleşmiştir. İlk hataya yer bırakmayan (loophole-free) test, 2015 yılında TU Delft'te yapıldı ve Bell eşitsizliğinin ihlal edildiğini doğruladı[20]. İlk ticari kuantum bilgisayarı olan IBM Q System One'da da kuantum dolanıklılık ilkesi kullanılarak geliştirmeler yapıldı. Kuantum kriptografide de kuantum dolanıklılıktan yararlanan E91, BBM92 gibi protokoller ortaya çıkmıştır.

3 Bit ve Kubit Kavramı

Klasik bilgisayar işlemcileri transistor adı verilen ve üzerinden akım geçişine göre açık/kapalı olarak anahtarlama yapabilen yarı iletken devre elemanlarından oluşur. Shockley ve arkadaşlarının 1947 yılında transistörün icadından ve ilk transistör bilgisayarı TRADIC'den bu yana transistör boyutlarında çok büyük değişimler yaşanmıştır. 1954 yılında ilk ortaya çıkışında 3 küp feet boyutlarında olan transistörler Apple'ın 2023 yılında M3 işlemcisini[21] duyurmasıyla beraber 3 nm boyutlarına kadar indirilmiştir.

Intel şirketinin kurucu ortağı Gordon Earle Moore tarafından 1965 yılında *"Electronics Magazine*" dergisindeki makalesinde belirttiği[22] ve bugün Moore Yasası olarak bilinen gözleme dayalı tahminde her 18 ayda bir tümleşik devre üzerine yerleştirilebilecek bileşen sayısının iki katına çıkarken üretim maliyetlerinin aynı kalacağını, hatta düşme eğiliminde olacağını, bu sayede işlem kapasitelerinde çok yüksek artışlar yaşanacağını belirtmiştir. Ancak günümüzde 5nm boyutlarına indirilen transistor boyutlarında fiziğin sınırlarına ulaşılmış, atomik boyutlara inildikçe kuantum dünyasının yasaları ve zorluklarıyla başa çıkmak güçleşmiştir. Her ne kadar elektronik endüstrisinin 2025 planları arasında 2 nm'ye kadar küçültme planları olsa da belirli bir boyut altında yaşanan sorunlar (soğutma, kablo elektrik alanı vb.) nedeniyle limitlere ulaşılmak üzeredir.

20. yüzyılın ortalarındaki gelişmelerle daha iyi anlaşılmaya başlanan kuantum mekaniği, 1960'ların sonunda Stephen Wiesner "Conjugate Coding" makalesini yazışıyla [23] fotonların bilgi taşıyabileceği teorisini yani kuantum kodlama ortaya çıktı. Kubit kavramı ise Kuantum Bit olarak [24] 1995 yılında yayınlanan Benjamin Schumacher'in makalesinde ilk kez yerini almış, bir şakalaşma sırasında William Wootters'ten duyduğunu belirtmiştir.

Kuantum bilgi teorisinde, verinin iletilmesi için gerekli en küçük birime kübit (kuantum biti) denir. Kübit($|\Psi\rangle$)iki boyutlu Hilbert uzayında ortonormal taban vektörlerinin doğrusal süperpozisyonu olarak bra$\langle|$, ket$|\rangle$ notasyonuyla[25] ifade edilir.

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$= \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha\\0\end{pmatrix} + \begin{pmatrix}0\\b\end{pmatrix} = \begin{pmatrix}\alpha\\b\end{pmatrix}$$
$$= \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \quad (3.1)$$

$\alpha, \beta \in \mathbb{C}$ olasılık genliklerini

$$|\alpha|^2 + |\beta|^2 = 1 \quad (3.2)$$
$$P_{0\rangle} = |\alpha|^2 = a^* * a \quad (3.3)$$
$$P_{1\rangle} = |\beta|^2 = b^* * b \quad (3.4)$$

ifade etmektedir. Kübitin klasik sistemdeki bitten temel farkı; bitin belirli bir 0 veya 1 değerine sahip olması, kübitin ise ölçüm yapılana dek durumunun belirsiz olmasıdır. Ölçümle beraber kübit durumu ($|\Psi\rangle$), taban vektör durumlarından $|0\rangle$, $|1\rangle$ birine "çöker". Kübit durumu yarıçapı 1 olan Şekil 3-1'de gösterilen Bloch küresinde tasvir edilmektedir $\theta \in (0,\pi)$, $\phi \in (0,2\pi)$. Kübit durumu,

$$\theta = 0\,,\pi \quad (3.5)$$

iken Z tabanında kutup bölgelerindedir.

$$\theta = \frac{\pi}{2} \quad (3.6)$$

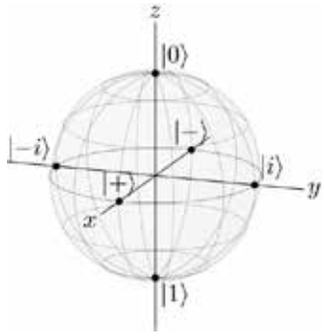
olduğunda kübit, ekvator bölgesinde olmakla birlikte

$$\phi = 0,\pi \quad (3.7)$$

için X tabanında,

$$\phi = \frac{\pi}{2}\,,\frac{3\pi}{2} \quad (3.8)$$

için Y tabanındadır. Aşağıda özel durumlar detaylı olarak tanımlanmıştır.



Şekil 3-1Bloch Küresindeki Özel Durumlar[26]

$|0\rangle$ ve $|1\rangle$ durumları iki boyutlu Hilbert uzayında Pauli operatörünün Z tabanındaki öz durumlarıdır.

$$\theta = 0: |0\rangle \equiv \begin{matrix}1\\0\end{matrix} \quad (3.9)$$

$$\theta = \pi: |1\rangle \equiv \begin{matrix}0\\1\end{matrix} \quad (3.10)$$

$$\sigma_z = Z = \begin{matrix}1 & 0\\0 & -1\end{matrix} \quad (3.11)$$

$|+\rangle$ ve $|-\rangle$ durumları iki boyutlu Hilbert uzayında Pauli operatörünün X tabanındaki öz durumlarıdır.

$$\phi = 0: |+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad (3.12)$$

$$\phi = \pi: |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \quad (3.13)$$

$$\sigma_x = X = \begin{matrix}0 & 1\\1 & 0\end{matrix} \quad (3.14)$$

$|+i\rangle$ ve $|-i\rangle$ durumları iki boyutlu Hilbert uzayında Pauli operatörünün Y tabanındaki öz durumlarıdır.

$$\phi = \frac{\pi}{2}: |+i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle \quad (3.15)$$

$$\phi = \frac{3\pi}{2}: |-i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle \quad (3.16)$$

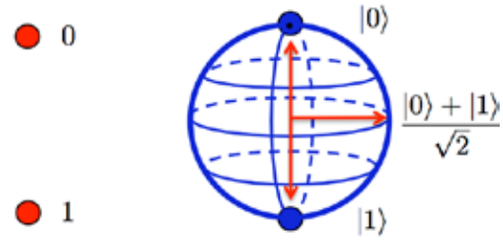
$$\sigma_y = Y = \begin{matrix}0 & -i\\i & 0\end{matrix} \quad (3.17)$$

Ortogonal tabanda d boyutlu Hilbert uzayında bir fi durumunun psi durumunda olma ihtimali herhangi bir i, j için aşağıdaki gibi tanımlanır.

$$P = |\langle\Psi_i|\phi_j\rangle|^2 = \langle\Psi_i|\phi_j\rangle\langle\Psi_i|\phi_j\rangle^*$$
$$= \langle\Psi_i|\phi_j\rangle\langle\phi_j|\Psi_i\rangle = \frac{1}{d} \quad (3.18)$$

Örneğin $|+\rangle$ durumunun $|0\rangle$ 'da olma ihtimali aşağıdaki gibi gösterilmektedir.

$$|\langle 0|+\rangle|^2 = \langle 0|+\rangle\langle 0|+\rangle^*$$
$$= \langle 0|+\rangle\langle +|0\rangle$$
$$= \left((1 \quad 0)\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix}\right)\left(\left(\frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}}\right)\begin{pmatrix}1\\0\end{pmatrix}\right)$$
$$= \left(\frac{1}{\sqrt{2}} + 0\right)\left(\frac{1}{\sqrt{2}} + 0\right) = \frac{1}{2} \quad (3.19)$$

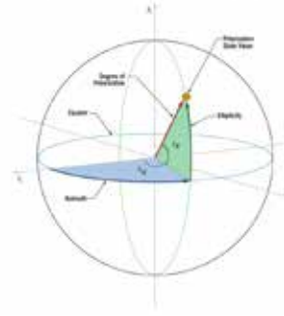


Şekil 3-2 Bit-Kübit Gösterimi

Bir kübit durumunun fiziksel anlamı fotonun elektromanyetik alanın salınım yönü yani polarizasyon durumuyla ilişkilendirilebilir. Bu noktada Bloch küresi Şekil 3-3,4'te görünen Poincaré küresine evrilmekle beraber herhangi bir anlam değişikliğine uğramaz. Yalnızca Poincaré küresinin kutuplarındaki (Z tabanı) taban vektörleri yatay $|H\rangle = |0\rangle$ ve dikey $|V\rangle = |1\rangle$ olarak doğrusal polarizasyonla, X tabanındaki taban durumları diyagonal $|D\rangle = |+\rangle$ ve anti diyagonal $|A\rangle = |-\rangle$ olarak yine doğrusal polarizasyonla ilişkilendirilirken, Y tabanındaki taban durumları dairesel polarizasyonla $|R\rangle = |+i\rangle$, $|L\rangle = |-i\rangle$ ilişkilendirilmektedir. Poincaré küresinin içinde kalan diğer tüm durumlar eliptik polarizasyon ile açıklanmakta, θ ve ϕ parametreleri kullanılarak gösterilmekte, elektromanyetik faz ϕ ile tanımlanmaktadır.

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \quad (3.20)$$

Şekil 3-3Poincaré Küresi 1[27]



Şekil 3-4Poincaré Küresi 2[27]

Günümüzde genellikle bilgi, kübitin polarizasyon, faz ve zaman durumlarına kodlanabilmektedir.

Polarizasyon kodlamalı sistemlerde polarize foton hazırlama işlemi çoklu lazer kaynakları veya elektrooptik modülatörlerle sağlanırken, polarizasyon ölçümü ise aşağıdaki Bölüm 6.3'te bahsedildiği üzere polarize ışın ayrıştırıcılar

(PBS) veya elektrooptik modülatörlerin kullanıldığı alıcı sistemleri tarafından gerçekleştirilmektedir.

Faz kodlamalı sistemlerde kübit ortogonal olmayan durumlarda hazırlanabilmekte, bu için işlem için Mach-Zehnder interferometresi (MZI) kullanılmaktadır. Şekil 3-5'te görüldüğü üzere kaynaktan çıkan fotonlar ışın ayrıştırıcıda (BS) bölündükten sonra 2 farklı koldan alıcıya gönderilmektedir. Verici bölünmüş foton demetinin bir koluna faz modülatörü aracığıyla kodlama işlemi yapmaktadır. Diğer koldaki demete ise Alıcı tarafında faz modülasyon işlemi uygulanmakta, bölünmüş fotonlar alıcının BS'sine aynı anda sokularak Hong-Ou-Mandel etkisinin oluşması beklenmektedir. Eğer kollar arasındaki faz farkı 0 veya π ise girişim oluşmakta ve BS çıkışında beraber hareket etmekte, aksi halde girişim gözlenmemekte, fotonlar ayrı ayrı hareket etmektedir; ancak sistemin tamamını MZI'ye dönüştürerek 2 koldan iletim gerektiğinden çok pratik bir yaklaşım değildir.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi_{A-B}}|1\rangle\right) \tag{3.21}$$

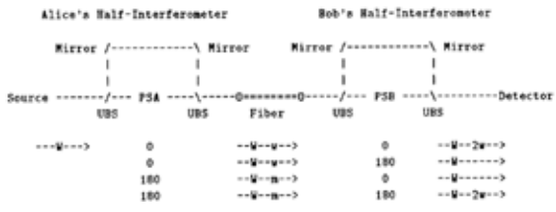
Şekil 3-5Faz Kodlamalı Sistem Örneği [28]

Zaman - Faz kodlamalı sistemlerde ise faz kodlamaya ek olarak kullanılan ayarsız Mach-Zehnder interferometreleriyle (MZI) demetler arasında mesafe kaynaklı zaman farkı yaratılmaktadır. Şekil 3-6'da görüldüğü üzere vericinin ayarısız MZI'sinde bir koldaki demete faz modülasyonu uygulanırken, diğer kolda fotonlar doğrudan gönderilir. Uzun ve kısa kol nedeniyle zaman farkına sahip fotonlar alıcıda ters kollardan ayarsız MZI'ye sokulur. Alıcı faz modülasyonu uygulanmamış demete uyguladığı faz modülasyonu sonrası demetler BS'de aynı anda karşılaşır. Fotonlar arası faz farkı

$$\phi = \phi_A - \phi_B = 0 \; veya \; \pi \tag{3.22}$$

ise Hong-Ou-Mandel etkisiyle girişim oluşmakta ve BS çıkışında beraber hareket etmekte, aksi halde girişim gözlenmemektedir. Sistemin en büyük avantajı zaman farkları nedeniyle tek kanal üzerinden iletim sağlanabilmesidir. Bölüm 9.2'de detaylı bahsedildiği üzere günümüzde çift yönlü iletişimin olduğu "Tak ve Çalıştır" sistemler de faz-zaman kodlamasıyla çalışmaktadır.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|e\rangle + e^{i\phi_{A-B}}|l\rangle\right) \tag{3.23}$$



Şekil 3-6Zaman- Faz Kodlamalı Sistem Örneği [28]

4 Kuantum Anahtar Dağıtımı

Wiesner'in makalesi 1960'ların sonunda zamanının ötesinde olmasına karşın çoğunlukça fark edilmedi ve reddedildi. Makale, foton polarizasyonlarının kullanılarak mesaj iletimi, kuantum banknot gibi kavramları içeriyordu. 1981'de Rabin, "habersiz transfer tekniği" adı altında kriptografik bir teknik yayınlayarak aslında yeniden icat etmiş oldu[29]. Wiesner'in makalesi ise 1983'te SIGACT News'de yayınlandı.

Ardından fotonların anahtar dağıtımında kullanılabileceğinin anlaşılmasıyla çalışabilecek sistemlerin tasarlanabileceği anlaşıldı. 1984 yılı itibariyle BB84 adıyla ilk kuantum anahtar dağıtım protokolü ortaya çıktı. BB84 ile başlayan süreç bu makalede de birkaçının incelendiği üzere E91[30], B92[28], BBM92[31], SARG04[32], Altılı Durum[33], Ölçüm Cihaz Bağımsız KAD gibi birçok protokolün yayınlanmasını beraberinde getirdi. Günümüzde halen farklı protokoller ortaya çıkmaktadır.

Günümüzde KAD sistemleri Ayrık Değişkenli ve Sürekli Değişkenli olmak üzere 2 kategoride incelenebilir. Ayrık değişkenli sistemlerde bilgi, 2 boyutlu kompleks vektör uzayında kübite kodlanarak iletilmektedir. Bu çalışmada incelenmeyecek olsa da Sürekli Değişkenli sistemlerde bilgi >2 boyutlu kompleks vektör uzayında küditlere kodlanır. Ölçüm işlemi genellikle homodin dedektörler ile sağlanmaktadır. Küdit bazlı sistemler çok daha yüksek hızlarda işlem yapabilmeye olanak sağlasa da (kübit=(2^k) küdit=(>2^k)) stabilite sorunları henüz aşılamamıştır, çalışmalar devam etmektedir. Detaylı bilgi [34]için makalesi incelenebilir.

Kuantum ağlar ve internet kuantum internetin geleceğiyle ilgili [35-39]makaleleri incelenebilir.

4.1 Hazırla ve Ölç Protokolleri

4.1.1 Kuantum Kriptografinin Doğuşu ve BB84

Protokol, Bell Laboratuvarlarında C. H. Bennett ve G. Brassard ikilisi tarafından Wiesner ile tanışmaları sonrası 1984 yılında bir konferansta foton polarizasyonlarını kullanarak kriptolama yapılabileceği üzerine çıkan makaleyle öne sürüldü[40]. Makaledeki fikir, gizli anahtarın her bir kübitin tek fotonun polarizasyon durumuna kodlamak üzerinedir. Tek fotonun polarizasyon durumu no-cloning teoremde de anlatıldığı üzere foton yok edilmeden ölçülemediğinden, foton ile iletilen bilgi "kırılgan" olacaktır.

Herhangi bir saldırgan ölçmek/ele geçirmek için tek fotonu yok etmek zorunda kalacak, böylelikle ya kendini ortaya çıkarmış olacak ya da fotonu yeniden üreterek göndermek zorunda kalacaktır. Ancak BB84 protokolünde kullanılan 4'lü polarizasyondan dolayı tekrar üretilen tek foton %50 olasılıkla yanlış bir polarizasyon durumuna sahip olarak gönderileceğinden; bu durum sistemde hata yüzdesinin artışına yol açacak ve saldırgan açığa çıkacaktır.

Tablo 4-1BB84 Kubit Kodlaması

Durum	0	1
Computational veya Z Tabanı +	→	↑

Hadamard veya X Tabanı ×	↗	↘

Protokol, Tablo 4-1'de görüldüğü üzere 4 farklı polarizasyon durumundaki fotonları kübit olarak tanımlamıştır. Z tabandan sadece 0° ve 90° fotonlar değişime uğramadan geçebilirken, X tabandan sadece artı 45° ve 135° dereceli fotonlar değişime uğramadan geçebilmektedir. Farklı polarizasyondaki fotonlar ise tek fotonun bölünememe ilkesi ve kuantum mekaniğinin doğasından dolayı %50 olasılıkla 0 veya 1 olarak ölçülecektir. Unutulmamalıdır ki protokolde tek foton gönderimi kritik önemde olup, aksi durumda farklı saldırı türlerine açıktır.

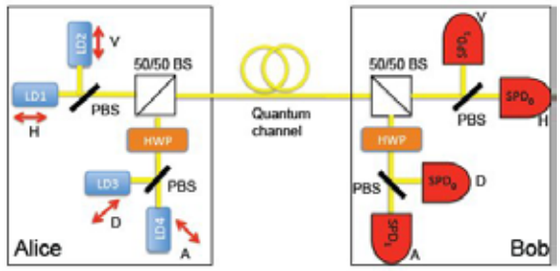
Protokolün adımları şöyle sıralanmıştır;

1. Alice (Verici) tarafından rastgele hazırlanan tek foton rastgele seçilmiş PBS'lerden geçirilerek veya belirli bir voltaja tabi tutularak istenilen 4 ortogonal polarizasyon durumumdan birine getirilir.
2. Ardından fotonlar Bob (Alıcı) tarafına serbest uzay, fiber vb. herhangi bir kanalla gönderilir. Polarize fotonların gönderildiği bu kanal, kuantum kanalı olarak tanımlanmıştır.

Transmitting station bit	0	1	1	0	1	0	0	1
Transmitting station basis	+	+	X	+	X	X	X	+
Polarization	↑	→	↖	↑	↖	↗	↗	→
Receiving station basis	+	X	X	X	+	X	+	+
Receiving measurement	↑	↗	↖	↗	→	↗	→	→
Open channel discussion								
Shared key	0		1			0		1

Şekil 4-1BB84 Protokol Gösterimi[41]

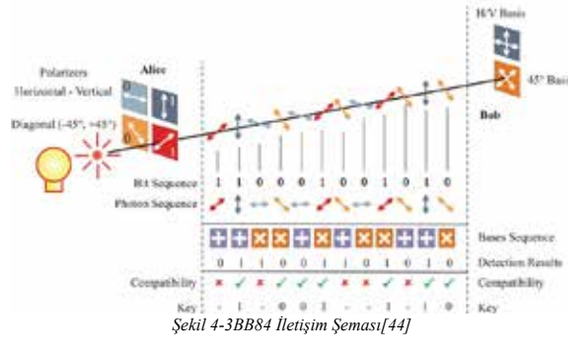
3. Bob fotonları aldıktan sonra Alice'ten bağımsız tamamen rassal olarak seçilmiş Z veya X tabanda tek foton algılayıcısıyla (SPD) polarizasyon ölçümlerini gerçekleştirir.



Şekil 4-2Örnek KAD Sistemi (Pasif Taban Seçimli)[42]

4. Ölçümün ardından Z ve X tabanlar karşılıklı olarak açık (public) herhangi bir kanaldan sırayla karşılaştırılır. Fotonlar sıra ile gönderildiği ve alındığı için Alice ve Bob hangi tabanda ölçüm yaptığını birbirine söyler, yani karşılaştırır.
5. Eğer tabanlar aynı ise fotonun süperpozisyonuna göre belirlenen 0 veya 1 'i anahtar olarak alır. Böylelikle anahtar adım adım oluşmaya başlar. Açık veya gizli kanaldan hiçbir zaman 0 veya 1 olarak anahtar paylaşımı yapılmaz.

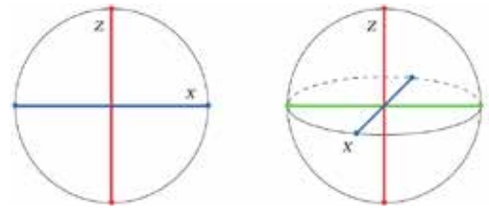
İstenilen anahtar uzunluğuna ulaşılıp, karşılaştırma sonucu anahtar oluşturulduktan ve sistemdeki kuantum bit hata oranı (QBER) hesaplandıktan sonra eğer hata oranı %25'in altında kalıyorsa aynı anahtar ile devam edilerek mesajlaşma başlayabilir; ancak hata payları ve rassallık sorunları dolayısıyla Bölüm 5'de gösterildiği üzere bu oran %11 olarak belirlenmiştir[43].



Şekil 4-3BB84 İletişim Şeması[44]

4.1.2 Altılı Durum Protokolü (SSP)

İlk kez 1998 yılında Dagmar Bruß'un makalesinde[33] görülen altılı durum protokolü Pasquinucci ve Nicolas Gisin tarafından 1999 yılında yayınlanan makalelerinde[45] çalışılarak ortaya çıkmıştır. SSP, BB84 protokolüne yalnızca iki tane daha farklı polarizasyon eklenmesi ve buna bağlı olarak bir PBS daha eklenmesiyle oluşturulmuştur. BB84 ve SSP ölçüm yönleri Şekil 4-4'de gösterilmiştir[46].



Şekil 4-4BB84 ve SSP Ölçüm Yönleri[46]

Altı Durum Protokolü (SSP), BB84'e benzer, ancak iki baz yerine, altı farklı polarizasyon için toplam üç baz kullanır. Böylece saldırgan araya girerek ölçüm yapmak için yanlış filtre kullanma olasılığı %50'den %66'ya çıkmakta olup BB84 protokolüne göre daha güvenlidir. Bu protokolde Tablo 5-1'te görüldüğü üzere tolere edilebilir hata oranı %12,7'dir [43]

4.1.3 SARG04

Bir grup İsviçreli araştırmacı tarafından 2004 yılında [32] BB84 protokolünün PNS ataklarına karşı zayıf olması nedeniyle ortaya sürülen hazırla ve ölç protokollerinden birisidir. BB84'ün aksine tek foton yerine tutarlı zayıf foton darbeleriyle oluşan ikili foton çifti göndermektedir. BB84'teki gibi Alice ölçüm tabanlarını ifşa etmek yerine, bitin kodlanmış olabileceği ortogonal olmayan dört durumdan (d_x) birini duyurur:

$$d_1 = (|1\rangle, |+\rangle), d_2 = (|1\rangle, |-\rangle),$$
$$d_3 = (|0\rangle, |+\rangle) \; ve \; d_4 = (|0\rangle, |-\rangle) \qquad (4.1)$$

Örneğin bit + (Computational veya Z) tabanında 1 olarak gönderilirse Alice ölçüm tabanlarını açıklarken hem 1 + 'yı hem de x (Hadamard veya X) tabanından herhangi bir biti (1 x veya

0 x) açıklar. Bob'da bu sonuçlarla kendi ölçüm sonuçlarını karşılaştırır. Eğer Bob açıklanan polarizasyon çiftinden tamamen farklı bir sonuç elde etmişse farklı tabanda ölçüm yaptığını anlar ve Alice'in açıklamış olduğu diğer tabandaki sonucu anahtar olarak kaydeder.

Tablo 4-2SARG04 Örnek İletişim

ALICE Polarizasyonu	ALICE Açıklanan Polarizasyon		BOB Ölçüm Filtresi	BOB Ölçüm Polarizasyonu	Kabul/Ret
– 1 +	– 1 +	/ 1 x	×	/ 1 x	RET
| 0 +	| 0 +	\ 0 x	+	| 0 +	RET
/ 1 x	/ 1 x	– 1 +	×	/ 1 x	RET
– 1 +	– 1 +	\ 0 x	+	– 1 +	RET
– 1 +	– 1 x	/ 1 x	×	\ 0 +	KABUL

4.2 Dolanıklılık Tabanlı Protokoller

4.2.1 E91

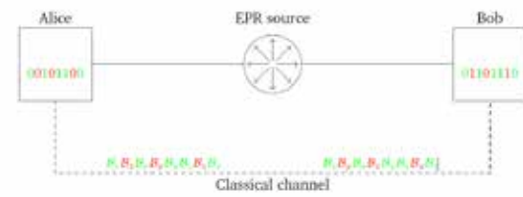
Hazırla ve ölç protokolleri olarak adlandırılan BB84 ve B92 protokollerinden farklı olarak E91, kuantum dolanıklılığa dayalı bir kuantum anahtar dağıtım protokolüdür. 1991 yılında Artur Ekert tarafından önerilmesinden bu yana, mucidinin adı ve yayın yılının birleşiminden almaktadır[30]. E91, diğer adıyla EPR şeması, dolanık foton çiftlerini kullanır ve dolanıklılığın iki temel özelliğine dayanır. Bunlar; foton çiftlerinin mükemmel korelasyonu ve herhangi bir gizli dinleme girişiminin kübiti çökerterek EPR durumunu yok etmesidir. Standart yaklaşım olarak dolanıklılık kaynağı Alice ve Bob'un tam ortasına yerleştirilmektir. Dolanık bir foton çifti oluşturulduğunda, iki parçacık farklı hedeflere (Alice ve Bob) yönlendirilir. Kaynak tarafından oluşturulan dolanık çift matematiksel olarak aşağıdaki gibi temsil edilir. Dolanıklılık özelliği mesafe bağımsız olduğundan, kaynaktan gönderilen kübitlerden biri Alice veya Bob'un herhangi biri tarafından ölçüldüğünde ikinci kübit de kuantum dolanıklılık sebebiyle ilişkili bir sonuç gösterecektir.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01|) + (|10|) \qquad (4.2)$$

Ekert önerisinde eğer Alice ve Bob kübitleri arasındaki dolanıklılığı test edebilirlerse, dolanıklılığın tek eşliliği sayesinde sistemlerinin Eve tarafından ele geçirilmediğini kanıtlanmış olacağını belirtmiştir. Protokolde Alice ve Bob, kuantum dolanık foton kaynağından gelen fotonları hangi tabanlarda ölçtüklerini birbirlerine açık kanal yoluyla belirtir ve böylelikle aynı tabanları kullandıklarından emin olurlar. Sonraki maddede açıklanan BBM92 protokolünden farklı olarak burada Bell eşitsizliğinin ihlallerini doğrulayan istatistiksel bir testle, EPR çiftlerinin Eve tarafından dinlenmeye tabi tutulmadığını doğrulayabilirler.

4.2.2 BBM92

E91 protokolünün basitleştirilmiş bir hali olup dolanık foton çiftlerinden yararlanmaktadır[31]. Bununla birlikte E91 protokolünde kullanılan Bell eşitsizlik testi ihtiyacını ortadan kaldırır. Alice ve Bob kuantum dolanıklılık kaynağından gelen fotonları alır ve rastgele olarak filtrelerle ölçümleri gerçekleştirirler. Daha sonra karşılıklı olarak filtre seçimlerini açık kanaldan karşılaştırırlar. Her ikisi de yalnızca aynı filtreleri kullanarak yaptıkları ölçümler için oluşan anahtar çiftlerini kullanırlar. Sonra Alice ve Bob, QBER'i tahmin etmek için bazı bitleri birbirleriyle paylaşır. QBER belirli bir eşiğin üzerindeyse, hataların yalnızca doğal hatalardan gelmediğini, Eve'in bilgi elde etmeye çalıştığını varsayarlar. Aksi takdirde, hata düzeltme ve gizlilik yükseltme aşamasına geçerler. Protokol dolaylı olarak Alice'in ve Bob'un SPD'lerinin ölçümleri kusursuz bir şekilde gerçekleştirebileceğini varsaymaktadır.



Şekil 4-5BBM92 Şeması

4.3 Decoy State

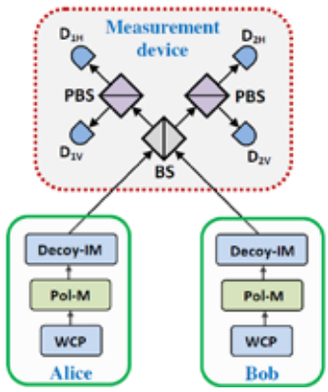
İlk kez 2003 yılında Hwang tarafından ortaya atılan Decoy-State metodu[47], foton kaynağından gelen kusurlarla mücadele etmek için en etkili yöntemlerden birisidir. Günümüzde kullanılan foton kaynaklarında tekli foton gönderimi neredeyse imkansızdır. Eve çoklu olarak gönderilen foton demetinden bir fotonu yakalayabilir ve daha sonra saldırı düzenlemek için fotonu saklayabilir. Çoklu foton bileşenlerinin etkilerini azaltmak için Alice, düşük yoğunluklu optik darbeler kullanmak zorundadır.

Bu sebeple decoy-state metodunda rastgele olarak farklı yoğunluklarda foton darbeleri gönderilerek Eve yemlenir. Decoy-State de kullanılan darbe yoğunlukları Alice tarafından kaydedilerek anahtar dağılımı sonrası açık kanaldan Bob ile paylaşılır. Alice'in yoğunluk bilgisine sahip olmadan Eve eğer araya girerse her halükârda ölçüm oranlarını değiştirmek zorunda kalacaktır. Bob tarafından alınan fotonlar asıl

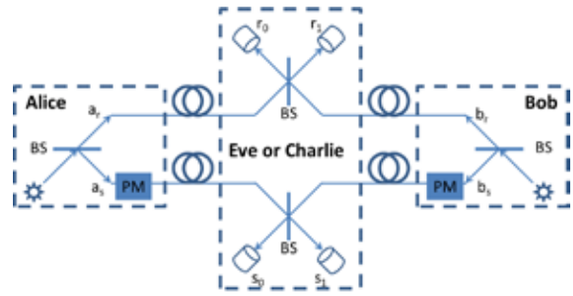
anahtardaki foton yoğunluğundan farklıysa iletişim geçersiz sayılır, diğer durumda iletişim güvenli kabul edilerek devam edilir. Eve her decoy-state de düzeneğini yeniden konfigüre etmekte zorlanacağı için özellikle foton bölme (PNS) ve Ortadaki Adam saldırılarına (MITM) karşı decoy-state etkili bir yöntemdir. İlk deneysel gösterimi ise Decoy-State KAD sistemi olarak 2005 yılında 15 km'lik bir fiber bağlantı üzerinden başarıyla gerçekleştirilmiş olmakla birlikte[48] bu gösterim çift yönlü iletişimi kullanmaktaydı ve Trojan Atı saldırılarına açıktı. Bu kapsamda [49] tarafından tek yönlü iletişimi kullanılarak 102 km'de gösterim gerçekleştirildi .

4.4 Ölçüm Cihaz Bağımsız KAD (ÖCB-KAD)

Günümüze değin KAD sistemlerine saldırılar çoğunlukla cihazların yeterince mükemmel olmaması nedeniyle gerçekleştirebilmiştir. Bu nedenle araştırmacılar cihaz bağımsız KAD (DI-QKD) sistemleri geliştirmek konusunda çaba sarfetmişlerdir[50-52]. Bu cihazlardan en önemli zafiyete sahip olanlar ise dedektörlerdir. Bu sebeple E. Biham, B. Huttner ve T. Mor tarafından 1996 yılında; H. Inamori tarafından da 2002 yılında ölçüm cihaz bağımsız KAD'ın üzerine zaman geri dönüşümlü dolanıklılık ilkesini benimseyen sistemler ortaya konmuştur[53, 54]; ancak bu sistemler gerçek tekli foton kaynağı, uzun süreli kuantum hafıza ve yemleme gibi farklı özelliklerde cihaz ve yöntemler gerektirdiğinden hayata geçirilememiştir. Decoy-State metodunun ortaya çıkışından sonra bu makaleleri baz alarak 2012 yılında Lo, Curty ve Qi tarafından "Ölçüm Cihaz Bağımsız Kuantum Anahtar Dağıtımı" adında makale yayınlanmıştır[55]; ancak polarizasyon kodlamalı olduğundan fiber optik sistemlerde çalışması daha zorludur. Bu kapsamda günümüzde daha yaygın olarak kullanılan faz kodlamalı ÖCB KAD şeması yayınlanmıştır[56]. Protokolün ilk deneysel gösterimi 2013 yılında 0.12 bit ile 50 km'de gerçekleştirilmiştir[57]. Farklı gruplar da 2013 yılı itibariyle deneysel gösterim çalışmaları yaparak protokolün uygulanabilirliğini kanıtlamışlardır[58-60].



Şekil 4-6İlk ÖCB KAD Şeması[55]

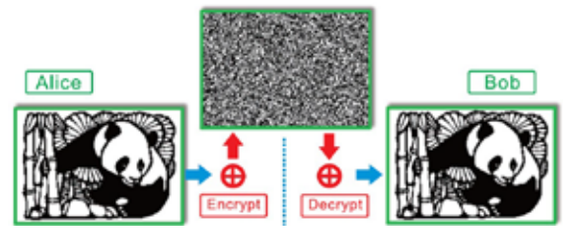


Şekil 4-7Genel ÖCB KAD Sistemi[56]

Protokolün ana bileşeni, Charlie adında, 50/50 ışın ayırıcılar ve tek foton dedektörleri kullanılarak uygulanan kısmi bir Bell durum ölçümü (BSM) yapan röle modülüdür. Alice ve Bob, her ikisi de gönderici olarak dört olası BB84 durumunda zayıf tutarlı foton darbeleri hazırlar. BS'de bölünen bu foton darbelerinin birer kolu faz modülasyonuna (PM) tabii tutularak kısmi Bell durum ölçümü gerçekleştiren Charlie (ölçüm cihazı) isimli güvenilir olmayan bir röleye gönderir. Eğer faz farkları

$$\phi = \phi_A - \phi_B = 0 \; veya \; \pi \qquad (4.3)$$

ise gelen sinyaller Charlie'nin içinde Hong-Ou-Mandel etkisi sebebiyle etkileşime girer ve faz farkına göre birer dedektör "clickler". Charlie, başarılı Bell ölçüm sonuçları açıkça duyurur. Alice ve Bob, bu örneklere karşılık gelen durumları (0,1) saklar ve geri kalanını elimine eder.



Şekil 4-8ÖCB KAD Sisteminde Gönderilen Mesaj[61]

Diğer yandan zayıf tutarlı foton darbeleri yerine tek foton bazlı ölçüm yapan ÖCB KAD sistemleri günümüzde bulunmaktadır[62]. ÖCB KAD sistemlerinin en önemli faydası ise taban açıklanması yapılmadığından Charlie'ye güvenmek zorunda olunmamasıdır. Bu durum da bizlere "Kuantum Ağlar"'ın kapısını aralamaktadır. İlk kuantum ağ deneyi 2017 yılında 4 düğümlü olarak gerçekleşmiştir[63].

Bugünkü teknolojide tek modlu 1550 nm ticari fiber kablolar km başına 0.2 dB kayba uğramaktadır. Serbest uzay olarak adlandırılan sistemlerde ise açık havada km başına 0.1 dB kayba uğramaktadır. Bu kayıplar ticari fiber sistemlerinde 300 km, serbest uzay optik sistemlerde de 1000 km[64] ve üzerinde oldukça dikkate alınması gereken bir değere dönüşmektedir. Bu demektir ki mesafe arttıkça oluşturulan anahtarda kayıp artmaktadır. Her ne kadar kuantum röleler ve hafızalar tam olarak bulunmasa da 2020 yılında kuantum hafıza destekli rölenin kısmi bir uygulaması ÖCB KAD sistemi şeklinde hayata geçirilmiştir[65].

Bu bölümün konusu olmasa da kuantum hafızaya ihtiyaç duymayan cihaz bağımsız protokoller de mevcuttur. Bu protokole ikiz bölge KAD protokolü adı verilmiş olup, en güncel gösterimleri 2021 yılında röle gibi bir yapıya sahip 605 km'ye[66] ve 2022 yılında 833 km'ye ulaşan[67] KAD

sistemleridir. Bu kayıpları engellemek ve böylece kuantum ağların kapısını aralayabilmek için stabil çalışan kuantum rölelere ihtiyaç bulunmakta olsa da günümüz teknolojisinde kuantum röleler henüz mümkün değildir; ancak konu hakkında yukarıda belirtildiği üzere çalışmalar devam etmektedir.

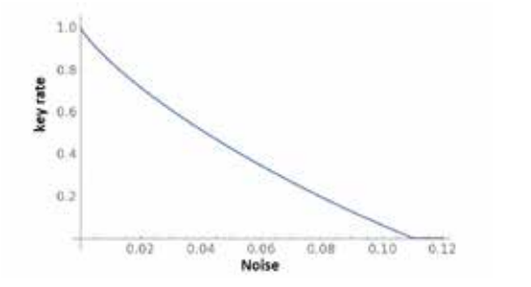
5 Kuantum Hata Biti (QBER)

Şimdiye kadar açıklanan özellikler KAD'ın, Shannon'un bilgi teorisi gereksinimlerini karşıladığı için teorik olarak güvenli bir iletişime izin verebileceğini söyleyebiliriz. İdeal bir senaryoda KAD, anahtar değişimi sorununa etkin ve mükemmel bir çözümdür. Gerçek dünyada kullanıldığında ise dikkat edilmesi gereken hatalar ve sorunlar vardır.

Üçüncü bir kişinin varlığından kaynaklanabilecek hataların yanı sıra, klasik iletişimde olduğu gibi gerçek cihaz kaynaklı iletim hataları da meydana gelebilir. Teori her ne kadar kusursuz olsa da gerçek dünyada cihazlar mükemmel olarak çalışmadığı, sistem iyi izole edilmediği için polarizasyon hataları, algılama verimsizliği, iletim kaybı oluşabilir. Ayrıca herhangi bir dış kaynaklı parazit de bir fotonun polarizasyon durumunu değiştirebilir.

Kuantum kanalı üzerinden iletişim sırasında oluşabilecek her türlü hatayı Kuantum Bit Hata Oranı (QBER) ile takip edebiliriz. Bu parametreler, iletişim sırasında meydana gelen hataların yüzdesini yansıtır ve hem kanal hatalarına hem de gizli dinlemeden kaynaklanan hatalara atıfta bulunabilir. Kanaldaki her hata, potansiyel olarak, iletişimi sezmeye çalışan bir üçüncü şahıstan kaynaklanabileceğinden dolayı sızdırılan bilgi miktarını anlamak için QBER'i verimli olarak tahmin edebilmek önemlidir.

QBER'in yüksek çıkması durumunda anahtar dağıtımı iptal edilerek iletişim geçersiz sayılır ve yükseklik nedenleri incelenir. QBER bu nedenle kuantum iletişimi için bir güvenlik göstergesi haline gelir. QBER için doğru eşiği belirleyebilmek çok önemlidir. QBER hesaplamasına kanal hataları da dahil edildiğinden, düşük bir eşiği aşan iletişimlerin iptal edilmesi, tüm iletişimin iptal edilmesine yol açabilir; diğer yandan, potansiyel olarak tüm hataların bilgi sızıntılarından kaynaklandığı düşünülürse, yüksek bir eşik seçmek riskli olabilir.



Şekil 5-1BB84 Protokolünde Gürültüye Bağlı Teorik Anahtar Limitleri[68]

2000 yılında Shor ve Preskill, kuantum iletişimi için ideal QBER eşiği tanımlayan bir güvenlik makalesi sunmuştur. [69]. BB84 protokolünde %11'lik bir QBER ile, olası bir dinleyicinin, tüm hatalar kendisine yöneltilebilir olsa bile, değiş tokuş edilen bilgileri kurtaramayacağını göstermişlerdir. Bu nedenle QBER için, tek yönlü kuantum iletişiminde, %11 ve altındaki değerlerin anahtar oluşturmak için güvenli olduğunu düşünmek yaygın bir kullanım olacaktır.[68, 70]

Tablo 5-1QBER Sınır Yüzde Değerleri[43]

	BB84 Protokolü		**Altılı Durum Protokolü**	
İletişim	Tek Yönlü	Çift Yönlü	Tek Yönlü	Çift Yönlü
Üst Sınır	%14,6	%25	%16,67	%33
Alt Sınır	%11	%18,9	%12,7	%26,4

Tablo 5-1'de görüldüğü üzere[43] PNS ataklarına karşı geliştirilen Altılı Durum Protokolü BB84 protokolünden daha yüksek yüzdelerde QBER oranlarını tolere edebilmektedir.

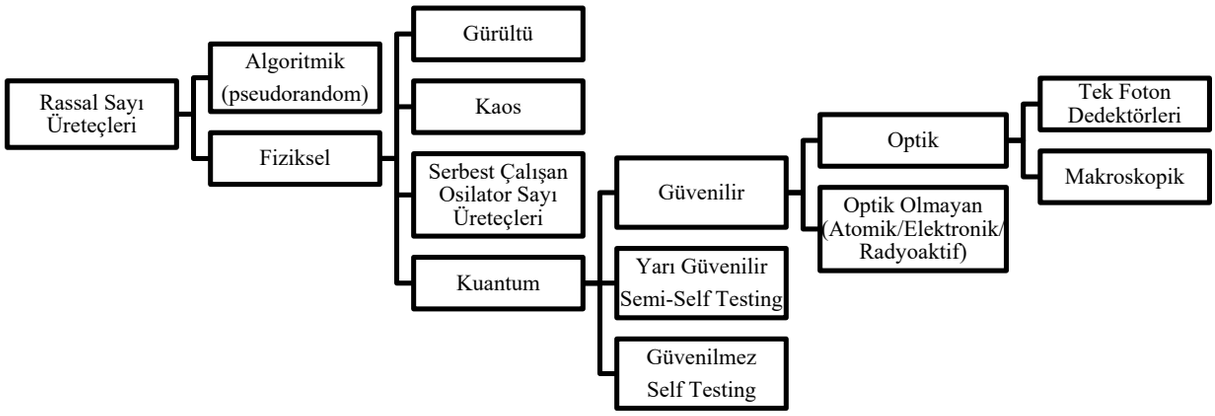
6 Donanım Araçları ve Sorunlar

6.1 Tek Fotonun Önemi ve Kaynakları (SPS)

Orijinal BB84 protokolü tek foton üretimi ve kullanımına dayanmaktadır. Bununla birlikte, karmaşıklık, kararlılık, maliyet gibi etmenlerden dolayı genel bir KAD sistemi için mükemmel bir tekli foton kaynağı (SPS) halen mevcut değildir. 1992 yılında tamamlanan ilk deneyden bu yana çoğunlukla zayıf tutarlı darbeler gönderebilen foton kaynakları kullanılmaktadır. Bu nedenle, pratik bir KAD protokolü için kaynak, tutarlı ortalama yoğunlukta ve bilinen foton sayısı dağılımı ile zayıf bir optik darbe üretir. Pratik bir KAD sisteminde en yaygın olarak kullanılan kaynak Poisson dağılımıyla zayıf tutarlı darbeler üretebilen ve ortalama yoğunluğu $m \approx 0.1$ olan zayıflatıcı ile kombine edilmiş lazer diyotlardır; ancak gelişen teknolojiyle günümüzde kuantum nokta, kristaller, boron kitrit gibi farklı SPS'ler de kullanılmaktadır.

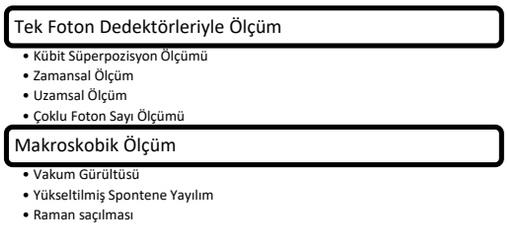
6.2 Işın Ayrıştırıcılar (BS, PBS) ve Rastgele Sayı Üretimi

Bu bölümde rassal sayı üreteçleri, ışın ayrıştırıcılar ve rassal sayı üretiminde kuantum etkisine genel bir bakış sunulacaktır. Rassal sayı üreteçleri hakkında detaylı bilgi için [71-74] makaleleri incelenebilir. Rastgele sayılar, Monte Carlo simülasyonları ve programlama gibi hesaplama yöntemlerinden şifreleme, mesaj iletimi ve hatta şans oyunlarına kadar birçok uygulamada hayati bir bileşendir. Şifrelemede algoritmaların çoğunluğu açık kaynak kodlu olmasına karşın plain text ile XOR'lanacak olan rastgele oluşturulan anahtarın çözülmesi durumu ile karşılaşılabilmekte, bu da bizleri anahtarların ne kadar güvenli olduğu sorusuna götürmektedir. Alışılmış bir örnek olan zar olasılık probleminde atılan bir zarın seçilen bir sayı gelme olasılığı 1/6'dır; ancak bu gerçekten rastgele midir? Eğer zarın atıldığı ortamla ilgili yeterli derecede sürtünme, yerçekimi, ağırlık, hız vb. bilgiye sahip olduğumuzda atılan zardaki gelecek olan sayıyı bilebiliriz. Bilgisayarlar kesin bir yapıda çalıştıkları için gerçek anlamda rastgele bir sayı üretemezler. Üretilen rastgele sayılar bir bağımlı değişkene sahiptir. Bu sebeple bilgisayarlar tarafından üretilen bu rastgele sayılar "yalancı rastgele sayı" olarak adlandırılmaktadır. Kuantum rassallığın ilk örneklerinden biri olarak radyoaktif bozunmayı kullanan Geiger-Müller Tüpünü verilebiliriz[75].



Şekil 6-1Optik Kuantum Rassal Sayı Üreteçleri Hiyerarşi Ağacı

Bununla beraber elektronik gürültü (termal[76] ve shot[77]) ve atomik (hapsedilmiş iyonlar[78], spin gürültüsü[79]) sistemler de kuantum rassal sayı üreteçlerinin örneklerindendir. Ancak günümüzde kuantum rassal sayı üreteçleri yukarıda belirtilenler dışında çoğunlukla "optik" sistemler kullanmaktadır. Optik bazlı kuantum rastgele sayı üreteçleri (KRSÜ) tek foton ölçümü veya foton özelliklerine göre ölçüm olmak üzere 2 kategoride incelenebilmektedir.



Tam bu noktada elmaslar ve camlar göze hitap eden görünümlerinin yanı sıra optik alanında foton ayırıcı özelliklerini de kullanabilmemize imkân sağlamaktadır. Elmaslar ve camlar gelen fotonları farklı oranlarda yansıtma(r) veya geçirme(t) özelliğine sahiptirler. Bu ışın ayrıştırıcılara Beam Splitter (BS) denmektedir. Gelen fotonun, kübit durumu

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (6.1)$$

$$|\alpha|^2 + |\beta|^2 = 1 \quad (6.2)$$

olduğundan, yansıtma (r) ve geçirme (t) ihtimalleri

$$|r|^2 + |t|^2 = 1 \quad (6.3)$$

olarak belirtildiğinde Bloch küresinde

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \quad (6.4)$$

ihtimaller

$$r = \cos\left(\frac{\theta}{2}\right) \quad (6.5)$$

$$t = e^{i\phi}\sin\left(\frac{\theta}{2}\right) \quad (6.6)$$

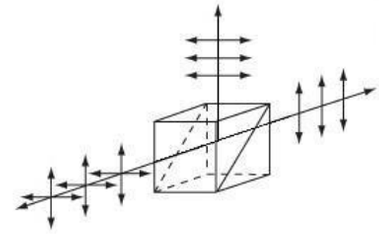
olarak ifade edilir. Durumların oluşma ihtimalleri %50 olduğunda $\theta = \pi/2$ olmakta ve BS'ten sonra fotonun durumu;

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right) \quad (6.7)$$

Şekil 6-2Polarize Işın Ayrıştırıcı (BS)[80]

olarak ifade edilir. BS'ler bir kübit durumunu süperpozisyona soktuğundan Hadamart kapısı olarak işlev görür. Birçok faklı olasılık seçeneğinde (30:70, 99:1, 50:50) ayrıştırma yapabilen BS olduğu unutulmamalıdır. Bu durum herhangi bir değişkene bağlı olmadığı için "true randomness" olarak geçer.

BS'larda oluşan diğer bir etki ise Hong-Ou-Mandel girişimidir (HOM)[81]. Girişim aynı özelliklere sahip bir foton eğer BS üzerinde aynı anda karşılaşır/girişir ise BS'ten aynı yönde yansımak zorunda olduklarını gösterir. Bu etki Bölüm 4.4'te bahsedilen Ölçüm Cihaz Bağımsız KAD (ÖCB-KAD) protokollerinin en önemli adımlarından birini oluşturmaktadır.



Şekil 6-3Polarize Işın Ayrıştırıcı Çizimi [80]

Farklı polarizasyonlarda olan fotonlar polarize ışın ayrıştırıcılardan (PBS) geçirilerek ortogonal polarizasyonlarına göre ayrıştırılırlar. Polarize ışın ayrıştırıcılar her ne kadar görünüş olarak BS'lere benzese de özellik bakımından polarizasyonlara göre sınıflandırma yaptıklarından dolayı farklıdırlar. Bu tip ışın ayrıştırıcılara da kısaca PBS

denmektedir.

Bu duruma en basit örneklerden biri polarize güneş gözlükleri veya diğer adıyla üç boyutlu gözlüklerdir. Polarize güneş gözlüklerine gelen fotonlar gözlük camında bulunan PBS ile sadece dikey polarize ışığın geçişine izin verir. Yatay polarizasyondaki ışık su gibi yüzeylerde daha güçlü yansıma yaptığından dolayı yapılan filtreleme sayesinde daha yalın bir görüntü elde edilmektedir. 3D görüntüleme için polarize gözlük olması durumunda, bir göz dikey polarizasyondaki, diğer göz ise yatay polarizasyondaki ışığın geçişine izin verir. Bu şekilde, bir 3D ekran, gözler için ayrı görüntüler iletebilir. Kuantum kriptografide kullanılan Kalsit, Kuvartz ve Turmalin gibi maddelerin filtre özellikleri kullanılarak polarizasyonları farklı olan alıcıya gelen fotonlar yansır veya maddenin içerisinden geçer. Bu durumda aynı polarizasyona sahip fotonlar PBS'ten geçmiş olacağı veya yansıtılmış olacağı için her zaman aynı noktada buluşacaktır.

Birçok ticari firma bu alanda çalışmalarını sürdürmektedir. İsviçre merkezli ID Quantique firması 2001 yılında kuantum etkilerine dayalı gerçek rastgele sayı üreteçlerini (TRNG) ilk kez tanıttı. Halen kuantum rasgele sayı üreteci çözümleri olarak Şekil 6-4'de[82] görünen "Quantis" ürün serisi ile devam etmektedirler. Günümüzde TRNG cihazları Gb/sn seviyesinde rastgele bit üretme yeteneğine ulaşmış durumdadır. Yakın gelecekte işlem kapasitelerinin artmasıyla beraber tüketici elektroniği olarak günlük yaşamda yerini alması beklenmektedir. Tablo 6-1'de farklı markalara ait ticari Kuantum Rastgele Sayı Üreteçleri de gösterilmiştir [74].

Şekil 6-4QUANTIS Rastgele Sayı Üreteci

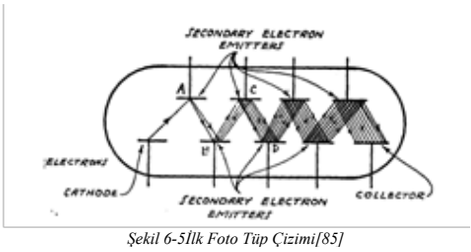
Tablo 6-1Ticari olarak temin edilebilen Kuantum Rastgele Sayı Üreteçleri[74]

Şirket	QRNG	Hız	Arayüz	Sertifikasyon
IDQ	Quantis-IDQ250C2	250 Kbps	Chip	NIST SP800-22/90B, DieHarder
	Quantis-USB-4M	4 Mbps	USB	NIST SP800-22, CTL, METAS, AIS31
	Quantis-IDQ6MC1	6 Mbps	Chip	NIST SP800-22/90A/B/C, DieHarder, AEC-Q100
	Quantis-IDQ20MC1	20 Mbps	Chip	NIST SP800-22/90A/B/C, DieHarder
	Quantis-PCIe-16M	16 Mbps	PCLe	NIST SP800-22, CTL, METAS, BSI AIS 31
	Quantis-PCIe-40M	40 Mbps	PCLe	NIST SP800-22/90A/B/C, DieHarder
	Quantis-PCIe-240M	240 Mbps	PCLe	NIST SP800-22/90A/B/C, DieHarder
	Quantis-Appliance 2.0	232 Mbps	Ethernet	NIST SP800-22/90B, DieHarder
PicoQuant	PQRNG150	150 Mbps	USB	TESTU01
QuatumCTek	QRNG100E	600 Mbps	Ethernet	NIST SP800-22, GM/T 0005-2012
	QRNG100E	200 Mbps	USB	NIST SP800-22, GM/T 0005-2012
ComScire	PQ4000KS	4 Mbps	USB	ComScire QNGmeter
	PQ128MS	128 Mbps	USB	ComScire QNGmeter
	CS128M	128 Mbps	USB	ComScire QNGmeter
Quitessence Labs	qStream 100	1 Gbps	Ethernet	NIST SP800-22/90A/B/C, DieHarder
	qStream 200	1 Gbps	Ethernet	NIST SP800-22/90A/B/C, DieHarder, OASIS KMIP 1.0/1.1/1.2/1.3/1.4
Quantum eMotion	QNG2	1 Gbps	Chip	NIST SP800-22, Diehard
EYL	QRNG-H	1 Gbps	USB	NIST SP800-22/90B, BSI AIS 31
	QRNG- L	1 Mbps	USB	NIST SP800-22/90B, BSI AIS 31
	MQRNG	1 Gbps	PCLe	NIST SP800-22/90B, BSI AIS 31
qutools	quRNG	50 Mbps	USB	NIST SP800-22, DieHarder
MPD	QRN-16	16 Mbps	USB	NIST SP800-22, DieHarder, TESTU01

	QRN-32	32 Mbps	USB	NIST SP800-22, DieHarder, TESTU01
	QRN-64	64 Mbps	USB	NIST SP800-22, DieHarder, TESTU01
	QRN-128	128 Mbps	USB	NIST SP800-22, DieHarder, TESTU01
Quside	Quside FMC 400	400 Mbps	Ethernet	Quside randomness metrology toolkit
	Quside PCLe 400	400 Mbps	PCLe	Quside randomness metrology toolkit
	Quside PCLe One	2 Gbps	PCLe	Quside randomness metrology toolkit
QNU	TROPOS QNL-QRNG-X100	100 Mbps	Ethernet	NIST SP800-22, DieHard

6.3 Foton Algılayıcılar (SPD)

Alıcı tarafında bulunan Bob, fotonların gelişini algılayabilmelidir. Bu algılama durumu tek foton dedektörü (SPD) adıyla bilinen foton sayaçları aracılığıyla gerçekleştirilir. SPD'ler fotonları fotoelektrik etki [83] ve ikincil emisyon etkisinin [84] yaratmış olduğu elektrik akımı nedeniyle algılayabilmektedir. Fotoelektrik etki bir foton veya foton demetinin bir metal veya farklı bir maddeye çarptığında o maddeden elektron koparmasını tasvir eder. İkincil emisyon ise kopan elektronların tekrardan farklı bir madde tarafından emilerek/çarparak yeni elektronlar koparmasını ifade eder. Her çarpma işleminde daha yüksek sayıda elektron maddeden kopar.



Şekil 6-5İlk Foto Tüp Çizimi[85]

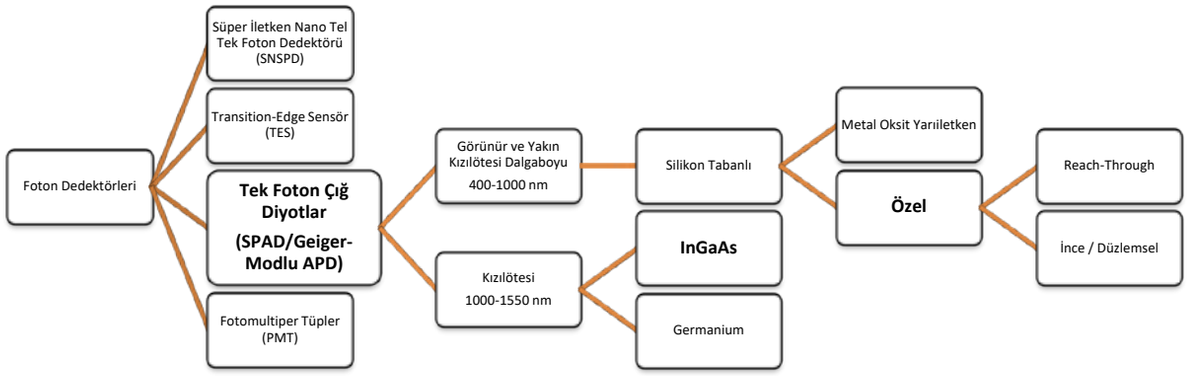
Şekil 6-6Dünyanın İlk Foto Tüpü: Kubertsky'ın Tüpü[86]

Bu duruma en iyi örneklerden birisi 1930'lı yıllarda keşfedilen ve halen batı ile doğu arasında mucit tartışmalarının [86] sürdüğü, televizyon teknolojisinin gelişmesinde büyük katkısı olan Fotomultiper Tüpler (PMT) olup, çalışma prensipleri aşağıda gösterilmiştir. Fotomultiper Tüplerde dışarıdan gelen ışık fotoelektrik olay ve ikincil emisyon neticesinde tüp içerisindeki yüzeye çarparak elektronları harekete geçirir. Harekete geçen elektronlar tüp içindeki diğer yüzeye çarparak ikincil emisyonu sağlar ve bu hareketlenmeyi yükseltir. Böylelikle gelen foton darbesi yükseltilerek okunabilecek bir seviyede elektrik sinyali üretilmiş olur. İlk prototiplerde 10^3 düzeyinde yükseltme sağlanırken günümüzdeki PMT'lerde 10^7 seviyesinde yükseltme sağlanabilmektedir; ancak PMT'ler düşük algılama verimliliği (AV) sorunuyla karşı karşıyadır. Görünür bölgede, geleneksel bialkali ve multialkali fotokatotların AV 400 nm ile 500 nm arasında %20 ila %25'e ulaşırken, GaAsP fotokatotları kullanılarak 450 nm ile 650 nm arasında %40'a kadar AV elde edilebilir[87]. Kızılötesi bölgede ise PMT'lerin AV'si çok daha düşüktür. Günümüzde halen kullanılmaktaysa da yerini her geçen gün daha kompakt yapıları ve yüksek algılama verimlilikleri nedeniyle Tek Foton Çığ Diyotlara (SPAD), diğer bir deyişle Geiger sayacındaki iyonlaştırıcı radyasyon etkisinden hareketle Geiger-Mode APD'lere bırakmaktadırlar. Bir foton sayacını karakterize eden birkaç önemli parametre bulunmakta olup, bazıları;

Tablo 6-2 Foton Sayacı Özellikleri

Kuantum Verimliliği	Bir foton çarptığında foton sayacının doğru clickleme olasılığı (sinyal verme)
Karanlık Sayım	Foton sayacına hiç foton çarpmadığında clickleme olasılığı (yanlış sinyal)
Ölü Zaman	Bir klikten sonra dedektörün sıfırlanması için gereken süre
Geç-Sinyal	Tek bir fotonun birden çok clicke neden olma olasılığı
Zaman Sapması	Fotonun dedektöre ulaşmasıyla dedektörün tespit etme zamanı arasındaki fark
Jitter	Her bir foton darbesinin dedektör tarafından ölçüm zamanları arasındaki fark.

Farklı özelliklere sahip foton dedektörü teknolojileri mevcut olup bazı örnekleri aşağıda sıralanmıştır. Daha ayrıntılı inceleme için [88-90] makalelerine göz atılabilir.



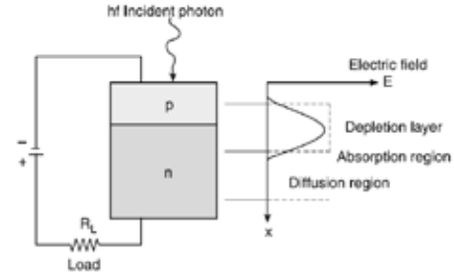
Şekil 6-7Tek Foton Dedektörleri Hiyerarşi Ağacı

Süper İletken Nano Tel Tek Foton Dedektörleri (SNSPDs) ve Transition-Edge Sensörlerinin (TES) yüksek verimlilik oranlarına karşın kriyojenik sıcaklıklarda çalışması gerekli olduğundan ve bu sıcaklıklara inmek/kalabilmek günümüzde hem maliyet hem de teknoloji bakımından büyük zorluk oluşturmaktadır. Bu sebeple Tek Foton Çığ Diyotlar (SPAD), KAD protokollerinde büyük ölçüde kullanılan SPD sınıfıdır. Diğer SPD türlerine göre en büyük avantajları ise hem silikon (Si) SPAD'ler hem de (InGaAs) SPAD'ler geniş aktif alan yüzeyleri, düşük jitter zamanları ve düşük karanlık sayım oranları sayesinde yüksek foton tespit verimliliğine sahip olurken makul[91] sıcaklıklarda çalıştırılabilmesidir. Kızılötesi bölgede InGaAs SPAD'ler alternatif olarak Germanium tabanlı SPAD'ler de kullanılmaktadır; ancak bu makalede işlenmeyecektir.

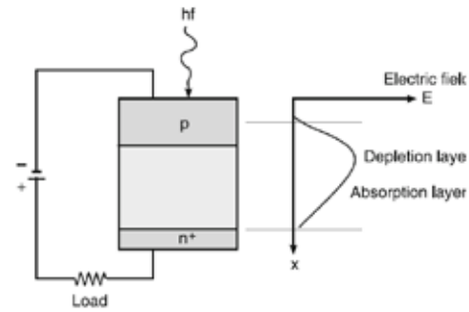
Tek Foton Çığ Fotodiyotlara (SPAD) geçmeden önce fotodiyotların nasıl çalıştığını anlamamız gereklidir. Genellikle fotodiyotları 3 ana kategoride inceleyebiliriz. Bunlar;

1. Positive-Negative (PN) Fotodiyotlar
2. Positive-Intrinsic-Negative (PIN) Fotodiyotlar
3. Çığ Fotodiyotlar

PN fotodiyotlarda p ve n bölümleri bulunmakta olup bu bölümlerin içerisinde boşluk ve elektronlar bulunmaktadır. P bölgesinde boşluklar yüksek oranda bulunurken N bölgesi elektronlar yüksek oranda bulunmaktadır. Bu materyallerin birleştirilmesiyle P ve N arasında difüzyon oluşacak ve birbirlerine geçiş sağlamaya çalışacaklardır. Öte yandan birleşim noktasında yaşanan bu olay sonucu difüzyon akımı oluşmaktadır. Difüzyonun oluştuğu birleşim bölgesinin doygunluğa ulaşmasıyla difüzyon akımı azalacaktır. Difüzyon akımı P'den N'ye doğrudur ancak; termal enerji dolayısıyla oluşan bir sızıntı akımı da bulunmakta olup, bu akım da difüzyon akımının tersi yönündedir. Foton emilim bölgesinin daha da genişletilebilmesi için I (intrinsic) bölgesi eklenmiş PIN fotodiyotlar da kullanılmaktadır. PN ve PIN fotodiyotlarda gelen foton enerjisiyle oluşan elektron-boşluk çifti için yükseltme/kazanç sınırlı olmaktadır. Eğer fotodiyota ters bir güç kaynağı bağlanırsa p bölgesindeki boşluklar ve n bölgesindeki elektronlar ters kutuplama dolayısıyla diyotun anot ve katot uçlarına doğru yaklaşacak ve difüzyon akımı 0'a yakınsayacaktır. Bu durumdaki diyotlara ters kutuplama (reverse-biased) yapılmış fotodiyotlar denilmektedir. PN fotodiyotlarda ters kutuplama zorunlu değilken PIN ve Çığ fotodiyotlarda ters kutuplama gereklidir. Şekil 6-8,9'da PN ve PIN fotodiyotların yapıları elektrik alan grafikleriyle gösterilmiştir[92].

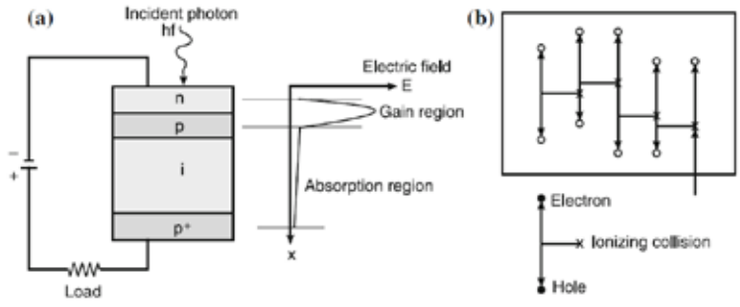


Şekil 6-8PIN Fotodiyot Yapısı[92]



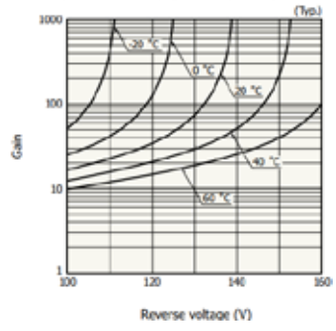
Şekil 6-9PIN Fotodiyot Yapısı[92]

Çığ fotodiyotlarda ise Şekil 6-10'da[92] görüldüğü üzere farklı çeşitlerde değişmekle birlikte ≥4 katman bulunmakta olup gelen foton, fotoelektrik etkiyle enerjisini elektron-boşluk çifti oluşturan bir hücre elektronuna bırakır. Üretilen yük taşıyıcısı, darbe iyonizasyonuyla yüksek elektrik alanın bulunduğu yükseltme/kazanç bölgesinde çığ etkisini tetikler. Ölçümün ardından APD'de oluşan akım bastırma/söndürme direnci ile sınırlandırılarak gelen yeni bir fotonu tespit edebilmek için çığ durdurulur.

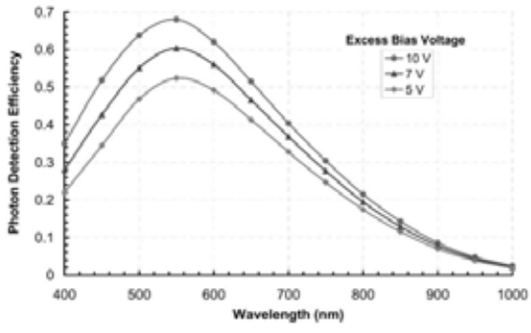


Şekil 6-10 a) Çığ Fotodiyot Yapısı b) Elektron-Boşluk Çifti Darbe İyonizasyonu[92]

Ortalama dahili yükseltme/kazanç günümüz APD'lerinde 10^5-10^6 seviyelerindedir; ancak bu kazanç Şekil 6-11'de[93] de gösterildiği üzere APD'nin çalıştırıldığı sıcaklığa da bağımlıdır. Sıcaklık artışı aynı zamanda darbe iyonizasyonunu oluşan termal enerji dolayısıyla olumsuz etkileyeceğinden yükseltme/kazanç bölgesinde oluşması beklenen elektron-boşluk çiftleri daha yüksek gerilimlerde oluşabilecektir. Bu durum fotodiyotun kırılma geriliminin de artmasına neden olacaktır. APD'lerin foton algılama verimliliği (PDE) malzemenin iyonizasyon faktörü (k), kuantum verimliliği (QE), sinyal-gürültü oranı (SNR) vb. gibi birçok farklı parametreye bağlıdır. Günümüzde mükemmel APD'ye ulaşmak bu gibi parametrelerin arasındaki ters orantılar nedeniyle mümkün değildir. Bu durum APD üreticileri tarafından parametreler arasında trade-off yapılmasını ve bu sebeple farklı APD modellerinin oluşturulmasını zorunlu kılmıştır.

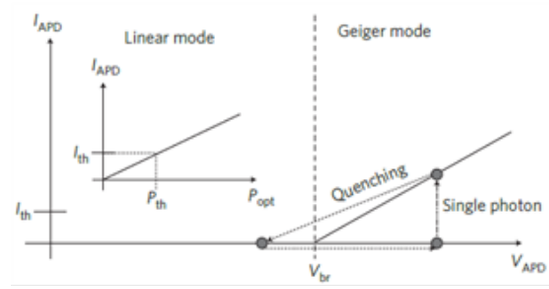


Şekil 6-11Sıcaklığa bağlı Dahili Yükseltme/Kazanç - Ters Voltaj Grafiği

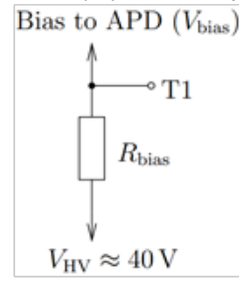


Şekil 6-12Örnek bir SPAD'nın Kırılma Gerilimi Sonrasındaki Farklı Gerilimlerde Dalgaboyuna Bağlı Foton Algılama Verimliliği[89]

SPAD'ler Şekil 6-12,13'te gösterildiği üzere APD'lerden farklı olarak ters kutuplama bölgesinde olmanın yanı sıra kırılma geriliminin (breakdown voltage) üzerinde çalışmaktadır. SPAD'ler, Geiger Modunda çalıştığı için tek fotona duyarlı olup daha yüksek oranda, yükseltme/kazanç sağlayabilmektedir. Kırılma gerilimi aşıldığı durumda düşük voltaj farkları dahi yüksek akım değişimlerine neden olmaktadır. Ölçüm sonrası çığ etkisi direnç yardımıyla aktif veya pasif bastırma/söndürme yöntemleriyle[94] SPAD'nin kırılma geriliminin (breakdown voltage) altına düşürülmesiyle durdurulur. Bir sonraki ölçümün yapılabilmesi için SPAD'nin tekrar kırılma gerilimini aşması gerekli olduğundan voltaj yükseltilir. Bu geçen hazırlık süresi "ölü zaman" olarak ifade edilmekte olup, APD halen foton hassasiyetini korumakla beraber henüz tek foton için yeterli hassasiyeti kazanmamıştır.

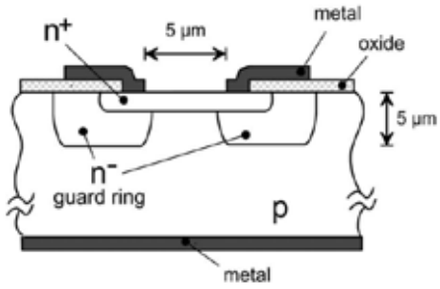


Şekil 6-13 SPAD Çalışma Prensibi Grafiği

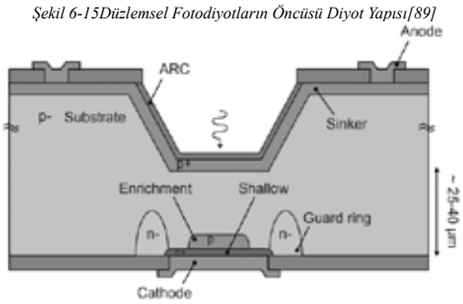


Şekil 6-14SPAD Söndürme/Bastırma Direnci

Geiger Modu 1950'lerden itibaren çalışılmaya başlanmış[95] ve foton sayımı (PC) için çalışmalar[96-98] yapılmış olsa da Tek Foton Çığ Diyotlar (SPAD) veya diğer adıyla Geiger-Modlu Çığ Fotodiyotlar (Geiger-Mode APD) ilk olarak R.J. McIntyre ve P.P Webb'in geliştirmiş olduğu ve bugün Reach-Through[99] olarak bilinen yapıdaki SPAD Modülüyle[100] ortaya çıkmış ve patentlenmiştir[101, 102]. Bu yapıda üretilen SPAD'lar halen ticari olarak Excelitas Technologies, ID Quantique gibi firmalar tarafından üretilmektedir; ancak Reach-Throughun üretim süreçlerindeki karmaşıklıklar ve yüksek voltaj gereksinimleri dolayısıyla farklı SPAD model yapılarının da oluşturulması gerekli hale gelmiş, daha önceki çalışmalardaki diyot model yapısı dikkate alınarak geliştirmeler yapılmış ve fotodiyot olarak düzlemsel model yapısındaki farklı yapılar da ortaya çıkmıştır, çıkmaya devam etmektedir.

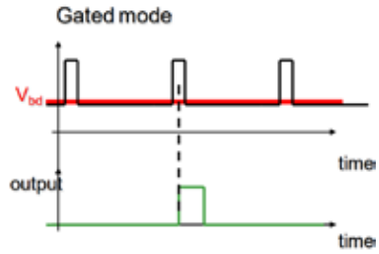


Şekil 6-15Düzlemsel Fotodiyotların Öncüsü Diyot Yapısı[89]

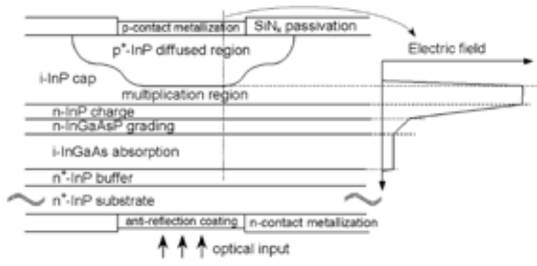


Şekil 6-16Reach Through Fotodiyot Yapısı[88]

Si APD'ler 400 ila 1100 nm [89] arasındaki dalga boyunda çalışmakta iken InGaAs SPAD'ler 950 ila 1700 nm [103] arasındaki dalga boyunda çalışmaktadır. Silikon tabanlı SPAD'lerin telekom dalga boyunda çalışması nedeniyle uygulama alanları InGaAs SPAD'lerden ayrılmaktadır. InGaAs SPAD'ler ise daha çok uzun mesafeli kızılötesi ve devamındaki dalga boyuna sahip fiber optiğin kullanıldığı sistemler de daha yaygın görülmektedir.

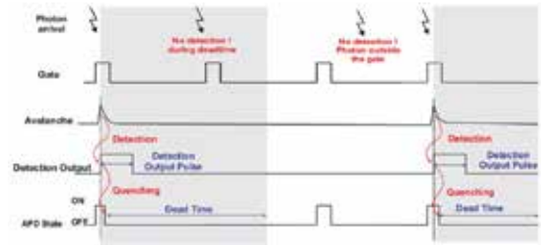


Şekil 6-17Ölçüm Penceresi/Kapı Modu[104]



Şekil 6-18InGaAs/InP Fotodiyot Yapısı[105]

InGaAs materyalinin özellikleri dolayısıyla dahili çığ etkisindeki yükselme/kazanç oluşamamaktadır. Dolayısıyla farklı materyaller ile birleştirerek foton emilimi dolayısıyla oluşan elektron-boşluk çiftinin yükseltilmesi/kazanç sağlanması amaçlanmış, bu doğrultuda InP materyalinin kazanç/yükseltme bölgesi olarak doğru aday olduğu tespit edilmiştir. InGaAsP Çığ Fotodiyotları daha önceleri [106] tarafından gösterilse de düşük verim dolayısıyla ancak 2000'lerin ortalarından sonra daha yüksek kuantum verimliliklerine ulaşabilmiştir. InGaAs/Ip SPAD yapıları dolayısıyla yüksek "karanlık sayım" ve "geç-sinyal" oranlarına sahiptir; ancak bu oranlar fotonun geldiği zamanla senkronize olarak APD'yi kırılma geriliminin üzerine belirli periyotlarda çıkarılmasını sağlayan "ölçüm penceresi/kapı modu" nun geliştirilmesiyle düşürülmüştür. Öte yandan foton kaynağıyla senkronizasyon zorunluluğunu aşmak için günümüzde pasif bastırma/söndürme yöntemini temel alan serbest koşan (free-running) SPAD'lar da geliştirilmektedir. InGaAs/Ip Çığ Fotodiyotlarının KAD sistemlerindeki uygulamaları ve genel bakış için [107] makalesi incelenebilir.

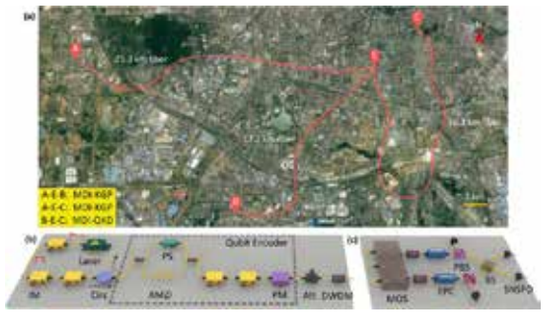


Şekil 6-19Ölçüm Penceresi/Kapı Modu Kullanılan Bir SPAD'de Foton Sayım İşlemi[104]

7 Kuantum Dijital İmzalar (QDS)

Her ne kadar kuantum sonrası için bugünden hazırlansak da farklı çözümler de aramalıyız. Bu kapsamda Kuantum Anahtar Dağıtımı tabanlı ilk dijital imza önerisi 2001 yılında Gottesman ve Chuang tarafından "Quantum Digital Signatures"[108] adıyla çıkan makalede görülmüştür. Makale içerisinde teorik olarak nasıl yapılabileceği anlatılsa da kübit durumunun yıkılmadan karşılaştırılabilmesi, uzun süreli kuantum hafıza ve güvenli kuantum kanalının gerekliliğini gösteriyordu. Ardından gelen protokoller kübit durumunun yıkılmadan karşılaştırılabilmesi[109] ve kuantum hafıza[110, 111] sorunlarına çözüm bulsalar da kuantum kanalının güvenli olacağı fikri üzerine inşa edilmişlerdi[112, 113].

2016 yılı itibariyle ortaya çıkan 2 protokol ise güvenli kuantum kanal olmadan da QDS'in çalışabileceğini gösterdi[114, 115]; ancak örneğin [114]'de her bir kullanıcı için ayrı KAD linklerine ihtiyaç duyması gibi problemler vardı. Ardından ÖCB QDS[116] daha verimli bir protokol oluştu; ancak Alice ve Bob'u birbirine güvenli olarak bağlasa da merkezi otoritenin onlarla doğrudan iletişim kuramaması nedeniyle örneğin bir yazılım güncellemesi dahi yapılamaz bir şemaydı. Bu açığı gören Toshiba araştırma merkezi 2017 itibariyle QCrypto konferansında gösterilen yeni ÖCB QDS deneysel olarak tanıttı[117]; ancak en hızlı imza olmasına karşın halen çok yavaştı.



Şekil 7-1Şehir içi 55.6 km ÖCB QDS Gösterimi[118]

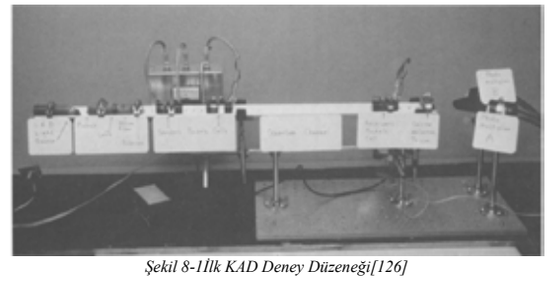
KAD sistemlerinin her geçen gün gelişmesiyle beraber QDS sistemleri de ivme kazandı ve bugün halen ticari kullanımdan uzak olsalar da 2023 yılı itibariyle çıkan tek seferlik evrensel hash (OTUH) protokoller[119, 120] kuantum e-ticaretin[121] dahi yakında olduğunun işaretlerini sunmaktadır. K-Günü ile beraber QDS sistemleri de özellikle fiziksel katmanda doğrulama sağlamak isteyen kişi ve kurumlar için post-kuantum'a alternatif olacaktır.

Tablo 7-1Kuantum Dijital İmza Algoritmaları Deneyleri

Ref	[122]	[118]	[117]	[123]	[124]	[120]
Protokol	SARG04	ÖCB	ÖCB	BB84	BB84	OTUH
Tekrar Oranı	75MHz	75MHz	1GHz	50MHz	1GHz	200 MHz
İletim Uzaklığı (km)	102	55.6	50	280	125	227
Güvenlik Parametresi	10^{-9}	10^{-7}	10^{-10}	10^{-5}	10^{-10}	10^{-32}
Bit başına imzalanma süresi (sn)	66840	149987	45	21407	22.7	1.22

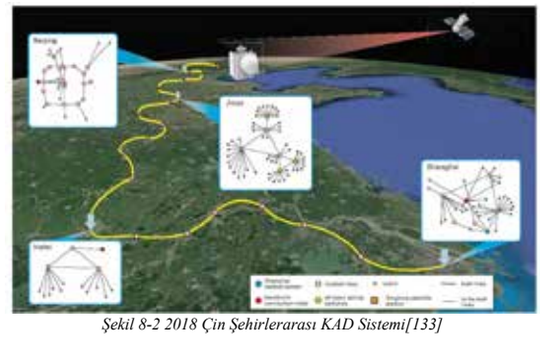
8 Akademik ve Ticari Uygulamalar

İlk deneysel gösterim Bennett, Smolin, Bessette, Salvail, ve Brassard tarafından 1989 yılında taslak olarak[125], 1992 yılında ise resmi olarak[126] yayınlandı. İlk denemede tekli fotonlar yerine aşırı derecede zayıflatılmış (10Hz) lazer darbeleri gönderilerek kullanıldı. Deney 32,5 cm lik bir uzaklıkta gerçekleştirildi ve anahtarlar yaklaşık 10bit/s dağıtıldı. Gündelik iletişimde 32.5 cm'in yeterli uzaklık olmadığı bilinmesine karşın lazer kaynağının ve dedektörlerin ilk gösterim için yüksek mesafelerde tam olarak hizalanma güçlüğü yaşanmaktaydı. 1993 yılında Townsend, Rarity, ve Tapster üçlüsü 10 km lik uzaklıkta fiber optik bazlı olarak KAD deneyini tekrarladı[127]. 1996 yılında ilk kez KAD sistemi laboratuvar dışına taşınarak gün ışığında test yapıldı ve başarıyla tamamlandı[128]. 2000'li yıllara değin laboratuvar ortamında birçok deney gerçekleştirilmiş ve KAD sistemlerinin başarıyla çalıştığı kanıtlanmıştır. Bu noktadan sonra açık alan çalışmalarına yoğunluk verildi.



Şekil 8-1İlk KAD Deney Düzeneği[126]

Dünyanın ilk kuantum kriptografi network ağı 2002 yılında Defense Advanced Research Projects Agency (DARPA) tarafından 10 güvenilir düğümden oluşacak şekilde Harvard Üniversitesi ve Boston Üniversitesi arasında kuruldu[129]. Secure Communication based on Quantum Cryptography (SECOQC) projesi ile, 2008 yılında Viyana'da birkaç KAD sistemini tek bir KAD ağında birleştirdi ve uzun mesafeli iletişim için güvenilir bir network ağı oluşturuldu[130]. 2007 İsviçre seçimlerinde[131] ve 2010 Dünya Kupası'nda güvenlik iletişimini şifrelemek için kullanıldı. 2010 yılında Tokyo'da Japonya ve Avrupa'dan farklı kuruluşların katılımıyla bir KAD ağı kurulmuştur[132]. İlk kuantum şehir ağı ise 2017'de güvenilir röleler kullanılarak Şekil 8-2'de görüldüğü üzere Çin'in Wuhu bölgesinde Beijing, Shanghai, Jinan ve Hefei şehirlerini birbirine bağlayacak şekilde 2000-4600 km olarak kurulmuştur[133]. Günümüzde Çin Merkez Bankası, Çin BDDK kurumu ve Çin Sanayi ve Ticaret Bankası dahil olmak üzere hükümet ve finans ve enerji sektörlerindeki çok sayıda kullanıcı için uzun vadeli güvenlik sağlamak amacıyla yaygın olarak kullanılmaktadır[134].



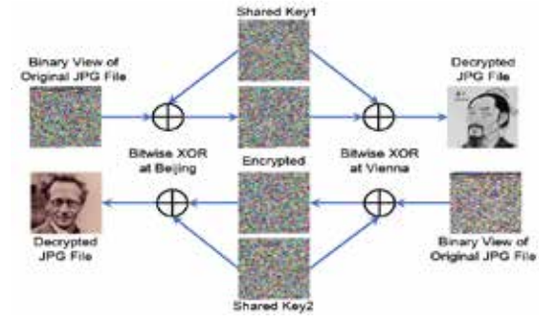
Şekil 8-2 2018 Çin Şehirlerarası KAD Sistemi[133]

Şekil 8-3 290km/s hız Uçak-Yer KAD Deneyi[135]

Sabit istasyonlardan sonra uzay yarışına kuantum iletişiminin entegre edilebilmesi hareketli istasyonlara geçiş kapsamında deneyler yapılmaya başlanmış, Şekil 8-3'te görüldüğü üzere bu deneylerin ilki Almanya'da 2012 yılında uçak-yer iletişimiyle gerçekleşmiştir[135]. Dünyanın ilk kuantum uydusu 635 kg'lık Micius 16 Ağustos 2016'da Çin Halk Cumhuriyeti tarafından fırlatılmış, yaklaşık 500 km

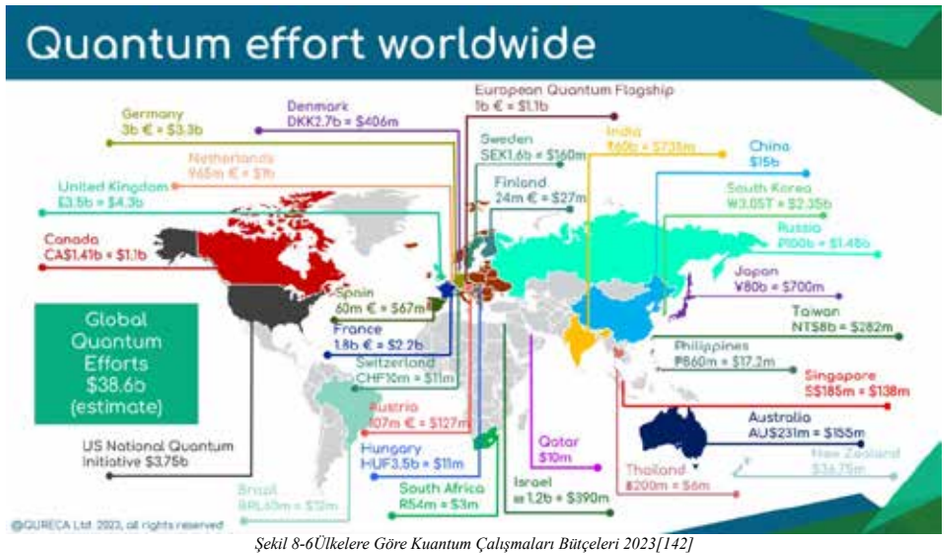
yükseklikte yörüngeye oturmuştur. Fırlatma öncesinde farklı testlerle hazırlıklar yapılmıştır[136]. İlk olarak Uydu-Yer haberleşmesini 23 farklı gün boyunca decoy-state BB84 protokolüyle başarıyla gerçekleştirmiştir [137]. Ardından ikinci görevi olan dolanık fotonları arası 1200 km olan 2 farklı yer istasyonuna iletmiş; ancak QBER oranının %8.1 gözlemlenmesi dolayısıyla başarısız olmuştur. Yine de fotonların çoğunluğunun başarıyla iletildiği belirtilmelidir. Deney 2020 yılında tekrarlanmış ve QBER oranı %4.5'a düşürülerek BBM92 protokolüyle kuantum anahtar dağıtımı başarıyla sağlanmıştır, deney sırasında KAD sistemine bilinen tüm kuantum atak çeşitleriyle saldırılmış olmasına iletişim başarıyla devam ettirilebilmiştir [138]. 2017'de Micius uydusu güvenilir röle olarak kullanılarak kıtalararası KAD ağının deneysel gösterimi yapılarak Çin'deki Xinglong şehri ve Avusturya'daki Graz şehri birbirine bağlandı[139]. Böylelikle toplam 7.600 km'yi kapsayan bir ağ kurulmuş oldu.

Şekil 8-4 Micius Entegrasyon Öncesi[140]



Şekil 8-5 Xinglong-Viyana Arasında Gönderilen Veriler[139]

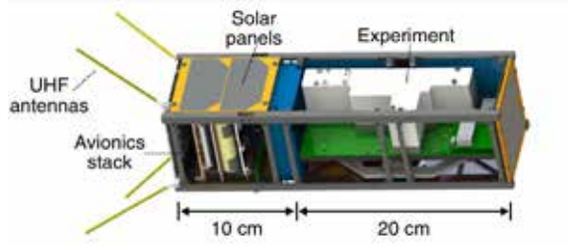
Günümüzde İsviçre merkezli ID Quantique, ABD'den MagiQ Technologies ve Hindistan'dan QNu Labs gibi şirketler ticari KAD sistemleri sunmaya başladı. HP, IBM, Toshiba ve Mitsubishi gibi firmalar da KAD sistemleri için aktif olarak araştırma yapmaktadır. Bununla beraber Çin orta ve uzun vadeli planlarına devlet stratejisi olarak kuantum teknolojisini koydu. Bunun için 14. 5 yıllık kalkınma planında ABD'nin 8, AB'nin 2 katı büyüklükte kaynak ayırarak 15.3 milyar USD ile en önde gelen ülke oldu[141].



Şekil 8-6Ülkelere Göre Kuantum Çalışmaları Bütçeleri 2023[142]

Fiber kablolarda yaşanan kayıplar nedeniyle uydu-yer haberleşmesi KAD sistemleri için bir alternatif oluşturmuş, düşük maliyetli uyduların güvenilir düğümler (trusted nodes) olarak atanabileceği anlaşılmıştır. Öte yandan uzay yarışındaki yüksek maliyetler günümüzde CubeSat standartlarında[143] maliyet etkin mikro/nano uydu projelerinin ön plana çıkmasını zorunlu hale getirmiştir. Böylelikle kuantum internetin kapıları aralanmaya başlamıştır. Bu kapsamda 2016 yılında Şekil 8-7'de görünen[144] mikro SOCRATES uydusunda Japonya tarafından B92 protokolüyle anahtar değişimi yapıldı, QBER oranı %5 olarak ölçüldü [145]. 2012 yılında Singapur Ulusal Üniversitesi tarafından nano uydu projeleri kapsamında başlatılan SpooQySat programı, Galassia ve SpooQy-1(SpeQtre) 'de yapılan deneylerin[146-149] ardından dolanık parçacıklarla KAD için uluslararası boyut kazandırılarak günümüzde CQuCoM ve SpeQtre programlarına evrilmiştir[150].

Şekil 8-7SOCRATES Mikro Uydusu (48 kg)



Şekil 8-8SpooQy-1Nano Uydusu (2.6 kg)[149]

Tablo 8-1'de KAD sistemleri özelinde bazı uydu çalışmaları yer almakta olup, daha detaylı bilgi için [151-155]makaleleri incelenebilir. Kuantum internet yol haritası ve çalışmalar için de [35, 37, 38] makalelerine göz atılabilir.

Tablo 8-1Kuantum Uydu Çalışmalar[154]

Ülke	Görev
Çin	Quantum Experiments at Space Scale (QUESS) Kuantum Uydusu Micius (2016)
Japonya	Space Optical Communications Research Advanced Technology Mikro Uydu SOCRATES (2016)
Singapur&Birleşik Krallık	Space Photon Entanglement Quantum Technology Readiness Experiment (SpeQtre) Nano Uydu SpooQy-1 (2019)
Rusya	Nano Uydu Impuls-1 (2023)
ABD	The Deep Space Quantum Link (DSQL) Marconi 2.0
Kanada	Quantum EncrYption and Science Satellite (QEYSSat)
Avrupa	Quantum Cryptography Telecommunication System (QUARTZ/EAGLE-1) / Konsorsiyum Lideri Özel Şirket (SES) The Quantum Key Distribution Satellite QKDSat / Konsorsiyum Lideri Özel Şirket (ArQit)
Almanya	QUBE 1 / QUBE 2
Birleşik Krallık	Quantum Research CubeSat (QUARC) Responsive Operations for Key Services (ROKS) National Network of Quantum Technology Hubs (UK NQT Hub)
Fransa-Avusturya	NanoBob
6'lı Konsorsiyum	CubeSat Quantum Communications Mission (CQuCoM)

9 Kuantum Hacking

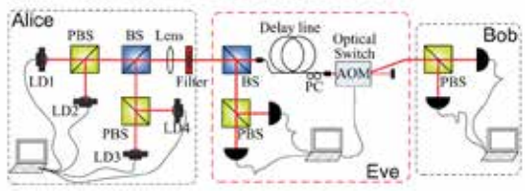
KAD protokolleri güvenliğini evrenin fizik yasalarından almasına karşın günümüzde insanoğlunun teknolojik yetersizliği dolayısıyla bu protokollerin çalışabileceği mükemmel cihazlar yapmak henüz mümkün değildir. Buradan hareketle geçmişten günümüze KAD Sistemlerine birçok faklı saldırı gerçekleşmiştir. Bu saldırılar 3 bölümde incelenebilir. Bunlar; 1-Kaynak 2- Kanal 3- Dedektör. Bu bölümde KAD sistemlerine yapılan başlıca saldırılar incelenecek, bu saldırılara karşı önlemler hakkında bilgi verilecektir. Daha detaylı bilgi için [156-158] makalelerine göz atılabilir.

9.1 Foton Numarası Bölme (PNS)

KAD sistemlerinin 1984'te doğuşu ve 1989'daki ilk deneyi ardından saldırı yöntemleri araştırılmaya başlanmıştır[126]. İlk başarılı hacking saldırısı 2000 yılında PNS atağı olarak [159-161] makalelerinde gösterilmiştir. Saldırı kaynak saldırılarının başlıca örneklerindendir.

Bölüm 6.1'de açıklandığı üzere KAD Sistemleri tek foton üretmenin günümüz teknolojisindeki zorluğu nedeniyle tek foton yerine zayıf tutarlı lazer darbeleri kullanmaktadır. Kaynaktan bir darbede/atımda gönderilen tüm fotonların birebir aynı özelliklere sahip olduğu bilindiğinden; saldırgan, gönderilen foton darbeleri üzerinde öncelikle Kuantum Nondemolition Ölçümü (QND) yaparak foton sayıları hakkında

bilgi sahibi olur. Ardından fotonları optik materyaller yardımıyla (örn: BS) bölerek belirli sayıdaki fotonları kuantum hafıza cihazında saklar. BB84 protokolü gereği tüm gönderim işlemi tamamlanıp Bob ve Alice ölçüm tabanlarını/filtrelerini sırayla açık kanal üzerinden paylaşmaya başladığında saldırganın taban/filtre bilgisine erişimi olacağı için doğru filtreleri kullanarak ölçümü yapacak ve anahtara ulaşabilecektir. Saldırı her ne kadar teoride çok başarılı olsa da günümüzde kuantum hafıza cihazlarının henüz bulunmamasından dolayı deneysel olarak gösterilememiştir; ancak yine de bu teorik saldırının gücü dolayısıyla BB84 KAD sistemlerinin güvenli iletişim aralığı 20 km'ye kadar düşmüştür[162]. Yalnızca BS ile gerçekleştirilen modifiye PNS saldırısı ise 2011 yılında Liu[163] ve arkadaşları tarafından gösterilmiştir. Saldırının L1-L2 lazerlerini kullanan 2 durum polarizasyon kodlamalı KAD sisteminde başarılı olduğu görülmüş, decoy state veya dört durum polarizasyon kodlamalı (BB84) sistemlerde başarılı olamayacağı görülmüştür.



Şekil 9-1 2011 Modifiye PNS Saldırı Şeması
L1,L2 –Ortogonal Darbeleri Üreten Lazerler
L3,L4-Decoy State Lazerler[163]

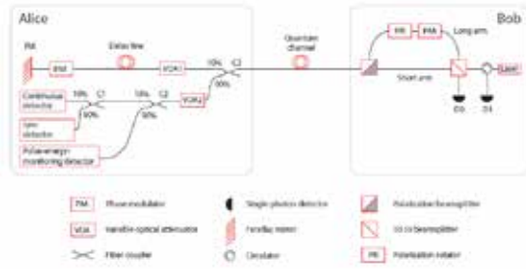
Saldırının önlenebilmesi için Decoy State yöntemi geliştirilmiş, hatta bu saldırı türüne karşı filtrelerin açıklanmadığı SARG04[32] gibi protokolleri oluşturulmuştur. Günümüzde KAD Sistemleri bu saldırıdan kaçınabilmek için çoğunlukla Decoy State [47] gibi yemleme yani önceden karar verilmiş olarak rastgele sinyaller gönderilmesi yöntemini kullanmaktadır.

9.2 Trojan Atı

Fotonik malzemelerin kendilerine gelen ışığın bir bölümünü yansıtma özelliği açık olarak kullanılmaktadır. Eve, sisteme yoğun lazer darbeleri göndererek sistemde o sırada modüle edilen fotonlarla aynı modülasyona sahip olup, geri yansıyanlar üzerinde ölçüm yaparak bilgiye erişebilmeyi amaçlamaktadır.

2001 yılında literatüre Large-Pulse saldırısı olarak geçirilen yöntem[164], ilerleyen zamanlarda evrimleşerek Trojan Atı Saldırısı ismini aldı[165]. Saldırı Tak ve Çalıştır tipinde(Çift Yönlü İletişim) SARG04 protokolünü kullanan ID Quantique Clavis2[166, 167] ve SeQureNet Cygnus [168] gibi ticari KAD sistemlerinde başarıyla test edildi. Bu saldırı türü yeterli önlemler bulunmadığı takdirde cihaz bağımsız KAD sistemleri dahil tüm KAD sistemlerine karşı yapılabilmektedir. Saldırı verici (Alice) tarafına tüm protokollerde uygulanabilmekteyken, alıcı (Bob) tarafına yalnızca çift yönlü iletişimin sağlandığı protokollerde uygulanabilmektedir.

Tek yönlü haberleşmede çevresel gürültü ve foton polarizasyonunun stabil tutulması gibi etmenler sorun teşkil etmekte olduğundan farklı Tak ve Çalıştır gibi farklı sistem önerileri ortaya çıkmıştır[169, 170]. Ticari sistemdeki saldırının nasıl çalıştığını anlamak için öncelikle saldırının yapıldığı Tak ve Çalıştır Tipi CLAVIS2 KAD sisteminin nasıl çalıştığını açıklamak gereklidir. Detaylı açıklama için [171] makalesi incelenebilir.



Şekil 9-2CLAVIS2 Şeması[171]

Sistemde Bob, hem kaynağa (SPS) hem de ölçüm dedektörlerine (SPD) sahiptir. Bob tarafından gönderilen parlak ışığa sahip lazer darbeleri (200 ns'de bir darbe) ayarsız bir Mach-Zehnder interferometresinden (MZI) geçtikten sonra kuantum kanalına girer. Lazer tarafından üretilen her darbede Bob'un interferometresinin iki kolu arasındaki yol farkından kaynaklanan 50 ns'lik bir gecikme yaşanmaktadır. 50 ns farkla kuantum kanalına giren lazer darbesi Alice'e ulaşır. Alice tarafında bu darbeler 10:90 oranında ayırıcı ile karşılaşır ve darbenin sadece %10'u KAD için kullanılırken, kalan %90 senkronizasyon ve güvenlik amaçları için Şekil 9-2'de gösterildiği gibi ayrılır. Alice'in foton zayıflatıcısı (attenuator) istenilen zayıflatmayı sağlar. Faz modülatörü (PM) ikinci darbe üzerinde rastgele bir faz(0, $\pi/2$, π, $3\pi/2$) uygular. Ardından faraday aynası (FM) her iki darbeyi de yansıtır, yansıtma polarizasyonların dik olarak dönmesine neden olur. 50ns farkla gelen her iki darbe Bob'a ulaştığında, daha önce geçtikleri yolun tam tersi yolu izler. İlk başta kapalı durumda olan uzun koldaki faz modülatörü (PM) bu sefer rastgele bir faz (0 veya $\pi/2$) uygular. Böylelikle iki darbe Bob'un 50:50 ışın bölücüsüne (BS) aynı anda ulaşmış olur. Eğer Alice ve Bob aynı faz modülasyonunu (0, 2π) kullanmışlarsa darbeler girişim yaparak tek bir dedektör tarafından (D_1 veya D_2) ölçülmek üzere tek bir yöne gider; ancak Alice ve Bob farklı faz modülasyonu uygulamışlarsa, fotonlar D_0 ve D_1 dedektörleri arasında eşit olasılıkla bölünür.

Yukarıda açıklandığı üzere Bob'un lazerinden gelen darbe dönüşte Bob'un PM'sinde faz işlemine tabii tutulduğundan Eve, Bob'un PM'sine yeterli sayıda fotonu aynı anda gönderdiğinde Bob'un oluşturduğu kübiti etkilemeden Eve tarafından gönderilen fotonlar Bob'un o sırada uyguladığı fazla aynı duruma gelir. Her fotonik malzemenin belirli oranda geri yansıtma özelliği bulunmaktadır. Gönderilen darbelerin bir kısmı geri yansıyacağından Eve, Bob'un faz bilgisini içeren fotonlara sahip olacaktır.

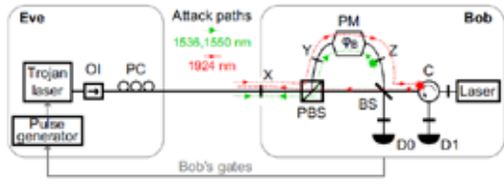
2014'te 1550 nm dalga boyunda denenen saldırı SPD'lerde geç sinyal oluşumuna neden olduğundan başarıya ulaşılamamasına karşın 2017'de farklı bir grup tarafından 1924 nm dalga boyunda denendiğinde geç sinyal oluşmadığı gözlemlenmiş, kısmi başarı sağlanmıştır.

Burada Bob'un PM'sine Trojan Atı darbenin gönderildiği zamanlama, dalga boyu ve yoğunluk en önemli parametrelerdir.

- PM'in yapısı dolayısıyla Trojan Atı darbeleri yalnızca belirli bir süre içerisinde PM'e girişim yapmalıdır.
- Gönderilen Trojan Atı darbeleri sistemde QBER

yaratabilecek olan dedektörlerde oluşan geç-sinyal etkisi yaratmayacak parametrelerde seçilmelidir.

- Eve'e geri ulaşan Trojan Atı darbeleri Bob'un sistemindeki cihazlar tarafından ölçülebilecek düzeyin altına zayıflatışmış olmamalıdır.

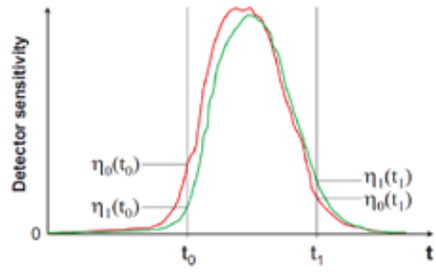


Şekil 9-3 Kırmızı / 2017 Başarılı Trojan Atı Saldırısı
Yeşil / 2014 Kısmi Başarılı Trojan Atı Saldırısı[167]

Saldırıdan kaçınmanın en iyi yolları tek yönlü KAD sistemlerinde optik izolatörler ve dalga boyu filtreleri kullanmak iken [164] , çift yönlü KAD sistemlerinde watchdog monitörü, optik izolatörler uygulamak ve faz modülatörlerinin voltaj uygulama aralıklarını daraltmaktır.

9.3 Sahte Durum Saldırısı

Bölüm 6.3'te belirtildiği üzere dedektörler, birkaç nanosaniye süren ve kapı/pencere modu adı verilen süre boyunca gelen tek fotona duyarlıdır. Bu mod dışında tek foton için neredeyse sıfır hassasiyete sahiptir. Aynı marka model dedektörlerin dahi verimlilik grafiği birbirine çok yakın olmasına karşın üretim kaynaklı verimlilik zamanlarında kaçınılmaz olarak kaymalar meydana gelmektedir. Makarov ve Hjelme tarafından 2004 yılında bu zamana bağlı verimlilik farkından kaynaklanan zafiyetin sömürülebileceği fikri ortaya çıkmış[172], 2005 yılında saldırı deneysel KAD sistemine gerçekleştirilmiş; ancak her ne kadar teoride güçlü bir saldırı olsa da dedektör karanlık sayımı vb. etmenlerden dolayı pratikte yüksek QBER oluşturduğundan tam olarak başarılı olamamıştır.



Şekil 9-4Zamana Bağlı Dedektör Verimliliği

Saldırı aşağıdaki gibi gerçekleştirilmektedir;

- Alice'in gönderdiği fotonlar Eve tarafından yakalanarak rastgele tabanlarda (Z veya X) ölçülür.
- Eve yaptığı ölçümün tam tersi polarizasyonda ve bitte yeni kübit hazırlar. (örn: Z1 ölçümüne karşılık X0)
- Eve, hazırlanan yeni kübite kodlanmış bitin ölçülebileceği dedektörün (1 ise D_1, 0 ise D_0) kapı/pencere modunda olmadığı zamanda ulaşacak şekilde Bob'a fotonu gönderilir. Bunun için optik elemanlarla dedektörler arası zaman farkı yaratabilir. Ayrıca Alice'ten aldığı foton darbelerinden daha kısa darbeleri Bob'a göndererek dedektörlerin ölçüm zamanları konusunda avantaj elde edebilir.
- Eve'den gelen fotonlar Bob tarafından rastgele tabanlara (Z veya X) sokularak D_1 ve D_0 dedektörlerine gönderilir. Eğer Eve, Bob'a dedektörlerden birinin ölçüm verimliliği yüksek, diğerinin kör olduğu bir zamanda tarafından foton darbesini göndermişse kör olan dedektörde hiçbir zaman ölçüm gerçekleşmeyecektir. Örnek, Tablo 9-1'de aşağıda verilmiştir.

Tablo 9-1Sahte Durum Saldırı Olasılık Tablosu

Alice	Eve	Eve	Bob	Bob Ölçüm Olasılığı
X0	X0	Z1	X0	%50
X0	X0	Z1	X1	1 DEDEKTÖRÜ KÖR OLDUĞUNDAN %0
X0	X0	Z1	Z0	%0
X0	X0	Z1	Z1	1 DEDEKTÖRÜ KÖR OLDUĞUNDAN %0
X0	Z0	X1	X0	%0
X0	Z0	X1	X1	1 DEDEKTÖRÜ KÖR OLDUĞUNDAN %0
X0	Z0	X1	Z0	%50
X0	Z0	X1	Z1	1 DEDEKTÖRÜ KÖR OLDUĞUNDAN %0
X0	Z1	X0	X0	0 DEDEKTÖRÜ KÖR OLDUĞUNDAN %0
X0	Z1	X0	X1	%0
X0	Z1	X0	Z0	0 DEDEKTÖRÜ KÖR OLDUĞUNDAN %0
X0	Z1	X0	Z1	%50

Denklem 9-1,2,3'de $n_x(t)$ x dedektörünün t anındaki verimliliğini ifade etmektedir. Eğer dedektör verimlilik uyumsuzluğu 1:15'ten büyükse, Eve anahtarı %11 limitinin üzerinde QBER yaratmadan elde edebilir. Altılı Durum, B92 ve E92 gibi protokoller sahte durum saldırısına karşı dirençlidir.

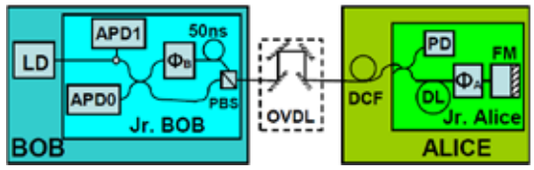
$$QBER = \frac{P(hata)}{P(varış)} = \frac{2n_0(t_1) + 2n_1(t_0)}{n_0(t_0) + 3n_0(t_1) + 3n_1(t_0) + n_1(t_1)} \quad (9.1)$$

$$Simetrik\ Olayda\ \frac{n_1(t_0)}{n_0(t_0)} = \frac{n_0(t_1)}{n_1(t_1)} = n \quad (9.2)$$

$$n \leq 0.066(\sim 1:15), QBER \leq 11\% \quad (9.3)$$

9.4 Zaman Kaydırma

Sahte durum saldırı teoriğinden yola yıkan Zhao ve arkadaşları 2005 yılında dedektörlerdeki zamana bağlı ölçüm verimlilik farklarını zafiyet olarak kullanıp bu saldırıyı geliştirdi[173]. Saldırı 2007 yılında ticari olarak kullanılan ID500 KAD sistemine (Çift Yönlü İletişim) yapılmış olup, ticari sistemlere yapılan ilk saldırı olarak tarihe geçti[174].

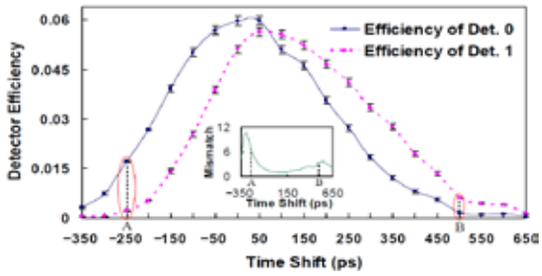


Şekil 9-5 ID500 KAD Sistem Şematiği[174]

Bu saldırıda Eve, Alice tarafından gönderilen fotonlar üzerinde herhangi bir ölçüm yapmaz. Bunun yerine sadece Alice'in foton darbelerinin Bob'a ulaşım zamanını ileri veya geri kaydırarak dedektörlerin zamana bağlı ölçüm verimliliği farkından yararlanarak her iki dedektörden birinin (D_1 veya D_0) kör olduğu zamanda fotonların Bob'a ulaşmasını sağlayarak anahtar hakkında bilgi elde eder. İki faklı SPD'nin ölçüm için kullanıldığı KAD sistemlerindeki dedektörlerde $n_x t$ x dedektörünün t anındaki verimliliğini ifade etmektedir. Bu kapsamda

$$r = \frac{n_1 t_0}{n_0 t_0} = \frac{n_0 t_1}{n_1 t_1} \tag{9.4}$$

denkleminde r eğer 0'a eşitse 1 bitinin ölçümü t_0 anında mümkün değilken, 0 bitinin ölçümü de t_1 anında mümkün değildir. Saldırı yapılan çift yollu iletişimin kullanıldığı ID500 sistemin şematiği Şekil 9-5 ve dedektör farkları Şekil 9-6'da gösterilmiştir.



Şekil 9-6 SPD'ler Arası Zamana Bağlı Verimlilik Farkları[174]

ID500 sistemindeki t_1 ve t_0 anları arasındaki fark maksimum 100ps olarak ölçülmüş olup, araştırmacılar tarafından 2844 defa test edilmiş ve bu tekrarların 106'ında 100ps ve üzerine çıkıldığı görülmüştür. Diğer bir deyişle dedektörler arası fark maksimum aralığına %4 ihtimalle ulaşmaktadır. Öte yandan dedektörler 500 ps süresince kapı/pencere modunda kalmaktadır. Orijinal lazer yerine PicoQuant lazer kaynağı kullanılmış gönderilen darbe uzunluğu süresi 100 ps'ye modifiye edilmiştir. Saldırı pratiğinde eğer 100ps kaydırma sistemin doğasından da kaynaklı oluşan QBER sorun yaratabilir, saldırı başarısız olabilirdi. Bu kapsamda araştırmacılar 50ps'lik zaman kaydırmasının yeterli olacağını yapılan simülasyonlarda görmüş ve 15 dakika süren saldırıyı başlatmıştır. Eve, denemelerinin %4'ünde toplam %5,68 QBER yaratarak anahtarla ilgili kısmi bilgi ele geçirdi. Böylece tüm olası anahtar olasılıkları üzerinde kava kuvvet saldırısı (brute-force) imkânı elde etti.

Tablo 9-2Deney Sonuçları[174]

Deneysel					
μ	Y_0	$d_{0/1}$	E	K_U	K_L
0.1	2.26×10^{-5}	3479	5.68%	1131 bit	1297 bit

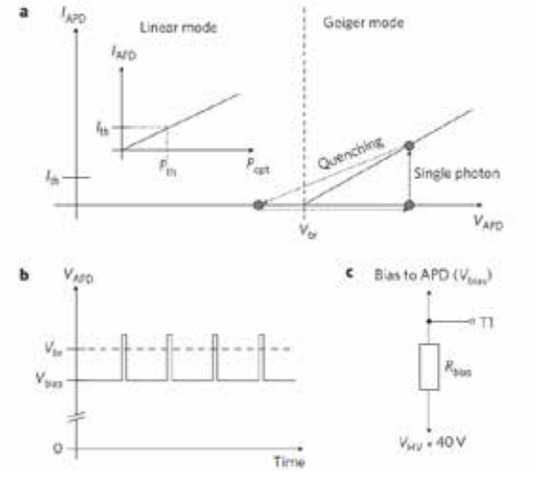
Dörtlü durum ölçümü yapılan KAD sistemleri saldırıya karşı dirençli olmakla beraber ilgili sistemlere de sahte durum saldırısıyla kombine şekilde zaman kaydırma saldırısının yapılması mümkündür.

9.5 Dedektör Kontrol Saldırısı

Bölüm 6.3'te açıklandığı üzere tek foton ölçümü için günümüzde çoğunlukla Geiger Modunda çalışan APD'ler kullanılmakta, bunlar SPAD olarak adlandırılmaktadır. Karanlık sayım, geç sinyal vb. gibi QBER artışını tetikleyen etmenlerden kaçınmak üzere bu APD'ler çoğunlukla foton darbesinin beklendiği zaman dilimlerinde kırılma geriliminin (breakdown voltage) üzerine çıkartılarak foton sayımı sağlanmakta bu duruma da zaman dilimlerine de kapı/pencere denmektedir. Tek foton SPAD'ye ulaştığında elektron-boşluk çiftini tetikleyerek çığ oluşturup tek fotonları tespit edebilmektedir. Çığ, APD içerisindeki direnç yardımıyla aktif veya pasif olarak bastırılıp/söndürülmekte, APD yeni ölçüm için tekrar ters kutuplama bölgesinde yüksek voltaj uygulanarak Geiger moduna alınmaktadır.

Doğrusal modda APD'ler tek fotona duyarlı olmamakla beraber halen fotodiyot özelliğini korumakta ve foton sayımı yapabilmektedir. 2009 yılında pasif dirençle çığ bastırmanın/söndürmenin sağlandığı kapı/pencere modu bulunmayan SPAD'lere sürekli parlak ışık tutulduğunda APD'nin Geiger modunda geçemeyerek doğrusal modda kaldığını, böylelikle tek fotonlara karşı kör olduğu fark edilmiş[175], 2010 yılında aktif bastırmalı/söndürmeli kapı/pencere modunda çalışan SPAD'lerde saldırının yapılabileceği görülmüş ve bu açık kullanılarak ID Quantique id3110 Clavis2 ve MagiQ Technologies QPN 5505 sistemleri başarıyla hacklenerek, anahtar ele geçilmiştir[176]. Saldırı 2011 yılında Gerhardt ve arkadaşları tarafından dolanık foton çiftlerini kullanan BBM92 protokolünün koştuğu bir KAD sisteminde de başarıyla gösterilmiştir[177]. Bununla beraber yine 2011 yılında saldırının dinamiklerini ayrıntılı açıklamak üzere PerkinElmer AQR model tek foton sayaç modülü üzerinde deney gerçekleştirilmiş, modüldeki dedektörün kör edilme işlemi ayrıntılarıyla açıklanmıştır[178].

Saldırıda kullanılan sürekli parlak ışık yöntemine alternatif olarak APD'lerin, kısa foton darbeleri uygulanarak sıcaklık yükselmesiyle Geiger modundan çıkıp doğrusal moda geçtiği ve böylelikle tek foton duyarlılığını kaybederek körleştiği gösterilmiştir[179]. Diğer yandan yine sürekli ışıkla körleştirmeye alternatif olarak kapı/pencere modlu SPD'lerdeki açıktan yararlanan "kapı sonrası saldırısı" ortaya çıkmıştır[180]. Saldırının doğası gereği körleştirme tekniğine nazaran daha fazla geç-sinyal ürettiğinden QBER daha yüksek olmaktadır. Farklı tekniklerle dedektör kontrolü sağlayan saldırılar da ortaya çıkmaya devam etmektedir[181-183]. Ayrıca, Bölüm 6.3'te bahsedilen kriyojenik sıcaklıklarda çalışan Süper İletken Nano Tel Tek Foton Dedektörler (SNSPDs)'in de dedektör kontrol saldırısına hedef olabileceği gösterilmiştir [184].

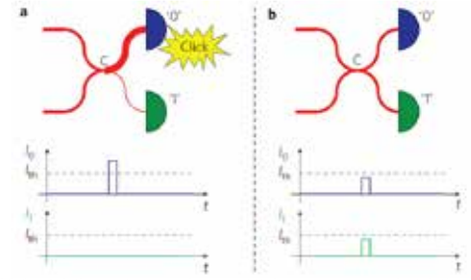


Şekil 9-7a) APD voltaja Bağlı Akım Grafiği b) Kapı/Pencere Modu Gösterimi c) APD Söndürme/Basturma Direnç Gösterim[176]

Şekil 9-7 açıklaması: a) APD V_{br} üzerinde olduğunda, gelen tek bir foton dahi yüksek bir akıma (I_{APD}) neden olur. Ölçüm sinyali eşiği (I_{th}) geçtiğinde "tıklama" olarak adlandırılan ölçüm gerçekleşir. Doğrusal modda ise akım IAPD, optik güç P_{opt} ile orantılıdır. b) Ticari KAD sistemlerinde ortalama olarak 3V'luk fazladan voltaj, kapı/pencere modu adı verilen ölçüm zamanları yaratır, bu zamanlarda V_{br} aşılmış durumdadır. c) T1'de V_{bias} APD'ye uygulanmadan önce yüksek voltaj kaynağı V_{HV}'nin R_{bias} olarak belirtilen empedansı (Clavis2'de 1 kΩ , QPN 5505'de ise 20kΩ) bulunmaktadır. Bu nedenle R_{bias} üzerinden geçen herhangi bir akım V_{bias}'ı azaltır.

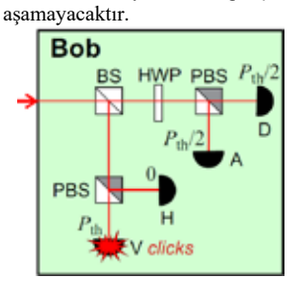
Saldırı aşağıdaki gibi gerçekleştirilmektedir;

1. Saldırıda Eve öncelikle dedektörlerin tek foton duyarlılığını körleştirmek için sürekli parlak ışık darbesi veya sıcaklık yükselmesiyle V_{bias} 'ı düşürür. Kutuplama gerilimindeki bu düşüş kapı/pencere zamanlarında tek foton duyarlılığı sağlamak için gerekli geiger moduna geçişi de engelleyecektir. Bob V_{bias}'ın düştüğünün farkında olmadığından uyguladığı voltaj V_{br} yı aşamayacaktır.
2. Alice'ten gelen foton darbelerini Eve rastgele tabanlarda ölçer. Eve yaptığı ölçümün aynı polarizasyonunda yeni kübit hazırlar; ancak tek foton göndermek yerine kısa parlak foton darbelerini Bob'a gönderir.
3. Bob rastgele tabanlarda ölçüm yapar. Eğer Bob, Eve ile aynı polarizasyonda ölçüm yaptıysa beklendiği gibi tek bir dedektör "click" ler.
4. Ancak Bob Eve'den farklı bir taban seçim yaparsa ışın 2 ye ayrılarak her fotonlar D_0 ve D_1 dedektörleri arasında eşit olasılıkla bölünür.
5. Bob'un aktif taban seçimi yaptığı durumlarda (2 dedektör) Eve P_{th} nin hemen üzerinde bir güç ile bu darbeyi göndermişse her iki dedektöre ulaşan fotonların oluşturduğu akım I_{th} 'nin altında kalacağından herhangi bir "click" leme oluşmaz.



Şekil 9-8a)Bob ile Eve'in aynı tabanı seçtiği durum b)Bob ile Eve'in aynı tabanı seçtiği durum[176]

6. Bölüm 4.1.1'de de bahsedildiği üzere tek foton bölünmesi gibi bir durum söz konusu olmadığından tek foton kullanılan KAD sistemlerinde farklı taban seçim durumlarında %50 olasılıkla D_1 'de %50 olasılıkla D_0'da ölçüm görülecektir; ancak Eve tek foton yerine kısa parlak foton darbeleri gönderirse fotonlar 2'ye bölünecek ve her iki dedektöre de çarpacaktır. Fotonlar 2 ye bölündüğü için P_{th} 'de ½ olacak ve I_{th} yi aşamayacaktır.
7. Bob'un pasif taban seçimi yaptığı durumlarda (4 dedektör) ise Eve P_{th} yerine $2P_{th}$ gücünde kısa lazer darbeleri göndermelidir. Şekil 9-9'da[178] gösterildiği üzere pasif taban şeçimi durumlarında Bob'un girişindeki BS ile ışınlar 2 ye ayrılmakta her kola P_{th} gücünde darbe ulaşmaktadır. Bu darbeler Bob'un Eve'den farklı tabana sahip kolunda tekrar 2'ye bölünerek $P_{th}/2$ gücünde olacağından I_{th} 'yi aşamayacak, "click" oluşmayacaktır. Eve ile aynı tabana sahip kolda ise doğrudan tek bir dedektöre giderek "click" 'leme oluşacak ve ölçüm yapılmış olacaktır.



Şekil 9-9Pasif Taban Şeçimi

Saldırı, bitlerin yarısının kaybolmasına neden olur; ancak normalde Alice'ten Bob'un dedektörlerine olan ulaşan foton darbeleri yoldaki (fiber veya açık hava) kayıplar nedeniyle ½'den daha düşük olduğundan bu durum sorun oluşturmaz. Ayrıca, genellikle Bob'un SPAD'leri %50'nin üzerinde kuantum verimliliğine sahip değildir. Eve tarafından gönderilen tüm darbeler "click"'lemesi istenen dedektörde I_{th} 'yi geçtiği için Bob'da %100 olarak ölçüm gerçekleşmiş olacaktır.

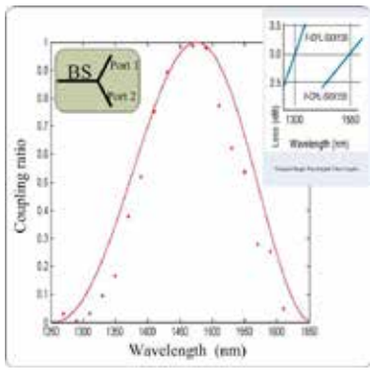
Saldırıdan korunmak için halen araştırmalar devam etmedir. Her ne kadar bit-mapped gating gibi yöntemler[185] önerilse de verimli bir çözüm olarak görülmemiş, Bob'un girişine güç ölçer koymanın saldırıyı tespit edebileceği düşünülmüş; ancak 120 foton ile dahi saldırı gerçekleştirilebileceğinden güç ölçerin faydasız olduğu ortaya çıkmıştır[186]. Doğru şekilde kullanılan [187, 188] ve gerçek zamanlı izlenen[189] SPAD'lerin veya bazı KAD sistemlerinde kullanılan homodin dedektörlerin saldırıdan etkilenmeyeceği belirtilmiş olsa da tartışmalar devam etmektedir. Ayrıca 2019'da Bob'un girişine zayıflatıcı konularak gelen fotonların gücünün düşürülmesi ve böylelikle dedektörün körleşmesinin önüne geçilmesi yöntemi de ortaya çıkmıştır[190-192]. 2023 yılında dedektör kontrol saldırılarını algılayabilmek için bir yazılım ve donanımın bir arada koştuğu bir test düzeneği dahi

oluşturulmuş; ancak bu düzenek dahi yeterli verimliliğe ulaşamamış, farklı yöntemlerle sağlanan dedektör kontrol saldırı çeşitlerinde ise (sıcaklığa bağlı, lazer zarar verme vb.) tamamen işlevsiz kalmış ve/veya geliştirmeye ihtiyaç duymaktadır[193]. Nitekim, günümüzde saldırıdan korunmanın en gerçekçi çözümü her ne kadar yüksek maliyetli olsa da Bölüm 4.4'te anlatılan Ölçüm Cihaz Bağımsız KAD sistemi kullanmaktır.

9.6 Dalga Boyuna Bağlı Saldırı

Pasif taban seçimli KAD sistemlerinde Alice'ten gönderilen fotonlar Bob'un girişinde 50:50 ışın ayırıcı (BS) tarafından rastgele olarak X ve Z tabanlarında ölçüm yapılan dedektörlere gönderilirler. KAD sistemlerinde yaygın olarak kullanılan 2 BS türü fused biconical taper (FBT) teknolojisi [194] ve ayna kaplamadır (MC); ancak FBT BS'ler de dalga boyuna bağlı yansıtma/geçirme oranları değişebilmektedir. Öte yandan genellikle KAD sistem çiplerinde çoklayıcı olarak kullanılan multimode interference (MMI) BS'ler, FBT BS'lerin dalga boyu değişkenlik karakteristiğini taşımaktadır[195].

2011 yılında Hong-Wei Li ve arkadaşları[196] Fused biconical taper (FBT) teknolojisiyle üretilmiş 1550 nm'de 50:50 olarak ayrıştırma yapan BS'in kullanıldığı KAD sistemine saldırıp anahtarı ele geçirmeyi başarmıştır. Eve'in sisteme 1470 nm ve 1290 nm dalga boyunda fotonlar gönderdiğinde BS'in geçirgenlik oranının sırasıyla % 98.6 ve 99.7% olarak değiştiği gözlemlenmiştir. Saldırıda Alice'ten gelen fotonlar Eve tarafından yakalanarak rastgele tabanlarda ölçülmekte, ölçüm sonuçlarıyla aynı polarizasyonda ve yeni dalga boyunda (1470, 1290) foton hazırlanarak Bob'a gönderilmektedir. Saldırıda sistemde ölçüm için kullanılan id 200 SPD'sinin de dalga boyuna bağlı verimliliğinin değiştiği gözlemlenmiş, verimlilik sırasıyla 1550nm: 12.1% , 1470nm: 10.7% 1290nm: 5.0% olarak ölçülmüştür. Saldırı süresince QBER %1.3'ten %1.4'e çıkmış, toplam %0.1 artış gözlemlenmiştir. QBER %11 sınırının altında olduğundan Eve yakalanmadan anahtarı ele geçirebilmektedir.



Şekil 9-10El Yapımı FBT BS'in Dalga Boyuna Bağlı Yansıtma/Geçirme Oranları[196]

Saldırı, 2013 yılında Sürekli Değişkenli (CV) KAD sistemine gerçekleştirilmiş, heterodin ölçüm yapılan sistemlerde başarıyla uygulanabileceği; ancak homodin ölçüm yapılan sistemlerde başarılı olamayacağı belirtilmiştir[197]. Öte yandan 2019 yılında 4 boyutlu faz-zaman kodlamalı KAD sistemlerinde uygulanabileceği gösterilmiştir[198].

Şekil 9-11 Güç Ölçerle Saldırıdan Korunma Yöntemi[199]

Saldırıdan korunmak için güç ölçer ile sistemin izlenmesi, yalnızca ayna kaplamalı (MC) BS'lerin kullanımı, QBER seviyesinin daha aşağıda tutulması gibi farklı çözüm önerileri sunulmuş[199], yalnızca dalga boyu filtreleriyle saldırıdan korunmanın darbe yoğunluğuna bağlı by-pass dolayısıyla mümkün olmadığı belirtilmiştir. Faz, zaman-faz kodlamalı KAD sistemleri ile ÖCB ve CB KAD protokollerini kullanan sistemler saldırıya karşı tam korumalıdır.

9.7 Double Click

En basit saldırı yöntemlerindendir. KAD sistemleri, bit 0 ve bit 1 olmak üzere iki farklı bit değerinin algılanmasını gerektirdiğinden, en az iki SPD'ye ihtiyaç duyarlar. Double click, her iki SPD'nin aynı anda sinyalleri algıladığı durumu ifade eder. SPD'ler Bölüm 6.3'te anlatıldığı üzere ölü zaman, Afterpulsing, karanlık sayım gibi sebeplerden ötürü aynı anda click (ölçüm) yapabilirler.

Saldırıda Eve, Alice tarafından gönderilen fotonun yakalayıp rastgele bir tabanda ölçer. Ölçümün ardından Eve ölçüm yaptığı polarizasyon durumunda tek foton yerine parlak ışık darbesi hazırlayarak Bob'a gönderir. Eğer Bob, Eve'den farklı bir tabanda ölçüm yaparsa, double click olayı gerçekleşir ve her iki dedektör aynı anda ölçüm yapar. Bob'un aynı tabanı kullandığı durumda tek dedektörde ölçüm gözlenir.

Eğer double click olayı yalnızca sistem hatası olarak algılanıp göz ardı edilirse Eve, Alice ve Bob ile aynı bilgiyi paylaşmış olur. Önceleri geliştiriciler double click olayı olduğunda sayımı dikkate almamayı tercih etmekteydiler; ancak Eve tarafından atak geliştirilebileceğinin anlaşılmasıyla double click olayı meydana gelmesi durumunda göz ardı etmek yerine rastgele olarak seçim yapmayı tercih ettiler[160].

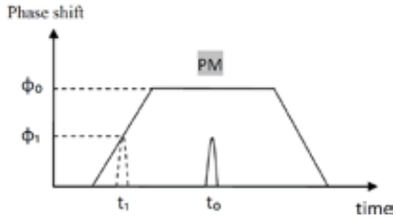
9.8 Faz Yeniden Haritalama

2007 yılında Fung ve arkadaşları[200] teorik olarak faz, faz-zaman kodlamalı sistemlerde kullanılan faz modülatörlerinin (PM) tepki sürelerindeki açıktan yararlanarak bir saldırı gerçekleştirilebileceğini göstermiş, 2010 yılında Xu ve arkadaşları[201] tarafından ID Quantique ID-500 ticari KAD sistemine saldırı gerçekleştirilmiştir. Saldırıda QBER %19.7 ölçülerek kısmi başarı sağlandığı kanıtlanmıştır.

Tak ve Çalıştır tipi çift yönlü iletişimin kullanıldığı KAD sistemleri Bölüm 9.2'de açıklanmıştır. Bu sistemlerde Bob hem SPS'e hem de SPD'ye sahiptir. Bob'un SPS'sinden gelen darbeler ayarsız MZI ile sinyal ve referans darbeleri olarak ayrılıp Alice'e gönderilir. Alice öndeki referans darbesini PM'nin aktivasyonu için kullanarak arkadaki sinyal darbesine faz modülasyonu uygulayabilmek için PM'yi hazır hale getirir. Faraday aynasından yansıyan darbeler sinyal darbesine uygulanan faz modülasyonu işlemi sonrası Bob'a gönderilir. Bob öndeki referans darbesini ayarsız MZI'den geçirip faz modülasyonu uygular. Böylelikle sinyal ve referans darbeleri

Bob'un BS'sinde karşılaşarak faz farklarına göre girişir veya girişmez.

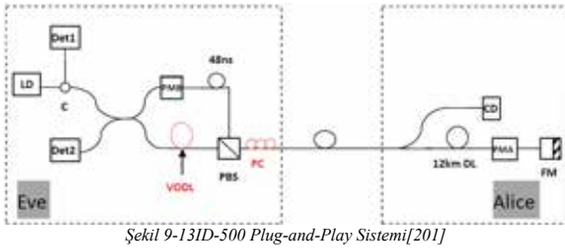
Eğer Eve, Bob'dan gönderilen referans darbesinin zamanını değiştirebilirse Alice PM aktivasyonu için yeterli vakit bulamayacak, farkına varmadan sinyal darbesine farklı bir faz uygulamış olacaktır; saldırı yakala ve tekrar gönder saldırısının farklı bir çeşididir.



Şekil 9-12Faz Modülatörü Grafiği[201]

Saldırıda Eve, Bob ile aynı düzeneği kullanmaktadır. Eve, Bob'dan gelen referans darbesinin zamanını değiştirerek veya yakalayıp tekrar göndererek sinyal ve referans darbeleri arasında zaman farkı yaratır. Bu sayede Alice istediği modülasyonda faz uygulayamaz. Alice'ten gelen darbeler Eve tarafından yakalanır ve Bob'da olduğu gibi ayarsız MZI'ye sokulur; ancak Eve daha önceden sinyal ve referans darbeleri arasındaki farkı bildiği için buna uygun olarak ayarsız MZI'yi hazırlamıştır. MZI'de girişime uğrayan darbelerde eğer başarılı ölçüm yapılabilirse Eve tarafından aynı durumda foton darbeleri hazırlayarak Bob'a gönderir, ölçüm başarısızsa yok sayılır.

Burada önemli olan diğer bir nokta ise polarizasyondur. Ana eksende hizalanmış polarizasyondaki fotonlar büyük faz modülasyonuna uğrarken, ortogonal polarizasyona sahip fotonlar ise daha düşük faz modülasyonuna uğrar[202]. Deneyde LiNbO3 PM için bu oran 1:3 olarak bulunmuştur. Alice'ten gelen sinyal darbesinin polarizasyonu, denetleyici (PC) yardımıyla ana eksene ortogonal alacak şekilde ayarlanır.

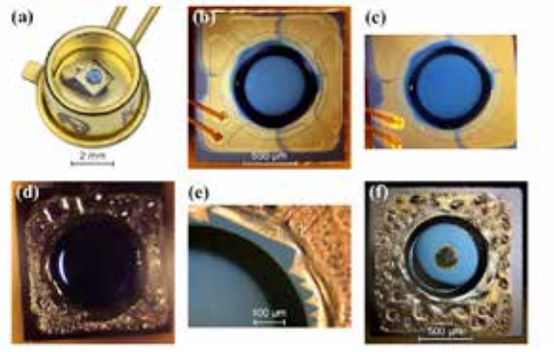


Şekil 9-13ID-500 Plug-and-Play Sistemi[201]

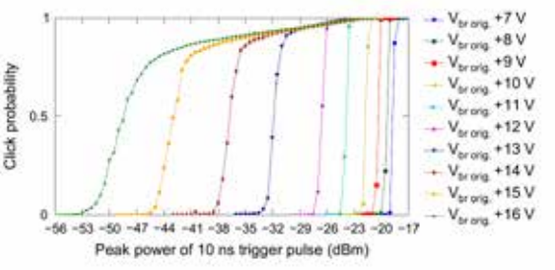
Saldırıdan korunmak için Alice referans ve sinyal darbeleri arasındaki zaman farkını ölçebilir. Günümüzde watchdog dedektörleri tarafından bu işlem yapılmaktadır. Ayrıca Alice, sinyal darbesine doğru fazı uygulayıp uygulamadığından emin olmak için faz modülasyonu sonrası zayıflatma işleminden önce darbeyi bölerek ölçüm gerçekleştirebilir. Son olarak saldırı, zaman kaydırma saldırısıyla da beraber uygulanabileceğinden maksimum tolere edilen QBER'in buna uygun olarak güncellenmesi gereklidir. Günümüzde bu durum dikkate alınarak çift yönlü sistemler için %18,9 seviyesi belirlenmiştir.

9.9 Lazer Zarar Verme

Kuantum iletişimi teorik olarak kırılamaz olsa da günümüz teknolojisindeki cihazların mükemmel olmamasından kaynaklı sorunlar nedeniyle KAD sistemlerine saldırılar gerçekleştirilebilmektedir. 2014 yılında Bugge ve arkadaşları[203] halihazırda olan açıkları kullanmak yerine, fark edilmeden SPAD'lere hasar vererek yeni bir açık yaratıp anahtarın ele geçirilebileceğini göstermişlerdir. Saldırının ticari KAD sistemlerine uygulanabilirliğinin gösterimi amacıyla 2016'da fiber ve serbest uzayda çalışan 2 farklı KAD sisteminde uygulanmıştır[204]. Bu çalışmaları temel alan Huang ve arkadaşları 2020 yılında SPAD'ler yerine optik zayıflatıcılara hasar vererek saldırının farklı tip cihazlar için de bir tehdit olduğunu kanıtlamışlardır[205]. Saldırıda Eve, yüksek güçte lazer darbeleri göndererek kalıcı hasar oluşturmakta, hasarın yol açtığı değişikliklerini sömürmektedir.

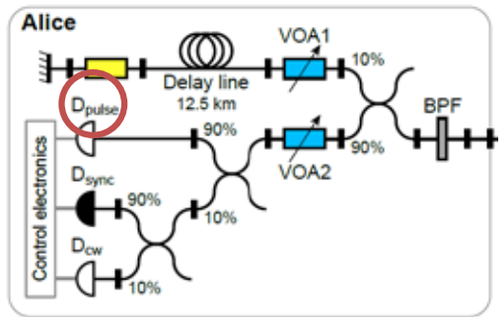


Şekil 9-14 2014 SPAD Hasarı[203]

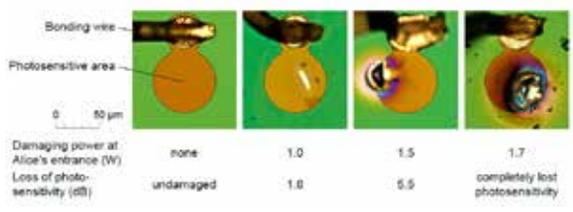


Şekil 9-15 2014 Ölçüm Tetikleme Darbesinin Güç/Olasılık Grafiği[203]

2014 yılındaki ilk deneyde[203] farklı üretim partilerinden alınmış 10 adet PerkinElmer C30902SH model Si APD 6 farklı güç düzeyinde 60 sn boyunca kesintisiz kare dalga ışığa maruz bırakılmış, SPAD'lerin 1.2W üzerinde kalıcı olarak körleştiği ve karanlık sayım olasılığının %0'a düştüğü ve tek foton hassasiyetini kaybettiği görülmüştür. Bilindiği üzere SPAD'ler kırılma geriliminin (V_{br}) üzerinde tek fotona duyarlı olmaktadır. SPAD'lerin ortalama V_{br}'nin 10-15 V üzerinde çalıştığı dikkate alındığında kalıcı körleşmenin akabinde gönderilen 10 ns'lik bir lazer darbesinin güç/click olasılık grafiği aşağıda sunulmuştur

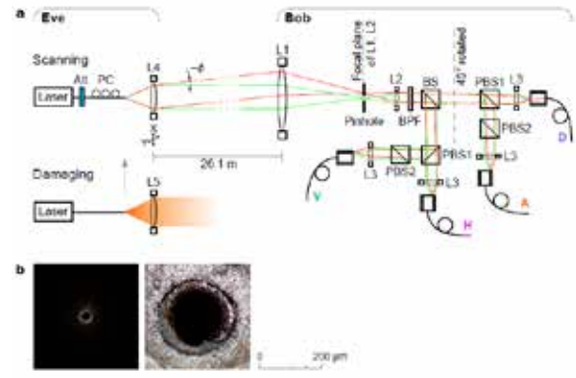


Şekil 9-16CLAVIS2 Alice Şeması[204]

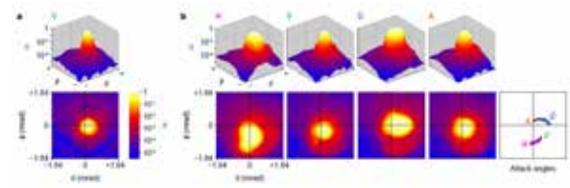


Şekil 9-17Darbe İzleme Dedektörü Hasarı[204]

2016 yılındaki deneyde[204] ilk olarak 1550nm dalga boyunda fiberde çalışan Tak ve Çalıştır Tipi Clavis2 KAD sistemi hedef alınmış, sistemde Trojan saldırılarına karşı önlem olarak kullanılan darbe enerji izleme dedektörüne 20-30 sn boyunca tutulan 0.5-1.5W lazer darbesi dedektörün algılama hassasiyeti 1-6 dB düşürmüş 1.5W üzerinde ise yok edilmiştir. Sistemde darbe enerji izleme dedektörü (D_{darbe}) olarak fiber-pigtailed InGaAs PIN fotodiyot (JDSU EPM 605LL) kullanılmaktadır. Saldırı 6 fotodiyot ayrı ayrı gerçekleştirilmiş, 3 tanesinde KAD sistemi yeniden başlatmayı gerektirecek herhangi bir alarm oluşturmadan algılama hassasiyeti düşürülerek D_{darbe} kör edilebilmiştir. Böylelikle D_{darbe} fotonların yoğunluğunun düşürülmesi gerektiğini öngöremeyecek ve yüksek sayıdaki fotonu kuantum kanalına girecektir; bu durumda Eve, Trojan Atı saldırısını başarıyla uygulayabilir.



Şekil 9-18 a) Deney Düzeneği Şeması
b) Filtrede 20 µm'den 150 µm'ye genişleyen açıklık[204]



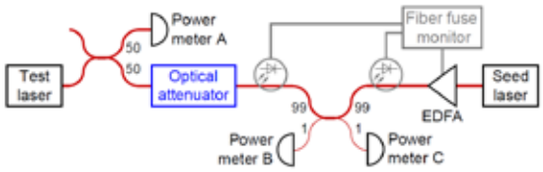
Şekil 9-19 a) Saldırı öncesi açısal hassasiyeti
b)Saldırı sonrası açısal hassasiyet[204]

2016 yılındaki aynı çalışmada[204] serbest uzayda 532nm dalga boyunda çalışan BB84 protokolünün koştuğu KAD sisteminde Bob hedef alınmıştır. Dedektör kontrol saldırısına önlem olarak sistemde kullanılan uzamsal filtreye 26.1 metreden 810nm dalga boyunda 10 sn süresince 3.6W'lık sürekli ışık gönderildiğinde filtredeki 20 µm'lik açıklığın 150 µm'ye genişlediği görülmüş, gönderilen darbenin dedektörlerde verimlilik farkına yol açarak sistemi sahte durum saldırısına açık hale getirdiği anlaşılmıştır.

Tablo 9-3 2020 Lazer Zarar Verme Saldırısı Sonuç Değerleri[205]

TİP (Marka)	Toplam	Başarı	Başarısızlık	Maks. Güvenli Güç (dBm)	Ort. Başarı Δ(dB)	Ort. Saldırı Eşiği (dBm) 1dB'den fazla düşüş	Ort. "Fail" Eşiği (dBm) 3dB'den fazla artış
Manual VOA (OZ Optics)	2	0	0	>39.5	-	-	-
Fixed (İzin Yok)	12	4	6	32.8	-1.37	34.0	37.2
MEMS VOA (2 Üretici) (İzin Yok)	13	8	4	34.5	-5.34	36.2	36.6
VDMC VOA (FOD)	(25)	(18)	0	32.9	-9.59	34.5	36.5

Bu çalışmayı temel alan Huang ve arkadaşları 2020 yılında dedektörler yerine 4 farklı tip optik zayıflatıcıya 20m mesafeden 1550nm lazer ile 9W'a kadar bir güçte saldırdı[205]. Saldırılan cihazların zayıflatma görevini yerine getiremeyecek duruma gelip sistemin PNS saldırılarına açık hale getirilmesi amaçlandı. Saldırıda 4 zayıflatıcıdan 2'si kalıcı olarak hasar alıp dBm düşüşü yaşarken, 1 zayıflatıcı geçici olarak (10dk) dBm düşüşü yaşadı. OZ Optics zayıflatıcısı ise 20 dk boyunca 9W'lık lazer darbesine rağmen herhangi bir dBm düşüşü yaşamadı. Saldırı sonuçları Tablo 9-3'te, saldırı düzeneği Şekil 9-20'de sunulmuştur.

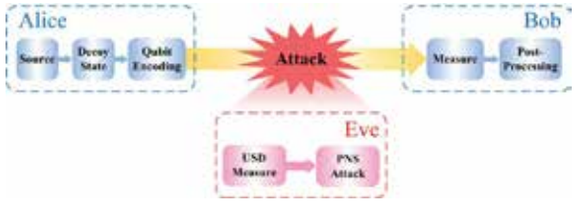


Şekil 9-20 Saldırı Düzeneği / Test Laser- Sistem 5 mW CW / Seed Laser- Eve 20 mW CW / EDFA- 9W Yükseltici / Power Meter A-Sistem lazeri güç ölçümü / Power Meter B- Eve lazeri güç ölçümü / Power Meter C- Saldırı öncesi ve sonrası Optik Zayıflatıcıdaki güç ölçümü[205]

Saldırıdan korunmak için watchdog monitorünün sisteme eklenmesi düşünülse de 2016'daki çalışmada monitorün de yüksek lazer gücünden etkilenerek izleme görevini yerinee getiremeyebileceği gösterilmiştir. Bunun yerine pasif izleme için optik izolatörler ve sirkülasyon cihazlarının sisteme eklenmesi düşünülebilir[206]. Öte yandan lazer çıkışına optik sigorta benzeri yüksek güç altında fiziksel olarak hasar alıp lazerin çalışmasını durduracak cihazlar eklenebilir[207].

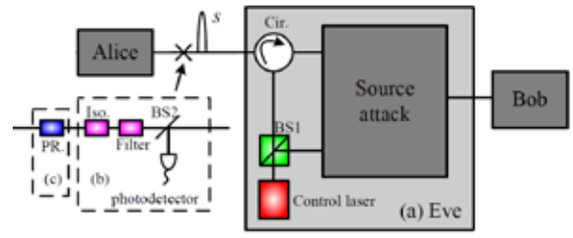
9.10 Rastgele Faz ve Lazer Tohum Kontrol

KAD'ının mucitlerinde Bennett'in dediği gibi dedektörler, KAD Sistemleri için "Aşilin Topuğu"[208] haline geldi; ancak ÖCB KAD'ının ortaya çıkışıyla, Alıcının güvenli olması ihtiyacı ortadan kalktı. Böylece ÖCB KAD protokolünün kullanıldığı sistemlerde dedektörlere yapılan saldırılar etkisizleşti. Öte yandan kaynak saldırıları her ne kadar çok daha az bulunabilmiş olsa da büyük bir tehdit olarak günümüzde geçerliliklerini korumaktadır.

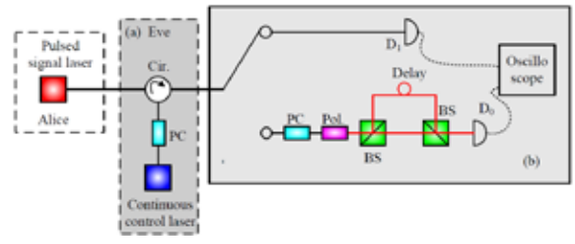


Şekil 9-21Rastgele Olmayan Faz Saldırı Şeması[209]

Decoy State yöntemi foton sayısına bağlı saldırıların önüne geçmek için en etkili yöntemlerden birisidir. Bu yöntemde decoy durumlarının yoğunluk harici ayırt edilemez olmaları temel bir varsayımdır. Öte yandan 2013'te Tang ve arkadaşları[209] faz, faz-zaman kodlamalı decoy-state sistemlerde faz randomizasyonunun sağlanmadığı durumda Eve'in yapabileceği saldırılar üzerine bir çalışma gerçekleştirdi. Saldırıda, belirsiz durum ayrım (USD) ölçümü ve PNS saldırısının kombine edilerek sinyal ve decoy darbelerinin ayırt edilebileceği böylelikle güvenli anahtar oluşturma sınırlarının ihlal edileceği doğrulandı. Bölüm 9.1'de açıklandığı üzere, Kuantum Nondemolition Ölçümü (QND) günümüzde teknolojik yetersizlik nedeniyle henüz gerçekleştirilemediğinden saldırıda yalnızca USD ölçümü deneysel olarak, PNS bölümü teorik olarak yapıldı.

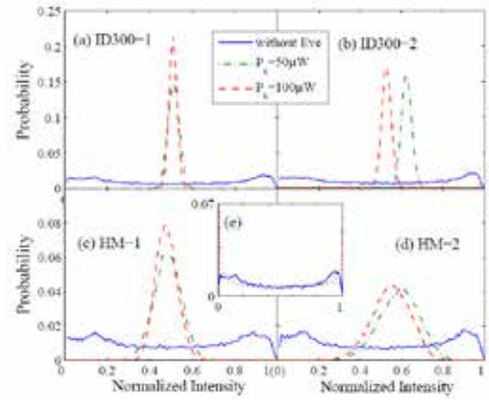


Şekil 9-22 Saldırı Şeması b) Saldırıdan korunmak için önlem şeması c)aktif faz randomizasyonu[210]



Şekil 9-23 a)Eve'in Lazeri b) Üst kol:Alice dalga formu ölçümü Alt kol: Alice-Eve ayarsız MZI ölçümü)[210]

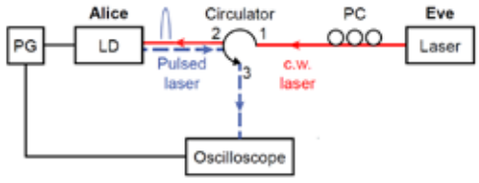
2015'te Sun ve arkadaşları[210] KAD sistemlerinde foton kaynağı olan lazerlere dışarıdan bir etkiyle faz rastgeleliğini bozmak için bir çalışma gerçekleştirdiler. Inter-driven modundaki yarı iletken lazer diyotta (SLD) akan akım sırasında spontane yayılan tohum fotonlar tarafından bir lazer darbesi üretilmektedir. Normalde tamamen rastgele fazlardaki tohum fotonlar Eve yeterli yoğunlukta belirli bir faza sahip foton gönderimi sağlayabilirse Alice'in lazerinden yayılan fotonların faz bilgisine erişmiş olacaktır.



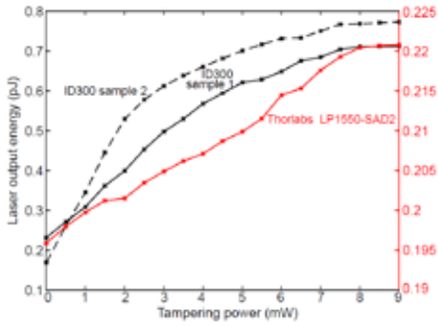
Şekil 9-24Saldırı Altında Ölçüm[210]

Eve, lazer ile (Agilent 81600B-201) CW parlak ışık altında (50μW,100 μW) Alice'e ait 2 ticari, 2 el yapımı lazere saldırdı. Alice'in lazerinden çıkan fotonların dalga formu doğrudan ölçümle(D_1), faz farkları ayarsız MZI'yle ölçüldü(D_0). Faz farkının 0-2π olduğu durumlarda yoğunluk dağılımı tekdüze olmaktadır. Alice'in lazerindeki foton yoğunluğu normal durumda tekdüze dağılım göstermekteyken saldırı altında normal dağılım (Gaussian) oluştuğu gözlendi. Eve'in lazerindeki faz gürültüsü ve/veya ayarsız MZI'deki mükemmel olmayan girişim nedeniyle bu durum yaşanmış olabilir; ancak yine de Eve gönderdiği CW ışık ile Alice'in faz rastgeleliğini bozabilmiştir. Bu durumda sisteme rastgele olmayan faz

saldırısı yapılabilir.



Şekil 9-252019 Saldırı Şeması[211]



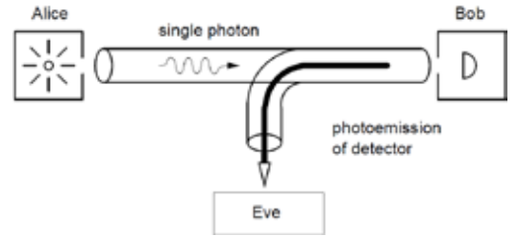
Şekil 9-26Eve'in Saldırı Gücüne Bağlı Alice'in Lazer Çıkış Enerji Değişimi[211]

Bu saldırıyı temel alan Huang ve arkadaşları 2019'da[211] Eve'in gönderdiği fotonların Alice'in lazerinde oluşturduğu yoğunluk artışını gözlemlemek ve olası saldırı stratejileri için çalışma gerçekleştirdi. Deneyde 2 adet ID300 ve 1 adet LP1550-SAD2 lazer hedef alındı. Gönderilen ortalama 1550nm dalga boyundaki 9mW'a kadarlık CW ışıkla Alice'in lazerindeki yoğunluk değişimleri gözlendi. Makalede decoy-state ve ÖCB-KAD sistemlerine saldırı yapıldığında artan yoğunluk nedeniyle güvenlik parametrelerinin anahtar oluşum oranları üzerindeki etkisi incelenerek, saldırının güvenli anahtar oluşumunu zaafiyete uğrattığı gösterildi.

Saldırıdan korunmak için sisteme izolatör, filtre ve güç ölçer eklenebilir; ancak izolatörler sınırlı izolasyon kapasitesi nedeniyle, dalga boyu filtreleri saldırının sistemle aynı dalga boyunda yapılabilme ihtimali nedeniyle, güç ölçerler ise lazer zarar verme saldırı ihtimali nedeniyle bütünleşik bir çözüm olmayabilir. En gerçekçi çözüm Tak ve Çalıştır gibi aktif faz randomizasyonunun sağlandığı protokoller kullanmaktır.

9.11 Geri Flaş Saldırısı

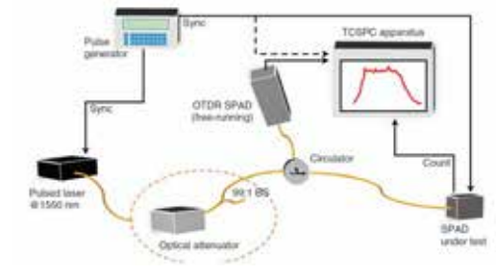
Bölüm 6.3'te açıklanan APD çalışma prensibindeki çığ etkisi sırasında düşük güçte de olsa foton emisyonunun gerçekleştiği 1955'te Newman tarafından ortaya çıkartılmış[212], 1956'da Chynoweth ve McKay konu hakkında detaylı bir makale yayınlayarak[213] bu emisyonun nasıl ve ne zaman gerçekleştiğini bulmaya çalışmışlardır. Emisyonun farklı olası nedenleri, miktarı ve özellikleri hakkında günümüze değin farklı araştırmacılar tarafından çalışmalar yapılmıştır[214-217].



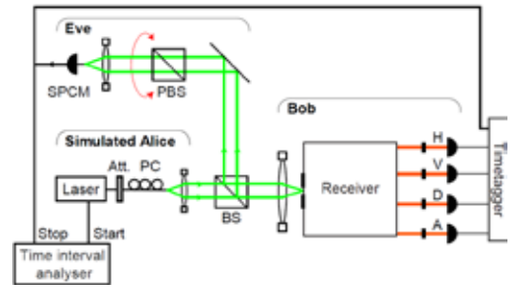
Şekil 9-27Geri Flaş Saldırı Şeması[218]

Bu durumun KAD sistemlerine saldırı için kullanılabileceği fikri 2001 yılında Kurtsiefer ve arkadaşları tarafından Si SPAD'ler üzerinde araştırılmış; ancak kesin bir sonuca varılamamıştı[218]. Makalede InGaAs SPAD'lerde daha fazla foton emisyonunun olabileceği ayrıca belirtilmiş ve farklı gruplar tarafından çalışmalar yapılmış olsa da serbest uzayda ölçüm yapan dedektörlerde başarılı sonuç alınamadı.

2017 yılında Meda ve arkadaşları[219], günümüzde birçok ticari KAD sisteminde kullanılan fiber-pigtailed SPAD'lerde henüz çalışma yapılmadığını fark ederek 2 farklı ticari fiber-pigtailed InGaAs SPAD'de deney gerçekleştirdi. Deneyde, Bob'un dedektörlerinden geri flaş dolayısıyla elde edilen bilginin D_1 için %9.8 , D_2 için %6'a kadar ulaştığı gösterildi. Bu çalışmayı temel alarak 2018 yılında Pinheiro ve arkadaşları[220] bir ticari Si SPAD ve PMT üzerinde deney gerçekleştirip, Si SPAD'de %6.5 veya daha yüksek; ancak PMT'de çok daha az geri flaş oluştuğu gözlemlediler.



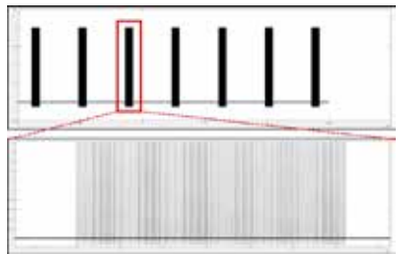
Şekil 9-28Meda 2017 Saldırı Düzeneği[219]



Şekil 9-29Pinheiro 2018 Saldırı Düzeneği[220]

Saldırıdan Bölüm 4.4'te anlatılan Ölçüm Cihaz Bağımsız KAD sistemlerinin kullanılması ile tamamen kaçınılabilmenin yanı sıra, optik izolatörler veya dar dalga boyu geçirgenliğine sahip filtreler kullanılarak Bob'un dedektöründeki geri flaş olasılığı en aza indirilebilir.

9.12 RF Tek İz



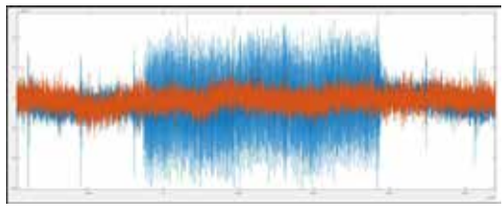
Şekil 9-30Sinyalin elektromanyetik izi

Her elektronik sistemde olduğu gibi KAD sistemlerinde de kullanılan elektronik cihazlar farklı işlemler için farklı güç tüketimleri gerçekleştirmekte, dolayısıyla belirli bir iz bırakmaktadırlar. Saldırı, 2018 yılında bu açığı kullanarak Kim ve arkadaşları[221] tarafından tak ve çalıştır tipi KAD sistemlerinde kullanılan faz modülatörlerine (PM) karşı gerçekleştirilmiştir. PM'lerdeki farklı faz kodlamaları için farklı voltaj değerleri Tablo 9-4'de verilmiştir. Lazer darbesine uygulanan bu voltaj değerleri elektromanyetik yayılıma neden olmaktadır. Saldırılan KAD sisteminde 875 bitlik bir anahtar üretimi için Şekil 9-30'da[221] gösterildiği üzere 7 kez 125'lik darbe üretilmektedir. Bu darbelere uygulanan faz modülasyonu dolayısıyla oluşan elektromanyetik yayılımın karakteristiği LeCroy HDO6104A osiloskop ve Langer LF-R 400 prob ile ortaya çıkartılmıştır.

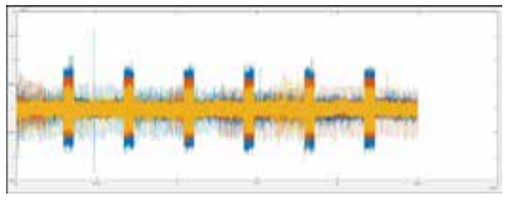
Tablo 9-4Faz Modülatörü Voltaj Değerleri[221]

	0V	2.5V	5V	-2.5V
Bit	0	0	1	1
Taban	+	×	+	×
Faz	0	π/2	π	3π/2

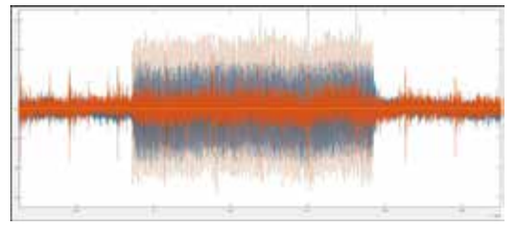
Şekil 9-31 + tabanında 1 bitine ait EM izi[221]



Şekil 9-32 + tabanında 0 ve 1'in EM iz kombinasyonu[221]



Şekil 9-33 x tabanında 0 ve 1'in EM iz kombinasyonu[221]



Şekil 9-34Dört Durumun Beraber Kombinasyonu[221]

Deneyde öncelikle 1, + kübit durumuna denk gelen PM izi incelenip eşik değerleri ortaya çıkartılmış, ardından sırasıyla 0,1 + ve 0,1 x kübit durumlarına karşılık gelen PM izleri incelenmiştir. Son olarak dört farklı faz modülasyonunun rastgele olarak uygulandığı 7x125'lik darbe ile 875bitlik foton darbesi incelenmiştir.

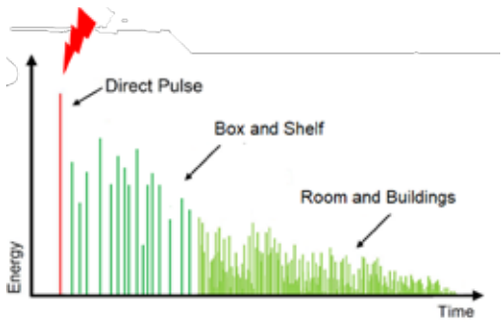
Tablo 9-5 PM Kodlama Karakteristiği

	0	1
+	$0, 2 \times 10^{-4}$	2×10^{-4} - 5×10^{-4}
×	5×10^{-4} - 7×10^{-4}	7×10^{-4} - ∞

Deneyde, her bir durum için eşik ve tepe değerleri çıkartılarak PM'nin modülasyon karakteristiği öğrenilmiştir. Yakalanan sinyaller gürültüden ayrıştırılarak incelenebilirse gönderilen fotonlarına kodlanan kübit durumların öğrenilerek anahtara ulaşılabileceği gösterilmiştir. Saldırıdan KAD sistemlerinde kullanılan elektronik cihazların Faraday kafesi gibi RF korumalı kasalarda kullanımı ile kaçınılabilir.

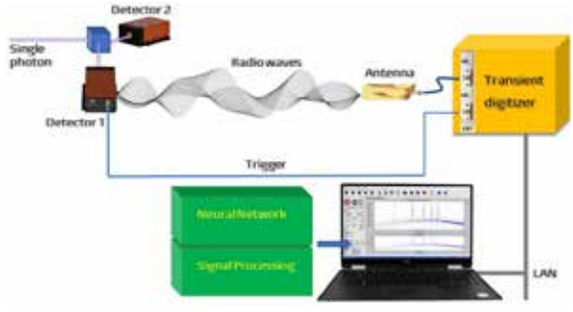
9.13 RF Parmak İzi Saldırısı

RF sinyalleri ile tam olarak gerçekleşmiş ilk saldırı olarak literatüre geçmiştir[222]. Bölüm 6.3'te açıklandığı üzere Geiger Modlu APD'ler günümüzde KAD sistemlerinde yaygın olarak kullanılan SPD çeşididir. Gelen foton APD'de elektron-boşluk çifti oluşturarak çığ etkisini tetiklemekte, ölçüm sonrası çığ etkisi direnç yardımıyla bastırılmakta/söndürülmektedir. Yük taşıyıcılarının hızlanarak oluşturdukları çığ sırasında güçlü olmasa da foton emisyonunun gerçekleştiği 1950'li yıllarda gözlemlenmiş[212, 213], bu durumun KAD sistemlerinde saldırı için kullanılabileceği araştırılmıştır[218]. Elektrodinamik teoriler, bir yükün hızlandığı her durumda uzak alan elektromanyetik radyasyona sahip olduğumuzu göstermekte olduğundan RF sinyali de bekleyebiliriz. Bu sinyal Lienard-Wiechert potansiyeli ile ifade edilebilir. SPAD'den yayılan RF sinyalleri SPD'nin bulunduğu konum, ortam yapısı, koşulları vb. etmenler dolayısıyla Finite Impulse Response (FIR) filtresi gibi davranarak benzersiz bir yanıt oluşturur. Bu durum SPAD'nin parmak izi olarak adlandırılır.

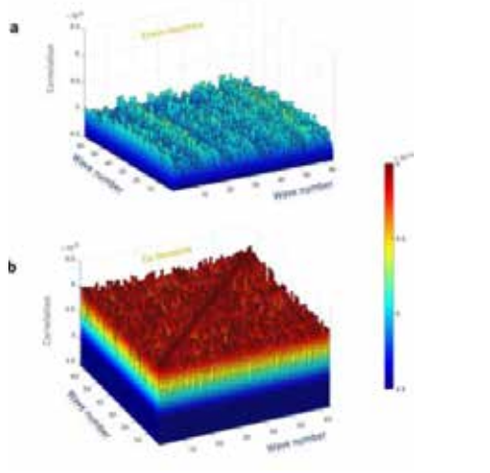


Şekil 9-35SPAD'nin faklı ortam koşullarındaki ham parmak izi[222]

RF sinyallerin karakterizasyonunu ayırt edebilmek için öncelikle Eve'in lazeri ile SPD'lere foton gönderimi sağlanır. Oluşan yüksek voltajlı çığ dolayısıyla SPD'lerden ultra genişbantlı elektromanyetik darbeleri (EMP) ortama yayılır. EMP anten yardımıyla toplanıp gürültüden arındırılır. KAD sisteminde ölçüm için en az iki SPD bulunması gerektiğinden, SPD'ler arası korelasyon da ölçülerek yeterli farklılığın olduğu gözlemlenir. Ardından makine öğrenmesi yardımıyla SPD'lerin parmak izleri nihai olarak tanımlanmış olur. Bu aşamadan sonra Eve lazerini KAD sisteminden ayırır. Alice ve Bob, oluşan QBER dolayısıyla iletişimi belirli bir süre durdursa dahi yeni anahtar oluşumu için tekrar başlatacaktır. Elde edilen parmak izleri sayesinde Eve herhangi bir QBER yaratmadan anahtarı elde edebilecektir.

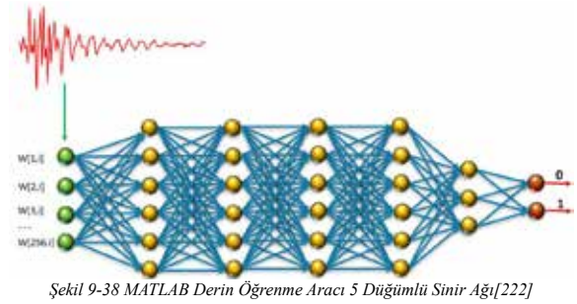


Şekil 9-36Eve Saldırı Düzeneği[222]



Şekil 9-37İki SPD'den yakalanan 64 Dalga Formunun Korelasyonları[222]

Saldırı, BB84 protokolü koşan bir KAD sisteminde aralarında 20 cm bulunan 2 farklı ticari SPD üzerinde başarıyla gösterilmiştir. 2 metre uzaklıktan 7 cm çapında bir Antipodal Vivaldi anteni yardımıyla her bir SPD'den 1GS/s hızda 64 farklı dalga biçimi ve her bir dalga biçimi için 1200 örnek toplanmıştır. Gürültünün temizlenmesiyle 1200 örnek her bir dalga biçimi için 256'ya düşürülmüş, bu örnekler ile SPD'ler arasındaki korelasyon incelenmiş, yeterli farklılık olduğu tespit edildikten sonra örneklem 5 düğümlü sinir ağında makine öğrenmesine tabii tutulmuştur. Makine öğrenmesi sonucunda anten tarafından yakalanan sinyallerin 99.5 doğrulukta tespit edilebildiği başarıyla gösterilmiştir.



Şekil 9-38 MATLAB Derin Öğrenme Aracı 5 Düğümlü Sinir Ağı[222]

Saldırıdan SPD'lerin birbirine olabildiğince yakın konumlandırılması, RF korumalı kasalarda çalıştırılması, ultra genişbant sinyal boğucular kullanılması gibi yöntemlerle kaçınılabilir.

10 Sonuç

Bu derlemede Kuantum Anahtar Dağıtımı (KAD) alanındaki temel kavramları, saldırıları ve son gelişmeleri kapsamlı olarak sundum. Derlemenin odağını KAD saldırılarında tutarken kriptografi ve kuantum alanındaki gelişmelere de dikkat çektim. Teknolojideki son gelişmeler, Shor ve Grover algoritmalarının yakın gelecekte stabil kuantum bilgisayarlarda çalıştırılabileceğini işaret ediyor. Bu tehdide karşı Kuantum Sonrası Kriptografi (KSK) algoritmaları günümüzde yeterli görünüyor. Öte yandan gelecekte kuantum bilgisayarların ulaşabileceği işlem hızı, özellikle çok boyutlu stabil sistemlerin geliştirilebilecek olması dikkate alındığında bilgi güvenliğini tehdit etme potansiyelini devam ettiriyor. Bu nedenle güvenliğini doğa yasalarından alan ve 40 yıl önce "iyi bir fikir" olarak başlayan KAD sistemleri, bugün laboratuvarlardan ticari uygulamalara ve uzay çalışmalarına kadar birçok alanda kuantum sonrası bilgi güvenliğinin sağlanabilmesi için geliştirilmeye devam ediyor.

KAD sistemlerindeki sorunlar Ölçüm Cihaz Bağımsız (ÖCB), E91 gibi farklı protokollerin ve gelişen teknolojiyle mükemmele daha yakın cihazların ortaya çıkışıyla giderilmeye çalışılsa da KAD sistemleri halen "tam güvenli" değil. Dedektörler, KAD sistemleri için ÖCB KAD'ın geliştirilmesiyle "Aşil'in Topuğu" olmaktan çıktı ;ancak mükemmel kuantum durumlarının hazırlanmasındaki problemler, düşük dedektör verimliliği, kuantum röle ve yüksek maliyet gibi sorunlar halen KAD sistemlerinin genel kullanımının önünde aşılmayı bekleyen meydan okumalar olarak duruyor. Son yıllarda yaşanan gelişmeler ve KAD uydu çalışmaları ise kuantum ağlara giden yolda aşılması gereken noktadan noktaya bağlantı uygulamalarının yaygınlaşması hususunda araştırmacıları gelecek yıllar için heyecanlandırıyor.

Mükemmel (loophole-free) donanım cihazları geliştirilene kadar geçmişte olduğu gibi gelecekte de KAD sistemlerinin güvenliğini tehdit eden saldırıların yapılacak ve bu saldırılara önlemler alınmaya devam edilecektir. Öte yandan KAD'ın doğa yasalarıyla korunduğu dikkate alındığında gelişen teknolojiyle beraber saldırganlar bu "kedi-fare" oyununda kaçınılmaz ve ebedi mağlubiyete her geçen gün biraz daha yaklaşmaktadırlar.

11 Kaynakça

1. Singh, S., *The code book: the science of secrecy from ancient Egypt to quantum cryptography*. 2000: Anchor.
2. Yerlikaya, T., E. Buluş, and N. Buluş, *Kripto algoritmalarinin gelişimi ve önemi*. 2006.
3. Shor, P.W. *Algorithms for quantum computation: discrete logarithms and factoring*. in *Proceedings 35th annual symposium on foundations of computer science*. 1994. Ieee.
4. Grover, L.K. *A fast quantum mechanical algorithm for database search*. in *STOC '96*. 1996.
5. Yan, B., et al., *Factoring integers with sublinear resources on a superconducting quantum processor.* arXiv preprint arXiv:2212.12372, 2022.
6. Khattar, T. and N. Yosri, *A comment on" Factoring integers with sublinear resources on a superconducting quantum processor".* arXiv preprint arXiv:2307.09651, 2023.
7. Arute, F., et al., *Quantum supremacy using a programmable superconducting processor.* Nature, 2019. **574**(7779): p. 505-510.
8. Zhong, H.-S., et al., *Quantum computational advantage using photons.* Science, 2020. **370**(6523): p. 1460-1463.
9. Chen, L., et al., *Report on post-quantum cryptography*. Vol. 12. 2016: US Department of Commerce, National Institute of Standards and Technology ….
10. NIST, C., *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. 2016, NIST Gaithersburg, MD, USA.
11. Alagic, G., et al., *Status report on the first round of the NIST post-quantum cryptography standardization process.* 2019.
12. Alagic, G., et al., *Status report on the second round of the NIST post-quantum cryptography standardization process.* US Department of Commerce, NIST, 2020. **2**: p. 69.
13. Alagic, G., et al., *Status report on the third round of the NIST post-quantum cryptography standardization process.* 2022.
14. Heisenberg, W., *Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik.* Zeitschrift für Physik, 1927. **43**(3): p. 172-198.
15. Wootters, W.K. and W.H. Zurek, *A single quantum cannot be cloned.* Nature, 1982. **299**(5886): p. 802-803.
16. Einstein, A., B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Physical Review, 1935. **47**(10): p. 777-780.
17. Schrödinger, E. *Discussion of probability relations between separated systems*. in *Mathematical Proceedings of the Cambridge Philosophical Society*. 1935. Cambridge University Press.
18. Bell, J.S., *On the einstein podolsky rosen paradox.* Physics Physique Fizika, 1964. **1**(3): p. 195.
19. Freedman, S.J. and J.F. Clauser, *Experimental Test of Local Hidden-Variable Theories.* Physical Review Letters, 1972. **28**: p. 938-941.
20. Hensen, B., et al., *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres.* Nature, 2015. **526**(7575): p. 682-6.
21. Apple. *Apple unveils M3, M3 Pro, and M3 Max, the most advanced chips for a personal computer*. 2023 [cited 2024 22/07]; Available from: https://web.archive.org/web/20240721210117/https://www.apple.com/newsroom/2023/10/apple-unveils-m3-m3-pro-and-m3-max-the-most-advanced-chips-for-a-personal-computer/.
22. Moore, G.E., *Cramming more components onto integrated circuits, Reprinted from Electronics, volume 38, number 8, April 19, 1965, pp. 114 ff.* IEEE solid-state circuits society newsletter, 2006. **11**(3): p. 33-35.
23. Wiesner, S., *Conjugate coding.* SIGACT News, 1983. **15**(1): p. 78–88.
24. Schumacher, B., *Quantum coding.* Physical Review A, 1995. **51**(4): p. 2738.
25. Dirac, P.A.M. *A new notation for quantum mechanics*. in *Mathematical Proceedings of the Cambridge Philosophical Society*. 1939. Cambridge University Press.
26. Wong, T.G., *Introduction to Classical and Quantum Computing*. 2022: Rooted Grove.
27. Thorlabs. *Using the Poincare Sphere to Represent the Polarization State*. 2020 [cited 2024 22/07]; Available from: https://web.archive.org/web/20240721220956/https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=14200.
28. Bennett, C.H., *Quantum cryptography using any two nonorthogonal states.* Physical review letters, 1992. **68**(21): p. 3121.
29. Rabin, M.O., *How To Exchange Secrets with Oblivious Transfer.* IACR Cryptol. ePrint Arch., 2005. **2005**: p. 187.
30. Ekert, A.K., *Quantum cryptography based on Bell's theorem.* Physical review letters, 1991. **67**(6): p. 661.

31. Bennett, C.H., G. Brassard, and N.D. Mermin, *Quantum cryptography without Bell's theorem.* Physical Review Letters, 1992. **68**(5): p. 557-559.

32. Scarani, V., et al., *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations.* Physical Review Letters, 2004. **92**(5).

33. Bruß, D., *Optimal Eavesdropping in Quantum Cryptography with Six States.* Physical Review Letters, 1998. **81**(14): p. 3018-3021.

34. Zhang, Y., et al., *Continuous-variable quantum key distribution system: A review and perspective.* arXiv preprint arXiv:2310.04831, 2023.

35. Cao, Y., et al., *The evolution of quantum key distribution networks: On the road to the qinternet.* IEEE Communications Surveys & Tutorials, 2022. **24**(2): p. 839-894.

36. Sharma, P., et al., *Quantum key distribution secured optical networks: A survey.* IEEE Open Journal of the Communications Society, 2021. **2**: p. 2049-2083.

37. Wehner, S., D. Elkouss, and R. Hanson, *Quantum internet: A vision for the road ahead.* Science, 2018. **362**(6412): p. eaam9288.

38. Azuma, K., et al., *Quantum repeaters: From quantum networks to the quantum internet.* Reviews of Modern Physics, 2023. **95**(4): p. 045006.

39. Adnan, M.H., Z. Ahmad Zukarnain, and N.Z. Harun, *Quantum key distribution for 5G networks: A review, State of Art and Future Directions.* Future Internet, 2022. **14**(3): p. 73.

40. Bennett, C.H. and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing.* Theoretical computer science, 2014. **560**: p. 7-11.

41. Pljonkin, A. *Interface of the Quantum Key Distribution System*. in *WRAP 2017-Workshop on Recent Advances in Photonics*. 2018.

42. Tang, Z. *Measurement-Device-Independent Quantum Cryptography*. 2016.

43. Gottesman, D. and H.-K. Lo, *Proof of security of quantum key distribution with two-way classical communications.* IEEE Transactions on Information Theory, 2003. **49**(2): p. 457-475.

44. Mavroeidis, V., et al., *The impact of quantum computing on present cryptography.* arXiv preprint arXiv:1804.00200, 2018.

45. Bechmann-Pasquinucci, H. and N. Gisin, *Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography.* Physical Review A, 1999. **59**(6): p. 4238-4248.

46. Wolf, R. and R. Wolf, *Quantum key distribution protocols.* Quantum Key Distribution: An Introduction with Exercises, 2021: p. 91-116.

47. Hwang, W.-Y., *Quantum Key Distribution with High Loss: Toward Global Secure Communication.* Physical Review Letters, 2003. **91**(5): p. 057901.

48. Zhao, Y., et al., *Experimental Quantum Key Distribution with Decoy States.* Physical Review Letters, 2006. **96**(7): p. 070502.

49. Peng, C.-Z., et al., *Experimental long-distance decoy-state quantum key distribution based on polarization encoding.* Physical review letters, 2007. **98**(1): p. 010505.

50. Mayers, D. and A. Yao. *Quantum cryptography with imperfect apparatus*. in *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*. 1998. IEEE.

51. Barrett, J., L. Hardy, and A. Kent, *No signaling and quantum key distribution.* Physical review letters, 2005. **95**(1): p. 010503.

52. Acín, A., et al., *Device-independent security of quantum cryptography against collective attacks.* Physical Review Letters, 2007. **98**(23): p. 230501.

53. Biham, E., B. Huttner, and T. Mor, *Quantum cryptographic network based on quantum memories.* Physical Review A, 1996. **54**(4): p. 2651.

54. Inamori, H., *Security of practical time-reversed EPR quantum key distribution.* Algorithmica, 2002. **34**(4): p. 340-365.

55. Lo, H.-K., M. Curty, and B. Qi, *Measurement-device-independent quantum key distribution.* Physical review letters, 2012. **108**(13): p. 130503.

56. Ma, X. and M. Razavi, *Alternative schemes for measurement-device-independent quantum key distribution.* Physical Review A, 2012. **86**(6): p. 062319.

57. Liu, Y., et al., *Experimental measurement-device-independent quantum key distribution.* Physical review letters, 2013. **111**(13): p. 130502.

58. Rubenok, A., et al., *Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks.* Physical review letters, 2013. **111**(13): p. 130501.

59. Da Silva, T.F., et al., *Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits.* Physical Review A, 2013. **88**(5): p. 052303.

60. Tang, Z., et al., *Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution.* Physical review letters, 2014. **112**(19): p. 190503.

61. Liu, Y., et al. *Experimental Realization of Measurement Device Independent Quantum Key Distribution*. in *CLEO: 2013*. 2013. San Jose, California: Optica Publishing Group.

62. Kaneda, F., et al., *Quantum-memory-assisted multi-photon generation for efficient quantum information processing.* Optica, 2017. **4**(9): p. 1034-1037.

63. Tang, Y.-L., et al., *Measurement-device-independent quantum key distribution over untrustful*

metropolitan network. Physical Review X, 2016. **6**(1): p. 011024.

64. Bloom, S., et al., *Understanding the performance of free-space optics.* Journal of optical Networking, 2003. **2**(6): p. 178-200.

65. Bhaskar, M.K., et al., *Experimental demonstration of memory-enhanced quantum communication.* Nature, 2020. **580**(7801): p. 60-64.

66. Pittaluga, M., et al., *600-km repeater-like quantum communications with dual-band stabilization.* Nature Photonics, 2021. **15**(7): p. 530-535.

67. Wang, S., et al., *Twin-field quantum key distribution over 830-km fibre.* Nature Photonics, 2022. **16**(2): p. 154-161.

68. Amer, O., V. Garg, and W.O. Krawec, *An introduction to practical quantum key distribution.* IEEE Aerospace and Electronic Systems Magazine, 2021. **36**(3): p. 30-55.

69. Shor, P.W. and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol.* Physical Review Letters, 2000. **85**: p. 441-444.

70. Fuchs, C.A., et al., *Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy.* Physical Review A, 1997. **56**(2): p. 1163.

71. Herrero-Collantes, M. and J.C. Garcia-Escartin, *Quantum random number generators.* Reviews of Modern Physics, 2017. **89**(1): p. 015004.

72. Stipčević, M. and Ç.K. Koç, *True random number generators*, in *Open Problems in Mathematics and Computational Science*. 2014, Springer. p. 275-315.

73. Ma, X., et al., *Quantum random number generation.* npj Quantum Information, 2016. **2**(1): p. 1-9.

74. Mannalatha, V., S. Mishra, and A. Pathak, *A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness.* Quantum Information Processing, 2023. **22**(12): p. 1-45.

75. Alkassar, A., T. Nicolay, and M. Rohe. *Obtaining true-random binary numbers from a weak radioactive source*. in *International conference on computational science and its applications*. 2005. Springer.

76. Schottky, W., *Über spontane Stromschwankungen in verschiedenen Elektrizitätsleitern.* Annalen der physik, 1918. **362**(23): p. 541-567.

77. Nyquist, H., *Thermal agitation of electric charge in conductors.* Physical review, 1928. **32**(1): p. 110.

78. Pironio, S., et al., *Random numbers certified by Bell's theorem.* Nature, 2010. **464**(7291): p. 1021-1024.

79. Katsoprinakis, G., et al., *Quantum random number generator based on spin noise.* Physical Review A, 2008. **77**(5): p. 054101.

80. Thorlabs. *Thorlabs* 2024 [cited 2024 21/07]; Available from: https://www.thorlabs.de/newgrouppage9.cfm?objectgroup_id=9028.

81. Hong, C.-K., Z.-Y. Ou, and L. Mandel, *Measurement of subpicosecond time intervals between two photons by interference.* Physical review letters, 1987. **59**(18): p. 2044.

82. *Quantis AIS31 Validated RNG*. 2020 [cited 2024 21/07]; Available from: https://web.archive.org/web/20200415092817/https://www.idquantique.com/random-number-generation/products/quantis-ais-31/.

83. Hertz, H., *Ueber einen Einfluss des ultravioletten Lichtes auf die electrische Entladung.* Annalen der Physik, 1887. **267**(8): p. 983-1000.

84. Austin, L. and H. Starke, *Ueber die Reflexion der Kathodenstrahlen und eine damit verbundene neue Erscheinung secundärer Emission.* Annalen der Physik, 1902. **314**(10): p. 271-292.

85. Zworykin, V., G. Morton, and L. Malter, *The secondary emission multiplier-a new electronic device.* Proceedings of the Institute of Radio Engineers, 1936. **24**(3): p. 351-375.

86. Lubsandorzhiev, B.K., *On the history of photomultiplier tube invention.* Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 2006. **567**(1): p. 236-238.

87. Becker, W., *Advanced Time-Correlated Single Photon Counting Techniques*, ed. A.W. Castleman, J.P. Toennies, and W. Zinth.

88. Ceccarelli, F., et al., *Recent advances and future perspectives of single-photon avalanche diodes for quantum photonics applications.* Advanced Quantum Technologies, 2021. **4**(2): p. 2000102.

89. Ghioni, M., et al., *Progress in silicon single-photon avalanche diodes.* IEEE Journal of selected topics in quantum electronics, 2007. **13**(4): p. 852-862.

90. Cusini, I., et al., *Historical Perspectives, State of art and Research Trends of Single Photon Avalanche Diodes and Their Applications (Part 1: Single Pixels).* Frontiers in Physics, 2022: p. 607.

91. Amiri, I., et al., *Temperature effects on characteristics and performance of near-infrared wide bandwidth for different avalanche photodiodes structures.* Results in Physics, 2019. **14**: p. 102399.

92. Gupta, K.M. and N. Gupta, *Advanced Semiconducting Materials and Devices*. 2016: Springer International Publishing.

93. A. Ghassemi, K.S., K. Kobayashi. *MPPC*. 2022 [cited 2024 21/07]; Available from: https://web.archive.org/web/20240721204630/https://www.hamamatsu.com/content/dam/hamamatsu-photonics/sites/documents/99_SALES_LIBRARY/ssd/mppc_kapd9005e.pdf.

94. Cova, S., et al., *Avalanche photodiodes and*

quenching circuits for single-photon detection. Applied optics, 1996. **35**(12): p. 1956-1976.

95. Champlin, K.S., *Microplasma fluctuations in silicon.* Journal of Applied Physics, 1959. **30**(7): p. 1039-1050.

96. Haitz, R.H., et al., *Avalanche effects in silicon p—n junctions. I. Localized photomultiplication studies on microplasmas.* Journal of applied physics, 1963. **34**(6): p. 1581-1590.

97. Haitz, R.H., *Mechanisms contributing to the noise pulse rate of avalanche diodes.* Journal of Applied Physics, 1965. **36**(10): p. 3123-3131.

98. Webb, P. and R. McIntyre. *Single photon detection with avalanche photodiodes*. in *Bulletin of the American Physical Society*. 1970. AMER INST PHYSICS CIRCULATION FULFILLMENT DIV, 500 SUNNYSIDE BLVD, WOODBURY ….

99. Webb, P., *Properties of avalanche photodiodes.* RCA review, 1974. **35**: p. 234.

100. Dautet, H., et al., *Photon counting techniques with silicon avalanche photodiodes.* Applied optics, 1993. **32**(21): p. 3894-3900.

101. McIntyre, R.J., *Silicon avalanche photodiode with low multiplication noise*. 1990, Google Patents.

102. McIntyre, R.J. and P.P. Webb, *Low-noise, reach-through, avalanche photodiodes*. 1996, Google Patents.

103. Inc, T. *InGaAs Photodiodes*. 2020 [cited 2024 22/07]; Available from: https://www.thorlabs.com/drawings/1413919b38b38188-92FBBCEE-E338-9094-34937538F04D38EF/APD430C-Manual.pdf.

104. Quantique, I. *Photon Counting for Brainies*. 2019 [cited 2024 21/07]; Available from: https://web.archive.org/web/20240616084325/https://marketing.idquantique.com/acton/attachment/11868/f-006e/1/-/-/-/-/Photon_counting_for_Brainies.pdf.

105. Itzler, M.A., et al., *Single photon avalanche diodes (SPADs) for 1.5 μ m photon counting applications.* Journal of modern optics, 2007. **54**(2-3): p. 283-304.

106. Nishida, K., K. Taguchi, and Y. Matsumoto, *InGaAsP heterostructure avalanche photodiodes with high avalanche gain.* Applied Physics Letters, 1979. **35**(3): p. 251-253.

107. Zhang, J., et al., *Advances in InGaAs/InP single-photon detector systems for quantum communication.* Light: Science & Applications, 2015. **4**(5): p. e286-e286.

108. Gottesman, D. and I. Chuang *Quantum Digital Signatures*. 2001. quant-ph/0105032.

109. Clarke, P.J., et al., *Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light.* Nature communications, 2012. **3**(1): p. 1174.

110. Dunjko, V., P. Wallden, and E. Andersson, *Quantum digital signatures without quantum memory.* Physical review letters, 2014. **112**(4): p. 040502.

111. Collins, R.J., et al., *Realization of Quantum Digital Signatures without the Requirement of Quantum Memory.* Physical Review Letters, 2014. **113**(4): p. 040502.

112. Wallden, P., et al., *Quantum digital signatures with quantum-key-distribution components.* Physical Review A, 2015. **91**(4): p. 042304.

113. Croal, C., et al., *Free-space quantum signatures using heterodyne measurements.* Physical review letters, 2016. **117**(10): p. 100503.

114. Amiri, R., et al., *Secure quantum signatures using insecure quantum channels.* Physical Review A, 2016. **93**(3): p. 032325.

115. Yin, H.-L., Y. Fu, and Z.-B. Chen, *Practical quantum digital signature.* Physical Review A, 2016. **93**(3): p. 032316.

116. Puthoor, I.V., et al., *Measurement-device-independent quantum digital signatures.* Physical Review A, 2016. **94**(2): p. 022328.

117. Roberts, G.L., et al., *Experimental measurement-device-independent quantum digital signatures.* Nature Communications, 2017. **8**(1): p. 1098.

118. Yin, H.-L., et al., *Experimental measurement-device-independent quantum digital signatures over a metropolitan network.* Physical Review A, 2017. **95**(4): p. 042338.

119. Pelet, Y., et al., *Unconditionally secure digital signatures implemented in an eight-user quantum network.* New journal of physics, 2022. **24**(9): p. 093038.

120. Yin, H.-L., et al., *Experimental quantum secure network with digital signatures and encryption.* National Science Review, 2022. **10**(4).

121. Cao, X.-Y., et al., *Experimental quantum e-commerce.* Science Advances, 2024. **10**(2): p. eadk3258.

122. Yin, H.-L., et al., *Experimental quantum digital signature over 102 km.* Physical Review A, 2017. **95**(3): p. 032334.

123. Ding, H.-J., et al., *280-km experimental demonstration of a quantum digital signature with one decoy state.* Optics Letters, 2020. **45**(7): p. 1711-1714.

124. An, X.-B., et al., *Practical quantum digital signature with a gigahertz BB84 quantum key distribution system.* Optics Letters, 2019. **44**(1): p. 139-142.

125. Bennett, C.H. and G. Brassard, *Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working].* SIGACT News, 1989. **20**(4): p. 78–80.

126. Bennett, C.H., et al., *Experimental quantum cryptography.* Journal of Cryptology, 1992. **5**(1): p. 3-28.

127. Townsend, P.D., J.G. Rarity, and P.R. Tapster, *Single photon interference in 10 km long optical fibre interferometer.* Electronics Letters, 1993. **29**: p. 634-635.

128. Jacobs, B. and J. Franson, *Quantum cryptography in free space.* Optics Letters, 1996. **21**(22): p. 1854-1856.

129. Elliott, C., et al. *Current status of the DARPA quantum network*. in *Quantum Information and computation III*. 2005. SPIE.

130. Peev, M., et al., *The SECOQC quantum key distribution network in Vienna.* New Journal of Physics, 2009. **11**(7): p. 075001.

131. Paul, R., *Geneva brings quantum cryptography to internet voting.* Ars Technica, October, 2007. **12**.

132. Sasaki, M., et al., *Field test of quantum key distribution in the Tokyo QKD Network.* Optics Express, 2011. **19**(11): p. 10387-10409.

133. Chen, Y.-A., et al., *An integrated space-to-ground quantum communication network over 4,600 kilometres.* Nature, 2021. **589**(7841): p. 214-219.

134. Chen, T.-Y., et al., *Implementation of a 46-node quantum metropolitan area network.* npj Quantum Information, 2021. **7**(1): p. 134.

135. Nauerth, S., et al., *Air-to-ground quantum communication.* Nature Photonics, 2013. **7**(5): p. 382-386.

136. Wang, J.-Y., et al., *Direct and full-scale experimental verifications towards ground–satellite quantum key distribution.* Nature Photonics, 2013. **7**(5): p. 387-393.

137. Liao, S.-K., et al., *Satellite-to-ground quantum key distribution.* Nature, 2017. **549**(7670): p. 43-47.

138. Yin, J., et al., *Entanglement-based secure quantum cryptography over 1,120 kilometres.* Nature, 2020. **582**(7813): p. 501-505.

139. Liao, S.-K., et al., *Satellite-Relayed Intercontinental Quantum Network.* Physical Review Letters, 2018. **120**(3): p. 030501.

140. Gibney, E., *One giant step for quantum internet.* Nature, 2016. **535**(7613): p. 478-479.

141. Carmack, D., *Beating China in the Race for Quantum Supremacy.*

142. Kaur, M., *Overview of Quantum Initiatives Worldwide 2023.* Qureca. Accessed: Nov, 2023. **16**.

143. Heidt, H., et al., *CubeSat: A new generation of picosatellite for education and industry low-cost space experimentation.* 2000.

144. Krebs, G.D. *SOCRATES*. 2024 [cited 2024 21/07]; Available from: https://web.archive.org/web/20240301095646/https://space.skyrocket.de/doc_sdat/socrates.htm#citation.

145. Takenaka, H., et al., *Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite.* Nature photonics, 2017. **11**(8): p. 502-508.

146. Tang, Z., et al., *The photon pair source that survived a rocket explosion.* Scientific reports, 2016. **6**(1): p. 25603.

147. Chandrasekara, R., et al. *Generation and analysis of correlated pairs of photons on board a nanosatellite*. in *Quantum Information Science and Technology II*. 2016. SPIE.

148. Grieve, J.A., et al., *SpooQySats: CubeSats to demonstrate quantum key distribution technologies.* Acta Astronautica, 2018. **151**: p. 103-106.

149. Villar, A., et al., *Entanglement demonstration on board a nano-satellite.* Optica, 2020. **7**(7): p. 734-737.

150. Oi, D.K., et al., *CubeSat quantum communications mission.* EPJ Quantum Technology, 2017. **4**: p. 1-20.

151. Bedington, R., J.M. Arrazola, and A. Ling, *Progress in satellite quantum key distribution.* npj Quantum Information, 2017. **3**(1): p. 30.

152. Sidhu, J.S., et al., *Advances in space quantum communications.* IET Quantum Communication, 2021. **2**(4): p. 182-217.

153. Lu, C.-Y., et al., *Micius quantum experiments in space.* Reviews of Modern Physics, 2022. **94**(3): p. 035001.

154. Jennewein, T., et al., *QEYSSat 2.0--White Paper on Satellite-based Quantum Communication Missions in Canada.* arXiv preprint arXiv:2306.02481, 2023.

155. Mujumdar, S., V. Bhat, and R. Chatterjee, *A brief review of free-space quantum key distribution experiments towards satellite QKD.* Asian Journal of Physics Vol, 2022. **31**(3-6): p. 577-591.

156. Xu, F., et al., *Secure quantum key distribution with realistic devices.* Reviews of Modern Physics, 2020. **92**(2): p. 025002.

157. Jain, N., et al., *Attacks on practical quantum key distribution systems (and how to prevent them).* Contemporary Physics, 2016. **57**(3): p. 366-387.

158. Sun, S. and A. Huang, *A review of security evaluation of practical quantum key distribution system.* Entropy, 2022. **24**(2): p. 260.

159. Brassard, G., et al., *Limitations on Practical Quantum Cryptography.* Physical Review Letters, 2000. **85**(6): p. 1330-1333.

160. Lütkenhaus, N., *Security against individual attacks for realistic quantum key distribution.* Physical Review A, 2000. **61**(5): p. 052304.

161. Félix, S., et al., *Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses.* Journal of Modern Optics, 2001. **48**(13): p. 2009-2021.

162. Gottesman, D., et al. *Security of quantum key*

distribution with imperfect devices. in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.* 2004. IEEE.

163. Liu, W.-T., et al., *Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution.* Physical Review A, 2011. **83**(4): p. 042326.

164. Vakhitov, A., V. Makarov, and D.R. Hjelme, *Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography.* Journal of modern optics, 2001. **48**(13): p. 2023-2038.

165. Gisin, N., et al., *Trojan-horse attacks on quantum-key-distribution systems.* Physical Review A, 2006. **73**(2): p. 022320.

166. Jain, N., et al., *Trojan-horse attacks threaten the security of practical quantum cryptography.* New Journal of Physics, 2014. **16**(12): p. 123030.

167. Sajeed, S., et al., *Invisible Trojan-horse attack.* Scientific reports, 2017. **7**(1): p. 8403.

168. Stiller, B., et al. *Quantum hacking of continuous-variable quantum key distribution systems: realtime Trojan-horse attacks*. in *2015 Conference on Lasers and Electro-Optics (CLEO)*. 2015. IEEE.

169. Muller, A., et al., *"Plug and play" systems for quantum cryptography.* Applied physics letters, 1997. **70**(7): p. 793-795.

170. Stucki, D., et al., *Quantum key distribution over 67 km with a plug&play system.* New Journal of Physics, 2002. **4**(1): p. 41.

171. Sajeed, S., et al., *Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing.* Physical Review A, 2015. **91**(3): p. 032326.

172. Makarov*, V. and D.R. Hjelme, *Faked states attack on quantum cryptosystems.* Journal of Modern Optics, 2005. **52**(5): p. 691-705.

173. Qi, B., et al., *Time-shift attack in practical quantum cryptosystems.* arXiv preprint quant-ph/0512080, 2005.

174. Zhao, Y., et al., *Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems.* Physical Review A, 2008. **78**(4): p. 042333.

175. Makarov, V., *Controlling passively quenched single photon detectors by bright light.* New Journal of Physics, 2009. **11**(6): p. 065003.

176. Lydersen, L., et al., *Hacking commercial quantum cryptography systems by tailored bright illumination.* Nature photonics, 2010. **4**(10): p. 686-689.

177. Gerhardt, I., et al., *Full-field implementation of a perfect eavesdropper on a quantum cryptography system.* Nature communications, 2011. **2**(1): p. 349.

178. Sauge, S., et al., *Controlling an actively-quenched single photon detector with bright light.* Optics Express, 2011. **19**(23): p. 23590-23600.

179. Lydersen, L., et al., *Thermal blinding of gated detectors in quantum cryptography.* Optics express, 2010. **18**(26): p. 27938-27954.

180. Wiechers, C., et al., *After-gate attack on a quantum cryptosystem.* New Journal of Physics, 2011. **13**(1): p. 013043.

181. Gras, G., et al., *Optical control of single-photon negative-feedback avalanche diode detector.* Journal of Applied Physics, 2020. **127**(9).

182. Wu, Z., et al., *Hacking single-photon avalanche detectors in quantum key distribution via pulse illumination.* Optics Express, 2020. **28**(17): p. 25574-25590.

183. Gao, B., et al., *Strong pulse illumination hacks self-differencing avalanche photodiode detectors in a high-speed quantum key distribution system.* arXiv preprint arXiv:2205.04177, 2022.

184. Lydersen, L., et al., *Controlling a superconducting nanowire single-photon detector using tailored bright illumination.* New Journal of Physics, 2011. **13**(11): p. 113042.

185. Lydersen, L., V. Makarov, and J. Skaar, *Secure gated detection scheme for quantum cryptography.* Physical Review A, 2011. **83**(3): p. 032306.

186. Lydersen, L., et al., *Superlinear threshold detectors in quantum cryptography.* Physical Review A, 2011. **84**(3): p. 032320.

187. Yuan, Z., J.F. Dynes, and A.J. Shields, *Avoiding the blinding attack in QKD.* Nature Photonics, 2010. **4**(12): p. 800-801.

188. Yuan, Z., J. Dynes, and A. Shields, *Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography.* Applied physics letters, 2011. **98**(23).

189. da Silva, T.F., et al., *Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems.* Optics express, 2012. **20**(17): p. 18911-18924.

190. Qian, Y.-J., et al., *Robust countermeasure against detector control attack in a practical quantum key distribution system.* Optica, 2019. **6**(9): p. 1178-1184.

191. Wu, Z., et al., *Robust countermeasure against detector control attack in a practical quantum key distribution system: comment.* Optica, 2020. **7**(10): p. 1391-1393.

192. He, D.-Y., et al., *Robust countermeasure against detector control attack in a practical quantum key distribution system: reply.* Optica, 2020. **7**(10): p. 1415-1416.

193. Acheva, P., et al., *Automated verification of countermeasure against detector-control attack in quantum key distribution.* EPJ Quantum Technology, 2023. **10**(1): p. 1-16.

194. Eisenmann, M. and E. Weidel, *Single-mode fused biconical coupler optimized for polarization*

beamsplitting. Journal of lightwave technology, 1991. **9**(7): p. 853-858.

195. Lee, Y., et al., *Characteristics of a multi-mode interference device based on Ti: LiNbO 3 channel waveguide.* Optics Express, 2009. **17**(13): p. 10718-10724.

196. Li, H.-W., et al., *Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources.* Physical Review A, 2011. **84**(6): p. 062308.

197. Huang, J.-Z., et al., *Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack.* Physical Review A, 2013. **87**(6): p. 062329.

198. Du, G.-H., et al., *Attacking a high-dimensional quantum key distribution system with wavelength-dependent beam splitter.* Chinese Physics B, 2019. **28**(9): p. 090301.

199. Li, D.-D., et al. *Security of optical beam splitter in quantum key distribution*. in *Photonics*. 2022. MDPI.

200. Fung, C.-H.F., et al., *Phase-remapping attack in practical quantum-key-distribution systems.* Physical Review A, 2007. **75**(3): p. 032314.

201. Xu, F., B. Qi, and H.-K. Lo, *Experimental demonstration of phase-remapping attack in a practical quantum key distribution system.* New Journal of Physics, 2010. **12**(11): p. 113026.

202. Yariv, A., P. Yeh, and A. Yariv, *Photonics: optical electronics in modern communications*. Vol. 6. 2007: Oxford university press New York.

203. Bugge, A.N., et al., *Laser damage helps the eavesdropper in quantum cryptography.* Physical review letters, 2014. **112**(7): p. 070503.

204. Makarov, V., et al., *Creation of backdoors in quantum communications via laser damage.* Physical Review A, 2016. **94**(3): p. 030302.

205. Huang, A., et al., *Laser-damage attack against optical attenuators in quantum key distribution.* Physical Review Applied, 2020. **13**(3): p. 034017.

206. Ponosova, A., et al., *Protecting fiber-optic quantum key distribution sources against light-injection attacks.* PRX Quantum, 2022. **3**(4): p. 040307.

207. Todoroki, S.-i. and S. Inoue, *Observation of blowing out in low loss passive optical fuse formed in silica glass optical fiber circuit.* Japanese journal of applied physics, 2004. **43**(6A): p. L728.

208. Bennett, C. *Let Eve do the heavy lifting, while John and Won-Young keep her honest*. 2011 [cited 2024 22/07]; Available from: https://web.archive.org/web/20240721210757/https://dabacon.org/pontiff/2011/10/20/let-eve-do-the-heavy-lifting-while-john-and-won-young-keep-her-honest/.

209. Tang, Y.-L., et al., *Source attack of decoy-state quantum key distribution using phase information.* Physical Review A, 2013. **88**(2): p. 022308.

210. Sun, S.-H., et al., *Effect of source tampering in the security of quantum cryptography.* Physical Review A, 2015. **92**(2): p. 022304.

211. Huang, A., et al., *Laser-seeding attack in quantum key distribution.* Physical Review Applied, 2019. **12**(6): p. 064043.

212. Newman, R., *Visible light from a silicon p− n junction.* Physical review, 1955. **100**(2): p. 700.

213. Chynoweth, A. and K. McKay, *Photon emission from avalanche breakdown in silicon.* Physical Review, 1956. **102**(2): p. 369.

214. Waldschmidt, M. and S. Wittig, *Backscattering and bremsstrahlung of electrons in a silicon detector.* Nuclear Instruments and Methods, 1968. **64**(2): p. 189-191.

215. Lacaita, A., et al., *Photon-assisted avalanche spreading in reach-through photodiodes.* Applied physics letters, 1993. **62**(6): p. 606-608.

216. Akil, N., et al., *Photon generation by silicon diodes in avalanche breakdown.* Applied Physics Letters, 1998. **73**(7): p. 871-872.

217. Huang, T., et al., *Photon emission characteristics of avalanche photodiodes.* Optical Engineering, 2005. **44**(7): p. 074001-074001-4.

218. Kurtsiefer, C., et al., *The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?* Journal of Modern Optics, 2001. **48**(13): p. 2039-2047.

219. Meda, A., et al., *Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution.* Light: Science & Applications, 2017. **6**(6): p. e16261-e16261.

220. Pinheiro, P.V.P., et al., *Eavesdropping and countermeasures for backflash side channel in quantum cryptography.* Optics express, 2018. **26**(16): p. 21020-21032.

221. Kim, S., et al. *Single trace side channel analysis on quantum key distribution*. in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*. 2018. IEEE.

222. Durak, K., N.C. Jam, and S. Karamzadeh, *Attack to quantum cryptosystems through RF fingerprints from photon detectors.* IEEE Journal of Selected Topics in Quantum Electronics, 2021. **28**(2: Optical Detectors): p. 1-7.

Özgeçmişler

Derin Akata, 2018 yılında İstanbul Ticaret Üniversitesi Endüstri Mühendisliği bölümünden lisans, 2022 yılında Marmara Üniversitesi Fen Bilimleri Enstitüsü Siber Güvenlik Anabilim Dalı'ndan tezsiz yüksek lisans derecelerini almıştır.
2019-2020 yılları arasında ASPİLSAN Enerji bünyesinde savunma sanayi projelerinde çalışmıştır.
2020-2023 yılları arasında Hyperion Technologies firmasında, NATO STO-CMRE tarafından fonlanan Sualtı Kuantum Anahtar Dağıtım Sistemi projesi başta olmak üzere optik kablosuz haberleşme sistemlerine yönelik projelerde proje yöneticiliği yapmıştır.
Halen bilgi teknolojileri alanında proje yöneticisi olarak kariyerine devam etmektedir.