BB84 Kuantum Anahtar Değişim Protokolünün Benzetimi ve Saldırı Analizi

Simulation of BB84 Quantum Key Exchange Protocol and Attack Analysis

İlker Burak Adıyaman
Gebze Teknik Universitesi
Bilgisayar Mühendisliği Bölümü
iadiyaman@gtu.edu.tr

İbrahim Soğukpınar
Gebze Teknik Universitesi
Bilgisayar Mühendisliği Bölümü
ispinar@gtu.edu.tr

***Öz*—Kuantum anahtar dağıtımı protokollerinin temel amacı şifrelemede kullanılan tek kullanımlık anahtarın gönderici ve alıcı tarafında pratik ve güvenli bir şekilde iletimini sağlamaktır. Klasik yöntemde her iki taraf da anahtarın bir saldırgan tarafından ele geçirilmediğinden emin olamaz. Kuantum anahtar değişim yöntemi ise, temelde kuantum fiziğine dayandığından klasik anahtar dağıtım yöntemlerine göre daha yüksek güvenlik sağlamaktadır. Bu çalışmada kuantum anahtar dağıtım (KAD) protokollerinden ilk ve en çok kullanılan BB84 protokolü ile alıcı ve gönderici arasında anahtar dağıtımı sırasında saldırganın anahtarı elde etmeye çalışması durumu dikkate alınarak benzetim ortamında gerçekleştirilmiştir. Son bölümde elde edilen sonuç verileri analiz edilerek gelecek çalışmalar için önerilerde bulunulmuştur.**

Anahtar Sözcükler — kuantum anahtar dağıtım protokolleri, QKD, kuantum iletişimi, BB84, yakala/tekrar gönder saldırısı, kuantum atakları.

***Abstract*—The main purpose of quantum key distribution protocols is to provide a practical and secure transmission of the single-use key used in encryption at the sender and receiver side. In the classical method, both parties cannot be sure that the key has not been taken over by an attacker. Since the quantum key exchange method basically relies on quantum physics, it provides higher security than conventional key distribution methods. In this study, the first and most used BB84 protocol, which is one of the quantum key distribution (QKD) protocols, and the distribution of the key between the receiver and the sender in the simulation environment and the attempt of the attacker to achieve the key was performed in the simulation environment. The results obtained in the last section are analyzed and suggestions are made for future studies.**

Keywords — quantum key exchange protocols, QKD, quantum communication, BB84, intercept/resend attack, quantum attacks.

I. GİRİŞ

Kuantum kriptografi tekniğinde veri iletimi klasik yöntem olan elektriksel işaretler yerine fotonlar ile yapılmaktadır [16] ve temel olarak alıcı ile gönderici arasındaki fotonların durumlarının iletimine dayanmaktadır. Kuantum durumu fotonların polarizasyon adı verilen fiziksel karakterlerini temsil eder. Aynı zamanda anahtarı alıcıya göndermek için foton üreteci tabancalara ve kristal süzgeçlere ihtiyaç vardır. Anahtar iletişimi fotonun baz alınan bir sisteme (filtre) göre herhangi bir açıyla polarize olma özelliğinden faydalanılır. Fotonların dikeyde veya yatayda polarize olması için kristal süzgeç çiftleri kullanılmaktadır. İletimin güvenli bir şekilde tamamlanabilmesi için kuantum kanal ve açık kanal olmak üzere iki kanal kullanılmaktadır. Kuantum şifrelemenin temeli Heinsberg'in belirsizlik ilkesine [17] dayanmaktadır. Buna göre fotonunun dönüş, kutuplanma özellikleri ölçülmek istendiğinde foton değişim gösterir ve bu da iletişim esnasında aradaki dinleyicinin tespit edilmesini sağlar.

Kuantum anahtar değişim protokolünü kullanan ağlar ekstra güvenlik sağlıyor olsalar da bu ağlara karşı geliştirilen birtakım saldırı stratejileri mevcuttur. Foton bölme saldırısı, yakala/tekrar gönder saldırısı, sahte durum saldırısı, zaman kaydırma atağı bunlardan birkaçıdır.

Bu çalışmada gönderici (Ayşe) ve alıcı (Bora) arasında BB84 kuantum anahtar değişimi benzetim ortamında gerçekleştirilmiş, arada yakala/tekrar gönder atağı yapan saldırganın olması durumunda sonuç verilerine etkisi ve saldırganın tespiti üzerine yorumlarda bulunulmuştur. İlk olarak sabit bir başlangıç kübit sayısı ile iletişim adım adım incelenmiş, saldırganın anahtar uzunluğu ve hata oranına etkisi gözlemlenmiştir. Sonraki aşamada aynı benzetim ortamında farklı başlangıç kübit uzunluklarıyla benzetim tekrar edilerek saldırı olması ve olmaması durumları karşılaştırılmıştır.

Makalenin ikinci bölümünde saldırı teknikleri ile ilgili önceki çalışmalar hakkında bilgi verilmiş, üçüncü bölümde BB84 anahtar değişim protokolü [1] benzetim ortamında gerçekleştirilmiş, engelle/tekrar gönder atağı olması durumunda oluşan sonuçlar analiz edilerek yorumlar paylaşılmıştır.

II. İLGİLİ ÇALIŞMALAR

BB84 bugün hala kullanılmakta olan ilk kuantum şifreleme protokolüdür. BB84 protokolü Charles Bennet ve Gilles Brassard tarafından 1984 yılında kuantum anahtar değişim protokolü olarak ortaya konmuştur [1]. Daha sonraki yıllarda B92 [18], Ekert [2] ve SARG [6] protokolleri geliştirilmiştir.

BB84 kopyalanamama teoremine dayanır ve gizli anahtarın güvenli olmayan bir kanal üzerinden güvenli şekilde dağıtımını sağlar. Temelde iki farklı taban kullanır ve kuantum bir kanal üzerinden iletilen rasgele sıralı dizi (anahtar) oluşturmak için ışığın kutuplaşmasından yararlanır. B92 protokolünde ise iletimden sonra gönderici alıcıya ne zaman bit tespit ettiğini bildirir fakat kullandığı tabanı açıklamasına gerek yoktur çünkü alıcı fotonu tespit etmişse kullandığı taban göndericinin göndermiş olduğu biti zaten başarılı bir şekilde tanımlar. Ekert protokolünde

978-1-7281-7565-2/20/$31.00 ©2020 IEEE

BB84'te olduğu gibi Heisenberg belirsizlik ilkesi [17] kullanılmaz, onun yerine kuantum halleri birbirine bağlaşık iki foton kullanılır, sonuçta alıcı ve vericiye birer foton gelir. Bu fotonların kuantum halleri birbirine zıt olduğundan bir taraf diğer taraftaki kuantum halini tahmin edebilir, böylece ortak bir kod anahtarı elde edilmiş olur. SARG protokolü foton bölme saldırılarına [3] karşı 2004 yılında Scarani ve arkadaşları tarafından öne sürülmüştür. BB84 protokolü ile benzerlik gösterir ancak bitleri kodlamak için filtreler kullanılır. SARG04 protokolü foton numarası bölme (PNS) saldırısına karşı BB84'ten daha sağlamdır.

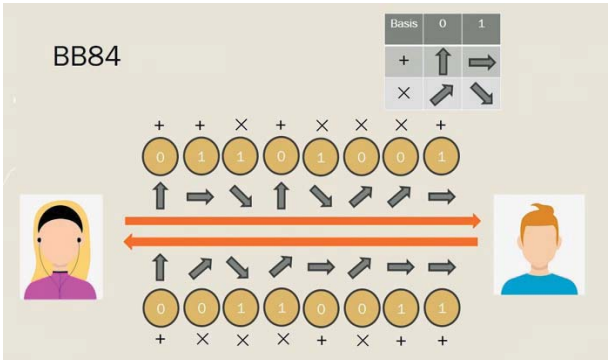
Yakala/tekrar gönder atağında saldırgan göndericinin ve alıcının sahip olduğu araçların (foton yayıcı ve toplayıcı) aynısına sahiptir. Saldırgan kendi cihazlarını gönderici ve alıcı arasına konumlandırır, böylece göndericinin gönderdiği fotonlara alıcıdan önce ulaşır, göndericinin ilettiği fotonu yakalayarak alıcıya kendi ürettiği fotonu gönderir. Bir başka önemli saldırı türü olan foton numarası bölme saldırısı ise saldırganın bir sinyal içinde birden fazla foton olması durumunda fotonlardan birini yakalayarak ölçümleme yapması ve bilgi elde etmesine dayanır [3]. Bu sinyal içindeki iki foton tamamen birbiriyle aynıdır. Saldırgan sadece tek fotonu yakalayacağından alıcının ölçümlemesinde fark edilmemesini amaçlar. Bunun için iletişim esnasında fotonların yarısını dinleyerek ölçümlemeye çalışır. Bunun için bazı çözümler öne sürülmüştür. Sinyal içerisinde sadece bir foton gönderilmesi bu tür saldırıları önleyecektir [5]. SARG protokolü bu saldırıya karşı dayanıklıdır [6]. Bu saldırı türünü önlemenin bir diğer yolu da göndericinin rastgele düşük ortalama foton numarasına sahip lazer darbeleri göndererek (yemleme) dinleyicinin gerçek fotonları ayırt edememesi sağlanır [7][11]. Truva atı atağında ise saldırgan gönderici veya alıcının cihazına sinyal gönderir (enjekte eder), yansıyan sinyalden göndericinin seçtiği filtre hakkında edinmeye çalışır [4]. Sahte durum atağında saldırgan sinyali tekrar oluşturmak yerine kendi türettiği formda özel olarak oluşturduğu sinyali kullanarak tüm iletişimi ele geçirmeyi amaçlamaktadır. [8]

Zaman kaydırma atağı ise saldırganın zaman parametrelerini inceleyerek sisteme saldırmasına olanak sağlamaktadır [9]. Bir diğer saldırı türü olan spektral saldırı türünde polarizasyon tespiti yerine renk ölçümlemesi yapılır. Fotonlar her bir diyot bir polarizasyon çeşidini oluşturacak şekilde 4 farklı diyot tarafından oluşturulmaktadır, bu da fotonların farklı spektral karakterlere sahip olmasına neden olur. Bu spektral karakterlerin analiz edilmesi ile gizli anahtar hakkında birçok bilgiye ulaşılabilir.

III. Benzetim Ortamı

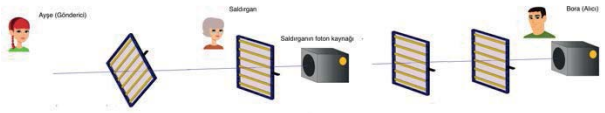
Bu bölümde BB84 protokolü ile kuantum anahtar değişimi QDK Simülatör yazılımıyla gerçekleştirilmiştir [12]. QDK Simülatör kuantum anahtar değişim protokollerini analiz etme amaçlı geliştirilmiş web tabanlı bir yazılımdır. Hata tahmini, gizlilik artırımı, bilgi uzlaşımı, eleme gibi birçok özellikte parametre kullanımını desteklemektedir.

BB84 protokolünde gönderici (Ayşe) rastgele bir tek kullanımlık anahtar seçer ve dört polarizasyonun rastgele seçilen birinde gönderir. Alıcı (Bora) gelen her bir foton için ölçüm türünü (filtre) kenarsal veya köşegensel türlerden biri olarak seçer. Alıcı ölçüm sonuçlarını kaydeder ancak onları gizli tutar. Alıcı, daha sonra ölçüm filtrelerini (ölçüm sonuçlarını değil) açıklar ve gönderici, alıcıya hangi ölçümlerin doğru türde olduğunu söyler.



Şekil. 1.BB84 iletişimi esnasında foton gönderimi

İki taraf alıcı ölçümlerinin aynı türde olduğu tüm durumları saklar. Bu durumlar daha sonra bitlere (1 ve 0) dönüştürülür ve anahtar elde edilmiş olur. Var olan üçüncü kişi bu iletişimde çeşitli hatalara sebep olacaktır, çünkü fotonun polarizasyon türünü bilememektedir. Haberleşen iki kişi hata bitlerini kontrol ederek dinlemeyi test edebilirler.



Şekil. 2.BB84 iletişimi ve saldırganın yakala/tekrar gönder atağıyla anahtarı elde etmeye çalışması

Benzetim ortamında Ayşe ve Bora arasında BB84 protokolü üzerinden gürültüsüz ortamda ortak anahtar oluşturma esnasında saldırganın yakala/tekrar gönder atağı yaptığı durum oluşturulmuştur. Bu saldırı türünde saldırgan göndericinin ve alıcının sahip olduğu araçların (foton yayıcı ve toplayıcı) aynısına sahiptir. Saldırgan bu kendi cihazlarını gönderici ve alıcı arasına konumlandırır, böylece göndericinin gönderdiği fotonlara alıcıdan önce ulaşır [14]. Saldırgan bu noktada alıcıdan gelen fotonlar üzerinde ölçümleme yaparak ve sonuçlarına dayanarak yeni oluşturduğu fotonları alıcıya gönderir. Oluşan hata oranının belirli bir eşik değerini aşması durumunda arada saldırgan olduğu varsayılarak iletişim iptal edilir.

Benzetim aşağıdaki başlangıç değerleriyle çalıştırılmıştır.

TABLO I. Benzetim Başlangıç Parametreleri

Başlangıç kübit sayısı	500
Temel seçim önyargısı farkı	0.5
Saldırgan temel seçim önyargısı	0.5
Sapmalı hata tahmini	Yok
Hata tahmini örnekleme oranı	0.2
Hata toleransı	0.11
Gürültü	Yok
Saldırgan	Var
Dinleme oranı	0.1

İlk aşamada gürültüsüz bir ortamda arada dinleyici olması durumunda 500 kübit için her adım incelenmiş, ikinci

bölümde 500,550…900 olarak farklı başlangıç kübit değerleri ile sonuç anahtar uzunluğu değerleri ve hata oranı analiz edilmiştir.

BB84 protokolünde anahtar değişimi açık ve kuantum olmak üzere iki kanaldan yapılmaktadır. İletim esnasında ham anahtar çıkarımı, hata tahmini, anahtar mutabakatı, güvenlik artırımı gibi ek adımlar uygulanmaktadır. Benzetimin çalışması esnasında bu adımlar aşağıda detaylı anlatılmıştır.

Aşama 1: BB84 Kuantum Kanal Üzerinden İletim

Ayşe 500 kübitlik bir dizi hazırlar ve bunları kuantum kanalı üzerinden Bora'ya gönderir. Aynı zamanda her bir kübit icin doğrusal polarizasyon (yatay / 0 derece ve dikey / 90 derece) veya çapraz polarizasyon (+45 derece ve -45 derece) için rastgele bir polarizasyon filtresi seçer. Daha sonra yatay ve dikey kübit durumlarını | 0> ve | 1>, +45 derece ve -45 derece | +> ve | -> durumlarıyla sırasıyla eşler.

Bu adımda Ayşe, 0.5 temel seçim eğilimi ile Bora'ya 500 kübit göndermiştir. Bu esnada saldırgan kuantum kanalı üzerinde 0,1 oranında ve temel seçim eğilimi 0,5 olarak kuantum kanalını dinlemektedir. Saldırgan kübitleri keserek iki filtreden birinde rastgele ölçer ve böylece orijinalleri yok eder ve daha sonra ölçümlerine ve temel seçimlerine karşılık gelen yeni bir kübit grubunu Bora'ya gönderir (Yakala/tekrar gönder atağı). Saldırgan doğru filtreyi ortalama sadece % 50 olarak doğru bildiğinden bitlerinin yaklaşık 1/4'ü Ayşe'den farklı olacaktır.

Aşama 2.1: Eleme

Bora, klasik bir kanalda başarılı bir şekilde ölçmeyi başardığı kübitleri duyurur. Ayşe ve Bora daha sonra kullandıkları filtreleri açıklar. Polarizasyon filtreleri ortalama zamanın yaklaşık % 50'si eşleştiğinde, her ikisi de karşılık gelen bitlerini kişisel anahtarlarına ekler. Kanal gürültüsünün olmaması durumunda kulak misafiri olmadıkça iki anahtar aynı olmalıdır. Kullanılan parametrelere göre eleme aşaması 500 aktarılmış kübit ile başlamış ve elde edilen bit dizisi 260 bite indirilmiştir. Ayşe ve Bora'nın seçilen ölçüm tabanlarının 0,52'si eşleşir. Seçtikleri filtrelerin 0,48'i eşleşmemektedir. İki tarafın ölçülen kübitlerinin 0.746'sı eleme öncesi eşleşir ve 0.254'ü eşleşmez. İki tarafın ölçülen kübitlerinin 0.9615'i eleme sonrasında eşleşir ve 0.0385 tanesi eşleşmez.

Aşama 2.2: Eleme Aşaması Kimlik Doğrulaması - Linear Feedback Shift Register (LFSR)

Ayşe ve Bora, LFSR evrensel hash şemasını ve kimlik doğrulama için karşılıklı olarak paylaşılan bir gizli anahtarı kullanarak temel değişim mesajlarını doğrular. Eleme aşamasında 3 mesaj doğrulanır. Bora, Ayşe'yi başarılı bir şekilde ölçmeyi başardığı kübitlerden haberdar eder ve mesajına bir kimlik doğrulama etiketi ekler. Anahtar açısından kimlik doğrulama maliyeti 64'tür. Bora, kübitleri ölçmek için seçtiği filtreleri Ayşe'ye bildirir ve mesajına bir kimlik doğrulama etiketi ekler. Ayşe, Bora'yı kübitleri hazırlamak için seçtiği filtrelerden haberdar eder ve mesajına bir kimlik doğrulama etiketi ekler.

Aşama 3.1: Uzlaşma / Hata Oranı Tespiti

Ayşe ve Bora hata düzeltmesine devam edip etmeyeceklerini veya protokolü önceden tanımlanmış bir hata tolerans eşiğine (genellikle yaklaşık %11) dayanarak iptal edip etmeyeceklerini belirlemek için elenmiş anahtarlarındaki hata oranı tespiti yapar.

Aşama 3.2: Uzlaşma / Kademeli Hata Düzeltme

Ayse ve Bora elenmiş bit dizelerindeki hatalı bitleri bulmak ve düzeltmek için genel kanalda Cascade adlı etkileşimli bir hata düzeltme şeması uygular. Art arda sıralı hataları düzeltmek için işlem 5 defa uygulanmıştır. 7 hatalı bit tespit edilmiş ve düzeltilmiştir. Hataları tespit etmek ve düzeltmek için 57 bit sızdırılmıştır.

Aşama 4: Hata Düzeltme Onayı ve Kimlik Doğrulaması

Bu adımda Ayşe ve Bora hata düzeltmeli anahtarlarının karma değerini karşılıklı olarak önceden paylaşılan gizli anahtarlarını kullanarak ve ilgili özetlerini karşılaştırarak hata düzeltme aşamasını doğrular. Kimlik doğrulaması için 64 bit anahtar (önceden paylaşılmış gizli anahtar) kullanılmıştır. Kimlik doğrulama için Linear Feedback Shift Register (LFSR) evrensel karma şeması kullanılmıştır.

Aşama 5: Gizlilik Artırımı

Bu adımda amaç saldırganın anahtarda tespit edebildiği bit sayısını en aza indirmektir. Ayşe ve Bora, genel bilgi sızıntısını hesaplar ve saldırganın kanala kulak misafiri olacak şekilde elde ettiği bilgiyi azaltmak/en aza indirmek için bir dizi gizlilik yükseltme protokolü çalıştırır. Bunu yerel olarak Toeplitz matrislerine dayanan evrensel bir karma şema uygulayarak yaparlar. Ayrıca bir güvenlik parametresi tanımlayabilirler. Gizlilik artırımı çalıştırmadan önceki anahtar uzunluk 208 bit, son anahtar uzunluğu 94 bit olmaktadır.

IV. DENEYSEL SONUÇLAR VE ANALİZ

Benzetim 500, 550, 600, …, 900 olarak 9 kez farklı başlangıç kübit değerleri ile çalıştırılarak gürültüsüz ortamda arada saldırgan olması durumunda sonuç anahtar uzunluğu değerleri ve hata oranı analiz edilmiştir. Sabit 500 başlangıç kübit sayısı için elde edilen sonuç değerleri Tablo II' de görülmektedir.

TABLO II. BENZETİM SONUÇLARI

Başlangıç kübit sayısı	500
Sonuç anahtar uzunluğu	108
Dinleme aktif	Evet
Dinleme oranı	0.1
Gönderici/alıcı temel seçim yanlılığı	0.5
Saldırgan temel seçim yanlılığı	0.5
Hata düzeltmesinden önce ham anahtar uyuşmazlığı	0.0191
Hata düzeltmesinden sonra ham anahtar uyuşmazlığı	0
Bilgi kaçağı (toplam bit)	82
Kimlik doğrulama için genel anahtar maliyeti	256
Hata düzeltmeden önceki anahtar uzunluğu	210
Bit hatası olasılıgı	0.0238
Hata düzeltme sırasında sızdırılan bit sayısı	50
Sızıntı için Shannon sınırı	35
Güvenlik parametresi	20

Gürültüsüz ortamda arada dinleyici bulunması durumunda farklı başlangıç kübit sayısı için hata oranları Tablo III'de görülmektedir.

TABLO III. SALDIRI DURUMUNDA HATA ORANI

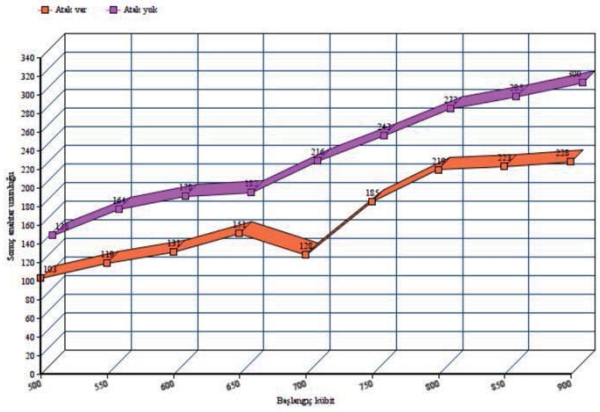
Başlangıç kübit sayısı	Hata oranı
500	0.0741
550	0.0392
600	0.0345
650	0.0161
700	0.0758
750	0.0282
800	0.0256
850	0.012
900	0.0549

Saldırı olması durumunda ortalama hata oranının belirgin seviyede olduğu görülmektedir. Benzetimde dinleme oranı başlangıç parametresi 0.1'dir. Hata oranının belirli eşik değerinde olması iletimin dinlendiğini ve artık güvenilir olmadığını göstermektedir. Sonuç değerlerinden görüldüğü üzere yakala/tekrar gönder atağının tespiti konusunda en etkili şekilde anahtardan hata oranı tespitiyle gerçekleştirilebileceği belirlenmiştir. Başlangıç dinleme oranı artırıldığında sonuç hata oranı verileri de artma göstermektedir.

TABLO IV . BAŞLANGIÇ KONFİGURASYONU SABİT TUTULARAK SALDIRI VE SALDIRI OLMADIĞI DURUMDA ANAHTAR UZUNLUKLARI

Başlangıç kübit sayısı	Anahtar uzunluğu (Saldırı var)	Anahtar uzunluğu (Saldırı yok)
500	103	136
550	119	164
600	131	178
650	151	182
700	128	216
750	185	243
800	219	272
850	223	285
900	228	300

Tablo IV' de görüldüğü üzere saldırı olması durumunda elde edilen anahtar uzunluğu saldırı olmama durumuna göre çok daha düşük olmaktadır. Başlangıç kübit sayısı ile sonuçta elde edilen anahtar uzunluğu arasında direkt ilişki görülmemekte, genel olarak gönderilen başlangıç kübit sayısının %20 - %25'i civarında anahtar uzunluğu elde edilmektedir. Arada saldırı bulunması bu oranı düşürmektedir.



Şekil. 3.Saldırı olması ve olmaması durumunda elde edilen sonuç anahtar uzunluklarının karşılaştırılması

V. SONUÇ VE ÖNERİLER

Kuantum mekaniğinin prensiplerinin ve kuantum kopyalanamama teoreminin anahtar dağıtımına uyarlanması kötü niyetli saldırganların anahtara habersiz bir şekilde erişemeyeceği sonucunu vermektedir. Benzetim sonuçları analiz edildiğinde anahtar değişiminde saldırganın tespitinde en iyi yöntemin hata oranının belirli bir eşik değerini aşıp aşmadığının iletişim esnasında düzenli olarak kontrol edilmesi olduğu görülmektedir. Eğer hata oranı eşik değerini aşmışsa hattın izinsiz olarak dinlendiği varsayılarak iletişim iptal edilir.

Kuantum anahtar dağıtımı cihazları henüz ticari olarak yaygınlaşmamakla birlikte kuantum anahtar dağıtım iletişimi ile elde edilen sonuç anahtarı günümüzde kullanılan iki aşamalı kimlik doğrulama, tek kullanımlık şifre gibi doğrulama yöntemleriyle veya rastgele anahtar üretici uygulamalar ile birleştirildiğinde tamamen güçlü bir güvenlik sağlayacaktır.

REFERANSLAR

[1] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.

[2] Ekert, Artur K. (5 August 1991). "Quantum cryptography based on Bell's theorem". Physical Review Letters. 67 (6): 661–663. Bibcode:1991PhRvL..67..661E. doi:10.1103/PhysRevLett.67.661. PMID 10044956.

[3] Brassard, Gilles; Lütkenhaus, Norbert; Mor, Tal; Sanders, Barry C. (7 August 2000). "Limitations on Practical Quantum Cryptography". Physical Review Letters. American Physical Society (APS). 85 (6): 1330–1333. arXiv:quant-ph/9911054. Bibcode:2000PhRvL..85.1330B. doi:10.1103/physrevlett.85.1330. ISSN 0031-9007. PMID 10991544.

[4] Jain, N.; et al. (2014). "Trojan-horse attacks threaten the security of practical quantum cryptography". New Journal of Physics. 16 (12): 123030. arXiv:1406.5813. Bibcode:2014NJPh...16l3030J. doi:10.1088/1367-2630/16/12/123030.

[5] Intallura, P. M.; Ward, M. B.; Karimov, O. Z.; Yuan, Z. L.; See, P.; et al. (15 October 2007). "Quantum key distribution using a triggered quantum dot source emitting near 1.3μm". Applied Physics Letters. 91 (16): 161103. arXiv:0710.0565. doi:10.1063/1.2799756. ISSN 0003-6951.

[6] Scarani, Valerio; Acín, Antonio; Ribordy, Grégoire; Gisin, Nicolas (6 February 2004). "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations". Physical Review Letters. 92 (5): 057901. arXiv:quant-ph/0211131.

[7] Bibcode:2004PhRvL..92e7901S. doi:10.1103/physrevlett.92.057901. ISSN 0031-9007. PMID 14995344.

[8] Wang, Xiang-Bin (16 June 2005). "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography". Physical Review Letters. 94 (23): 230503. arXiv:quant-ph/0410075. Bibcode:2005PhRvL..94w0503W.

doi:10.1103/physrevlett.94.230503. ISSN 0031-9007. PMID 16090451.
[9] Makarov *, Vadim; Hjelme, Dag R. (20 March 2005). "Faked states attack on quantum cryptosystems". Journal of Modern Optics. Informa UK Limited. 52 (5): 691–705. Bibcode:2005JMOp...52..691M. doi:10.1080/09500340410001730986. ISSN 0950-0340.
[10] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Info. Compu. 7, 43 (2007)
[11] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, "Security aspects of practical quantum cryptography", International conference on the theory and applications of cryptographic techniques. Springer, 2000, pp. 289–299.
[12] M. Haitjema, “A survey of the prominent quantum key distribution protocols”, 2007.
[13] QDK Simulator, Simulation and Analysis of QKD (https://www.qkdsimulator.com)
[14] Makarov V., Anisimov A., Skaar J., Effects of detector efficiency mismatch on security of quantum cryptosystems, Physical Review A, vol. 74, pp. 1-11, 2005.
[15] Shuang Zhao and Hans De Raedt, "Event-by-Event Simulation of Quantum Cryptography Protocols", Journal of Computational and Theoretical Nanoscience Vol.5, 490–504, 2008.
[16] Gisin, N., Ribordy, G., Tittel, W. and et al., (2002), "Quantum Cryptohraphy", Rev. Mod. Phys. , 74:145.
[17] W. Heisenberg, “Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik,” Zeitschrift für Physik, vol. 43, no. 3-4, pp. 172–198, mar 1927.
[18] Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68(21), 3121 (1992).