Süleyman Demirel Üniversitesi
Mühendislik Bilimleri ve Tasarım Dergisi
3(1), 29-42, 2015
ISSN: 1308-6693 Araştırma Makalesi Research Article

Suleyman Demirel University
Journal of Engineering Sciences and Design
3(1), 29-42, 2015
ISSN: 1308-6693

KUANTUM KRİPTOGRAFİDE GÖNDERİLEN FOTON SAYISININ, GÜRÜLTÜSÜZ ORTAMDA ELDE EDİLEN ANAHTAR UZUNLUKLARINA ETKİSİ

Ozan İNCETAŞ[1*], Şeref SAĞIROĞLU[2]

[1] Ankara Üniversitesi, Nallıhan Meslek Yüksekokulu, Bilgisayar Teknolojisi Bölümü, Ankara, Türkiye
[2] Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Ankara, Türkiye

Anahtar Kelimeler
Kuantum kriptografi, Dinleyici etkisi, Anahtar uzunluğu

Özet

Bilgi güvenliğinin sağlanması konusunda gelinen son noktalardan biri de Kuantum Anahtar Dağıtım Protokolüdür. Kuantum Kriptografi olarak da bilinen bu teknik, fotonların gönderilmesi yoluyla, gönderici ve alıcı arasında bir ortak anahtar oluşturulmasını sağlamaktadır. Bu çalışmada, cihazlardan ya da ortamdan kaynaklanabilecek gürültülerin olmadığı bir ortamda, BB84 Kuantum Anahtar Dağıtım Protokolüne dayanarak, gönderici ile alıcı arasında ortak anahtar oluşturan bir simülasyon tasarlanmıştır. Bu simülasyon yardımıyla, bir dinleyicinin olması ve olmaması durumunda oluşan anahtar uzunlukları ile araya giren bu dinleyicinin, oluşturulan anahtarlar üzerine etkisi araştırılmaya çalışılmıştır. Bu amaçla belirli sayılarda (100, 150, 200,…,900, 950, 1000) rastsal foton dizileri oluşturulmuş ve bunların her biri, dinleyicinin olması ve olmaması durumları için ayrı ayrı 1000'er kez gönderilmiştir. Bu işlemin ardından oluşan ham anahtarlar üzerinde, gönderilen foton sayıları da dikkate alınarak dinleyiciden kaynaklanan hataların yaklaşık oranları belirlenmiştir. Böylece gerçek bir ortamda oluşacak hataların, kuantum kanalındaki bir dinleyicinin varlığına dayandırılmasına ilişkin yorumların yapılmasının kolaylaştırılacağı düşünülmektedir.

THE IMPACT ON THE KEY LENGTH OF THE NUMBER OF SENDING PHOTON IN NOISELESS ENVIRONMENT IN QUANTUM CRYPTOGRAPHY

Keywords
Quantum cryptography Impact of an eavesdropper Key length

Abstract

Quantum Key Distrubution Protocol is one of the last points in ensuring the security of information. This technique, also known as Quantum Cryptography, provides to form a common key between the sender and the receiver via sending photons. In this study, we desing a simulation, which is based on noiseless BB84 Quantum Key Distrubution Protocol and which forms a common key between the sender and the receiver. Then, we investigate that key lengths whether there is an eavesdropper and that the impact of an eavesdropper via this simulation. We made random photon arrays with certain numbers (100, 150, 200, 250,….,950, 1000 etc.) for this purpose, and then each arrays had been sent 1000 times. After this phase, key lengths were compared. So, in noisely environment, we can easily identify how many faults are from the noise in environment and how many faults are from the an eavesdropper.

1. Giriş

Kriptoloji ve kriptografi zaman zaman birbirinin yerini alan terimler olarak kullanılsa da (Trappe ve Washington, 2002: 1), kriptoloji daha geniş bir terim olarak karşımıza çıkmaktadır. Kriptoloji kısaca şifreleme bilimi olarak tanımlanmaktadır (Sağıroğlu ve Alkan, 2005: 21). Bu tanım genişletildiğinde kriptoloji, verilerin ve bilgilerin şifrelenmesi, saklanması ya da istenilmeyen kişilerin anlamasını zorlaştırma ve şifrelenmiş verilerin veya bilgilerin çözülmesi üzerine çalışılan bilim dalı olarak karşımıza çıkmaktadır (Canbek ve Sağıroğlu, 2006: 17). Kriptoloji genel olarak kriptografi ve kriptoanaliz şeklinde iki ana başlık altında incelenmektedir (Spillman, 2005: 3).

* İlgili yazar: oincetas@ankara.edu.tr

Kriptografi, iletişimde gizliliği sağlayıcı sistemleri tasarlama sürecidir (Trappe ve Washington, 2002: 2). Benzeri şekilde daha güçlü ve daha etkili şifreleme-şifre çözme metotları geliştirme bilimi olarak da tanımlanabilir (Spillman, 2005: 3). Kriptografi oldukça geniş bir disiplinler arası alandır (Sağıroğlu ve Alkan, 2005: 21, Canbek ve Sağıroğlu, 2006: 17). Matematik, elektronik, optik, bilgisayar bilimleri, sosyal mühendislik, yönetim bilimi, hukuk gibi alanlar bunların başında gelmektedir.

Kriptoanaliz ise kriptografik sistem mekanizmalarını ve yaklaşımlarını inceleme ve çözme bilimidir (Sağıroğlu ve Alkan, 2005: 22). Biraz daha açık şekilde, anahtar bilgisi olmadan bir düz metnin (plain text) ele geçirilebilmesi için var olan kriptografi metotlarındaki zayıflıkların araştırıldığı bilim dalıdır (Spillman, 2005: 3). Kısaca kriptoanaliz, kriptografik metotların kırılması ile ilgilenir (Trappe ve Washington, 2002: 2).

Günümüzün gelişmiş kriptografi teknikleri, verinin gizlenmesini büyük oranda sağlasa da, dayandıkları temel prensip, çözülmesi çok uzun bir zaman alan matematiksel problemlerdir. Ancak gelecek yıllarda ortaya çıkması beklenen üstün hesaplama yetenekleri ile donatılmış yeni bilgisayarlar, bu teknikler için ciddi bir tehdit oluşturacaktır (Öztarhan et al., 2005: 154). İşte bu noktada kuantum kriptografi olarak bilinen, kuantum anahtar dağıtım protokolüne ihtiyaç duyulacaktır.

Kuantum kriptografi, temel olarak verinin gizlenmesine değil, yeterince uzun bir ortak anahtar oluşturulmasına yardımcı olmaktadır. Yeterince uzun bir rastsal anahtar, veri güvenliğinin sağlanmasındaki en önemli unsurdur (Bruen ve Forcinito, 2005: 76). Bu teknik ile istenilen özelliklerde bir anahtarın oluşturulması için de, kuantum fiziği yasalarından yararlanılmaktadır.

Bu çalışmada kuantum kriptografi tekniklerinden ilki olan BB84 protokolüne göre, gürültüsüz bir ortamda araya giren bir dinleyicinin varlığının, iletişime ve oluşan anahtarlara etkisi üzerinde durulmuş, ortaya çıkan hata oranları incelenmiştir. Bu amaçla aşağıdaki sorulara yanıt aranmıştır.

1. Oluşan anahtar üzerinde, dinleyicinin neden olduğu hatalı bitlerin oranı ne kadardır?
2. Gönderilen foton sayısının, dinleyicinin neden olduğu hatalı bitlerin oranına etkisi var mıdır?
3. Gönderilen foton sayısının, dinleyicinin neden olduğu, polarizasyonu değişen fotonların oranına etkisi var mıdır?
4. Gönderilen foton sayısının, dinleyicinin neden olduğu, bit değeri değişen fotonların oranına etkisi var mıdır?
5. Gönderilen foton sayısının, dinleyicinin doğru yakalayabildiği bitlerin oranına etkisi var mıdır?

Ancak bu konuda yapılan simülasyonlara ve bunların sonuçlarına geçmeden önce, ikinci bölüm içerisinde kriptografinin gelişimi, kuantum kriptografinin ortaya çıkışı ve BB84 protokolünün çalışma prensibi üzerinde durulmuştur.

2. Kriptografinin Gelişimi ve Kuantum Kriptografi

Kriptografinin gelişimi incelendiğinde, kriptograflar ile kriptoanalistler arasında geçmişten beri süregelen bir savaş karşımıza çıkmaktadır. Hatta bu savaş, kriptografinin gelişimindeki en önemli etken olarak düşünülmektedir (Singh, 2004:8). Yukarıda değinildiği gibi kriptografi bilgileri gizlerken, kriptoanaliz bu bilgileri ortaya çıkarmakla uğraşmaktadır. Kriptograflar, verileri hep daha güvenli şekilde saklama çabası içindeyken, kriptoanalistler ise bu gizli verilere ulaşma çabasındadırlar.

Kriptografinin, insanlığın tarihi kadar eski olduğu rahatlıkla söylenebilir. Çünkü bilgi kavramı insanlıkla başlar ve bu bilginin gizlenmesi için en eski çağlarda bile çaba harcanması gayet doğaldır. Bununla beraber, günümüz kriptografi tekniklerinin gelişimi, bilgi ve iletişim güvenliğinin kurumsallaştığı, Birinci Dünya Savaşı yılları ile başlar (Singh, 2004: 129). 1918 yılında Vernam ve Mauborgne, tanınabilir sözcükler serisi yerine rastgele harflerden oluşan bir anahtar kavramını ortaya atarak, hala bilinen en güvenli teknik olan Tek Kullanımlık Anahtar (One Touch Pad) yöntemini geliştirmişlerdir (Canbek ve Sağıroğlu, 2006: 42). Shannon'ın teorisine uygun şekilde, güvenliği anahtarın uzunluğu ile sağlayan bu teknik, halen kırılamaz olarak bilinen tek tekniktir (Bruen ve Forcinito, 2005: 76, Shannon, 1949: 27). Ancak teoride oldukça üstün olan bu teknik, uygulamada büyük sorunlar doğurmuştur. Bunların başında, mesajların boyutu ve sıklığı, anahtarların transfer hızı ile anahtarların güvenilirliğinin denetimi gelmektedir (Şahin ve Selçuk, 2006: 2). Bu teknik, sayılan nedenlerle uzun bir süre kullanım alanı bulamamıştır.

1970'ler, gelişen ve ucuzlayan bilgisayarlar sayesinde, bankaların ve şirketlerin kriptografiyi kullanmaya başladıkları bir dönemdir. Ancak her kurumun farklı şifreleme teknikleri kullanmaları, bir süre sonra ciddi karışıklıklara neden olduğundan Amerika Ulusal Standartlar Bürosu, 1977 yılında IBM firmasında çalışan Horst Feistel tarafından geliştirilen Lucifer adlı ürünü Veri Şifreleme Standardı (Data Encryption Standard) olarak kabul etmiştir (Trappe ve Washington, 2002: 98, Spillman, 2005: 138). Ancak bu algoritmanın geliştirilmesi ile pek çok sorun çözülmüş gibi görünse de aslında yeni problemler ortaya çıkmıştır. Bu problem anahtarların dağıtımıdır. Çünkü DES gibi simetrik şifreleme tekniklerinin kullanılabilmesi için, öncelikle anahtarın alıcıya teslim edilmesi gerekmektedir. Anahtar dağıtımı sorunu 1970'ler boyunca kurumlara çok büyük bir mali yük getirmiştir (Singh, 2004: 305).

Simetrik yaklaşıma dayalı yöntemlerin neden olduğu bu dağıtım ve güvenlik problemi, Açık Anahtar Algoritması (Public Key Algorithm) olarak isimlendirilen yeni bir şifreleme yöntemi ile çözülmüştür. İlk olarak 1976 yılında Diffie ve Hellmann (Diffie ve Hellman, 1976: 644-654) tarafından ortaya atılan bu yaklaşımda, güvenli iletişim kurmak isteyen iki taraf, seçtikleri birer üs değeri ve modüler aritmetiğe dayalı gerçekleştirdikleri bir işlem ile ortak bir anahtarı paylaşmaktadırlar. Bu fikrin ortaya atılmasından sonra, çeşitli asimetrik yaklaşımlar geliştirilmiştir (Sağıroğlu ve Alkan, 2005: 32). Bunlar genel olarak iki farklı anahtara sahiptirler. Bu farklı anahtarlardan birisi şifreleme için, diğeri ise şifreyi çözmek için kullanılmaktadır. Şifreleme için kullanılan anahtar açıktır (public key), yani isteyen herkes bu anahtara sahip olabilmekte ve kullanabilmektedir. Yalnızca şifreyi çözmek için gerekli anahtar gizlidir ve özel anahtar (private key) olarak ifade edilmektedir. Bu yöntem asimetrik şifreleme olarak da bilinmektedir.

Geliştirilen asimetrik şifreleme tekniklerinin başında, 1977 yılında Rivest, Shamir ve Adleman tarafından tasarlanan RSA'dır. RSA içerisinde kullanılan asimetrik yani tek yönlü fonksiyon, temelde iki asal sayının çarpılması esasına dayanmaktadır (Rives et al., 1978: 120-126). Kriptoloji içerisinde en çok kullanılan üç karakter olan Alice, Bob ve Eve örneği üzerinden açıklamak gerekirse, Alice, Bob'a bir mesaj göndermek istemekte ve Eve de elinden gelen her türlü yola başvurarak bu mesajı dinlemeye çalışmaktadır. RSA kullanılarak sağlanacak bir iletişim için Alice öncelikle Bob'un açık anahtarını bilmelidir. Bob p ve q ile gösterilen iki asal sayı seçer. Bu sayıları çarparak $n=p \bullet q$ sayısını elde eder ve $Ø=(p-1)(q-1)$ değerini hesaplar. $1<e<Ø$ ve gcd(e, Ø)=1 (en büyük ortak bölen) şartlarını sağlayan rastgele bir e değeri seçer. Hemen ardından da, Öklid algoritmasını kullanarak, $1<d<Ø$ ve $e \bullet d \equiv 1 \pmod{Ø}$ koşullarını sağlayan d sayısını hesaplar. Bu durumda Bob'un açık anahtarı (n,e) ikilisi, özel anahtarı ise d olacaktır. Bob kendisine ait (n,e) ikilisini Alice'e yolladığında, Alice göndereceği açık metini bu ikili ile şifreler. m açık metni, c ise şifreli metni ifade ederse, $c \equiv m^e \pmod{n}$ işlemi ile şifreli metin elde edilmiş olur. Daha sonra elde ettiği bu c metnini, Bob'a yollar. Bob elindeki d özel anahtarını kullanarak, Alice'in gönderdiği şifreli metinden, açık metni $m \equiv c^d \pmod{n}$ işlemi ile elde eder. RSA tek yönlü bir algoritma olduğundan şifrelenmiş metin, n sayısı kullanılarak çözülemez. Kısacası, mesajı şifreleyen Alice de dahil olmak üzere, p ve q değerlerini bilmeyen hiç kimse bu mesajı çözemez. Mesajı çözmek için p ve q değerlerinin bilinmesi gerekmektedir. Her ne kadar n değerinin çarpanlarına ayrılması işlemi, anahtarın ve dolayısıyla şifrenin kırılması anlamına gelse de bu işlem çok kolay değildir.

Rivest, Shamir ve Adleman 1978 yılında Communications (ACM) dergisinde yayınlanan makalelerinde 129 hanelik bir anahtarla şifrelenen mesajı çözebilecek herkese $100 vereceklerini açıklamışlardır. O günün şartlarında katrilyon yıl sürmesi hesaplanan bu şifre 17 yıl gibi bir sürede çözülmüştür. Yine 155 haneli RSA anahtarlarından birisi de 1999 yılında çarpanlarına ayrılmıştır (Canbek ve Sağıroğlu, 2006: 49-50).

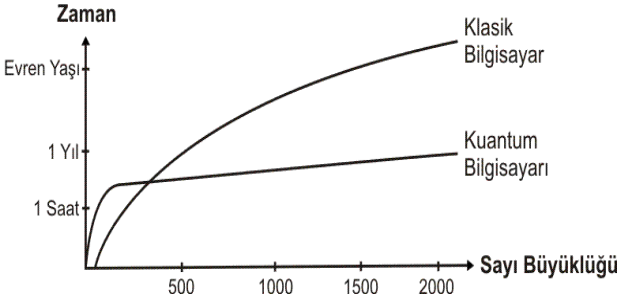
2.1. Gelişen Teknolojiye Karşı Kuantum Kriptografi

Daha önce de değinildiği gibi, açık anahtarlı sistemlerin sağladığı güvenlik, genelde hesapsal zorluğa dayanmaktadır ve Shannon'ın ortaya attığı mükemmel gizlilik kavramından çok uzaktır. Bunun nedeni, açık anahtarlı sistemlerin entropisinin, sıfır (0) olmasıdır (Bruen ve Forcinito, 2005:: 196). Yani, açık anahtarlı sistemlerin pek çoğunda belirsizlik yoktur. Örneğin en çok kullanılan açık anahtarlı sistemlerden biri olan RSA, çok basit olan bir çarpanlara ayırma problemine dayanmaktadır. Ancak güvenliği sağlayabilmesinin en büyük nedeni, çok büyük sayıların çarpanlara ayrılmasının getirdiği hesapsal zorluktur. Yapılan hesaplamalara göre günümüzün teknolojisinin, açık anahtarlı bu sistemleri çözmesi binyıllar sürecektir (Singh, 2004: 336). Ancak yapılan çalışmalar ışığında, teknolojinin gelişimi hakkındaki öngörüler, çok yakında bu açık anahtarlı sistemlerin kısa sürelerde kırılacağını göstermektedir.

Örneğin, 1965 yılında Gordon Moore'un belirttiği ve Moore Yasası olarak bilinen gelişim sürecine göre, yarıiletken teknolojisindeki gelişme her 18 ayda iki katına çıkmaktadır (Singh, 2004:389). Yine Moore yasasına göre bir çip üzerine yerleştirilen bileşenlerin sayısı arttıkça, bileşenlerin büyüklükleri de o oranda azalmaktadır (Stolze ve Suter, 2004: 2). Bu eğilim sonraki 40 yıl içerisinde de devam etmiş ve öngörülebilir gelecekte de devam etmesi beklenmektedir. Çip bileşenlerinin boyutları günümüzde 100 nm civarındadır ve her yıl yaklaşık olarak %12 azalmaktadır. Bu tahminler doğrultusunda 2013 yılında büyüklüğü 50 nm seviyesinde olması beklenen bileşenlerin, 2040 yılına gelindiğinde birkaç atomdan oluşabileceği tahmin edilmektedir. Bu durum, kuantum yasalarının bilgisayarlar için de geçerli olacağını bir göstergesidir. Yani, artık hesaplamada atomlar ve atom altı parçacıklar için geçerli olan fiziksel kurallar geçerli olacaktır (Öztarhan et al., 2005: 153). Böylece imkansız gibi görünen hesaplama işlemleri, çok kısa bir zaman içerisinde yapılabilecektir.

Şekil 1'de verilen grafik, çarpanlara ayırma işleminde, kuantum bilgisayarlar ile klasik bilgisayarlar arasındaki en önemli farkı vermektedir. Buna göre, gelecekte sayılar ne kadar büyük olurlarsa olsunlar, bugün için oldukça kısa sayılabilecek bir sürede çarpanlarına ayrılabileceklerdir (Stolze ve Suter,

2004: 12, Marinescu ve Marinescu, 2005: 9). Bu da, gelecekte açık anahtarlı sistemlerin ciddi problemler yaşayacağı anlamına gelmektedir. Dolayısıyla, açık anahtarlı sistemler ve özellikle elektronik imza, gelecekte ciddi bir tehdit altında olacaktır. Benzer görüşler Öztarhan ve arkadaşları tarafından da dile getirilmiştir (Öztarhan et al., 2005: 154).



Şekil 1. Klasik ve Kuantum bilgisayarların çarpanlara ayırma işlem süreleri (Stolze ve Suter, 2004: 12)

Bu gelişmeler, DES ya da Tek Kullanımlık Anahtar gibi simetrik yöntemlerde kullanılmak üzere, anahtar dağıtımına yeni çözümler için harcanan çabaları arttırmış, sonuçta da kuantum kriptografi olarak da bilinen Kuantum Anahtar Dağıtımı kavramı ortaya çıkmıştır. Kuantum anahtar dağıtımı, ilk olarak 1984 yılında Bennett ve Brassard tarafından (Bennet ve Brassard, 1984: 176-179) ortaya atılmış olup, mevcut yöntemlerden farklı olarak kuantum fiziği yasalarını kullanarak anahtar dağıtımını gerçekleştirmektedir. Veri iletiminde dijital veriden yararlanmak yerine maddelerin fiziksel özelliklerinden yararlanması, kuantum anahtar dağıtımı sisteminin teknolojinin gelişiminden olumsuz yönde etkilenmeyeceği anlamına gelmektedir (Toyran, 2007: 2).

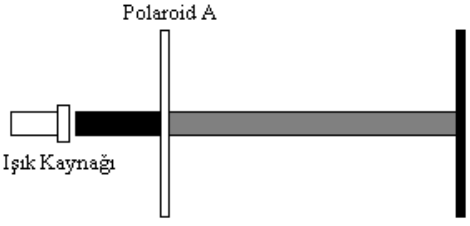
DES gibi simetrik şifreleme tekniklerinde, anahtarın güvenli şekilde dağıtımında ciddi problemlerle karşılaşıldığına bu bölümde değinilmiştir. Benzer şekilde RSA gibi asimetrik şifreleme tekniklerinin ise güvenliği tam olarak sağlamadığı buna karşın günümüz bilgisayarlarının hesaplama yetenekleri karşısında oldukça dirençli olduğu bilinmektedir. Ancak bu şifreleme tekniklerinin, geleceğin hızlı bilgi işleme ortamlarında güvenliği sağlayamayacakları da açıktır (Öztarhan et al., 2005: 154). Mükemmel gizliliğin sağlanabilmesi için ilk olarak güvenliğin, tamamen rastsal olarak belirlenmiş ve en az mesaj kadar uzun olan bir anahtara dayanması gerekmektedir (Bruen ve Forcinito, 2005: 76, Shannon, 1949: 681). İkinci olarak ise alıcı ve verici arasına giren bir kişinin kendisini fark ettirmeden anahtarı tamamıyla elde etmesinin engellenmesi gereklidir (Algan, 2008).

Kuantum kriptografi ise, tek kullanımlık anahtarın, fotonlar yardımıyla iletilmesi ile gerçekleştirilen bir tekniktir (Trappe ve Washington, 2002: 353, Spillman, 2005: 274, Algan, 2008, Toyran, 2007: 1, Kale, 2005: 6). Kriptografinin ve kuantum bilgisayarların gelişimi devam ederken, çok daha yeni olan kuantum kriptografi kavramı şekillenmeye başlamıştır. Kuantum kriptografi %100 güvenliği sağlamak amacıyla geliştirilmiştir. Gizli dinleyicilerin, şifrelenmiş iletilerin içeriğini okumasını önlemek yani bilginin güvenliğini sağlamak için çeşitli matematiksel fonksiyonları kullanan geleneksel şifreleme tekniklerinin aksine, kuantum şifreleme tekniği, kuantum fiziğini yasalarını temel almaktadır.

2.2. Kuantum Kriptografinin Doğuşu

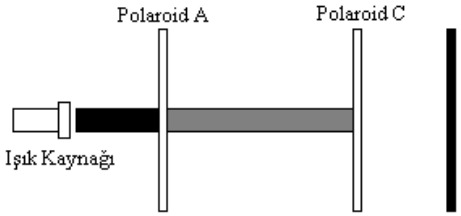
Bilginin gizlenmesinin, asırlardır devletlerin ve askeri birliklerin en değer verdiği konulardan biri olduğu bilinen bir gerçektir. Bu konuda yapılan çalışmalarda gelinen son nokta kuantum kriptografidir. %100 güvenliğin sağlanması için geliştirilen bu teknik, kuantum fiziği yasalarına ve fotonların fiziksel özelliklerine dayanmaktadır. Kuantum kriptografinin temel aldığı ilk kuantum prensibi, Heisenberg belirsizlik ilkesidir (Singh, 2004: 407-408, Algan, 2008). Bu ilke bir parçacığın aynı anda iki özelliğinin bilinemeyeceği üzerinde durmaktadır (Çimen et al., 2008: 105). Temel alınan ikinci kuantum ilkesi ise yapılan gözlemin parçacığın durumunu değiştirme ilkesidir (Trappe ve Washington, 2002: 355). Dış gözlem olarak bilinen, deney gerçekleştirilirken yapılan ve sonucu etkilemeyen klasik gözlem kavramı, parçacık seviyesinde doğru değildir. Bu özellik pek çok alanda ilgiye neden olabilir, ancak bunların hiçbirisi kriptolojinin ilgisi kadar yoğun olamaz. Çünkü Trappe ve Washington'ın da belirttikleri gibi bu özellik mükemmel bir saldırı tespit sistemidir.

Trappe ve Washington, basit bir kuantum deneyinin yardımıyla fotonların hareketleri konusunda önemli bilgiler vermişlerdir (Trappe ve Washington, 2002: 356). Fotonlar, belirli bir yönde ilerlerken farklı polarizasyonlara (kutuplaşma) sahiptirler. Bu nedenle fotonların bir kısmı önlerine konulan filtreleri aşarken, bir kısmı bu filtrelere takılırlar. Bu deneyde güçlü bir ışık kaynağından gelen ışınların önüne çeşitli açılarla 3 farklı Polaroid filtre, sırasıyla yatay, 45° ve düşey biçimde konularak ışığın hareketi anlaşılmaya çalışılmıştır. Yatay filtre sadece yatay polarizasyonlu, düşey filtre sadece düşey polarizasyonlu, 45° ile yerleştirilen filtre ise sadece 45° polarizasyonlu fotonların geçmesine izin vermektedir. Şekil-2'de görüldüğü gibi ışık kaynağının önüne yatay olarak konulan A filtresi kaynaktan gelen ışığın yoğunluğunu dolayısıyla foton sayısını azaltmaktadır.



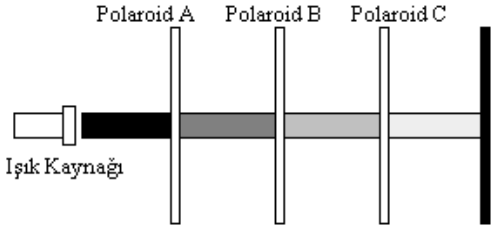
Şekil 2. Sadece yatay polaroid filtre kullanılarak yapılan foton deneyi

Şekil 2'deki deneyde, yatay polarizasyonlu fotonlar filtreyi geçerken, düşey polarizasyonlu fotonlar filtreye takılmışlardır. Şekil 3'de gösterilen ikinci deneyde ise yatay konumlu A filtresi ile duvar arasına düşey konumlu C filtresi eklenmiştir. Bu durumda ise duvara hiçbir foton ulaşamamıştır. Bu deneyde, yatay konumlu A filtresinden geçen fotonlar sadece yatay polarizasyona sahip olduklarından, düşey konumlu C filtresine takılarak duvara ulaşamamışlardır.



Şekil 3. Yatay ve düşey polaroid filtreler kullanılarak yapılan foton deneyi

Bu deney sonucunda fotonların düşey ve yatay olmak üzere sadece iki polarizasyona sahip oldukları düşünülebilir. Ancak bu düşüncenin yanlış olduğu Şekil 4'deki deneyde görülebilecektir. Işık kaynağı ile duvar arasına sırasıyla yatay, 45° ve düşey konumlu filtrelerin konulması ile yapılan bu deneyde, A filtresinden çıkan bütün fotonlar yatay polarizasyonludur. 45° ile konumlandırılan B filtresine gelen fotonların bir kısmı bu filtreye takılırken, diğerleri 45°'lik polarizasyonlara sahip olarak bu filtreden çıkmış ve C filtresine gelmişlerdir. Yine burada fotonların bir kısmı filtreye takılırken, bir kısmı da düşey polarizasyona sahip olarak filtreyi geçmiş ve duvara ulaşmışlardır.



Şekil 4. Yatay, 45° ve düşey polaroid filtreler kullanılarak yapılan foton deneyi

Bu deneylerin en önemli göstergesi, bir fotonun polarizasyonunu belirlemek için yapılan ölçümün, fotonun polarizasyonunu değiştirebileceğidir. Bu özellik, fotonların kuantum kriptografide kullanılması için oldukça elverişlidir. Çünkü hattın dinlenmesi gibi bir durumda veriler değişeceği için, bu durum kolaylıkla ortaya çıkarılabilecektir.

Fotonların farklı polarizasyonlara sahip olmaları ve bunların ölçülememeleri oldukça önemli bir özelliktir. Bu özellik ilk olarak 1960'ların sonlarında Weisner'ın ilgisini çekmiş ancak yaptığı teorik çalışma ilgi görmemiştir (Singh, 2004: 403). Wiesner'a göre, fotonların farklı polarizasyonlara sahip oldukları bilindiğine göre bu fotonların polarizasyonlarının ölçülmesi üzerinde durmak gerekecektir. Fotonlar düşey, yatay, 45° ya da herhangi bir polarizasyona sahip olabilirler. Ancak temel olarak –, ǀ, / ve \ şeklinde 4 farklı polarizasyon ele alınırsa, fotonların veri iletiminde kullanımları kolaylaşacaktır. Bir fotonu ölçmenin tek yolu polaroid filtreler kullanmaktır. İlk olarak ǀ (düşey) bir polaroid filtre ile ölçüm yapılırken, filtreye gelen fotonun 4 temel polarizasyondan birine sahip olduğunu farz edelim. Eğer filtreye gelen foton ǀ şeklinde yani dikey olarak yönlendirilmişse, filtreden geçecektir ve bu fotonun dikey polarizasyona sahip olduğu açık hale gelecektir. Ancak foton filtreden geçmemişse, bu fotonun polarizasyonu hakkında kesin bir yargıda bulunmak imkansız hale gelecektir. Örneğin – (yatay) polarizasyona sahip bir foton, ǀ (dikey) bir filtreden geçemeyecektir. Bununla birlikte ǀ (dikey) filtreden geçemeyen bir fotonun, – (yatay) yönlenmiş olduğu kesin değildir. Eğer foton \ ya da / şeklinde yönlenmişse bu durumda fotonların yarısı ǀ (dikey) olarak geçecek, diğer yarısı ise filtreye takılacaktır. Bu durumun fark edilmesi ile kriptografinin aradığı en önemli iki özellik ortaya çıkarılmıştır. Yani bir verinin değerini bilmek şansa kalmıştır ve bunun yanında yanlış bir filtre kullanmak veriyi tamamen değiştirebilmektedir. Bu özellik kriptografi için çok önemlidir, çünkü veriler iletilirken araya bir dinleyicinin girmesi imkansız hale gelmektedir.

Fotonların ya da diğer kuantum parçacıklarının, kriptografide kullanılmasını sağlayan bir diğer önemli özellik ise bilinmeyen bir parçacığın durumunun birebir kopyasının oluşturulmasının imkansız oluşudur (Spillman, 2005: 271). Teorik olarak, diğer kuantum parçacıklarının da kullanılması mümkündür, ancak fotonlar gerekli olan bütün özellikleri sağlarken, çok yüksek bant genişliğine sahip olan fiber optik kablolarda da temel bilgi taşıyıcısı konumundadırlar (Toyran, 2007: 2). Bennett ve Brassard bu özelliklerin kriptografide kullanılabileceğini düşünmüşler ve önemli bir çalışmaya imza atmışlardır. Böylece Kuantum Kriptografi olarak da bilinen "Kuantum Anahtar Dağıtımı" kavramı ortaya atılmıştır.

2.3. Kuantum Anahtar Dağıtımı ve BB84 Protokolü

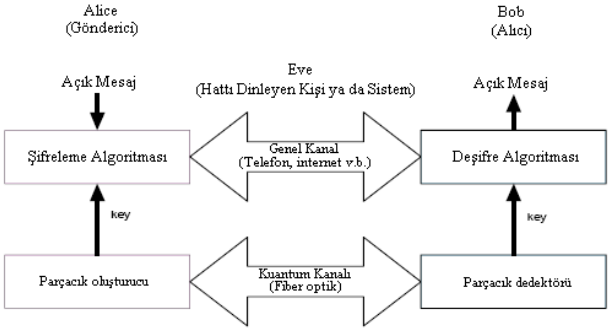
Kuantum Anahtar Dağıtımı kavramı daha önce de değinildiği gibi ilk olarak Bennett ve Brassard tarafından 1984 yılında ortaya atılmıştır (Bennet ve Brassard, 1984: 176-179). Bu sistem kurucularının soyadlarının baş harfleri ve bulunduğu yıl olan 1984'ün kısaltması şeklinde, BB84 Protokolü olarak da bilinmektedir. BB84 protokolünün mevcut yöntemlerden farkı, kuantum fiziği yasalarını kullanarak anahtar dağıtımını gerçekleştirmesidir (Spillman, 2005: 274, Algan, 2008, Toyran, 2007: 1, Kale, 2005: 6). Veri iletiminde dijital veriden yararlanmak yerine parçacık seviyesindeki maddelerin fiziksel özelliklerinden yararlanması,

kuantum anahtar dağıtımı sisteminin teknolojinin gelişiminden olumsuz yönde etkilenmeyeceği anlamına gelmektedir (Toyran, 2007: 2). Bu durum iki önemli avantaj getirmektedir (Dalkılıç ve Ayhan, 2005: 8). Bunlardan ilki, matematiğe oranla teknolojik öngörülerde bulunmak kolay olacaktır. Yani bilinen sistemlerden farklı olarak, kuantum kriptografinin bir gecede çökertilmesi ihmal edilebilir. İkincisi ise, mesajın kopyalanıp kırılabildiği temel şifreleme sistemlerinden farklı olarak, kuantum kriptografinin güvenilirliğinin anahtar dağıtımı sırasında dinleyicinin teknolojik seviyesine bağlı oluşudur.

Kuantum mekaniğinin kriptografi içerisinde iki taraf arasında bir gizli anahtarın güvenli şekilde iletilmesi için kullanılmasında, parçacıkların (fotonlar) kopyalanamaması ve belirsizlik ilkelerinden yararlanıldığına daha önce de değinildi. İki taraf arasında anahtar dağıtımı yapılırken yaşanan problem, bu anahtarın üçüncü bir şahıs tarafından belirlenemeden ya da değiştirilmeden hedefine nasıl iletileceğidir.

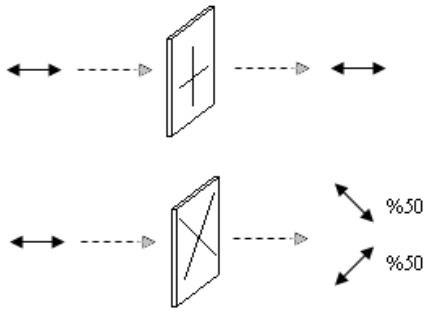
Kuantum anahtar dağıtımında, Şekil 5'de de görülebileceği gibi iki ayrı kanal kullanılmaktadır (Kale, 2005: 5). İlki anahtarın belirlenmesi için gönderilecek parçacıkların kullanıldığı kuantum kanalı, ikincisi ise şifrelenmiş mesajların ve diğer bilgilerin doğruluğunun test edildiği telefon ya da internet gibi bir genel kanaldır.

Kuantum anahtar dağıtım protokolü daha önce de değinildiği gibi fotonlar kullanılarak geliştirilmiştir. BB84 protokolü, iletimde fotonları kullandığından fiber-optik iletimde rahatlıkla kullanılabilir. Bu protokol, her bir 0 (sıfır) ve 1 (bir) değeri için iki farklı polarizasyon olmak üzere dört farklı polarizasyona sahip fotonlarda saklayarak iletişimi gerçekleştirmektedir (Trappe ve Washington, 2002: 356, Spillman, 2005: 274, Singh, 2004: 411, Toyran, 2007: 2). Bu polarizasyonlar yine önceki bölümlerde belirtildiği gibi yatay, dikey, 45° ve -45° (sırasıyla –, ׀, / ve \) şeklindedirler.



Şekil 5. Kuantum Anahtar Dağıtımı (Kale, 2005: 5)

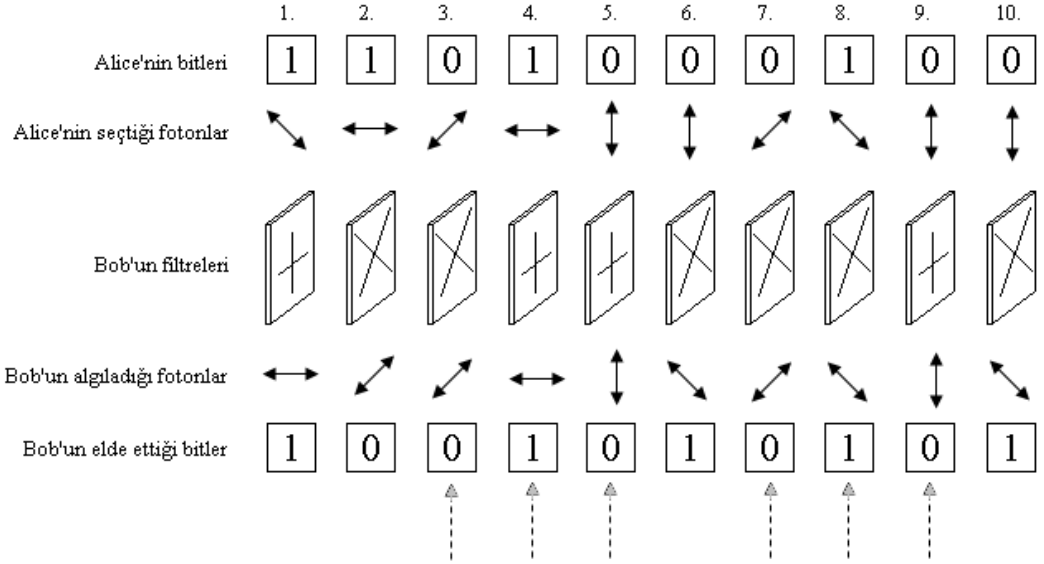
Fotonların durumlarını belirlemek için ise iki farklı polaroid filtre kullanılmaktadır (Spillman, 2005: 275, Singh, 2004: 412, Toyran, 2007: 2). Bunlardan birincisi yatay ve dikey polarizasyonlu fotonları belirlemek için kullanılan + şeklindeki doğrusal filtre, ikincisi ise 45° ve -45°'lik fotonları belirlemek için kullanılan X şeklindeki diyagonal filtredir. Eğer filtreye uygun bir foton filtreyi geçerse, fotonun durumu değişmeyecektir. Ancak filtreye uygun olmayan bir foton filtreye takılmadan geçerse bu durumda fotonun polarizasyonu değişecek ve bu durum rastsal olacaktır. Şekil 6'da verildiği gibi – (yatay polarizasyonlu) bir foton + (doğrusal) filtreden geçtiğinde bu foton yine – olarak (yatay polarizasyonla) yoluna devam edecektir. Ancak aynı – foton, X (diyagonal) filtreden geçebilirse, bu durumda %50 ihtimalle \ ve yine %50 ihtimalle / şeklinde olacaktır. Aynı durum diğer polarizasyonlara sahip tüm fotonlar için geçerlidir.



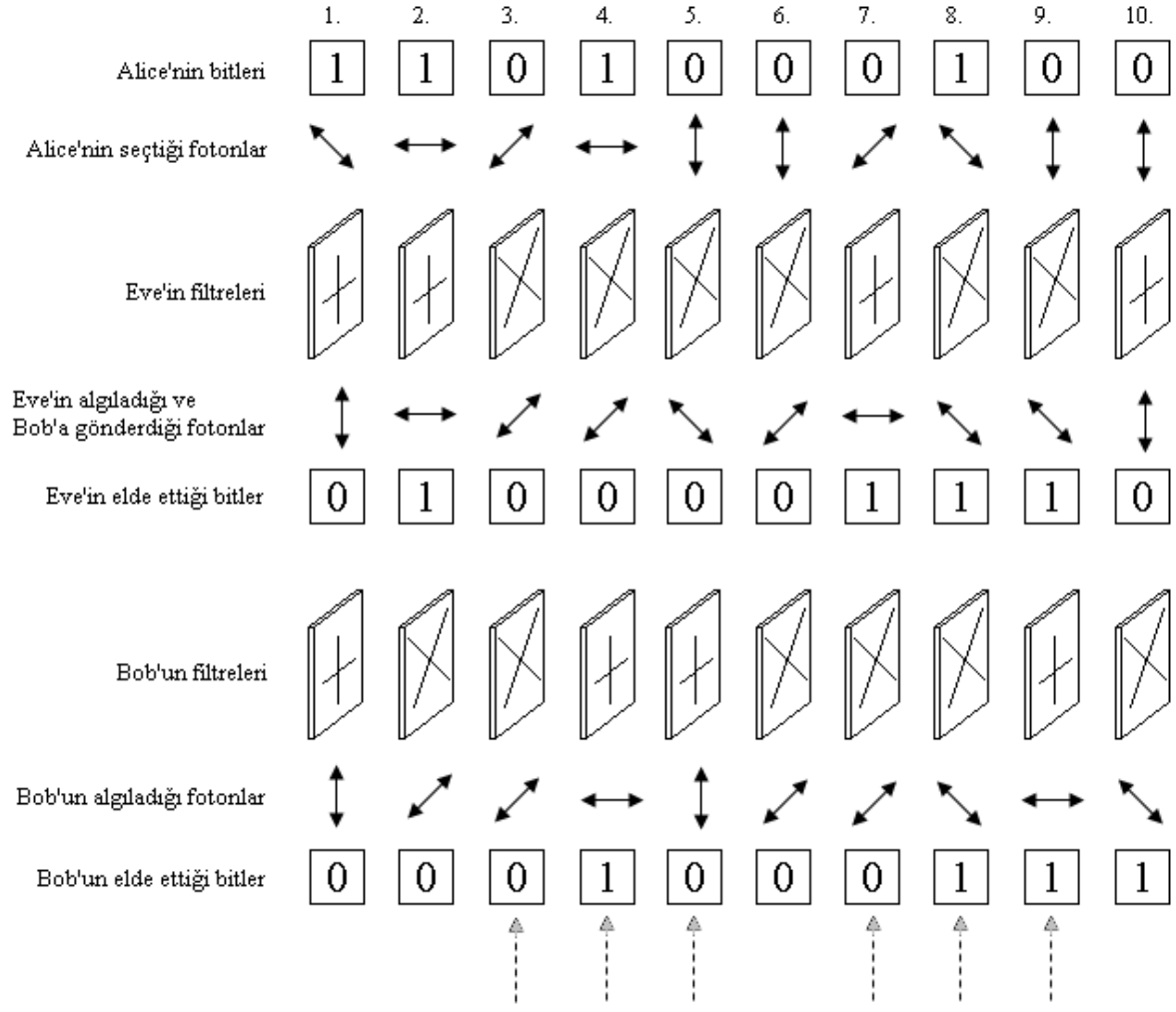
Şekil 6. Doğru ve yanlış filtrelerin kullanılması (Spillman, 2005: 275)

Kuantum anahtar dağıtım protokolünde amaç iki taraf arasında, güvenli iletişimde kullanılması amacıyla tek seferlik bir anahtar oluşturmak olduğuna göre, öncelikle iletime hangi değerin hangi polarizasyonla gönderileceğine karar vererek başlanmalıdır (Singh, 2004: 413-415, Toyran, 2007: 2). Buradaki işleyişin tam olarak anlaşılması için de yine kriptografinin üç karakterinden yani Alice, Bob ve Eve'den yardım almak doğru olacaktır. Alice, Bob'a bir mesaj iletmeye çalışırken, Eve de bu mesajı elde etmek için çaba harcamaktadır. Bu amaçla Alice ve Bob, öncelikle bir anahtar dizisi üzerinde anlaşmak için kuantum kriptografiden yararlanacaklardır. Bunun için öncelikle 0 ve 1 değerlerine karşılık gelen fotonları belirlemekle işe başlamalıdırlar. Örneğin 0 (sıfır) değeri için ׀ ve /, 1 (bir) değeri için ise – ve \ polarizasyona sahip fotonları kullanmaya karar verebilirler. Bu iletişim süreci Şekil 5'de de görülen dinlemeye açık, yani güvenliğin sağlanmasının gerekmediği telefon ya da internet gibi genel bir hat üzerinden yapılabilir. Daha sonra Alice göndermek istediği anahtarı ikilik bitler şeklinde seçer ve bu bitlere uygun şekilde polarizasyonları rastsal olarak seçilmiş fotonları Bob'a gönderir. Alice her polarizasyonu kaydeder ancak bunları gizli tutar. Bob ise fotonları alırken rastsal olarak seçtiği filtreleri kullanır. Bu işlem sırasında her foton için kullandığı filtre tipini (doğrusal ya da diyagonal) ve elde ettiği bitin değerini kaydeder. Alice bütün fotonları gönderdikten sonra, Bob ile genel bir hat üzerinden tekrar iletişime geçer. Bob, her foton için kullandığı

filtre tipini Alice'e söyler ve Alice de Bob'a seçtiği filtrelerin hangilerinin doğru olduğunu söyler. İşte bu noktada anahtar oluşturulmuş olur. Bob'un seçmiş olduğu filtrelerden okuduğu bitler anahtarı meydana getirmiştir (Singh, 2004: 416, Toyran, 2007: 2). Bu anahtar, henüz doğruluğu tam olarak incelenmediğinden ham anahtar olarak da adlandırılmaktadır.



Şekil 7. Anahtar bitlere karar verilmesi



Şekil 8. Hattın dinlenmesi ve sonuçları

Örneğin Alice 10 rastgele biti 10 rastgele polarizasyon üzerinden göndermiş olsun. Şekil 7'de görüldüğü gibi 1 değerine sahip ilk bit \ polarizasyonlu foton ile gönderilirken, yine 1 değerine sahip ikinci bit ise – polarizasyonlu foton ile gönderilmektedir. Bob ise ilk foton için +, ikinci foton için ise X filtrelerini kullanmıştır. Alice'in gönderdiği tüm bitler 1101000100 şeklindedir ve sırasıyla \, –, /, –, |, |, /, \, |, | polarizasyonlara sahip fotonları kullanmıştır. Bob'un kullandığı filtreler ise +, X, X, +, +, X, X, X, +, X ve elde ettiği bitler de 1001010101 şeklindedir. Alice ile yaptığı görüşmede kullandığı 3., 4., 5., 7., 8. ve 9. filtrelerin doğru olduğunu tespit etmiştir. Bu durumda anahtar 010010 olacaktır.

Eğer Eve bu sürece dahil olmazsa, Alice ve Bob gizli bir ortak anahtara sahip olurlar. Asıl sorun Eve'in de hattı dinlemeye ve Bob gibi rastgele filtreler kullanarak fotonları belirlemeye çalıştığında ne olacağıdır. Bu durumda hattı dinleyen Eve, fotonları ölçtükten sonra bunları Bob'a tekrar göndermelidir. Fotonları göndermediğinde Bob hiçbir veri alamayacağı için iletişim de gerçekleşmez. Eve'in Alice ve Bob'u dinlemeye çalışması durumu, Şekil 8'de görülmektedir.

Elbette ki Eve tahmini olarak seçtiği filtrelerin doğruluğu konusunda bir fikre sahip olamayacaktır ve bunların doğruluğunu test etmek için Alice'i araması olanaksızdır. Ancak yine de Eve, Bob ve Alice arasındaki iletişimi dinleyebilmektedir. Öyleyse Eve bir önceki örnekteki aynı değerler için Bob'un 3., 4., 5., 7., 8. ve 9. filtreleri doğru kullandığını dolayısıyla doğru filtre dizilimini yani X++XX+ filtrelerini öğrenecektir. Eve kendi yaptığı filtre diziliminde ise 2., 3., 8. ve 10. bitlerin doğru olduğunu bilecektir. Bu durumda Eve, Bob ve Alice'in anahtar olarak kullanacakları bitler arasından sadece 3. ve 8. bitlerin değerini bilmektedir.

Bu durum riskli gibi görünse de aslında Alice ve Bob için rahatlatıcı bir durum ortaya çıkmak üzeredir. Çünkü bu yolla Eve sadece anahtarı bulamamakla kalmaz, Alice ve Bob'un kendisini fark etmelerine de neden olur. Şekil 8'de görüldüğü gibi Bob doğru filtreleri kullanarak 010011 verisini elde etmiştir. Ancak Alice'in gönderdiği veriler 010010 şeklindedir. Yapılacak basit testler ile Alice ve Bob'un anahtarlarındaki bu farklılık kolayca belirlenebilecek ve bu gönderimde araya bir dinleyicinin girdiği ortaya çıkartılabilecektir.

3. Materyal ve Yöntem

Bu çalışmada, öncelikle Delphi 7 programı ile TGUID kütüphanesi kullanılarak rastsal sayı üretimine dayanan iki aşamalı bir simülasyon hazırlanmıştır. Simülasyonda BB84 protokolü esas alınmıştır. Bu simülasyonun ilk aşamasında gürültüsüz bir ortamda araya bir dinleyicinin girmediği düşünülerek fotonlar gönderilmiş ve foton sayısına göre alıcının seçtiği rastsal filtrelerle elde edilen ham anahtarların uzunlukları ölçülmüştür. İkinci aşamada ise araya bir dinleyicinin girmesi durumu canlandırılarak, dinleyicinin bu iletişim üzerindeki etkisi ölçülmeye çalışılmıştır.

Her iki aşamada da 50, 100, 150, …., 900, 950 ve 1000 fotondan oluşan dizilerden 1000'er adet olmak üzere, gönderici ve alıcı arasında toplam 20.000 farklı gönderim işlemi gerçekleştirilmiştir. Yapılan her işlem MySQL veritabanı kullanılarak iki ayrı tabloda saklanmıştır. Böylece bu iki tabloya toplam 40000 farklı kayıt eklenmiştir. Bu veritabanından alınan bilgiler, Microsoft Excel programı aracılığıyla değerlendirilmiş ve analiz edilmiştir.

Simülasyonun birinci aşaması, Şekil 7'ye uygun şekilde çalışmaktadır ve gürültüsüz bir ortamda araya giren bir dinleyici olmadan gerçekleştirilen anahtar dağıtımını canlandırmaktadır. Bu amaçla, öncelikle Alice tarafından gönderilecek bitler ve bu bitleri temsil edecek fotonların polarizasyonları rastsal olarak belirlenmektedir. Daha sonra her bir fotonun polarizasyonunu belirlemek için Bob'un kullanacağı filtrelerin konumları rastsal olarak belirlenmektedir. Son aşamada ise fotonlar için seçilen doğru filtreler karşılaştırılarak, oluşan ham anahtarlar saklanmaktadır.

İkinci aşama ise Şekil 8'e uygun şekilde çalışmakta ve yine gürültüsüz bir ortamdaki anahtar dağıtımını canlandırmaktadır. Ancak bu kez araya giren bir dinleyicinin olduğu varsayımı ile hareket edilmektedir. Dolayısıyla birinci aşamadaki ilk adım bu aşamada da tekrar edilmektedir. Yani Alice'in göndereceği bitler ve bu bitleri gösteren fotonların polarizasyonları belirlenir. Ancak bu kez Eve için de tıpkı Bob'da olduğu gibi fotonların polarizasyonlarını belirleyecek rastsal filtreler belirler. Bu filtreler kullanılarak polarizasyonları belirlenen fotonlar, Bob'a gönderilir. Böylece Bob ile Alice'in arasındaki iletişimi kesmemiş olur. Ancak burada, Eve'in kullanmış olduğu yanlış filtreler sonucunda fotonların polarizasyonları rastsal olarak değişmektedir. Dolayısıyla Bob, Alice'in gönderdiği bir fotona uygun filtre seçmiş olsa bile, elde ettiği bit değeri, Alice'in gönderdiği bit değeri olmayabilecektir. Simülasyonun ikinci aşamasının en önemli noktası da işte bu adımdır. Bu adımdan hemen sonra Bob için birinci aşamada gerçekleştirilen işlemler aynen kullanılır. Yani Bob'un seçtiği filtreler ile Alice'in seçtiği foton polarizasyonları karşılaştırılarak oluşan ham anahtarlar saklanır.

Tüm bu süreçlerin kaydedilmesinden sonra aşağıda da açıklandığı gibi her probleme ilişkin bilgiler analiz edilmiştir. Bu analiz sonucunda da bir sonraki bölümde verilen çizelgelere ulaşılmıştır. Yine bu çizelgelerin nasıl oluşturulduklarına ilişkin bilgiler de aşağıda belirtilmiştir.

4. Araştırma Bulguları

Bu simülasyonda, boyutları önceden belirlenmiş 20.000 adet rastsal foton dizisi, gürültüsüz ve dinleyicinin olmadığı bir ortamda gönderilirken, 20.000 foton dizisi de, aynı şekilde gürültüsüz ve bir dinleyicinin olduğu bir ortamda gönderilmiştir.

İlk aşamada gerçekleştirilen gönderim işleminde gönderici, kuantum kanalı üzerinden foton dizilerini gönderirken, BB84 protokolüne göre alıcı tek tek bu fotonlar için rastsal filtreler seçer. Daha sonra, hangi filtreleri seçtiğini alıcıya açık bir kanal üzerinden bildirir ve gönderici bunların hangilerinin doğru olduğunu alıcıya söyler. Bu işleyişi temel alan simülasyon sonuçları Çizelge 1'de verilmiştir.

Çizelge 1'de, gönderilen foton dizilerinin uzunluğu Foton Sayısı, bunların gönderilmesi sonucunda elde edilen ham anahtarların uzunlukları ise Uzunluk ile ifade edilmiştir. % ile belirtilen sütunlarda ise oluşan anahtar uzunluğunun, gönderilen foton sayısına oranının yüzde ile ifadesi bulunmaktadır. Ayrıca gönderilen foton sayısına göre oluşan en uzun ve en kısa anahtarların uzunlukları ile oluşan anahtarların ortalama uzunlukları ve de bunların gönderilen foton sayısına göre yüzdeleri de yine aynı çizelgede yer almaktadır.

Çizelge 1'deki değerlere göre, gürültüsüz bir ortamda ortalama anahtar uzunluğunun, gönderilen foton sayısının yaklaşık yarısı olduğu görülmektedir. Bu oranlar %49.88 ile %50.25 arasındaki çok küçük bir aralıkta değişmektedir. Dolayısıyla ortalama anahtar uzunluğu, gönderilen foton sayısıyla doğrudan bağlantılı değildir ve ortalama anahtar uzunluğu, gönderilen fotonların yaklaşık yarısıdır.

Çizelge 1. Dinleyicinin olmaması durumunda, gürültüsüz bir ortamda gönderilen foton sayısına göre oluşan ham anahtar uzunlukları

Foton Sayısı	En Kısa Anahtar		En Uzun Anahtar		Ortalama Anahtar	
	Uzunluk	%	Uzunluk	%	Uzunluk	%
50	12	24.00	36	72.00	24.95	49.90
100	34	34.00	65	65.00	50.25	50.25
150	57	38.00	96	64.00	74.86	49.91
200	78	39.00	121	60.50	99.99	49.99
250	102	40.80	148	59.20	125.14	50.05
300	118	39.33	178	59.33	149.63	49.88
350	145	41.43	208	59.43	174.59	49.88
400	168	42.00	240	60.00	200.25	50.06
450	191	42.44	260	57.78	224.74	49.94
500	215	43.00	283	56.60	250.23	50.05
550	241	43.82	312	56.73	274.98	50.00
600	262	43.67	338	56.33	300.23	50.04
650	282	43.38	370	56.92	325.48	50.07
700	312	44.57	388	55.43	349.88	49.98
750	332	44.27	427	56.93	374.63	49.95
800	338	42.25	441	55.13	399.34	49.92
850	379	44.59	473	55.65	425.58	50.07
900	407	45.22	501	55.67	449.62	49.96
950	421	44.32	527	55.47	475.00	50.00
1000	445	44.50	559	55.90	500.17	50.02

Daha detaylı incelendiğinde, en kısa anahtar uzunluklarının, gönderilen foton sayısına göre yüzdeleri, foton sayısı arttıkça artmaktadır. Örneğin gönderilen foton sayısı 50 iken, en kısa anahtar uzunluğu bunun %24'ü kadardır. Foton sayısı 100 olduğunda ise en kısa ham anahtarın uzunluğu, bu foton sayısının %34'ü olmaktadır. Foton sayısı 1000'e yaklaştığında ise, bu oran %44'ler seviyesine çıkmaktadır.

Benzer şekilde, en uzun anahtar oranları da foton sayısı arttıkça azalmaktadır. Örneğin gönderilen 50 foton için en uzun anahtarın oranı %72, 100 foton için ise %65'dir. Foton sayısı 1000'e yaklaştığında ise bu oran %55'ler seviyesine gerilemektedir. Bu sonuçlara göre, foton sayısının arttıkça, dağılım normale

yaklaşacağından, oluşan ham anahtarın uzunluğu da foton sayısının yarısına yaklaşmaktadır.

4.1. Birinci Alt Problem (First Sub Problem)

Araya giren bir dinleyicinin neden olduğu hatalı bitlerin oranı ne kadardır? Bu sorunun yanıtını bulmak amacıyla, simülasyonun ikinci aşaması, daha önce değinildiği şekilde canlandırılmıştır. Buna göre, gönderici rastsal olarak seçtiği filtreleri kuantum kanalından göndermiş, bir dinleyici ise bu fotonlar alıcıya ulaşmadan önce, seçtiği rastsal filtreler ile bu fotonların polarizasyonunu belirlemiş ve daha sonra bunların alıcıya ulaşmasına izin vermiştir. Ancak kuantum mekaniğinin ve kuantum kriptografinin en önemli özelliklerinden biri olan gözlemin deneyi etkilemesi prensibine göre, yanlış filtreyle ölçülen fotonların polarizasyon yönleri rastsal olarak değişmiştir. Bu durumda da alıcı doğru filtreyi seçmiş olsa bile, elde ettiği bit yanlış olacaktır. Ancak ham anahtarın oluşturulması, alıcının, rastsal olarak seçtiği filtrelerin gönderilen fotonlara uygunluğunu gönderici ile karşılıklı olarak belirlemesine dayandığından, dinleyicinin doğrudan ham anahtar uzunluğuna bir etkisi olmaz. Bu durum, simülasyonun ikinci aşamasında elde edilen ve Çizelge 2'de verilen veriler yardımıyla da rahatlıkla görülebilmektedir. Çizelge 1'e benzer şekilde, oluşan ham anahtar uzunlukları, gönderilen foton sayısının yaklaşık yarısıdır. Ayrıca en kısa ve en uzun anahtarların, foton sayısına göre oluşma oranları da, Çizelge 1'deki değerlerle örtüşmektedir.

Çizelge 2. Dinleyicinin olması durumunda, gürültüsüz bir ortamda gönderilen foton sayısına göre oluşan ham anahtar uzunlukları

Foton Sayısı	En Kısa Anahtar		En Uzun Anahtar		Ortalama Anahtar	
	Uzunluk	%	Uzunluk	%	Uzunluk	%
50	13	26.00	37	74.00	25.12	50.25
100	32	32.00	65	65.00	49.84	49.84
150	52	34.67	94	62.67	75.06	50.04
200	78	39.00	123	61.50	100.12	50.06
250	102	40.80	147	58.80	125.00	50.00
300	124	41.33	182	60.67	150.67	50.22
350	144	41.14	201	57.43	175.14	50.04
400	167	41.75	233	58.25	200.09	50.02
450	198	44.00	260	57.78	225.18	50.04
500	214	42.80	298	59.60	249.98	50.00
550	239	43.45	307	55.82	274.83	49.97
600	262	43.67	336	56.00	300.17	50.03
650	284	43.69	365	56.15	324.15	49.87
700	309	44.14	394	56.29	349.31	49.90
750	339	45.20	414	55.20	374.95	49.99
800	359	44.88	449	56.13	400.46	50.06
850	369	43.41	475	55.88	424.78	49.97
900	403	44.78	503	55.89	450.22	50.02
950	430	45.26	529	55.68	474.96	50.00
1000	454	45.40	546	54.60	499.79	49.98

Dolayısıyla gönderici ve alıcı, ham anahtarlarında oluşabilecek hatalardan habersiz olacaklardır. Ham anahtarlar üzerinde yapılan kontrolden sonra, Çizelge 3'deki verilere ulaşılmıştır. Bu veriler incelendiğinde, gönderilen foton sayısına göre farklılıklar olsa da araya giren bir dinleyicinin ham anahtar içerisinde neden olduğu hatalı bit oranının %30 civarında olduğu görülmektedir. Bu bilgi gürültülü ortamlar için oldukça büyük önem taşımaktadır. Çünkü gerçek bir uygulamada, ortamdan ya da ölçüm aletlerinden kaynaklanabilecek gürültüler de hatalara sebep olabileceklerdir. Bu hataların oranının %30 seviyesini geçmesi muhtemel bir saldırıya işaret edebilecektir.

4.2. İkinci Alt Problem (Second Sub Problem)

Gönderilen foton sayısının, dinleyicinin neden olduğu hata oranına etkisi var mıdır? Bu sorunun yanıtını

belirlemek için, simülasyonun ikinci aşamasında elde edilen verilerin incelenmesi gerekmektedir. Çizelge 3'de, bir dinleyicinin var olduğu gürültüsüz bir ortamda, alıcı ve göndericinin elde ettikleri ham anahtarlar arasındaki farklı bitlerin değerleri verilmiştir.

Çizelge 3. Dinleyicinin olması durumunda, gürültüsüz bir ortamdaki hatalı bit sayıları

Foton Sayısı	En Az Hatalı Bit		En Çok Hatalı Bit		Ortalama Hatalı Bit	
	Sayı	%	Sayı	%	Sayı	%
50	4	8.00	13	26.00	6.30	12.60
100	7	7.00	36	36.00	21.50	21.50
150	23	15.33	52	34.67	41.44	27.62
200	43	21.50	69	34.50	56.58	28.29
250	59	23.60	84	33.60	70.68	28.27
300	70	23.33	111	37.00	87.57	29.19
350	81	23.14	122	34.86	106.16	30.33
400	99	24.75	146	36.50	123.16	30.79
450	121	26.89	167	37.11	141.57	31.46
500	132	26.40	196	39.20	159.56	31.91
550	152	27.64	203	36.91	178.34	32.42
600	169	28.17	217	36.17	196.78	32.80
650	184	28.31	240	36.92	210.60	32.40
700	203	29.00	262	37.43	227.01	32.43
750	219	29.20	272	36.27	246.00	32.80
800	235	29.38	295	36.88	264.83	33.10
850	241	28.35	314	36.94	280.69	33.02
900	267	29.67	335	37.22	297.95	33.11
950	285	30.00	356	37.47	315.06	33.16
1000	300	30.00	372	37.20	332.89	33.29

Çizelge 3'deki verilere göre, gönderilen foton sayısı 50 olduğunda, ortalama hatalı bit oranı %12 seviyelerindeyken, foton sayısı 1000'e yaklaştığında, ortalama hatalı bit sayısı da %33 seviyelerine gelmektedir. Bu durum, karşılaşılan en az ve en çok hata sayısında da görülmektedir. Tıpkı Çizelge 1 ve Çizelge 2'deki gibi gönderilen foton sayısının artmasıyla bu oranların da ortalamaya doğru yaklaştığı görülmektedir. Örneğin 50 foton gönderildiğinde en az hatanın olduğu durumda oran %8 iken 1000 foton gönderildiğinde ise %30'dur. Aynı foton sayıları için en çok hatayla karşılaşılan durumdaki oranlar ise %26'dan %37'lere çıkmaktadır. Bu nedenle de ikinci alt problemin cevabı, "gönderilen foton sayısının, dinleyicinin neden olduğu hata oranına etkisi vardır" şeklindedir.

4.3. Üçüncü Alt Problem (Third Sub Problem)

Gönderilen foton sayısının, dinleyicinin neden olduğu, polarizasyonu değişen fotonların oranına etkisi var mıdır? Bu soru da, yine simülasyonun ikinci aşamasında elde edilen veriler ile yanıtlanabilir. Çizelge 4'de, bir dinleyicinin var olduğu gürültüsüz bir ortamda, göndericinin gönderdiği fotonlardan, alıcıya polarizasyonu değişerek ulaşanların oranları verilmiştir.

Çizelge 4'deki veriler incelendiğinde, gönderilen foton sayısının artmasının, polarizasyonu değişen en az ve en çok foton sayılarını ortalamaya yaklaştırdığı, ancak ortalama değerlerini değiştirmediği görülmektedir. Polarizasyonu değişen ortalama foton oranının ise %50 civarında olduğu görülmektedir. Bu nedenle üçüncü alt problemin cevabı "gönderilen foton sayısının, dinleyicinin neden olduğu, polarizasyonu değişen fotonların oranına etkisi yoktur" şeklindedir.

4.4. Dördüncü Alt Problem (Fourth Sub Problem)

Gönderilen foton sayısının, dinleyicinin neden olduğu, bit değeri değişen fotonların oranına etkisi var mıdır? Bu sorunun yanıtlanabilmesi için de sümülasyonun ikinci aşamasında elde edilen verilerle oluşturulan Çizelge 5'in incelenmesi gerekmektedir.

Çizelge 4. Dinleyicinin olması durumunda, gürültüsüz bir ortamda polarizasyonu değişen foton sayıları

Foton Sayısı	Polarizasyonu Değişen Foton Sayısı					
	En Az		En Çok		Ortalama	
	Sayı	%	Sayı	%	Sayı	%
50	13	26.00	36	72.00	25.02	50.03
100	34	34.00	68	68.00	49.99	49.99
150	57	38.00	94	62.67	75.00	50.00
200	76	38.00	125	62.50	100.02	50.01
250	98	39.20	150	60.00	124.84	49.93
300	119	39.67	183	61.00	150.11	50.04
350	144	41.14	210	60.00	174.88	49.97
400	164	41.00	232	58.00	199.60	49.90
450	192	42.67	260	57.78	224.90	49.98
500	216	43.20	288	57.60	250.45	50.09
550	234	42.55	311	56.55	275.17	50.03
600	262	43.67	333	55.50	300.31	50.05
650	288	44.31	360	55.38	324.84	49.97
700	312	44.57	389	55.57	351.20	50.17
750	333	44.40	419	55.87	374.68	49.96
800	357	44.63	445	55.63	400.06	50.01
850	369	43.41	469	55.18	425.38	50.04
900	402	44.67	492	54.67	449.13	49.90
950	434	45.68	524	55.16	475.08	50.01
1000	444	44.40	552	55.20	500.45	50.04

Çizelge 5. Dinleyicinin olması durumunda, gürültüsüz bir ortamda bit değeri değişen foton sayıları

Foton Sayısı	Bit Değeri Değişen Foton Sayısı					
	En Az		En Çok		Ortalama	
	Sayı	%	Sayı	%	Sayı	%
50	4	8.00	24	48.00	12.49	24.97
100	11	11.00	38	38.00	25.07	25.07
150	23	15.33	54	36.00	37.56	25.04
200	27	13.50	69	34.50	50.11	25.05
250	43	17.20	85	34.00	62.57	25.03
300	53	17.67	97	32.33	75.31	25.10
350	65	18.57	117	33.43	87.30	24.94
400	73	18.25	127	31.75	99.92	24.98
450	86	19.11	144	32.00	112.75	25.06
500	92	18.40	151	30.20	125.55	25.11
550	103	18.73	169	30.73	137.67	25.03
600	115	19.17	184	30.67	150.47	25.08
650	123	18.92	200	30.77	163.05	25.08
700	137	19.57	213	30.43	175.68	25.10
750	140	18.67	225	30.00	187.21	24.96
800	167	20.88	237	29.63	199.87	24.98
850	173	20.35	259	30.47	212.28	24.97
900	184	20.44	269	29.89	224.86	24.98
950	192	2021	277	29.16	237.88	25.04
1000	207	20.70	295	29.50	251.45	25.14

Çizelge 6. Dinleyicinin, gürültüsüz bir ortamda, doğru olarak yakalayabildiği bit sayıları

Foton Sayısı	Dinleyicinin, Doğru Yakalayabildiği Bit Sayısı					
	En Az		En Çok		Ortalama	
	Sayı	%	Sayı	%	Sayı	%
50	4	8.00	22	44.00	12.43	24.87
100	12	12.00	39	39.00	24.87	24.87
150	21	14.00	54	36.00	37.42	24.94
200	31	15.50	72	36.00	50.20	25.10
250	43	17.20	86	34.40	62.86	25.14
300	50	16.67	98	32.67	75.23	25.08
350	61	17.43	115	32.86	87.50	25.00
400	67	16.75	126	31.50	100.11	25.03
450	83	18.44	146	32.44	112.43	24.98
500	97	19.40	162	32.40	124.92	24.98
550	109	19.82	167	30.36	137.27	24.96
600	121	20.17	185	30.83	150.05	25.01
650	130	20.00	201	30.92	162.13	24.94
700	137	19.57	213	30.43	174.32	24.90
750	151	20.13	229	30.53	188.39	25.12
800	165	20.63	232	29.00	200.25	25.03
850	170	20.00	258	30.35	212.49	25.00
900	190	21.11	267	29.67	225.94	25.10
950	201	21.16	279	29.37	237.73	25.02
1000	205	20.50	291	29.10	249.56	24.96

Çizelge 5'deki verilere göre, gönderilen foton sayısının artmasının, bit değeri değişen en az ve en çok foton sayılarını ortalamaya yaklaştırdığı, ancak ortalama değerlerini değiştirmediği görülmektedir. Bit değeri değişen ortalama foton oranının ise %25 civarında olduğu görülmektedir. Bu nedenle, üçüncü alt probleme benzer şekilde, dördüncü alt problemin de cevabı "gönderilen foton sayısının, dinleyicinin neden olduğu, bit değeri değişen fotonların oranına etkisi yoktur" şeklindedir.

4.5. Beşinci Alt Problem (Fifth Sub Problem)

Gönderilen foton sayısının, dinleyicinin doğru yakalayabildiği bitlerin oranına etkisi var mıdır? Bu yanıt araştırılırken, simülasyonun ikinci aşamasında elde edilen veriler üzerinde bir inceleme yapılmıştır. Öncelikle göndericinin gönderdiği fotonların polarizasyonlarına göre, hem alıcının hem de dinleyicinin seçmiş olduğu filtrelerin doğru olduğu fotonlar ele alınmıştır. Böylece ham anahtar dışında, dinleyicinin elde ettiği bitler önemsenmemiştir. Bunun nedeni, ham anahtar dışında kalan bitler için yapılan ölçümlerin doğru olup olmamasının, anahtarla ilişkili bir bilgi vermemesidir. Bu incelemeden elde edilen veriler Çizelge 6'da verilmiştir.

Çizelge 6'daki değerler de Çizelge 5'de verilen değerlere benzerlik göstermektedir. Çizelge 6'da da yine gönderilen foton sayısı arttığında, dinleyicinin doğru yakalayabildiği bit sayısının ortalama değerlere yaklaştığı ancak yine de bu artışın ortalama değerleri değiştirmediği görülmektedir. Foton sayısı artsa da, dinleyici tarafından yakalanan fotonların ortalamasının %25 civarında olduğu görülmektedir. Buna göre beşinci alt problemin yanıtı da "gönderilen foton sayısının, dinleyicinin doğru yakalayabildiği bitlerin oranına etkisi yoktur" şeklinde olacaktır.

5. Sonuç ve Tartışma

Bu çalışmada, gürültüsüz bir ortamda farklı sayılarda fotonlardan oluşan diziler gönderilerek BB84 Kuantum Anahtar Dağıtımı Protokolüne göre anahtarlar üreten bir simülasyon tasarlanmıştır. Daha sonra bu simülasyon yardımıyla, bir dinleyicinin olması ve olmaması durumunda oluşan anahtar uzunlukları ve araya giren bir dinleyicinin etkisi araştırılmıştır. Bu amaçla belirli sayılarda (100, 150, 200, 250,….950, 1000 gibi) rastsal foton dizileri oluşturulmuş ve bunların her biri dinleyicinin olması ve olmaması durumları için ayrı ayrı 1000'er kez gönderilmiştir. Bu işlemin ardından elde edilen veriler ile aşağıdaki değerlendirmeler yapılmıştır.

1. Gürültüsüz bir ortamda araya giren bir dinleyici olmadığında, anahtar uzunluğu gönderilen foton sayısının yaklaşık olarak %50'si olmaktadır.
2. Gürültüsüz bir ortamda, araya giren bir dinleyicinin, oluşan ham anahtarın uzunluğuna bir etkisi olmamaktadır.
3. Gürültüsüz bir ortamda oluşan anahtar üzerinde, araya giren bir dinleyicinin neden olduğu hatalı bitlerin sayısı, foton sayısının yaklaşık olarak %30'udur.
4. Gürültüsüz bir ortamda, araya giren bir dinleyici varken, gönderilen foton sayısı arttıkça, anahtar üzerinde dinleyicinin neden olduğu hatalı bitlerin oranı artmaktadır.
5. Gürültüsüz bir ortamda, araya giren bir dinleyici varken, gönderilen foton sayısı artmasına rağmen, polarizasyonu değişen fotonların oranında değişme olmamaktadır.
6. Gürültüsüz bir ortamda, araya giren bir dinleyici varken, gönderilen foton sayısı artmasına rağmen bit değeri değişen fotonların oranında değişme olmamaktadır.
7. Gürültüsüz bir ortamda, araya giren bir dinleyici varken, gönderilen foton sayısındaki artış, dinleyicinin doğru yakalayabildiği bitlerin oranını etkilememektedir.

Bu değerlendirmeler doğrultusunda, gönderilen foton sayısındaki artışın, oluşan ham anahtarın uzunluğuna etkisi olmadığı açıktır. Ancak bu değerlendirmeler arasında oldukça önemli bir nokta göze çarpmaktadır. Her ne kadar foton sayısındaki artışın, saldırganın belirlenebilmesi için gereken bilgilere doğrudan bir etkisinin bulunmadığı gözlense de, gönderilen foton sayısı arttıkça dinleyicinin neden olduğu ortalama hata oranının arttığı ve yaklaşık olarak 300'den fazla foton gönderildiğinde bu hata oranının %30 civarında olduğu gözlenmektedir. Çok önemli olan bu durum, BB84 Kuantum Anahtar Dağıtım protokolü kullanılırken, oluşturulacak anahtarın da çok kısa olmamasını gerektirmektedir. Oluşan ham anahtarın uzunluğunun, gönderilen foton sayısının yaklaşık yarısı (%50) olduğu gözlendiğinden, oluşturulacak anahtarın en az 150 bit uzunluğunda olmasının, bir saldırganın varlığını belirlemede oldukça önemli olduğu rahatlıkla söylenebilir. Bu sayede, uzun bir anahtar oluşturulması için gereken foton sayısı da fazla olacaktır. Çok sayıda foton gönderilmesi ise, dinleyicinin neden olacağı hatalı bitlerin oranının yaklaşık olarak belirlenmesine yardımcı olacaktır. Böylece bir dinleyicinin varlığının belirlenebilmesi için ilk adım atılmış olur.

İkinci adım ise uygun bir hata tespit tekniği belirlenmesidir. Gönderici ve alıcı arasında oluşturulan ham anahtarın tüm bitlerinin, açık bir kanaldan iletilmesi gibi bir durum söz konusu değildir. Ancak hem alıcının hem de göndericinin, anahtarın doğruluğundan emin olmaları gerekmektedir. Oluşan ham anahtardaki hataların belirlenebilmesi için, açık bir kanal üzerinden bir dinleyicinin en az bilgiye ulaşabildiği hata tespit teknikleri kullanılmaktadır. Bu teknikler, bu çalışmanın konusu olmamasına karşın,

bu çalışmadan elde edilen bilgiler söz konusu hata tespit tekniklerinin geliştirilmesine ışık tutabilecektir. Örneğin, dinleyicinin neden olduğu hatalı bitlerin oranı yaklaşık %30 olarak belirlenmiştir. Bu bilgi doğrultusunda ortalama hata oranları incelenerek, gürültülü bir ortamda, hataların ne kadarının dinleyici, ne kadarının da ortamdaki ve cihazlardaki gürültüden kaynaklandığı rahatlıkla belirlenebilecektir. Seçilecek olan hata tespit tekniği, hatalı bitlerin oranını yaklaşık olarak belirleyebilirse, bu teknik aynı zamanda bir saldırı tespit tekniği olarak da kullanılabilecektir. Böylece belirlenen hata oranları ile bu simülasyondan elde edilen hata oranları karşılaştırılarak, alıcı ve gönderici arasındaki kuantum iletim kanalında, bir dinleyicinin varlığı belirlenebilecektir.

Conflict Of Interest

No conflict of interest was declared by the authors.

Kaynaklar

Algan, S., 2008. İnternet: "Kuantum Kriptografi (Quantum Cryptography) Nedir?", http://www.csharpnedir.com/makalegoster.asp?MId=223

Bennet, C. H., ve Brassard, G., 1984. "Quantum cryptography: public key distribution and coin tossing,", Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, New York, s. 175–179.

Bruen, A. A. ve Forcinito, M. A., 2005. Cryptography, Information Theory and Error-Correction, John Wiley & Sons, New Jersey.

Canbek, G. ve Sağıroğlu, Ş., 2006. Bilgi Ve Bilgisayar Güvenliği: Casus Yazılımlar Ve Korunma Yöntemleri, Grafiker Yayınları, Ankara.

Çimen, C., Akleylek, S. Ve Akyıldız, E., 2008. Şifrelerin Matematiği:Kriptografi, Ankara: ODTÜ Yayıncılık

Dalkılıç, G., Ayhan, E., 2005, Kuantum Kriptografide Dinleme (Eavesdropping) ve Optik Açıklar (Loopholes) Kullanılarak Gerçekleştirilen Ataklar, Akademik Bilişim Konferansı, Gaziantep

Diffie, W. ve Hellman, M. 1976. "New Directions in Cryptography", IEEE Transactions on Information Theory, 22 (6) 644–654

Kale, Z., 2005. Low Temperature Operation Of APD For Quantum Cryptographic Applications, (Yayımlanmamış Yüksek Lisans Tezi), ODTÜ, Fen Bilimleri Enstitüsü.

Marinescu, D. C. ve Marinescu, G. M., 2005. Approaching Quantum Computing, Prentice Hall, New Jersey.

Öztarhan A., Kubilay A. ve Ünal D., 2005. "Nicem Hesaplama (Quantum Computation) ve Bilgi Güvenliğinin Yeni Rotaları", Ağ ve Bilgi Güvenliği Ulusal Sempozyumu – ABG 2005, İstanbul, s. 153-156.

Rivest, R. L., Shamir, A. ve Adleman, L., 1978. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, 21 (2) 120-126

Sağıroğlu, Ş. ve Alkan, M., 2005. Her Yönüyle Elektronik İmza, Grafiker Yayınları No:27, Ankara.

Şahin, A. B. ve Selçuk, G., 2006 "İletişim Ağ Güvenliğinde Son Aşama: Kuantum Kriptografi ve Fiber Optik Ortamda Kuantum Temelli Rastsal Sayı Üretimi", Ulusal Elektronik-İmza Sempozyumu, Ankara, 57.

Shannon, C.E., 1949, "Communication Theory of Secrecy Systems", Bell Systems Tech Journal, 28: 656-715.

Singh, S., 2004. Kod Kitabı, İstanbul: Klan Yayınları, Çev: Cemal Hamitoğulları ve Emin Yaşar Sınır

Spillman, R. J., 2005. Clasical and Contemporary Cryptography, Prentice Hall, New Jersey.

Stolze, J. ve Suter, D., 2004. Quantum Computing: A Short Course from Theory to Experiment, Wiley-VCH, Weinheim.

Toyran, M., 2007. "Quantum Cryptography", Signal Processing and Communications Applications, Eskişehir, S. 1-4.

Trappe, W. ve Washington, C., 2002. Introducing to Cryptography with Coding Theory, New Jersey: Prentice Hall