Kuantum Kriptografi ve Anahtar Dağıtım Protokolleri

Ergün Gümüş[1]

[1]İstanbul Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul

egumus@istanbul.edu.tr

Özet: Günümüze kadar verinin gizliliğini sağlamak amacıyla pek çok matematiksel yöntem öne sürülmüştür. Bu yöntemlerin şifreleme gücü, dayandıkları algoritmanın çözümü için gerekli süreyle doğru orantılıdır. Dolayısıyla bu yöntemler verinin güvenliğini sadece sınırlı bir süre boyunca garanti edebilmektedir ve bu süre her geçen gün gelişen bilgisayar sistemleriyle kısalmaktadır. Veriyi elektriksel işaretler yerine foton olarak adlandırılan ışık tanecikleriyle tanımlayıp işleyebilen kuantum bilgisayarların kullanılmasıyla söz konusu sürenin artık veri güvenliğini sağlayamayacak kadar kısalması öngörülmektedir. Bu noktada, artık verinin saklanmasından ziyade güvenli bir şekilde iletildiğinden emin olunabilecek yöntemler aranmaya başlanmıştır. Kuantum kriptografi, matematik kuralları yerine fizik kurallarına dayandığından bu yönde iyi bir aday olarak ön plana çıkmaktadır. Bu çalışmada kuantum kriptografinin dayandığı ilkeler, anahtar dağıtım ve oluşturma yöntemleri işlenmiştir.

Anahtar Sözcükler: Kuantum Kriptografi, Kuantum Anahtar Dağıtım Protokolleri, Optik Ağlar, BB84, B92, SARG

Quantum Cryptography and Key Distribution Protocols

Abstract: Till present day, many mathematical approaches have been proposed in order to provide data privacy. Encryption power of these techniques is positively correlated with the time required to break them. Thus, they guarantee data security only for a limited period of time which has been getting shorter because of developing computer systems. It is foreseen that this period of time will not be long enough to provide data security after usage of quantum computers which express data as light particles called photons instead of electrical signals. At this point a search for new techniques that guarantees private data transfer rather than encryption has been initiated. Quantum cryptography is a good candidate for this search because it is based on physics laws instead of mathematics. In this study, principles of quantum cryptography, key distribution and formation techniques have been explained.

Keywords: Quantum Cryptography, Quantum Key Distribution Protocols, Optical Networks, BB84, B92, SARG

1. Giriş

Veri gizliliği tarih boyunca önemini korumuş bir kavramdır. Bu amaçla matematikçiler, Sezar şifresinden günümüze kadar hesaplama karmaşıklığına dayanan pek çok şifreleme yöntemi geliştirmişlerdir. Söz gelimi bu yöntemlerden RSA, çok büyük sayıların asal bileşen analizinin zorluğuna[1] dayanırken, Eliptik eğri şifreleme yöntemi ayrık logaritma probleminin çözümünün zorluğuna dayanmaktadır.

On yıl önce, bu yöntemlerle şifrelenmiş verinin istenmeyen kişilerin eline geçmesinin teorik olarak yüz binlerce yıl süreceği düşünülmekteydi. Çünkü işlemciler ne kadar hızlanırsa hızlansın, sistemler ne kadar dağıtılmış olursa olsun mevcut donanım elektrik sinyallerinin iletimine dayanmaktaydı. Veriyi ifade etmek için

elektrik sinyallerinin yerine evrende bilinen en hızlı enerji olan ışığın kullanılması fikri "kuantum hesaplama" kavramını doğurmuş ve eski donanımlarla çözümü binlerce yıl sürecek olan problemlerin kuantum bilgisayarlar ile saatler içinde çözülebileceği görülmüştür. Bu durum, ilgiyi verinin şifrelenmesinden ziyade güvenli bir şekilde iletilmesine kaydırmıştır. Bu noktada mevcut şifreleme yöntemleri için bir tehdit haline gelen kuantum mekaniği çözümü de "Kuantum Kriptografi" kavramı ile beraberinde getirmiştir.

Kuantum kriptografi, temel bir fizik kanunu olan Heisenberg'in belirsizlik ilkesine dayanmaktadır. Bu ilkeye göre, kuantum fiziğinde bir nesnenin (foton) aynı anda iki özelliği (konum ve momentum) birden ölçülemez ve bu özelliklerden biri için sırayla yapılan ilk ölçüm ikinci ölçümün sonucunu belirsiz hale getirir. Bu ilke, optik hatlar üzerinden iletilen en küçük ışık parçacığı olan fotonun, polarizasyonuna bağlı olarak taşıdığı verinin (kubit) arka arkaya yapılacak ölçümler (okumalar) ile bozulacağını öne sürmektedir. Hatasız iletim hatlarında kaynaktan hedefe iletilmekte olan verinin bozulması, arada istenmeyen bir şahıs tarafından verinin okunmaya çalışıldığı anlamına gelir. Bu durumda alıcı ve gönderici taraflar hattın dinlenip dinlemediğinden emin olabilir. Ancak günümüz teknolojisiyle optik hatlar üzerinde hatasız veri (kuantum kriptografi için "anahtar") iletimi mümkün değildir. Bu nedenle hat üzerinden iletilen anahtarın kabulü ve düzeltilmesi için çeşitli anahtar dağıtım protokolleri öne sürülmüştür. Bu protokoller ikinci bölümde incelenmiştir.

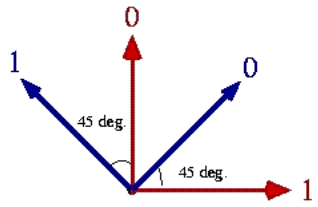
2. Kuantum Anahtar Dağıtım Protokolleri

Günümüze kadar kuantum kriptografi'de kullanılmak üzere pek çok anahtar dağıtım yöntemi öne sürülmüştür. Bu protokollerin başlıca örnekleri şu şekildedir:

2.1 BB84 (Bennett&Brassard 1984)

İlk anahtar dağıtım protokolü olan BB84, IBM araştırma bölümünden Charles Bennett ve Montreal üniversitesinden Gilles Brassard tarafından öne sürülmüştür. Bu nedenle literatürde kendisinden sonra önerilen diğer protokollerle en fazla karşılaştırılan protokoldür.

Bu protokolde anahtar iletimi için dört farklı tipte polarizasyon açısına sahip fotonlar kullanılmaktadır. Şekil 1'de görülen bu dört polarizasyon açısı iki farklı kubit değerini simgelemektedir.



Şekil 1. BB84 protokolü için polarizasyon-kubit değeri eşleşmesi

45º ve 90º polarizasyona sahip fotonların 0 anlamlı bir kubit bilgisini taşıdığı, 0º ve 135º polarizasyona sahip fotonların da 1 anlamlı kubit bilgisini taşıdığı görülmektedir. Bu seçim isteğe göre düzenlenebilir. Ancak bu eşleşme doğru gönderim/okuma işlemi için hem gönderici hem de alıcı tarafta aynı şekilde belirlenmelidir.

Sistemde fotonlar – , /, | , \ tipinde 4 farklı polarizasyon temelinden geçirilerek sırasıyla 0º, 45º, 90º ve 135º polarizasyonlara sahip olmakta ve yine bu fotonlar + (düz) veya × (köşegen) tipte ikili filtrelerden geçirilerek okunmaktadır[2]. Düz ve köşegen filtrelerin ikisi de 0 ve 1 değerli kubit'leri okuyacak yapıya sahiptir.

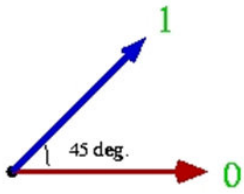
Anahtar iletimi sonunda gönderici ve alıcı açık bir kanaldan iletişime geçerek her bit için sırayla kullandıkları filtrelerin tipini birbirleriyle paylaşmakta ve gönderim ve

alım sırasında aynı tipte filtre kullanılmayan bitleri kalıcı olarak elemektedir.

Bu protokol "araya giren" (man in the middle) ve "foton kopyalama" (photon number splitting) tipi saldırılara açıktır. Çünkü alıcı okuma işlemi sırasında kullandığı filtrelerin tipini açıklamaktadır.

2.2 B92 (Bennett 1992)

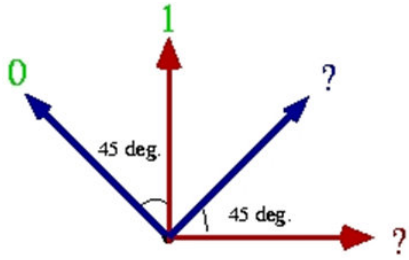
BB84'ün geliştiricilerinden Charles Bennett tarafından öne sürülmüştür. Bu protokolde her kubit Şekil 2'de görüldüğü gibi 0º veya 45º polarizasyonla ifade edilir[3].



Şekil 2. B92 protokolü için polarizasyon-kubit değeri eşleşmesi

0º polarizasyona sahip fotonlar 0 kubit anlamını 45º polarizasyona sahip fotonlar ise 1 kubit anlamını taşımaktadır.

Alıcı gönderilen fotonları okumak için BB84 protokolünde olduğu gibi düz ve köşegen filtreler kullanır. Ancak polarizasyonunu 0º veya 45º olarak okuduğu fotonları eleyerek anahtara dahil etmez. 90º ve 135º açıya sahip okumaları geçerli kabul eder. Bu durum Şekil 3'de görülmektedir.



Şekil 3. B92 protokolü için okuma basamağında polarizasyon-kubit değeri eşleşmesi

Bu durumda Tablo 1'de görülen polarizasyon ve filtre eşleşmeleri için ilgili sonuçlar oluşacaktır.

Görüldüğü üzere, BB84 protokolünde alıcı ve göndericinin aynı tip filtre kullanmamasına bağlı olarak bir fotonun geçerli kabul edilme olasılığı %50 iken B92 protokolünde bu oran %33'e inmektedir. Bu da söz konusu iki protokol kıyaslandığında eşit uzunlukta anahtarların oluşturulabilmesi için B92 protokolüyle yapılan iletimin BB84 protokolüne göre daha uzun sürmesi gerektiği anlamına gelmektedir. B92 protokolü bu yönden dezavantaja sahipken "araya giren" (man in the middle) tipi saldırılarda daha yüksek dinleme tespit oranı sağlayarak güvenlik açısından bir avantaj elde etmektedir. Bu durum Tablo 2'de görülmektedir. Buna göre BB84 protokolünde geçerli kabul edilen bitlerin %40'ının dinlendiği anlaşılırken B92 protokolünde bu oran %50'ye çıkmaktadır.

Yollanan Kubit	Foton Polarizasyonu	Okuma Filtresi	Okunan Polarizasyon	Okunan Değer	Sonuç
1	/	×	/	?	Geçersiz
0	–	+	–	?	Geçersiz
1	/	+	|	1	Geçerli
1	/	+	–	?	Geçersiz
0	–	×	/	?	Geçersiz
0	–	×	\	0	Geçerli

Tablo 1. İletimleri B92 protokolüyle yapılan altı kubit için olası okuma sonuçları

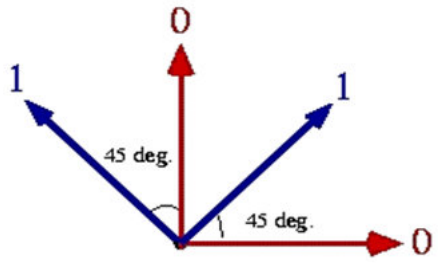
Gönderen	Dinleyen		Alıcı		BB84		B92	
Çıkış	Filtre	Çıkış	Filtre	Çıkış	Durum	Dinleme	Durum	Dinleme
–	+	–	+	–	OK	Yok	NOK	
–	+	–	×	/	NOK		NOK	
–	+	–	×	\	NOK		OK	Yok
–	×	/	+	–	OK	Yok	NOK	
–	×	/	+	|	OK	Var	OK	Var
–	×	/	×	/	NOK		NOK	
–	×	\	+	–	OK	Yok	NOK	
–	×	\	+	|	OK	Var	OK	Var
–	×	\	×	\	NOK		OK	Yok

Tablo 2. 0º polarizasyona sahip bir fotonun BB84 ve B92 protokolleriyle iletilmesi sonucu dinleme saldırısının tespit durumu

2.3 SARG (Scarani&Acin&Ribordy&Gisin)
2004 yılında öne sürülen ve kuantum kriptografinin ticari uygulamalarında[4] kullanılmaya başlayan yeni bir protokoldür. Yöntem, henüz icat edilmemiş ancak gelecekte kullanılması öngörülen teknolojilerin BB84 türü protokoller için ne kadar büyük bir risk oluşturduğunu göstermektedir[5].

Günümüz kuantum anahtar iletimi uygulamalarında fiber optik kablo ya da ışın dalgası iletimi (lightwave transmission) türü hatlar kullanılmaktadır. Ancak bu uygulamalarda karşılaşılan güçlüklerden biri "pulse generator" olarak bilinen foton üreteçlerinin bir kubit'in iletimi esnasında sadece bir adet foton üretememesi bunun yerine aynı polarizasyona sahip birden fazla foton üretmesidir. BB84 protokolü için risk de tam bu noktada doğmaktadır. Daha önce de belirtildiği gibi BB84 protokolünde gönderim tamamlandıktan sonra alıcı, okuma işleminde kullandığı filtreleri açık bir kanaldan gönderen kişiye bildirmekteydi. Eğer hattı dinleyen kişi her kubit için üretilip yollanan N adet fotondan birer tane yakalayıp okuma işleminde kullanılan filtre tipleri açık kanaldan yayınlanana kadar kuantum belleklerde[6] saklayabilirse anahtarı öğrenebilir. Bu saldırılar PNS (Photon Number Splitting) türü saldırılar olarak bilinmektedir.

BB84'ün PNS tipi saldırılara karşı ne kadar savunmasız olduğunu gören Scarani ve arkadaşları açık kanaldan yapılan anahtar doğrulama işlemini düzenlemişlerdir. Yeni modele göre alıcı, okuma işleminde kullandığı filtreleri açıklamamakta sadece gönderen taraf gönderdiği polarizasyonu ve bu polarizasyonla 45º açı yapan başka bir polarizasyonu açıklamaktadır. Eğer alıcı açıklanan polarizasyonlardan herhangi birine dik açıda bir okuma yapmışsa ilgiliyi okumayı geçerli saydığını karşı tarafa bildirir ve okuduğu kubit'in tümleyenini anahtara ekler. Bu protokolde gönderim işlemi için polarizasyon-kubit ilişkisi ve 0º polarizasyona sahip bir fotonun olası altı farklı iletimi için oluşan durumlar sırasıyla Şekil 4 ve Tablo 3'de görülmektedir.



Şekil 4. SARG protokolü için polarizasyon-kubit değeri eşleşmesi

Gönderim Polarizasyonu	Açıklanan Pol. Çifti	Okuma Filtresi	Okunan Polarizasyon	Kabul Durumu	Kubit Değeri
–	/ –	+	–	Geçersiz	
–	/ –	×	/	Geçersiz	
–	/ –	×	\	Geçerli	0
–	\ –	+	–	Geçersiz	
–	\ –	×	/	Geçerli	0
–	\ –	×	\	Geçersiz	

Tablo 3. 0º polarizasyona sahip bir fotonun SARG protokolüyle olası altı farklı iletimi

3. Kuantum Anahtar Oluşturma Basamakları

Optik hat üzerinden yapılan iletim sonucunda toplanan kubit'ler dört ana basamaktan geçtikten sonra şifreleme işleminde kullanılacak olan asıl anahtar elde edilir. Bu basamaklar şu şekilde sıralanabilir:

3.1 Ham Anahtar Çıkarımı (Raw Key Extraction)

Bu basamak, telefon, faks, internet vb. açık hatlar üzerinden gerçekleştirilir ve farklı gönderilen/alınan kubit'lerin elenmesini sağlar.

BB84 protokolü kullanıldığında bu basamakta alıcı okuma işleminde kullandığı filtreleri, gönderici de gönderim işleminde kullandığı bazı içeren filtre tipini açıklar. Aynı bit için taraflar farklı filtreler kullanmışsa ilgili bit kalıcı olarak elenir.

B92 protokolünde gönderici sadece iki baz kullandığından kullandığı filtreleri açıklaması söz konusu değildir. Bunun yerine sadece alıcı, geçerli olarak okuduğu bitlerin indislerini göndericiye yollar ve kalan bitler iptal edilmiş olur.

SARG protokolünde ise gönderici gönderdiği her bit için iki farklı polarizasyon açıklar, alıcı da bunlardan geçerli saydıklarının bit pozisyonlarını açıklar.

3.2 Hata Oranı Tespiti (Error Estimation)

Optik hatlarda hatalı kubit iletimi sadece hattı dinleyen bir saldırgandan değil aynı zamanda hattaki fiziksel gürültüden de kaynaklanabilir. Bu basamakta hat gürültüsünün ardına saklanan bir saldırganın tespit edilmesi ön görülmektedir. Bunun için taraflar önceden hattın dinlenmediğinden emin oldukları bir anda anahtar iletimi gerçekleştirip bu iletimde hat gürültüsü nedeniyle hatalı iletilen kubit'lerin sayısından bir **Rmax** hata oranı belirler. Daha sonraki iletimlerde de elde ettikleri ham anahtardan rastgele seçilen bit pozisyonlarındaki bitleri karşılaştırıp **R** hata değerini belirler ve $\mathbf{R} \leq \mathbf{Rmax}$ için hattın dinlenmediğinden emin olurlar.

3.3 Anahtar Uzlaşımı (Key Reconciliation)

Taraflar hattın dinlenmediğinden emin olsalar bile fiziksel gürültü nedeniyle ellerindeki bitlerin bir kısmı hatalı olabilir. Bu basamakta bu hataların elenmesi hedeflenir.

Bu amaçla taraflar anahtarlarındaki hatalı bitlerin tüm anahtar boyunca eşit yoğunlukta dağıldığından emin olmak için anahtarlarını önceden belirledikleri bir permütasyona göre yeniden sıralar. Sonrasında anahtarlarını **k** bitlik alt bloklara bölüp her bloğun eşlik bitini yayınlarlar. Eşlik biti farklı olan her

blok ikili arama (binary search) yöntemi ile alt bloklara bölünür ve bu alt blokların eşlik bitleri karşılaştırılır[7]. Bu işlemler iki taraf da anahtarın doğruluğundan emin oluncaya dek daha büyük **k** değerleri için tekrarlanır.

3.4 Gizlilik Artırımı (Privacy Amplification)

Bu basamak, saldırganın anahtarda bildiği bit sayısını en aza indirgemek için uygulanır. Bu amaçla anahtar, taraflarca önceden belirlenen sayıda alt bloğa bölünür ve blokların eşlik biti değerlerinin birleşimi şifreleme algoritması için yeni anahtar olarak kabul edilir.

4. Sonuç

Bu çalışmada kuantum kriptografi'nin matematiksel şifreleme yöntemlerine göre avantajına değinilmiş ve mevcut anahtar dağıtım protokolleri incelenmiştir. Bu protokollerin zaman içerisindeki değişimi sürekli olarak donanımdaki gelişime ve kusurlardan kaynaklanabilecek olası saldırılara bağlı olmuştur.

70'li yıllarda Stephen Wiesner'in "Eşlenik kodlama" [8] isimli kuantum bilgi saklama sistemi kuantum anahtar dağıtımı için öncü olmuş, laboratuar ortamında birkaç santimetre mesafeden yapılan denemeler takip eden yıllarda bilgi güvenliği alanında hizmet sunan firmalarca (ID Quantique, MagiQ Technologies gibi) yüz kilometrelerle ifade edilen optik hatlarda çalışan ticari uygulamalara dönüşmüştür. Gelişen foto dedektör ve optik yineleyici teknolojisi sayesinde bu mesafenin artışı kaçınılmaz olacaktır. 2003 yılında ABD savunma bakanlığınca kurulan altı düğümlü ilk kuantum kriptografi bilgisayar ağı [9] ve Avrupa Birliğinin desteğiyle 2004 yılında çalışmalarına başlanan ve 2008 yılında Viyana'da uygulaması yapılan SECOQC (Secure Communication based on Quantum Cryptography) projesi bu gelişimin en heyecan verici sonuçlarındandır.

5. Kaynaklar

[1] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining Digital Signatures and Public Key Cryptosystems", **Communications of the ACM**, Feb. 1978 21(2) p: 120-126

[2] C. H. Bennett & G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing", **in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing**, Bangalore, p. 175 (1984)

[3] C. H. Bennett, "Quantum Cryptography: Uncertainty in the Service of Privacy", **Science**, vol. 257, p. 752-753 (1992)

[4] CLAVIS^2 URL: http://www.idquantique.com/images/stories/PDF/clavis2-quantum-key-distribution/clavis2-specs.pdf

[5] Valerio Scarani, Antonio Acin, Gregoire Ribordy, Nicolas Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations", **Quantum Physics**, Phys. Rev. Lett. 92, 057901 (2004)

[6] Morgan P. Hedges, Jevon J. Longdell, Yongmin Li, Matthew J. Sellars, "Efficient quantum memory for light", **Nature**, Vol: 465, p: 1052–1056, 2010

[7] N. K. Papanikolaou, "Techniques for design and validation of quantum protocols", Master's thesis, Department of Computer Science, University of Warwick, 2005.

[8] Wiesner S., "Conjugate Coding", Sigact News, Vol: 15, No: 1, p: 78-88, 1983

[9] Press Releases, "BBN Technologies Unveils World's First Quantum Cryptography Network", 2004