Kara Harp Okulu Bilim Dergisi
Science Journal of Turkish Military Academy
Aralık /December 2019, Cilt/Volume 29, Sayı/Issue 2, 179-202.
ISSN (Basılı) : 1302-2741 ISSN (Online): 2148-4945

KUANTUM KRİPTOANALİZİN SİBER SAVUNMADAKİ YERİ

Muharrem Tuncay GENÇOĞLU[1]

Öz

Bu çalışmada gelişen kuantum teknolojileri ile birlikte siber dünyada güveliğin öneminin daha da belirginleşmesi nedeniyle bu alanda kullanılan kuantum teknikler anlatılmaya çalışılmıştır. Bu doğrultuda kuantum mekaniği hakkında temel bilgiler de verilmiştir. Ayrıca modern kriptografide, kriptografik algoritma ve protokol parametrelerinin, şifreleme ve şifre çözme anahtarlarının oluşturulmasında esas teşkil eden rastgele sayıları üretmek için kuantum fiziğini kullanan kuantum rastgele sayı üretiminden bahsedilmiştir. Modern kripto sistemlerde en ciddi sorun olan gizli anahtarın güvenliğini, teknolojik gelişmelerden etkilenmeden ve kalıcı olarak gizliliğini sağlayan, bir başka deyişle, siber alandaki güvenliği kuantum mekaniğine dayanarak sağlayan kuantum kriptografi açıklanmıştır. Kuantum Anahtar Dağıtım (KAD) protokolleri ve bunların çalışma ilkeleri belirtilmiştir.

Kuantum kriptografinin olduğu yerde mutlaka, kriptografinin aksine gizli yazıları çözme ve okuma sanatı ya da bilimi olarak tanımlanan kriptanalizin kuantum alanında da var olan, kuantum kriptanaliz de olmak zorundadır. Kuantum Kriptoanaliz, bazı kuantum mekaniksel sistemlerden, bir takım kuantum mekaniksel etkilerden yararlanarak yani kısacası kuantum bilgisayarlar kullanarak şifre kırmayla ilgilenen kriptografik bir uygulama alanıdır. Kuantum kriptoanalizde kullanılan algoritmalara değinilmiş ve bunları işletecek kuantum bilgisayar anlatılmıştır. Yaşanan bilimsel ve teknolojik gelişmelerin gerisinde kalmamak adına hızlı bir şekilde KRSÜ, kuantum kriptografi, kuantum kriptoanaliz, kuantum bilgisayar, kuantum haberleşme gibi teknolojiler üzerinde yoğunlaşılması gerektiği sonuç kısmında özellikle vurgulanmıştır. Hem kuantum kriptografi hem de kuantum kriptoanaliz hakkında yeteri kadar Türkçe kaynağın olmaması nedeniyle bu araştırma makalesi, millî siber güvenlik çalışmalarına katkıda bulunması amacıyla kaleme alınmıştır.

Makalenin Türü: *Araştırma Makalesi*

Anahtar Kelimeler: *Siber Savunma, Kuantum Algoritmaları, Kuantum Rastgele Sayı Üreteci, Kuantum Kriptoanaliz.*

Jel Kodu: *C65, Z19*

The Role of Quantum Cryptanalysis in Cyber Defense

Abstract

The importance of security in cyber world becomes clear as a result of developing quantum technologies. Therefore, in this study, quantum techniques used in cyber defense are tried to be explained. In this respect, basic information about quantum mechanics is given. Furthermore, the generation of quantum random numbers that uses quantum physics to generate random numbers that are essential in the generation of cryptographic algorithms and protocol parameters, encryption and decryption keys in modern cryptography is mentioned. Quantum cryptography that provides the security of the secret key that is not affected by technological developments and that provides permanent confidentiality has been explained. The security of the secret key is the most serious problem in modern cryptosystems. Quantum Key Distribution (KAD) protocols and their working principles are mentioned.

Where quantum cryptography exists, there must be quantum cryptanalysis that is defined as the art or science of decoding and reading encrypted information. Quantum Cryptanalysis is a cryptographic field of application which deals with the decryption of keys by using some quantum

[1] Dr. Öğr. Üyesi, Fırat Üniversitesi Bilgisayar Teknolojileri Bölümü, mt.gencoglu@firat.edu.tr, ORCID: 0000-0002-8784-9634

Geliş Tarihi / Arrived : 16.10.2019
Kabul Tarihi / Accepted : 21.11.2019

mechanical systems and quantum mechanical effects, briefly quantum computers. The algorithms used in quantum cryptanalysis are mentioned and the quantum computer to operate them is explained. In order to avoid lagging behind the scientific and technological developments, it has been emphasized in the conclusion that urgent technologies such as KRSÜ, quantum cryptography, quantum cryptanalysis, quantum computer, and quantum communication should be focused on. Due to the lack of sufficient Turkish resources on both quantum cryptography and quantum cryptanalysis, this research article was written in order to contribute to national cyber security studies.

Article Type: *Research article*

Key Words: *Cyber Defence, Quantum Algorithms, Quantum Random Number Generator, Quantum Cryptanalysis*

Jel Code: *C65, Z19*

GİRİŞ

Verilerin işlenmesi esnasında iç/dış tüm casusluk türü saldırılara karşı korunması ve iletimi; saklanması esnasında güvenliğinin sağlanması siber güvenlik olarak tanımlanabilir. Bilginin bir takım yerine koyma, yer değiştirme veya matematiksel formülasyonlarla okunamaz yapıldığı geri dönüşümlü yöntemler gizli yazı yazma sanatı olarak bilinen kriptografi biliminin konusudur. Kriptografi; bilginin güvenliğini sağlamak amacıyla şifreleme ve şifre çözme işlemleri ile ilgilenmektedir. Bu nedenle siber dünyada güvenlik genellikle kriptografi yöntemleri kullanılarak sağlanır. Modern kriptografinin iletişim güvenliğini sağlamada ortaya koyduğu ana hizmetleri; gizlilik, bütünlük, kimlik doğrulama ve inkâr edememedir. İhtiyaca göre bunların birinden, bir kaçından ya da tamamından faydalanmak gerekebilir. Siber dünyada bugün güvenli iletişim için kullanılan esas araç kriptografidir.

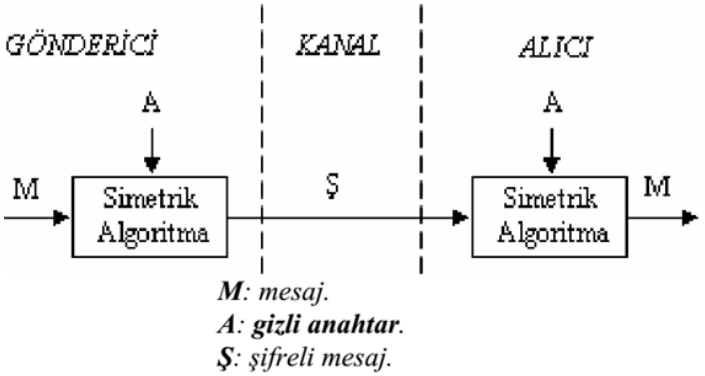
Çalışmanın bundan sonraki kısmında; II. bölümde modern kriptografi, III. bölümde kuantum mekaniğine temel seviyede değinilecektir. Ardından IV. bölümde kuantum rastgele sayı üretimi, V. bölümde kuantum kriptografi, VI. bölümde kuantum kriptanaliz konuları ele alınacak ve VII. bölümde sonuçlar yer alacaktır.

Modern Kriptografi

Kriptografinin gizlilik hizmeti, alıcı dışındaki hiç kimsenin bilgiyi okuyamamasını garantiler. Bu amaçla, bilgiyi şifreleme de kullanılan başlıca yöntemdir.

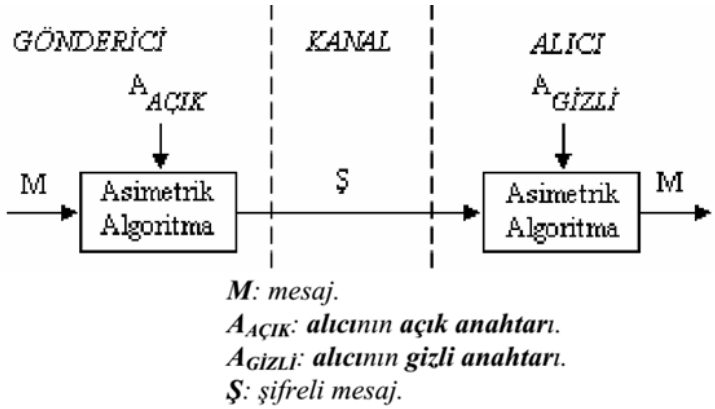
Günümüzde simetrik ve asimetrik şifreleme sistemleri olarak adlandırılan iki tür şifreleme sistemi kullanılır (Toyran, 2011). Simetrik sistemlerde gönderici ile alıcı şifreleme ve şifre çözme işlemi için ortak gizli anahtarı kullanır. Şekil 1'de bir simetrik şifreleme görülmektedir. Simetrik şifreleme sistemleri hızlı olduklarından dolayı şifreleme işlemlerinde daha

çok kullanılırlar. Vernam, DES, AES, IDEA, RC4 gibi algoritmalar sıkça tercih edilen şifreleme algoritmalarıdır.



Şekil 1 Simetrik Şifreleme

Asimetrik şifreleme sistemlerinde, açık anahtar ve gizli anahtar olmak üzere iki farklı anahtar kullanılır. Şekil 2'de bir asimetrik şifreleme görülmektedir. Şifreleme için açık anahtar kullanılır ve bu anahtar aşikârdır. Şifre çözmede ise gizli anahtar kullanılır, bunu da sadece alıcı bilmelidir. Açık anahtarla şifrelenen bir bilgiyi yalnızca (Açık Anahtar, Gizli Anahtar) çiftini elinde bulunduran çözebilir. Asimetrik sistemler yavaş olması nedeniyle, daha çok e-imza, gizli anahtar dağıtımı ve rastgele sayı üretimi gibi kısa uzunluktaki mesajları şifrelemek için kullanılır. RSA, Diffie-Helman, El Gamal, DSS en sık kullanılan asimetrik şifreleme algoritmalarıdır. Modern kriptografide algoritmalar gizli değildir herkese açıktır ve asıl gizlenen gizli anahtardır.



Şekil 2 Asimetrik Şifreleme

Modern kripto sistemlerde güvenliğin bağlı olduğu başlıca parametre gizli anahtardır. Gizli anahtar:

-Oldukça güvenilir üreteçler vasıtasıyla ve asla tahmin edilmemeli prensibine dayalı olarak üretilmelidir.

-Üretilen anahtarlar kullanıcılara güvenli bir şekilde dağıtılmalıdır.

-Kullanılan anahtarların güvenli bir şekilde imha edilmesi yani yönetimidir (Boyacı, 2013).

Kuantum Mekaniği

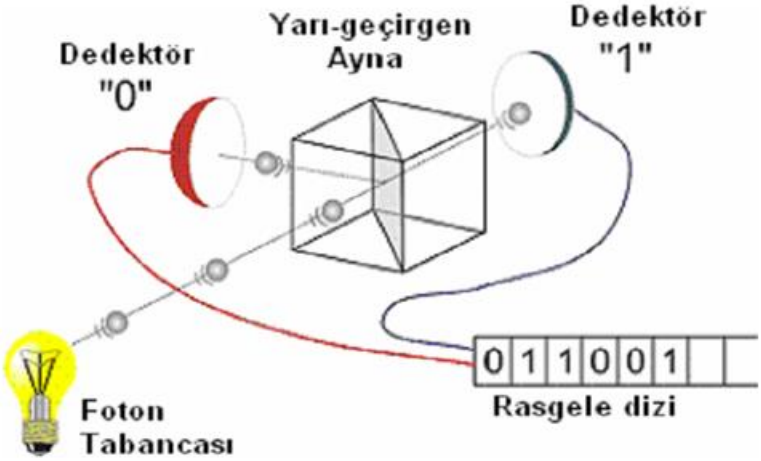
Kuantum mekaniği; atomlar ve atomların altı parçacıkları olarak adlandırılan çekirdek, elektron, foton gibi mikroskobik sistemler seviyesinde maddenin davranışlarını ve enerji ile etkileşimini matematiksel olarak ifade eden fizik yasalarının bütünüdür. Kuantum mekaniği, Planck yasası ile başlamış; Einstein, Bohr, Heisenberg, Born, Neumann, Dirac, Pauli gibi bilim adamlarının çalışmalarını kapsayan uzun bir dönemde gelişmiştir. Nihayet 1927'de Schrödinger denkleminin bulunmasıyla bugünkü hâline gelmiştir. Kuantum mekaniği, atom, elektron, foton gibi mikroskobik sistemlerin davranışlarını açıklayan doğanın ya da hareketin yeni teorisidir. Klasik mekaniğin temel özelliği belirleyici olmasıdır. Kuantum mekaniğinin ise belirsizlik ve ayrılık, özellikleridir (Dereli, 2009).

Kuantum Rastgele Sayı Üretimi

Rastgele sayılar, kriptografiden istatistiğe, örneklemeden nümerik analize kadar günümüzde birçok uygulamada kullanılmaktadır. Modern kriptografide de, kriptografik algoritma ve protokol parametrelerinin, şifreleme - şifre çözme anahtarlarının oluşturulmasında kullanılırlar.

Günümüzde rastgele sayıları üretmek için iki temel üreteç türü vardır: Gerçek rastgele sayı üreteci (GRSÜ) ve sözde rasgele sayı üreteci (SRSÜ). Bu üreteçler incelendiğinde her ikisi de rastgele gibi görünen bir bit dizisi üretmek için tamamen belirleyici olan klasik fiziği esas alır. Bu nedenle, aslında her iki üreteç de tam anlamıyla rastgele değildir.

Kuantum rastgele sayı üreteci (KRSÜ), rastgele sayılar üretmek için kuantum fiziğini kullanan bir üreteçtir. Klasik fiziğin aksine kuantum fiziği belirleyici değildir. Kuantum mekaniğine tam olarak rastgeledir diyebiliriz. Şekil 3'te rastgele bitlerin, fotonun gittiği yol boyunca belirlendiği basit bir KRSÜ görülmektedir.



Şekil 3 Kuantum Rastgele Sayı Üreteci

Bu KRSÜ'de ışıkla ilgili bir kuantum süreç kullanılır. Kuantum fiziğinde ışık, foton denilen parçacıklardan oluşur. Fotonlar belirli durumlarda rastgele davranış sergilerler. Mevcut KRSÜ'ler, bileşenlerinin şu an itibarıyla kusursuz çalışmamasından dolayı klasik ve kuantum kısımlardan oluşur:

-Kuantum Kısım: Rastgelelik için kuantum süreci içerir. Bileşenler henüz mükemmel olmadığından elde edilen 0,1 dizisi eşit olasılıklı değildir.

-Klasik Kısım: Eşit olasılıklı olmayan 0,1'lerin mümkün olduğu kadar eşit olasılıklı hâle getirilmesi için bazı işlemleri içerir.

Kuantum rastgele sayı üreteçleri tek gerçek rastgelelik üreteçlerdir. Klasik fiziğin aksine, kuantum fiziği tamamen rastgeledir (Bennet, Brassard, 1984; Dereli, 2009:54-57; Gedik, 2009; ; Gümüş, 2011; Kalem, 2013; Scarani, vd. 2009).

Kuantum Kriptografi

Kriptoloji bilimi, matematiğin alt dalı olup; matematiksel tekniklerden faydalanıp şifreleme sistemlerini kullanarak bilgiyi gizleme sanatı ve bilimi olarak bilinen kriptografi ve benzer matematiksel teknikleri, tasarımlardaki zayıflıkları kullanarak geliştirilmiş güvenlik sistemlerini alt etme olarak tanımlanan kriptanalizden oluşur.

Modern kripto sistemlerde en ciddi sorun anahtar dağıtım problemi olarak bilinen gizli anahtarın güvenliğidir. Bu tür problemlerin olmadığı bir kripto sistem gereklidir. Bu da teknolojik gelişmelerden etkilenmeyen ve uzun vadeli, kalıcı gizlilik sağlayan yeni bir alan olan kuantum kriptografidir.

Kuantum kriptografi, siber alandaki güvenliğin kuantum mekaniğinin belirsizlik yasası, foton polarizasyonu, dolaşıklık yasası ile garantilendiği kriptografi tekniğidir. Bu tekniğin en önemli yönü ispatı yapılmış kuantum mekaniği yasalarını kullanması, bunların klasik olarak eşdeğerinin bulunmaması ve güvenliğin ispatlanabilir olmasıdır.

Mevcut kuantum kriptografi şu an için, Kuantum Anahtar Dağıtımı ile bilinen kuantum kısım ve klasik yöntemlerle şifreleme olarak bilinen klasik kısımdan oluşmaktadır.

- Klasik Kısım: Geleneksel kriptografi ile şifreleme.

Günümüzde kuantum kriptografinin çalışma prensibi ise şu şekildedir:

- Anahtar, taraflar arasında kuantum anahtar dağıtımı ile dağıtılır, böylece anahtar dağıtım problemi de çözülmüş olur. Güvenliği kanıtlanmış, tamamen güvenli tek anahtar dağıtım yöntemi kuantum anahtar dağıtımıdır.
- Şifreleme, vernam şifresi ile yapılır. Vernam şifresi kırılmazlığı teorik olarak da ispatlanmış tek şifredir.

Klasik iletişimde benzeri olmayan şu özelliklerinden dolayı KAD protokolleri, aralarında mesafe olan kullanıcılar arasında rastgele, aynı ve güvenli bir gizli anahtar oluşturur. Kuantum mekaniğinin özelliğinden dolayı anahtar dağıtımı sırasında iletişime müdahale edilip edilmediği belirlenir.

KAD'ın çalışma ilkesi aşağıdaki gibidir;

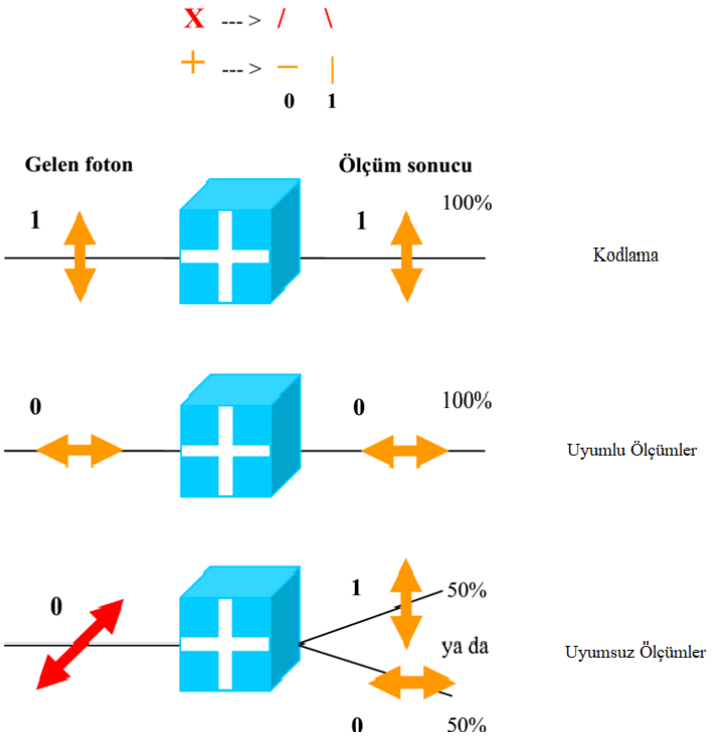
- Anahtar dağıtımında tam güvenlik garanti edilir,
- Aksi durumda, iletişim kesilir ve yeniden başlatılır.

Böylece güvenli bir şekilde anahtar dağıtımı yapılmış olur.

KAD, kuantum mekaniğinin en temel ilkelerinden olan Heisenberg belirsizlik ilkesini kullanarak iletişim güvenliğini garanti eder. Bu ilke ilk defa Alman fizikçi W. Heisenberg tarafından "birbirine bağlı iki büyüklükten birinin ölçülmesindeki duyarlılık arttıkça diğerinin ölçülmesindeki duyarlılık azalır. Öyle ki, ölçümler sonucu her iki büyüklüğe ait belirsizliğin çarpımı daima Planck sabitinden büyük veya en az ona eşittir" olarak tanımlanmıştır. Bu gerçek özetle: "Bilinmeyen bir kuantum sistemi ölçmek o sistemi değiştirecektir." der. Dolayısıyla bu şekilde temsil edilen kuantum bilgi de değişecektir. Aynı zamanda, bir kuantum sistemde belli özellikteki çiftlerin aynı anda asla tam olarak ölçülemeyecek demektir. Bu nedenle, belirsizlik ilkesi gereğince, kuantum bilgi üzerinde ölçüm yapmak hatta yalnızca gözlem yapmak bile bozulmalara sebep olacağından

bilgiyi elde etmek imkânsızdır. Bu da kuantum bilgi kopyalanamaz demektir. Yani iletişime saldıranın varlığı tespit edilebilir.

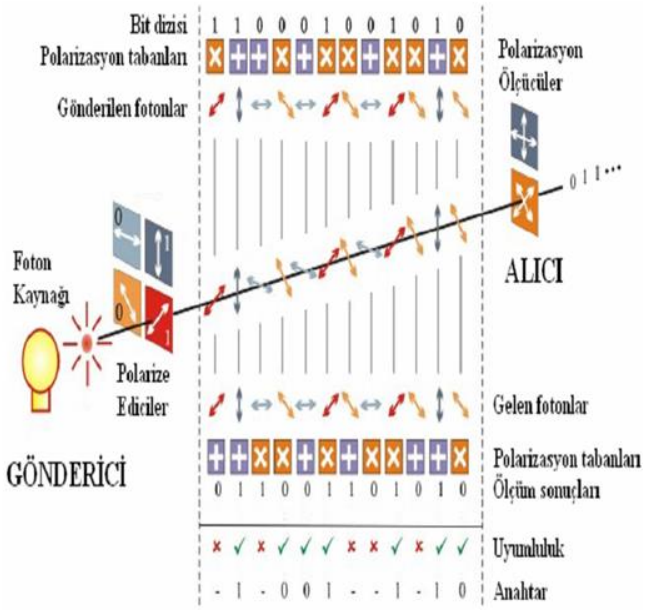
KAD, iletişim için temel kuantum parçacıklarından, fotonlardan, faydalanır ve fotonların polarizasyon özelliğinden yararlanarak anahtar bitlerini belirler. Yani anahtar taşıyıcısı olarak her bir anahtar biti için tek bir foton kullanılır. Şekil 4'te fotonlarda kuantum ölçümler görülmektedir.



Şekil 4 Fotonlarda Kuantum Ölçümler Ve Belirsizlik İlkesi

KAD Protokolleri

Yukarıda anlatılan ilkelere dayanan basit bir KAD protokolü Şekil 5'te görülmektedir.



Şekil 5 Basit Anlamda Bir KAD Protokolü

Bugüne kadar kuantum kriptografide kullanmak için birçok anahtar dağıtım protokolü açıklanmış olup bazıları aşağıda verilmiştir:

BB84 Protokolü

Bahsedilen bu ilkelere dayanan ve şu an kullanılan, Charles Bennelt ve Gilles Brassard tarafından önerilen, BB84 protokolü hem kuantum hem de klasik kısımdan oluşmaktadır. Şekil 6'da bu görülmektedir.

Şekil 6 BB84 Protokolü

-Kuantum Kısım: Aday anahtar bitleri foton tanecikleriyle birer birer taşınarak oluşturulur.

1. Adım;

Gönderici, ham anahtar bitlerini KRSÜ kullanarak rastgele oluşturur. Her bir bit fotonun polarizasyon durumu ile ifade edilerek fotonlar, iletişimin tek yönlü olduğu, dış ortam ile etkileşimden yeterince izole edilmiş olan kuantum kanal üzerinden rastgele tabanda teker teker alıcıya gönderilir.

2. Adım:

Alıcı, gelen her bir fotonu rastgele seçtiği bir tabanda ölçer. Seçilen taban gönderici ile aynı ise, ölçüm sonucu da göndericinin biti ile aynı olacaktır. Farklı bir taban seçilmişse, ölçüm sonucu %50 ihtimalle doğru olacaktır. Ancak bu bilinmemektedir. Aynı durumlar istenmeyen kişi için de oluşur.

-Klasik Kısım: Alıcının ölçüm sonuçlarının değerlendirilmesinden oluşur.

3. Adım:

Tüm iletim ve ölçümler tamamlandıktan sonra alıcı, sadece gelen fotonları hangi tabanlarda ölçtüğünü, iletişimin iki yönlü olduğu, kimlik doğrulamalı ve iletişimin pasif olarak dinlenebildiği bir korumasız iletişim kanalıyla açıklar. Gönderici, alıcıya kullandıkları aynı tabanları açıklar. İdealde bu indekslerdeki bitler de aynı olmalıdır.

4. Adım:

Aradaki istenmeyen kişinin varlığı, bitlerin bit alt kümesi açıklanarak tespit edilebilir. Aynı indekslerin kullanıldığı bitler de mutlaka aynı olmalıdır. Aynı değilse, ilgili fotonlara müdahale edildi demektir. O hâlde protokol iptal edilmelidir. Dış etkenlerden dolayı %15'lik bir hataya kadar protokol devam ettirilebilir.

5. Adım:

Güvenliğin sağlandığından emin olunmuş ise kalan ortak bitler gizli anahtar olarak kabul edilir.

B92 Protokolü

Charles Bennett tarafından öne sürülen bu protokolde her kubit 0º veya 45º polarizasyonla temsil edilir. Bu protokolde kubit değeri eşleşmesi 0º polarizasyona sahip fotonlar 0 kubit, 45º polarizasyona sahip fotonlar ise 1 kubit olarak iade edilir. Gelen fotonların okunmasında BB84 protokolünde olduğu gibi düz ve köşegen filtreler kullanır. Fakat 0º veya 45º olarak okunan fotonlar elenerek anahtara dâhil edilmez. 90º ve 135º okumalar geçerli kabul edilir.

E91 Protokolü

1. Adım:

Gönderici tarafından aşağıda belirtilen durumda N spin çifti hazırlanır;

$$\left|\psi >= \frac{1}{\sqrt{2}}(|\uparrow\downarrow> - |\downarrow\uparrow>) = \frac{1}{\sqrt{2}}(|01> - |10>)\right.$$

2. Adım:

Her bir çiftin 2. spini açık bir kuantum kanaldan gönderilir.

3. Adım:

Açık bir kanalda, yapılan ölçüm yönleri açıklanır.

Tablo 1 Ölçüm yönleri

	1. Çift	2. Çift	3. Çift	4. Çift	5. Çift	...
A	σ_x	σ_x	σ_z	σ_z	σ_x	…
B	σ_x	σ_z	σ_x	σ_z	σ_x	…

4. Adım:

Spinin aynı yöndeki bileşeni ölçülmüşse göndericinin sonucu, alıcının sonucunun eksi işaretlisi olmalıdır.

Tablo 2 Ölçüm sonuçları

	1. Çift	2. Çift	3. Çift	4. Çift	5. Çift	...
A	σ_x	σ_x	σ_z	σ_z	σ_x	…
B	σ_x	σ_z	σ_x	σ_z	σ_x	…
GÖN. SON.	+	+	-	+	-	…
ALI. SON.	-	+	-	-	+	…
ANAHTAR	0			0	1	…

Farklı yönlerde ölçümler alınmış ise bunlar anahtarda kullanılmazlar.

SARG04 Protokolü

2004 yılında öne sürülmüş, kuantum kriptografinin ticari uygulamalarında kullanılan bir protokoldür. Metot, henüz icat edilmemiş ama gelecekte kullanılacağı öngörülen teknolojilerin, BB84 tipi protokoller için oldukça büyük bir risk oluşturduğunu göstermektedir.

EPR- EKERT Protokolü

Bu protokolde BB84'te kullanılan Heisenberg belirsizlik yasası kullanılmaz. Burada kuantum hâlleri birbirine bağlaşık olan, alıcı ve vericiye birer tane olmak üzere, iki foton kullanılır. Bu fotonların kuantum hâlleri birbirine zıt olduğu için taraflar birbirlerinin kuantum hâlini tahmin edebilirler, bu şekilde ortak bir anahtar elde edilebilir (Elliot, 2004; Gisin, Ribordy, Tittel, Zbinden, 2002; Nielsen, Chuang, 2000; Mullins, 2002; Toyran, 2006; Trappe, Washington, 2002; Williams, Clearwater, 1998).

Kuantum Kriptoanaliz

Kriptoanaliz

Kriptografinin tersine, şifre çözme ve şifreli mesajı okuma sanatı ve bilimidir. Gizli anahtarı bir şekilde ele geçirerek ya da geçirmeden şifreli bilgiyi çözme işlemlerini kapsar. Kriptanaliz, gizli anahtarı elde etmenin en zor yoludur. Çünkü aynı işi sistemdeki zayıflıklara odaklanarak daha kolay yapabiliriz.

Kuantum Kriptoanaliz

Bazı kuantum mekaniksel sistemlerden, bir takım kuantum mekaniksel etkilerden yararlanarak yani kısacası kuantum bilgisayarlar kullanarak şifre kırmayla ilgilenen kriptografik bir uygulama alanıdır.

Kuantum kriptoanalize en meşhur örnek bir matematikçi olan Peter Shor tarafından 1994 yılında önerilen, çarpanlara ayırma problemini çözmenin verimli bir yolunu ortaya koyan, shor algoritmasıdır. Bu algoritma bir kuantum bilgisayar kullanılarak çok büyük tam sayıları rahatlıkla çarpanlarına ayırabilecektir. Böylece bazı simetrik şifreleme algoritmalarının güvenirliliği ortadan kalkacaktır.

Bir başka örnek ise, bir bilgisayar bilimcisi Lov Grover tarafından önerilen, kuantum bilgisayar yardımıyla, kaba kuvvet saldırısı marifetiyle anahtar aramalarının karesel olarak daha hızlı yapılabileceğini belirten Grover algoritmasıdır.

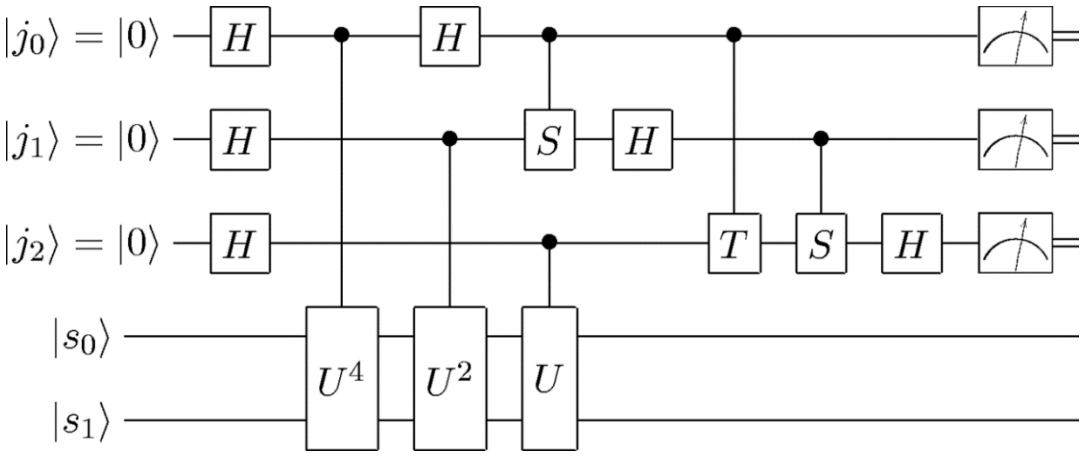
Kuantum özel kanallar, kuantum simetrik şifreleme, kuantum hesaplama gibi kuantum kriptoanalizde kapsamlı bir kuantum bilgisayarın yapılmasını beklemektedir.

Kuantum Bilgisayar

Veri işleme teorisine farklı bir yaklaşım getiren oldukça güçlü makinelerdir. Bilgi üzerinde bir takım işlemleri gerçekleştirmek için süperpozisyon ve dolaşıklık gibi kuantum fiziğinin prensiplerini kullanan paralel bir hesaplama makinesidir. Kuantum bilgisayarlarda kuantum bilginin birimi olarak kubit kullanılır. Bir kuantum sistem klasik bitleri kuantum bitler ile değiştirir. Klasik bitler 0 ve 1 değerini alırken kubitler aynı anda hem 0 hem de 1 değerini alabilen yani aynı anda tüm olasılıklara

sahip olan süperpozisyon ve iki kubitin birbiriyle ilişkili olması nedeniyle birindeki bir değişikliğin diğerini de etkilediği dolaşıklık olaylarını kullanır. Bu ise kuantum hesaplamanın gücünün temel unsurudur ki; kubitleri kullanan bilgisayarların daha az enerji kullanarak daha fazla bilgi depolayabileceği demektir. Kubitler bu şekilde elektron spinine veri kaydedebildiklerinden kuantum bilgisayarların temel veri birimi bit değil kubit ile ifade edilmiştir.

Bir kuantum bilgisayar hem giriş hem de çıkış kubitlerinin doğrusal kombinasyonundaki tüm temel durumları üzerinde aynı anda çalışabilir. Yani problemlere aynı anda odaklanır, tüm muhtemel çözümleri bir kerede ele alır ve çalışmayanları atar. Aslında, kuantum bilgisayar bir paralel makinedir. Şöyle ki n kubitlik bir kuantum bilgisayarda işlem gücü n bitlik 2^n tane klasik bilgisayarınkine eşittir diyebiliriz. Bu durumda kuantum bilgisayar dendiğinde kuramsal alandaki bir insan olarak ilk aklıma gelen şey kuantum devreleridir. Çünkü kuantum bilgi sayımının klasikten farkı kullanılan devre modelidir ve esas olan devredir. Zira bu teknoloji harikası ve milyon dolar maliyetli ürünler kuantum devre şemasının fiziksel olarak gerçekleştirilmesidir. Şekil 7'de bir kuantum devre modeli görülmektedir.



Şekil 7 Kuantum Devre Modeli

Bir klasik bilgisayar x girişi için f(x) çıkışını verir. Ancak kuantum bilgisayar, giriş olarak mümkün ve muhtemel bütün x durumlarının toplamını alabilir;

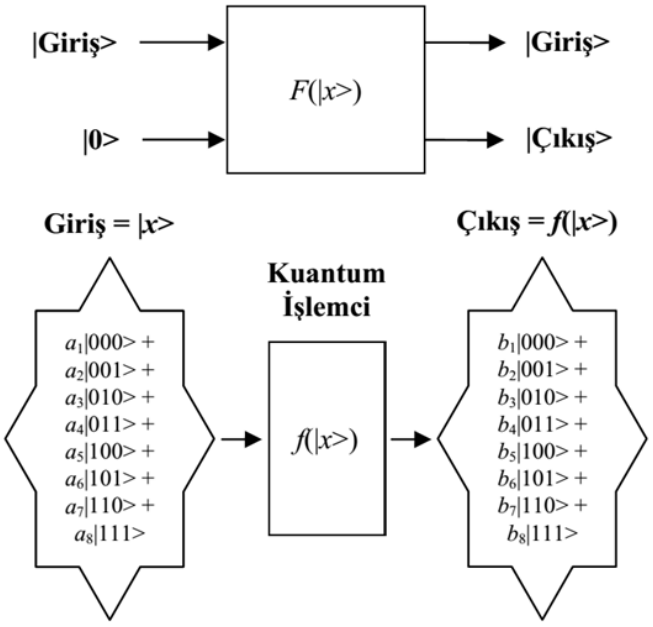
$$\frac{1}{c}\sum_{k=0}^{n}|x_k> = \frac{1}{c}\,(|x_0> + |x_1> + |x_2> + \cdots + |x_n>) \qquad (1)$$

Burada c sabiti normalleştirme için kullanılır. Ürettiği çıkış ise;

$$\frac{1}{c}\sum_{k=0}^{n}|x_k, f(x_k)> = \frac{1}{c}\ (|x_0, f(x_0)> + |x_1, f(x_1)> \ + |x_2, f(x_2)> + \cdots + |x_n, f(x_n)>) \quad (2)$$

olabilir.

Burada eğer bir ölçüm yapacak olursak yani rastgele seçeceğimiz bir x_0 değeri için $|x_0, f(x_0)>$ sonucunu elde edeceğimizden dolayı çıkıştaki tüm diğer durumlar yok edilecektir. Buda f(x) değerlerine bakmak için tek bir şansımızın olduğu anlamına gelir. Bu nedenle bir kuantum bilgisayarı programlarken temel hedef hesaplamayı tasarlama olacaktır. Şekil 8'de bir kuantum bilgisayarın çalışma prensibi görülmektedir.



Şekil 8 Bir Kuantum Bilgisayarın Çalışma Prensibi

Kuantum Algoritmaları

Donanımcılar kullanılabilir bir kuantum bilgisayarı yapmaya uğraşırken, bilgisayar bilimciler ve matematikçiler de kuantum bilgisayarlarda uygulanabilecek algoritmaları geliştirmek için uğraşıyorlar. Verileri saklamak için bitler yerine kubitlerin kullanıldığı, kuantum mekaniğinin geçerli olduğu durumda kuantum bitlerinin süperpozisyon özelliğini kullanıp işlem yapan algoritmalar kuantum algoritmalarıdır. Bugüne kadar geliştirilmiş ve en çok bilinen kuantum algoritmaları Deutsch, Shor ve Grover algoritmalarıdır.

Deutsh Algoritması

Tarihte ilk kuantum algoritması olarak bilinen ve David Deutsch tarafından geliştirilen algoritmadır. Yalnızca tek bir kubit üzerinde işlem yapabilen bu algoritma, klasik algoritmaların yetersiz kaldığı yerde kuantum algoritmalarının olağanüstü bir işlem hızıyla sonuca gidebildiğini ispatlaması yönüyle oldukça önemlidir. David Deutsch ve Richard Josza tarafından sınırsız sayıda kubitle işlem yapabilecek şekilde yeniden formüle edilip genelleştirilerek, Deutsch-Jozsa algoritması adını alan Deutsch algoritması, daha sonraki yıllarda geliştirilecek olan Shor ve Grover algoritmaları için alt yapı oluşturmuştur.

Shor Algoritması

Amerikalı matematikçi Peter W. Shor tarafından geliştirilen bu algoritma kuantum bilgisayarlarda çok büyük sayıları kolaylıkla çarpanlarına ayırabilme özelliğine sahiptir. Belirli bir olasılık dâhilinde periyodu bulur. Shor algoritmasının bu özelliği kriptoloji açısından oldukça önemlidir. Bugün kullanılan şifreleme sistemleri çok büyük sayıların klasik bilgisayarlar tarafından kabul edilir bir zaman dilimi içerisinde çarpanlara ayrılmasının mümkün olmadığı varsayımına dayanarak çalışmaktadır. Laboratuvar ortamları için geliştirilen, az sayıda kubite sahip olan kuantum bilgisayarların çok büyük sayıları, çok daha kısa zamanda çarpanlarına ayırabilmesi klasik kriptolojinin temellerini sallayarak kuantum kriptoloji adıyla yeni bir bilim dalının yolunu açmaktadır.

-Klasik Kısım

Çarpanlara ayırma problemi bir periyot bulma problemine indirgenir. N'nin asal çarpanları

1. Rastgele bir $\propto < N$ sayısı üretir.

2. $OBEB(\propto, N)'i$ hesaplar. Eğer $OBEB(\propto, N) \neq 1$ ise $\propto, N$'nin bir asal çarpanıdır, işlem tamam.

3. $N^2 \leq Q = 2^m \leq 2N^2$ olan bir Q belirler ve $f(x) = \propto^x \ mod\ N$ fonksiyonunun r periyodunun bulunması için kuantum kısma geçer.

4. Eğer r tek ise 1. adıma döner.

5. Eğer $\propto^{\frac{r}{2}} \equiv -1\ (mod\ N)$ ise 1. adıma döner.

6. $OBEB\left(\propto^{\frac{r}{2}} \pm 1, N\right) = N$ 'nin asal çarpanı ise işlem tamam.

-Kuantum Kısım

İçerdiği kuantum algoritma sayesinde periyot bulma problemi çözülür. Başka bir ifadeyle; periyot bulma kuantum mekaniği sayesinde gerçekleştirilir.

1. Saklayıcılar ilklendirilir;

$Q^{-\frac{1}{2}} \sum_{x=0}^{Q-1} |x, 0>$, m qubitlik giriş, $\frac{m}{2}$ kubitlik çıkış.

2. f(x), kuantum bir fonksiyon olarak gerçeklenip yukarıdaki kuantum duruma uygulanır.

$Q^{-\frac{1}{2}} \sum_x |x, f(x)>$. Tüm olası $Q = 2^m$ durumun bir süperpozisyonudur. Dolayısıyla tüm olası girişler ve çıkışlar saklayıcılardadır.

3. İkinci yarıda ölçüm yapılır;

$\frac{1}{c} \sum_{0 \le x \le 2^m} |x, u>$. Burada c, toplamdaki terimlerin sayısının karekköküdür. Yani vektör uzunluğunu 1 yapmak için gereken faktördür.

Bu ölçüm, mod N'de bir u sayısı verir ve tüm sistemi $|x, u>$ formundaki durumların bir doğrusal kombinasyonuna zorlar ki;

tüm $a^x \equiv u\ (mod\ N)$ elde edilir.

4. Giriş saklayıcısına kuantum fourier dönüşümü uygulanır;

$U_{QFT} \left|x>= Q^{-\frac{1}{2}} \sum_y W^{xy} |y\ >\right.$, burada $W = e^{\frac{2\pi}{Q}}, 0 \le y < Q$.

Periyodun bulunması için gereken frekansların ölçümü kuantum fourier dönüşümü ile yapılır. Eğer r 2^m'nin bir böleni ise elde edilen frekanslar f_0 temel frekansının katlarıdır ve $rf_0 = 2^m$ olur. Ancak genelde r, 2^m'nin böleni değildir. Bu durumda bazı baskın frekanslar olacaktır ve bunlar bir f_0 temel frekansının yaklaşık katları olur. Yani $rf_0 \approx 2^m$'dir. Kuantum fourier dönüşümü sonucunda oluşan kuantum durum üzerinde ölçüm yapılır ve bir $f = j.f_0$ frekansı belirlenir.

5. r'yi elde etmek için $frekans = \frac{Uzunluk}{Periyot}$ tanımı kullanılarak dizinin kaç defa tekrar ettiğini hesaplayan $\frac{j.f_0}{r.f_0} \approx \frac{f}{2^m} \Rightarrow \frac{j}{r} \approx \frac{f}{2^m}$ ilişkisi üzerinde sürekli bölme açılımı uygulanır. Çünkü uzunluğu belli olan bir dizinin frekansı bulunursa periyodu da bulunur.

Euler'in Ø fonksiyonu, p, q asal ve N=p.q olmak üzere;

Ø(N) =(p-1)(q-1) alınarak r ≤ Ø(N)< N eşitsizliğinden r periyodu bulunur. Genel olarak, yukarıdaki bölme açılımından N'den küçük en son payda aranılan r periyodudur.

6. $a^r \equiv 1 \pmod N$ ise işlem tamamlanır.

7. $a^r \not\equiv 1 \pmod N$ ise 1. adıma geri dönülür.

Bu algoritmanın kuantum kısmı için her bir N ve a'ya bağlı olan özel olarak kuantum devreler tasarlanır. Yöntem bazen düzgün çalışmayabilir, o zaman algoritma baştan tasarlanır ve çalıştırılır.

Grover Algoritması

Hint asıllı Amerikalı bilgisayar bilimci Lov Grover tarafından geliştirilen bu algoritma, çok büyük veri kümelerinde aranan bilginin, araştırmanın detaylı bir şekilde formülasyonuna gerek kalmadan ama hızlıca bulunmasına imkân sağlar. Grover algoritması diğer kuantum algoritmalarının çoğu gibi ihtimal teorisine dayalı olduğundan doğru cevabı bulabilmesi için veriler üzerinde genellikle yalnızca bir defa değil, birçok kez çalıştırılması gerekir. Bu şekilde aynı verileri birçok defa işleyen algoritma, nihayetinde doğru olma olasılığı en yüksek cevabı bulur.

1. İlklendirme: Walsh-Hadamard dönüşümü uygulanarak aşağıdaki süperpozisyon elde edilir;

$$\left|\delta > = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x > . \right. \quad (3)$$

2. Yenileme: Aşağıdaki tüm işlemler M defa tekrar edilir;

a) Mevcut süperpozisyondaki her bir $|x >$ durumu için F(x) =1 ise faz π radyanlık döndürülür, aksi takdirde sistem değişmemiştir durdurulur.

b) Walsh-Hadamard dönüşümü ve Faz rotasyon matrisinden oluşan

$$D_{ij} = \begin{cases} \frac{2}{N}, & i \neq j \\ -1 + \frac{2}{N}, & i = j \end{cases} \quad (4)$$

difüzyon dönüşümü uygulanır.

3. Ölçüm: Ortaya çıkan süperpozisyon ölçülür ve genliklerin belirlediği olasılıklara göre bir durum elde edilir (Bonnetain, Plasencia, 2018; Beth, Mueller, Steinwandt, 2004; Ege, 2012; Yamaura, Ishizuka, 2000).

SONUÇ

Kriptograflarla kriptanalistler arasında yıllardır süregelen mücadele yeni yüzyılda kuantum alanında da devam edecektir. Zira gizli anahtar üretiminde kullanılan KRSÜ ve kuantum kriptografi şimdilik anahtar dağıtımı için kullanılmaktadır. Hatta ticari ürünlerde piyasaya sürülmüştür. Günümüzde kuantum teknolojiyle güvenli olarak mesaj 150 km'den daha fazla mesafelere gönderilmesi başarılmış durumdadır. Bununla beraber IBM piyasaya sürülebilir 50-qubit kuantum bilgisayarı, ABD'den bir ekip 51-qubitlik kuantum simülatörü ve Google yalnızca araştırma amaçlı 2000-qubitlik bilgisayarı ilan ettiler bile. Ayrıca Madrid Teknik üniversitesi araştırmacıları faktörizasyon problemi dediğimiz çarpanlarına ayırma problemi için faktörizasyonda kullanılan aritmetiği taklit eden bir kuantum simülatörü teorik olarak kurguladılar (Bonnetain, Plasencia, 2018; Beth, Mueller, Steinwandt, 2004; Ege, 2012; Rosales, 2016; Rosales, 2018; Yamaura, Ishizuka, 2000).

Büyük ihtimalle bu işlemci gücüne sahip programlar ve hatta yapay zekâ programları da yapılmıştır. Bu durum kuantum kriptanalizin önemini bir kez daha ortaya koymuştur. Tüm bu gelişmeler açıkça ortaya koymuştur ki; temel bilimlerde ve matematikte kim öndeyse gelecek onundur.

Günümüzde millî güvenliğimiz açısından en önemli hususların başında millî bilgi güvenliği gelmektedir. Bu nedenle millî güvenliğimizin en önemli güvencesi de dışa bağımlılıktan kurtulmaktır. Yaşanan bilimsel ve teknolojik gelişmelerden geri kalmamak için acilen KRSÜ, kuantum kriptografi, kuantum kriptoanaliz, kuantum bilgisayar, kuantum haberleşme gibi teknolojiler üzerinde yoğunlaşıp çalışmalara başlamalı ve bu alanda millî kuantum teknolojileri seferberliği başlatılmalıdır.

KAYNAKÇA

Kitaplar

Dereli, T. Verçin, A. (2009). *Kuantum mekaniği temel kavramlar ve uygulamaları.* Anakara: Tüba Yayınları.

Nielsen, M. A. Chuang, I. L. (2000). Q*uantum computation and quantum ınformation.* London: Cambridge University Press.

Trappe, W. Washington, L. C. (2002). *Introduction to cryptography with coding theory*. Toronto: Prentice-Hall, Inc.

Williams, C. P. Clearwater, S. H. (1998). *Explorations in quantum computing*. Springer-Verlag NewYork: TELOS.

Makaleler

Bennet, C. H. Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing, *Proc. Int'l Conf. Computers, Systems & Signal Processing*, CS Press, 175–179.

Beth, T. Mueller-Quade, J., Steinwandt, R. (2004). Cryptanalysis of a practical quantum key distribution with polarization-entangled photons. *Quantum Physics*, 12, 3865-387.

Boyacı, U. K. (2013). Günümüzde kriptoloji. *UEKAE Dergisi*, 1, 32-41.

Dereli, T. (2009).İletişimde mutlak güvenlik için kuantum kriptografi, *Bilim Teknik*, Temmuz(500), 54-57.

Ege, B. (2012). Kuantum mekaniğinden kuantum bilgisayarlarına. *Bilim Teknik*, Ekim(539), 12-15.

Elliott, C. (2004). Quantum cryptography. *Security & Privacy Magazine*, IEEE, 2(4), 57–61.

Gedik, Z. (2009). Kuantum bilgisayarları, *Bilim Teknik*, Temmuz(500), 58-59.

Kalem, Ş. (2013). Kuantum bilgi güvenliğine doğru, *UEKAE Dergisi*, 1, 42-47.

Gisin, N. Ribordy, G. Tittel, W. Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, 1-57.

Mullins, J. (2002). Making unbreakable code, *Spectrum*. IEEE, 39(5), 40–45.

Rosales, J. Martin, V. (2016). Quantum simulation of the factorization problem. *Phys. Rev. Lett*. 117, 200502.

Rosales, J. Martin, V. (2018). Quantum simulation of the integer factorization problem: Bell states in a penning trap. *Phys. Rev. Lett*. A 97, 032325.

Scarani, V. Bechmann-Pasquinucci, H. Cerf, N. J., Dusek, M., Lutkenhaus, N., Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 1301-1351.

Yamamura, A. Ishizuka, H. (2000). Quantum cryptanalysis of block ciphers. *Research Institute for Mathematical Sciences*, Kyoto University, 1166, 235-243.

Kongre bildirileri

Bonnetain, X. Plasencia, M. (2018). H*idden shift quantum cryptanalysis and implications*. 24th International Conference on the Theory and Application of Cryptology and Information Security, December 2–6, Australia, 560-592.

Gümüş, E. (2011). *Kuantum kriptografi ve anahtar aağıtım protokolleri*. Akademik Bilişim Konferansı, 2-4 Şubat, Malatya, 547-552.

Toyran, M. (2006). *EEB Mühendisliklerinde kuantum hesaplama eğitimi*. 3. EEB Mühendislikleri Eğitimi Sempozyumu, 16-18 Kasım, İatanbul, 31-35.

Toyran, M. (2011). *Bilgi güvenliğinde kuantum teknikler*. IV.Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, 25-26 Kasım, Ankara, 98-107.

EXTENDED SUMMARY

The Role of Quantum Cryptanalysis in Cyber Defense

Introduction

Cryptography; It deals with encryption and decryption to ensure the security of information. For this reason, information security in cyber world is mostly provided by using modern cryptographic methods. The main services provided by modern cryptography for information security are confidentiality, integrity, authentication and denial. It may be necessary to make use of one, several or all of these as needed. In the cyber world, the security of communication is possible by changing the content of the message, eliminating threats such as identity imitation and denial; and today the main tool used for this purpose is cryptography.

In the next part of the study; modern cryptography in chapter III and basic information about quantum mechanics in chapter II will be given. Then quantum random number generation in chapter IV, quantum cryptography in chapter V and quantum cryptanalysis issues in chapter VI and results will be discussed in chapter VII.

Privacy service of cryptography: It ensures that information is never understood by anyone other than the actual recipient. For this purpose, information encryption is the main method used. Nowadays, two types of encryption systems, called symmetric and asymmetric encryption systems, are used. In symmetric systems, both the sender and the receiver use the same secret key for encryption and decryption. These systems are quite fast and are more preferred in encryption. Algorithms such as Vernam, DES, AES, IDEA, RC4 are the most commonly used encryption algorithms.

In asymmetric systems, two different keys, called public key and secret key, are used. The public key is used for encryption, and this key is obvious. Decryption uses a secret key and no one should know it except the owner. Only the owner of the public and private key pair can decode the information encrypted with the public key. Because asymmetric systems are slow, they are mostly used to encrypt short-length messages, such as electronic signatures, secret key distribution and random number generation. RSA, Diffie-Helman, El Gamal, DSS are the most commonly used asymmetric encryption algorithms. In modern cryptography, algorithms are not secret, they are open to all, in fact, the secret key is hidden.

Quantum Mechanics

Quantum mechanics is the basis of the laws of physics which allow the definition of atoms and sub-atomic particles called microscopic systems such as nuclei, electron, photon, and mathematically expressing the behavior of matter and its interaction with energy at the level of atoms and atomic particles. Quantum mechanics is the new theory of nature or movement that explains the behavior of microscopic systems such as atoms, electrons, and photons. The most important feature of classical mechanics is that it is deterministic. In contrast, the two most important features of quantum mechanics are uncertainty and separation.

Quantum Random Number Generation

Random numbers are used in many applications from cryptography to statistics, sampling, numerical analysis and games of chance. In modern cryptography, they also play a central role in the creation of cryptographic algorithms and protocol parameters, encryption and decryption of keys.

Nowadays, there are two basic types of generators for generating random numbers: the actual random number generator and the pseudo random number generator. When these generators are examined, they are based on classical physics, both of which are completely deterministic to produce a seemingly random sequence of bits. Therefore, in fact, there cannot be complete randomness for both types of generators.

Quantum Cryptography

The most serious problem in modern cryptosystems is the security of the secret key known as the key distribution problem. Therefore, there is a need for a cryptosystem that does not have key distribution problems and risks. This is called quantum cryptography, a new field that is not affected by technological advances and provides long-term, lasting privacy.

Quantum cryptography is a cryptography technique in which security in cyberspace is guaranteed by laws such as uncertainty of quantum mechanics, photon polarization and entanglement. Its main advantage is that it is based on proven universal laws of quantum mechanics, that they are not classically equivalent and that security can be proved.

The current quantum cryptography currently consists of classical and quantum parts;

- Quantum Part: Quantum Key Distribution
- Classic Part: Encryption with traditional cryptography.

Nowadays, the working principle of quantum cryptography is as follows:

- The key is distributed between the parties by quantum key distribution, thus solving the key distribution problem. The proven, fully secure single key distribution method is the quantum key distribution.
- Encryption is done with Vernam. Vernam is the only password that has proven theoretically unbreakable.

Quantum Cryptanalysis

It is a cryptographic field of application that deals with the decryption of keys by using some quantum mechanical systems and quantum mechanical effects, briefly, using quantum computers.

The most famous example of quantum cryptanalysis is the Shor algorithm, proposed by a mathematician Peter Shor in 1994, which provides an efficient way of solving the factorization problem. This algorithm can easily factorize large integers with a quantum computer. Thus, some symmetric encryption algorithms will be broken.

Another example is the Grover algorithm, proposed by a computer scientist Lov Grover, that with the help of a quantum computer, key searches can be made faster by means of brute-force attacks.

Quantum special channels, quantum symmetric encryption, quantum computation, such as quantum cryptanalysis, expect a comprehensive quantum computer to be built.

Quantum Computer

They are incredibly powerful machines that bring a new approach to data processing knowledge. A parallel computing machine that uses the principles of quantum physics such as superposition and entanglement performs a number of operations on information. In quantum computers, qubit is used as the unit of quantum information. A quantum system replaces classic bits with quantum bits. The classical bits take the value 0 and 1, while the qubit uses superposition, which can take both 0 and 1 at the same time, that is, all possibilities at the same time, and entanglement events in which one change affects the other because the two-qubit are related. This is the basic element of the power of quantum computation. This means that computers using qubit can store more information using less energy. Since Qubits can record data to electron spin in this way, the basic data unit of quantum computers is expressed as qubit, not bit.

A quantum computer can simultaneously work on all the basic states of a linear combination of both input and output qubits. So, it focuses on the problems at the same time, handles all possible solutions at once and discards those which do not work. In fact, the quantum computer is a parallel machine so we can say that the computing power of an n-qubit-quantum computer is equal to n-bit 2^n conventional computers.

Quantum Algorithms

While hardware experts are trying to create the first available quantum computer, computer scientists and mathematicians naturally are not indifferent to this resarch and have been trying to develop the first algorithms that can be applied to quantum computers since the early 1990s. In this environment where information is stored in cubits instead of bits and quantum mechanics is valid, quantum algorithms process using superposition of quantum bits. There are only a handful of quantum algorithms developed from the mid-1980s to the present. The best known ones are the Deutsch, Shor and Grover algorithms.

Conclusion

The years of struggle between cryptographers and cryptanalysts will continue in the quantum field in the new century because quantum random number generator and quantum cryptography used in secret key generation are currently used for key distribution. This has once again demonstrated the importance of quantum cryptanalysis. All these developments made it clear that whoever is ahead in basic sciences and mathematics, the future is hers.

Today, national information security is one of the most important issues for our national security. Therefore, the most important assurance of our national security is to get rid of dependence on foreign countries. In order not to fall behind the scientific and technological developments, quantum random number generator, quantum cryptography, quantum cryptanalysis, quantum computer, and quantum communication technology studies should be started and national quantum technology mobilization studies should be put in action.