Bilgi Güvenliğinde Kuantum Teknikler

Mustafa Toyran[1] Thomas B. Pedersen[2] A. S. Atilla Hasekioğlu[3]
M. Ali Can[4] Savaş Berber[5]

[1-4]UEKAE, BİLGEM, TÜBİTAK, Gebze, Kocaeli
[5]Fizik Bölümü, GYTE, Çayırova, Kocaeli

[1]e-posta: mustafa.toyran@uekae.tubitak.gov.tr [2]e-posta: pedersen@uekae.tubitak.gov.tr
[3]e-posta: atilla@uekae.tubitak.gov.tr [4]e-posta: can@uekae.tubitak.gov.tr
[5]e-posta: savasberber@gyte.edu.tr

Özetçe

Bu bildiride Kuantum Mekaniği'nin günümüz Bilgi Güvenliği Sistemleri'ne etkisi incelenmeye çalışılacaktır. Bilgi güvenliği, Kriptografi biliminin sahasına giren bir konudur. Modern kriptografide güvenliğin bağlı olduğu başlıca parametre "gizli anahtar"dır. Gizli anahtar, rasgele seçilen, yeterince uzun, sadece bilgi alış-verişi yapanlarca bilinmesi gereken bir bit dizisidir. Gizli anahtar ile ilgili en önemli konular üretimi, dağıtımı ve yönetimidir. Diğer taraftan, modern Kriptanaliz eldeki bütün imkanları kullanarak gizli anahtarı ele geçirmeye çalışır. Modern kriptanaliz, modern kriptografide de olduğu gibi, daha çok Matematik'e ve Klasik Fizik'e dayanmaktadır. En son gelişmelere göre kuantum mekaniği de, özellikle bilgi güvenliğini de ilgilendiren bu konularda, bizlere daha önce bir benzeri görülmemiş birçok olumlu-olumsuz uygulamalara olanak sağlamaktadır.

1. Giriş

Bilgi güvenliği, bilginin ***iletim***i ve ***saklanma***sı esnasında güvenliğinin sağlanmasıdır[1]. İnsanlar çok eski zamanlardan beri [1] daima ***gizli bilgi***lerini ***meraklı***lardan gizleme ihtiyacı duymuştur[2]. Bunu yapmak için kullandıkları temel *araç* ya onları hiç kimsenin bulamayacağı bir yerlere *saklamak* ya da ele geçse dahi gerçek alıcısı dışındaki herkesin ondan birşey anlayamayacağı şekilde *anlamsız hale getirmek* olmuştur.

Bilgiyi hiçbir işleme tabi tutmadan olduğu gibi saklamaya dayalı çözümler ***steganografi*** (*steganography*, aslen Yunanca olan *steganos*: *saklı* ve *gráphein*: *yazı yazma* sözcüklerinin yan yana gelmesinden oluşmaktadır [2]) adlı bilim dalının konusudur. Örneğin, İkinci Dünya Savaşı sırasında kullanılan *mikronokta* yöntemi bir steganografi tekniğidir. Bu teknikte gönderici taraf göndermek istediği mesajın önce resmini çeker, sonra bu resmi bir nokta boyutuna kadar küçültür ve bu noktayı sahte bir mesajın, örneğin en son cümlesinin, sonuna yerleştirirmiş. Alıcı tarafta ise bu nokta bulunup tekrar büyütülerek gerçek mesaj okunurmuş. Steganografide bilgi olduğu gibi saklandığından ve bulunduğunda da kolayca okunabildiğinden güvensiz olabilmektedir. Mesajı *görünmez mürekkeple yazma*, mesajı *yazıp sonra onu yutma*, *vücudun görünmeyen kısımlarına yazma*, *ses/görüntü/video* ya da *başka bir mesaj içine saklama*, vb. yöntemler de çeşitli steganografi teknikleridir. Anlaşılacağı üzere tüm bu yöntemlerde mesajın anlamı üzerinde bir değişiklik olmamakta, mesaj olduğu gibi saklanmaya çalışılmaktadır. Steganografinin kriptografiye başlıca üstünlüğü daha az dikkat çekmesi olarak söylenebilir. Ayrıca, kriptografi kullanımına yasal olarak izin verilmeyen kimi yerlerde steganografi kullanımı daha avantajlı veya tek yol da olabilir. Ancak, kullanımı daha ***risk***li bir yöntemdir.

Bilginin birtakım *yerine koyma* (*substitution*)[3], *yer değiştirme* (*transposition*)[4] ya da *matematiksel* (*asal sayılar*, *eliptik eğriler*, *sonlu cisimler*, *modüler aritmetik*, *çarpma*, *üs alma* gibi) işlemler ile görünümünün değiştirilip anlamsız hale getirildiği geriye dönüşümlü yöntemler ise ***kriptografi*** (*cryptography*, aslen Yunanca olan *kryptós*: *gizli* ve *gráphein*: *yazı yazma* sözcüklerinin yan yana gelmesinden oluşmaktadır [3]) biliminin konusudur. Bu bilim, bilgi güvenliğini sağlamak üzere yapılan *şifreleme* (anlamsız hale getirme) ve *şifre çözme* (tekrar anlamlı hale getirme) çalışmaları ile ilgilenmektedir. Kriptografide şifreli bilgi ele geçse bile meraklı kimse bundan hiç birşey anlayamayacaktır. Şifreli bilgiden asıl bilgiyi elde etmesi ise, günümüz ***Matematik bilgisi*** ve ***bilgisayar hesaplama gücü*** ile, *neredeyse* imkansızdır. Bu nedenle, bilgi güvenliği için çoğunlukla modern kriptografik tekniklerden yararlanılır. Modern kriptografinin bilgi güvenliğini sağlamaya yönelik olarak sunduğu başlıca ***servis***leri şunlardır: ***gizlilik***, *bütünlük*, *kimlik doğrulama* ve *inkarın önüne geçme*. İhtiyaç duyulan bilgi güvenlik düzeyine ulaşmak için pratikte bu servislerin birinden, birkaçından veya hepsinden birden yararlanmak gerekebilir. ***Bilgi güvenliği***, *başkası tarafından dinlenme*, *bilginin içeriğinin değiştirilmesi*, *kimlik taklidi* ve *inkar etme* gibi ***tehdit***lerin ortadan kaldırılması ile sağlanır ve günümüzde bu amaçla kullanılan temel araç kriptografidir.

Kriptografi ile steganografinin birlikte kullanıldığı uygulamalar da bulmak mümkündür: örneğin, bilgi önce şifrelenerek anlamsız hale getirilir, daha sonra şifreli bilgi bir dijital görüntü dosyasının içinde saklanır (bu işlem saklanacak bilgiye ait bilgi *bit*lerinin, görüntüyü oluşturan *piksel*ler denen görüntü birimlerinin, örneğin en düşük anlamlı bitlerine yerleştirilmesiyle yapılabilir) ve *iletişim kanalı*ndan da bu görüntü dosyası gönderilirse hem kriptografik hem de steganografik bir uygulama elde edilmiş olur. Böylesi bir çözüm, bilginin önce kriptografik tekniklerle gizlendiği ve

[1] Bilginin, ***işlenme***si esnasında ***bilgisayar virüsü***, ***truva atı*** gibi ***casus*** *yazılım*lara karşı (*güncel* ***antivirüs*** yazılımları kullanmak yoluyla) korunması gerektiği de unutulmamalıdır. Daha genel olarak, bilginin tüm ***casusluk*** türü ***iç***/***dış*** saldırılara karşı da korunması gerekir.

[2] ***Ulusal*** (askeri, diplomatik, vb.) ya da ***bireysel*** (banka hesap ***şifre***leri, özel hayata ilişkin ***sır***lar, vb.) çok ***değerli varlık***ların ***düşman***lar eline geçmesinin doğurabileceği kötü sonuçları düşününüz.

[3] İlk örneği olarak kabul edilen Roma'lıların ***Sezar şifresi***nde her harf alfabede kendisinden sonraki 3. harf ile yer değiştirmekteydi.

[4] *Permutation* da denir. İlk örneği, eski Yunan'lıların, özellikle de Sparta'lıların, kullandığı söylenen ***Scytale*** *cihazı*dır.

arkasından steganografik tekniklerle saklandığı bir yazı yazma yöntemini ifade etmektedir. Steganografi tek başına güvensiz bir teknik olmasına karşın kriptografik tekniklerle birlikte kullanıldığında tüm sistemin güvenliğinin daha fazla artmasına ***katkı**da* bulunabilir (meraklının önce şifreli mesajı bulması gerekecektir!). Ancak, çalışmamızda bundan sonraki incelemelerimiz daha çok modern kriptografi ve kuantum mekaniğinin günümüz modern kriptografik bilgi güvenlik sistemleri'ne ***etkisi***ni incelemek üzerine yoğunlaşacaktır.

Bildirinin sonraki kısımlarında sırasıyla şu konular ele alınmaktadır: Bölüm 2'de ve Bölüm 3'te sırasıyla *modern kriptografi* ve *kuantum mekaniği* bilimleri hakkında temel bilgiler verilmektedir. Daha sonra, Bölüm 4'te *kuantum rasgele sayı üretimi*, Bölüm 5'te *kuantum kriptografi* ve Bölüm 6'da *kuantum kriptanaliz* konuları ele alınmaktadır. Son olarak, Bölüm 7'de *sonuçlar* yer almaktadır.

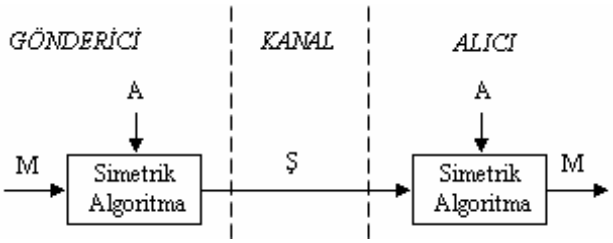
2. Modern Kriprografi

Kriptografinin ***gizlilik*** servisi bilginin gerçek alıcısı dışındaki kimseler tarafından asla anlaşılamamasını ***garanti***ler. Yani, örneğin, sizden başka hiçbir kimsenin size gönderilmiş olan bir elektronik postayı asla okuyamaması gibi. Bu amaçla, kullanılan başlıca yöntem bilgiyi ***şifreleme***dir.

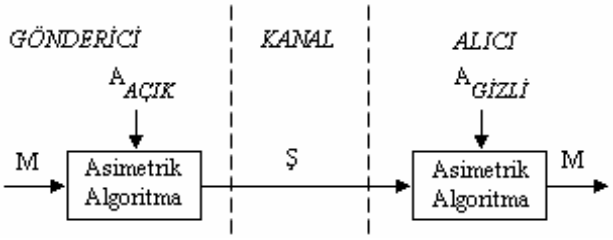
Günümüzde yaygın olarak kullanılan iki tür şifreleme sistemi bulunmaktadır [4]: ***Simetrik*** ve ***Asimetrik*** şifreleme sistemleri. Simetrik sistemlerde tek bir ***gizli anahtar*** vardır (bkz. Şekil 1.a). Hem *gönderici* hem de *alıcı* şifreleme ve şifre çözme işlemleri için aynı gizli anahtarı kullanır. Simetrik sistemler oldukça ***hızlı*** olup şifrelemede öncelikli olarak tercih edilirler. ***Vernam şifresi***, *DES*, *AES*, *IDEA*, *RC4*, vb. en çok bilinen ve kullanılan simetrik şifreleme algoritmalarıdır.

Asimetrik sistemlerde ise ***açık anahtar*** ve ***gizli anahtar***[1] olarak adlandırılan iki farklı anahtar kullanılır (bkz. Şekil 1.b). Her kullanıcı bu anahtar çiftinden kendisine has olan bir tanesine sahiptir. Şifreleme için *açık anahtar* kullanılır ve herkese açıklanmasında bir mahsur yoktur. Şifre çözme için ise *gizli anahtar* kullanılır ve sahibi dışında başka hiç kimse bilmemelidir. Açık anahtarla şifrelenen bir bilgiyi sadece ilgili gizli anahtar, yani o açık ve gizli anahtar çiftinin sahibi, çözebilir. Tersi de geçerlidir; ancak, açık anahtar herkesçe bilindiğinden, gizli anahtarla şifrelenen bir bilgiyi herkes çözebilecek ve okuyabilecektir. Asimetrik sistemler ***yavaş*** olmaları nedeniyle daha çok kısa uzunluktaki mesajları şifrelemede tercih edilir[2]. ***RSA***, *Diffie-Hellman*, *ElGamal* ve *DSS* en çok kullanılan asimetrik şifreleme algoritmalarıdır.

Yukarıda sözü geçen ***anahtar*** kelimeleri şifreleme ve şifre çözme işlemlerinde kullanılan elektronik bir bilgi (*bit dizisi*) anlamındadır. Anahtarlar olmadan şifreleme ve şifre çözme işlemlerini gerçekleştirmek mümkün değildir. Anahtarlar, *şifreleme* ya da *şifre çözme* ***algoritma***sı ile birlikte kullanılarak iletilecek olan bilgiler gönderici tarafta önce şifrelenirler ve alıcı tarafta da tekrar çözülürler. Algoritmaları, tanımlarını ve hatta gerçeklemelerini, rahatlıkla İnternet'te, kitaplarda, dergilerde, vb. pek çok herkese açık ortamlarda bulmak mümkündür. Modern kriptografide algoritmaların gizli olmadığına dikkat ediniz. Algoritmalar herkese açık olup asıl gizlenen parametre, *gizli anahtar*dır. ***Kerckhoff Yasası*** ("*Gizli olması gereken sadece anahtardır.*" [5]) ve ***Shannon***'un ünlü "*Düşman, sistemi bilir.*" sözü de bunu ifade eder [6,7].



***M**: mesaj.*
***A**: **gizli anahtar**.*
***Ş**: şifreli mesaj.*
a)



***M**: mesaj.*
***A**AÇIK: **alıcı**nın **açık anahtar**ı.*
***A**GİZLİ: **alıcı**nın **gizli anahtar**ı.*
***Ş**: şifreli mesaj.*
b)

Şekil 1: Kriptografi, *a*) ***Simetrik kriptografi***: gönderici ve alıcı *aynı* gizli anahtarı kullanır. *b*) ***Asimetrik kriptografi***: gönderici ve alıcı *farklı* anahtarlar kullanır.

Modern kriptosistemler ***gizli anahtar***ların *varlığı*na ve *gizliliği*ne güvenmektedir. Güvenliğin bağlı olduğu başlıca parametre gizli anahtardır: ***rasgele*** seçilen, yeterince ***uzun***, sadece bilgi alış-verişi yapanlarca bilinmesi gereken ***gizli*** bir bit dizisi. Sadece gizli anahtar bilinirse, tüm şifreli bilgilerin kolaylıkla çözülebilmesi özelliğine sahiptirler. Gizli anahtar ile ilgili en önemli konular ise ***üretim***i, taraflar arasında güvenli ***dağıtım***ı ve beşikten mezaradek güvenli ***yönetim***idir.

Öncelikle, çok güvenilir ***üreteç***lere ihtiyaç vardır; öyle ki, gizli anahtar asla *tahmin edilemez* olmalıdır (***üretim***). Sonraki aşama, üretilen anahtarların kullanacaklara *güvenli* bir şekilde *ulaştırılması*dır (***dağıtım***). Son aşama, *kullanılan* anahtarların güvenli bir şekilde *imha* edilmesidir (*yönetim*).

3. Kuantum Mekaniği

Kuantum (*quantum*, aslen Latince olan *quantus*: *ne kadar* sözcüğünden gelmektedir) ***mekaniği***, ***atom***ların ve ***atom-altı*** (*çekirdek*, *elektron*, *foton* gibi *mikroskopik*) ***parçacıklar***ın tarifine olanak veren ***fizik yasaları***nın temelidir[3]. Kuantum mekaniğinin keşfi, ısıtılan cisimlerin ışımasını açıklamak için 1900 yılında önerilen Planck yasası (Max Planck: 1858-1947) ile başlar. Gelişimi, Albert Einstein (1879-1955), Niels Bohr (1885-1962), Werner Heisenberg (1901-1976), Max Born

[1] ***Private key***. Türkçe'mize daha çok ***özel anahtar*** olarak da çevrilir.
[2] ***Elektronik imza***, ***gizli anahtar dağıtımı*** ve ***rassal sayı üretimi*** diğer başlıca yaygın kullanım alanlarıdır.

[3] ***Atom***lar ve ***atomik*** parçacıklar düzeyinde ***madde***nin ***davranış***larını ve ***enerji*** ile ***etkileşim***ini ***matematik***sel olarak ifade eder.

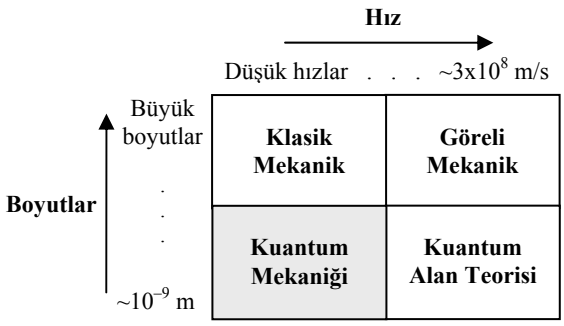
(1882-1970), John von Neumann (1902-1957), Paul Dirac (1902-1984), Wolfgang Pauli (1900-1958) gibi bilim insanlarının çalışmalarını da kapsayan 27 yıllık bir döneme yayılmıştır. 1927 yılında Schrödinger denkleminin (Erwin Schrödinger: 1887-1961) bulunmasıyla, esas olarak bugün öğrendiğimiz son halini almıştır. Kuantum mekaniğinin başarısı, ***Schrödinger denklemi***nin çözümlerinin ***doğa***nın özellikle ***mikro*** yapısında var olan pek çok ***deneysel gerçek*** ile tam ***uyuşum***lu sonuçlar vermesine dayanır. Buna göre kuantum mekaniğinin temel varsayımları (***postüla***ları), pek çok deneysel gerçeğin esasının ele alınmasıdır [8,9].

Kuantum mekaniği, ***doğa***nın/***hareket***in yeni ***teori***sidir. Bu teori atom, elektron, foton gibi ***mikroskopik*** sistemlerin ***davranış***larını açıklar (bkz. Şekil 2). 20. yüzyılın başlarına gelindiğinde artık klasik mekanik ***yasa***ları ile açıklanamayan bir dizi ***gözlem*** bulunmaktaydı [1]. Üstelik, bu gözlemlerin anlaşılması için, klasik fizikte yeri olmayan, *ışığın parçacık* (*tanecik*) *özelliği*, *kütleli parçacıkların dalga karakteri göstermesi* (*maddenin dalga özelliği*) ve hemen hemen tüm *fiziksel niceliklerin kesikli* (*kuantumlu*) *yapısı* gibi yepyeni kavramlardan söz edilmekteydi ve bunlar temel kavramlar olarak kullanılıyordu. Problemler, özellikle atom ve elektron gibi *çok küçük kütle*li ve *çok yüksek hız*lı cisimlerin işe karıştığı ve bunların ışık ve elektromanyetik alanlar ile ***etkileşim*** süreçlerinde ortaya çıkmaktaydı. Bu ***olay***ların en önemlileri şunlardır: *Siyah cisim ışıması*, *Katıların ısı sığası*, *Fotoelektrik olay*, *Compton olayı*, *Elektronlarla kırınım*, *Atomların ışıma ve soğurma spektrumları*. Başlangıçta bu olaylar, amaca uygun özel (ad hoc) ve o zamanlar garip görünen bir takım ***varsayım***larla açıklandı. Zamanla bunların başka olaylar için de geçerli olabileceği öngörüldü. Bu varsayımların sayıları arttıkça ve aralarındaki ilişkiler belirginleştikçe artık mekaniğin yepyeni bir ***formülasyon***u gerekti. 1920'li yılların ikinci yarısına gelindiğinde, sayıca artmış bütün varsayımlar üzerine kurulu yeni bir hareket teorisi gerekiyordu. Sonuç, kuantum mekaniğidir [8].

Kuantum mekaniği ve ***bilgi teorisi*** 20. yüzyılın dünyayı kavrayışımızı değiştiren en önemli buluşlarından ikisidir. Şimdi bilim insanları bu iki farklı disiplini bir şekilde birleştirmenin çabası içindeler. Çalışmamızın bundan sonraki kısımlarında bu gayretlerin, bilgi güvenliğini ilgilendiren sonuçlarına pratiklik sırasıyla yer verilmektedir.

4. Kuantum Rasgele Sayı Üretimi

Rasgele/rassal sayılar[2], kriptografiden istatistiğe, benzetime, örneklemeye, sayısal analize, şans oyunlarına kadar bugün pek çok önemli uygulamada yoğun olarak kullanılmaktadır. Bahsedilen uygulamaların hepsinde de uygulamanın ***başarım***ı açısından rasgele sayıların ***önem***i büyüktür ve hepsinin ***kalite*** gereksinimleri de farklıdır. ***Modern kriptografi***de, gizliliğin doğrudan bağlı olduğu kriptografik ***algoritma*** ve ***protokol*** parametrelerinin (tohum, ilklendirme vektörleri, sorgular, vs.) ve gizli ***oturum*** (şifreleme ve şifre çözme) ***anahtar***larının oluşturulmasında merkezi bir rol oynarlar [11,12].



Şekil 2: Mekaniğin 4 büyük uğraş alanı [10].

Günümüzde yeterince ***kaliteli*** ve ***hızlı*** rasgele sayıları üretmek üzere 2 temel ***üreteç*** türü mevcuttur[3] [13,14]: ***gerçek rasgele sayı üreteci*** (GRSÜ) ve ***sözde rasgele sayı üreteci*** (SRSÜ). GRSÜler ***fiziksel*** bir ***rasgelelik kaynağı***[4] kullanırlar ve daha çok da ürünlere daha sonradan eklenen ayrı bir ***donanım*** olarak tasarlanırlar. SRSÜler ise ***yazılımsal*** olarak gerçeklenirler, bilgisayar ya da ürün içinde koşan ayrı bir ***algoritma***/***program***[5] olarak tasarlanırlar. SRSÜler, GRSÜler kadar *kaliteli*/*güvenilir* olmasalar da daha ***basit***, ***ucuz***, ***hızlı*** ve ***esnek***[6] olmaları nedeniyle daha çok tercih edilirler. Bununla birlikte, SRSÜnün ***durum*** parametresi *fiziksel* bir kaynaktan elde edilen ***entropi***[7] ile en başta ***tohum***lanmalı ve daha sonra da güvenlik için periyodik olarak tekrar tekrar tohumlanmaya devam edilmelidir. SRSÜlerde tüm *entropi* bu *tohum*da yer almaktadır. Bu nedenle, SRSÜ kullanılması durumunda bile tohumu ***beslemek*** üzere GRSÜlere, en azından basit ama *güvenilir* bir GRSÜye, de ihtiyaç olmaktadır. Günümüz GRSÜlerinin *hız*larının henüz çok yüksek olmaması[8], çok hassas olup çalıştıkları ortamın koşullarından çok fazlaca etkilenebilmeleri, zaman zaman ***hata***/***arıza*** da yapabilmeleri SRSÜ kullanımını daha cazip kılan diğer başlıca nedenlerdir.

Yukardaki açıklamalardan da görüldüğü üzere, mevcut ***rasgelelik*** kaynakları, rasgeleliğin doğasına göre iki ana gruba ayrılabilir: sadece *sözde*-rasgele bit dizileri üretebilen ***yazılım*** çözümleri ile *gerçeksi*-rasgele bit dizileri üretebilen ***fiziksel*** kaynaklar. Burada bilinmesi gereken önemli nokta, hem ***klasik bilgisayar***ların hem de ***klasik fizik***in tamamen ***deterministik*** olduğudur. Sonuç olarak, her iki rasgelelik üreteci de rasgele gibi görünen bir bit dizisi üretmek için tamamen ***deterministik***

---

[1] Klasik mekaniğin en önemli niteliği ***deterministik*** olmasıdır. Buna karşılık, ***kuantum mekaniği***nin en önemli özelliklerinden ikisi ***belirsizlik*** (uncertainty) ve ***ayrıklık***tır (discreteness).

[2] ***Rasgele seçilen***, ***tahmin edilemez***, ***tekrar üretilemez*** olan sayılar. Bir sayının ya da sayı katarının rasgele olup olmadığına karar vermek günümüzün en çok tartışılan konularından biridir.

[3] Diğer bir yöntem, ***hibrid rasgele sayı üreteci***dir (HRSÜ). Bu yöntemde, GRSÜ ve SRSÜ birlikte kullanılır. SRSÜ, rasgele sayıları üretir; GRSÜ ise SRSÜyü *tohum*lamakta kullanılır.

[4] ***Zar*** atma, ***para*** atma, direncin ***termal gürültü***sü, avalanj diyodun ***cığ gürültüsü***, ***atmosferik gürültü*** ya da o anki ***zaman*** gibi kuantum olmayan ama çok ***karmaşık*** klasik ***fiziksel prosesler*** sıkça kullanılan gerçeksi rasgelelik kaynaklarıdır. Bunlar aslında tam rasgele değildir, ***deterministik***tir, ***hesaplanabilir***ler ama çok ***kompleks***tirler. Gerçekte, bunlarda ***determinizm*** karmaşıklığın arkasında gizlidir [12].

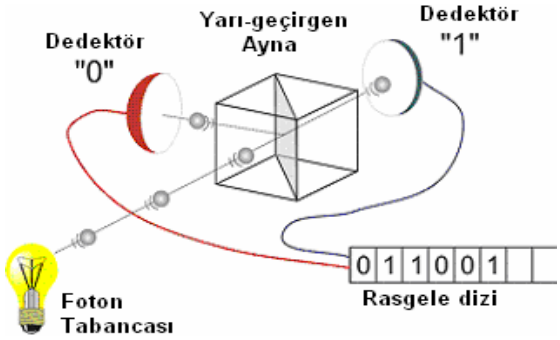
[5] Örneğin, $X_{n+1} \equiv (214013 \cdot X_n + 2531011) \pmod{2^{32}}$ **formül**ü (X_0, rasgele atanması gereken ***başlangıç değeri*** ya da *tohum*dur) ya da π **'nin dijitleri** gibi deterministik bir algoritma kullanılır. Daha genel bir ifade ile bilgisayarlar zaten deterministik sistemlerdir.

[6] SRSÜde değişiklik gerektiğinde tek yapılması gereken sadece ***yazılım***ı değiştirmek, *yazılım*la oynamaktır. GRSÜlerde olduğu gibi çok daha pahalı ve çok daha zor bir çözüm olan yeni bir ***donanım*** tasarımına ve donanım değişikliğine gerek yoktur.

[7] ***Belirsizlik***, ***bilinmezlik miktarı***nı ifade eden matematiksel bir terim.

[8] Buna karşılık, ***iletişim*** ve uygulama ***hız***ları çok daha yüksektir.

olan klasik fiziğe dayanır. Dolayısıyla, aslında, her iki üreteç türü için de tam bir rasgelelikten söz edilemez.



Şekil 3: ***Rasgele bitler***, ***foton***un gittiği ***yol*** uyarınca belirlenmektedir [12].

Bir ***kuantum rasgele sayı üreteci*** (KRSÜ), rasgele sayıları üretmek için ***kuantum fiziği***ni kullanan bir üreteçtir. Klasik fiziğin aksine kuantum fiziği ***deterministik değil***dir. ***Kuantum mekaniği***nde ***tamamen rasgelelik*** hakimdir. Ve KRSÜler de ***rasgelelik kaynağı*** olarak kuantum dünyasının bu ***içsel*** rasgeleliğini kullanır. Rasgele sayılar üretmek için çok ***basit*** birtakım kuantum prosesleri, bunlardaki içsel rasgeleliği, bile kullanmak mümkündür. Örneğin, Şekil 3'te şu an ticari bir ürün haline de gelmiş olan basit bir KRSÜ görülmektedir.

Quantis adı verilen bu KRSÜ, rasgelelik kaynağı olarak ***optik***sel bir kuantum proses kullanır. Optik, ışığın bilimidir. Kuantum fiziği bakış açısından ışık, ***foton*** adı verilen temel ***parçacık***lardan oluşur. Fotonlar belirli durumlarda rasgele bir davranış sergilerler. Örneğin, ikili rasgele sayıların üretimine de çok iyi uyan böylesi bir durum, fotonların ***yarı-geçirgen*** bir aynadan geçişleridir. Bir fotonun *yarı-transparan* bir aynadan geçmesi ya da yansıması tamamen rasgele bir olaydır, başka herhangi bir parametreden de etkilenmez. Şekil 3'teki optik sistemde de olduğu gibi *yarı-gümüşlenmiş* bir aynaya ***tek tek*** fotonlar göndermek ve geçtiklerini ya da yansıdıklarını ölçmek sonucunda elde edilen 0 ve 1 katarı ***gerçek rasgele***dir. Yarı-geçirgen bir aynaya fotonlar göndermek ve geçtiklerini ya da yansıdıklarını ölçmek, kuantum belirsizliğini kullanmanın sadece bir yoludur. Konum, momentum, elektrik alan gibi başka fiziksel büyüklüklerdeki herhangi bir belirsizlik de aynı şekilde işimizi görebilecektir. Sonuçta, elde edilen 0 ve 1 dizisi gerçekten rasgele olmalıdır[1].

Sonuç olarak, kuantum rasgele sayı üreteçleri tek gerçek rasgelelik üreteçleridir. Rasgele bitleri üretmek için kuantum proseslere güvenir/dayanır. Klasik fiziğin aksine, kuantum fiziği tamamen rasgeledir. Genel kanı, rasgeleliğin en iyi kaynağının belirsizliğin tek geçerli olduğu yer olan kuantum dünyası olduğu yönündedir. Buradaki başlıca ***problem***lerden biri ise gerçek rasgele sayıların üretilebileceği hızdır. Fotonlar ve yarı-geçirgen aynalarla çalışan ticari cihazlar için şimdilik 16 Mbps hıza kadar rasgele sayı üretimi yapılabilmektedir[2].

5. Kuantum Kriptografi

Kriptoloji (*cryptology*, aslen Yunanca olan *kryptós*: *gizli*, *gizlenmiş* ve *logia*: *çalışma*, *inceleme*, *araştırma* sözcüklerinin yan yana gelmesinden oluşmaktadır [3]) bilimi, Matematiğin alt dalı olup iki kısımdan oluşur: ***Kriptografi*** ve ***Kriptanaliz*** (*cryptanalysis*, aslen Yunanca olan *kryptós*: *gizli* ve *analýein*: *açmak*, *çözmek*, *halletmek* sözcüklerinden oluşmaktadır [16]). Kriptografi, bilgiyi gizli tutma ***sanat***ı ve ***bilim***idir. Çok özel, zekice ve güçlü matematiksel teknikler kullanarak ***bilgi güvenliği***ni ***garanti***lemeye yönelik çalışır. Bu amaç için tasarlanmış ***algoritma*** ve ***protokol***lerden oluşur. Modern ***kriptosistem***lerde bilgi, ***algoritma*** kullanılarak bir ***anahtar***la karıştırılır ve bir ***şifreli bilgi*** elde edilir. ***Güvensiz*** ortamlar üzerinde bu *şifreli bilgi* iletilir veya saklanır. ***İdeal*** bir kriptosistemde *doğru anahtar* olmadan şifreli bilgiyi çözmek ve ***asıl bilgi***ye ulaşmak ***imkansız*** olmalıdır. Sonuç olarak, şifreleme sisteminin gücü anahtarın gücüne dayanmaktadır[3]: ***hesaplanamaz***lığına[4] ve ***tahmin edilemez*** olmasına[5].

Kriptanaliz ise en zeki, güçlü ve kötü niyetli birisiymiş gibi davranıp yine benzer ***matematik***sel teknikleri, eldeki tüm ***teknoloji***k hesaplama gücünü ve tasarımlardaki ***zayıflık***ları da kullanarak geliştirilmiş mevcut bilgi güvenlik sistemlerini alt etmeye çalışır. Bunu başarmanın başlıca yolu aslında ***gizli anahtar***ı ele geçirmektir, yeterince güçlü olan olan günümüz kriptosistemlerinde algoritma ve protokoller zaten herkesçe bilinmektedir. Bu sistemler, gizli anahtar bilindiğinde şifreli bilgileri çözmenin çok kolay; aksi halde, ise imkansız olması özelliğine sahiptirler. Ancak, bilinmesi gereken diğer bir gerçek de hem Kriptografi hem de Kriptanalizin her ikisinin de Matematik yanında aynı zamanda daha çok klasik fiziğe de dayandığı, ***klasik fizik*** yasaları ile sınırlı olduklarıdır.

Gizli anahtarın güvenliği modern kriptosistemlerde çok ciddi bir meseledir. Bu sorun, ***anahtar dağıtım problemi***[6] olarak da bilinir. Hem modern simetrik hem de asimetrik kriptosistemler ***gizli anahtar***ların varlığına güvenirler; ancak, her iki kriptosistemde de esas problem gizli anahtarlarının gizliliğinin hiç bir zaman tam olarak ***garanti*** edilememesidir. Kırılamazlığı ***teorik*** olarak da ***kanıtlanmış*** tek kriptosistem olan ***Vernam şifresi*** [17,18] bilgi ile aynı uzunlukta gizli

---

[1] Mevcut KRSÜ'ler, bileşenlerinin henüz ***kusursuz*** çalışmaması (örneğin, yarı-geçirgen aynanın ***49%*** geçirgen olması ya da tek foton kaynağının ara sıra ***2*** ya da ***3*** foton da üretebilmesi gibi ***kusur***lar) nedeniyle ***klasik*** ve ***kuantum*** kısımlardan oluşmaktadır:

- ***Kuantum kısım***: Rasgelelik kaynağı olan ***kuantum proses***i içerir. Bileşenlerin henüz ***mükemmel*** olmaması nedeniyle elde edilen 0, 1 dizisi ***düzgün dağılım***lı (*eşit olasılıklı*) değildir.
- ***Klasik kısım***: Düzgün dağılımlı olmayan 0, 1 katarını mümkün olduğunca *düzgün dağılımlı* (*eşit olasılıklı*) hale getirmek için bazı ***son-işleme*** (*post-processing*) adımlarını içerir.

[2] Bir US takımı *detektöre ulaşan fotonlar arasındaki aralıklar*a dayanan ***çözüm***leri ile 100 Mbps, Çinliler *faz gürültüsü*nü kullanan yöntemleri ile 300 Mbps ve bir İsrail takımı bir *lazerin kaotik çıkışı*nı kullanan çözümleriyle 3 Gbps kadar pratik hızlara da çıkabilmektedir. Son yöntem oldukça iyi gibi görünmesine karşın, buradaki rasgelelik tam olarak kuantum-tabanlı bir rasgelelik değildir [15].

[3] Modern şifreleme ve şifre çözme algoritmalarının yeterince ***güçlü*** olduğu kabul edilmektedir. Gerçekten de günümüzde yeterince güçlü şifreler kullanılmaktadır. Tek sorun, güvenliğin henüz ***ispatlanmamış*** birtakım ***matematik***sel ***problem***lere dayanıyor olmasıdır.

[4] Yeterince ***uzun*** olmalıdır. Modern kriptografide ***güvenlik düzeyi***ni ayarlamaya yarayan esas parametre ***anahtar uzunluğu***dur.

[5] Gerçekten ***rasgele*** olmalıdır. ***Tekrar üretilemez*** olmalıdır.

[6] ***Anahtar dağıtımı***, modern kriptografinin en önemli konularından ve en büyük problemlerinden biridir. ***Anahtar dağıtım protokolleri***, birbiriyle *güvenli* haberleşmek isteyen; ancak, *mekan* olarak birbirinden çok uzakta olan iki kullanıcının sadece ikisinin bildiği ***ortak*** ve ***gizli*** bir ***anahtar*** üzerinde anlaşmasını sağlar. En güvenli yollardan ikisi: *i*) *güvenilir* ***kurye***, *ii*) *müdahalelere karşı korumalı, özel olarak tasarlanmış, çok güvenli taşıyıcı* ***cihaz***lar.

anahtarlar kullanır. Tek kullanımlık bu anahtarların her iki tarafta da olması gerekir. Anahtarın karşı tarafa güvenli olarak ulaştırılması simetrik kriptografide ciddi bir problemdir. Meraklı kişiler anahtar dağıtımı esnasında araya girerek bir şekilde anahtarın bir kopyasını ele geçirebilir.

Asimetrik kriptosistemlerde ise durum daha da kötüdür. Örneğin, özellikle *İnternet* sayesinde dünya çapında yaygın kullanım alanı bulan ***RSA***'de [19] açık anahtarda açıklanan bir sayıyı asal çarpanlarına ayırarak gizli anahtarı elde etmek mümkündür. Çok büyük olan bu sayıyı günümüz ***matematik bilgisi*** ve ***bilgisayar hesaplama gücü***yle ***makul bir süre***de çarpanlarına ayırmak neredeyse imkansızdır[1] [20]. Ancak, eğer teknolojik gelişmelerdeki hız gözönüne alınırsa bunun oldukça ***risk***li bir varsayım olduğu da açıktır. 10-15 yıl içinde geliştirilmesi ümit edilen ***kuantum bilgisayar***ın bu işlemi çok rahatlıkla gerçekleştirebileceği ***ispat***lanmış durumdadır[2].

Dolayısıyla, bahsedilen anahtar dağıtım sorunlarının ve ***risk***lerinin olmadığı bir kriptosisteme ihtiyaç vardır. Ulaşılan sonuç ise yepyeni bir alan olan ***kuantum*** *kriptografi*dir[3].

Kuantum kriptografi (KK), *bilgi güvenliği*nin *kuantum mekaniği*ne ait (***belirsizlik ilkesi***, ***foton polarizasyonu***, ***dolaşıklık*** gibi) ***yasa***lar ile ***garanti*** edildiği kriptografi tekniğidir[4] [21,22]. Temel avantajı, ***kanıtlanmış evrensel*** kuantum mekaniği yasalarına dayanıyor olması[5], güvenliğin ***ispatlanabilir*** olmasıdır. En bilinen ve ilk pratik uygulaması ***kuantum anahtar dağıtımı***dır (KAD) [23]. Yakın zamana kadar KK ve KAD aynı anlamda kullanılmaktaydı. Doğrusu, KK'nın KAD'ı da içine alan daha geniş bir disiplin olduğudur. ***Kuantum bilgisayar***a karşı tüm bilgi güvenliğini sağlama çalışmaları (klasik ya da kuantum olsun) da KK'nın kapsamı içinde kabul edilmektedir[6] [24,25]. Mevcut KK, şimdilik klasik ve kuantum kısımlardan oluşmaktadır:

- ***Kuantum kısım***: Kuantum anahtar dağıtımı (KAD).
- ***Klasik kısım***: Geleneksel kriptografi ile şifreleme.

Mutlak (*koşulsuz*, asla *kırılamaz*) ***güvenlik***te bir iletişim için KK'nın günümüzdeki temel çalışma prensibi şöyledir:

- ***Anahtar***, taraflar arasında ***KAD*** ile dağıtılır. Dolayısıyla, KK'da *anahtar dağıtım problemi* KAD ile çözülmektedir. KAD, güvenliği ***kanıtlanmış***, *tamamen* güvenli tek anahtar dağıtım yöntemidir.
- ***Şifreleme***, ***Vernam şifresi*** ile yapılır. Vernam şifresi kırılamazlığı ***kanıtlanmış*** tek şifredir.

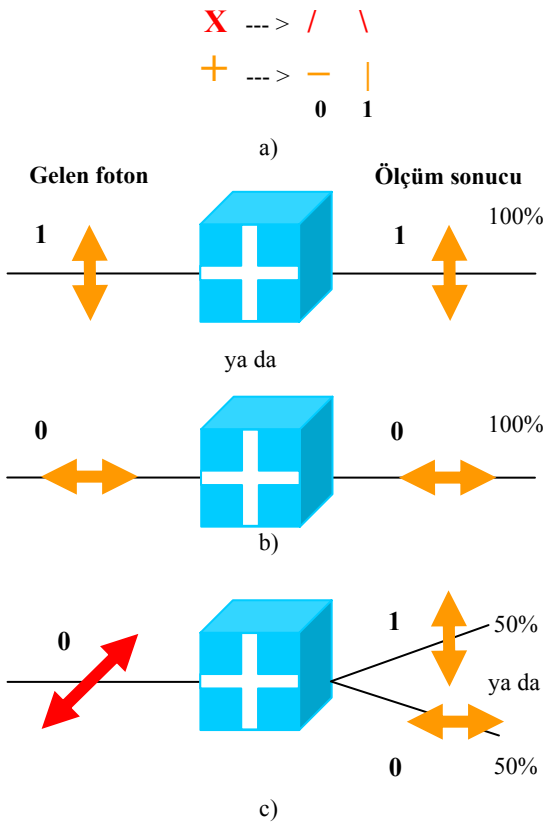
Böylece, KK'da ***mutlak*** (asla *kırılamaz*) güvenlikte bir iletişim ortamı ***garanti*** edilmiş olmaktadır.

KAD protokolleri, birbirinden çok uzakta olan iki kullanıcı arasında ***aynı***, ***rasgele*** ve ***güvenli*** bir ***gizli anahtar*** oluşturulmasını sağlar. Kuantum mekaniği yasaları, anahtar dağıtımı esnasında, gerçekleştirilen iletişime herhangi bir müdahale olup olmadığını (kuantum bilgi ile etkileşimde olan meraklı kimselerin varlığını) açığa çıkarabilmeyi de sağlar[7]. KAD'ın, temel çalışma ilkesi ise şu şekildedir:

- ***Anahtar***, tam ***güvenli*** bir şekilde dağıtılır.
- Aksi halde, protokol ***iptal*** edilir ve ***tekrar*** denenir.

Böylece, anahtarın taraflar arasında ***mutlak*** güvenli bir şekilde dağıtılması ***garanti*** edilmiş olmaktadır.

KAD, güvenli iletişim (birbirinden uzak iki kullanıcı arasında güvenli anahtar dağıtımı) için kuantum mekaniğinin en temel ***postüla***larından olan ***Heisenberg belirsizlik ilkesi***ne güvenir[8]. İletişim için temel kuantum taneciklerden olan ***foton***lar kullanılır ve anahtar bitlerini temsil etmek üzere de fotonların ***polarizasyon*** özelliğinden yararlanılır[9].



Şekil 4: Fotonlarla kuantum iletişim ve belirsizlik ilkesi [26]. a) ***Kodlama*** kuralı, b) Alıcıda gerçekleşen ***uyumlu ölçüm***lerin sonucu ***kesinlikle*** doğru olmaktadır. c) Alıcıda gerçekleşen ***uyumsuz ölçüm***lerin sonucu ***50%*** doğru olur.

[1] Gereken sürenin evrenin ömrü ($10^{10} \approx 2^{34}$ yıl, yaklaşık 10 milyar yıl civarı bir süre) ile sınırlı olduğu öngörülmektedir.

[2] Bu işi gerçekleştirecek ***kuantum algoritma*** şimdiden hazır bile: ***Shor'un algoritması***. Dolayısıyla, tek eksik bu algoritmanın üzerinde koşturulabileceği geniş ölçekli bir kuantum bilgisayardır.

[3] Klasik kriptografi sınırlı bir ***zaman dilimi*** ve ***teknolojik düzey*** için gizlilik sağlarken, kuantum kriptografi teknolojik gelişmelerden dahi etkilenmeyen çok daha ***uzun vade***li ve ***kalıcı*** gizlilik sağlar.

[4] ***Kriptografik servisler***i gerçeklemek üzere ***kuantum mekaniği***nin sonuçlarından (***foton***, ***Heisenberg belirsizlik ilkesi***, vb.) yararlanılır.

[5] Ve bunların klasik olarak bir eşdeğerlerinin de bulunmamasıdır.

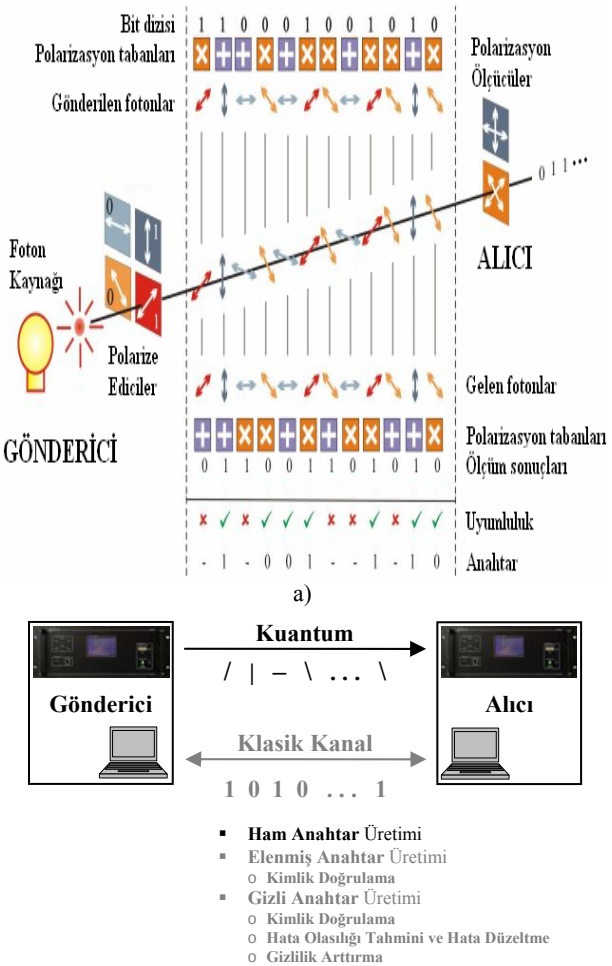
[6] Halen kuantum bilgisayar tarafından bir saldırı keşfedilmemiş klasik problemler ve ***post-kuantum*** kriptosistemler de mevcuttur.

[7] Bu klasik iletişimde bir eşdeğeri olmayan özelliklerdendir.

[8] Bu ilke özetle, "(***Bilinmeyen***) *Bir kuantum sistemi* ***ölçmek*** *o sistemi* ***değiştirecektir***." der. Bunun bir sonucu olarak, böylesi bir kuantum sistemle (ya da *bilinmeyen* bir *kuantum durum* ile) temsil edilmiş olan ***kuantum bilgi*** de değişmiş olacaktır. İlke aynı zamanda, bir kuantum sistemin (*bilinmeyen*) belirli özellik çiftlerinin (*konum* ile *momentum*, bir *doğrusal polarizasyon* ile bir *dairesel polarizasyon*, vb.) ***aynı anda*** asla tam olarak ölçülemeyeceğini de ifade eder Dolayısıyla, *belirsizlik yasası*nın gereği olarak, kuantum bilgiyi rahatsız etmeden üzerinde ölçümler yapmak ve bilgiyi elde etmek mümkün değildir. Bu da bizleri (*bilinmeyen*) ***kuantum bilgi kopyalanamaz*** sonucuna götürür. Bu sonuçlar, bizlere bilgi ile etkileşimde olan saldırganların varlığını çok rahatlıkla tespit edebilme olanağını da verir.

[9] Anahtarı taşıyıcı güvenilir ***kurye*** olarak ***foton***lar kullanılmaktadır. ***İdeal***de her bir anahtar ***bit***i tek bir ***foton*** ile taşınır.

Şekil 4'te tek tek fotonlarla gerçekleştirilen bir kuantum haberleşme örneği görülmektedir[1]. Alıcı, gelen herbir fotonu (/, \, – veya |) ölçeceği yönteme (X veya +) ***rasgele*** olarak[2] karar verir[3]. Eğer ***uyumlu*** bir ölçüm yaparsa foton bu ölçümden rahatsız olmaz ve ölçüm sonucu da kesinlikle doğru olur. Eğer ölçüm uyumsuz olursa, yapılan ölçüm hem fotonu rasgele olarak değiştirir hem de ölçümün sonucunu[4].



a)

- **Ham Anahtar** Üretimi
- **Elenmiş Anahtar** Üretimi
  - **Kimlik Doğrulama**
- **Gizli Anahtar** Üretimi
  - **Kimlik Doğrulama**
  - **Hata Olasılığı Tahmini ve Hata Düzeltme**
  - **Gizlilik Arttırma**

b)

Şekil 5: ***BB84 protokolü*** [27]: a) *Gizli anahtar* bitleri, tek tek fotonlarla taşınmaktadır. b) ***Gizli anahtar***, ***kuantum*** ve ***klasik iletişim***ler sonucu belirlenmektedir

Şekil 5.a'da, anlatılan bu ilkelere dayanan ve şu an ticari bir ürün [28] haline de gelmiş olan basit bir KAD protokolü görülmektedir. Protokol ilk olarak Charles **B**ennett ve Gilles **B**rassard tarafından ve 19**84** yılında önerilmiş olması [29] nedeniyle ***BB84*** protokolü olarak da adlandırılır.

BB84 KAD protokolü, hem kuantum hem de klasik kısımlardan oluşmaktadır (bkz. Şekil 5.b):

- ***Kuantum kısım***: İlk aşama, aday anahtar bitlerinin tek tek foton tanecikleriyle taşınmasından oluşur.
- ***Klasik kısım***: Sonraki aşama ise alıcının ölçüm sonuçlarının değerlendirilmesidir.

Protokol, özetle şu şekilde gerçekleşmektedir:

BB84 PROTOKOLÜ:

Kuantum kısım

Adım 1: Gönderici, *ham anahtar* bitlerini rasgele olarak oluşturur. Bunun için bir KRSÜ kullanır. Herbir bitini bir *fotonun polarizasyon durumu* ile ifade edip fotonları ***kuantum kanal*** üzerinden teker teker alıcıya gönderir. Herbir bitini hangi tabanda kodlayacağına *rasgele* karar verir.

Adım 2: Alıcı, gelen herbir fotonu *rasgele* seçtiği[5] bir tabanda ölçer. Eğer seçtiği taban gönderici ile aynı ise, *ideal* durumda ölçüm sonucu da göndericinin biti ile kesinlikle ***aynı*** olacaktır. Farklı bir taban seçmişse, ölçüm sonucu ***50%*** ihtimalle/şansla doğru olacaktır. Ancak, henüz bunu bilmemektedir. Aynı durumlar aradaki bir saldırgan için de sözkonusudur.

Klasik kısım

Adım 3: Tüm iletim ve ölçümler tamamlandıktan sonra alıcı, sadece gelen fotonları hangi ***taban***larda ölçtüğünü bir ***klasik kanal*** üzerinden[6] açıklar. Gönderici, alıcıya aynı tabanı kullandıkları indeksleri açıklar. İdealde (gürültü, kusurlar, dinleme, vb. yoksa) bu indekslerdeki bitler de kesinlikle aynı olmalıdır.

Adım 4: Arada bir meraklının varlığını tespit etmek için bitlerin bir alt kümesi de açıklanır. Aynı tabanların kullanıldığı bitler de kesinlikle aynı olmalıdır. Eğer aynı değilse, bu ilgili fotonlara bir müdahale olduğu anlamına gelir ve protokol ***iptal*** edilir[7].

Adım 5: Herşey güvenli ise kalan ortak bitler **gizli anahtar** olarak kabul edilir.

BB84 protokolünün bahsedilen tüm aşamalarını standart kuantum optik laboratuvarı ekipmanları ile gerçekleştirmek mümkündür. Anahtar dağıtımı için hem gönderici hem de alıcının temel olarak şu iki ana bileşene ihtiyacı vardır:

- **Kuantum Kanal**: İletişim ***tek yönlü***dür. Göndericiden alıcıya ***kuantum sinyal***leri (***kübit***: *kuantum bit*) oluşturmak ve göndermek için kullanılır. İletim ortamı (*fiber optik kablo*, *hava boşluğu*, vb. optik ortamlar) ve tüm diğer iletim ekipmanları (*tek foton üreteci*, *foton polarize edici*, *foton polarizasyon ölçücü*, *foton detektörü*, vb. optik bileşenler) kuantum

[1] Alıcının gelen her bir fotonu ölçmeden önce göremeyeceğine ve bilemeyeceğine dikkat ediniz. KAD'da, hem alıcı hem de saldırgan bilmedikleri kuantum durumları ölçmek zorundadır.

[2] Rasgelelik için KRSÜ'lerden yararlanılması protokolün güvenliği açısından büyük önem taşımaktadır.

[3] ***Heisenberg belirsizlik ilkesi*** gereği, alıcının aynı anda hem X hem de + tabanında ölçümler yapması kesinlikle yasaktır. Aynı durum meraklı kişi için de geçerlidir.

[4] Alıcının yaptığı bir ölçümün sonucunun doğru mu ya da yanlış mı olduğunu bilemeyeceğine de dikkat ediniz. Aynı durum saldırgan için de söz konusudur.

[5] Bunun için bir KRSÜ kullanır.

[6] İnternet, telefon, cep telefonu, vb. yaygın kablolu/kablosuz ya da optik/elektriksel iletişim yöntemleri olabilir.

[7] Gerçek hayatta arada bir saldırgan olmasa bile kanal gürültüsü, optik ve elektriksel bileşenlerin henüz kusursuz olmaması gibi nedenlerle de bu bitler farklı olabilmektedir. Dolayısıyla, örneğin, 15%'lik bir hata olasılığına kadar protokolün devamına izin verilir.

kanal olarak ifade edilebilir. Kuantum kanalın dış ortam ile etkileşimden yeterince izole edilmiş olması gerekir. Ayrıca, kanalın kendisi de kuantum sinyal ile herhangi bir etkileşime girmemelidir. Sonuç olarak, ortamın fotonları değiştirmez olması önemlidir. Meraklı kişiler kuantum kanalda fotonları hem gözleyebilir hem de tekrar gönderebilirler. Fizik yasaları dışında kısıtlama olmaksızın kanala erişip istediği ***aktif*** ve ***pasif*** müdahaleleri yapabileceği varsayılır. Ancak, yaptığı ölçümler ilgili kübitleri değiştirecektir, bu da meraklıyı ele verecektir.

- **Klasik Kanal**: İletişim ***iki yönlü***dür. Göndericinin ve alıcının birbirlerine sıradan ***klasik sinyal***leri (klasik ***bit***ler) oluşturması ve gönderip alması için kullanılır (İnternet, cep telefonu, vb. telli/telsiz ortamlar). ***Kimlik doğrulama***lı olmak zorundadır; yani, gönderici ve alıcı birbirlerinin kimliklerini doğrulayabilmelidir. Bu nedenle, meraklı kişiler kimlik doğrulamalı klasik kanaldan gidip gelen mesajları sadece ***pasif***çe dinleyebilir, gözleyebilir; aktif herhangi bir müdahalede ise bulunamazlar. Sonuç olarak, meraklıların klasik kanalda gidip gelen bilgileri sadece gözleyebileceği varsayılır. Klasik iletişimin dinlendiği ise anlaşılamaz.

BB84 protokolü, bu iki ana bileşen üzerinde yer yer içiçe geçmiş şu 3 ana aşamadan oluşmaktadır:

- **Ham anahtar değiş-tokuşu**[1]: Kuantum durumların iletildiği ve ölçüldüğü kısımdır. İki taraf arasında ***kübit***ler (*polarize edilmiş foton*lar) değiş-tokuş edilir. KAD'ın tek kuantum olan kısmıdır, iletişim kuantum kanal üzerinden gerçekleştirilir. Bu adımın sonucunda ***ham anahtar***lar oluşur. Göndericinin ham anahtarı kuantum kanaldan gönderdiği tüm bitlerdir. Alıcının ham anahtarı ise ölçebildiği tüm bitlerdir. Gönderici ve alıcı ellerindeki ***bit***lerinin ve polarizasyon ***taban***larının bir kaydını tutarlar. *Ham anahtar*lardan *gizli anahtar*a götüren sonraki tüm adımlar ve iletişimler *kimlik doğrulama*lı bir klasik haberleşme kanalı üzerinden gerçekleştirilir.
- **Anahtar eleme**[2]: Kuantum kanaldaki kayıplardan dolayı göndericinin ve alıcının ham anahtar uzunlukları farklı olabilir. Öncelikle, alıcı tespit ettiği kübitlerin indeksini *kimlik doğrulamalı* klasik kanaldan açıklayarak göndericiyi haberdar eder. Daha sonra, bu bitlerden de polarizasyon tabanlarının uyumlu olduğu durumlardakiler seçilir. Bu adımın sonucunda ortaya bir ***elenmiş anahtar*** çıkar. Göndericinin ve alıcının elenmiş anahtarı büyük ölçüde aynıdır ve uzunlukları da eşittir.
- **Damıtma**[3]: Gönderici ve alıcı elenmiş anahtarlarını birlikte işleyerek daha güvenli ve tamamen aynı bir hale getirirler. ***Gizli anahtar***, bu adımın sonucunda ortaya çıkar. Bu adımın kendisi de yine içiçe şu 3 temel aşamadan oluşmaktadır [30]:
  1) Kimlik doğrulama,
  2) Hata düzeltme ve
  3) Gizlilik arttırma.

Böylece, ***güvenli***, ***rasgele*** ve her iki tarafta da ***aynı*** olan bir ***gizli anahtar*** oluşturulmuş olur.

Görüldüğü üzere, mevcut KAD protokollerinin güvenliği şu üç ana etkene bağlıdır [31]:

- ***Kuantum mekaniği***nin doğru olmasına.
- Gönderici ve alıcı arasındaki ***kimlik doğrulama***nın koşulsuz güvenlikte olmasına: *Aksi halde, protokol* ***ortadaki adam saldırısı****na karşı savunmasız hale gelmektedir.* ***Simetrik anahtarlı kimlik doğrulama*** *yöntemleri, koşulsuz güvenlikte kimlik doğrulama olanağı sağlayabilirler; ancak, taraflar arasında bir öngörüşme ile dağıtılmış simetrik anahtarların varlığını gerektirirler. Diğer bir yöntem olarak, güvenli* ***asimetrik anahtarlı kimlik doğrulama*** *yöntemlerinden de yararlanılabilir.*
- Kullanılan ***ekipman***ların güvenli olmasına: *Gönderici ve alıcı arasında doğrudan bir bağlantı gerektirir. KAD'da rasgeleliğin gerektiği yerlerde bir KRSÜ'nün kullanılması ise özellikle önerilen bir diğer önemli noktadır. Gerçeklemelerde de herhangi bir zayıf nokta olmamalıdır.*

İlk KAD protokolü olan BB84'ten sonra, başka protokol önerileri de olmuştur: B92, E91, SARG04, vb.. KK, KAD ve protokolleri hakkında daha detaylı bilgi için [32,33]'ten ve kaynaklarından da faydalanılabilir.

6. Kuantum Kriptanaliz

Kriptanaliz, kriptografinin aksine, şifreleri çözme ve şifreli bilgileri okuma ***sanat***ı ve ***bilim***idir[4]. ***Kuantum kriptanaliz***, ***kuantum bilgisayar***lar kullanarak[5] şifreleri kırmakla ilgilenen kriptografik bir uygulama alanıdır [34].

Kuantum kriptanalizin şu an için en çok bilinen örneklerinden birisi 1994 yılında matematikçi Peter W. Shor (1959) tarafından önerilen ***Shor algoritması***dır [35][6]. Bu algoritma, çarpanlara ayırma problemini çözmenin verimli bir yoludur. Geleneksel kriptografik teknikler anahtar iletiminin güvenliğini sağlamak için daha çok matematiksel yaklaşımlara güvenirler[7]. Ancak önerdikleri güvenlik, henüz *kanıtlanmamış* bazı *varsayım*lara dayanmaktadır ve teknolojiye de çok bağımlıdır. Örneğin, henüz araştırılma safhasında olan ***kuantum bilgisayar*** kariptanalizde kullanılma potansiyeline sahiptir. Shor'un algoritması geniş ölçekli bir kuantum bilgisayar ile çok büyük tamsayıları kolaylıkla çarpanlarına ayırabilecektir. Böylece, yaygın kullanımda olan bazı açık-anahtarlı şifreleme algoritmaları da kırılmış olacaktır.

Aynı şekilde, bilgisayar bilimci Lov K. Grover (1961) tarafından önerilen ***Grover algoritması***nın [38] bir kuantum bilgisayarda çalıştırılmasıyla, kaba-kuvvetle anahtar aramaları

---

[1] ***Raw key Exchange (RKE)***.

[2] ***Key sifting***. Kaynaklarda bu aşama ***information reconciliation***: *anahtar uzlaştırma* (*hata düzeltme* teknikleriyle) olarak da verilir.

[3] ***Key distillation***. Kaynaklarda bu aşama ***privacy amplification***: *gizlilik arttırma* (*özet fonksiyonları* yoluyla) olarak da verilir.

[4] Gizli anahtarı bir şekilde ele geçirerek ya da geçirmeden. Genellikle, kriptanaliz gizli anahtarı ele geçirmenin en zor yolu olarak kabul edilir. Sistemdeki zayıflıklarla aynı iş daha kolayca yapılabilir.

[5] Dolayısıyla, bazı ***kuantum mekaniksel sistem***lerden, birtakım ***kuantum mekaniksel etki***lerden yararlanılmış olmaktadır.

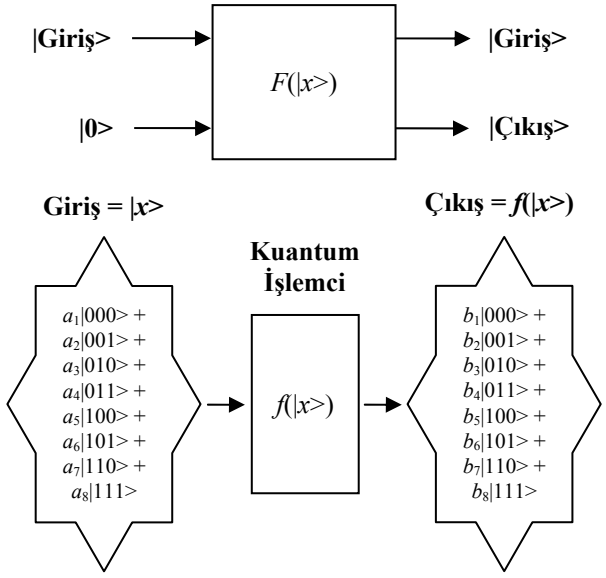
[6] Fizikçi Richard P. Feynman (1918-1988) [36] ve teorik fizikçi David E. Deutsch (1953) [37] gibi bilim insanlarının 1980'lerdeki çalışmaları ile Kuantum hesaplama konusu gündeme gelmişti. Ancak, esas reklamını aslen bir matematikçi olan Peter Shor yapmıştır. Ancak Shor'un algoritmasından sonra çeşitli ulusal ve özel güvenlik kurumları, bankalar, vs. bu işin peşine ciddiyetle düşmüştür.

[7] Hesapsal karmaşıklığa güvenir. Çözülmesi neredeyse imkansız kabul edilen bazı matematik problemlerinin çözülemezliğine bağlıdır.

da karesel olarak daha hızlı yapılabilir. Bununla birlikte, anahtar uzunluğu iki katına çıkartılmak suretiyle bu tehditten kurtulabilmek şimdilik mümkündür.

KAD'ın aksine, diğer birçok kuantum uygulama[1] gibi kuantum kriptanaliz de büyük ölçekli bir kuantum bilgisayarın yapılmasını beklemektedir.

Kuantum bilgisayar, bilgi üzerinde birtakım işlemler gerçekleştirmek için doğrudan ***süperpozisyon***[2], ***dolaşıklık***[3] gibi kuantum fenomenleri kullanan aşırı derecede paralel bir hesaplama makinesidir [39]. Henüz var olan şeyler değildir; ancak, eğer teknik problemlerin üstesinden gelinir ve geniş ölçekli kuantum bilgisayarlar yapılırsa, kriptografiye ve dolayısıyla da bilgi güvenliğine etkisi çok büyük olacaktır. Şu an ki versiyonları henüz sadece birkaç kübiti (***kübit***: kuantum bit [40]) idare edebilmektedir ve en son haberlere göre 128 kübite kadar çıkılabildiği de görülmektedir [41].



Şekil 6: Kuantum bilgisayarın çalışma prensibi. *n* kübitlik bir kuantum saklayıcı, olası 2^n değerin hepsini birden aynı anda tutabilir. Kuantum işlemci de bu olası 2^n değerin hepsi üzerinde aynı anda işlem yapabilir.

Bir kuantum bilgisayarın ne olduğunu ve neler yaptığını daha iyi anlayabilmek için öncelikle bir klasik bilgisayarın neler yaptığına bakabiliriz. Klasik bilgisayar, bir ***ikili*** giriş alır (örneğin, 100010) ve bir ikili çıkış verir (belki, 0101). Eğer birden çok giriş varsa, herbiri üzerinde tek tek çalışması gerekir. Benzer şekilde, bir kuantum bilgisayar da giriş olarak belirli sayıda kübit alır ve birkaç kübit çıkarır. Ana fark, kuantum bilgisayarda hem giriş hem de çıkış kübitlerinin belirli temel durumların lineer kombinasyonları olabilmesidir. Kuantum bilgisayar, bu lineer kombinasyondaki tüm temel durumlar üzerinde aynı anda çalışabilir (bkz. Şekil 6). Gerçekte, kuantum bilgisayar bir paralel makinedir[4].

Örneğin, üç parçacığı temsil etmek üzere |100> temel durumunu[5] düşünelim: ilk parçacık 1 durumunda ve son ikisi ise 0 yönelimindedir[6]. Kuantum bilgisayar, sadece bu |100> durumunu alabilir ve bir çıkış üretebilir. Bununla birlikte,

$$\frac{1}{\sqrt{3}}(|100> + |011> + |110>) \qquad (1)$$

gibi temel kuantum durumların normalize edilmiş[7] lineer bir kombinasyonunu[8] da giriş olarak alabilir ve yine tek bir temel durumla çalıştığı kadar hızlıca çalışarak bir çıkış üretebilir. İşte bir kuantum bilgisayarı potansiyel olarak çok daha güçlü yapan bu, durumların lineer kombinasyonu ile aynı anda çalışma, yeteneğidir. Buna rağmen, kuantum bilgisayar üzerinde çalıştığı bir kuantum durumun temel durumlardan sadece birisi mi yoksa temel durumların lineer bir kombinasyonu mu olduğunu ölçüm yapmadan bilemez. Ancak, böylesi bir ölçüm de girişi değiştirecektir[9].

Bir klasik bilgisayarda x girişiyle çalıştırılabilen bir $f(x)$ fonksiyonumuz olduğunu varsayalım. Klasik bilgisayar bir x girişi ister ve bir $f(x)$ çıkışı üretir. Diğer taraftan, bir kuantum bilgisayar, giriş olarak aşağıdaki gibi tüm olası x giriş durumlarının bir toplamını kabul edebilir:

$$\frac{1}{C}\sum_x |x\rangle = \frac{1}{C}(|x_0> + |x_1> + \dots) \qquad (2)$$

(C bir normalizasyon faktörüdür/sabitidir) ve aşağıdaki gibi bir çıkışı da üretebilir:

$$\frac{1}{C}\sum_x |x, f(x)\rangle = \frac{1}{C}(|x_0, f(x_0)> + |x_1, f(x_1)> + \dots) \qquad (3)$$

Burada, $|x, f(x)>$ kübitlerin daha uzun bir dizisidir: hem x hem de $f(x)$ değerlerini temsil eder[10]. Böylece, $f(x)$'in tüm değerlerinin bir listesini elde edebiliriz. Bu noktada sorun, hesaplamanın sonucuna ulaşmaktır. Eğer bir ölçüm yaparsak, kuantum durumu ölçümün sonucuna zorlarız. Yani, rasgele seçilen bir x_0 değeri için $|x_0, f(x_0)>$ sonucunu elde ederiz, ve çıkıştaki tüm diğer durumlar yok edilir. Bu nedenle, $f(x)$'in değerlerinin listesine bakacaksak eğer, tek bir şansımız olduğu için, bunu çok dikkatlice yapmalıyız. Özellikle, onu daha çok istenilen bir şekle sokmak için belki çıkışa bir dönüşüm uygulamak gerekir. İşte, bir kuantum bilgisayarı programlamadaki temel hedef de hesaplamayı tasarlamak şeklindedir; öyle ki, görmek istediğimiz çıkışlar diğerlerinden çok daha yüksek bir olasılıkla görünsün. Shor'un çarpanlara ayırma algoritmasında[11] yapılan da tam olarak budur[1].

---

[1] Kuantum özel kanallar, kuantum açık anahtarlı şifreleme, kuantum zar atma, kör kuantum hesaplama, kuantum para, vs..

[2] Bir kübitin aynı anda hem 0 hem de 1'i tutabilmesi kuantum sistemlerin süperpozisyon (ya da *üst üste binme*) özelliğinin bir sonucudur. *n* durumlu bir kuantum sistem belli bir anda bu olası *n* durumun hepsinde birden bulunabilir. Bu özelliğe süperpozisyon ya da üst üste binme denir. Üstkonum dendiği de olur.

[3] Dolaşıklık, iki kübitin birbiriyle ilişkili olmasıdır. Öyle ki, birinde yapılan bir değişiklik diğerini de etkiler.

[4] *n* kübitlik tek bir kuantum bilgisayarın işlem gücü açısından *n* bitlik 2^n adet klasik bilgisayara eşit olduğu söylenebilir.

[5] Özdurum: $|\psi> = a_0|0> + a_1|1>$, $a_1 = 0$ veya $a_2 = 0$, a_1, a_2 kompleks.

[6] $|\boldsymbol{x}>$: x kuantum durumunu ifade etmek üzere Dirac notasyonudur. Bir kuantum parçacığı, istenilen bir kuantum duruma sokmak için, örneğin Şekil 4'teki gibi işlemler uygulanabilir.

[7] Yani, 1 uzunluklu.

[8] Süperpozisyon: $|\psi> = a_0|0> + a_1|1>$, $a_1 \neq 0$ ve $a_2 \neq 0$.

[9] Bir kuantum bilgisayar belirli işlemleri oldukça verimli olarak yapabilmektedir: örneğin, ***periyot bulma***.

[10] Bazı kuantum parçacıkları da f(x) değerine değiştirmek üzere girişi $(1/C)\sum|x, 00\dots0\rangle$ şeklinde yapmak notasyon olarak daha iyi olabilirdi; ancak, basitlik için bu yapılmamıştır.

[11] Yeteri kübitlikte bir kuantum bilgisayar ile çarpanlara ayırma işini polinomsal zamanda yapmaktadır.

KRSÜ, KK ve KAD'da olduğu gibi Shor'un algoritması da klasik ve kuantum kısımlardan oluşmaktadır[2]:

- ***Klasik kısım***: Klasik bir bilgisayarda yapılabilecek olan bu kısımda, çarpanlara ayırma problemi bir *mertebe/periyot-bulma* [3] problemine indirgenir. Bu kısım, eskiden beri bilinmekte olan bir kısımdır.
- ***Kuantum kısım***: Mertebe-bulma problemini çözmek üzere bir kuantum algoritma içerir. Yani, kuantum mekaniği kullanılarak ***mertebe***/***periyot-bulma*** işlemi yerine getirilmektedir.

Shor algoritması belirli bir olasılık dahilinde periyodu bulur. Algoritma özetle aşağıdaki gibidir [42]:

SHOR ALGORİTMASI:

Klasik kısım: *N*'nin asal çarpanları

1. Rasgele bir $a < N$ sayısı üretilir.
2. *OBEB*(a, N) hesaplanır[4]. Eğer, *OBEB*(a, N) $\neq 1$ ise a, N'nin bir asal çarpanıdır. Durulur.
3. $N^2 \le Q = 2^m \le 2N^2$ olan bir Q belirleyip $f(x) = a^x \bmod N$ fonksiyonunun r periyodunu [5] bulmak üzere *kuantum kısım*a geçilir ve aşağıda verilen *kuantum periyot-bulma altyordamı* çalıştırılır.
4. Eğer bulunan r tek ise, ***1. adım***a dönülür.
5. Eğer $a^{r/2} \equiv -1 \pmod N$ ise, ***1. adım***a dönülür.
6. *OBEB*($a^{r/2} \pm 1$, N) değeri, N'nin asal çarpanıdır. Durulur.

Kuantum kısım: Periyot-bulma altyordamı

Adım 1. (Kuantum) Saklayıcılar ilklendirilir: $Q^{-1/2}\sum_{x=0}^{Q-1}|x,0\rangle$. İlk yarıda (giriş), tüm olası x değerlerinin bir listesi yer almaktadır. m kübitlik olan giriş (gerekli kübit sayısı $\lceil \log_2 2^m \rceil$ ile hesaplanır, $0 \le x < Q$), $Q = 2^m$ durumun bir süperpozisyonunda olup 0'dan $(Q-1)$'e kadar tüm değerleri içerir. $m/2$ kübitlik olan çıkış (kübit sayısı $\lceil \log_2 N \rceil$ ile hesaplanabilir, $0 \le r < N-1$) saklayıcısı (ikinci yarı) ise henüz hep 0'dır. Ayrıca, giriş ve çıkış saklayıcıları dolaşıktır.

Adım 2. $f(x)$, kuantum bir fonksiyon olarak gerçeklenip yukarıdaki kuantum duruma (ilk yarısına) uygulanır: $Q^{-1/2}\sum_x |x, f(x)\rangle$. Son durum, halen tüm olası $Q = 2^m$ durumun bir süperpozisyonudur. İlk yarı, tüm x değerlerinin bir listesini; çıkış ise tüm $a^{|x>} \pmod N$ değerlerinin listesini içerir. Dolayısıyla, şu an itibariyle tüm olası girişler ve çıkışlar saklayıcılardadır.

Adım 3. İkinci yarı üzerinde bir ölçüm yapılır: $\frac{1}{C}\sum_{\substack{0\le x<2^m \\ a^x \equiv u \pmod N}} |x,u\rangle$. ($C$, vektör uzunluğunu 1 yapmak için gereken faktördür; aslında, toplamdaki terimlerin sayısının kareköküdür). Böylesi bir ölçüm, bize bir $u \pmod N$ sayısı verir ve tüm sistemi $|x, u>$ formundaki durumların bir lineer kombinasyonuna zorlar; öyle ki, tüm $a^x \equiv u \pmod N$ durumlarını elde etmiş oluruz.

Adım 4. Giriş saklayıcısına Kuantum Fourier Dönüşümü (QFT: Quantum Fourier Transform) uygulanır: $U_{QFT}|x\rangle = Q^{-1/2}\sum_y w^{xy}|y\rangle$, burada, $w = e^{2\pi i/Q}$, $0 \le y < Q$. QFT, periyodu bulmak için gerekli olan frekansları ölçer. Eğer r değeri 2^m değerinin bir böleni ise, bu durumda elde edeceğimiz frekanslar bir f_0 temel frekansının katları olur ve $rf_0 = 2^m$ sağlanır. Genel olarak, r değeri 2^m değerinin bir böleni değildir. Böylesi durumlarda ise bazı baskın frekanslar olacaktır ve bunlar bir f_0 temel frekansının yaklaşık olarak katları olacaktır; öyle ki, $rf_0 \approx 2^m$. QFT sonucu olan kuantum durum üzerinde ölçüm yapılır ve sonuçta bir $f = j.f_0$ frekansı belirlenir.

Adım 5. r'yi elde etmek için aşağıdaki oran üzerinde sürekli bölmeler açılımı uygulanır[6]:

$$\frac{j \cdot f_0}{r \cdot f_0} \approx \frac{f}{2^m} \Rightarrow \frac{j}{r} \approx \frac{f}{2^m} \qquad (4)$$

ilişkisinden bir r değeri hesaplanır, $r \le Ø(N)$[7] $< N$. Genellikle, bu bölmenin açılımındaki N'den küçük en son payda aranılan r periyodu olmaktadır.

Adım 6. $a^r \equiv 1 \pmod N$ olup olmadığı kontrol edilir? Evet ise, işlem tamam.

Adım 7. Aksi halde, ***altyordam***ın ***1. adım***ına geri dönülür ve işlem tekrarlanır.

Bu algoritmanın kuantum kısmına ilişkin kuantum devreler her bir N ve a için özel olarak tasarlanırlar. Yöntemin doğru çalışmadığı da olmaktadır, bu durumda algoritma yeniden tasarlanır ve baştan çalıştırılır.

Konularla ilgili daha detaylı bilgi için [43-54]'teki kaynaklardan da faydalanılabilir.

7. Sonuçlar

Kuantum mekaniği ve bilgi teorisi 20. yüzyılın dünyayı kavrayışımızı değiştiren en önemli buluşlarından ikisidir. Şimdi bilim insanları bu ikisini bir şekilde birleştirmenin çabası içindeler ve büyük ölçüde de başarmışlardır.

Kriptograflarla kriptanalistler arasında asırlardan beridir devam etmekte olan mücadele bundan sonra da kuantum

---

[1] Bugün bazı açık anahtarlı kriptosistemlerin güvenliği bu problemin çözülmesinin zorluğuna dayanmaktadır.

[2] Shor'un algoritması ilk olarak 2001 yılında IBM'de ilk 7-kübitlik kuantum bilgisayar üzerinde çalıştırılmış ve 15 sayısını asal çarpanlarına ayırmıştır. Eğer büyük ölçekli bir kuantum bilgisayar yapılırsa bunun kriptografide önemli etkileri olacaktır.

[3] ***Order-finding***: mertebe bulma, ***period-finding***: periyot bulma.

[4] Bu hesaplama ***Öklid algoritması*** ile çok kolayca yapılabilir.

[5] $(Z_N)^x$ grubunda (tamsayılar mod N'nin çarpımsal grubu), a elemanının mertebesi, $f(x + r) = f(x)$ koşulunu sağlayan en küçük r tamsayısıdır. Grup, cebirsel yapılardan biridir.

[6] ***Frekans***, ***uzunluğun periyoda bölümü*** olup dizinin kaç kere tekrar ettiğini ifade eden matematiksel bir terimdir: $f\,(frekans) = \frac{L\,(uzunluk)}{T\,(periyot)}$. Dolayısıyla, ***uzunluğu*** belli olan bir dizinin ***frekansı*** bulunabilirse ***periyodu*** da çok rahatlıkla bulunabilir.

[7] Euler'in Ø-fonksiyonu. p, q asal ve $N = p \cdot q$ ise $Ø(N) = (p-1)\cdot(q-1)$.

dünyada devam edecek gibi görünmektedir. İlk büyük-ölçekli kuantum bilgisayarın henüz yıllarca uzakta olmasına ve olabilirliğinden birçoklarının şüpheli olmasına rağmen, KRSÜ (*gizli anahtar üretimi* için) ve kuantum kriptografi (*anahtar dağıtımı* için) şimdiden ticari ürünler haline bile geldi. Kuantum kriptocular, 150 km'den daha uzak bir mesafe için güvenli mesajlar iletmeyi başardı. Bununla birlikte, çok az sayıda kübiti idare edebilen ilk kuantum bilgisayarlar da yapıldı ve 15'i asal çarpanlarına ayırabildi. Daha büyüklerini yapabilmek için çalışmalar hızlı bir şekilde sürmektedir.

Ulusal güvenlik açısından en önemli konulardan biri de ***ulusal bilgi***lerin güvenliğidir. Ve ulusal güvenliğin en büyük gereklerinden birisi de ***dışa bağımlılık***tan kurtulmaktır. Çağın ve yaşanmakta olan bilimsel-teknolojik gelişmelerin gerisinde kalmamak için acilen kuantum teknolojileri (*KRSÜ*, *kuantum kriptografi*, *kuantum kriptanaliz*, *kuantum bilgisayar*, *kuantım haberleşme*, vb.) üzerinde çalışmalar yapacak bir ***Ulusal Kuantum Teknolojileri Araştırma (Geliştirme ve Test) Merkezi*** (UKTAM) kurulması çalışmalarına başlanması çağrımızı [55] burada da tekrarlamak istiyoruz[1].

8. Kaynakça

[1] Çeşmeci, M. Ü., "Kriptoloji Tarihi", UEKAE Dergisi, Sayı 1, s21-31, http://www.uekae.tubitak.gov.tr. Erişim: Haziran 2011.
[2] Steganography, http://en.wikipedia.org/, Wikipedia The Free Encyclopedia. Erişim: Haziran 2011.
[3] Cryptography, http://en.wikipedia.org/.
[4] Boyacı, U. K., "Günümüzde Kriptoloji", UEKAE Dergisi, Sayı 1, s32-41, http://www.uekae.tubitak.gov.tr.
[5] Kerckhoffs, A., "La cryptographie militaire", *Journal des sciences militaires*, vol. IX, pp. 5–83, Jan. 1883, pp. 161–191, Feb. 1883.
[6] Auguste Kerckhoffs, http://en.wikipedia.org/.
[7] Claude Shannon, http://en.wikipedia.org/.
[8] Dereli, T., Verçin, A., *Kuantum Mekaniği Temel Kavramlar ve Uygulamaları*, Ciltli, Tübа Yayınları, Ağustos 2009.
[9] Quantum mechanics, http://en.wikipedia.org/.
[10] Classical mechanics, http://en.wikipedia.org/.
[11] Geçkinli, C. N., "Rasgelelik (Rastlantısallık) Kavramına Genel Bir Bakış", UEKAE Dergisi, Sayı 1, s96-103, http://www.uekae.tubitak.gov.tr.
[12] QUANTIS, True RANDOM NUMBER Generator Exploiting QUANTUM PHYSICS, http://www.idquantique.com/. Erişim: Haziran 2011.
[13] Pseudorandom number generator, http://en.wikipedia.org/.
[14] Hardware random number generator, http://en.wikipedia.org/.
[15] Quantum Noise Breaks Random Number Generator Record, http://www.technologyreview.com/blog/arxiv/25355/, Erişim: Haziran 2011.
[16] Cryptanalysis, http://en.wikipedia.org/.
[17] Shannon, C.E., 1949, "Communication theory of secrecy systems", *Bell System Technical Journal*, 28, 656-715.
[18] Vernam, G., 1926, "Cipher printing telegraph systems for secret wire and radio telegraphic communications", *J. Am. Institute of Electrical Engineers*, Vol. XLV, 109-115.
[19] Rivest, R.L., Shamir A. and Adleman L.M., 1978, "A Method of Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, 21, 120-126.
[20] Schneier, B., *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 2nd Edition, John Wiley & Sons. Inc, 1996.
[21] Kalem, Ş., "Kuantum Bilgi Güvenliğine Doğru", UEKAE Dergisi, Sayı 1, s42-47, http://www.uekae.tubitak.gov.tr.
[22] Quantum cryptography, http://en.wikipedia.org/.
[23] Quantum key distribution, http://en.wikipedia.org/.
[24] Post-quantum cryptography, http://en.wikipedia.org/.
[25] Bernstein, D. J., Buchmann J., Dahmen, E., *Post-Quantum Cryptography*, 1 edition, Springer, November 17, 2008.
[26] Raw Key Exchange, http://swissquantum.idquantique.com/?Raw-Key-Exchange, SwissQuantum, Erişim: Haziran 2011.
[27] Key Sifting, http://swissquantum.idquantique.com/?Key-Sifting.
[28] CLAVIS2, QUANTUM KEY DISTRIBUTION FOR R&D APPLICATIONS; CERBERIS, A fast and secure solution: high speed encryption combined with quantum key distribution, http://www.idquantique.com/.
[29] Bennet, C. H., Brassard, G., "Quantum Cryptography: Public Key Distribution and Coin Tossing", *Proc. Int'l Conf. Computers, Systems & Signal Processing*, CS Press, 1984, pp. 175–179.
[30] Quantum Key Distribution Protocols, http://swissquantum.idquantique.com/?Quantum-Key-Distribution-Protocols.
[31] Stebila, D., Mosca, M., Lütkenhaus, N., "The Case for Quantum Key Distribution", *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, volume 36, page 283--296. Springer, 2010. DOI: 10.1007/978-3-642-11731-2_35.
[32] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., 2002, "Quantum Cryptography", 57 pages, 32 figures, submitted to *Reviews of Modern Physics*, quant-ph/0101098. DOI: 10.1103/RevModPhys.74.145.
[33] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dusek, M., Lutkenhaus, N., Peev, M., 2009, "The Security of Practical Quantum Key Distribution", 50 pages, 9 figures, submitted to *Reviews of Modern Physics*, arXiv:0802.4155. DOI: 10.1103/RevModPhys.81.1301.
[34] Quantum Cryptoanalysis, http://www.qubit.org/. Erişim: Haziran 2011.
[35] Shor, P. W., 1994, "Algoritms for quantum computation: discrete logarithms and factoring", *Proceedings of the 35th Symposium on Foundations of Computer Science*, Los Alamitos, edited by Shafi Goldwasser (IEEE Computer Society Press), 124-134.
[36] Richard Feynman, http://en.wikipedia.org/.
[37] David Deutsch, http://en.wikipedia.org/.
[38] Grover, L. K., 1996, "A fast quantum mechanical algorithm for database search", *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, STOC'96 (ACM, New York), p. 212.
[39] Quantum computer, http://en.wikipedia.org/.
[40] Qubit, http://en.wikipedia.org/.
[41] Integrated quantum computing system with 128 qubit chipset, http://www.dwavesys.com/, D-Wave, Erişim: Haziran 2011.
[42] Shor's algorithm, http://en.wikipedia.org/.
[43] Elliott, C., "Quantum cryptography", *Security & Privacy Magazine*, IEEE, Vol. 2, Issue: 4, July-Aug. 2004, sf. 57–61.
[44] Mullins, J., 2002, "Making unbreakable code", *Spectrum*, IEEE, Volume: 39, Issue: 5, sf 40–45.
[45] Nielsen, M. A., Chuang, I. L., *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
[46] Williams, C. P., Clearwater, S. H., *Explorations in QUANTUM COMPUTING*, Springer-Verlag NewYork, Inc. TELOS,1998.
[47] Trappe, W., Washington, L. C., *Introduction to Cryptography with Coding Theory*, Prentice-Hall, Inc. 2002.
[48] http://www.biltek.tubitak.gov.tr/
[49] http://www.quantum-computer.com/
[50] http://ww.magiqtech.com.
[51] http://www.quantiki.org/.
[52] http://www.random.org/.
[53] http://www.qubit.org/.
[54] http://arxiv.org/.
[55] Toyran, M., "EEB Mühendisliklerinde Kuantum Hesaplama Eğitimi", *3. EEB Mühendislikleri Eğitimi Sempozyumu*, 2006.

[1] Böylece, ülkemizin örneğin klasik kriptolojide elde ettiği ***bağımsızlık*** ve ülke dışına yayılan ***başarı***sı kuantum kriptolojide de tekrarlanabilir.