Dr. Mahir E. Oca

TÜBİTAK Bilim ve Teknik Dergisi

Kuantum Kriptografi

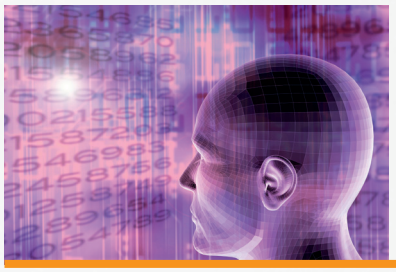
Kriptografi genel olarak bir mesajı yetkisiz insanların anlayamayacağı biçime getirme sanatı olarak adlandırılabilir. Daha geniş bir alan olan kriptoloji ise kriptografinin yanı sıra şifrelenmiş metinleri çözme sanatı olan kriptoanalizi de içine alır. İnternetin hayatımızda gün geçtikçe daha çok yer ettiği günümüzde, kriptografi de giderek daha fazla önem kazanıyor.

Şifrelemenin, ideal olarak, şifrenin nasıl çözüleceğini bilmeyen biri tarafından asla çözülemeyecek biçimde yapılması istenebilir. Fakat klasik kriptografi yöntemleri ile bu mümkün değildir. İnternet ortamında şifreleme amacıyla kullanılan klasik yöntemlerin tamamı, şifre kırmanın "imkânsızlığına" değil "zorluğuna" dayanır. Başka bir deyişle yeterince uzun süre uğraşarak şifrelenmiş tüm metinleri çözmek mümkündür. Fakat bu süre genel olarak çözme işlemi bittiğinde metnin içeriğinin hiçbir değer taşımayacağı kadar uzundur.

Uygulamada karşılaşılacak zorluklar göz ardı edilirse, kuantum mekaniğine özgü ölçüm sonuçlarının olasılığa dayalı olması, kırılması imkânsız bir biçimde şifrelenmiş metinler hazırlanmasına imkân verebilir. Üstelik bunun nasıl gerçekleşebileceğini anlamak için kuantum mekaniği ile ilgili birkaç temel bilgiden daha fazlası gerekmiyor.

>>>

Klasik Kriptografi



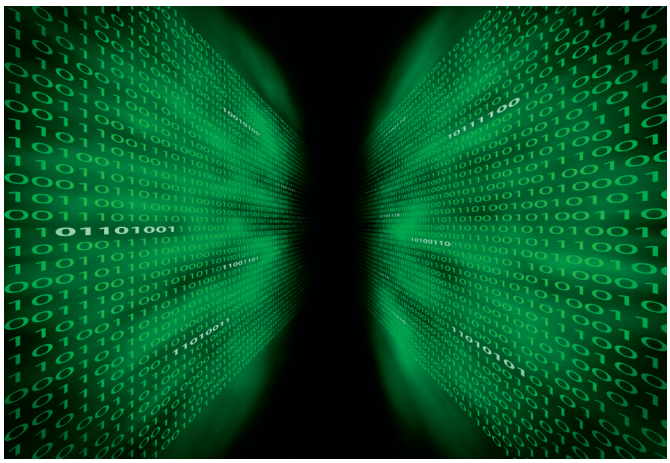
Şifreleme sürecinde "kriptosistem" ya da "şifre" adı verilen bir algoritma kullanılır. Önce gönderilecek mesaj "anahtar" adı verilen bir ek bilgiyle birleştirilir ve "kriptogram" adı verilen yeni bir metin oluşturulur. Kriptolama olarak adlandırılan bu süreçten sonra şifrelenmiş metin alıcıya gönderilir. Alıcı ise yine bir anahtar kullanarak şifrelenmiş mesajı çözer. Klasik kriptografide kullanılan yöntemler, göndericinin ve alıcının kullandıkları anahtarlara göre ikiye ayrılır: Ya tek bir anahtar ya da farklı anahtarlar kullanılır.

Asimetrik Sistemler

Göndericinin ve alıcının farklı anahtarlar kullandığı kriptosistemlere, asimetrik veya açık anahtarlı sistemler denir. Bu sistemlerin dayandığı temel ilke, Stanford Üniversitesi araştırmacıları Whitfield Diffie ve Martin Hellman tarafından 1976'da önerilmiş. İlk pratik uygulama ise 1978'de Massachusetts Institute of Technology (MIT) araştırmacıları Ronald Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiş. RSA olarak adlandırılan bu algoritma hâlâ yaygın olarak kullanılır. Özellikle internet üzerinden aktarılan verilerin güvenliği kısmen de olsa asimetrik kriptosistemlerle sağlanır.

Asimetrik sistemlerde alıcı önce kendisi için bir "gizli anahtar" seçer ve bu gizli anahtardan bir "açık anahtar" üretir. Alıcıya mesaj göndermek isteyen herhangi birisine bu açık anahtar verilir. Sistemin güvenliğini sağlayan şey, açık anahtar kullanılarak üretilmiş şifreli metinlerin gizli anahtar olmadan çözülmesinin çok zor olmasıdır. Örneğin RSA yöntemi büyük tam sayıları asal çarpanlarına ayırmanın zorluğuna dayanır. Algoritmanın dayandığı temel düşünceyi şöyle örneklendirebiliriz. İki asal sayıyı çarpmak -örneğin 17'yi ve 19'u çarparak 323 sayısını bulmak- gayet kolay bir işlemdir.

Fakat bu işlemin tersi yani 323 sayısını alıp bu sayının asal çarpanları olan 17'yi ve 19'u bulmak daha zordur. RSA algoritmasını kullanan bir alıcı kendine iki asal sayıdan oluşan bir gizli anahtar belirler ve bu sayıların çarpımını kendisine mesaj gönderecek olan kişilere açık anahtar olarak verir. Bu açık anahtar kullanılarak şifrelenmiş mesajları ise kendine sakladığı gizli anahtarı kullanarak çözer. Daha önce de belirtildiği gibi bu algoritmanın güvenliği şifreyi kırmanın imkânsızlığına değil zorluğuna dayanır. Örneğin iki yüzer basamaklı iki asal sayıdan oluşan gizli bir anahtar kullanan alıcı şifrelenmiş bir metni bir saniyeden kısa bir sürede çözebilir. Sadece bu sayıların çarpımı olan açık anahtarı bilen birisinin ise bu açık anahtarı çarpanlarına ayırarak gizli anahtarı bulması günümüzün en gelişmiş bilgisayarlarıyla bile yıllar sürer. Fakat imkânsız değildir. Hatta ileride geliştirilebilecek kuantum bilgisayarlar ile klasik bilgisayarların çözmekte zorlandığı pek çok problemin kolayca çözülebileceği düşünülüyor.



Simetrik Sistemler

Simetrik kriptosistemlerde -yani gizli anahtarlı kripto sistemlerde- hem şifreleme hem de şifre çözme için aynı anahtar kullanılır. Örneğin 1926 yılında AT&T Laboratuvarları'nda çalışan Gilbert Vernam tarafından öne sürülen "tek kullanımlık şifre" algoritması bu sınıfa girer. Bu yöntemde gönderici mesajla aynı uzunlukta bir anahtar belirler ve mesajdaki tüm bitleri anahtarın bitleri ile toplar. Alıcı ise yine aynı anahtarı kullanarak gelen mesajdaki bitlerden anahtardaki bitleri çıkarır ve çözülmüş metni elde eder. Bu algoritma bugüne kadar tamamen güvenli olduğu ispatlanmış tek algoritmadır. Fakat kuramsal olarak mükemmel olmasına rağmen, uygulaması zordur. Örneğin şifreleme için kullanılan anahtarın gönderici ve alıcı arasında güvenli bir yolla -mesela güvenilen bir kurye ile ya da hatta gönderici ve alıcının bir araya gelmesiyle- aktarılması gerekir. Fakat bu her zaman mümkün olmayabilir veya mümkün olsa bile süreç çok karmaşık ya da pahalı olabilir. Ayrıca bu sistemin tam güvenli olması için gizli anahtarın sadece bir kez kullanılması esastır. Aksi takdirde gönderilen şifreli mesajları dinleyen birisi, mesajları karşılaştırarak anahtarı ve dolayısıyla şifrelenmiş metinleri çözebilir.

Asimetrik kriptosistemler yavaş oldukları için pratik uygulamalar sırasında tercih edilmez. Bunun yerine, önce kullanılması planlanan simetrik anahtar, asimetrik şifreleme yapılarak gönderilir. Daha sonra simetrik anahtar kullanılarak mesaj şifrelenir. Dolayısıyla bu yöntemlerin güvenliği de asimetrik kriptosistemleri kırmanın zorluğuna dayanır. Eğer asimetrik sistemleri kırmanın kolay bir yolu -örneğin kuantum bilgisayarlar kullanarak- bulunabilirse klasik kriptografi tamamen çöker. Fakat kuantum kriptografi kullanılarak şifre dağıtımı yapılması kuramsal olarak tamamen güvenlidir.

Kuantum Kriptografi

Sonuçları olasılığa dayalı olduğu için, kuantum mekaniğine özgü ölçümler kriptosistemler geliştirilmesine uygundur. Örneğin ölçüm yapılacak özellikle ilgili operatörün iki özdurumu olsun (|a>, |b>). Bir parçacık ölçüm yapılmadan önce bu iki durumun herhangi bir lineer kombinasyonunda ($c_1|a> + c_2 |b>$) bulunabilir. Ölçüm yapıldığı zaman parçacığın $|c_1|^2$ ihtimalle |a> durumunda, $|c_2|^2$ ihtimalle de |b> durumunda olduğu bulunacaktır. Mesela c_1=0,6 ve c_2=0,8 ise 0,36 ihtimalle parçacığın |a> durumunda, 0,64 ihtimalle de |b> durumunda olduğu bulunur. Başka bir deyişle 100 özdeş parçacık üzerinde aynı ölçüm yapılırsa 36 tanesi |a> durumunda, 64 tanesi |b> durumunda çıkacaktır. Daha ilginç olan ise, parçacığın ölçümden sonra hangi durumda olduğu bulunursa o duruma "çökmesidir". Yani ölçümden önce $c_1|a> + c_2 |b>$ durumunda olan parçacık, ölçümden sonra ya |a> ya da |b> durumunda olacaktır. Dolayısıyla sisteme etkide bulunmadan kuantum mekaniğine özgü bir ölçüm yapılamaz. Bu durum şifrelenmiş bilgileri dinlemeye çalışan birisi olup olmadığının kolayca belirlenmesine yardımcı olur. Eğer veri transferi sırasında sisteme herhangi bir müdahalede bulunulmuşsa, bu bir dinleyici olduğuna işaret eder. Önce gönderici alıcıya anlamsız bir veri gönderir, daha sonra gönderici ve alıcı ellerindeki verileri açıkça karşılaştırır. Veriler arasında makul olmayan bir uyumsuzluk varsa, sisteme müdahale edilmiş yani "konuşma" dinlenmiş demektir. Bu durumda gönderici alıcıya anlamlı herhangi bir veri göndermeden iletişim sonlanır. Böylece gizli bilgilerin istenmeyen kişilerin eline geçmesi engellenir.

BB84 Protokolü

Kuantum kriptografinin pratik uygulamaları ile ilgili ilk protokol Charles H. Bennett ve Gilles Brassard tarafından 1984'te geliştirildi. BB84 adıyla anılan bu protokol, kuantum kriptografi araştırmaları için hâlâ yaygın olarak kullanılıyor.

	|↑>	|↓>	|→>	|←>
|↑>	1	0	0,5	0,5
|↓>	0	1	0,5	0,5
|→>	0,5	0,5	1	0
|←>	0,5	0,5	0	1

BB84 protokolünün mantığını spini ½ olan parçacıklar ile örneklendirebiliriz. Bilindiği gibi böyle bir parçacığın spini hangi yönde ölçülürse ölçülsün sonuç ya +½ ya da -½ olacaktır. Bu protokolü uygularken farklı iki yön (baz) yani farklı dört durum kullanılır ve farklı bazlar arasındaki örtüşme maksimum yapılır. Yani eğer bir bazdaki iki durumu |↑> ve |↓>, diğer bazdaki iki durumu |→> ve |←> olarak gösterirsek |→> = (|↑> + |↓>)/√2 ve |←> = (|↑> - |↓>)/√2 olarak seçilir. Bu dört durumdan |↑> ve |→> değeri "1" olan bitleri, |↓> ve |←> ise değeri "0" olan bitleri kodlamak için kullanılabilir.

Charles H. Bennett

Gilles Brassard

Uygulama sırasında, şifreleme için kullanılacak bir anahtar elde etmek için gönderici farklı iki bazdan herhangi birinde hazırlanmış bir kübiti (kuantum biti) alıcıya gönderir. Fakat bilginin hangi bazda hazırlandığını gizli tutar. Alıcı ise bazlardan birini seçer ve ölçüm yapar. Göndericinin ve alıcının hangi bazları seçtiğine göre olası sonuçlar aşağıdaki tabloda özetlendiği gibidir. Örneğin |↑>, |↓> bazını seçen bir gönderici değeri 1 olan bir kübiti kodlamak için |↑> durumunda bir foton hazırlar ve alıcıya gönderir. Eğer alıcı ölçümü aynı bazda yaparsa fotonun |↑> durumunda olduğunu, yani kübitin değerinin 1 olduğunu bulacaktır. Fakat eğer alıcı |→>, |←> bazını seçerse 0,5 ihtimalle fotonun |→> durumunda olduğunu -yani kübitin değerinin 1 olduğunu- 0,5 ihtimalle de fotonun |←> durumunda olduğunu -yani kübitin değerinin 0 olduğunu- bulacaktır.

Özet olarak gönderici ve alıcı aynı bazı kullanırsa sonuçlar tamamen uyumlu olur. Farklı bazları kullanırlarsa alıcının elde ettiği ölçüm sonuçlarının yarısı gönderilen bilgiyle uyumsuz olacaktır. Alıcının %50 ihtimalle doğru bazı seçeceği düşünülürse, veri aktarımı sonunda göndericinin ve alıcının elindeki bitler arasındaki uyumsuzluk %25 olacaktır. Veri aktarımı tamamlandıktan sonra gönderici ve alıcı aynı anahtara sahip olabilmek için kullandıkları bazları -kübitlerin değerini değil- açıklar. Eğer aynı bazları kullanmışlarsa verileri saklarlar, farklı bazları kullanmışlarsa verileri silerler. Bu süreç sonunda aktarılan verilerin yarısı silinecektir. Aktarılan "ham anahtar"dan geriye kalana "elenmiş anahtar" denir. Eğer veri aktarımı sırasında herhangi bir dış müdahale olmamışsa, göndericinin ve alıcının elindeki elenmiş anahtarlar aynı olacaktır. Burada ilginç olan nokta ne göndericinin ne de alıcının anahtarı belirleyebilmesidir. Anahtar, göndericinin ve alıcının rastgele tercihlerine göre, işlem sırasında belirlenir.

Bu protokol ile çalışan bir kripto sistemi dinlemeye çalışan birisinin yapması gereken şey ölçüm yaparak göndericiden alıcıya giden bitlerin değerini bulmaktır. Fakat ideal olarak her kübit tek bir foton ile gönderilmelidir. Öyleyse dinleyici ölçüm yaparsa alıcıya hiçbir şey ulaşmaz. Gönderilen sadece şifreleme için kullanılacak anahtar olduğu için dinleyen kişinin elde ettiği bilgilerin tamamı anlamsızdır. Eğer dinleyici anahtar oluşturulduktan sonra gönderilecek şifreli mesajları elde etmek istiyorsa, göndericinin ve alıcının bir anahtar oluşturmasına izin vermelidir. Dolayısıyla dinleyicinin yapması gereken şey, anahtar oluşturulması sırasında, önce göndericiden gelen veriler üzerinde ölçüm yapmak, daha sonra elde ettiği sonuçlara uygun verileri alıcıya göndermektir. Fakat dinleyici sadece kübitlerin hangi bazda hazırlandığını bilirse mükemmel bir kopya elde edebilir. Gönderici ise bu bilgiyi alıcı kübit üzerinde ölçüm yapana kadar gizli tutmaktadır. Dolayısıyla dinleyici anahtarın mükemmel bir kopyasını yapamaz.

Araya Gir, Yeniden Gönder Taktiği

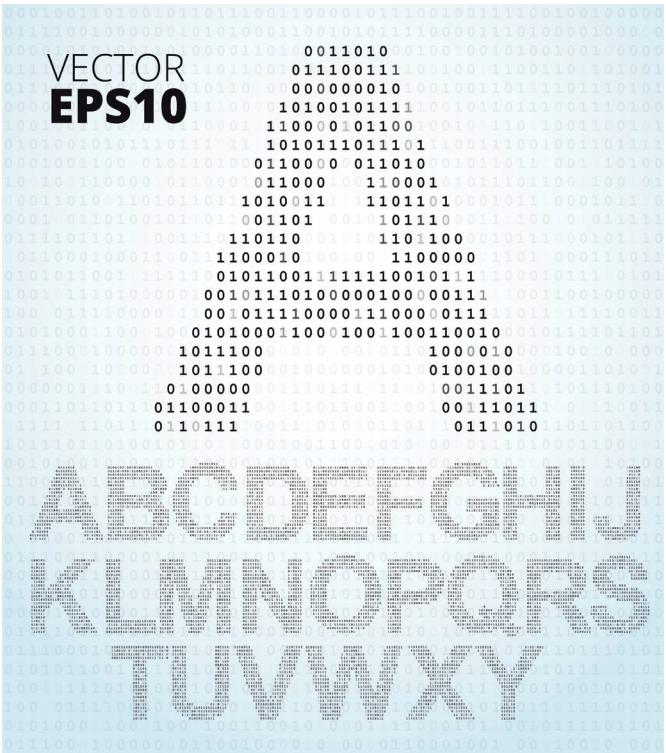
Gizli bilgileri ele geçirmeye çalışan birisinin önce araya girip daha sonra alıcıya elde ettiği sonuçlara uygun bilgiler gönderdiği durumda neler olacağına bir göz atalım. Eğer dinleyici doğru bazı kullanırsa, alıcının kübite yüklediği bilgiyi doğru olarak öğrenecek ve bu doğru bilgiyi alıcıya da gönderecektir. Fakat dinleyicinin binlerce kübitten oluşan bir anahtardaki tüm bitleri şans eseri doğru bazda ölçmesi neredeyse imkânsızdır.

Dinleyici, yanlış bazı kullandığı durumlarda yaptığı ölçümlerin yarısında doğru sonucu, yarısında yanlış sonucu elde edecektir. Dinleyici elde ettiği sonuçlara uygun kübitleri alıcıya göndereceği için, elde edilen yanlış sonuçlar alıcının elde ettiği elenmiş anahtara da yansıyacaktır. Basit bir olasılık hesabı, tüm kübitler ölçülüp yeniden gönderildiği zaman dinleyicinin elde edeceği doğru bilgi oranının %50, elenmiş anahtardaki hata oranınınsa %25 olacağını gösterir.

Hataların Düzeltilmesi ve Güvenliğin Artırılması

Bilgi aktarımı sırasında hiç bir dış müdahale olmasa bile teknik donanımlar mükemmel olmadığı için gönderilen bilgi ile alınan bilgi arasında farklar olabilir. Teknik yetersizliklerden kaynaklanan hata oranı modern optik iletişim cihazları için 10^{-2} ölçeğindedir ve standart hata düzeltme algoritmalarıyla 10^{-9}'a kadar düşürülebilir. Dolayısıyla bir dinleyicinin araya girmesi durumunda oluşabilecek %25'lik hata oranı çok yüksektir. Bu sebeple gönderici ve alıcı elenmiş anahtardaki hata oranına bakarak bir dinleyicinin varlığını belirleyebilir. Gönderici ve alıcı önce elenmiş anahtarın rastgele seçilmiş bir kısmını karşılaştırır ve anahtarın bu kısmındaki hata oranını belirler. Eğer hata oranı yüksek çıkarsa bir dinleyici olduğu belirlenmiş olur ve iletişim sonlandırılır. Eğer hata oranı düşükse karşılaştırılan kısımlar atılır ve daha sonra yapılacak olan gizli iletişimde şifreleme için kullanılacak olan elenmiş anahtarın geri kalan kısmındaki hatalar düzeltilir.

Tüm kübitleri dinlemesi durumunda varlığının belli olacağını bilen bir dinleyici, kübitlerin sadece bir kısmını dinleyerek varlığını gizlemeye ve böylece anahtarın tamamını olmasa bile bir kısmını öğrenmeye çalışabilir. Örneğin dinleyici kübitlerin sadece %10'una müdahale ederse, gönderici ve dinleyici anahtarda meydana gelecek %2,5'lik hata oranının teknik imkânsızlıklardan kaynaklandığını düşünebilir. Bu yüzden hata oranı düşük bile olsa, klasik protokoller kullanılarak güvenliğin artırılması gerekir.



Güvenliği artırmak için kullanılan algoritmalardan biri kübitlerin XOR değerinin hesaplanması esasına dayanır. İki kübitin XOR değeri bu kübitlerin değerlerinin toplamının ikiye bölünmesinden kalandır (0⊕0 =0, 1⊕0 =1, 0⊕1 = 1, 1⊕1 = 0). Gönderici ve alıcı, güvenliği artırmak için rastgele iki kübit seçer ve bu kübitler anahtardan silinip kübitlerin XOR değeri anahtara eklenir. Böylece anahtara yeni hatalar eklenmeden güvenlik artırılır. Örneğin dinleyicinin seçilen kübitleri 0,7 olasılıkla doğru bildiğini varsayalım. Protokol uygulandıktan sonra dinleyicinin kübitlerin XOR değerini doğru bilme olasılığı 0,58'e düşer. Olasılığın neden 0,7*0,7=0,49'a düşmediğini merak eden okuyucularımızın, protokolün nasıl çalıştığını daha dikkatli incelemesini öneririz.

BB84 protokolünün güvenli bir biçimde çalışabilmesi için göndericinin ve alıcının kiminle iletişim kurduklarından emin olması gerekir. Tüm iletişim gizli bilgileri ele geçirmeye çalışan yetkisiz birisiyle de yapılıyor olabilir. Dolayısıyla gönderici ile alıcı ilk kez iletişim kurmadan önce birbirlerinin kimliklerini doğrulayacak ortak bir anahtara sahip olmalıdır. Daha sonraki iletişimlerden önce yapılacak kimlik doğrulaması ise bir önceki iletişim sırasında kullanılan ve kuantum kriptografi ile elde edilen anahtarın küçük bir kısmı kullanılarak yapılabilir.

Güvenliğin artırılması ve kimlik doğrulaması için klasik protokoller uygulanması gerekmesinden de anlaşılabileceği gibi, kuantum kriptografi tüm kriptografik amaçlar için tek başına yeterli değildir. Esasen klasik simetrik kriptosistemlerde kullanılacak anahtarların dağıtımı amacıyla kullanıldığı için "kuantum anahtar dağıtımı" ifadesinin daha uygun bir terim olduğu söylenebilir.

Diğer Protokoller

BB84 protokolünün dışında kuantum kriptografi uygulamaları için önerilmiş çok sayıda protokol vardır. Bu protokollerden biri Einstein-Podolsky-Rosen protokolüdür. EPR protokolünde, ortak bir anahtar elde etmek için gönderici alıcıya kübitler göndermez. Bunun yerine ortak bir kaynak tarafından üretilen kübitler hem göndericiye hem de alıcıya gönderilir. BB84 protokolünde olduğu gibi kübitler rastgele seçilen farklı iki bazda hazırlanır ve gönderici ile alıcı kübitlerin hangi bazda hazırlandığını bilmeden ölçüm yapar. Daha sonra kaynak, gönderici ve alıcı kullandıkları bazları açıklar. Eğer hepsi aynı bazı kullanılmışsa kübit tutulur, yoksa silinir. Eğer kübitleri üreten kaynak güvenilirse, bu protokol BB84 protokolü ile denktir.

Geliştirilen diğer kuantum kriptografi protokolleri arasında -BB84 protokolündeki gibi 4 değil- farklı 2 ya da 6 durumun kullanıldığı protokoller sayılabilir. Ayrıca boyutu ikiden daha büyük olan sistemlerin kullanıldığı kriptosistemler de vardır.

Teknolojik Zorluklar

Kuantum kriptografinin güvenliği kübitlerde kodlanan bilginin tek bir foton ile taşınmasına bağlıdır (bu durumun sebebi aşağıda açıklanıyor). Fakat bunun deneysel olarak gerçekleştirilmesi zordur. Pratik uygulamalar sırasında kullanılan zayıf lazer atımlarındaki foton sayısı Poisson istatistiğine uyar. Bunun yanı sıra bilginin fotonlarla taşınması sürecinde de pek çok teknik sorun vardır. Örneğin optik iletişim kanallarında taşınan fotonun çevreden korunması gerekir. Çevrenin fotona yapabileceği herhangi bir etki, kübitteki bilginin kaybolmasına sebep olabilir. Ayrıca kübitlerin tek bir foton ile taşındığı bir sistemin başarılı olabilmesi için verimli foton algılayıcılar olması esastır.

Dinleme

Anahtar oluşturulması sürecinde eğer her şey mükemmel olarak gerçekleştirilebilirse göndericinin ve alıcının elindeki elenmiş anahtarlar aynı olmalıdır. Fakat pratik uygulamalar sırasındaki teknik imkânsızlıklar sebebiyle bu mümkün değildir. Hataların kaynağı gizli bilgilere ulaşmaya çalışan bir dinleyici de olabileceği için hangi hata oranlarının kabul edilebilir olduğunun incelenmesi gerekir.

"Dinleme analizinin" amacı kriptosistemlerin güvenliği için "nihai" ve "pratik" ispatlar bulmaktır. Nihai ispatlar, dinleyicinin tüm teknik imkânlarına rağmen sistemin güvenli olduğunu ispatlamaya çalışır. Pratik ispatlar ise iletişim için kullanılan teknik cihazların özelliklerine odaklanır.

İdeal durum ile gerçek uygulamalar arasında çok büyük farklar vardır. Öncelikle kullanılan cihazlar mükemmel değildir. Örneğin göndericinin ve alıcının aynı bazı kullanması imkânsızdır. Ufak da olsa bir fark her zaman vardır. Ayrıca gerçek bir foton kaynağı -tek bir foton üretmek için tasarlanmış olsa bile- bir seferde hepsi aynı bilgiyi taşıyan birden fazla foton üretebilir. Bu durumda iletişimi dinleyen birisi fotonları sayabilir ve birden fazla foton olduğu durumlarda fotonlardan bir tanesini kendine ayırıp diğerlerinin alıcıya ulaşmasına izin verebilir. Böylece dinleyicinin varlığını belli etmeden iletişimi dinlemesi mümkün olur.

Önemli bir diğer nokta iletişim için kullanılan cihazların doğru çalışıp çalışmadığıdır. Bu amaçla kripto sistemlerin test edilmesi gerekir. Fakat dinlemeye çalışan kişinin cihazların üreticisi bile olabileceği düşünülürse, bu pek kolay değildir. Müşteriler kriptosistemlerde kullanılacak cihazlarla birlikte güven de satın alır ve bu güvenin ölçülmesi zordur.

Son olarak kriptosistemin güvenliği analiz edilirken gönderici ve alıcının dinleyiciden yalıtılmış olduğu varsayılır. Fakat bu varsayım her zaman doğru olmayabilir. Örneğin dinleyici göndericinin iletişim kurduğu kanalı kullanarak göndericinin bulunduğu ortama ışık gönderebilir. İdeal durumda, göndericiyi dışarıya bağlayan kanaldan içeriye ışık girmesini engelleyen filtreler olmalıdır. Ancak böyle filtreler olsa bile verimleri her zaman sınırlıdır.

Sonuç

Sonuç olarak, kuantum kriptografinin ideal bir uygulamasının mükemmele yakın bir güvenlik sağlayabileceği söylenebilir. Fakat kusursuz bir uygulamanın yapılabileceğini düşünmek gerçekçi değildir. Soyut matematiksel düşüncelerin, teknolojik cihazlar ile ne derece uygulanabileceği ya da uygulandığı her zaman sorgulanacaktır. Yine de kuantum kriptografinin klasik sistemlere göre çok önemli üstünlükleri vardır.

Öncelikli olarak klasik kriptosistemlerde olduğunun aksine, kuantum kriptosistemleri kırmak için yöntem bulunması daha zordur. Örneğin açık anahtarlı kripto sistemleri çözmek için bir algoritma geliştirilebilirse, sistem anında çöker. Kuantum kriptosistemleri çökertmek için kısa bir sürede bir yöntem geliştirmek ise imkânsızdır. Böyle bir yöntem bulunması için geliştirilmesi gereken şey, kuram değil teknolojidir. Teknolojik gelişmelerin geleceğini tahmin etmek matematiksel gelişmeler göre çok daha kolaydır. Bunun yanı sıra kuantum kriptosistemlerin çökertilebilmesi, dinleyicinin "anahtar oluşturulması sırasında" sahip olduğu teknolojik düzeye bağlıdır. Klasik sistemlerde olduğu gibi anahtar değişimi sırasındaki bilgilerin kaydedilip şifrenin daha sonra kırılması mümkün değildir.

Kaynaklar

- Gisin, N. ve ark., "Quantum Cryptography", *Reviews of Modern Physics*, Cilt 74, Sayı 1, s. 145-195, 2002.
- Dereli, T., "İletişimde Mutlak Güvenlik İçin Kuantum Kriptografi", *TÜBİTAK Bilim ve Teknik*, Sayı 500, s. 54, Temmuz 2009.
- Kara, O., "Kriptograik Algoritmalar ve Protokoller", *TÜBİTAK Bilim ve Teknik*, Sayı 500, s. 34, Temmuz 2009..