

KUANTUM KRİPTOGRAFI

Kriptoloji, kriptosistem ya da şifre adı verilen bir algoritma kullanılarak bir mesajın sadece anahtar olarak bilinen ek bilgilerle birleştirilip okunmasının sağlanması bilimidir. Bir kriptosisteme güvenli denebilmesi için anahtar olmadan kriptogramın kilidini çözmek imkansız olmalıdır.

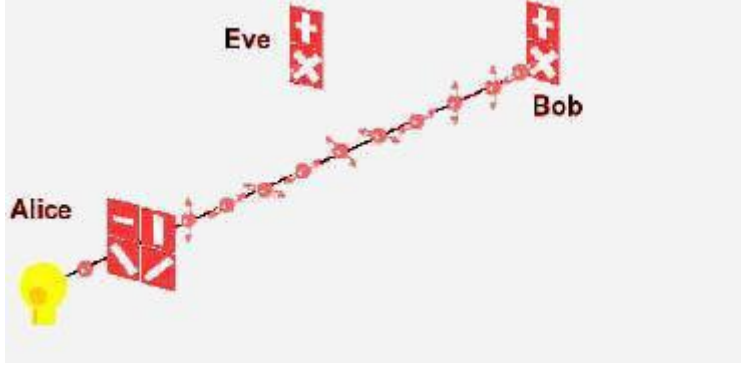
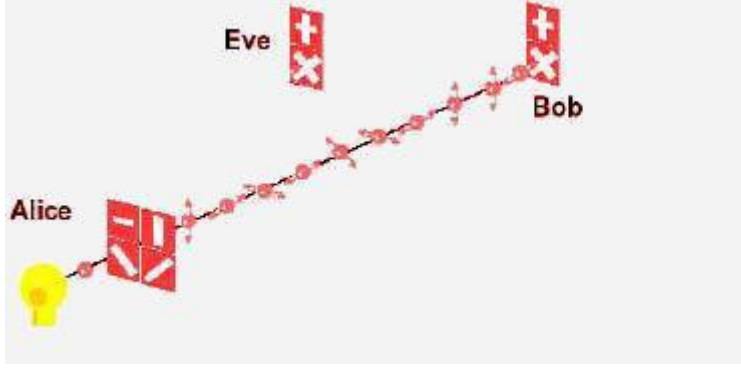
Kriptolojide amaç, bilgiyi sadece gerçek alıcıya ulaşabilecek şekilde iletmektir. Modern şifrelerde anahtar diye çağrılan belirli parametrelerin bir kümesi, düzmetin ile birlikte şifreleme algoritmasına ve şifre metin ile birlikte de şifre çözme algoritmasına giriş olarak uygulanır. Şifreli metnin güvenliği tamamen anahtarın gizliliğine bağlıdır. Şifreleme ve şifre çözme algoritmalarının herkese açıklanmasında herhangi bir mahsur bulunmamaktadır. Anahtar tamamen rasgele seçilen yeterli uzunluktaki bir bit dizisinden oluşur. Anahtar oluşturulduğunda, sonraki iletişim şifreli mesajları herkese açık, kalabalık bir ortamda yapılan bir anons gibi pasif dinlemeye karşı tamamen savunmasız bir kanal üzerinden göndermeyi içerir. Prensipte olarak, herhangi bir klasik anahtar dağıtımını meşru kullanıcılar gizlice dinlediklerinin farkına varmaksızın her zaman pasif olarak dinlenebilir.

Kuantum kriptografi ya da diğer adıyla kuantum anahtar dağıtımını, güvenlik modelinin anahtar yönü olarak matematiğin aksine daha fazla fiziğe güvenmesi bakımından geleneksel kriptografik sistemlerden farklıdır. Kuantum kriptografi, güvenli iletişimi garanti edebilmek için kuantum mekaniğinin yasalarını kullanır. Haberleşecek iki tarafın, yalnızca kendilerinin bilebileceği rastgele ortak bir bit dizisi üretebilmelerini ve bu bit dizisinin mesajların şifrelenmesinde veya şifrelerinin açılmasında kullanılmasını sağlar. Kuantum kriptografinin önemli bir özelliği, anahtarı ele geçirmeye çalışan üçüncü bir tarafın varlığını, haberleşen iki tarafın tespit edebilmesidir. Bu durum; kuantum fiziğinin, bir kuantum sistemi ölçme sürecinin sistemin bozulmasına neden olduğu ilkesi ile ilintilidir. Anahtarı gizlice dinleyen üçüncü taraf onu bir şekilde ölçmek zorundadır ki bu da sistemde birtakım anormalliklere sebep olur. Eğer gizli dinleme seviyesi belli bir eşik değerinin altındaysa anahtar üretilebilir, aksi takdirde güvenli bir anahtar üretmek mümkün değildir ve iletişim durdurulur.

Varolan üçüncü kişi Eve, bu iletişimde çeşitli hatalara sebep olacaktır, çünkü fotonun polarizasyon türünü bilememektedir. Haberleşen iki kişi hata bitlerini kontrol ederek dinlemeyi test edebilirler. Dinlemeyi durduramamalarına rağmen kendilerini dinleyen Eve tarafından da aldatılamazlar. Aşağıda verilen iki grafik dinleme olması ve dinleme olmaması durumundaki test bitlerini göstermektedirler.

Kuantum kriptografi, yalnızca anahtar üretmek ve bu anahtarı dağıtmak için kullanılır, veri taşınmasında kullanılmaz. Üretilen anahtar daha sonra herhangi bir şifreleme algoritmasında şifreleme ve şifreyi açma için kullanılır.

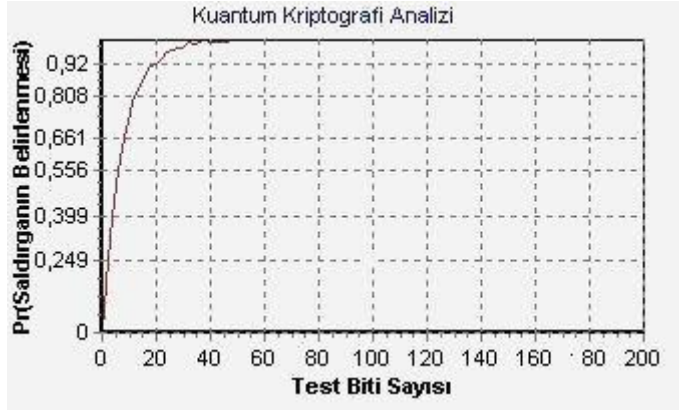
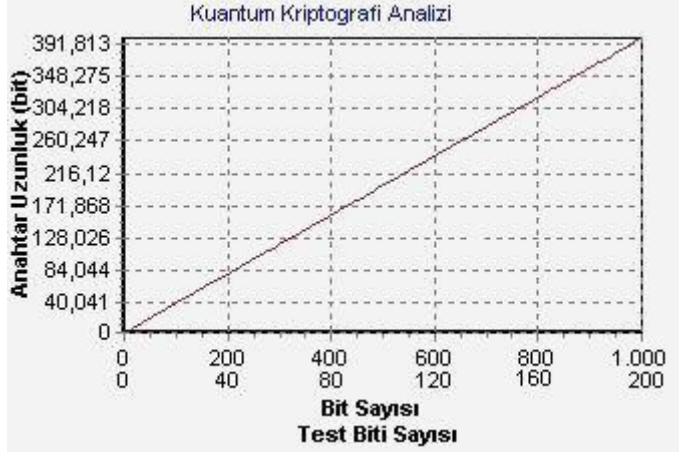
Kuantum Anahtar Dağıtımını



Kuantum kriptografinin bu örneğinde iki kişi gizli haberleşmek istemektedir, üçüncü kişi ise onları gizlice dinlemek. Varolan iki kişi, askeri jetler, on-line ticaretler ya da sadece gizli bir sohbet yapmak isteyen arkadaşlar olabilir. Üçüncü kişinin radyo sinyallerini dinlemesine ya da telefon hatlarına gizli bir bağlantı kurmasına ya da her türlüüne engel olamazlar. Kuantum kriptosistemi şu basit örnekle açıklanabilir. Sistem bir gönderici ve bir alıcı içermektedir. Takma ismi Alice olan birinci kişi, göndericiyi dört polarizasyondan birine sahip fotonlar göndermek için kullanabilir: 0° , 45° , 90° ve 135° . Takma ismi Bob olan ikinci kişi, diğer uçta polarizasyonu ölçmek için alıcıyı kullanır. Kuantum mekaniği yasalarına göre alıcı kenarsal polarizasyonları (0° ve 90°) ayırt edebilir veya köşegensel polarizasyonları (45° ve 135°) ayırt etmek için çabucak yeniden konfigüre edilebilir. Anahtar dağıtımı birkaç adım gerektirmektedir. Alice, fotonları dört polarizasyonun rasgele seçilen birinde gönderir.

Bob, gelen her bir foton için ölçüm türünü rasgele seçer; kenarsal tür veya köşegensel tür. Bob, ölçüm sonuçlarını kaydeder ancak onları gizli tutar. Bob, daha sonra ölçüm türünü (ölçüm sonuçlarını değil) açıklar ve gönderici, alıcıya hangi ölçümlerin doğru türde olduğunu söyler. İki taraf (Alice ve Bob), alıcı ölçümlerinin aynı türde olduğu tüm durumları saklar. Bu durumlar daha sonra bitlere (1'lere ve 0'lara) dönüştürülür ve anahtar elde edilmiş olur.

Varolan üçüncü kişimiz Eve, bu iletişimde çeşitli hatalara sebep olacaktır, çünkü fotonun polarizasyon türünü bilememektedir. Haberleşen iki kişi hata bitlerini kontrol ederek dinlemeyi test edebilirler. Dinlemeyi durduramamalarına rağmen kendilerini dinleyen Eve tarafından da aldatılamazlar. Aşağıda verilen iki grafik dinleme olması ve dinleme olmaması durumundaki test bitlerini göstermektedirler.



Herhangi bir dinleme olmadığında anahtarda bulunan test bitlerinde bir problem oluşmamaktadır. Ancak dinleme durumunda anahtarda bulunan test bitleri bozulmaya uğramaktadır.

Kuantum Kriptografi'de Kullanılan Algoritmalar

BB84 Algoritması

Bennet ve Brassard isiminde iki bilim adamının 1984'te yazdıkları bir makalede kuantum kriptografiden bahsetmeleri sebebiyle algoritmanın adı BB84'tür. Makaleye göre gönderici ve alıcı arasında güvenli bir iletişimi sağlamak amacıyla tek kullanımlık bir anahtarın göndericisi ve alıcısı Alice ve Bob şeklinde tanımlanmıştır. Mesajı göndermek isteyen kişi Alice, mesajı almak isteyen kişi Bob olarak belirlenmiştir. Alice ve Bob'dan her ikisi de birbirleriyle 45° açı yapan iki kristal süzgeç çiftine (+ ve x şeklinde) sahiptirler, bunlar arasında bir optik fiber ağı bulunmaktadır ve her iki taraf da foton üretebilmektedir.

Alice ve Bob, I ve / süzgeçleri için 0 değerinde, - ve \ süzgeçleri için ise 1 değerinde anlaşılır. Yani her iki taraf da I ve / yönünde polarize olmuş foton için 0 bitinin; - ve \ yönünde polarize olmuş foton için 1 bitinin geldiğini anlayacaklardır. Bu seçimin tam tersi de uygulanabilir.

Basis	0	1
+	↑	→
×	↗	↘

Alice iletişimde kullanılacak rastgele bir tek kullanımlık anahtar seçer. Bu anahtarı Bob'a yollamak için BB84 algoritmasını kullanır.

Algoritma şu yolla işler:

- Örneğin Alice (1101010010) bit dizisini aşağıdaki süzgeç takımlarıyla göndermek istesin. Seçilen süzgeç takımları ve bitler tamamen rastgeledir.
- Bob rastgele bir süzgeç takımı (+ veya x) seçer ve aşağıdaki yönlerde polarize olmuş fotonları elde eder.
Sonuç olarak Bob'un elde ettiği bit dizisi Alice'in göndermiş olduğuyla aynı değildir. İstatistiksel olarak Alice'in gönderdiği bitlerin sayısının yarısı kadar bit Bob'da aynıdır. Bu yüzden algoritmanın bundan sonraki kısmında her iki tarafta ortak kullanılan bitlerin belirlenmesi gerekecektir.
- Bob, Alice'e hangi bitler için hangi süzgeç çiftlerini kullandığını açık olarak iletir. Bunu üzerine Alice bu süzgeçlerden hangilerinin doğru, hangilerinin yanlış seçim olduğunu Bob'a iletir. Böylece hem Alice hem Bob tarafından ortak kullanılan süzgeç çiftlerine karşılık gelen bit dizisi anahtar olarak kullanılır. Sonuçta bu anahtar her iki taraf için de bilindiğinden mesaj bu anahtar ile XOR işlemine sokularak güvenli hale getirilir. Mesajın XOR'lanması ve iki taraf arasında mesaj iletimi tamamen klasik yollarla yapılabilir. Kuantum kriptografinin ana teması şifrelemede kullanılan anahtarın iki tarafça pratik bir şekilde bilinir hale getirilmesini sağlamaktır. Üçüncü bir kişinin anahtarı dinleyip dinlemediğini öğrenmek için Alice ve Bob bit dizilerini kontrol ederler. Eğer üçüncü bir kişi fotonların polarizasyonu ile ilgili bilgileri almaya çalışırsa bu durum Bob'un ölçümlerinde bozulmalar yol açar. Eğer belirli bir sayının üzerinde bit farklılık gösteriyorsa anahtar iptal edilerek farklı bir anahtar üretilmeye ve üçüncü kişinin bu anahtar hakkında en az bilgiye sahip olması sağlanmaya çalışılır.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		×			✓		✓

EPR-Ekert Protokolü

Ekert protokolü'nde BB84 'te olduğu gibi Heisenberg belirsizlik ilkesi kullanılmaz. Bu protokolda kuantum halleri birbirine bağlaşık iki foton kullanılır, alıcı ve vericiye birer foton

gelir. Bu fotonların kuantum halleri birbirine zıt olduğundan bir taraf diğer taraftaki kuantum halini tahmin edebilir, böylece ortak bir kod anahtarı elde edilebilir.