KUANTUM ŞİFRELEME SANATI

Teknoloji geliştikçe daha çok bilgi çevrimiçi haline geliyor ve özel bilgilerin açığa çıkarılması gittikçe kolaylaşıyor. Buna bağlı olarak, klasik şifreleme teknikleri bugüne kadar yaygın olarak kullanıldı ve konuşmaların üçüncü şahıslar tarafından dinlenilmesi engellenmeye çalışıldı. Ancak, klasik şifreleme yöntemleri şu anda yeterli gibi gözükse de, işlemci hızlarında öngörülen artış ve yeni bulunan matematiksel yöntemlerle klasik şifrelemenin geleceği tehdit altında. Birkaç on yıldır devam eden araştırmalarsa % 100 güvenlik sağlayacak çözüm önerileri üzerine yoğunlaşmıştır. Bu araştırmaların ilk sonuçlarına göre, kuantum şifreleme yöntemleri aranan cevap olma yetisine sahip görünüyor.

Klasik Şifreleme

Kuantum şifreleme sanatının derinliklerine inmeden 'klasik' şifrelemeden neyi kastettiğimizi biraz daha açıklamamız yerinde olacak. Ana hatlarıyla düşünüldüğünde, klasik şifreleme sanatı iki ana kola ayrılır.

Simetrik-anahtar Şifrelemesi Sanatı: Bu şifreleme sisteminde gönderen ve alıcı ortak bir anahtarı paylaşmaktadır. Bu anahtarla mesaj şifrelenir ve çözülür. Bu yöntemi kullanarak güvenilir iletişime olanak sağlayan başlıca iki standart belirlenmiş bulunuyor. Bunlar, Veri Şifreleme Standardı (DES) ve İleri Şifreleme Standartları (AES). Simetrik-anahtar şifrelemesinde yollanması planlanan mesajların halka açık kanaldan gönderilmesine karşın anahtar, güvenli bir şekilde alıcıya gitmeli. 'Elden ele teslim' zihniyetini en güvenli yol olarak gören birçok kurum/kişi anahtar dağıtımında kurye yöntemini kullandılar. Ancak büyük ağlarda, anahtarın birden çok kişiye gönderilmesi gerektiğinde büyük bir zaman ve para kaybı söz konusuydu. Örnek olarak, n tane kullanıcısı olan bir ağda, kullanılmak üzere $n(n-1)/2$ adet anahtar gerekir. Dolayısıyla, simetrik-anahtar şifreleme yöntemi oldukça verimsiz ve emniyetsiz bir yöntem olarak nitelendirildi.

Açık-anahtar Şifrelemesi Sanatı: Bu şifreleme sisteminde matematiksel açıdan birbirine bağlı iki adet anahtar vardır. Hem açık anahtar hem de gizli anahtar, gizli şekilde üretilir. Açık anahtar ağ üzerinde serbestçe hareket ederken, gizli anahtar saklı tutulur. Açık anahtar mesajları şifrelemek, gizli anahtarsa şifrelenmiş mesajları çözmek için kullanılır. Bazı durumlarda tam tersi de sözkonusudur; yani gizli anahtar kullanarak mesajlar şifrelenip, açık anahtarla bu şifrelenmiş mesajlar çözülebilir. 1977'de, Ron Rivest, Adi Shamir ve Leonard Adleman (RSA) algoritması tanıtıldı. RSA, simetrik şifrelemede kullanılan anahtarın ne kadar güvenli olduğunu test eder. Buna "dijital imzalama" adı verilir ve şu an dünyada sık kullanılan algoritmadır. Ancak, bu sistem de bazı olası sorunlarla karşı karşıya.

İlk olarak anahtar değişim hızı, sorun oluşturuyor. İkinci olarak, kuantum bilgisayarlarının ileride kullanılmaya başlanmasıyla tamsayıları çarpanlarına ayırma işlemi klasik bilgisayarlardakine göre binlerce kez hızlı olacak. RSA gizli anahtarları yaparken oldukça büyük tamsayılar kullandığından, bu sayıların kısa zaman aralıklarında bulunması ciddi sorunlar yaratacak.

Kuantum Şifreleme Sanatı

Kuantum şifreleme kuramı ilk olarak Stephen Wiesner tarafından öne sürüldü. Kısa sürede, kuantum şifrelemesinin eşsiz doğası birçok bilim insanının ilgisini çekti. Alışılagelmiş klasik şifreleme sanatı, bilgiyi Eve adı verilen üçüncü kişilerden korumaya çalışırken karışık matematiksel tekniklerin yardımına gereksinim duyar. Oysa, kuantum şifreleme sanatı kuantum mekaniği ilkelerini kullanarak güvenli iletişim ortamı sunmakta.

Kuantum şifreleme sanatının arkasındaki mekanizmayı tam anlamıyla anlamak için, öncelikle kuantum şifrelemesinin dayandığı fizik ilkelerine göz atalım.

Heisenberg Belirsizlik İlkesi: Kuantum mekaniğindeki anlamıyla belirsizlik ilkesi şöyle tanımlanıyor: Eğer kişi bir nesnenin moment ya da konum değeri giderek artan duyarlılıkta ölçülmeye çalışılırsa, diğer değerin doğruluğunda azalma olacaktır. Başka bir deyişle, bir nesnenin hem konumunu hem de momentini kesin duyarlılıkla ölçmek olanaksızdır. Fiziksel özelliklerin bir kısmı vermiş olduğumuz örnekteki gibi birbirini bütünler niteliktedir ve birini kesin duyarlılıkla ölçmeye çalışırsanız diğer değerin yapısını bozmuş olursunuz.

Kuantum şifrelemesindeki bütünler özellikse, fotonun kutuplaşma biçimidir: Dikey veya çapraz. Kutuplaşması bilinmeyen bir fotonun kutuplaşmasını öğrenmek için yapılacak her ölçüm, fotonun doğasını bozacak ve onu dikey ya da çapraz olmayan bir kutuplaşma biçimine sokacaktır. Alıcı, böyle bir durumla karşılaştığında davetsiz bir misafirin mesajları dinlediğini anlayacaktır.

Kuantum Dolanıklığı: Kuantum dolanıklığı, iki ya da daha fazla kuantum taneciğinin (örnek: fotonlar) her ne kadar nesneler tek tek birbirinden ayrı konumlarda bulunsalar da, birbirlerine bağlı olarak tanımlanmaları durumudur. İki parçacığı tek bir kuantum durumunda hazırlamak mümkündür. Buna göre bir tanesi her zaman yukarı kutuplaşmış, diğeri de aşağı kutuplaşmış olacaktır. Sonuç olarak sistemlerden birinde yapılacak bir ölçme işlemi, diğer sistemi de eşzamanlı olarak etkileyecektir.

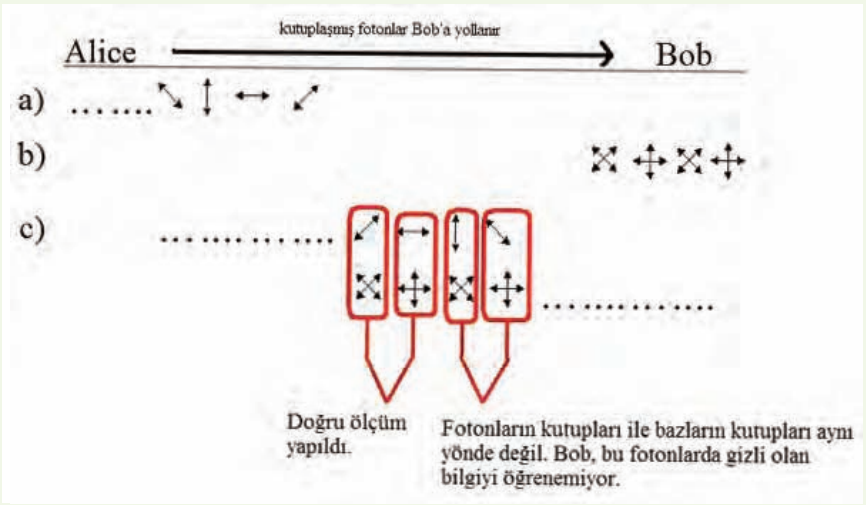
Kuantum Mekansızlığı: Kuantum dolanıklığı genelde ilk kez Bell'in deneylerinde, bulunan kuantum mekansızlığıyla birlikte anılır. Hâlâ tam olarak anlaşılamayan kuantum mekansızlığı, bir kuantum sisteminde fiziksel olarak ayrı ama hâlâ birbirine dolanıklığı bulunan parçaları ilişkilendirmekten sorumludur. Bu ilişki, dolanık parçalar birbirlerinden konum ve zaman olarak çok ayrı olsalar da devam eder. Bu yüzden, konum ve/veya zaman olarak birbirinden ayrılmış kuantum sistemi parçaları, birbirleriyle kusursuz şekilde eşleşir. Bu ilişki ayrıca öyle özeldir ki; bu parçalar ışık hızından daha hızlı bir şekilde birbirleriyle iletişim halindedirler.

Kuantum Kopyalanamazlık Kuramı: Bu kuram bilinmeyen bir kuantum durumunun kopyalanamayacağını söyler.

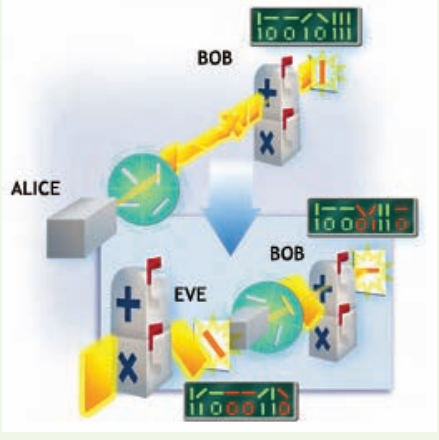
Kuantum mekaniğinin bu dört özelliği, iki farklı tipteki kuantum şifreleme protokollerinin temelini oluşturmuştur.

Kuantum Anahtar Dağıtım Protokolleri

Kuantum anahtar dağıtımı (QKD) güvenli bağlantı yöntemi olarak önerildiyse de, aslında üçüncü şahısların konuşmayı dinlemesini engellemez. Ancak eğer Eve konuşmayı dinlemek isterse, yüksek bir hata değerine neden olacaktır ve bu durum da Alice ve Bob tarafından kolayca anlaşılabilecektir. Böylece, onlar anahtarı değiştirip güvenli iletişime devam edeceklerdir. Şimdi en yaygın şekilde kullanılan QKD protokollerine bir göz atalım.



Bennett ve Brassard Şeması (BB84): Bu şema kutuplaşmış foton tekniğini kullanır. Buna göre fotonların kutuplaşma şekilleri, bilginin bit'ler halinde kodlanmasıyla belirlenir. Klasik yöntemlerden farklı olarak burada Alice ve Bob ortak bir anahtar yaratıp birbirlerine göndermezler. BB84 şemasında iki kanal gereklidir. Bunlardan ilki Alice'ten Bob'a mesaj giderken sinyalleri karıştırılmayacak, temiz ve düzgün yayın yapabilen bir açık kanaldır (gazete, radyo vs.). İkincisiyse bilgiler yüklenilmiş fotonların transferine olanak sağlayan kuantum kanalıdır. Mesajın yollanma prosedürü şöyle betimlenebilir: Protokolü hayata geçirmeden önce Alice ve Bob maksimum kabul edilebilir bir hata oranında $\varepsilon_{maksimum}$ anlaşırlar.



a. Alice, Bob'a çok sayıda foton gönderir. Fotonlarsa raslantısal olarak şu kutuplara sahiptir: ↕ (dikey), ↔ (yatay), ⬈ (45 derece) ve ⬊ (135 derece).

b. Bob, her yapılacak ölçüm için raslantısal olarak düz ya da çapraz baz seçer. (Hesapsal olarak % 50 doğru ölçüm yapma şansı var.)

c. Bob, Alice'e bazlarını açıklar.

d. Alice ona hangi bazların doğru olduğunu geri bildirir.

e. Bob, ölçüm yaptığı verileri 1 ve 0'lar haline çevirir ve mesajı öğrenir.

Dışarıdan bağlantıya sızılıp sızılmadığını öğrenmek için belirli sayıda foton alınır ve deneysel hata oranı ε hesaplanır. Eğer $\varepsilon > \varepsilon_{maksimum}$ ise, o zaman ya kanalın çok gürültülü olduğu ya da dışarıdan bir müdahale olduğu kanısına varılır. Böyle bir durumda haberleşme anında kesilir ve yapılan ölçümler geçersiz sayılır. (a) adımına geri dönülür ve tüm prosedür baştan sonra tekrarlanır. Eğer her şey beklenildiği gibi gerçekleşirse, o zaman konuşmanın (e) aşaması sırasında uzlaşma ve

gizlilik genişletmesi teknikleri uygulanır.

Ekert Şeması: Ekert şeması, Artur Ekert tarafından 1991'de öne sürüldü. Bu şema, foton çiftinin kuantum mekaniğindeki dolanıklık ilkesini kullanır. Foton çifti tek parçacıklara ayrılır ve biri Alice'de diğeri Bob'da olacak şekilde dağıtılır. Alice ve Bob fotonların dolanıklık doğalarından dolayı her zaman zıt kutuplu parçacıklara sahip olurlar. Öte yandan, bireysel olarak elde ettikleri sonuçlar, tümüyle raslantısal olarak değişkenlik gösterir. Kimse Alice'in yapacağı ölçümün dikey mi yoksa yatay mı olacağını öngöremez. İkinci olarak, bu tek parçacıklar önceden birbirleriyle etkileşime girdiklerinden kuantum mekansızlığı özelliğini taşırlar. Bu özellik der ki; eğer Alice ve Bob kutuplaşmaları ölçmeye kalkışırlarsa, bulacakları sonuçlar birbirleriyle kusursuz biçimde bağdaşmayacaktır. Ama % 50'den daha yüksek bir olasılıkla Alice, Bob'un ölçümlerini anlayabilecektir. Aynı durum tersi için de geçerlidir. Bu durum, ortalama olarak Alice'in yapacağı öngörülerin diğer tüm yöntemlerden daha başarılı olacağını söyler. Üçüncü ve son olarak, haberleşmeye sızma girişimi parçacıklar arasındaki bu etkileşimi zayıflatacaktır. Bu durum Alice ve Bob tarafından hemen farkına varılabileceğinden, güvenlik açısından sorun oluşturmayacaktır.

Bennet 1992 Şeması (B92): B92 kuantum şifreleme protokolü BB84 şemasına benzer. B92'de BB84'tekinden farklı olarak yalnızca iki birbirine dik olmayan kuantum durumu vardır ve bilgiler bu iki duruma yüklenir. Belirsizlik ilkesinden biliyoruz ki birbirine dik olmayan iki kuantum durumu, yapılacak bir ölçümle ayırt edilemez. Bu yüzden, bit'lerin gerçek değerleri hiçbir zaman bilinemeyecektir. Eğer biri ölçüm yapmaya kalkışırsa durumların değerleri bozulacak ve bu olay Alice ve Bob tarafından anında duyulacaktır. İlkece, bu şema BB84 şemasına göre daha hızlıdır çünkü Bob bit'leri aldığı anda mesajın içeriğini öğrenecektir. Tekrar Alice ile konuşmasına gerek kalmayacaktır. Ayrıca yalnızca iki tane kuantum durumuna sahip olduğundan, B92'yi uygulamak daha kolaydır. Klasik bit olan 0 yatay kutuplaşmış foton olarak, 1 ise 45-derece kutuplaşmış foton olarak kodlanacaktır. Bob, kendi alıcısını '+' (düz baz) yaparsa yatay kutuplaşmış fotonları; eğer 'x' (çapraz baz) yaparsa da 45-derece kutuplaşmış fotonları ölçebilecektir. Baz seçimi her foton için rastlantısal olarak ayrı ayrı yapılır. Eğer baz yönüyle fotonun kutbu aynı yöndeyse bilgi Bob tarafından öğrenilir, değilse de Bob kötü bir gönderim olduğunu varsayıp bu durumu Alice'e bildirir.

Kısıtlar ve Tehditler

Veri Gönderim Ortamı: Fotonlar aracılığıyla yaşam bulan kuantum durumları, Alice'ten Bob'a optik kablolarla ya da boşlukta gönderilebilir. Ancak mesafeyle gelen bazı sınırlamalar var. Optik nabız yol aldıkça zayıflar ve uzak mesafelerde alıcı tarafından anlaşılması oldukça zorlaşır. Kuantum tekrarlayıcılarının ileride bu sorunun üstesinden geleceği düşünülüyor. Boşlukta ya da havada yapılan gönderimlerde de bazı sorunlar bulunuyor. Gönderen ve alıcı arasındaki nişan çizgisi korunmalıdır. Ayrıca, kötü hava koşullarında bu tip bağlantılar çalışamaz.

Kuantum Şifre Çözme İlmi: Araştırmacılar çeşitli teknikler kullanarak Alice'ten Bob'a yollanan şifreli mesajları çözmeye çabalamaktalar. Genel amaçları QKD şemalarındaki olası zayıflıkları bulmak, bunları geliştirmeye çalışmak ve belli saldırılara dayanıklı yeni protokoller bulmak. Başlıca saldırı yöntemleri, sahte-durumlar saldırısı, yüksek nabız saldırısı, foton-sayısı bölme saldırısı (PNS).

Günümüzdeki Durumu

Haziran 2006'da Los Alamos Ulusal Laboratuvarı'ndaki (LANL) biliminsanları şifrelenmiş kuantum anahtarını optik kablolar kullanarak 184,6 km uzağa gönderebildiler. Bu başarıyla bir önceki rekoru (122 km) da kırmış oldular. Öte yandan, Avrupalılar da boşluk deneyleri yapmaktalar ve QKD mesafe rekorunu Ekert Şeması kullanarak kırdılar. Kuantum anahtarı, boşlukta 144 km yol aldı.

2006'ya kadar tek-foton detektörlerinin yapımında yalnızca yarıiletken maddeler kullanılmıştı. Silikon, görünür ışık detektörleri için; indiyum-galyum-arsenik (InGaAs) ise kızılötesi detektörler için tercih edilen maddeler oldular. Yarıiletken foton sayaçlarına çığ fotodiyotları deniyor ve bunlar ticarette yerlerini almış durumdalar.

Bu yıl içinde, Prof. Roman Sobolewski ve takımı, Rochester Üniversitesi'nde süperiletken tek-foton detektörleri (SSPD) için yeni bir alıcı icat ettiler. Bu alıcıların özellikle kuantum şifreleme ilminde ve kuantum haberleşmelerinde kullanışlı olacağı bildiriliyor.

Şu sıralar üç büyük ticari firma, kuantum şifreleme ürünlerini pazarlamakta: id Quantique (Cenevre), MagiQ Technologies (New York) ve SmartQuantum (Fransa). Toshiba, IBM, HP ve NEC'in de bulunduğu diğer firmalar da kuantum şifreleme araştırmalarına para ve zaman harcamaktalar.

Gelecek

Kuantum şifreleme teknikleri daha çok orduda, yüksek teknoloji laboratuvarlarında ve gizli hükümet birimlerinde denenmekte ve geliştirilmekte. İlk ticari ürünleri piyasaya çıkmış olsa da kuantum şifreleme sanatının genel çevrelerce bilinirliği oldukça az. Bu yüzden, şu anki güvenlik sistemlerinde kısa sürede büyük değişiklikler bekleniyor. Ancak, gelecekte klasik ağların yerini kuantum ağlarının alacağı ve böylece iletişimin daha güvenli olacağı düşünülüyor.

Ömer Demirel,
Fizik Bölümü, Koç Üniversitesi

Dr. Özgür E. Müstecaplıoğlu'na paha biçilemez rehberliği ve desteği için çok teşekkür ederim.

Kaynaklar

FIPS PUB 197, Advanced encryption standard, Federal Information Processing Standards Publications, US Department of Commerce/NIST, National Technical Information Service, November 2001.

Beutelspacher, A. (1994). The Future Has Already Started or Public Key Cryptography. Cryptology (102) ISBN 0-88385-504-6.

Diffie, W., & Hellman, M. (1976, June 8). Multi-user Cryptographic Techniques. AFIPS Proceedings (45), s. 109-112.

Wiesner, S. (1983). Conjugate Coding, Sigact News, 15(1), 78 - 88.

Lo, H.-K., Popescu, S., & Spiller, T. (Eds.). (1998). Introduction to Quantum Computation and Information. Singapore: World Scientific.

Schrödinger, E. (1935). Discussion of Probability Relations Between Separated Systems. Proceedings of the Cambridge Philosophical Society, 31, s. 555-563.

Albert, E., Podolsky, B., & Rosen, N. (1935). Physical Review Letters , 47, 777-780.

Bell, John S. (1966). Reviews of Modern Physics 38, 447-452.

Wootters, W. K., and Zurek, W. Nature 299, 802 (1982); Dieks, D. Phys. Lett. A 92, 271 (1982).

Bennett, C. H., & Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers Systems and Signal Processing, (pp. 175-179). Bangalore India.

Brassard, G., & Salvail, L. (May 1993). Secret-key Reconciliation by Public Discussion. Advances in Cryptology Eurocrypt '93 Proceedings.