Işık Kuvantumları: Lazer ışınından fotonlar veri transferi için kullanılıyor. Bu ışık parçacıkları verilerin güvenli şifrelenmesi için kullanılabilecek şekilde manipüle ediliyor.

Kuvantum Kriptografisi

“DİİR Cjmnfçf Rftjoef”

Bankalar ve askeri kuruluşlar gözlerini Cenevre Gölü’ne çevirmiş heyecanla bekliyorlar... Orada gizli verilerin ağ üzerinden gönderilmesini olanaklı kılan bir yöntem geliştiriliyor. Ayrıca, şifre çözücüler de casusluğa karşı güvenli bir biçimde transfer edilebiliyor.

Korkmayın, niyetimiz sizleri yeni bir harf düzeniyle karşı karşıya getirmek değil. Bir bilmece gibi duran yazımızın başlığı aslında bir kriptografi (şifreleme) örneği. Bizim seçtiğimiz kaydırma kodu ilkesini Julius Caeser da kullanmış. Örnek cümlede yan yana gelen harflerin her biri alfabede kendinden sonra gelen harfin yerini tutuyor: Örneğin A yerine B, B yerine C, C yerine D kullanılıyor. James Bond bile bizim başlığımızı çözemez herhalde(!) **“CHIP Bilmece Peşinde”**

Şimdiye kadar kriptologlar da aynı sorunla karşı karşıya bulunuyorlardı: Bazen biraz uzun sürse de hemen hemen bütün anahtarlar çözülüyordu. Ama casusların işi giderek zorlaşıyor. Kuvantum kriptografisi gizli anahtarları (şifreleri) koruyacak. Buradaki hile her bir dinleme denemesinin derhal göze çarpması. Bunun anlamını kavramak için ardında yatan teorik bilgiyi tanımak gerekiyor. Kuvantum kriptografisi ilkesi ışığın yalnızca dalga özelliklerine değil, aksine parçacık özelliklerine de sahip olmasına dayanıyor. Bu tip bir ışık parçacığının (foton) kutuplandırılması yatay, dikey, sola doğru eğik ya da sağa doğru eğik yönelimli olabiliyor. Bu farklılık olanağını kuvantum araştırmacıları cam elyaf üzerinden anahtarların transferinde kullanıyor (bkz. yan sayfadaki kutu).

Kuvantum kriptografisiyle güvenli transfer

Yıllarca süren araştırmalardan sonra ışık iletkenleri üzerinden anahtar transferi üzerinde çalışan bilimciler, ileriye doğru dev bir adım atmış bulunuyorlar. Bir gizli kodun güvenli transferi için gerekli süreyi dünya rekoru

SERİ

ARAŞTIRMA LABORATUARLARINDAN YENİLİKLER

Geleceğin dünyasıyla şimdiden tanışın: Bilim ve endüstri, yaşamınızı köklü şekilde değiştirecek anahtar teknolojiler üzerinde çalışıyor. CHIP bu yazı dizisinde sizi geleceğin dünyasıyla tanıştırıyor.

Üniversiteden Özel Firmaya: Cenevre'den Olivier Guinnard (solda) ve Grégoire Ribordy id Quantique firmasını spin-off (daha önce varolan bir firmayı temel alarak) olarak kurmuşlar.

olan 67,1 kilometreye çekmiş bulunuyorlar. Grégoire Ribordy Şubat ayında kuvantum teçhizatını bu uzaklığa ayarladığında, Cenevre Gölü'nün öteki ucundan cam elyaf içinde çok düşük bir lazer içtepisi kaydetmişti. Dört dakika sonra Lozan'da dünya üzerinde gönderenden başka hiçbir kimsenin tanımadığı bir anahtarın yaklaşık 13.000 bit'ini elde etmişti. USB bağlantılı ve ağ prizli paket üzerinde aslında "Quantumkryptography inside" yazmalıydı. "Ben kuvantum şifreleme demeyi tercih ediyorum" diyerek Ribordy alçakgönüllülük ediyor; o Cenevreli üretici id Quantique'in yöneticilerinden biri.

"Sistemimiz kuvantum fiziği ilkeleri yardımıyla bir anahtarı transfer ediyor ve yakalanıp yakalanmadığını sınıyor." Ribordy'ye göre kuvantum kriptografisi "fizik yasalarının olanaklı kıldığı tüm saldırılara" karşı koyuyor. Bunun nedeni doğanın mükemmel madde kopyalarını yasaklaması. Eğer bir saldırgan bir ışık parçacığını ikiye çıkarmak ve kopyayı kendi için dallandırmak istiyorsa, başlangıçtaki fotonu bozuyor. Bir casus gerçi lazer sinyali yakalayabiliyor, ölçebiliyor ve alıcıya benzer sinyaller gönderebiliyor. Oysa "mükemmel ve "yaklaşık olarak" kopyalama arasındaki fark saldırganın ensesine yapışıyor. Bu sinyaller ister istemez iletişim partnerinin farkına varacağı hatalar içeriyor.

Kuvantum casuslarına geçit yok

Önce hoş karşılanan fiziğin temel yasaları, birkaç kilometre sonra kuvantum casuslarının karşısına dikiliyor. "Belki gelecek yıllarda 100 kilometreyi aşmak olanaklı olacaktır, ama 1.000 kilometrelik bir mesafenin üstesinden gelmek kesinlikle olanaksız olacaktır" diyor Münih/Garching'te bulunan kuvantum optiği Max Planck Enstitüsü yöneticisi Ignacio Cirac. Bunun nedeni cam elyafın lazer ışınını birkaç düzine sonra acımasızca yutması. Olsa

VERİ TAŞIYICI OLARAK FOTONLAR

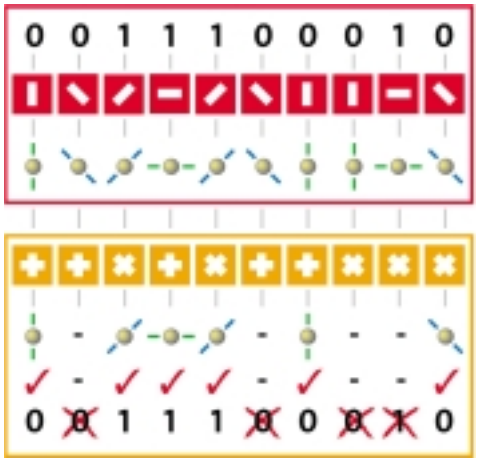
»Gizli anahtar nasıl oluşuyor?

GÖNDEREN

1. Gönderen rastlantısal sayı kodunu oluşturur.
2. Işık parçacıkları rastlantı ilkesine göre kutuplaştırılır.
3. Fotonlar (her biri iki olanağa sahip) 0 ya da 1 değerlerini alırlar.

ALICI

4. Rastlantısal ayarlara sahip detektör
5. Kutuplaştırılma ya muhafaza edilir ya da bozulur.
6. Gönderen ve alıcının uyuşan ayarları
7. Doğru transfer edilmiş değerler anahtarı oluşturur.



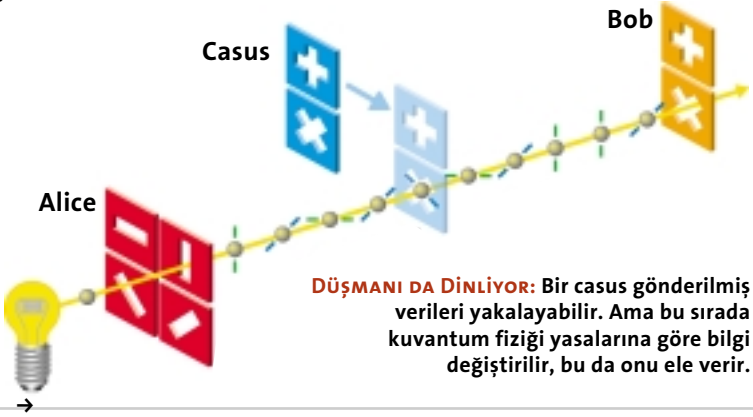
■ Kuvantum hileleriyle Alice ve Bob gizli bir anahtar yaratabilir ve dağıtabilir, (bkz. yukarıya).

▸ **Gönderici Alice** farklı kutuplaştırılmış yönlü ışık parçacıklarını (fotonları) cam elyaf üzerinden Bob'a gönderir. Gönderme sırasında Alice rastlantısal olarak "düz" ve "eğik" kutuplaştırmalar arasında geçişler yapar.

▸ **Alıcı Bob** da aynı şekilde detektörünü rastlantısal olarak düz ya da eğik olarak yönlendirir. Bob'un ölçümü hangi yönde gönderildiği hakkında bir bilgi vermez. Alice "eğik" yönlü bir foton gönderir ve Bob bunu "düz" yönde ölçerse, rastlantısal bir sonuç elde eder. Bob'un ölçümü Alice'in yanlış kutuplaştırmasını kendi ölçüm yönüne projekte eder ve bu sırada başlangıçtaki bilgiyi yok eder.

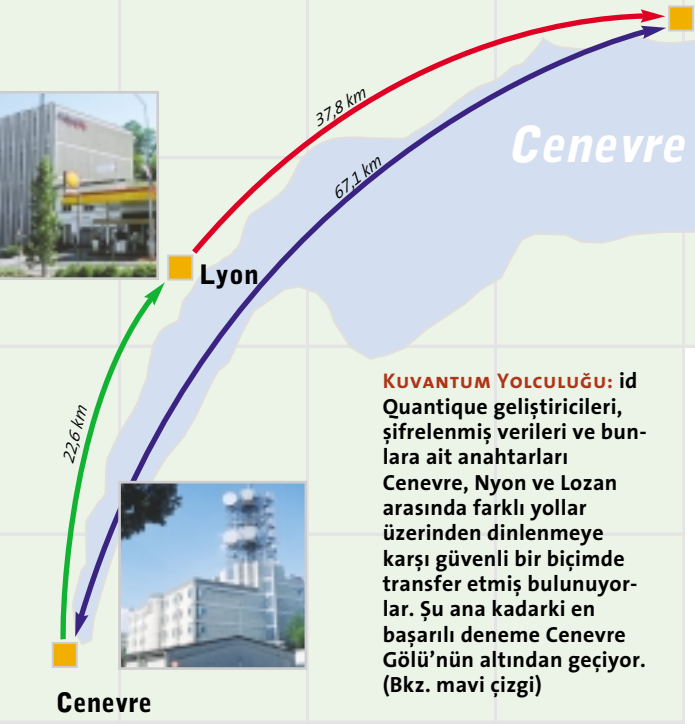
▸ **Transferden sonra** Alice ve Bob birbirlerine hangi yönü kullandıklarını iletirler. Daha sonra gönderme ve ölçme yönlerinin uyuşmadığı tüm olayları listelerinden silerler. Geriye kalan ölçümlerden her ikisi de birbiriyle uyuşan bir bit dizisi, yani gizli anahtarı elde ederler.

▸ **Teoride bir casus** transferi dinleyebilir, (bkz. aşağıdaki grafik). Ama onun ölçümleriyle transferde hatalar oluşur. Dinlenip dinlenmediklerini ortaya çıkarmak için, Alice ve Bob hata oranını belirlerler. Bu amaçla kendi "iyi" bit'lerini doğrudan ya da kutuplaştırılma bilgileri yardımıyla ("Bit 1 ve 4 birbirinden farklıdır") karşılaştırırlar. Eğer hata oranı belirli bir tolerans içersindeyse, sınama bit'lerine kadar tüm geçerli değerleri gizli anahtar olarak kullanabilirler.



Düşmanı da Dinliyor: Bir casus gönderilmiş verileri yakalayabilir. Ama bu sırada kuvantum fiziği yasalarına göre bilgi değiştirilir, bu da onu ele verir.

Dünya rekoru: Cenevre'den Lozan'a 67,1 km güvenli "kuvantum transferi"



Su Altında: Cenevre'den gönderilen lazer içtepileri gölün altındaki 67,1 km cam elyaf üzerinden Lozan'a varıyor.

Kuvantum Yolculuğu: id Quantique geliştiricileri, şifrelenmiş verileri ve bunlara ait anahtarları Cenevre, Nyon ve Lozan arasında farklı yollar üzerinden dinlenmeye karşı güvenli bir biçimde transfer etmiş bulunuyorlar. Şu ana kadarki en başarılı deneme Cenevre Gölü'nün altından geçiyor. (Bkz. mavi çizgi)

olsa havada, örneğin Relais istasyonu olarak düşük yörüngedeki bir uydu vasıtasıyla zayıf ışıkların da büyük mesafelerin üstesinden gelmesi sağlanabilir. "Ancak orada da transferi anaforlar, bulutlar ve etrafa saçılan ışık rahatsız edebilir" uyarısında bulunuyor Cirac.

Kuvantum yineleyiciler iş başında

Ancak ufukta daha uzun mesafeler için de bir çözüm belirmiyor değil: Sinyal yoldayken tazelenmek zorunda. Oysa telefon sinyallerine taze enerji sağlayan şey, gizli sinyaller için ölümcül darbe olabiliyor. Geleneksel güçlendiriciler bir casus etkisi yaratıyor ve hatasız transferi boşa çıkarabiliyor. Burada henüz yalnızca kağıt üzerinde varolan kuvantum Repeater (yineleyiciler) bir çıkış yolu sunabilir. Bunlar kuvantum bilgisayarı için bir tür ön basamak oluşturuyor ve "çaprazlama içice geçmiş çiftler" denilen özel bir tür ışık kuvantumlarıyla çalışıyor. Bu ikiz parçacıklar Albert Einstein'ın onları düşünsel deneylerde "hayaletvari uzaklık etkisi" için neden olarak ortaya çıkarması ile ün kazanmıştı. Parçacıklar birbirinden ne kadar uzak olursa olsunlar, birbirleriyle bağlantılarını asla kaybetmemiş görünüyor. O sırada karşılığı ile nelerin cereyan ettiğini bir parçacık adeta telepati yoluyla "biliyor".

Fizikçiler uzun zamandır bu tip kuvantum ikizlerinin varlığından kuşku duymuyor ve hatta kısa bir süre için çiftleri laboratuvarda yetiştiriyor. Çaprazlama içice geçmiş çiftlerle uzun mesafelerin üstesinden gelebilecek bir mekanizmayı çoktan bulmuş olan teorisyenler çok daha ileride. Buradaki sihirli sözcük çaprazlamayı temizleme. İlke ise şu: Birçok çaprazlama içice geçmiş çiftler, daha sonra içinden az sayıda bozulmamış çifti "damıtacağı" tüm rahatsız edici arızaları üstleniyor.

"Hışırtıların varlığında da böylelikle birçok mükemmel olmayan çiftten az sayıda neredeyse mükemmel çiftler yaratılabiliyor" diyerek kendileriyle birkaç yıl içinde kuvantum kriptografisinin bugünkü sınırlarının ortadan kaldırılabileceği kuvantum-repeater'ların temellerinden birini betimliyor Münih Üniversitesi'nden Hans Briegel.

"Kuvantum parmak izi" çalışmaları

"20 yıl içinde kuvantum-repeater'lar yardımıyla yerküresel uzaklıklar üzerinden de güvenli bir biçimde gizli anahtar değiştokuşu yapılabileceği düşünülebilir." Günümüzün Caesar'ları, devletle ilgili, iktisadi ve askeri merciler böylelikle başkaları bilecek korkusu olmadan gizli anahtar değiştokuşunda bulunabilirler.

Tüm sorunlara rağmen anahtar değiştokuşu bilgisayar branşının ulaşacağı yegane kuvantum tekniği olmakla kalmayacak. Araştırmacılar çoktandır kuvantum durumlarına damgasını vuran bir tür sınama toplamı olan veriler için bir "kuvantum parmak izi" üzerinde kafa patlatıyor. Böylelikle bilgisayar veritabanlarının kendilerinin karşılaştırılmasına gerek kalmaksızın iki veritabanının aynı olup olmadığını kuvantum bilgilerini karşılaştırmak yoluyla hızla karar verebilir.

Hollanda'da, Amsterdam'daki Matematik ve Bilgisayar Bilimleri Araştırma Merkezi'ndeki (CWI) bilimciler, Kanadalı meslektaşları ile bu görevin kuvantum çözümü için şimdiye kadarki teknikle olduğundan bariz bir biçimde daha az bilgi biriminin değiştokuş edilmek zorunda kalınacağını göstermiş bulunuyor. "Hata olasılığı %1'in altına çekilmek isteniyorsa, bir terabyte'lık bir veritabanı için konvansiyonel parmak izi yaklaşık 10 megabyte büyüklüğünde olacaktır" tahmininde bulunuyor CWI'den Hartmut Klauck. "Aynı amaca 3.000 kuvantum bit'le ulaşmak olanaklı olabilecektir."

Bu konuyla ilgili daha fazla bilgi için

www.qubit.org: Centre for Quantum Computation, Oxford
www.idquantique.com: id Quantique, Cenevre
www.cwi.nl: Centrum voor Wiskunde en Informatica, Amsterdam
www.mpq.mpg.de: Kuvantum optiği için, Garching
www.quantum.at: Viyana Üniversitesi kuvantum araştırma grubu

KK / Garo Antikacıoğlu, agaro@chip.com.tr