# Quantum key distribution

**Quantum Key Distribution** (QKD) is the task of generating a private key shared between two parties using a (completely insecure) quantum channel and an authenticated (but not private) classical channel (e.g., a telephone line). The private key can then be used to encrypt messages that are sent over an insecure classical channel (such as a conventional internet connection).

Unlike traditional **cryptography**, where the security is usually based on the fact that an adversary is unable to solve a certain mathematical problem, QKD achieves security through the laws of quantum physics. More precisely, it is based on the fact that an eavesdropper, trying to intercept the quantum communication, will inevitably leave traces which can thus be detected. In this case, the QKD protocol aborts the generation of the key.

The most well-known QKD protocols are the prepare and measure based **Bennett-Brassard-84 (http://www.quantiki.org/wiki/index.php/BB84#how_the_Ekert91_protocol_works)** (BB84) and **Bennett-92** (B92) protocols and the entanglement based **Ekert-91 (http://www.quantiki.org/wiki/index.php/BB84#how_the_Ekert91_protocol_works)** (E91) protocol.

For each of the protocols there is a number of **security proof**s, proving that with different techniques for **information reconciliation** and **privacy amplification**, a certain **private key rate** can be achieved.

Cryptographic schemes base on quantum key distribution are already commercially available, for example by ID Quantique or MagiQ.

## Quantum key exchange

A central problem in cryptography is the key distribution problem. One solution is based on mathematics, **public key cryptography**. Another approach is based on physics: quantum cryptography. While public-key cryptography relies on the computational difficulty of certain hard mathematical problems (such as integer factorisation), quantum cryptography relies on the laws of **quantum mechanics**.

**Uncertainty:** The act of measurement is an integral part of quantum mechanics, not just a passive, external process as in classical physics. So it is possible to encode information into some quantum properties of a photon in such a way that any effort to monitor them necessarily disturbs them in some detectable way. The effect arises because in quantum theory, certain pairs of physical properties are complementary in the sense that measuring one property necessarily disturbs the other. This statement is known as the Heisenberg uncertainty principle. It does not refer merely to the limitations of a particular measurement technology: it holds for all possible measurements. The two complementary properties that are often used in quantum cryptography, are two types of photon's polarization, e.g. rectilinear (vertical and horizontal) and diagonal (at 45° and 135°).

**Entanglement:** It is a state of two or more quantum particles, e.g. photons, in which many of their physical properties are strongly correlated. The entangled particles cannot be described by specifying the states of individual particles and they may together share information in a form which cannot be accessed in any experiment performed on either of the particles alone. This happens no matter how far apart the particles may be at the time. Entanglement is crucial for long-distance quantum key distribution.

## Two different approaches

Based on these two counter-intuitive features of quantum mechanics (uncertainty and entanglement), two different types of quantum cryptographic protocols were invented. Both are based on the fact that quantum systems are disturbed by measurements performed on them. The first type uses the polarization of photons to encode the bits of information and relies on quantum randomness to keep **Eve** from learning the secret key. The second type uses entangled photon states to encode the bits and relies on the fact that the information defining the key only "comes into being" after measurements performed by **Alice** and **Bob**.

## Polarized photons - Charles H. Bennett and Gilles Brassard (1984)

This cryptographic scheme uses pulses of polarized light, with one photon per pulse. Consider two types of polarization, linear and circular. Linear polarization can be vertical or horizontal and circular polarization can be left-handed or right-handed. Any type of polarization of a single photon can encode one bit of information, for example, vertical polarization for "0" and horizontal polarization for "1" or left-handed polarization for "0" and right-handed polarization for "1". In order to generate a random key, Alice must send either horizontal or vertical polarization with equal probability. To keep Eve from successfully eavesdropping, Alice also uses randomly the alternative circular polarizations randomly choosing between left-handed and right-handed photons. The security of this scheme is based on the fact that Eve does not know whether any given pulse codes for 0 or 1 using the linear or the circular polarizations. If Eve tries to measure the state and guesses wrongly, she will disturb it, and Alice and Bob can monitor for such disturbances to test for possible eavesdropping and even estimate what fraction of the transmitted key Eve might have obtained. Bob does not know which polarizations were used for any given pulse coding either. (Alice could tell him, but since it has to be kept secret from Eve they would need a cryptographically secure communication channel to do this, and if they had one they wouldn't need this scheme.) However, he can guess, and half the time he will get it right. Once the photons are safely received, so that Eve cannot use the information, Alice can tell him which guesses were right and which wrong.

## Entangled photons - Artur Ekert (1991)

The scheme relies on three properties of entanglement. First, we can make entangled states which are perfectly correlated in the sense that if Alice and Bob both test whether their particles have vertical or horizontal polarizations, they will always get opposite answers. The same is true if they both measure any other pair of complementary (orthogonal) polarizations. However, their individual results are completely random: it is impossible for Alice to predict if she will get vertical polarization or horizontal polarization.

Second, these states have a property often called quantum non-locality, which has no analogue in classical physics or everyday experience. If Alice and Bob carry out polarization measurements, their answers will not be perfectly correlated, but they will be somewhat correlated. That is, there is an above-50% probability that Alice can, from her measurement, correctly deduce Bob's measurement, and vice versa. And these correlations are stronger - Alice's guesses will on average be better - than any model based on classical physics or ordinary intuition would predict.

Third, any attempt at eavesdropping by Eve will weaken these correlations, in a way that Alice and Bob can detect.

## Privacy amplification

Quantum cryptography protocols achieve something that ordinary classical cryptography cannot. They allow Alice and Bob to generate and share random keys which are very similar - in perfect conditions they would be identical, but actually there will be some error rate. They also allow Alice and Bob to estimate the level of eavesdropping and so work out the maximum amount of information Eve can have about their shared random keys. These are interesting results, but on their own they are not enough to solve the key distribution problem. It could be disastrous if Eve learns even a small part of the cryptographic key: she could then read part - perhaps a critical part - of the secret message Alice wants to send. Because errors and background noise can never completely be avoided, Alice and Bob can never guarantee that Eve has no information at all about their keys - communication errors and eavesdropping cannot be distinguished, and so to be on the safe side Alice and Bob have to assume that all discrepancies are due to Eve.

Happily (for Alice and Bob), while quantum cryptography was being developed, Ueli Maurer and other classical cryptographers were developing a technique called privacy amplification, which turns quantum cryptography into a practical technology for secure communications.

Privacy amplification is a sort of cryptographic version of error correction, which allows Alice and Bob to start with similar shared random keys about which Eve has some information and make shorter shared random keys which are identical and about which Eve has (essentially) no information.

Though classical privacy amplification can be used for either the Bennett-Brassard or the Ekert protocols, it turns out that entanglement-based cryptography allows privacy amplification to be carried out directly at the quantum level. This is more efficient, and has other advantages. In particular, when the technology is fully developed, it will allow quantum cryptography to be carried out over arbitrarily long distances by using quantum repeater stations along the communication route.

incorrect detector. He cannot re-emit the photons to Bob correctly, which will introduce unacceptable levels of error into the communication.

If Alice and Bob are using an entangled photon system, then it is virtually impossible to hijack these, because creating three entangled photons would decrease the strength of each photon to such a degree that it would be easily detected. Mallory cannot use a man-in-the-middle attack, since he would have to measure an entangled photon and disrupt the other photon, then he would have to re-emit both photons. This is impossible to do, by the laws of quantum physics.

Other attacks are possible. Because a dedicated fiber optic line is required between the two points linked by quantum cryptography, a **denial of service attack** can be mounted by simply cutting the line or, perhaps more surreptitiously, by attempting to tap it. If the equipment used in quantum cryptography can be tampered with, it could be made to generate keys that were not secure using a **random number generator attack**.

## History

Quantum cryptography was discovered independently in the US and Europe. The first one to propose it was **Stephen Wiesner**, then at Columbia University in New York, who, in the early 1970's, introduced the concept of quantum conjugate coding. His seminal paper titled "Conjugate Coding" was rejected by IEEE Information Theory but was eventually published in 1983 in SIGACT News (15:1 pp. 78-88, 1983). In this paper he showed how to store or transmit two messages by encoding them in two “conjugate observables", such as linear and circular polarization of light, so that either, but not both, of which may be received and decoded. He illustrated his idea with a design of unforgeable bank notes. A decade later, building upon this work, **Charles H. Bennett**, of the IBM T.J. Watson Research Center, and **Gilles Brassard**, of the Université de Montréal, proposed a method for secure communication based on Wiesner’s “conjugate observables". In 1990, independently and initially unaware of the earlier work, **Artur Ekert**, then a Ph.D. student at the University of Oxford, developed a different approach to quantum cryptography based on peculiar quantum correlations known as quantum entanglement. Since then quantum cryptography has evolved into a thriving experimental area and is quickly becoming a commercial proposition.

## Prospects

Because entangled quantum states are, in the real world, rarely usefully stable, there is a serious practical problem in keeping them entangled long enough to meet the needs of real world interaction between correspondents or real world cryptanalytic use. The first commercial applications of quantum cryptography have thus a limited reach (100 kilometers maximum). Research is done into **satellite** transmission of the quantum states, since outside the atmosphere, there would be considerably less perturbating interactions.

Commercial quantum cryptography devices are on the market from a few vendors, and this technique shows promise of replacing such protocols as **Diffie-Hellman** key exchange in some high value applications. Factors weighing against its wide application include the cost of the needed equipment and dedicated fiber optic line, the requirement to trust the equipment vendor (as contrasted with **open source** encryption software running on off the shelf computers), and the lack of a demonstrated threat to existing key exchange protocols. It is also worth

Since the invention of quantum key distribution in 1984, it took more than a decade until Mayers came up with the first proof of security against the most general type of attack in 1996. This proof was followed by various alternative proofs, e.g., the one by Shor and Preskill which uses a relation between key agreement and entanglement purification.

## External links

- **Elementary explanation of quantum entanglement and quantum cryptography (http://pass.maths.org.uk/issue35/features/ekert/index.html)**
- **Quantum Cryptography with Entangled Photons (http://www.quantenkryptographie.at/)**
- **1 (http://www.idquantique.com)** website of a vendor offering QKE products
- **2 (http://www.magiqtech.com)** is also a website of a vendor of quantum devices for cryptography
- MetroWest Daily News **A quantum leap: Researchers create super-secure computer network (http://www.metrowestdailynews.com/localRegional/view.bg?articleid=77990)**
- The BB84 Protocol for Quantum Cryptography **3 (http://quantum.bbn.com/dscgi/ds.py/Get/File-18/BB84.pdf)**
- Error Detection and Correction in Quantum Cryptography (Cascade) **4 (http://quantum.bbn.com/dscgi/ds.py/Get/File-242/bs93.pdf)**
- Early article on experimental quantum cryptography **5 (http://quantum.bbn.com/dscgi/ds.py/Get/File-16/BBBSS92.pdf)**
- Entanglement-based quantum cryptography **6 (http://quantum.bbn.com/dscgi/ds.py/Get/File-369/Ekert_-_QKD_Based_On_Bells_Theorem.pdf)**
- The Register: **Quantum crypto comes to Blighty (http://www.channelregister.co.uk/2005/03/29/quantum_crypto/)**
- D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, H. Zbinden. **Quantum Key Distribution over 67 km with a plug & play system (http://xxx.lanl.gov/abs/quant-ph/0203118)**

**Category:Quantum Cryptography**

Last modified: Monday, October 26, 2015 - 17:56