Quantum key distribution

Quantum key distribution (**QKD**) is a secure communication method which implements a cryptographic protocol involving components of quantum mechanics. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. It is often incorrectly called quantum cryptography, as it is the best-known example of a quantum cryptographic task.

An important and unique property of quantum key distribution is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions or quantum entanglement and transmitting information in quantum states, a communication system can be implemented that detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure (i.e. the eavesdropper has no information about it), otherwise no secure key is possible and communication is aborted.

The security of encryption that uses quantum key distribution relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography, which relies on the computational difficulty of certain mathematical functions, and cannot provide any mathematical proof as to the actual complexity of reversing the one-way functions used. QKD has provable security based on information theory, and forward secrecy.

Quantum key distribution is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with a secret, random key.[1] In real-world situations, it is often also used with encryption using symmetric key algorithms like the Advanced Encryption Standard algorithm.

Contents

Quantum key exchange

Quantum communication involves encoding information in quantum states, or qubits, as opposed to classical communication's use of bits. Usually, photons are used for these quantum states. Quantum key distribution exploits certain properties of these quantum states to ensure its security. There are several different approaches to quantum key distribution, but they can be divided into two main categories depending on which property they exploit.

Prepare and measure protocols

In contrast to classical physics, the act of measurement is an integral part of quantum mechanics. In general, measuring an unknown quantum state changes that state in some way. This is a consequence of quantum indeterminacy and can be exploited in order to detect any eavesdropping on communication (which necessarily involves measurement) and, more importantly, to calculate the amount of information that has been intercepted.

Entanglement based protocols

The quantum states of two (or more) separate objects can become linked together in such a way that they must be described by a combined quantum state, not as individual objects. This is known as entanglement and means that, for example, performing a measurement on one object affects the other. If an entangled pair of objects is shared between two parties, anyone intercepting either object alters the overall system, revealing the presence of the third party (and the amount of information they have gained).

These two approaches can each be further divided into three families of protocols: discrete variable, continuous variable and distributed phase reference coding. Discrete variable protocols were the first to be invented, and they remain the most widely implemented. The other two families are mainly concerned with overcoming practical limitations of experiments. The two protocols described below both use discrete variable coding.

BB84 protocol: Charles H. Bennett and Gilles Brassard (1984)

This protocol, known as BB84 after its inventors and year of publication, was originally described using photon polarization states to transmit the information.[2] However, any two pairs of conjugate states can be used for the protocol, and many optical fibre based implementations described as BB84 use phase encoded states. The sender (traditionally referred to as Alice) and the receiver (Bob) are connected by a quantum communication channel which allows quantum states to be transmitted. In the case of photons this channel is generally either an optical fibre or simply free space. In addition they communicate via a public classical channel, for example using broadcast radio or the internet. Neither of these channels need to be secure; the protocol is designed with the assumption that an eavesdropper (referred to as Eve) can interfere in any way with both.

The security of the protocol comes from encoding the information in non-orthogonal states. Quantum indeterminacy means that these states cannot in general be measured without disturbing the original state (see No cloning theorem). BB84 uses two pairs of states, with each pair conjugate to the other pair, and the two states within a pair orthogonal to each other. Pairs of orthogonal states are

referred to as a basis. The usual polarization state pairs used are either the rectilinear basis of vertical (0°) and horizontal (90°), the diagonal basis of 45° and 135° or the circular basis of left- and right-handedness. Any two of these bases are conjugate to each other, and so any two can be used in the protocol. Below the rectilinear and diagonal bases are used.

Basis	0	1
+	↑	→
×	↗	↘

The first step in BB84 is quantum transmission. Alice creates a random bit (0 or 1) and then randomly selects one of her two bases (rectilinear or diagonal in this case) to transmit it in. She then prepares a photon polarization state depending both on the bit value and basis, as shown in the adjacent table. So for example a 0 is encoded in the rectilinear basis (+) as a vertical polarization state, and a 1 is encoded in the diagonal basis (x) as a 135° state. Alice then transmits a single photon in the state specified to Bob, using the quantum channel. This process is then repeated from the random bit stage, with Alice recording the state, basis and time of each photon sent.

According to quantum mechanics (particularly quantum indeterminacy), no possible measurement distinguishes between the 4 different polarization states, as they are not all orthogonal. The only possible measurement is between any two orthogonal states (an orthonormal basis). So, for example, measuring in the rectilinear basis gives a result of horizontal or vertical. If the photon was created as horizontal or vertical (as a rectilinear eigenstate) then this measures the correct state, but if it was created as 45° or 135° (diagonal eigenstates) then the rectilinear measurement instead returns either horizontal or vertical at random. Furthermore, after this measurement the photon is polarized in the state it was measured in (horizontal or vertical), with all information about its initial polarization lost.

As Bob does not know the basis the photons were encoded in, all he can do is to select a basis at random to measure in, either rectilinear or diagonal. He does this for each photon he receives, recording the time, measurement basis used and measurement result. After Bob has measured all the photons, he communicates with Alice over the public classical channel. Alice broadcasts the basis each photon was sent in, and Bob the basis each was measured in. They both discard photon measurements (bits) where Bob used a different basis, which is half on average, leaving half the bits as a shared key

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

To check for the presence of an eavesdropper, Alice and Bob now compare a predetermined subset of their remaining bit strings. If a third party (usually referred to as Eve, for "eavesdropper") has gained any information about the photons' polarization, this introduces errors in Bob's measurements. Other environmental conditions can cause errors in a similar fashion. If more than p bits differ they

abort the key and try again, possibly with a different quantum channel, as the security of the key cannot be guaranteed. p is chosen so that if the number of bits known to Eve is less than this privacy amplification can be used to reduce Eve's knowledge of the key to an arbitrarily small amount at the cost of reducing the length of the key

E91 protocol: Artur Ekert (1991)

Artur Ekert's scheme uses entangled pairs of photons. These can be created by Alice, by Bob, or by some source separate from both of them, including eavesdropper Eve. The photons are distributed so that Alice and Bob each end up with one photon from each pair

The scheme relies on two properties of entanglement. First, the entangled states are perfectly correlated in the sense that if Alice and Bob both measure whether their particles have vertical or horizontal polarizations, they always get the same answer with 100% probability. The same is true if they both measure any other pair of complementary (orthogonal) polarizations. This necessitates that the two distant parties have exact directionality synchronization. However, the particular results are completely random; it is impossible for Alice to predict if she (and thus Bob) will get vertical polarization or horizontal polarization. Second, any attempt at eavesdropping by Eve destroys these correlations in a way that Alice and Bob can detect.

Similarly to BB84, the protocol involves a private measurement protocol before detecting the presence of Eve. The measurement stage involves Alice measuring each photon she receives using some basis from the set $Z_0, Z_{\frac{\pi}{8}}, Z_{\frac{\pi}{4}}$ while Bob chooses from $Z_0, Z_{\frac{\pi}{8}}, Z_{-\frac{\pi}{8}}$ where Z_θ is the $\{|\uparrow\rangle, |\rightarrow\rangle\}$ basis rotated by θ. They keep their series of basis choices private until measurements are completed. Two groups of photons are made: the first consists of photons measured using the same basis by Alice and Bob while the second contains all other photons. To detect eavesdropping, they can compute the test statistic S using the correlation coefficients between Alice's bases and Bob's similar to that shown in the Bell test experiments. Maximally entangled photons would result in $|S| = 2\sqrt{2}$. If this were not the case, then Alice and Bob can conclude Eve has introduced local realism to the system, violating Bell's Theorem. If the protocol is successful, the first group can be used to generate keys since those photons are completely anti-aligned between Alice and Bob.

Information reconciliation and privacy amplification

The quantum key distribution protocols described above provide Alice and Bob with nearly identical shared keys, and also with an estimate of the discrepancy between the keys. These differences can be caused by eavesdropping, but also by imperfections in the transmission line and detectors. As it is impossible to distinguish between these two types of errors, guaranteed security requires the assumption that all errors are due to eavesdropping. Provided the error rate between the keys is lower than a certain threshold (20% as of April 2007[3]), two steps can be performed to first remove the erroneous bits and then reduce Eve's knowledge of the key to an arbitrary small value. These two steps are known as **information reconciliation** and **privacy amplification** respectively, and were first described in 1992.[4]

Information reconciliation is a form of error correction carried out between Alice and Bob's keys, in order to ensure both keys are identical. It is conducted over the public channel and as such it is vital to minimise the information sent about each key, as this can be read by Eve. A common protocol used for information reconciliation is the **cascade protocol**, proposed in 1994.[5] This operates in several rounds, with both keys divided into blocks in each round and the parity of those blocks compared. If a difference in parity is found then a binary search is performed to find and correct the error. If an error is found in a block from a previous round that had correct parity then another error must be contained in that block; this error is found and corrected as before. This process is repeated recursively, which is the source of the cascade name. After all blocks have been compared, Alice and Bob both reorder their keys in the same random way, and a new round begins. At the end of multiple rounds Alice and Bob have identical keys with high probability; however, Eve has additional information about the key from the parity information exchanged. However, from a coding theory point of view information reconciliation is essentially source coding with side information, in consequence any coding scheme that works for this problem can be used for information reconciliation. Lately turbocodes,[6] LDPC codes [7] and polar codes [8] have been used for this purpose improving the efficiency of the cascade protocol.

Privacy amplification is a method for reducing (and effectively eliminating) Eve's partial information about Alice and Bob's key. This partial information could have been gained both by eavesdropping on the quantum channel during key transmission (thus introducing detectable errors), and on the public channel during information reconciliation (where it is assumed Eve gains all possibl parity information). Privacy amplification uses Alice and Bob's key to produce a new, shorter key, in such a way that Eve has only negligible information about the new key. This can be done using a universal hash function chosen at random from a publicly known set of such functions, which takes as its input a binary string of length equal to the key and outputs a binary string of a chosen shorter length. The amount by which this new key is shortened is calculated, based on how much information Eve could have gained about the old key (which is known due to the errors this would introduce), in order to reduce the probability of Eve having any knowledge of the new key to a very low value.

Implementations

Experimental

The highest bit rate system currently demonstrated exchanges secure keys at 1 Mbit/s (over 20 km of optical fibre) and 10 kbit/s (ove 100 km of fibre), achieved by a collaboration between the University of Cambridgeand Toshiba using the BB84 protocol with decoy state pulses.[9]

In 2007, Los Alamos National Laboratory/NIST achieved quantum key distribution over a 148.7 km of optic fibre using the BB84 protocol.[10] Significantly, this distance is long enough for almost all the spans found in today's fibre networks. A European collaboration achieved free space QKD over 144 km between two of the Canary Islands using entangled photons (the Ekert scheme) in 2006,[11] and using BB84 enhanced with decoy states[12][13] in 2007.[14]

As of August 2015 the longest distance for optical fiber (307 km)[15] was achieved by University of Geneva and Corning Inc. In the same experiment, a secret key rate of 12.7 kbit/s was generated, making it the highest bit rate system over distances of 100 km.

In June 2017, physicists led by Thomas Jennewein at the Institute for Quantum Computing and the University of Waterloo in Waterloo, Canada achieved the first demonstration of quantum key distribution from a ground transmitter to a moving aircraft. They reported optical links with distances between 3–10 km and generated secure keys up to 868 kilobytes in length.[16]

Also in June 2017, as part of the Quantum Experiments at Space Scale project, Chinese physicists led by Pan Jianwei at the University of Science and Technology of China measured entangled photons over a distance of 1203 km between two ground stations, laying the groundwork for future intercontinental quantum key distribution experiments.[17] Photons were sent from one ground station to the satellite they had named *Micius* and back down to another ground station, where they "observed a survival of two-photon entanglement and a violation of Bell inequality by 2.37 ± 0.09 under strict Einstein locality conditions" along a "summed length varying from 1600 to 2400 kilometers.[18]

Commercial

There are currently four companies offering commercial quantum key distribution systems; ID Quantique (Geneva), MagiQ Technologies, Inc. (New York), QuintessenceLabs (Australia) and SeQureNet (Paris). Several other companies also have active research programs, includingToshiba, HP, IBM, Mitsubishi, NEC and NTT (See External links for direct research links).

In 2004, the world's first bank transfer using quantum key distribution was carried out in Vienna, Austria.[19] Quantum encryption technology provided by the Swiss company Id Quantique was used in the Swiss canton (state) of Geneva to transmit ballot results to the capital in the national election occurring on 21 October 2007.[20] In 2013, Battelle Memorial Institute installed a QKD system built by ID Quantique between their main campus in Columbus, Ohio and their manufacturing facility in nearby Dublin.[21] Field tests of Tokyo QKD network have been underway for some time.[22]

Quantum key distribution networks

DARPA

The DARPA Quantum network,[23] a 10-node quantum key distribution network, has been running since 2004 in Massachusetts, USA. It is being developed by BBN Technologies, Harvard University, Boston University and QinetiQ.

SECOQC

The world's first computer network protected by quantum key distribution was implemented in October 2008, at a scientific conference in Vienna. The name of this network is SECOQC (**Se**cure **Co**mmunication Based on **Q**uantum **C**ryptography) and the EU funded this project. The network used 200 km of standard fibre optic cable to interconnect six locations across Vienna and the town of St Poelten located 69 km to the west.[24]

SwissQuantum

Id Quantique has successfully completed the longest running project for testing Quantum Key Distribution (QKD) in a field environment. The main goal of the SwissQuantum network project installed in the Geneva metropolitan area in March 2009, was to validate the reliability and robustness of QKD in continuous operation over a long time period in a field environment. The quantum layer operated for nearly 2 years until the project was shut down in January 2011 shortly after the initially planned duration of the test.

Chinese networks

In May 2009, a hierarchical quantum network was demonstrated in Wuhu, China. The hierarchical network consisted of a backbone network of four nodes connecting a number of subnets. The backbone nodes were connected though an optical switching quantum router. Nodes within each subnet were also connected though an optical switch, which were connected to the backbone network though a trusted relay.[25]

Launched in August 2016, the QUESS space mission created an international QKD channel between China and the Institute for Quantum Optics and Quantum Information in Vienna, Austria − a ground distance of 7,500 km (4,700 mi), enabling the first intercontinental secure quantum video call.[26][27][28] By October 2017, a 2,000-km fiber line was operational between Beijing, Jinan, Hefei and Shanghai.[29] Together they constitute the world's first space-ground quantum network.[30] Up to 10 Micius/QUESS satellites are expected,[31] allowing a European–Asian quantum-encrypted network by 2020, and a global network by 2030.[32][33]

Tokyo QKD Network

The Tokyo QKD Network[34] was inaugurated on the first day of the UQCC2010 conference. The network involves an international collaboration between 7 partners; NEC, Mitsubishi Electric, NTT and NICT from Japan, and participation from Europe by Toshiba Research Europe Ltd. (UK), Id Quantique (Switzerland) and All Vienna (Austria). "All Vienna" is represented by researchers from the Austrian Institute of Technology (AIT), the Institute for Quantum Optics and Quantum Information (IQOQI) and the University of Vienna.

Los Alamos National Laboratory

A hub-and-spoke network has been operated by Los Alamos National Laboratory since 2011. All messages are routed via the hub. The system equips each node in the network with quantum transmitters—i.e., lasers—but not with expensive and bulky photon detectors. Only the hub receives quantum messages. To communicate, each node sends a one-time pad to the hub, which it then uses to communicate securely over a classical link. The hub can route this message to another node using another one time pad from the second node. The entire network is secure only if the central hub is secure. Individual nodes require little more than a laser: Prototype nodes are around the size of a box of matches.[35]

Attacks and security proofs

Intercept and resend

The simplest type of possible attack is the intercept-resend attack, where Eve measures the quantum states (photons) sent by Alice and then sends replacement states to Bob, prepared in the state she measures. In the BB84 protocol, this produces errors in the key Alice and Bob share. As Eve has no knowledge of the basis a state sent by Alice is encoded in, she can only guess which basis to measure in, in the same way as Bob. If she chooses correctly, she measures the correct photon polarization state as sent by Alice, and resends the correct state to Bob. However, if she chooses incorrectly, the state she measures is random, and the state sent to Bob cannot be the same as the state sent by Alice. If Bob then measures this state in the same basis Alice sent, he too gets a random result—as Eve has sent him a state in the opposite basis—with a 50% chance of an erroneous result (instead of the correct result he would get without the presence of Eve). The table below shows an example of this type of attack.

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	✓		✘			✓		✓

The probability Eve chooses the incorrect basis is 50% (assuming Alice chooses randomly), and if Bob measures this intercepted photon in the basis Alice sent he gets a random result, i.e., an incorrect result with probability of 50%. The probability an intercepted photon generates an error in the key string is then 50% × 50% = 25%. If Alice and Bob publicly compare n of their key bits (thus discarding them as key bits, as they are no longer secret) the probability they find disagreement and identify the presence of Eve is

$$P_d = 1 - \left(\frac{3}{4}\right)^n$$

So to detect an eavesdropper with probability $P_d = 0.999999999$ Alice and Bob need to compare $n = 72$ key bits.

Man-in-the-middle attack

Quantum key distribution is vulnerable to a man-in-the-middle attack when used without authentication to the same extent as any classical protocol, since no known principle of quantum mechanics can distinguish friend from foe. As in the classical case, Alice and Bob cannot authenticate each other and establish a secure connection without some means of verifying each other's identities (such as an initial shared secret). If Alice and Bob have an initial shared secret then they can use an unconditionally secure authentication scheme (such as Carter-Wegman,[36]) along with quantum key distribution to exponentially expand this key, using a small amount of

the new key to authenticate the next session.[37] Several methods to create this initial shared secret have been proposed, for example using a 3rd party[38] or chaos theory.[39] Nevertheless, only "almost strongly universal" family of hash functions can be used for unconditionally secure authentication.[40]

Photon number splitting attack

In the BB84 protocol Alice sends quantum states to Bob using single photons. In practice many implementations use laser pulses attenuated to a very low level to send the quantum states. These laser pulses contain a very small number of photons, for example 0.2 photons per pulse, which are distributed according to a Poissonian distribution. This means most pulses actually contain no photons (no pulse is sent), some pulses contain 1 photon (which is desired) and a few pulses contain 2 or more photons. If the pulse contains more than one photon, then Eve can split off the extra photons and transmit the remaining single photon to Bob. This is the basis of the photon number splitting attack,[41] where Eve stores these extra photons in a quantum memory until Bob detects the remaining single photon and Alice reveals the encoding basis. Eve can then measure her photons in the correct basis and obtain information on the key without introducing detectable errors.

Even with the possibility of a PNS attack a secure key can still be generated, as shown in the GLLP security proof;[42] however, a much higher amount of privacy amplification is needed reducing the secure key rate significantly (with PNS the rate scales as t^2 as compared to t for a single photon sources, where t is the transmittance of the quantum channel).

There are several solutions to this problem. The most obvious is to use a true single photon source instead of an attenuated laser. While such sources are still at a developmental stage QKD has been carried out successfully with them.[43] However, as current sources operate at a low efficiency and frequency key rates and transmission distances are limited. Another solution is to modify the BB84 protocol, as is done for example in the SARG04 protocol,[44] in which the secure key rate scales as $t^{3/2}$. The most promising solution is the decoy state protocol,[45][46][47][48][49] in which Alice randomly sends some of her laser pulses with a lower average photon number. These decoy states can be used to detect a PNS attack, as Eve has no way to tell which pulses are signal and which decoy. Using this idea the secure key rate scales as t, the same as for a single photon source. This idea has been implemented successfully first at the University of Toronto,[50][51] and in several follow-up QKD experiments,[52] allowing for high key rates secure against all known attacks.

Denial of service

Because currently a dedicated fibre optic line (or line of sight in free space) is required between the two points linked by quantum key distribution, a denial of service attack can be mounted by simply cutting or blocking the line. This is one of the motivations for the development of quantum key distribution networks, which would route communication via alternate links in case of disruption.

Trojan-horse attacks

A quantum key distribution system may be probed by Eve by sending in bright light from the quantum channel and analyzing the back-reflections in a Trojan-horse attack. In a recent research study it has been shown that Eve discerns Bob's secret basis choice with higher than 90% probability breaching the security of the system.[53]

Security proofs

If Eve is assumed to have unlimited resources, for example both classical and quantum computing power, there are many more attacks possible. BB84 has been proven secure against any attacks allowed by quantum mechanics, both for sending information using an ideal photon source which only ever emits a single photon at a time,[54] and also using practical photon sources which sometimes emit multiphoton pulses.[42] These proofs are unconditionally secure in the sense that no conditions are imposed on the resources available to the eavesdropper; however, there are other conditions required:

1. Eve cannot physically access Alice and Bob's encoding and decoding devices.

2. The random number generators used by Alice and Bob must be trusted and truly random (for example, a quantum random number generator).
3. The classical communication channel must be authenticated using an unconditionally secure authentication scheme.
4. The message must be encrypted using a one-time pad like scheme.

Quantum hacking

Hacking attacks target vulnerabilities in the operation of a QKD protocol or deficiencies in the components of the physical devices used in construction of the QKD system. If the equipment used in quantum key distribution can be tampered with, it could be made t generate keys that were not secure using a random number generator attack. Another common class of attacks is the Trojan horse attack[55] which does not require physical access to the endpoints: rather than attempt to read Alice and Bob's single photons, Eve sends a large pulse of light back to Alice in between transmitted photons. Alice's equipment reflects some of Eve's light, revealing the state of Alice's basis (e.g., a polarizer). This attack can be detected, e.g. by using a classical detector to check the non-legitimate signals (i.e. light from Eve) entering Alice's system. It is also conjectured that most hacking attacks can similarly be defeated by modifying the implementation, though there is no formal proof.

Several other attacks including faked-state attacks,[56] phase remapping attacks,[57] and time-shift attacks[58] are now known. The time-shift attack has even been demonstrated on a commercial quantum cryptosystem.[59] This is the first demonstration of quantum hacking against a non-homemade quantum key distribution system. Later on, the phase-remapping attack was also demonstrated on a specially configured, research oriented open QKD system (made and provided by the Swiss company Id Quantique under their Quantum Hacking program).[60] It is one of the first 'intercept-and-resend' attacks on top of a widely used QKD implementation in commercial QKD systems. This work has been widely reported in media.[61][62][63][64]

The first attack that claimed to be able to eavesdrop the whole key [65] without leaving any trace was demonstrated in 2010. It was experimentally shown that the single-photon detectors in two commercial devices could be fully remote-controlled using specially tailored bright illumination. In a spree of publications[66][67][68] thereafter, the collaboration between the Norwegian University of Science and Technology in Norway and Max Planck Institute for the Science of Light in Germany, has now demonstrated several methods to successfully eavesdrop on commercial QKD systems based on weaknesses of Avalanche photodiodes (APDs) operating in gated mode. This has sparked research on new approaches to securing communications networks.[69]

Counterfactual quantum key distribution

The task of distributing a secret key could be achieved even when the particle (on which the secret information, e.g. polarization, has been encoded) does not traverse through the quantum channel using a protocol developed by Tae-Gon Noh.[70] Here Alice generates a photon which randomly takes either path (a) or path (b). Path (a) stays inside Alice's secure device and path (b) goes to Bob. By rejecting the photons that Bob receives and only accepting the ones he doesn't receive, Bob & Alice can set up a secure channel, i.e. Eve's attempts to read the *counterfactual* photons would still be detected. This protocol uses the quantum phenomenon whereby the possibility that a photon can be sent has an effect even when it isn't sent. So-called interaction-free measurement also uses this quantum effect, as for example in the bomb testing problem, whereby you can determine which bombs are not duds without setting them off, except in a counterfactual sense.

History

Quantum cryptography was proposed first by Stephen Wiesner, then at Columbia University in New York, who, in the early 1970s, 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 Thomas J. Watson Research Center, and Gilles Brassard, of the

University of Montreal, proposed a method for secure communication based on Wiesner's "conjugate observables". In 1990, Artur Ekert, then a Ph.D. student at Wolfson College, University of Oxford, developed a different approach to quantum key distribution based on peculiar quantum correlations known as quantum entanglement.

Future

The current commercial systems are aimed mainly at governments and corporations with high security requirements. Key distribution by courier is typically used in such cases, where traditional key distribution schemes are not believed to offer enough guarantee. This has the advantage of not being intrinsically distance limited, and despite long travel times the transfer rate can be high due to the availability of large capacity portable storage devices. The major difference of quantum key distribution is the ability to detect any interception of the key, whereas with courier the key security cannot be proven or tested. QKD (Quantum Key Distribution) systems also have the advantage of being automatic, with greater reliability and lower operating costs than a secure human courier network.

Factors preventing wide adoption of quantum key distribution outside high security areas include the cost of equipment, and the lack of a demonstrated threat to existing key exchange protocols. However, with optic fibre networks already present in many countries the infrastructure is in place for a more widespread use.

An Industry Specification Group (ISG) of the European Telecommunications Standards Institute (ETSI) has been set up to address standardisation issues in quantum cryptography.[71] A European Metrology Research Programme project 'Metrology for Industrial Communications' is developing the measurements required to characterise the optical components of faint-pulse QKD systems.[72]

See also

- List of quantum key distribution protocols
- Quantum computing
- Quantum cryptography
- Quantum information science
- Quantum network

References

1. C. E. Shannon , Bell Syst. Tech. J. 28, 656 (1949)
2. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.
3. H. Chau, Physical Review A 66, 60302 (2002) [1] (http://hub.hku.hk/bitstream/123456789/43370/1/75688.pdf)
4. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin "Experimental Quantum Cryptography (http://cs.uccs.edu/~cs691/crypto/BBBSS92.pdf) Journal of Cryptology vol.5, no.1, 1992, pp. 3-28.
5. G. Brassard and L. Salvail "Secret key reconciliation by public discussion" Advances in Cryptology: Eurocrypt 93 Proc. pp 410-23 (1993) [2] (http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.42.9686)
6. Nguyen, Kim-Chi; Van Assche, Gilles; Cerf, Nicolas J. (10–13 October 2004). "Side-Information Coding with Turbo Codes and its Application to Quantum Key Distribution" arXiv:cs/0406001 (https://arxiv.org/abs/cs/0406001). Parma, Italy.
7. D. Elkouss and J. Martinez-Mateo and V. Martin, Quantum Information & Computation 11, 226 (2011) [3] (http://www.dma.fi.upm.es/jmartinez/doc/qic-11-34_0228-0238.pdf)
8. P. Jouguet and S. Kunz-Jacques, Quantum Information and Computation, Vol. 14, No. 3&4, (2013) [4] (https://arxiv.org/pdf/1204.5882v3.pdf)
9. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. Optics Express, Vol. 16, Issue 23, pp. 18790-18979 (http://www.opticsinfobase.org/oe/abstract.cfm?uri=oe-16-23-18790) ([5] (https://arxiv.org/pdf/0810.1069) See also [6] (http://spie.org/x34398.xml?ArticleID=x34398))
10. New Journal of Physics 8 193 (2006) [7] (http://www.iop.org/EJ/article/1367-2630/8/9/193/njp6_9_193.html)

11. R. Ursin, et al. Nature Physics 3, 481 - 486 (2007)[8] (http://lanl.arxiv.org/abs/quant-ph/0607182)
12. Wang, X.-B. (2005). "Beating the photon-number-splitting attack in practical quantum cryptography"*Physical Review Letters*. **94**: 230503. arXiv:quant-ph/0410075 (https://arxiv.org/abs/quant-ph/0410075). Bibcode:2005PhRvL..94w0503W (http://adsabs.harvard.edu/abs/2005PhRvL..94w0503W) doi:10.1103/physrevlett.94.230503 (https://doi.org/10.1103%2Fphysrevlett.94.230503)
13. H.-K. Lo, X. Ma and K. Chen: "Decoy State Quantum Key Distribution". Physical Review Letters 94, 230504 (See also [9] (http://interquanta.biz/qic)
14. T. Schmitt-Manderbach, et al.: "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km (http://xqp.physik.lmu.de/publications/files/articles_2007/prl_98_010504.pdf) Physical Review Letters 98.1 010504 (2007)
15. Korzh, Boris; Lim, Charles Ci Wen; Houlmann, Raphael; Gisin, Nicolas; Li, Ming Jun; Nolan, Daniel; Sanguinetti, Bruno; Thew, Rob; Zbinden, Hugo (2014-07-28). "Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre".*Nature Photonics*. **9**: 163–168. arXiv:1407.7427 (https://arxiv.org/abs/1407.7427) [quant-ph (https://arxiv.org/archive/quant-ph)]. Bibcode:2015NaPho...9..163K (http://adsabs.harvard.edu/abs/2015NaPho...9..163K). doi:10.1038/nphoton.2014.327 (https://doi.org/10.1038%2Fnphoton.2014.327)
16. Pugh, C. J.; Kaiser, S.; Bourgoin, J.-P.; Jin, J.; Sultana, N.; Agne, S.; Anisimova, E.; Makarov, V.; Choi, E.; Higgins, B. L.; Jennewein, T. (2017). "Airborne demonstration of a quantum key distribution receiver payload"*Quantum Science and Technology*. **2**: 024009. arXiv:1612.06396 (https://arxiv.org/abs/1612.06396). Bibcode:2017QS&T....2b4009P (http://adsabs.harvard.edu/abs/2017QS&T...2b4009P). doi:10.1088/2058-9565/aa701f (https://doi.org/10.1088%2F2058-9565%2Faa701f)
17. "China's quantum satellite achieves 'spooky action' at a record distance" (http://www.sciencemag.org/news/2017/06/chinas-quantum-satellite-achieves-spooky-action-record-distance) 2017-06-15. Retrieved 2017-06-15.
18. J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan "Satellite-based entanglement distribution over 1200 kilometers",*Science*, **356** (6343) 1140-4 (2017) doi:10.1126/science.aan3211 (https://doi.org/10.1126%2Fscience.aan3211)
19. http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf (http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf) Archived (https://web.archive.org/web/20130309095431/http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf) 9 March 2013 at the Wayback Machine. *secoqc.net*
20. Jordans, Frank (12 October 2007). "Swiss Call New Vote Encryption System 'Unbreakable'" (https://web.archive.org/web/20071209214958/http://www.technewsworld.com/story/59793.html) technewsworld.com. Archived from the original (http://www.technewsworld.com/story/59793.html) on 2007-12-09. Retrieved 8 March 2013.
21. Dillow, Clay (14 October 2013). "Unbreakable encryption comes to the U.S." (http://tech.fortune.cnn.com/2013/10/14/quantum-key/). fortune.cnn.com.
22. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD Network. Optics Express, Vol. 19, Issue 11, pp. 10387-10409 (2011) http://www.opticsinfobase.org/oe/fulltext.cfm?uri=oe-19-11-10387&id=213840
23. Knight, Will. "Quantum cryptography network gets wireless link" (https://www.newscientist.com/article/dn7484). Retrieved 18 August 2016.
24. "'Unbreakable' encryption unveiled" (http://news.bbc.co.uk/1/hi/sci/tech/7661311.stm) 9 October 2008. Retrieved 18 August 2016 – via bbc.co.uk.
25. Xu, FangXing; Chen, Wei; Wang, Shuang; Yin, ZhenQiang; Zhang, Yang; Liu, Yun; Zhou, Zheng; Zhao, YiBo; Li, HongWei; Liu, Dong (2009), "Field experiment on a robust hierarchical metropolitan quantum cryptography network", *Chinese Science Bulletin*, Springer, **54** (17): 2991–2997, Bibcode:2009ChSBu..54.2991X (http://adsabs.harvard.edu/abs/2009ChSBu..54.2991X) doi:10.1007/s11434-009-0526-3 (https://doi.org/10.1007%2Fs11434-009-0526-3)
26. Lin Xing (16 August 2016). "China launches world's first quantum science satellite" (http://physicsworld.com/cws/article/news/2016/aug/16/china-launches-world-s-first-quantum-science-satellite) *Physics World*. Institute of Physics Retrieved 17 August 2016.
27. "First Quantum Satellite Successfully Launched" (http://www.oeaw.ac.at/en/events-communication/public-relations-communication/public-relations-communication/ausgewaehlte-oeaw-pressemeldungen/press-releases/first-quantum-satellite-successfully-launched/) *Austrian Academy of Sciences* 16 August 2016. Retrieved 17 August 2016.
28. Wall, Mike (16 August 2016). "China Launches Pioneering 'Hack-Proof' Quantum-Communications Satellite" (http://www.space.com/33760-china-launches-quantum-communications-satellite.html) *Space.com*. Purch. Retrieved 17 August 2016.

29. "Is China the Leader in Quantum Communications?" (https://www.insidescience.org/news/china-leader-quantum-communications). *IEEE*. 19 January 2018. Retrieved 19 March 2018.
30. "China Demonstrates Quantum Encryption By Hosting a Video Call" (https://spectrum.ieee.org/tech-talk/telecom/security/china-successfully-demonstrates-quantum-encryption-by-hosting-a-video-call). *IEEE*. 3 October 2017. Retrieved 17 March 2018.
31. "A quantum communications satellite proved its potential in 2017" (https://www.sciencenews.org/article/global-quantum-communication-top-science-stories-2017-yir). *Science News*. 3 October 2017. Retrieved 19 March 2018.
32. huaxia (16 August 2016). "China Focus: China's space satellites make quantum leap" (http://news.xinhuanet.com/english/2016-08/16/c_135604287.htm). Xinhua. Retrieved 17 August 2016.
33. Jeffrey Lin; P.W. Singer; John Costello (3 March 2016). "China's Quantum Satellite Could Change Cryptography Forever" (http://www.popsci.com/chinas-quantum-satellite-could-change-cryptography-forever). *Popular Science*. Retrieved 17 August 2016.
34. Tokyo QKD Network unveiled at UQCC 2010 (http://www.uqcc2010.org/highlights/index.html)
35. Hughes, Richard J.; Nordholt, Jane E.; McCabe, Kevin P.; Newell, Raymond T.; Peterson, Charles G.; Somma, Rolando D. (2013). "Network-Centric Quantum Communications with Application to Critical Infrastructure Protection" arXiv:1305.0305 (https://arxiv.org/abs/1305.0305) [quant-ph (https://arxiv.org/archive/quant-ph)].
36. M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," Journal of Computer and System Sciences", 22, pp 265-279, (1981)
37. Romain Alleaume, et al. "SECOQC White Paper on Quantum Key Distribution and Cryptography" arXiv:quant-ph/0701168v1 pp. 7 (2007) [10] (https://arxiv.org/abs/quant-ph/0701168)
38. Zhang, Z.; Liu, J.; Wang, D.; Shi, S. (2007). "Quantum direct communication with authentication" *Phys. Rev. A*. **75**: 026301. arXiv:quant-ph/0604125 (https://arxiv.org/abs/quant-ph/0604125). Bibcode:2007PhRvA..75b6301Z (http://adsabs.harvard.edu/abs/2007PhRvA..75b6301Z) doi:10.1103/physreva.75.026301 (https://doi.org/10.1103%2Fphysreva.75.026301).
39. D. Huang, Z. Chen, Y. Guo and M. Lee "Quantum Secure Direct Communication Based on Chaos with Authentication", Journal of the Physical Society of Japan Vol. 76 No. 12, 124001 (2007) ("Archived copy" (https://web.archive.org/web/20120305062319/http://jpsj.ipap.jp/link?JPSJ%2F76%2F124001%2F). Archived from the original (http://jpsj.ipap.jp/link?JPSJ%2F76%2F124001%2F) on 5 March 2012. Retrieved 6 February 2016.)
40. "5. Unconditionally secure authentication" (http://www.lysator.liu.se/~jc/mthesis/5_Unconditionally_secure_au.html) Retrieved 18 August 2016.
41. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. "Limitations on practical quantum cryptography." Physical Review Letters, 85(6):1330+ (2000)
42. D. Gottesman, H.-K. Lo, N. L¨utkenhaus, and J. Preskill, Quant. Inf. Comp. 4, 325 (2004)
43. P. M. Intallura, M. B. Ward, O. Z. Karimov, Z. L. Yuan, P. See, A. J. Shields, P. Atkinson, and D. A. Ritchie, Appl. Phys. Lett. 91, 161103 (2007)
44. V. Scarani, A. Ac´ın, G. Ribordy and N. Gisin, Phys. Rev. Lett. 92, 057901 (2004)
45. W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003)
46. X.-B. Wang, "Beating the photon-number-splitting-attack in practical quantum cryptography", Physical Review Letters, 94, 230503 (2005)
47. S. H. Shams Mousavi, P. Gallion, "Decoy-state quantum key distribution using homodyne detection" (http://journals.aps.org/pra/abstract/10.1103/PhysRevA.80.012327), Phys. Rev. A 80, 012327 (2009)
48. Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, "Decoy State Quantum Key Distribution" (https://archive.is/20120712103031/http://prl.aps.org/abstract/PRL/v94/i23/e230504), Physical Review Letters, 94, 230504 (2005)
49. Xiongfeng Ma, Bing Qi, Y. Zhao, and Hoi-Kwong Lo, "Practical decoy state for quantum key distribution" (https://archive.is/20120717025134/http://pra.aps.org/abstract/PRA/v72/i1/e012326), Phys. Rev. A 72, 012326 (2005)
50. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett., 96, 070502 (2006).
51. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, in Proc. IEEE ISIT, pp. 2094--2098 (2006).
52. Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. 90, 011118 (2007)
53. Jain, N.; et al. (2014). "Trojan-horse attacks threaten the security of practical quantum cryptography" (https://arxiv.org/pdf/1406.5813v1.pdf) (PDF). *New Journal of Physics* **16**: 123030. arXiv:1406.5813 (https://arxiv.org/abs/1406.5813). Bibcode:2014NJPh...16l3030J (http://adsabs.harvard.edu/abs/2014NJPh...16l3030J) doi:10.1088/1367-2630/16/12/123030 (https://doi.org/10.1088%2F1367-2630%2F16%2F12%2F123030)

54. P. W. Shor and J. Preskill, Physical Review Letters 85, 441 (2000)
55. Vakhitov, A. V. Makarov and D. R. Hjelme, J.Mod. Opt. 48, 2023 (2001)
56. V. Makarov and D. R. Hjelme, J. Mod. Opt. 52, 691. (2005)
57. C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev A 75, 032314. (2007)
58. B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Info. Compu. 7, 43 (2007)
59. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H-K. Lo, Phys. Rev. A 78:042333 (2008)
60. F. Xu, B. Qi, and H.-K. Lo, New J. Phys. 12, 113026 (2010)
61. Quantum crypto bofins in successful backdoor sniff - Erroneous error-handling undermines bulletproofness (https://www.theregister.co.uk/2010/05/18/quantum_crypto_attack/) Retrieved 2010-05-26
62. Merali, Zeeya (20 May 2010). "Quantum crack in cryptographic armour" (http://www.nature.com/news/2010/100520/full/news.2010.256.html) *Nature*. doi:10.1038/news.2010.256 (https://doi.org/10.1038%2Fnews.2010.256) Retrieved 18 August 2016 – via www.nature.com.
63. "Light fantastic" (http://www.economist.com/node/16681905) *The Economist*. 26 July 2010.
64. Quantum cryptography system hacked - physicsworld.com (http://physicsworld.com/cws/article/news/42667)
65. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, Nat. Photonics 4, 686 (2010)
66. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, Opt. Exp. 18, 27938 (2010)
67. C. Wiechers, L. Lydersen, C.Wittmann, D. Elser, J. Skaar, Ch. Marquardt, V. Makarov and G. Leuchs, New J. Phys. 13, 013043 (2011)
68. N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, Ch. Marquardt, V. Makarov and G. Leuchs, Phys. Rev Lett. 107, 110501 (2011)
69. Richard Hughes and Jane Nordholt (16 September 2011). "Refining Quantum Cryptography". *Science*. **333** (6049): 1584–6. Bibcode:2011Sci...333.1584H (http://adsabs.harvard.edu/abs/2011Sci...333.1584H) doi:10.1126/science.1208527 (https://doi.org/10.1126%2Fscience.1208527) PMID 21921186 (https://www.ncbi.nlm.nih.gov/pubmed/21921186)
70. Tae-Gon Noh, *Counterfactual Quantum Cryptography*, Physical Review Letters, 103, Issue 23, 230501 (2009) serves to explain how this non-intuitive or counterfactual idea actually works.
71. "ETSI - Quantum Key Distribution" (http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution) *etsi.org*. 2014. Retrieved 28 July 2014.
72. "MIQC - European Metrology Research Programme (EMRP)" (http://projects.npl.co.uk/MIQC/index.html) *projects.npl.co.uk*. 2014. Retrieved 28 July 2014.

External links

General and review

- Quantum Computing 101
- Scientific American Magazine (January 2005 Issue) Best-Kept Secrets Non-technical article on quantum cryptography
- Physics World Magazine (March 2007 Issue) Non-technical article on current state and future of quantum communication
- arXiv:0802.4155 (quant-ph) February 2008 review of Quantum Cryptography
- arXiv:quant-ph/0702202v3 March 2007 review of Quantum Cryptography
- SECOQC White Paper on Quantum Key Distribution and Cryptography European project to create a large scale quantum cryptography network, includes discussion of current QKD approaches and comparison with classical cryptography
- The future of cryptography May 2003 Tomasz Grabowski
- ARDA Quantum Cryptography Roadmap
- Lectures at the Institut Henri Poincaré (slides and videos)
- Interactive quantum cryptography demonstration experiment with single photons for education

More specific information

- Ekert, Artur. "Cracking codes, part II | plus.maths.org". Pass.maths.org.uk. Retrieved 2013-12-28. Description of entanglement based quantum cryptography from Artur Ekert.
- Xu, Qing (2009). *Optical Homodyne Detections and Applications in Quantum Cryptography* (PDF) (Thesis). Paris: Télécom ParisTech. Retrieved 14 February 2017.
- "Quantum Cryptography and Privacy Amplification". Ai.sri.com. Retrieved 2013-12-28. Description of BB84 protocol and privacy amplification by Sharon Goldwater
- Original conference paper on the BB84 Protocol for Quantum Cryptography archived in the 2014 Theoretical Computer Science issue celebrating 30 years of BB84 - [11]
- Public debate on the Security of Quantum Key Distribution at the conference HotTopics in Physical Informatics, 11 November 2013

Further information

- Quantiki.org - Quantum Information portal and wiki
- Interactive BB84 simulation

Quantum key distribution simulation

- Online Simulation and Analysis Toolkit for Quantum Key Distribution

Quantum cryptography research groups

- Experimental Quantum Cryptography with Entangled Photons
- NIST Quantum Information Networks
- Free Space Quantum Cryptography
- Experimental Continuous Variable QKD, MPL Erlangen
- Experimental Quantum Hacking, MPL Erlangen
- Quantum cryptography lab. Pljonkin A.P.

Companies selling quantum devices for cryptography

- id Quantique sells Quantum Key Distribution products
- MagiQ Technologies sells quantum devices for cryptography
- QuintessenceLabs Solutions based on continuous wave lasers
- SeQureNet sells Quantum Key Distribution products using continuous-variables

Companies with quantum cryptography research programmes

- Toshiba
- Hewlett Packard
- IBM
- Mitsubishi
- NEC
- NTT
