A Quantum Leap for Cryptography

Introduction

Classical physics is adequate for the description of macroscopic objects. It applies basically to systems larger than one micron (1 micron = 1 millionth of a meter). It was developed gradually and was basically complete by the end of the XIXth century.
At that time, the fact that classical physics did not always provide an adequate description of physical phenomena became clear. A radically new set of theories, quantum physics, was consequently developed by physicists such as Max Planck and Albert Einstein, during the first thirty years of the XXth century. Quantum physics describes adequately the microscopic world (molecules, atoms, elementary particles), while classical physics remains accurate for macroscopic objects. The predictions of quantum physics drastically differ from those of classical physics. For example, it features intrinsic randomness, while classical physics is deterministic. It also imposes limitation on the accuracy of the measurement that can be performed on a system (Heisenberg's uncertainty principle).
Although quantum physics had a strong influence on the technological development of the XXth century – it allowed for example the invention of the transistor or the laser – its impact on the processing of information has only been understood recently. “Quantum information processing” is a new and dynamic research field at the crossroads of quantum physics and computer science. It looks at the consequence of encoding digital bits – the elementary units of information – on quantum system. Does it make a difference if a bit is written on a piece of paper, stored in an electronic chip, or encoded on a single electron? Applying quantum physics to information processing yields revolutionary properties and possibilities, without any equivalent in conventional information theory. In order to emphasize this difference, a digital bit is called a quantum bit or a "qubit" in this context. With the miniaturization of microprocessors, which will reach the quantum limit in the next fifteen to twenty years, this new field will necessarily become more and more prominent. Its ultimate goal is the development of a fully quantum computer, possessing massively parallel processing capabilities.
Although this goal is still quite distant, the first applications of quantum information processing have recently been introduced by id Quantique, a spin-off company of the university of Geneva. The first one, the generation of random numbers, will only be briefly mentioned in this paper. It exploits the fundamentally random nature of quantum physics to produce high quality random numbers, for cryptographic applications for example. id Quantique's QRNG is the first commercial product based on this principle. The second application, called quantum cryptography, exploits Heisenberg's uncertainty principle to allow two remote parties to exchange a cryptographic key. It is the main focus of this paper.

Cryptography

Cryptography is the art of rendering information exchanged between two parties unintelligible to any unauthorized person. Cryptography is an old science. However, until the development of electronic and optical telecommunications, its scope of applications remained mainly restricted to military and diplomatic purposes. In the past twenty-five years, cryptography evolved, from its status of "classified" science and offers now solutions to guarantee the secrecy of the ever-expanding civilian telecommunication networks. Although confidentiality – the focus of this paper – is the traditional application of cryptography, it is used nowadays to achieve broader objectives, such as authentication, digital signatures and non-repudiation[1].
The way cryptography works can be illustrated with Fig. 1. Before transmitting sensitive information, the sender – traditionally called Alice – combines the plain text with a secret key, using some encryption algorithm, to obtain the cipher text. This scrambled message can now be sent to the recipient – Bob – who reverses the process to recover the plain text by combining the cipher text with the secret key using the decryption algorithm. An eavesdropper – Eve – cannot deduce the plain message from the scrambled one, without knowing the key. To illustrate this principle, imagine that Alice puts her message in a safe and locks it with a key. Bob uses in turn his key to unlock the safe.
Numerous encryption algorithms exist. Their relative security essentially depends on the length of the key they use: the more bits the key contains, the better

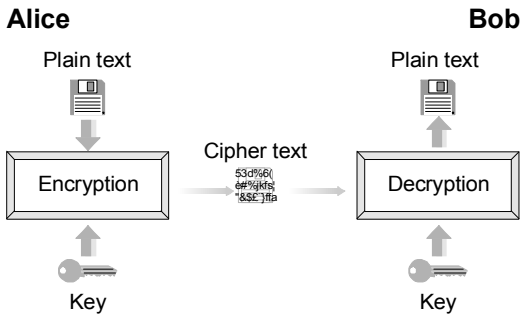


Figure 1: Principle of cryptography.

the security. One of the most common algorithm – the Data Encryption Standard or DES – has a 56 bits key. Since it can be cracked in a few hours with powerful computers, it is not considered secure any longer and will shortly be replaced by the Advanced Encryption Standard – AES – which has a 256 bits key. In addition to its length, the amount of information encrypted with a given key also

[1] “The codebook”, Simon Singh, *Fourth Estate*, presents an excellent non-technical introduction and historical perspective on cryptography.

influences the confidentiality of the scheme: the more often a key is changed, the better the security. In the very special case where the key is as long as the plain text and used only once – this scheme is called the "one-time pad" – it can be shown that decryption is simply impossible and that the scheme is absolutely secure.
As one usually assumes that the encryption algorithm is disclosed, the secrecy of such a scheme basically depends on the fact that the key is secret. This means first that the key generation process must be appropriate, in the sense that it must not be possible for a third party to guess or deduce it. Truly random numbers must thus be used as key. Second, it must not be possible for a third party to intercept the key during its exchange between Alice and Bob. This so-called "key distribution problem" is very central in cryptography.

One-way functions

The most common example of a one-way function is factorization. The RSA public key system is actually based on this mathematical problem. It is relatively easy to compute the product of two integers – say for example 37 × 53 = 1961, because a practical method exists. On the other hand, reversing this calculation – finding the prime factors of 1961 – is tedious and time-consuming. No efficient algorithm for factorization has ever been disclosed. It is important to stress however that there is no formal proof that such an algorithm does not exist. It may not have been discovered yet or… it may have been kept secret.

Key distribution

For years, it was believed that the only possibility to solve this key distribution problem was for Alice to send to Bob some physical medium – a disk for example – containing the key. In the digital era, this requirement is clearly unpractical. In addition, it is not possible to check whether this medium was intercepted – and its content copied – or not.
In the late sixties and early seventies, researchers of the British "Government Communication Headquarters" (GCHQ) invented an algorithm solving this problem. To take an image, it is as if they replaced the safe mentioned above by a padlock. Before the communication, Bob sends an open padlock to Alice, while keeping the key. Alice uses it to lock the data. Bob is the only one who can unlock the data with the key he kept. "Public key cryptography" was born. This invention however remained classified and was independently rediscovered in the mid-seventies by American researchers. Formally, these padlocks are mathematical functions called "one-way functions", because they are easy to compute but difficult to reverse (see Box). As public key cryptography algorithms require complex calculations, they are slow. They can thus not be used to encrypt large amount of data and are exploited in practice to exchange between Alice and Bob a short session key for a secret-key algorithm such as DES.
In spite of the fact that it is extremely practical, the exchange of keys using public key cryptography however suffers from two major flaws. First, it is vulnerable to technological progress. Reversing a one-way function can be done, provided one has a computer sufficiently powerful or enough time. The resources necessary to crack an algorithm depend on the length of the key, which must thus be selected carefully. One must indeed assess the technological progress over the course of the time span during which the data encrypted will be valuable. Eve can indeed record communications and wait until she can afford a computer powerful enough to crack them. This assessment is straightforward when the lifetime of the information is one or two years, as in the case of credit card numbers, but quite difficult when it spans a decade. In 1977, the three inventors of RSA – the most common public key cryptography algorithm – issued a challenge to crack a cipher encrypted with a 129 decimal digits key (428 bits). They predicted at the time that this might not occur over 40 quadrillion years. The 100$ prize was claimed in 1994 by a group of scientists working over the internet. Besides, it has been shown theoretically that a quantum computer, if it existed, could, with its massively parallel processing abilities, reverse one-way functions and crack public key cryptography. The development of the first quantum computer will consequently immediately make the exchange of a key with public key algorithms insecure.
The second flaw is the fact that public key cryptography is vulnerable to progress in mathematics. In spite of tremendous efforts, mathematicians have not been able yet to prove that public key cryptography is secure. It is has not been possible to rule out the existence of algorithms that allow reversing one-way functions. The discovery of such an algorithm would make public key cryptography insecure overnight. It is even more difficult to assess the rate of theoretical progress than that of technological advances. There are examples in the history of mathematics where one person was able to solve a problem, which kept busy other researchers for years of decades. It took for example half an hour to Clifford Cocks, of the GCHQ, to invent all the mathematics of public key cryptography. It is even possible that such an algorithm has already been discovered, but is kept secret. These two threats imply that public key cryptography cannot securely solve the key exchange problem.

Quantum Cryptography

Principle

Quantum cryptography solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security guaranteed by the laws of physics. This key can then be used with conventional cryptographic algorithms. Hence, "quantum key distribution" is a better name for this technology.
Contrary to what one could expect, the basic principle of quantum cryptography is quite straightforward. It exploits the fact, that according to quantum physics, the mere fact of observing a system will perturb it in an irreparable way. When you read this article for example, the sheet of paper must be lighted. The impact of the light particles will slightly heat it up and hence change it. This effect is very small on a piece of paper, which is a

macroscopic object. However, the situation is radically different with a microscopic object: if one encodes the value of a digital bit on a single quantum system, an interception will necessarily translate into a perturbation, because the eavesdropper is forced to observe it. This perturbation causes errors in the sequence of bits shared by Alice and Bob. By checking the presence of such errors, the two parties can verify whether their key was intercepted or not. It is important to stress that since this verification takes place after the exchange of bits, one finds out a posteriori whether the communication was eavesdropped or not. That is why this technology is used to exchange a key and not valuable information. Once the key is validated, it can be used to encrypt data. Finally, it is important to insist on the fact that it is impossible to intercept the key without introducing perturbations.

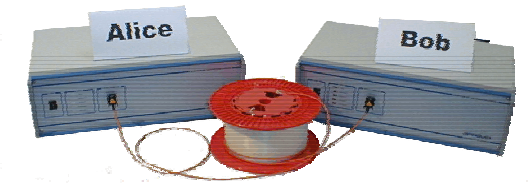


Figure 2: id Quantique's quantum cryptography system.

In practice

What does it mean in practice to encode the value of a digital bit on a quantum system? In telecommunications, light is routinely used to exchange information. For each bit of information, a pulse is emitted and sent down an optical fiber to the receiver where it is registered and transformed back into an electronic form. These pulses typically contain millions of particles of light, called photons. In quantum cryptography, one can follow the same approach, with the only difference that the pulses contain only a single photon. A single photon represents a very tiny amount of light (when reading this article your eyes register billions of photons every second) and follows the laws of quantum physics. In particular, it cannot be split into halves. This means that an eavesdropper cannot take half of a photon to measure the value of the bit it carries, while letting the other half continue its course. If he wants to obtain the value of the bit, he must detect the photon and will thus interrupt the communication and reveal its presence. A more clever strategy is for the eavesdropper to detect the photon, register the value of the bit and prepare a new photon according to the obtained result to send it to the receiver. In quantum cryptography, Alice and Bob cooperate to prevent the Eve from doing this, by forcing her to introduce errors (see Box).

Real world

Does quantum cryptography work in the real world? It does. The prototype developed by id Quantique (see Fig. 2) was tested over standard optical fibers part of the network of Swisscom – a Swiss telecommunication company. It allows exchanging a key between two stations – Alice and Bob – over an optical fiber. The devices are controlled by two PC's through the USB port.

The first important characteristic of a quantum cryptography system is the key exchange rate. It is low compared to the bit rates common in conventional telecommunication. id Quantique's prototype can typically exchange a thousand bits per second. This low bit rate is the price to pay for absolute secrecy. This limitation is not as critical as it may look at first. The bits exchanged using quantum cryptography constitute a key, which is then used to encrypt data. These data can then be exchanged over a conventional channel at a high rate. Using quantum cryptography, a 256 bits key can typically be changed four times a second. An additional important advantage of this technology is that a key can be generated on demand when it is needed, simplifying key management and making its storage useless.

Key transmission distance: the main limitation?

The second important characteristic of a quantum cryptography system is the transmission distance. Optical fibers, in spite of their very high quality, are not perfectly transparent. When propagating, a photon will sometimes get absorbed and thus not reach the end of the fiber. In conventional telecommunications, one deals with this problem by using devices called optical repeaters. They are located approximately every 80 km and amplify the signal. In quantum cryptography, it is not possible to use such repeaters. They would indeed have the same effect as an eavesdropper and corrupt the key by introducing perturbations[2]. Consequently the key exchange rate decreases with distance because less and less photon reach the end of the fiber. The fact that some photons are absorbed in the fiber does not constitute a problem, because they just do not enter in the final key. However, eventually when the distance becomes too long, the number of photons that reach the receiver end just becomes too small to allow a key exchange.

With present technology, the distance is thus limited to about 70 km. id Quantique's prototype was recently used to exchange keys over 67 km of standard installed optical fiber between the Swiss cities of Geneva and Lausanne (see Fig. 3).

Figure 3: id Quantique's system exchanged keys over 67 km of standard optical fiber.

[2] Note that if it were possible to use repeaters, an eavesdropper could exploit them. The laws of quantum physics forbid this.

It is clear that this distance can be increased by chaining quantum cryptography links with secure – Eve should not have access to them – secure intermediary stations. Another way to increase the distance is to get rid of the optical fiber. It is possible to exchange a key using quantum cryptography between a terrestrial station and a low orbit satellite (Absorption in the atmosphere takes place mainly over the first few kilometers. It can be kept very low by choosing an adequate wavelength… provided the weather is good.). Such a satellite moves with respect to the earth surface. When passing over a second station, located thousands of kilometers away from the first one, it can retransmit the key. The satellite is implicitly considered as a secure intermediary station. This technology is less mature than that based on optical fibers. Research groups have already performed preliminary tests of such a system, but an actual key exchange with a satellite remains to be done.

There are also several theoretical proposals for building quantum repeaters. They would relay qubits without measuring and thus perturbing them. They could, in principle, be used to extend the key exchange range over arbitrarily long distances. In practice, such quantum repeaters do not exist yet, not even in laboratories, and much research remains to be done.

Implementation and applications

Quantum cryptography is mature enough to allow the exchange of a key over an optical fiber between two locations separated by a distance up to about 70 km. This key can then be used to secure all the communications (voice and data) between these two sites. The distance limitation restricts, initially at least, the application of this technology to metropolitan area networks. It can for example be used between the offices of a financial institution located in a downtown area and its backoffice or archive center in the suburbs. It can also be used between ministers and government offices within a capital.

Conclusion

For the first time in history, the security of encryption technology does not depend on the computer resources of the adversary. It is guaranteed in an absolute way by the laws of quantum physics. This quantum leap in security is made possible by quantum cryptography.

References are available on www.idquantique.com

Principle

The value of each bit is encoded on the property of a photon, its polarization for example. The polarization of a photon is the oscillation direction of its electric field. It can be, for example, vertical, horizontal, or diagonal (+45° and -45°).

Alice and Bob agree that:

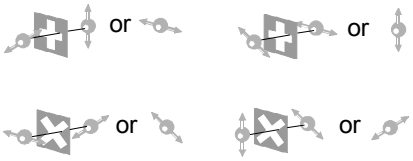
"0" = or

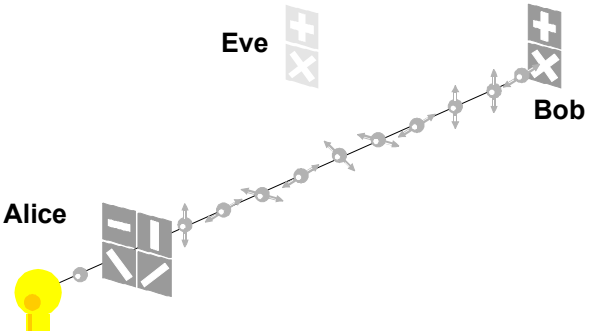
"1" = or

A filter can be used to distinguish between horizontal and vertical photons; another one between diagonal photons (+45° and -45°).

When a photon passes through the correct filter, its polarization does not change.

When a photon passes through the incorrect filter, its polarization is modified randomly.





1. For each key bit, Alice sends a photon, whose polarization is randomly selected. She records these orientations.
2. For each incoming photon, Bob chooses randomly which filter he uses. He writes down its choice as well as the value he records.

   If Eve tries to spy on the photon sequence, she modifies their polarization.
3. After all the photons have been exchanged, Bob reveals, over a conventional channel - the phone for example - to Alice the sequence of filters he used.

   If Eve listens to their communication, she cannot deduce the key.
4. Alice tells Bob in which cases he chose the correct filter.
5. Alice and Bob now know in which cases their bits should be identical - when Bob used the correct filter. These bits form the final key.
6. Finally, Alice and Bob check the error level of the final key to validate it.

id Quantique
Rue Cingria 10, CH-1205 Genève
Ph: +41 (0)22 379 69 29 Fax: +41 22 781 09 80
www.idquantique.com