

id Quantique
White Paper

Understanding Quantum Cryptography

Version 1.0

April 2005



id Quantique SA
Ch. de la Marbrerie, 3
1227 Carouge/Geneva
Switzerland

Tel: +41 (0)22 301 83 71
Fax: +41 (0)22 301 83 79
www.idquantique.com
info@idquantique.com

Information in this document is subject to change without notice.

Copyright © 2005 id Quantique SA. Printed in Switzerland.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means – electronic, mechanical, photocopying, recording or otherwise – without the permission of id Quantique.

Trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. id Quantique SA disclaims any proprietary interest in the trademarks and trade names other than its own.

Table of contents

1. Introduction	5
2. Cryptography	5
3. Key Distribution	7
4. Quantum Cryptography	8
Principle.....	8
Quantum Communications.....	8
Quantum Cryptography Protocols.....	8
Key Distillation	10
Real World Quantum Cryptography	10
Perspectives for Future Developments.....	12
5. Conclusion.....	12



Vectis Link Encryptors offer :

- ✓ Security against optical fibre cable tapping
- ✓ Strong cryptography
- ✓ Automated operation
- ✓ Eavesdropping revealed

Box 1: More information on Quantum Cryptography

- Future-proof Data Confidentiality with Quantum Cryptography – for a discussion of the importance of quantum cryptography for an organization.
- Securing Networks with the Vectis Quantum Link Encryptor – for information about practical applications of quantum cryptography and how it can be deployed in an existing network.
- Quantum Cryptography, Review Article– for more information on the scientific aspects, both theoretical and experimental, of quantum cryptography.
- Vectis Product Family Specification Sheets – for technical information on the Vectis Quantum Link Encryptor.

These documents are available online from www.idquantique.com.

1. Introduction

Classical physics is adequate for the description of macroscopic objects. It applies 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. Quantum physics features, for example, intrinsic randomness, while classical physics is deterministic. It also imposes limitation on the accuracy of the measurements 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 objects. 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 gain prominence. 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 are already commercialized by id Quantique. 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 Quantis quantum random number generator 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.

For more information on quantum information processing and quantum cryptography, refer to the documents listed in Box 1.

2. Cryptography

Cryptography is the art of rendering information exchanged between two parties unintelligible to any unauthorized person. Although it is an old science, its scope of applications remained mainly restricted to military and diplomatic purposes until the development of electronic and optical telecommunications. In the past twenty-five years, cryptography evolved out of its status of “classified” science and offers now solutions to guarantee the secrecy of the ever-expanding civilian telecommunication networks. Although confidentiality is the traditional application of cryptography, it is used nowadays to achieve broader objectives, such as authentication, digital signatures and non-repudiation¹.

The way cryptography works is illustrated in Fig. 1. Before transmitting sensitive information, the sender combines the plain text with a secret key, using some encryption algorithm, to obtain the cipher text. This scrambled message is then sent to the recipient who reverses the process to recover the plain text by combining the cipher text with the secret key using the decryption algorithm. An eavesdropper cannot deduce the plain message from the scrambled one without

¹ For a comprehensive discussion of cryptography, refer to “Applied Cryptography”, Bruce Schneier, *Wiley*. “The codebook”, Simon Singh, *Fourth Estate*, presents an excellent non-technical introduction and historical perspective on cryptography.

knowing the key. To illustrate this principle, imagine that the sender puts his message in a safe and locks it with a key. The recipient uses in turn a copy of the key, which he must have in his possession, to unlock the safe.

Numerous encryption algorithms exist. Their relative strengths essentially depends on the length of the key they use. The more bits the key contains, the better the security. The DES algorithm – Data Encryption Standard – played an important role in the security of electronic communications. It was adopted as a standard by the US federal administration in 1976. The length of its keys is however only 56 bits. Since it can nowadays be cracked in a few hours, it is not considered secure any longer. It has been replaced recently by the Advanced Encryption Standard – AES – which has a minimum key length of 128 bits. In addition to its length, the amount of information encrypted with a given key also influences the strength 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 for the key. Box 2 describes a quantum random number generator. Second, it must not be possible for a third party to intercept the key during its exchange between the sender and the recipient. This so-called “key distribution problem” is very central in cryptography.

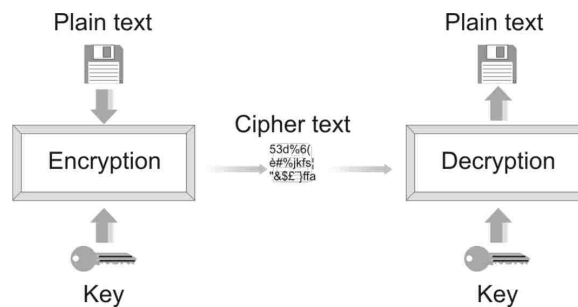
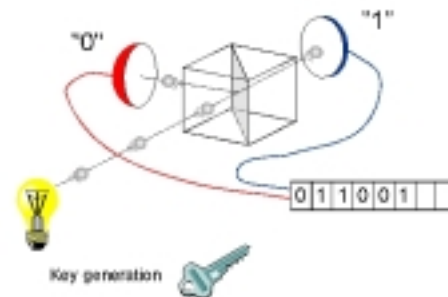


Figure 1: Principle of cryptography

Box 2: Quantum Random Number Generators

Classical physics is deterministic. If the state of a system is known, physical laws can be used to predict its evolution. On the contrary, the outcome of certain phenomena is, according to quantum physics, fundamentally random. One such phenomenon is the reflection or transmission of an elementary light “particle” – a photon – on a semi-transparent mirror. In such a case, the photon is transmitted or reflected by the mirror with a probability of 50%. It is thus completely impossible for an observer to predict the outcome. Because of this intrinsic randomness, it is natural to use this phenomenon to generate strings of random numbers. Quantis is a quantum random number generator exploiting this principle.



Single photons hitting a semi-transparent mirror will be transmitted or reflected with a probability of 50%.



Quantis, id Quantique’s Quantum Random Number Generators, provide truly random numbers at an unsurpassed bit-rate of 16Mbits/sec.

3. Key Distribution

For years, it was believed that the only possibility to solve the key distribution problem was to send 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, the intended recipient sends an open padlock to the party that will be sending valuable information, while keeping its key. The sender uses this open padlock to protect the data. The recipient is then 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 expressions called "one-way functions", because they are easy to compute but difficult to reverse (see Box 3). 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 short sessions keys for secret-key algorithms such as AES.

Box 3: 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 $37 \times 53 = 1961$, 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.

In spite of the fact that it is extremely practical, the exchange of keys using public key cryptography suffers from two major flaws. First, it is vulnerable to technological progress. Reversing a one-way function can be done, provided one has sufficient computing power or time available. 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. In principle, an eavesdropper could indeed record communications and wait until he 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 in an article entitled "A new kind of cipher that would take million of years to break" a challenge to crack a cipher encrypted with a 428-bits key. They predicted at the time that this might not occur before 40 quadrillion years. The 100\$ prize was however claimed in 1994 by a group of scientists who worked over the Internet. Besides, Peter Shor has proposed in 1994 an algorithm, which would run on a quantum computer² and allow to reverse one-way functions, to 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 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 or decades. It is even possible that an algorithm for reversing one-way functions has already been discovered, but kept secret. These threats simply mean that public key cryptography cannot guarantee future-proof key distribution.

² Quantum computers are computers that exploit the laws of quantum physics to process information. They are still in the realm of experimental research, but will eventually be built.

4. Quantum Cryptography

4.1 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. One may thus claim, with some merit, that “quantum key distribution” may be a better name for quantum cryptography.

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 quantum object perturbs 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 object, its interception will necessarily translate into a perturbation, because the eavesdropper is forced to observe it. This perturbation causes errors in the sequence of bits exchanged by the sender and recipient. By checking for 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. Quantum physics allows to prove that interception of the key without perturbation is impossible.

4.2 Quantum Communications

What does it mean in practice to encode the value of a digital bit on a quantum object? In telecommunication networks, light is routinely used to exchange information. For each bit of information, a pulse is emitted and sent down an optical fiber – a thin fiber of glass used to carry light signals – to the receiver, where it is registered and transformed back into an electronic signal. 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 observe the photon and will thus interrupt the communication and reveal his 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, the two legitimate parties cooperate to prevent the eavesdropper from doing so, by forcing him to introduce errors. Protocols have been devised to achieve this goal.

4.3 Quantum Cryptography Protocols

Although several exist, a single quantum cryptography protocol will be discussed here. This is sufficient to illustrate the principle of quantum cryptography. The BB84 protocol was the first to be invented in 1984 by Charles Bennett of IBM Research and Gilles Brassard of the University of Montreal. In spite of this, it is still widely used and has become a de facto standard.

An emitter and a receiver can implement it by exchanging single-photons, whose polarization states are used to encode bit values (refer to Box 4 for an explanation of what polarization is) over an optical fiber. This fiber, and the transmission equipment, is called the quantum channel. They use four different polarization states and agree, for example, that a 0-bit value can be encoded either as a horizontal state or a -45° diagonal one (see Box 5). For a 1-bit value, they will use either a vertical state or a $+45^\circ$ diagonal one.

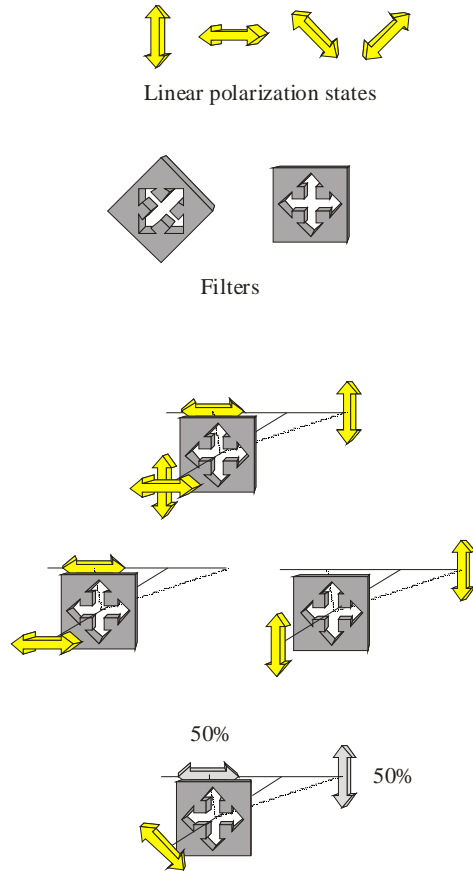
- For each bit, the emitter sends a photon whose polarization is randomly selected among the four states. He records the orientation in a list.
- The photon is sent along the quantum channel.
- For each incoming photon, the receiver randomly chooses the orientation – horizontal or diagonal – of a filter allowing to distinguish between two polarization states. He records these orientations, as well as the outcome of the detections – photon deflected to the right or the left.

Box 4: The Polarization of Photons

The polarization of light is the direction of oscillation of the electromagnetic field associated with its wave. It is perpendicular to the direction of its propagation. Linear polarization states can be defined by the direction of oscillation of the field. Horizontal and vertical orientations are examples of linear polarization states. Diagonal states (+ and - 45°) are also linear polarization states. Linear states can point in any direction. The polarization of a photon can be prepared in any of these states.

Filters exist to distinguish horizontal states from vertical ones. When passing through such a filter, the course of a vertically polarized photon is deflected to the right, while that of a horizontally polarized photon is deflected to the left. In order to distinguish between diagonally polarized photons, one must rotate the filter by 45°.

If a photon is sent through a filter with the incorrect orientation – diagonally polarized photon through the non-rotated filter for example – it will be randomly deflected in one of the two directions. In this process, the photon also undergoes a transformation of its polarization state, so that it is impossible to know its orientation before the filter.



Box 5 : Quantum Cryptography Protocol

Emitter bit value	0	1	1	0	1	0	0	1
Emitter photon source								
Receiver filter orientation								
Receiver photon detector								
Receiver bit value	1	1	0	0	1	0	0	1
Sifted key	-	1	-	0	1	-	0	-

After the exchange of a large number of photons, the receiver reveals over a conventional communication channel, such as the internet or the phone – this channel is also known as the classical channel – the sequence of filter orientations he has used, without disclosing the actual results of his measurements. The emitter uses this information to compare the orientation of the photons he has sent with the corresponding filter orientation. He announces to the receiver in which cases the orientations were compatible and in which they were not. The emitter and the receiver now discard from their lists all the bits corresponding to a photon for which the orientations were not compatible. This phase is called the sifting of the key. By doing so, they obtain a sequence of bits which, in the absence of an eavesdropper, is identical and is half the length of the raw sequence. They can use it as a key.

An eavesdropper intercepting the photons will, in half of the cases, use the wrong filter. By doing so, he modifies the state of the photons (refer to Box 4) and will thus introduce errors in the sequence shared by the emitter and receiver. It is thus sufficient for the emitter and the receiver to check for the presence of errors in the sequence, by comparing over the classical channel a sample of the bits, to verify the integrity of the key. Note that the bits revealed during this comparison are discarded as they could have been intercepted by the eavesdropper.

It is important to realize that the interception of the communications over the classical channel by the eavesdropper does not constitute a vulnerability, as they take place after the transmission of the photons.

4.4 Key Distillation

The description of the BB84 quantum cryptography protocol assumed that the only source of errors in the sequence exchanged by the emitter and the receiver was the action of the eavesdropper. All practical quantum cryptography will however feature an intrinsic error rate caused by component imperfections or environmental perturbations of the quantum channel.

In order to avoid jeopardizing the security of the key, these errors are all attributed to the eavesdropper. A post processing phase, also known as key distillation, is then performed. It takes place after the sifting of the key and consists of two steps. The first step corrects all the errors in the key, by using a classical error correction protocol. This step also allows to precisely estimate the actual error rate. With this error rate, it is possible to accurately calculate the amount of information the eavesdropper may have on the key. The second step is called privacy amplification and consists in compressing the key by an appropriate factor to reduce the information of the eavesdropper. A rudimentary privacy amplification protocol is described in Box 6. The compression factor depends on the error rate. The higher it is, the more information an eavesdropper might have on the key and the more it must be compressed to be secure. Fig. 2 schematically shows the impact of the sifting and distillation steps on the key size. This procedure works up to a maximum error rate. Above this threshold, the eavesdropper can have too much information on the sequence to allow the legitimate parties to produce a key. Because of this, it is essential for a quantum cryptography system to have an intrinsic error rate that is well below this threshold.

Key distillation is then complemented by an authentication step in order to prevent a “man in the middle” attack, where the eavesdropper would cut the communication channels and pretend to the emitter that he is the receiver and vice-versa. This is possible thanks to the use of a pre-established secret key in the emitter and the receiver, which is used to authenticate the communications on the classical channel. This initial secret key serves only to authenticate the first quantum cryptography session. After each session, part of the key produced is used to replace the previous authentication key.

4.5 Real World Quantum Cryptography

The first experimental demonstration of quantum cryptography took place in 1989 and was performed by Bennett and Brassard. A key was exchanged over 30 cm of air. Although its practical interest was certainly limited, this experiment proved that quantum cryptography was possible and motivated other research groups to enter the field. The first demonstration over optical fiber took place in 1993 at the University of Geneva. The 90s saw a host of experiments, with key distribution distance spans reaching up to several dozens of kilometers.

The performance of a quantum cryptography system is described by the rate at which a key is exchanged over a certain distance – or equivalently for a given loss budget. When a photon propagates in an optical fiber, it has, in spite of the high transparency of the glass used, a certain probability to get absorbed. If the distance between the two quantum cryptography stations increases, the probability that a given photon will reach the receiver decreases. Imperfect single-

photon source and detectors further contribute to the reduction of the number of photons detected by the receiver. The fact that only a fraction of the photons reaches the detectors, however, does not constitute a vulnerability, as these do not contribute to the final key. It only amounts to a reduction of the key exchange rate.

When the distance between the two stations increases, two effects reinforce each other to reduce the effective key exchange rate. First, the probability that a given photon reaches the receiver decreases. This effect causes a reduction of the raw exchange rate. Second, the signal-to-noise ratio decreases – the signal decreases with the detection probability, while the noise probability remains constant – which means that the error rate increases. A higher error rate implies a more costly key distillation, in terms of the number of bits consumed, and in turn a lower effective key creation rate. Fig. 3 summarizes this phenomenon.

Box 6: Rudimentary Privacy Amplification Protocol

Let us consider, as an illustration, a two-bit key shared by the emitter and the receiver and let us assume that it is 01. Let us further assume that the eavesdropper knows the first bit of the key but not the second one: 0?. The simplest privacy amplification protocol consists in calculating the sum, without carry, of the two bits and to use the resulting bit as the final key. The legitimate users obtain $0 + 1 = 1$. The eavesdropper does not know the second bit. For him, this operation could be either $0 + 0 = 0$ or $0 + 1 = 1$. He has no way to decide which one is the correct one. Consequently, he does not have any knowledge on the final key. There is a cost. This privacy amplification protocol shortens the key by 50%. In practice, more efficient protocols have obviously been developed.

Typical key exchange rates for existing quantum cryptography systems range from hundreds of kilobits per second for short distances to hundreds of bits per second for distances of several dozens of kilometers. These rates are low compared to typical bit rates encountered in conventional communication systems. In a sense, this low rate is the price to pay for absolute secrecy of the key exchange process. One must remember though that the bits exchanged using quantum cryptography are only used to produce relatively short keys (128 or 256-bits). Nothing prevents transmitting data encrypted with these keys at high bit rates.

The span of current quantum cryptography systems is limited by the transparency of optical fibers and typically reaches 100 kilometers (60 miles). In conventional telecommunications, one deals with this problem by using optical repeaters. They are located approximately every 80 kilometers (50 miles) to amplify and regenerate the optical signal. In quantum cryptography, it is not possible to do so. Repeaters would indeed have the same effect as an eavesdropper and corrupt the key by introducing perturbations. Note that if it were possible to use repeaters, an eavesdropper could exploit them. The laws of quantum physics forbid this. It is obviously possible to increase this span by chaining links.

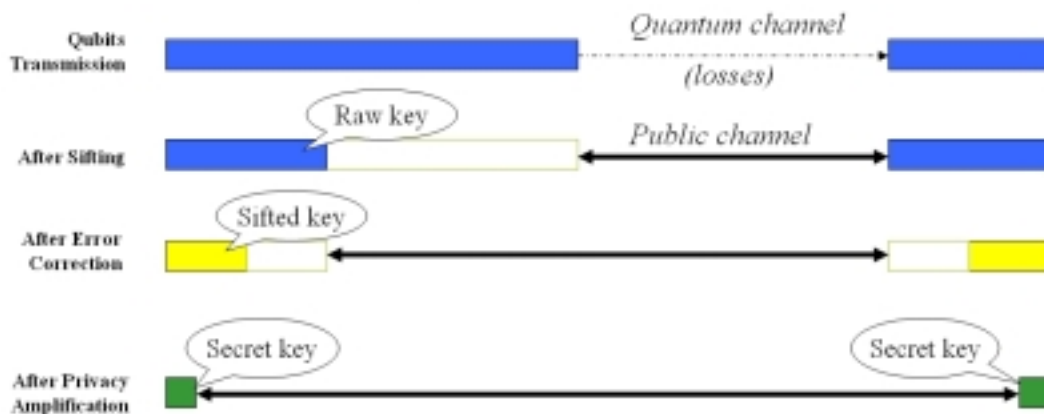


Figure 2: Impact of the sifting and distillation steps on the key size.

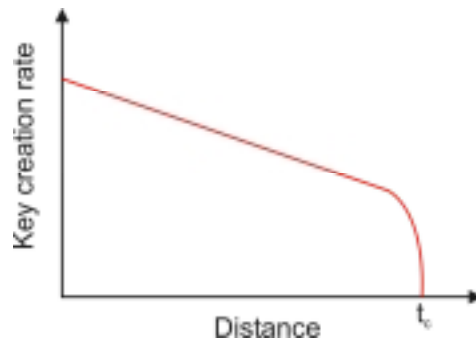


Figure 3: Key creation rate as a function of distance.

In 2002, id Quantique launched the first commercial quantum cryptography system called Clavis, designed for research and development applications. In 2004, this system was used in one of the first commercial applications of quantum cryptography. Data transmissions between two data centers of a data hosting company in Geneva were encrypted using keys exchanged by a Clavis system. The primary data center hosted mission critical information, which were replicated in the secondary data center, located 11 kilometers away, to guarantee business continuity of the company.

In early 2005, id Quantique has released a new version of its quantum cryptography system. It is called Vectis and consists of a link encryptor. It features automated key exchange by quantum cryptography over an optical fiber up to a distance of 100 kilometers (60 miles), as well as high-bit rate full duplex Ethernet traffic encryption and authentication. It can be easily deployed in an existing network and is used by private and public organizations to secure critical optical links.

For more information on the deployment of the Vectis link encryptor and its applications, refer to the documents listed in Box 1.

4.6 Perspectives for Future Developments

Future developments in quantum cryptography will certainly concentrate on the increase of the key exchange rate. Several approaches have also been proposed to increase the range of the systems. The first one 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 low, if an adequate wavelength is selected and... the weather is clear.) 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 demonstrated.

There are also several theoretical proposals for building quantum repeaters. They would relay quantum bits 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. It is nevertheless interesting to note that a quantum repeater is a rudimentary quantum computer. At the same time as it will make public key cryptography obsolete, the development of quantum computers will also allow to implement quantum cryptography over transcontinental distances.

5. Conclusion

For the first time in history, the security of cryptography does not depend any more on the computing resources of the adversary, nor does it depend on mathematical progress. Quantum cryptography allows exchanging encryption keys, whose secrecy is future-proof and guaranteed by the laws of quantum physics. Its combination with conventional secret-key cryptographic algorithms allows raising the confidentiality of data transmissions to an unprecedented level. Recognizing this fact, the MIT Technology Review and Newsweek magazine identified in 2003 quantum cryptography as one of the “ten technologies that will change the world”.