Redefining Security

# QUANTUM-SAFE SECURITY WHITE PAPER

## Understanding Quantum Cryptography

May 2020

**ID QUANTIQUE SA**
Chemin de la Marbrerie 3

1227 Carouge/Geneva
Switzerland

T +41 22 301 83 71
F +41 22 301 89 79

info@dquantique.com
**www.idquantique.com**

## Table of Content




**ID Quantique SA**
Ch. de la Marbrerie, 3
1227 Carouge
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.**

## 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 19th 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 then developed by physicists such as Max Planck, Albert Einstein, Werner Heisenberg, Erwin Schrödinger and many others during the first thirty years of the 20th century. Quantum physics describes 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, quantum physics features intrinsic randomness, while classical physics is deterministic. It also imposes a 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 20th century – it allowed for example the invention of the transistor or the laser – its impact on the processing of information has only been understood more recently. "Quantum Information Theory" 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? Indeed, it does. Applying quantum physics to information processing yields revolutionary properties and possibilities without any equivalent in conventional information theory. This is the domain of Quantum Computing, which has seen rapid progress in the last few years[1]. Here we concentrate on explaining quantum cryptography on a basic technical level.



Despite great progress in recent years the development of a quantum computer able to perform meaningful computations is still a challenge. However, the first applications of quantum information processing have already been commercialized by ID Quantique (IDQ). 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. IDQ's Quantis Quantum Random Number Generator (QRNG) was the first commercial product based on this principle. It has been used in security, online gaming and other applications since 2001. A more recent, chip-sized, QRNG is now available. It can be integrated into almost any computing device requiring randomness, such as computers, smart phones and IoT devices.

The second application – the main focus of this paper – is called quantum cryptography. It exploits Heisenberg's uncertainty principle, which prevent an eavesdropper from discovering the exact quantum state of a system, to allow two remote parties to exchange a cryptographic key in a provably secure manner.

[1] See for example a very readable introduction from the Institute for Quantum Computing: here

## 2. Cryptography

Before we turn to quantum cryptography per se, let us provide a quick overview of conventional cryptography, as needed for our purpose. 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 fifty years, cryptography evolved out of its status of "classified" science, and it is now increasingly mandated by regulations governing data protection for commercial and public institutions.

Although confidentiality is the traditional application of cryptography, it is also used nowadays to achieve broader objectives, such as data authentication, digital signatures, and non-repudiation[2].

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, recovering 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 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. The scheme relies on the fact that both sender and receiver have symmetric keys, and that these keys are known only to the authorized persons (also referred to as secret or symmetric key cryptography).



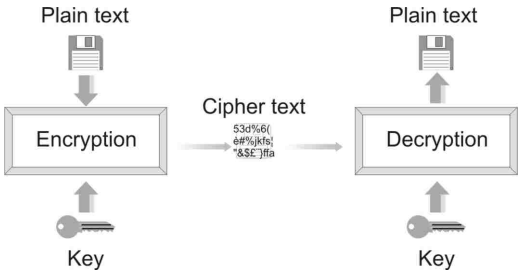



**Figure 1: Principle of Cryptography**

Numerous encryption algorithms exist. Their relative strengths essentially depend 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. Nowadays traditional DES can be cracked in a few hours. It has been replaced by the Advanced Encryption Standard – AES – which has a minimum key length of 128 bits[3], and is now commonly used with 256-bit keys.

[2] 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.
[3] For recommendations on minimum key lengths and the longevity of protection provided by each key scheme refer to www.keylength.com

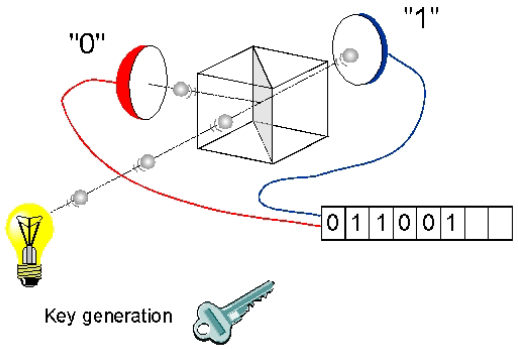
In addition to its length, the amount of information encrypted with a given key also influences the strength of the scheme. In general, the more often a key is changed, the better the security. In the very special case where the key is as long as the plain text and used only once – a “one-time pad” – it can be proven that decryption is impossible and that the scheme is absolutely secure.

In commercial applications, where general trust in the encryption scheme is necessary, the encryption algorithm is normally public – with the effectiveness of the encryption deriving from the fact that the key is secret.

This means firstly, 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 1 describes a quantum random number generator.

### Box 1: Quantum Random Number Generator (RNG)

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 example 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 impossible for an observer to predict the outcome. Because of this intrinsic randomness, it is natural to use this to generate strings of high-quality random numbers. IDQ’s Quantis is a quantum RNG exploiting this principle.






Secondly, it must not be possible for a third party to intercept the secret key during its exchange between the sender and the recipient. This so-called “key distribution problem” is absolutely central in cryptography.

## 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 impractical. In addition, it is impossible to check whether this medium has been intercepted and its content copied.

In the late sixties and early seventies, researchers of the British "Government Communication Headquarters" (GCHQ, now renamed the National Cyber Security Centre, or NCSC) invented an

algorithm to solve this key distribution 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 who will be sending valuable information. The recipient keeps the key to the padlock. Before transmitting the information, the sender closes the padlock, thus protecting the data he sends. The recipient is then the only person 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. An essential step in the process, the distribution of the open padlock, is often overlooked. The future sender of information has to be able to authenticate the open padlock, make sure that it is coming from the intended recipient and that it has not been tampered with. In public-key cryptography, this is achieved by special certificates, which are emitted by trusted partners, so-called Certificate Authorities, and attached to the public keys. A public-key cryptographic scheme has to be included in an underlying Public Key Infrastructure (PKI). Formally, these padlocks are mathematical expressions of so-called "one-way functions", because they are easy to compute but difficult to reverse (see Box 2). As public key cryptography algorithms require complex calculations, they are slow. For this reason, they are not used to encrypt large amount of data but instead to exchange short session keys for secret-key algorithms such as AES.

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 therefore be carefully selected.



### Box 2: 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 prime 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, especially with key lengths of 2048 or more bits. 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. Indeed, an algorithm for efficient factorization has been discovered in 1994 by Peter Shor. However, this algorithm must run on a quantum computer. This is the basis of the quantum threat on modern cryptography.

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 a challenge in an article entitled "A new kind of cipher that would take millions of years to break". The challenge was to crack a cipher encrypted with a 428-bits key. They predicted at the time that this would take 40 quadrillion years. However the $100 prize was claimed in 1994 after 6 months of work by a group of scientists using parallel computing over the Internet, and the resulting solution "The magic words are squeamish ossifrage" has gone down in the history of cryptanalysis.

Other public-key cryptography schemes based on the intractability of certain mathematical problems are now in use, such as elliptic curve cryptography (ECC). For elliptic-curve-based protocols, it is

assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible. The minimum recommended length for asymmetric keys continues to grow in response to threats from improvements in technology and increased computing power.

In addition in 1994 there was an attack on another front - Peter Shor, professor of Applied Mathematics at MIT, proposed an algorithm for integer factorization which would run on a quantum computer and allow to reverse one-way functions at the basis of both RSA and ECC - in other words to crack all existing versions of public key cryptography. The development of the first quantum computer will immediately make the exchange of a key with current public key algorithms, such as RSA and ECC, insecure. Due to the security threat posed by the quantum computer, the National Security Agency (NSA), in the USA, has issued a statement recommending transitioning to Quantum-Safe cryptography in the near future[4] . This transition, led by the NIST in the USA, which aims at certifying new Post-Quantum or Quantum-Resistant algorithms is now in full swing[5]. The initial 69 submissions to the Round 1 have been reduced to 26 for Round 2. NIST is now evaluating these for Round 3, which shall be completed during the summer of 2020. The final selection should be complete in 2022 to 2024.

The second major flaw with public key cryptography is that it is vulnerable to progress in mathematics. In spite of tremendous efforts, mathematicians have not yet been able to prove that public key cryptography is secure. It has not been possible to rule out the existence of even classical algorithms that allow the reversal of 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 other researchers busy for years or decades. It is even possible that an algorithm for reversing some one-way functions has already been discovered, but kept secret. These threats simply mean that public key cryptography cannot guarantee future-proof key distribution.



# 4. Quantum Cryptography

## 4.1 Principle

Quantum cryptography solves the problem of key distribution by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the fundamental laws of physics. This key can then be used securely with conventional cryptographic algorithms. The more correct name for quantum cryptography is therefore Quantum Key Distribution.

The basic principle of quantum key distribution (QKD) 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. For example, when you read this white paper, the sheet of paper must be illuminated. 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

[4] See for example on the NSA website: https://www.nsa.gov/
[5] See for example the NIST webpage on PQC: https://csrc.nist.gov/projects/post-quantum-cryptography

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 an eavesdropper was able to gain information on their key. 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 intercepted or not. This is why the technology is used to exchange a key and not valuable information. Once the key exchange is validated, and the key is provably secure, it can be used to encrypt data. Quantum physics allows to formally 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 key distribution the same approach is followed with the difference that the pulses contain only a single photon.

A single photon represents a very tiny amount of light (when reading this white paper your eyes register billions of photons every second) and it 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 better 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 QKD 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 Key Distribution Protocols

Although several QKD protocols exist, only one protocol will be discussed here to illustrate the principle of quantum key distribution. We choose the BB84 protocol, which was the first to be invented in 1984 by Charles Bennett of IBM Research and Gilles Brassard of the University of Montreal and is still widely used, as a good representative.

An emitter and a receiver can implement it by exchanging single photons, whose polarization states are used to encode bit values over an optical fiber (refer to Box 3 for an explanation of polarization). 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 4). For a 1-bit value, they will use either a vertical state or a +45° diagonal one.

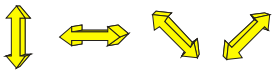
## Box 3: The Polarization of Photons

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.

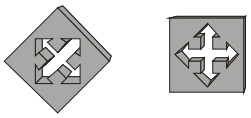
Diagonal states (+ and – 45°) are also linear polarization states. Linear states can point in any direction. The polarization of a photon can be prepared in any of these states.

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°.

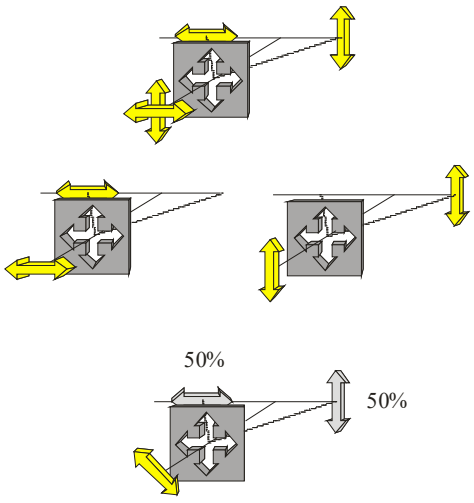
If a photon is sent through a filter with the incorrect orientation – diagonally polarized photon through the non-rotated filter for example – it will be randomly deflected in one of the two directions. In this process, the photon also undergoes a transformation of its polarization state, so that it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



Linear polarization states



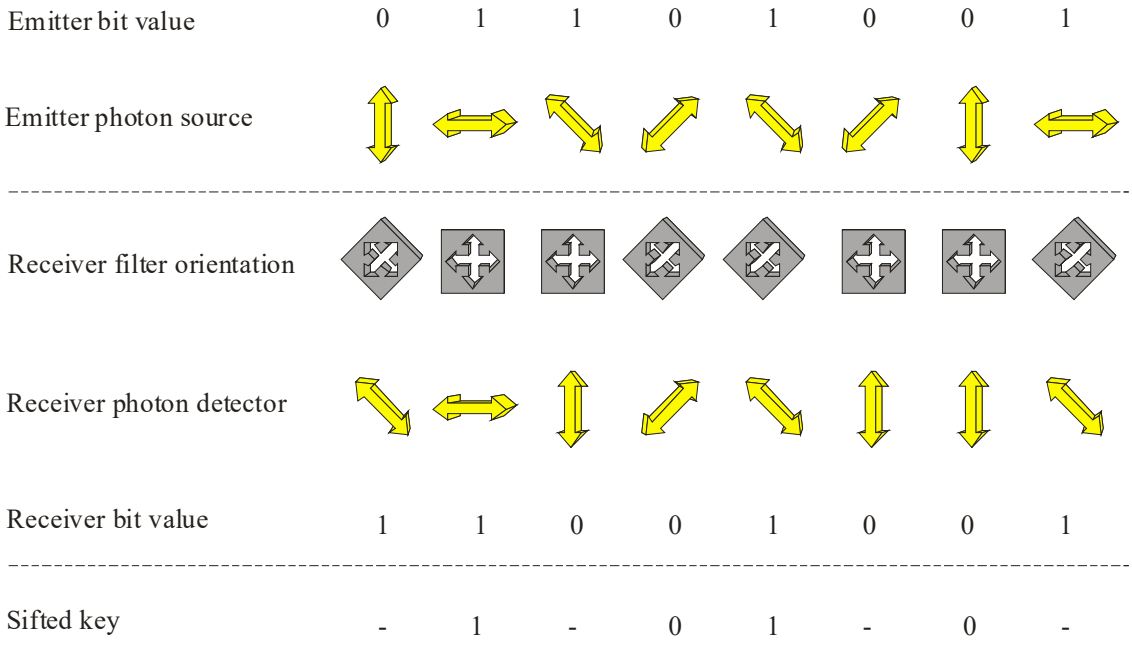
Filters






**ID QUANTIQUE SA**
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@dquantique.com
**www.idquantique.com**

## Box 4: Quantum Key Distribution Protocol




- For each bit, the emitter sends a photon whose polarization is randomly selected, typically with a QRNG (Box 1), 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.



After the exchange of a large number of photons, the receiver reveals the sequence of filter orientations he has used, without disclosing the actual results of his measurements. This information is exchanged over a so-called classical channel, such as the internet or the phone. 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 where 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.

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 QKD 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 QKD 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 5. 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 – this can be achieved through the system design and the choice of components.

Key distillation is then complemented by an authentication step in order to prevent a “man in the middle attack”. In this case the eavesdropper would cut the communication channels and pretend to the emitter that he is the receiver and vice versa.



Such an attack is prevented 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.

### Box 5: Rudimentary Privacy Amplification Protocol

Let us consider 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.

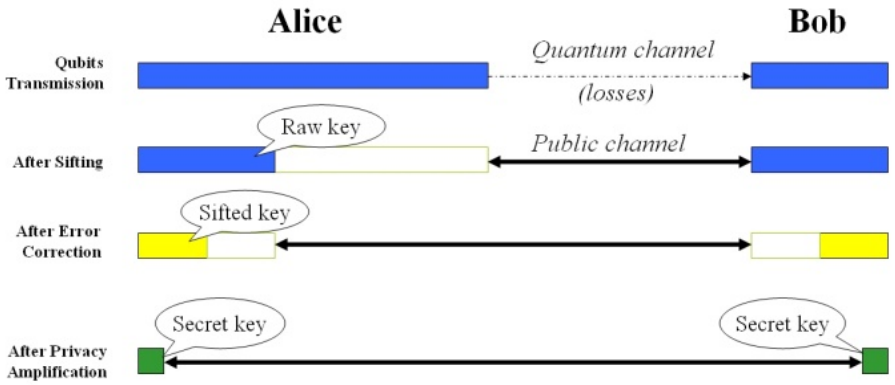



**Figure 2: Impact of the sifting and distillation steps on the key size**

## 4.5 Real World Quantum Key Distribution

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 QKD 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. Since then, QKD has been performed successfully many times, with various protocols.

The performance of a QKD 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 of getting absorbed. If the distance between the two QKD 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 does not however 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. However, the key after distillation remains safe. Fig. 3 summarizes this phenomenon.

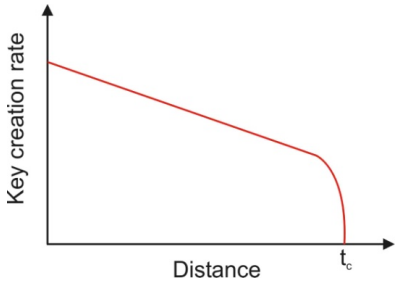



**Figure 3: Key creation rate as a function of distance.**

Typical key exchange rates for existing QKD systems range from hundreds of kilobits per second for short distances to hundreds of bits per second for greater distances. Since the bits exchanged by the QKD systems are used for the creation of relatively short encryption keys (128 or 256-bits), the bit exchange rate is sufficient to create a regular refresh rate of provably secret and absolutely random keys. Data is then encrypted with these keys at transmission rates up to 10 or even 100 Gbps.

The span of current QKD systems is limited by the transparency of optical fibers and typically reaches hundred kilometers (60 miles). A much longer distance of 300 km in an optical fiber has been demonstrated[6]. However, the lower key rate achievable for these distances makes real-world applications more challenging. 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 QKD it is not possible to do this as optical repeaters would have the same effect as an eavesdropper and corrupt the key by introducing noise and perturbations. One possible solution is to set up a network of trusted nodes, with QKD repeaters to increase the distance[7]. The nodes have to be trusted, and physically secured, because the keys are available at each node. They can only be setup in secure locations. This is the approach adopted for the Chinese QKD backbone, now installed between Beijing and Shanghai[8], and in the process of being implemented over a large 11'000 km long QKD backbone, which will cover most of Eastern China. Some of the links will even leave the ground and use optical satellites as trusted nodes (see Section 4.7). Another approach, which is still in progress, is to replace the trusted nodes with quantum repeaters (see Section 4.7).

## 4.6 Twenty years of QKD innovation at IDQ



In 2002, IDQ launched the first industrial QKD system called Clavis, designed for research and development applications, and in 2008 the next-generation Clavis2 was launched. Clavis2 uses a proprietary auto-compensating optical platform, which features outstanding stability and interference contrast, guaranteeing low quantum bit error rate. Secure key exchange became possible up to 100 km. This optical platform is well documented in scientific publications and has been extensively tested and characterized. The Clavis2 system is the most flexible product of its kind on the market. It consists of two stations controlled by one or two external computers. A comprehensive software suite implements automated hardware operation and complete key distillation. Two quantum cryptography protocols (BB84 and SARG) are implemented. The exchanged keys can be used in an encrypted file transfer application, which allows secure communications between two stations.

In 2007, IDQ launched Cerberis, a QKD server designed for commercial applications. This has been deployed and extensively field tested, by banks, governments and enterprises, since its installation that same year for use in elections by the government of Geneva, Switzerland. This QKD link is still in use today. In addition, the robustness and reliability of IDQ's QKD technology in a real-time telecommunications network was unequivocally proven in the SwissQuantum project. This documents a long-running test of uninterrupted deployment of a QKD network, starting from March 2009 until the project was dismantled in January 2011.

[6] Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre, in https://arxiv.org/abs/1407.7427
[7] For reference to secure key agreements over trusted repeater QKD networks see http://arxiv.org/pdf/0904.4072.pdf developed within framework of SECOQC project.
[8] Reported in: https://docbox.etsi.org/Workshop/2015/201510_IQCWORKSHOP/UofChongqing_HongXiang.pdf

The Cerberis QKD system provides fully automated, provably secure key exchange for Layer 2 link encryptors over standard optical fibers in an existing network. Future-proof confidentiality of the data is guaranteed by the use of QKD. IDQ's Cerberis QKD server is also compatible with wavelength division multiplexing (WDM). Quantum keys can be multiplexed with data over a single fiber for distances up to thirty km in Metropolitan Area Networks (MAN). In addition, in 2011 IDQ and Colt launched the world's first QKD-as-a-Service for enterprises and financial institutions.

The third generation of QKD systems was launched in 2016. The first implementation, the Clavis3, can distribute the keys over 100 km or more, with a much higher key rate than previous systems. This new system is designed for academic and research applications. Flexibility is the key word, with access to the several stages of key distillation and several options, including an external detector option, for lower detector noise and increased distance.

A new generation of the Cerberis system, the Cerberis3, is also available as a blade, to be inserted in standard telecom racks (in the so-called ATCA standard). The Cerberis3 is designed for real-world implementation of QKD. Here the key words are **automation, integrability, compliance and networks**.

Any commercial system seeking wide acceptance first has to be **easy to install**. The Cerberis3 can indeed be installed like any standard telecom system. No specific quantum knowledge is required.

The second requirement is **integrability**. The Cerberis3 does not replace any existing encryption system, but only adds one more layer to the security. For example, it can be combined with different brands of link encryptors. The QKD key is added (technically this is known as XORed) to the existing key exchange mechanism provided by the encryptor. The security of the combined system can only be superior to the security of each. This allows users to keep any current certification, which their current system may possess and adds an extra level of security, based on different principles.



This leads to our third requirement, **compliance**. Today specific standards for QKD are under development, both at the European Telecommunication Standards Institute (ETSI)[9] and at the International Telecommunication Union (ITU)[10]. The Cerberis3 QKD system leads the way towards standardization of QKD. The Cerberis3 can be used in telecom applications, for example in telecom exchanges.

Finally, the fourth requirement is **network**. Before the Cerberis3, QKD systems were designed for point-to-point applications. Alice wanted to exchange secure keys with Bob over one optical link. This is not sufficient anymore. QKD systems have to be able to work in a networking environment, with many systems together. This is addressed in the Cerberis3, where many QKD units are monitored and controlled through an external management system. This management system is able for example to establish a secure QKD link between all the elements of the connected network. Today, QKD is primarily used to secure the critical backbone or data recovery center links for financial institutions[11], large companies and defense & government organizations. It is also implemented in key parts of a real 5G telecom network, to provide quantum-safe security. An intriguing new application is the Quantum Vault, where QKD is used to provide provable security for the storage of digital assets, such as the public keys used for blockchains. In order to improve the usability of QKD in the real world, a large

[9] QKD standards are being development within the ETSI framework, more info here
[10] For the ITU-T, look at our work with SK Telecom
[11] For example, see our "Securing networks for disaster recovery" use case

European project, OpenQKD, is building several QKD testbeds, where users and manufacturers will collaborate to integrate QKD into optical networks[12]. QKD is truly leaving the laboratory and experimental stages to find its positioning into real cybersecurity.

## 4.7 Perspectives for Future Developments

Future developments in QKD will certainly focus on increasing the range of the systems and provide a global QKD network. In order to go beyond the trusted nodes mentioned in Section 4.5, which restrict QKD to ground systems, where nodes can be established every few tens of kilometers, the next option is to get rid of the optical fiber. It is possible to exchange keys using quantum cryptography in free space, between a terrestrial station and a low earth orbit satellite. Indeed, absorption in the atmosphere takes place mainly over the first few kilometers. If an adequate wavelength is selected, and the weather is fair, an optical link between the ground and the satellite at an altitude of roughly 800 km can be established. Such a satellite moves with respect to the earth's surface. When passing over a second station, located thousands of kilometers away from the first one, it can retransmit the key. This is outlined in Figure 4. 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. Advanced research is done in China, which has launched the first QKD satellite, named Micius[13] in August 2016. Micius is designed to implement various protocols and perform key exchange between the satellite and ground stations. Commercial applications should follow in a few years.

There are also several theoretical proposals for building quantum repeaters[14]. They would relay quantum bits without measuring and thus perturbing them. These quantum repeaters rely on quantum teleportation to send a photon from one node to another, without measuring its state. Therefore, since the state of the photon is not known, the nodes do not have to be trusted anymore. A single photon can be sent reliably from one end of a network to the other, while keeping the basic property of QKD: any attempt at measuring it, either in transit or at the nodes, will be discovered. Perhaps surprisingly, quantum teleportation is not the issue: it has already been realized experimentally. What is missing in order to have a QKD network with quantum repeaters are the quantum memories needed to store the photons at various stages during the transmission. Quantum repeaters could, in principle, be used to extend the key exchange range over arbitrarily long distances.



[12] The OpenQKD project
[13] This is reported in China Daily for example: http://usa.chinadaily.com.cn/business/2016-08/16/content_26492852.htm
[14] For more information on quantum repeaters see https://qt.eu/understand/underlying-principles/quantum-repeaters/

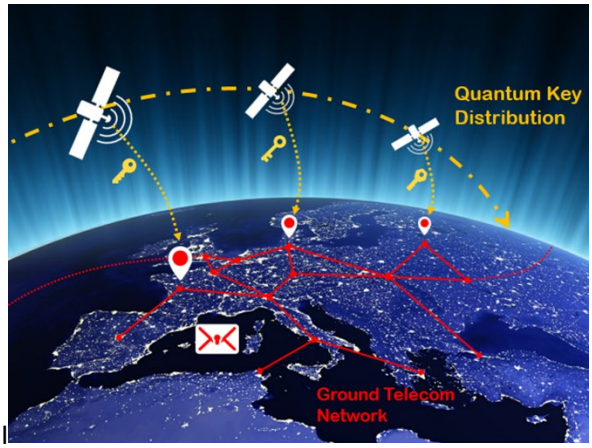



**Figure 4: QKD from space**

It is interesting to note that a quantum repeater is a rudimentary quantum computer. At the same time as making current public key cryptography obsolete, the development of quantum computers will also allow the implementation of quantum cryptography over transcontinental distances.

## 5. Conclusion

For the first time in history, the security of a cryptographic primitive is dependent neither on the computing resources of the adversary nor on mathematical progress. Quantum cryptography, and specifically QKD, allows the exchange of encryption keys whose secrecy is future-proof and guaranteed by the laws of quantum physics. Its combination with conventional secret-key cryptographic algorithms raises the confidentiality of data transmissions to an unprecedented level. The current distance limitations for QKD, which restrict its applications to some specific use cases, such as links between data centers and disaster recovery centers, will be lifted in the near future, through the use of trusted nodes, free space QKD, and quantum repeaters. QKD networks will soon become a reality. QKD is therefore set to become an integral part of a global security framework, where both computational methods and physical methods are used to guarantee data security, and in particular provide Quantum-Safe security against the threat of a quantum computer.



**ID QUANTIQUE SA**
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@dquantique.com
**www.idquantique.com**