Volume 2, Issue 6, June 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Key Distillation Process on Quantum Cryptography Protocols in Network Security

M. Indra Sena Reddy[1], K. Subba Reddy[2], M. Purushotham Reddy[3], P.J. Bhat[4], Rajeev[5]

[1,2]Dept. of CSE, RGMCET, India.

[3]Dept. of CSE, VBIT, India.

[4,5]ISRO Satellite centre, Bangalore, India.

mir555mittapalli@gmail.com

Abstract— **Quantum cryptography is an effort to allow two users of a common communication channel to create a body of shared and secret information. This information, which generally takes the form of a random string of bits, can then be used as a conventional secret key for secure communication. It is useful to assume that the communicating parties initially share a small amount of secret information, which is used up and then renewed in the exchange process, but even without this assumption exchanges are possible.**

The recent applications of the principles of quantum mechanics to cryptography have led to remarkable new dimension in secret communication. As a result of these developments, it is now possible to construct cryptographic communication systems which detect unauthorized eavesdropping should it occur, and which give a guarantee of no eavesdropping should it not occur.

The advantage of quantum cryptography over traditional key exchange methods is that the exchange of information can be shown to be secure in a very strong sense, without making assumptions about the intractability of certain mathematical problems. Even when assuming hypothetical eavesdroppers with unlimited computing power, the laws of physics guarantee (probabilistically) that the secret key exchange will be secure, given a few other assumptions.

Keywords— **Quantum cryptography, Cryptographic protocols, Security algorithms.**

I. INTRODUCTION

The uncertainty principle in quantum mechanics created a new paradigm for cryptography: Quantum cryptography, or more specifically Quantum Key Distribution (QKD). Unlike the classical cryptography which relies on mathematical complexity, quantum cryptography is based on the laws of quantum physics. These laws ensure that nobody can measure a state of an arbitrary polarized photon carrying information without introducing disturbances which will be detected by legitimate users. As all eavesdropping can be detected, quantum cryptography is considered as a promising key distribution means towards long term unconditionally secure cryptosystems.

Since the first QKD protocol proposed in 1984 with the name of BB84 [1], research on quantum cryptography gets significant advances. Experiments of different QKD systems have been realized in fiber networks and over free space [2-5]. Especially, a turnkey service using quantum cryptography to frequently generate fresh secret key has been commercialized in Switzerland [6]. While the use of quantum cryptography in fiber optical networks is successfully deployed in practice, the application of quantum cryptography in mobile wireless networks is still premature. Most research and experiments aim at providing QKD service outdoor for along distance in satellite networks [7] or between buildings in a city [8]. In these works, communication entities of the QKD protocol are mainly system devices but not final mobile users. For instance, communication entities in satellite networks are ground stations and the satellite. Our motivation of integrating quantum cryptography in mobile wireless networks is quite different. We aim at providing mobile wireless user's terminals with QKD service. In a mobile environment, one technical challenge in addition to those of free space environment is the maintenance of a line-of-sight path between mobile user and the fixed part of the network when the user moves around.

GSM or cellular networks in general is a wide area network, used essentially outdoor to provide mobile users with telephone service. As voice call is the main application of GSM networks, the terminals are small size cell phones allowing mobile users to move with a high level of mobility. The speed of mobile users in a GSM network can be at step speed or vehicle speed. With this level of mobility and the outdoor

Environment, cellular network presents some disadvantages for the use of quantum cryptography. It will be difficult to provide a line-of-sight path with a high user mobility level. The outdoor environment is not ideal

for free space quantum cryptography. Noise level can be raised because of rain or smoke. The large coverage area of the GSM network and the presence of natural obstacles such as trees or houses do not facilitate the provision of alternative line-of-sight paths.

In contrast to cellular networks, 802.11 networks [9]present many interests relating to the use of quantum cryptography. First, 802.11 is a wireless local area network, mainly used in offices and campus such as, class rooms, meeting rooms, universities, and halls in hotels or in airports. For the limited coverage area, 802.11 networks are mainly used indoor, reducing noise and natural obstacles caused by the outdoor environment This building-oriented environment also facilitates the deployment of a high density of quantum apparatus to provide alternative line-of-sight paths. Second, 802.11 terminals are mainly laptops or PDAs (Personal Digital Assistant) which have more computational capacity and more energy for the autonomy than cell phones in cellular networks. Quantum key distribution in mobile networks is a task requiring significant amount of computational resource and energy for the control protocol and the QKD protocol. Third, as 802.11 terminals are not small like cell phones and 802.11 applications usually requires that users watch the screen, the mobility level of users in WLAN 802.11 is low and sometimes static, promising a solution to provide line-of-sight paths between quantum transmitters and receivers. Fourth, from an application point of view, WLAN 802.11 is usually used to provide Internet access through an access point installed by an organization or by a wireless ISP (Internet Service Provider). This kind of application is critical from a network security point of view because users can realize e-commerce or banking transactions via the Internet. These applications need a very strong security that quantum cryptography can offer. Different from cellular and 802.11 networks, Bluetooth is a personal area network which is mainly used to interconnect peripheral devices such as mouse, desktop, keyboard, and computer which are in close proximity of each other. As the coverage area is small, the eavesdropping can be controlled within the vision of users. The contribution of quantum cryptography is less significant in such an environment. From a network security point of view, the application of replacing wires connecting devices in a close proximity is also less critical than the application of Internet access of 802.11 networks.For this analysis, our first tentative of integrating QKD in mobile networks is towards the 802.11 network. As a first step of the integration of quantum cryptography in 802.11 networks, we have defined the Quantum handshake [10] to establish the 802.11i encryption keys using the BB84 protocol.

II. The Importance Of Cryptography

At a time when the reliance upon electronic data transmission and processing is becoming every day more prevalent, unauthorized access to proprietary information is a real threat. In 2004, 53% of the respondents of the CSI/FBI Computer Security and Crime Survey1 admitted having been subjected to unauthorized use of computer systems. These attacks caused a total loss of more than 140 million USD for the respondents of the survey. Moreover, it is generally admitted by experts that the vast majority of information security incidents and attacks go unreported. These facts clearly demonstrate that it is vital for organizations to implement comprehensive information security policies and countermeasures in order to protect reputation, ensure business continuity and guarantee information availability, integrity and confidentiality. Besides, legal and compliance requirements also often demand such measures. Last but not least, the way an organization protects its information assets increasingly impacts the image projected to customers and partners.

A. Protecting Information

Efficiently protecting critical information within an organization requires the definition and the implementation of a consistent information security policy. Such a policy describes which processes and means must be applied within the company to achieve this goal. It puts into practice technologies such as biometrics or smartcards, for instance, to control access to the data processing and storage infrastructures – whether electronic or not – and guarantee the physical security of the information. It also resorts to solutions such as Intrusion Prevention and Detection systems, Firewalls and Antivirus Software to defend a secure perimeter around the internal computer network of the organization and prevent hackers from penetrating it. Finally, it defines measures to protect information transmission between remote sites. This last aspect of information security is often overlooked.

B. 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 nonrepudiation.

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 knowing the key.

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. 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. 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.

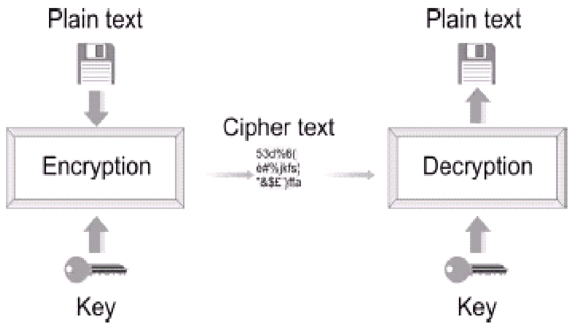


Figure 1: Principle of cryptography

III. 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 .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[11] AES is much stronger than RC4 but it requires a hardware modification for the transition from WEP-based systems. For the transition from WEP to CCMP, 802.11i defines also another encryption algorithm, TKIP (Temporal Key Integrity Protocol), which is based on the RC4 algorithm [12] and only requires a software upgrade on WEP-based systems..

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 computer and allow reversing 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.

IV. Quantum Cryptography

A. 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 key and not valuable information. Once the key is validated, it can be used to encrypt data. Quantum physics allows proving that interception of the key without perturbation is impossible.

B. 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.

C. 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° diagonal one.

- For each bit, the emitter sends a photon whose polarization is randomly selected among the four states. Herefords 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 distinguishing 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 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 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.

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.

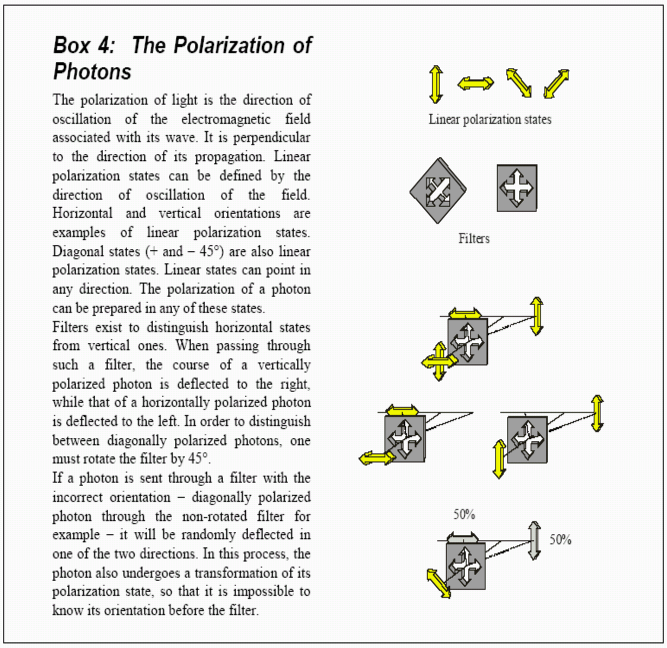
1) Key Distillation- The description of the BB84 quantum cryptography protocol assumed that the only source of errors in the sequence exchanged by the emitter and the receiver was the action of the eavesdropper. All practical quantum cryptography will however feature an intrinsic error rate caused by 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 estimating 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. 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.



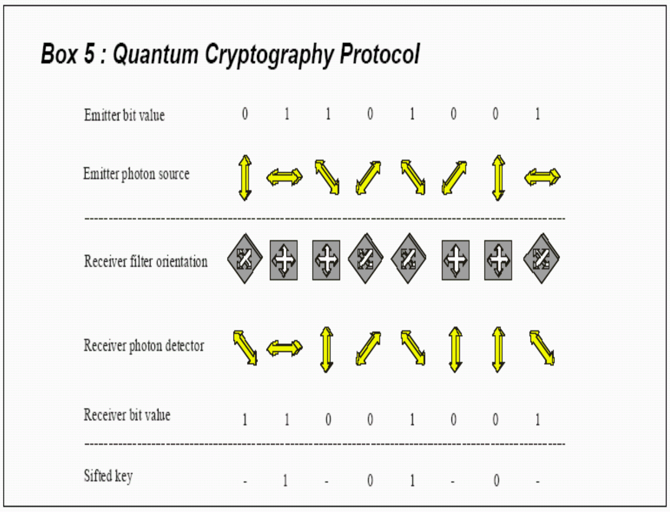
Box 4: The Polarization of Photons

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.

Linear polarization states
Filters
50%
50%



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	-

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.

2) 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 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.

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

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 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.

.

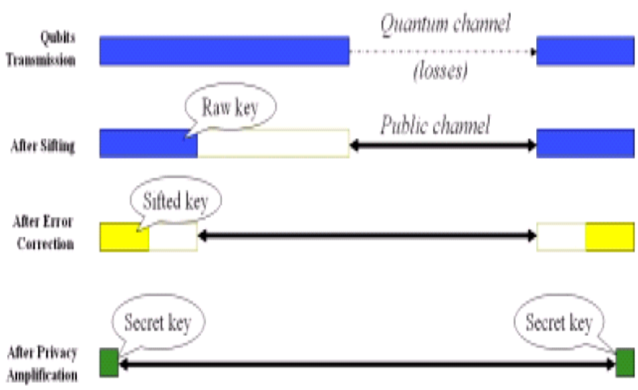


Figure 2: Impact of the sifting and distillation steps on the key size.

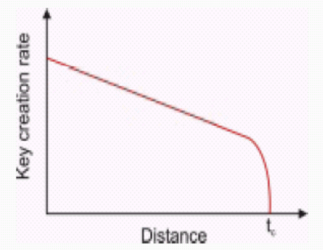


Figure 3: Key creation rate as a function of distance.

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.

V. 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. Quantum cryptography allows to reach unprecedented levels of security guaranteed by quantum physics for data transmissions over optical networks.

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”.

References

[1] C. Bennet, and G. Brassard, G. “Quantum cryptography: Public key distribution and coin tossing”, IEEE International Conference on Computers, Systems, and Signal Processing, IEEE Press, LOS ALAMITOS, 1984.

[2] N. Namekata, S. Mori, and S. Inoue, “Quantum key distribution over an installed multimode optical fiber local area network”, Optical Express, 2005.

[3] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, “Quantum key distribution over 67 km with a plug and play system,” New Journal of Physics, Vol. 4, 2002, pp. 41.1–41.8.

[4] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, “Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector”, Electronics Letters, Vol. 39,2003, pp. 1199–1200.

[5] C. Kurtsiefer, P. Zardaa, M. Halder, P.M. Gorman, P.R. Tapster, J.G. Rarity and H. Weinfurter. “Long Distance Free Space Quantum Cryptography”, 2003.

[6] http://www.idquantique.com.

[7] M. Aspelmeyer, T. Jennewein, and A. Zeilinger, “Longdistance quantum communication with entangled photons using satellites”, IEEE Journal of Selected Topics in Quantum Electronics, Vol. 9, Issue 6, November 2003.

[8] http://xqp.physik.unimuenchen.de/exp/qc2/index.html

[9] ANSI/IEEE Standard 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999 Edition, Reaffirmed June 2003.

[10] T.M.T. Nguyen, M. A. Sfaxi, and S. Ghernaouti-Hélie, "Integration of Quantum Cryptography in 802.11 Networks”, Proceedings of the First Intenational Conference on Availability, Reliability and Security (ARES), pp. 116-123, Vienna, April 2006.

[11] National Institute of Standards and Technology, FIPS Pub 197: Advanced Encryption Standard (AES), November 2001.

[12] B. Schneier, Applied Cryptography, John Wiley & Son, 1996.