Sección Especial en Óptica Cuántica / Special Section on Quantum Optics

Free-space quantum key distribution

Distribución cuántica de claves en espacio libre

M. J. García-Martínez(*), D. Soto, N. Denisenko, V. Fernández

Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Serrano 144, 28006 Madrid, Spain.

(*) Email: mariajose.garcia@iec.csic.es

Recibido / Received: 30/10/2010. Aceptado / Accepted: 15/12/2010

ABSTRACT:

Quantum key distribution (QKD) employs fundamental laws of quantum physics to distribute secret keys required for secure communications. Free-space QKD presents several advantages over fibre-optic systems, such as the possibility of implementing QKD between any two parties worldwide or the deployment of flexible and cheaper high-bit-rate secure links in metropolitan area networks. Some techniques and requirements for successfully implementing a free-space QKD system and the challenges of transmitting through the atmosphere will be discussed in this paper.

Key words: Quantum Key Distribution, Quantum Cryptography, Free-Space Communications, Data Encryption.

RESUMEN:

La distribución cuántica de claves (QKD) emplea leyes fundamentales de la física cuántica para distribuir las claves secretas necesarias en las comunicaciones seguras. En espacio libre la QKD presenta diversas ventajas frente a los sistemas en fibra óptica, como la posibilidad de ser implementada entre dos sitios cualesquiera en la Tierra o el despliegue de enlaces seguros, rápidos y flexibles en redes metropolitanas. En este artículo se comentan las diversas técnicas y requisitos de un sistema QKD en espacio libre y los retos que se presentan con la transmisión a través de la atmósfera.

Palabras clave: Distribución Cuántica de Claves, Criptografía Cuántica, Comunicaciones en Espacio Libre, Cifrado de la Información.

REFERENCES AND LINKS

[1]. R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM 21 (1978).

[2]. M. A. Wright, "The advanced encryption standard", *Network Security* **10**, 11-13 (2001).

[3]. P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", Proceedings of the Symposium on the Foundations of Computer Science, California, pp 124–134, IEEE Computer Society Press, New York (1994).

[4]. L. K. Grover, "A fast quantum mechanical algorithm for database search", Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC), pp 212-219 (1996).

[5]. G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications", *J. Am. Inst. Elect. Eng.* **45**, 109-115 (1926).

[6]. C. H. Bennett, G. Brassard, "Quantum cryptography: public key distribution and coin tossing", Proc. IEEE Int. Conf. Comput., Syst. Signal Process., Bangalore, India, 175 (1984).

[7]. G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, "Limitations on practical quantum cryptography", *Phys. Rev. Lett.* **85**, 1330-1333 (2000).

[8]. W. Y. Hwang, "Quantum key distribution with high loss: toward global secure communication", *Phys. Rev. Lett.* **91**, 057901 (2003).

[9]. D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes, J. E. Nordholt, "Practical long-distance quantum key distribution system using decoy levels", *New J. Phys.* **11**, 045009 (2009).

[10]. Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, J.-W. Pan, "Experimental demonstration of a BDCZ quantum repeater node", *Nature* **454**, 1098-1101 (2008).

[11]. J. G. Rarity, P. R. Tapster, P. M. Gorman, P. Knight, "Ground to satellite secure key exchange using quantum cryptography", *New J. Phys.* **4**, 82.1–82.21 (2002).

[12]. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, J. G. Rarity, "Quantum cryptography: a step towards global key distribution", *Nature* **419**, 450 (2002).

[13]. H. Willebrand, B. S. Ghuman, *Free Space Optics: Enabling Optical Connectivity in Today's Networks*, SAMS, USA (2002).

[14]. J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W Clark, C. J. Williams, E. W. Hagley, J. Wen, "Quantum key distribution with 1.25 Gbps clock synchronization", *Opt. Express* **12**, 2011-2016 (2004).

[15]. H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer, H. Weinfurter, "Free space quantum key distribution: Towards a real life application", *Fortschr. Phys.* 54, No. 8 – 10 (2006).

[16]. P. G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, "New high-intensity source of polarisation-entangled photon pairs", Physical Review Letters, 75, 4337-4341 (1995).

[17]. M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, W. J. Munro, "Secure self-calibrating quantum random-bit generator", *Phys. Rev. A* **75**, 032334 (2007).

[18]. C. H. Bennet, "Quantum cryptography using any two nonorthogonal states", *Phys. Rev. Lett.* **68**, 3121-3124 (1992).

[19]. E. Waks, E. Diamanti, Y. Yamamoto, "Generation of photon number states", *New. J. Phys.* **8**, 4 (2006).

[20]. R. H. Hadfield, J. L. Habif, J. Schlafer, R. E. Schwall, S. Nam "Quantum key distribution at 1550 nm with twin superconducting single-photon detectors", *Appl. Phys. Lett.* **89**, 241129 (2006).

1. Introduction

Nowadays, in the so-called Information Age, secure high-speed communications are extremely important. The protection of sensitive data relies so far on established and standard encryption algorithms, such as RSA [1] and AES [2]. The security of these techniques lies in the unproved computational difficulty to factorize large prime numbers or to find the correct key after solving an over-defined equation system, respectively. However, if faster algorithms that speed up these mathematical calculations were discovered or a quantum computer was ever to be developed, security and worldwide electronic transactions would be seriously threatened. In this line, Peter Shor formulated a quantum algorithm in 1994 for integer factorization [3], exponentially faster than any known classical algorithm, and thus jeopardizing public key cryptography. In the same way, Grover's algorithm —developed in 1996 for searching in an unsorted database with N entries in $O(N^{1/2})$ time and using O(log N) storage space [4]—, threatens symmetric encryption.

The only unbreakable classical cipher is the Vernam cipher [5], most commonly known as the one-time-pad. Provided the secret key is as long as the message, used only once and purely random, the one-time-pad withstands any attack of an eavesdropper with unlimited computational and technological power. The need for distributing large keys constitutes its main disadvantage and has prevented its wider use. In this sense, the goal of quantum key distribution (QKD) [6] is to provide the means for reliable and unconditionally secure communication. QKD is the only way to distribute cryptographic keys between two remote parties whose security is guaranteed by the laws of quantum mechanics. Specifically its security is based on Heisenberg uncertainty principle and on the No-cloning theorem, which establishes that, unlike classical information, an unknown quantum state cannot be perfectly copied. Therefore any eavesdropping attempt to copy or measure a transmitted quantum state will disturb it, introducing errors that can be detected by sender and receiver of the key. If this error exceeds an established secure limit

and jeopardizes the secrecy of the key, the legitimate users discard the key and start a new transmission.

Thus, in short, in a QKD system there are two parties, emitter and receiver, commonly named Alice and Bob. A QKD system typically comprises two communication channels: a quantum channel and an authenticated classical channel. The quantum channel is any means where photons can propagate, such as optical fibre or free space. Concerning the classical channel, there is no need for it to be secure and therefore it can be any conventional communication channel, such as a telephone line or Ethernet connection. This channel is used for the post-processing and error correction of the raw key. A fundamental principle of QKD is that the bits of the key have necessarily to be encrypted in quantum properties of single photons. Otherwise, if the same bit is encoded using two photons, an eavesdropper could keep one of the photons without disturbing the other one and therefore without increasing the error rate. This attack is known as photon-number-splitting attack [7] and it can be counteracted using the decoy-state method [8]. There are several protocols to implement QKD. However, the goal of this work is to give an idea of the characteristics and requirements of an experimental free-space QKD system, and therefore the theoretical details of the protocols themselves will be omitted.

To exchange a secret key using quantum cryptography there are five steps to be accomplished: authentication, single-photon transmission, sifting, error correction and privacy amplification. Authentication must be performed for Alice and Bob to verify that they are in fact communicating with each other. In the next step Alice sends Bob her quantum states over the quantum channel and Bob will perform measurements on them. As there is a Heisenberg uncertainty associated with the transmitted quantum states, in some cases Bob will measure the states correctly and in other cases he will make an error. The third step, the sifting process, consists of a discussion over the public channel between emitter and receiver so that they discard the bits where Bob measured a different state from the one Alice sent. At the end of this process they both share a common sequence of bits: the sifted key. The information they exchange to distil the sifted key varies according to the QKD protocol used, but they never reveal the value of the transmitted bits. Due to the background noise and imperfections of the photon sources and detectors, there will be errors in the sifted sequences and Alice and Bob must therefore perform error correction on the public channel to eliminate all errors to a high degree of certainty. In the final step, emitter and receiver use the quantum bit error rate (QBER) information from the previous step and assume that the QBER was entirely caused by Eve's attempts to measure the photon stream. Alice and Bob then apply a technique called "privacy amplification" that XOR together sequences of bits to produce new bits, in order to reduce Eve´s possible knowledge about the secret shared sequence to less than one bit. Alice and Bob have then produced a secure key.

As mentioned above, the quantum channel where photons travel from Alice to Bob can be either optical fibre or free space. The vast majority of the practical implementations of QKD use optical fibre. However, due to losses of today's optical fibre, together with the noise of available single-photon detectors, the distance that can be bridged with current fibre-optic quantum cryptography is limited to distances of the order of 140 km [9]. In theory, larger distances could be achieved subdividing the quantum channel into shorter links. Nevertheless, it is still not possible to use quantum repeaters, since a fully functional practical quantum repeater [10] is still beyond current technology and the delicate quantum states encoding the key would be perturbed. Satellite-based systems have been studied as an alternative approach to enable key exchange among users located in arbitrary points on the globe [11]. In this sense, research on free-space QKD systems has been especially focused on increasing the transmission distance of the free-space links in locations situated far from urban areas, designed to emulate satellite-to-earth links [12].

However, no less interesting is the application of free-space QKD to short-distance high-transmission rate links located in urban

areas. Nowadays metropolitan fibre-optic networks suffer from the so-called "connectivity bottleneck", referred to an imbalance located in many parts of the network caused by requirements of flexibility and cost effectiveness of service provisioning. Possibly the most viable alternative for addressing this bandwidth shortage is Free-Space Optics (FSO) [13]. Compared to optical fibre, FSO provides more flexibility and ease of deployment in multiple architectures, and therefore an economic advantage over optical fibre. Applied to QKD, FSO offers the possibility to establish high-bit-rate and secure short links that would help in achieving high-bit-rate secure communications in metropolitan networks with a high-bandwidth demand. Various QKD systems in urban areas have already been developed throughout the world [14,15]. In the next section, the practical issues to build an experimental free-space QKD system will be discussed.

2. Free-space quantum key distribution system

The main three blocks of an experimental QKD system are the transmitter (Alice), the transmission channel and the receiver (Bob) (see Fig. 1). In the next sections, the characteristics and requirements of these three blocks when free space is chosen as the transmission channel will be briefly described.

2.a. The transmitter

The purpose of the transmitter module is to generate and transmit the quantum states whose properties are used to encrypt the bits that will constitute the secret key. As the information has to be codified in quantum properties of single photons so that the security of the system is not endangered, single photons have to be transmitted. Therefore, quantum cryptography would ideally use single-photon emitters as the source, i.e. a device that would generate exactly one photon when required.

An excellent candidate to generate single photons is a quantum dot. This approach involves the use of radiative recombination of excitons in a semiconductor. Common materials used in quantum dots are gallium arsenide, gallium aluminium arsenide or indium phosphide, and sources operating at telecom wavelengths are possible. However, though the development of quantum dots as single-photon sources has been remarkable in recent years, their still low collection efficiency and the need for cooling to liquid-helium temperatures, prevent from its wider use. Another candidate for a single-photon source is colour centres, which are the result of defects in crystal lattices caused by impurities and vacancies. Crystals with colour centres can be easily prepared to be used as photon sources as they are stable and work at room temperature. However, their main drawback is that it is difficult to find crystals with the right defects. The radiative transitions between electronic levels of a single molecule, ion or atom, can also be used to generate single-photon sources. Nevertheless, the technological complexity, since high vacuum is required, reduces its practical feasibility.

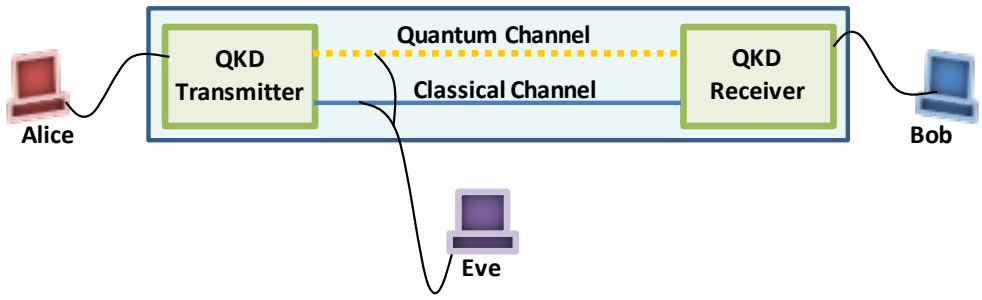

Fig. 1. Schematic of a QKD system. Alice and Bob are two remote parties that wish to share a secure secret key. Eve is a possible eavesdropper who can jeopardise the secrecy of the key. Two transmission channels are required: a quantum channel to transmit the photons that encrypt the key and a classical channel used for the post-processing of the raw key.

Currently-developed single-photon sources are still rather impractical for QKD due especially to their low collection efficiencies. Instead, the "single-photon regime" is generally achieved by strongly attenuating a pulsed laser beam to ensure that the probability of having more than one photon in a laser pulse becomes negligible. This technique is known as weak coherent pulses (WCP) or faint laser pulses and constitutes the most commonly used photon source in today's QKD systems. The electromagnetic field can be well approximated by a monochromatic coherent state, provided the spectral width of the laser pulses is much smaller than their mean wavelength. Those attenuated laser pulses, when phase randomised, follow a Poissonian distribution in the number of photons. In order to keep the probability of emission of a multi-photon pulse low, the mean number of photons is commonly set well below 1. The popularity of this technique lies in its simplicity, reliability and the possibility of reaching high repetition rates. However, this approximation has disadvantages due to the intrinsic behaviour of Poisson distribution. First, the vacuum probability is much higher than the probability of detecting a photon, so most of the pulses are empty, with the consequent decrease in the transmitted bit-rates and second, the probability of having more than one photon in a laser pulse is never zero, which has consequences on the overall security of the QKD system via beamsplitting attacks. Despite the disadvantages, WCPs have been used in the majority of QKD systems since only a standard semiconductor laser and a calibrated attenuator are needed to implement it. Another method of approximating single photons is the generation of photon pairs by parametric down-conversion [16], the phenomenon of the generation of two entangled photons when a laser beam pumps a nonlinear crystal. One of the photons is used as the trigger for the second photon, so that the second detector is activated only when the first one receives a count, and thus solving the problem of the empty pulses. The disadvantage of this technique is that the photon-pair creation process is highly inefficient so it is only worth substituting faint laser pulses for this technique when the entanglement of the photons is going to be exploited.

Figure 2 shows the blocks of a QKD transmitter. The electronic part of the system is used to generate the key. Ideally, Alice would use a "true" random number generator [17], although in experimental systems pseudo-random bit sequences generators constitute a practical alternative. The electronic sequence will serve to modulate the laser sources. Unlike optical fibre, the atmosphere exhibits almost no birefringence, which allows encoding the quantum information into the polarisation of photons. Depending on the QKD protocol, two or four polarisation states are used. Due to the inherent divergence of electromagnetic beams, they need to be expanded when transmitted at long distances to avoid large beam diameters at the receiving end. Moreover, due to turbulences in the atmosphere, the output beam will wander at the receiver. Therefore, to facilitate alignment tasks and to enhance the reception rate, it is also useful to have an enlarged output beam at the emitter, which will be accomplished by an output telescope.

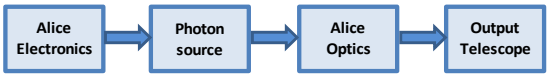

Fig. 2. Diagram of a free-space QKD transmitter. The electronic block is used to generate the random electronic sequence that modulates the laser source. The optics part provides the quantum states wherein the bits of the key are encrypted. The beam will be expanded and sent to the receiver using an output telescope.

2.b. Free space as the quantum channel

The transmission channel is the physical medium that will transport the quantum states between sender and receiver of the QKD system. It has a fundamental role, since it must preserve the quantum states encoding the binary data (hence the name it receives sometimes as the quantum channel). As mentioned in the first section there are two main candidates for a quantum channel: optical fibre and free space. The majority of the practical implementations of QKD use optical fibre at distances of up to 100-200 km. However the range is being limited by detectors' noise and absorption in the transmission medium. FSO can contribute to dramatically increase the range of the networks implementing QKD.

As mentioned in the previous section, the atmosphere does not perturb considerably the polarisation of the quantum states since it is a non-birefringent medium at optical wavelengths and does not need the type of compensation required in a fibre-optic implementation. Moreover, the existence of a low absorption window at wavelengths near 800 nm, where efficient single-photon detectors are available, makes this medium attractive for a QKD system. However, there are some issues concerning a free-space channel that need to be addressed and will be discussed in the following.

One is the beam divergence, unavoidable for all electromagnetic beams. This has to be taken into account by correctly designing the apertures of both the emitter and transmitters' telescopes. In a security analysis channel losses are attributed to Eve, who can split off a part of each signal state and perform measurements on it, and therefore a low-loss channel is desirable since it also allows for higher key rates. In clear weather conditions, atmospheric attenuation in the transmission windows (between 780 and 850 nm) is indeed low (< 0.1 dB km^{-1}). Turbulence in the atmosphere, especially at low altitudes and in urban areas, can lead to fluctuations of the beam position at the receiver and time jitter of the signal due to the changes in the refractive index of the optical path. Although this effect is not a fundamental limitation, it might lead to additional detection losses. The receiver should therefore be designed to collect all the incoming light by choosing appropriate aperture diameters. Since the fluctuations in the atmosphere are slow (0.01 s to 0.1 s) the time jitter can be compensated for by sending to the receiver a bright short-duration pulse at another wavelength. This timing pulse would contain no information but would allow the receiver to open a definite timing window where photons are expected, reducing the jitter. To ensure the required stability and efficiency of the optical link in the presence of atmospheric turbulence, the two telescopes in the transmitter and receiver must be equipped with a bi-directional tracking system. Faster fluctuations of the beam could be tackled by monitoring a reflected component of the signal and actively compensating for it with beam steering methods.

Another aspect of free-space QKD systems that needs special attention is the background photons from the sunlight or other sources of ambient light. They are collected by the detectors causing an increase in the error rate. However, several techniques can be applied to reduce this effect. Some of them involve the use of small solid angles for photon acceptance (spatial filtering), the use of narrow wavelength filters (spectral filtering) and the use of the appropriate time windows in the post-transmission analysis (software filtering).

2.c. The receiver

A receiver of a QKD system has to be able to detect single photons, since each photon carries one bit of information, in contrast with standard communications in which more than one photon represent each binary value. The main parameters characterizing single-photon detectors are the quantum efficiency, which represents the probability of a detector click when the detector is hit by a photon, and the dark count rate, characterizing the noise of the detector—dark counts are events when a detector sends an impulse even if no photon has entered it. An important parameter is also the dead time of the detector, i.e., the time it takes to reset the detector after a click. These three quantities are not independent. Most often, the overall repetition rate at which the detector can be operated is determined by the dead time. An ideal detector for a QKD system should have good detection efficiency, low dark noise, low timing jitter and low dead time.

The most commonly used detectors in QKD systems are single photon avalanche diodes (SPADs), which are avalanche photodiodes (APDs) biased slightly above the avalanche breakdown voltage, where the electric field applied to the union is so high that the absorption of a single photon creates an avalanche of electrons that generates a detectable pulse. Specifically, for wavelengths in the interval approximately 400–1000 nm Si SPADs can be used; for wavelengths from about 950 to 1650 nm, including telecom wavelengths, InGaAs/InP SPADs are most often applied, although these have very high background rates

and low efficiencies relative to those available for shorter wavelengths. Moreover, SPADs at these wavelengths are plagued with a phenomenon known as 'afterpulsing' which strongly limits the operation of these detectors at high rates and need to be cooled down. Si SPADs though, can be operated at room temperature, which makes these detectors a good candidate for practical QKD.

Other types of single-photon detectors are also being developed. For instance, visible light photon counters (VLPCs) are semiconductor detectors that can also distinguish the number of impinging photons [19]. Other photon detectors are based on the superconducting effect, for instance superconducting single photon detectors (SSPDs) [20] and transition edge sensors (TESs). A common weakness of all these types of detectors is that they must be operated at cryogenic temperatures.

Figure 3 represents a schematic of the typical receiver of a QKD system. In order to maximize the coupling efficiency Bob must be precisely pointed at Alice. Bob will use an input telescope to efficiently focus the beam coming from Alice. Bob's optics will spatially separate the different quantum states that encrypt the key. Several single-photon counting modules (the number depends on the protocol used) will determine where the photon emerges and thus its quantum state. Finally, to reconstruct the received signal an electronic time processing card with sufficient sensitivity must be used, as for instance a Time Interval Analyzer (TIA). This card will detect the arrival time of each of the photons that reach the receiver. These times will then serve to reconstruct the signal Alice sent and determine whether the transmission of the key has been secure or not by analysing the QBER of the transmission.

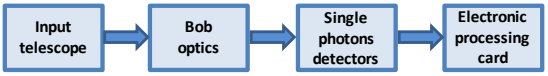

Fig. 3. Diagram of a free-space QKD receiver. The telescope focuses the beam coming from Alice into Bob's optics, which spatially separates the different quantum states. The single-photon detectors will transform the received photons in output voltage pulses that will be then sent to the electronic processing card to be processed and analyzed.

3. Conclusions

Free-space QKD schemes offer a solution to the distance restriction suffered from fibre-optic QKD systems. A potential application of particular interest is secure satellite-to-ground communications to allow key exchange among users located in arbitrary points on the globe. FSO QKD may be also well suited for ground-to-ground applications over campus or metropolitan areas with high-bandwidth demand. On a first glance free-space QKD presents more challenges than QKD in optical fibre. Fortunately, the atmosphere is a non-birefringent medium at optical wavelengths and provides several transmission windows where high-efficiency low-noise commercial single-photon detectors are available. The background can be reduced using a combination of spectral, spatial, and temporal filtering, and the acquisition, pointing and tracking requirements to establish and maintain the quantum channel can be also effectively solved by using techniques involving FSO and laser communication.

Acknowledgements

We would like to thank the Ministerio de Educación y Ciencia, project MTM2008-02194 and CDTI, Ministerio de Industria, Turismo y Comercio (Spain), in collaboration with Telefónica I+D, project SEGUR@ with reference CENIT-2007 2004.

