HOW IS QUANTUM CRYPTOGRAPHY USED FOR SECURE FINANCIAL TRANSACTIONS?

Sanwar Ali and Waleed Farag
Department of Computer Science
Indiana University of Pennsylvania
Indiana, Pennsylvania 15705, USA
Email: {sanwar, farag} @ iup.edu

ABSTRACT

In recent years quantum physicists have proposed a new type of cryptosystem known as quantum cryptography (QC) which has proven promising for online security in public key infrastructure (PKI). Researchers are now examining QC as a possible alternative to classical encryption algorithms, such as AES, RSA. Unlike many classical encryption algorithms, QC does not depend on factoring large integers into their primes but on the fundamental principles of quantum physics. It is more secure because an intruder will never be able to replicate a photon to recreate the key. QC allows the exchange of cryptographic keys, a method known as quantum key distribution (QKD), whose security is guaranteed by quantum physics. Any eavesdropping will change the state of the photon that will alarm the user of the presence of hacking. Once cryptographic keys have been exchanged, strong cryptographic algorithms are used to encrypt and decrypt the flow of data transmitted over an optical fiber. QC would allow users to overcome the vulnerabilities of public key cryptography. The paper reviews the systematic and chronological development of QC, pioneering methods of QKD, QKD products, secure quantum networks, and finally how QC has been used to securely transfer funds in Europe.

KEYWORDS

Quantum cryptography, secure financial transaction, quantum key distribution, entangled photon, quantum computer

1 ONLINE SECURITY CONCERNS AND PROBLEMS WITH PUBLIC KEY CRYPTOGRAPHY (PKC)

Online banking is increasingly becoming more complex and sophisticated because of mobile networking. As mobile phones are becoming more popular to surf the Internet, check account balances and transfer funds between accounts worldwide, their role in Internet banking has becoming increasingly significant. As wired and wireless banking are becoming more popular worldwide, their securities continue to be major concerns among consumers. Banks and other financial institutions have been using secure PKC, particularly the RSA algorithm, for online security. However, due to the advent of sophisticated technology and cryptanalysis techniques, security solutions in PKC are now uncertain. The success of PKC depends on the mathematical difficulty of factoring very large numbers. With increasing computing power, a 1024-bit key in RSA will be vulnerable in the near future. As computers become more powerful, encryption and decryption keys have to be longer in order to retain the level of difficulty. For example, in 1994 Citibank was hacked by Vladimir Levin who electronically transferred $12M from the New York Citibank to accounts in Finland, Israel, California, the Netherlands, Germany, Switzerland, and the Caribbean [1]. Ovum, a U.S. based research group, conducted a survey in 1998 among 400 corporate users in Germany, Spain, Sweden, and UK and the result revealed that up to 57% of users were concerned about secure e-commerce over the Internet [2]. Most recently, Alexey Mineev from New Hampshire was convicted for stealing $112,000 using a bank account hacking scheme [3]. Mineev set up several “drop accounts” that were wired stolen funds from banking and brokerage accounts by installing malicious Trojan horse software on victims’ computers. This is another example of the account theft that is a growing problem for banks and brokerage firms.

2 THE BASIC PRINCIPLES OF QUANTUM CRYPTOGRAPHY (QC)

Unlike conventional cryptography, QC is not threatened by the advancement of computing power, new mathematical algorithms, or by the development of quantum computers in the near future. Instead of using a 1024-bit long integer as the key in classical encryption algorithm, such as RSA, photons are used for QKD because its security is guaranteed by the principles of quantum physics.

QC is no longer confined to only laboratory research; rather, it is now being used by financial institutions and government agencies for secure transmission of sensitive information.

In 1979, Charles Bennett and his colleagues invented QC using the concept from quantum physics. They published their research in 1982 [4] and 1984 [5]. According to quantum mechanics, light has a dual nature: “wave” and “particles” (known as photons). Heisenberg’s uncertainty principle states that ‘there exist ultimate, insuperable limitations in the precision of our measurements’. QC is based on this Heisenberg’s uncertainty principle which guarantees that any eavesdropping activities will cause “an irreversible change in the quantum states” i.e. the wave function of photons will be collapsed and the recipient will be alerted [6]. Hughes *et al.* [6], [7] and Bennett *et al.* [4], [5], [8] thoroughly discussed the basic theory of QC in their papers.

QC employs individual photons that can be polarized in four specific directions, such as parallel (0^0), perpendicular (90^0) and two diagonals ($+45^0$ and -45^0), to create and transmit code. The sender transmits photons in one of the above four polarizations at random. The recipient at the other end also chooses any of the above four polarizations at random and records his measurements using a detector. A polarized photon can only be detected by a detector with the correct polarization; otherwise the photon will be destroyed. This detection criteria and the inherent randomness of quantum mechanics led to the invention of QC [9]. The 0s and 1s of the binary system are represented by the direction in which a photon’s electric field vibrates [10]. However, QC suffers from potential drawbacks with this technology. For example, laser sources with weak pulses may contain no photons or more than one photon. This extra photon, five or ten years later, might ‘enable an eavesdropper to steal photons from the signal and secretly gather information about the encryption key’. In the following sections various QKD methods are discussed.

3 QUANTUM KEY DISTRIBUTION (QKD)

QC can be used to distribute keys for PKI, a process known as QKD. The current problems with PKI are finding secure ways to deliver the keys necessary for secure and authenticated transactions. QC can support PKI by delivering those keys securely [9]. QKD is a method of distribution of secret keys in the form of light particles, known as photons, with unconditional security. Bennett and Brassard [5] published the first paper on a cryptographic protocol called BB84 protocol in 1984. It describes an unconditionally secure QKD system using single photons. Bennett and Brassard developed a quantum mechanical channel consisting of a device that transmits single photons whose orientation is horizontal (0^0), vertical (90^0), or one of the two diagonals ($+45^0$ and -45^0). A detector at the recipient end reads the polarization of the incoming photons. When the photon and the detector both are oriented in the same way, the detector is able to determine photons’ polarization (0^0, 90^0, $+45^0$, and 45^0) correctly. However, if the orientations of both photon and detector are different, the results are random.

In 2002, BBN Technologies implemented QKD in Internet Protocol Security (IPSec) [11]. The idea of QKD has been tested in physics laboratories. Most recently, a team from the University of Geneva and IdQuantique has demonstrated the ‘first fully integrated quantum cryptography prototype machine’ across a telecommunications network [12]. Even though this advancement is limited to fiber optic networks now, scientists are investigating how quantum keys can be shared over satellite or wireless networks. Richard Hughes and his team at the Los Alamos National Lab (LANL) have been working on a new way of transmitting QKD by photons so that it can be exchanged over radio networks [13], [14], [15].

QKD could be integrated in existing algorithms and protocols to secure communication networks. The Point-to-Point protocol (PPP), IPSec protocol and Transport Layer Security (TLS) can support the use of QKD [16]. QKD in PPP (or Q3P) requires three main features. First, an optical medium is necessary to provide the physical link between two adjacent nodes. At present, optical fiber and free-space are being used to carry QC transmission [15]. Second, a Q3P modem that includes a photon detector, a laser with single photon emitter, and a photon polarizer is needed. In recent years, various photon emitters and detectors have been developed by two leading companies, IdQuantique and MagiQ. Third, a QKD protocol must be implemented in the Q3P modem.

Stucki *et al.* [17] presented a QKD protocol to exchange keys over 67km between Geneva and Lausanne. Scientists from LANL and NIST achieved QKD at the telecom industry's wavelengths in a 50km optical fiber using new superconducting transition-edge sensors (TES). "TESs detect photons by measuring minute temperature increases in a superconducting material caused by the absorption of individual photons" [18]. Recently, Ursin *et al.* [19] experimentally demonstrated entangled-based QKD over 144km. One photon was measured locally at La Palma and the other was sent over an optical free-space link to Tenerife of the Canary Islands, where it was received by the Optical Ground Station of the European Space Agency. This experiment is an important 'step towards future satellite-based quantum communication'. The systematic development and improvement of QKD are shown in Table 1.

3.1 Entangled Photons (or Quantum Entanglement)

Quantum entanglement is a quantum mechanical property that allows two photons to behave the same no matter how far apart they are. The state of one photon instantly measures the state of the other. Researchers have developed a new form of QC based on quantum entanglement that uses a specially prepared crystal to split a single photon into a pair of entangled photons. Although the state of each photon in the pair is undetermined, the entangled photons can influence each other even if they are far apart spatially. Quantum mechanics states that the polarization properties of a photon can be in a combination of states until it is measured. The photon then gains a definite polarization and can represent a particular value to build a key. So, while each photon in the entangled pair can be detected as either a 0 or 1, once the polarization of one photon in the pair is determined, the second photon in the pair must adopt an identical polarization.

Quantum entanglement can thus be used to share an encryption key by two users. Each user receives one photon from the entangled pair. Both users then randomly make one of the two types of polarization measurements. When the same type of measurement is not used, the results are discarded. Entangled photons can be shared by two distant observers and therefore can be used in QC to establish an unconditionally secure key. QC works by checking the polarization of a pair of entangled photons to ensure that a key has not been intercepted. Jennewein *et al.* [20] established highly secure keys by realizing a QC system based on polarization of entangled photon pairs. Tittel *et al.* [21] made an experimental set up for QC based on photon pairs in energy-time Bell states. Naik *et al.* [22] implemented the Ekert QC protocol using entangled photon pairs. A research team from the University of Vienna, Austria successfully transmitted entangled photons across the Danube River. This technique could be a vital step towards ultra-secure QC using satellites to beam entangles photons to the earth [23]. The systematic improvements in producing entangled photons and their use in QC are shown in Table 1.

3.2 Decoy State Photons

Hwang [24] first proposed a decoy-state method to overcome the Photon-Number-Splitting (PNS) attack for BB84 QKD protocol in presence of high loss. In this method, 'a legitimate user intentionally and randomly replaces signal pulses by multiphoton pulses', known as decoy pulses. The yield of the decoy pulses is then measured, and if it is abnormally higher than that of other signal pulses, the protocol is aborted. Otherwise, the yield of signal multiphoton pulses is estimated based on that of decoy pulses.

Although QKD has been successfully performed over 150km of commercial telecom fibers, these QKD experiments with available hardware may have been vulnerable to eavesdropping attacks - for example, in the case of standard BB84 protocol. This is because highly attenuated lasers are used as sources for photon and these sources sometimes produce signals that contain more than one photon. These multiphoton signals may be vulnerable to eavesdropping attacks including PNS attack. For example, when a sender transmits some secret data to the recipient, hackers, in principle, can 'measure the photon number of each signal' transmitted by the sender and 'selectively suppress single photon signals' [25]. The hacker then splits multiphoton signals and sends one copy to the recipient, keeping the other copy for himself. This way the hacker possesses an identical copy of what the recipient has and therefore, the unconditional security is compromised. The standard BB84 protocol is guaranteed to be secure for signals originated from single photon pulses, not from multiphoton signals. Lo *et al.* [25] proposed a method of using decoy state photons, based on the idea first proposed by Hwang, to detect eavesdropping attacks. The idea of decoy state photons is that the sender transmits a set of additional photons, known as decoy state photons, along with standard BB84 photons. Decoy state photons are used in detecting eavesdropping attacks only and standard BB84 photons are used for key generation.

Using the decoy state method, Zhao *et al.* [26] presented the first experimental implementtation of decoy state QKD over 15km of telecom fiber. Later, Zhao *et al.* used a commercial QKD system, slightly modified by adding commercial variable attenuators, to accomplish higher key generation rates and achieve longer distances up to 60km. Peng *et al.* [27] demonstrated the decoy-state QKD with one-way quantum communication over 102km. Rosenberg, *et al.* [28] incorporated ultra-low-noise, high-efficiency transition-edge sensors into a one-way QKD system and implemented a three-state decoy protocol to successfully generate key secure against PNS and Trojan horse attacks over 107km of optical fiber. Schmitt-Manderbach *et al.* [29] did successful experimental demonstration of free-space decoy state QKD over 144km between the Canary Islands of La Palma and Tenerife. Most recently, Liu *et al.* [30] implemented a decoy-state QKD over 200km with photon polarization transmitted by optical fiber cable.

3.3 Differences between QKD using Entangled Photons and Decoy State Photons

- QKD via quantum entanglement relies on pairs of entangled photons.
- Measuring one of an entangled pair immediately affects its counterpart, no matter how far apart they are spatially.
- Entanglement is an extremely delicate condition because any background perturbation readily destroys the quantum state. This alerts the presence of any interception.
- Highly attenuated lasers, used as sources for photons, produce signals that contain more than one photon. These multiphoton signals may be vulnerable to eavesdropping attacks including PNS attacks. QKD via decoy state photons detect these attacks.
- Decoy state photons are transmitted along with standard photons. Decoy state photons detect eavesdropping attacks and standard photons generate the cryptographic key.

4 QKD PRODUCTS

Since photons, the carrier of information, cannot be duplicated due to the fundamental principles of quantum physics, an eavesdropper on a secure transmission can be immediately detected. National Physical Lab (NPL) in UK has been investigating technologies 'to underpin the security of online shopping and international financial transactions' using QC [31]. Even though various QC products are available in the market today, they are not yet standardized by national measurement institutes, such as NPL. NPL has been conducting a project named Entangled Photons in Quantum Metrology for the UK National Measurement System in collaboration with Cambridge University and Imperial College.

4.1 IdQuantique

IdQuantique, founded by a group of physicists at the University of Geneva, is the world-recognized first and leading company that has been producing various QC products commercially since 2001. It has been at the forefront of the advancement of this technology and is delivering cryptographic products, such as photon sources and detectors, and fiber optic connections needed for key exchange and uncompromised network security to service providers, enterprises and administrations. IdQuantique also offers Quantum Random Number Generators (QRNG) that are deployed by cryptographic equipment, such as hardware secure modules and virtual private networks manufacturers. The company is one of the recipients of the 2001 European Innovation Award from the Wall Street Journal Europe, as well as of the 2002 and 2004 Swiss Technology Awards, in recognition for its pioneering work in the field of QC. In March 2002, IdQuantique had used the system to send single photons through 67km telecommunication cables running under Lake Geneva [32]. IdQuantique developed three types of products discussed below.

4.1.1 Clavis

The Id3000 Clavis is a QKD System by which secure key exchange becomes possible up to 100km. This system is the most flexible product of its kind on the market. Clavis uses an auto-compensating optical platform that has been extensively tested and characterized. It features outstanding stability and interference contrast and guarantees low quantum bit error rate. The exchanged keys can be used in an encrypted file transfer application, which allows secure communications between two stations [33]. Clavis uses triple-DES and AES 128-bit, 192-bit or 256-bit encryption. The system uses BB84 and SARG protocols for QKD.

4.1.2 Vectis

Vectis Link Encryptor is a new product of IdQuantique. It allows secure communications between remote networks connected by an optical fiber up to 100km. Vectis Link Encryptor is a complete network-transparent QC device for point-to-point wire-speed link encryption. It combines QKD and AES encryption protocol in a stand-alone unit. It securely bridges two Fast Ethernet (IEEE 802.3u) fiber optic networks and provides an AES 128-bit, 192-bit, or 256-bit Layer 2 encryption engine. Vectis also uses BB84 and SARG protocols for QKD [34].

4.1.3 Quantis

The generation of random numbers is required in QC, and hence a physical source of randomness is necessary. ‘Quantum physics being intrinsically random, it is natural to exploit a quantum process for such a source’. QRNGs are not vulnerable to any environmental perturbations. Quantis is a physical random number generator exploiting an elementary quantum optics process and is used in connection with a computer or server. Photons are sent one-by-one onto a semi-transparent mirror and detected. Reflection and transmission are associated to 0-bit and 1-bit, respectively [35].

4.2 MagiQ

MagiQ Technologies was founded in 1999 in New York with its R&D based in Massachusetts. Navajo, the MagiQ’s first product, is ‘a quantum cryptographic solution offering unbreakable encryption’ based on quantum mechanics. Navajo’s real-time key generation and QKD make the cryptographic system most secure [36], [37]. It provides intrusion detection and protections from both internal and external threats. The potential customers for this product are large financial institutions, the Pentagon, defense contractors, and the gaming industry.

5 SECURE QUANTUM NETWORKS AND FINANCIAL TRANSACTIONS

In 2004, the European Union launched a project entitled “Development of a Global Network for Secure Communication Based on Quantum Cryptography (SECOQC)” with 41 partners of 12 European countries with a budget of 11.4M Euros [38]. SECOQC would be a global high-security communications network for secure financial transactions. On April 21, 2004 the *Bank Austria Creditanstalt* performed the world's first secure financial transaction via QC based on a pair of entangled photons [39]. This breakthrough technology was demonstrated by a group of scientists from the University of Vienna in collaboration with another group from Quantum Technologies. At the bank (sender), a pair of entangled photons was created by a laser passing through a crystal to split a single photon into two. One of the two entangled photon pairs was transmitted to the City Hall (recipient) through a 1,450m long fiber optic cable, and the other remained at the bank. Both the detector and transmitter measured properties of these two entangled photons and the measurements were then converted into strings of 0s and 1s. The sequence of 0s and 1s was completely random, and it was observed that identical strings of these numbers, known as cryptographic keys, were produced at both the sender and recipient ends. This key was used to encrypt information. No eavesdropping was observed because both the sender and recipient had identical key. This team intends to develop a commercial QC system for ultra-secure financial transactions using entangled photons [39].

In June 2004, BBN Technologies, in collaboration with DARPA, built the world's first QC network (also known as Quantum Net or Qnet) which has been operating beneath the streets of Cambridge, MA [40]. Even though the Qnet currently only consists of six servers, it can be integrated with regular servers and clients on the Internet. The implementation of more nodes in banks and credit card companies with the Qnet could make more secure data exchange over the Internet possible. Qnet is the first network consisting of more than two nodes to use QC. This network would be extended to the campus of Harvard and Boston Universities.

BBN Technologies built the world's first continuously operating QC network, a 12-mile long pilot stage network running under the streets of Cambridge and Boston [41]. The network has ten nodes and currently runs at up to 5Mbps. BBN predicted that financial firms would deploy QC within a few years and estimated that business would deploy within five years. The technology could move to the consumer market to protect the network between the home and the service provider, which is composed of two networks, one for QKD and the other which carries the encrypted traffic.

Mitsubishi and NEC developed a QC network system for the first time in Japan. They made a successful interconnection with the University of Tokyo [42]. Previously, there had been no standardization in encryption algorithms or optical devices, and it was, therefore, impossible to interconnect different systems. The new interface and shared encryption key allows for interconnection of different cryptography systems.

IdQuantique intended to bring QC to 'mainstream optical communications'. Its Vectis link encryptor would be installed in a data center as part of a pilot project that would provide business enterprises with a trail technology for secure data transaction [43]. IdQuantique, the University of Geneva, and the Univ. of Applied Sciences of Western Switzerland deployed a QC network that has been running for more than six months [44]. This network, known as Swiss Quantum network, distributes encryption keys to any of its three nodes. These keys are serving as 10GB Ethernet encryption for secure communications between CERN and the University of Geneva.

Quantum keys could not travel long distance through fiber optic links because of random noise. To send a signal over a longer distance, it is required to amplify the signal periodically using a series of repeaters without disturbing the polarization of the photons. This requires a quantum repeater that would first detect one photon and then send the other with the same polarization. Recently, researchers at Toshiba's European Lab in England developed a detector, known as avalanche photo-diode (APD) that uses a semiconductor-based sensor to detect photons [45]. Every photon that arrives at the APD triggers an avalanche of electrons.

The first commercial communication network using secure encryption based on QC was demonstrated in Vienna, Austria. The encryption utilizes keys that are generated and distributed by means of QC technologies. Government agencies, financial institutions, etc. are the potential users of this network, and they can encrypt their confidential communication with the highest level of security. The network consists of six nodes and eight intermediary links with distances between 6km and 82km. Seven links utilize commercial standard telecom fiber optics. One link exists in free-space along a line-of-sight between two telescopes. The links employ six different QC technologies for key generation which are integrated into the network over standardized interfaces [46]. The network is installed in a standard fiber optic communication ring. This system could allow online transactions to be PIN protected. The user would use secret bits shared with the bank to encode his/her PIN. The major advantages in a QC network are the following: longer distances can be bridged and alternative paths between two parties can be automatically chosen to increase key generation throughput or prevent denial-of-service attacks. Additionally, more than two partners can simultaneously obtain keys.

5 CONCLUSIONS

This paper first discussed the fundamental principles of QC as promising solutions to resolve security problems that occur in traditional cryptographic techniques. The paper then briefly reviewed the pioneering developments in QKD methods, such as entangled photons and decoy state photons. A number of contemporary research achievements in using QC to secure financial transactions and establish secure networking were presented. Current challenges facing QC systems were also identified, such as the need for effective repeaters to enable the transmission of light signals over longer distances. Furthermore, representative novel innovations in the field, such as avalanche photodiode, were discussed. This survey paper provided a detailed list of various achievements and milestones in the field which provides a valuable resource for researchers working in the area of QC. In the near future, all financial institutions, government agencies, and corporations may routinely use QC to transmit sensitive and secrete data; and to perform financial transactions securely worldwide. It is also possible that mobile banking via smart phones may use quantum cryptography within decades or less.

6 REFERENCES

1. URL: http://my.safaribooksonline.com/078972801X/ch07lev1sec7
2. Young, K.: "Online security threatens banks", The Banker, Vol. 49(883), 21(3), 1999.
3. McMillan, R.: "Man made $112,000 in bank account hacking scheme", Computerworld Security, June 2009, URL: http://www.computerworld.com/s/article/9134041/Man_made_112_000_in_bank_account_hacking_scheme
4. Bennett, C.H., Brassard, G., Breidbard, S., Wiesner, S.: "Quantum Cryptography, or Unforgivable Subway Tokens", *Proceedings of Crypto 1982*, Santa Barbara, California, pp 267-275, 1982.
5. Bennett, C.H. and Brassard, G.: "Quantum cryptography: Public key distribution and coin tossing", *Proc. of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, 175-179.
6. Hughes, R.J. *et al.*: "Quantum cryptography over underground optical fibers", *Crypto96-Proc. of the 16th Annual International Cryptology Conference on Advances in Cryptology*, Springer-Verlag, 1996, London, UK, ISBN: 3-540-61512-1.
7. Hughes, R.J. *et al.*: "Secure communications using quantum cryptography", in Photonic Quantum Computing, Eds. S.P. Hotaling and A.R. Pirich, Vol 3076, 2-11, 1997.
8. Bennett, C.H., Brassard, G. and Ekert, A.K.: "Quantum Cryptography", Scientific American, 50-57, October 1992.
9. DeJesus, E.: "Cryptography: Quantum Leap", Information Security, August 2001.
10. Harrison, A.: "Basically Uncrackable; New techniques use the laws of quantum physics to develop encryption systems that should by virtually fail-safe hackers", Computerworld, June 19, pp 82(1), 2000.
11. Elliott, C.: "Building the quantum network", New Journal of Physics, Vol. 4(1), 46.1-46.12, 2002.
12. Leyden, J.: "Team demos first quantum crypto prototype machine", The Register, 2002. URL: http://www.theregister.co.uk/2002/07/17/team_demos_first_quantum_crypto
13. Buttler, W.T. *et al.*: "Free Space Quantum Key Distribution", Physics Review-A, Vol. 57, 2379-2382, 1998.
14. Hughes, R. and Nordholt, J.: "Quantum cryptography takes to the air", Physics World, 31-35, May 1999.
15. Hughes, R. *et al.*: "Practical free-space quantum key distribution over 10km in daylight and at night", New Journal of Physics, Vol. 4(43), 1-14, July 2002. URL: http://iopscience.iop.org/1367-2630/4/1/343
16. Sfaxi, M.A., Tashi, I., Hélie, S.G.: "How QKD can improve the security level of future e-commerce transaction", *Proc. 18th European Regional*

International Telecommunication Society Conf. (ITS2007), Istanbul, 1-12, September 2007.

17. Stucki, D. *et al.*: "Quantum key distribution over 67km with a plug&play system", New Journal of Physics, Vol. 4 (41), 1-8, 2002.
18. "New Technologies Enhance Quantum Cryptography", Science Daily, February 2, 2006. URL: http://www.sciencedaily.com/print.php
19. Ursin, R. *et al.*: "Entanglement-based quantum communication over 144km", Nature Physics, Vol. 3, 481-486, July 2007.
20. Jennewein, T. *et al,*: "Quantum Cryptography with Entangled Photon", Physics Review Letters, Vol. 84(20), 4729-4732, May 2000.
21. Tittel, W., Brendel, J. Zbinden, H., and Gisin, N.: "Quantum Cryptography Using Entangled Photons in Energy-Time Bell States", Physics Review Letters, Vol. 84(20), 4737-4740, May 2000.
22. Naik, D.S. *et al.*: "Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol", Physics Review Letters, Vol. 84(20), 4733-4736, May 2000.
23. Ananthaswamy, A.: "Entangled photons dance across the blue Danube", New Scientist, Vol. 178(2401), 15, June 2003.
24. Hwang, W.Y.: "Quantum Key Distribution with High Loss: Toward Global Secure Communication", Physics Review Letters, 91(5), August 2003.
25. Lo, H-K, Ma, X, and Chen, K.: "Decoy State Quantum Key Distribution", Physics Review Letters, Vol. 94(23), June 2005.
26. Zhao, Yi *et al.*: "Experimental Quantum Key Distribution with Decoy States", Physics Review Letters, Vol. 96(7), 2006.
27. Peng, C-Z *et al.*: "Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding", Physics Review Letters, Vol. 98, January 2007.
28. Rosenberg, D. *et al.*: "Long-distance decoy-state quantum key distribution in optical fiber", Physics Review Letters, Vol. 98, 2007.
29. Schmitt-Manderbach, T. *et al.*: "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144km", Physics Review Letters, Vol. 98, January 2007.
30. Liu, Y. *et al.*: "Decoy-state quantum key distribution with polarized photons over 200km", Optics Express, Vol. 18(8), 8587-8594, April 2010.
31. "Quantum cryptography prevents financial fraud", URL: http://www.npl.co.uk/commercial-services/case-studies/quantum-cryptography-prevents-financial-fraud
32. "Can you keep a secret?", Nature, Vol. 418, 270-272, July 2002.
33. URL: http://www.idquantique.com/scientific-instrumentation/clavis2-qkd-platform.html
34. URL: http://www.whygeneva.org/index.php?option=com_content&task=view&id=662&Itemid=240&lang=en
35. URL: http://www.idquantique.com/true-random-number-generator/quantis-usb-pcie-pci.html
36. "MagiQ Technologies Launches with $6.9 Million in Seed Funding to Commercialize Advancements in Quantum Information Processing", Business Wire, November 4, 2002.
37. "MagiQ Technologies Offers a Different Kind of Grid Security", Grid Today, Vol. 1(23), November 18, 2002.
38. "European Scientists against Eavesdropping and Espionage", URL: http://www.secoqc.net/downloads/pressrelease/SECOQC_english.pdf, 2004.
39. "World Premiere: Bank Transfer via Quantum Cryptography Based on Entangled Photons", April 21, 2004, URL: http://colossalstorage.net/quantum_entanglement_austria.pdf
40. "First quantum cryptography network unveiled", New Scientist, June 4, 2004.
41. Schurr, A.: "Hooked on photonics", Network World, May 2, 2005. URL:http://www.networkworld.com/news/2005/050205widernet.html.
42. URL: http://phys.org/news66661337.html or, http://www.nec.co.jp/press/en/0605/1201.html
43. "Quantum cryptography targets the data centre", July 17, 2006, URL: http://fibers.org/articles/news/8/7/7/1
44. "Quantum Cryptography Network Up and Running for 12,000 hours", URL: http://www.prnewswire.co.uk/cgi/news/release?id=268306
45. Marks, P.: "Photon counter extends quantum communication systems", New Scientist, Vol. 198(2661), 32, June 2008.
46. "World first for sending data using quantum cryptography", URL: http://www.bris.ac.uk/news/5941.html
47. Wiesner, S.: "Conjugate coding", SIGACT News, Vol. 15(1), 78-88, 1983.
48. Feynman, R.: "Simulating physics with computers", International Journal of Theoretical Physics, 1981.
49. Deutsch, D.: "Quantum computers key to deeper knowledge", URL: http://earthsky.org/human-world/quantum-computers-key-to-deeper-knowledge
50. Bennett, C.H. *et al.*: "Experimental quantum cryptography", Journal of Cryptology, Vol. 5(1), 3-28, 1992.
51. Ekert, A.K.: "Quantum cryptography based on Bell's theorem", Physics Review Letters, Vol. 67(5), 66-663, 1991.

52. Bennett, C.H.: "Quantum cryptography using any two non-orthogonal states", Physics Review Letters, Vol. 68, 3121-3124, 1992. URL: http://prola.aps.org/pdf/PRL/v68/i21/p3121_1

53. Townsend, P.D., Rarity, J.G. and Tapster, P.R.: “Single photon interference in a 10km long optical fibre interferometer”, Electronics Letters, Vol. 29, 634-635, 1993.

54. Shor, P.: “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”, URL: http://www.physics.princeton.edu/~mcdonald/examples/QM/shor_ieeefcs_35_124_94.pdf

55. Kwait, P.G. *et al.*: “New High-Intensity Source of Polarization-Entangled Photon Pairs”, Physical Review Letters, Vol 75(24), 4337-4341, December 1995.

56. Zbinden, H. *et al.*: “Interferometry with Faraday mirrors for quantum cryptography”, IEEE Electronics Letters, 33(7), 586-588, March 1997.

57. Bourennane, M. *et al.*: “Experiments on long wavelength (1550nm) "plug and play" quantum cryptography systems”, Optics Express, Vol. 4(10), 383-387, 1999.

58. Poppe, A. *et al.*: “Practical quantum key distribution with polarization entangled photons”, Optics Express, Vol. 12 (16), 3865-3871, August 2004.

59. Buttler, W.T. *et al.*: “Daylight Quantum Key Distribution over 1.6 km”, Physics Review Letters, Vol. 84(24), 5652-5655, June 2000.

60. Kurtsiefer, C., *et al.*: “Quantum cryptography: A step towards global key distribution”, Nature 419, 450, October 2002.

61. “Quantum cryptosystem tested over 100km: 'Unbreakable' crypto system using quantum method tested over record distance”, URL: http://news.techworld.com/security/251/quantum-cryptosystem-tested-over-100km/, July 2003.

62. URL: http://www.idquantique.com

63. URL: http://www.magiqtech.com

64. “Breakthrough in Quantum Cryptography - Swiss partnership to release world’s first integrated Quantum Key Infrastructure”, WISeKey Press Release, Geneva, October 13, 2003.

65. Maslennikov, G.A. *et al.*: “Practical realization of a quantum cryptography protocol exploiting polarization encoding in qutrits”, Journal of Optics B: Quantum and Semi-classical Optics, Vol. 5, S530–S534, 2003.

66. Gobby, C., Yuan, Z.L., and Shields A.J.: “Quantum key distribution over 122km of standard telecom fiber”, Applied Physics Letters, Vol. 84, 3762-3764, 2004.

67. MagiQ Technologies Announces European Distribution Channel; Duepigreco to Distribute MagiQ's QPN, Business Wire, February 25, 2004.

68. “World’s longest single-photon transmission record extended to 150km”, NEC Press Release, March 12, 2004, URL: http://www.nec.co.jp/press/en/0403/1201.html.

69. “Quantum crypto gets a speed boost”, May 6, 2004, URL: http://optics.org/article/19485

70. Willian, P.: “EU seeks quantum cryptography responses to Echelon”, Computerworld, May 17, 2004, URL: http://www.computerworld.com/s/article/93220/EU_seeks_quantum_cryptography_response_to_Echelon

71. “MagiQ Technologies Enters Global Marketing Agreement with WorldTech on Quantum Cryptography Devices”, June 21, 2004, URL: http://www.businesswire.com/news/home/20040621005044/en/MagiQ-Technologies-Enters-Global-Marketing-Agreement-WorldTech

72. “Random Numbers Generation using Quantum Physics”, IdQuantique White Paper, August 2004.

73. “Secure data archiving thanks to quantum cryptography”, IdQuantique Press Release, September 28, 2004, URL: http://www.idquantique.com/news/release-deckpoint.htm

74. “Toshiba shows practical quantum cryptography”, December 14, 2004, URL: http://www.zdnet.com/toshiba-shows-practical-quantum-cryptography-3039181033/

75. Mo, X-F. *et al.*, “Intrinsic stabilization unidirectional quantum key distribution between Beijing and Tianjin”,
December 2004, URL: http://arxiv.org/ftp/quant-ph/papers/0412/0412023.pdf

76. “MagiQ Technologies Announces New, Next Generation Quantum Cryptography Solution”, Business Wire, March 28, 2005.

77. “New quantum cryptography link encryptor unveiled at Infosecurity Europe in London”, IdQuantique Press Release, April 25, 2005, URL: http://www.whygeneva.ch/index.php?option=com_content&task=view&id=662&Itemid=160&lang=fr

78. “China’s Great Wall holds the key to quantum future”, New Scientist, April 30, 2005.
URL: http://www.greatwall-of-china.com/43-8/chinas-great-wall-holds-the-key-to-quantum-future.html

79. Sheriff, L.: “Aussie boffins patent single-photon generator”, May 6, 2005. URL:http://www.theregister.co.uk/2005/05/06/single_photon_oz/

80. “CAS researchers make advance in global secure quantum communication”, May 17, 2005. URL: http://www.chinaembassy.org.ro/rom/kjwh/t196783.htm

81. “NEC Succeeds in World’s Fastest Continuous Quantum Cryptography Key Generation over Fortnight Period”, May 31, 2005, URL: http://www.physorg.com/news4330.html

82. Ghernaouti-Hélie, S. and Sfaxi, M.A.: “Guaranteeing Security of Financial Transaction by Using Quantum

Cryptography in Banking Environment”, Proc. 2nd International Conf. on E-Business and Telecommunication Networks (ICETE2005), UK, October 3-7, 2005.

83. URL: http://en.wikinews.org/wiki/First_quantum_byte_created

84. “New Technology Enables Faster, Super Secure Communications over Greater Distances”, BBN technologies Press Release, February 22, 2006, URL: http://www.bbn.com/News_and_Events/Press_Release/06_02_22.html

85. Blake, D.: Dr. Dobb’s Journal, March 1, 2006, URL: http://www.ddj.com/184406426

86. Dunn, J.E.: “Quantum cryptography record broken”, TechWorld, April 19, 2006. URL: http://news.techworld.com/security/5820/quantum-cryptography-record-broken

87. “LANL/NIST Team Sends Quantum Encryption Keys Over Record Distances”, NIST News Release, September 25, 2006. URL: http://www.nist.gov/public_affairs/releases/qkd_release.html

88. Duligall, J.L. *et al.*: “Low cost and compact quantum key distribution”, New Journal of Physics, Vol. 8, 249, October 24, 2006.

89. Pincock, S.: “Smallest Diamond Ring Could Help Computing”,URL:http://dsc.discovery.com/news/2008/03/28/smallest-diamond-ring.html

90. Lydersen, L. *et al.*: “Hacking commercial quantum cryptography systems by tailored bright light illumination”, Nature Photonics, Vol. 4, August 29, 2010, 686-689.

91. Jofre, M. *et al.*: “Fast optical source for quantum key distribution based on semiconductor optical amplifiers”, Optical Express, Vol. 19(5), 3825-3834, February 28, 2011.

92. Greenemeier, L.: “Quantum Cryptography Come to Smart Phone”, URL: http://www.scientificamerican.com/podcast/episode.cfm?id=quantum-cryptography-comes-to-smart-12-02-02, February 2, 2012.

93. Matson, J.: “Bits of the Future: First Universal Quantum Network Prototype Links 2 Separate labs”, URL: http://www.scientificamerican.com/article.cfm?id=universal-quantum-network, April 11, 2012.

Table 1. Systematic Development of Quantum Cryptography since 1970

Year	Development
1970c	Stephen Wiesner from Columbia University formulated the first protocol that includes ideas of QC to create quantum banknotes or counterfeit-proof money. His work was published in 1983 [47].
1979	Charles Bennett *et al.* [4] worked on the idea of QC. Their first paper was published in 1982.
1982	Nobel Laureate physicist Richard Feynman proposed the idea of a quantum computer [48].
1984	Charles Bennett and Gilles Brassard published their first and the main protocol of QC, the BB84 protocol describing an unconditionally secure QKD system [5].
1985	David Deutsch published the first paper on a quantum computer [49].
1989	Charles Bennett *et al.* [50] developed the first experimental QKD prototype of QC.
1991	Artur Ekert proposed the protocol of QC based on entangled photons [51].
1992	a. Charles Bennett proposed the protocol B92 of QC [52]. b. Charles Bennett *et al.* [50] implemented a system of QC in a laboratory using BB84 for the first time.
1993	Townsend *et al.* [53] implemented a system of QC phase-encoding on the distance of 10km.
1994	Peter Shor developed the algorithms for quantum computer to factorize prime number [54].
1995	Kwiat *et al.* [55] developed a high-intensity source of polarization-entangled photon pairs. Their technique may have immediate application in QC.
1997	Zbinden *et al.* [56] implemented a system of QC plug-&-play on the distance of 23km under Geneva lake using telecom optical fibers.
1999	Bourennane *et al.* [57] implemented a system of QC plug-&-play on the distance of 40km.
2000	a. Several research groups [20, 21, 22, 58] implemented systems of QC using entangled photons. b. The LANL transmitted a quantum key through 1.6km in air [59].
2002	a. Stucki *et al.* [17] presented a QKD prototype to exchange key over 67km between Geneva and Lausanne with a plug-&-play system. The system is commercially produced by IdQuantique. b. The University of Geneva and IdQuantique demonstrated ‘the first fully integrated QC prototype machine’ across a telecommunication network [12]. c. BBN Technology collaborated with Boston and Harvard Universities to build a quantum network connecting the three institutions [11]. d. QC keys encoded in photons have been transmitted more than 23km through air. This breakthrough indicated a possibility of a completely secured global communication system [60].

	e. Mitsubishi Electric achieved quantum-based key exchange over a distance of 87km, which was a record at time [61].
2003	a. A research team from the University of Vienna successfully transmitted entangled photons across the Danube river. This technique could be a vital step towards ultra-secure QC; using satellites to beam entangle photons to the earth [23]. b. First commercial QC prototypes are available from IdQuantique and MagiQ [62, 63]. c. Three leading e-Security organizations (WISeKey, OISTE, and IdQuantique) in Geneva joined together to deploy world's first integrated quantum key infrastructure (QKI) [64]. It is expected that this technology would provide ultra secure links to government agencies, banks and financial institutions. d. Maslennikov *et al.* [65] proposed the first experimental set-up for QC protocol exploiting polarization encoding in qutrits (biphotons). e. NEC and Japan Science & Technology tested a QC system with a distance between transmitter and receiver of over 100km for the first time [61]. f. Hwang [24] first proposed a decoy-pulse method to overcome the PNS attack for BB84 QKD protocol.
February 2004	a. Toshiba in Cambridge, England recently sent a quantum encrypted signal over 122km of standard telecom fiber using BB84 [66]. b. MagiQ Technologies announced its product QPN3505, the world's first commercially available QKD system [67].
March 2004	Japan succeeded in realizing the world's longest 150km-long single-photon transmission using QC for secure network communication [68].
April 2004	a. The European Union project SECOQC began with 41 partners of 12 European countries with a budget of 11.4M Euros [38]. b**.** The *Bank Austria Creditanstalt* performed the world's first secure financial transaction via QC based on a pair of entangled photons to create the key [39].
May 2004	a. NIST scientists transmitted a quantum key made of single photons through 730m free-space link at a rate of 1 Mbps, about 100 times faster than previous demonstration using optical fibers [69]. b. The European Union planned to invest $13M during next four years to develop secure communications system by creating unbreakable encryption keys [70].
June 2004	a. BBN Technologies in collaboration with DARPA built the world's first QC network which has been operating beneath the streets of Cambridge, MA. This network guarantees secure QKD and would be extended to the campus of Harvard and Boston Universities [40]. b. MagiQ made partnership with WorldTech and would offer their unbreakable data encryption solution, the QPN5505, to WorldTech's customers [71].
August 2004	IdQuantique published a White Paper explaining the application of their product, Random Number Generator, in QC [72].
September 2004	Deckpoint, IdQuantique, and the University of Geneva announced the first network for remote data archiving secured by QC [73].
December 2004	a. Toshiba Research Europe demonstrated the world's first reliable automated QC system that ran continuously for over a week. This system relied on single-photon to transmit a secure key over standard optical fibers and delivered thousands of keys a second over a distance of more than 100km [74]. b. A Chinese research team developed a unidirectional intrinsic-stabilization QKD. Using their scheme, they exchanged key from Beijing to Tianjin over 125km and the distance exceeds 150km. Their results showed the system was insensitive to environment and could run over day and night [75].
March 2005	MagiQ Technologies made a new model of quantum encryption product, QPN7505 [76].
April 2005	a. IdQuantique made Vectis Link Encryptor, the second generation QC product [77]. b. A team of Chinese scientists successfully transmitted entangled-photons through more than 7km of the earth's lower atmosphere without losing the photons' quantum properties [78].
May 2005	a. BBN Technologies built the world's first pilot stage continuously operating QC network, which is a 12-mile long network running under the streets of Cambridge and Boston [41]. The network has 10 nodes currently runs at up to 5Mbps. b. Australian scientists developed a new technique for producing single photons at room temperature that is suitable for real world and hold a worldwide patent for their invention. It is known that a laser beam could stimulate a diamond to emit single photon. Following this idea, physicist Rabeau from University of Melbourne built a device that would send single photons through an optical fiber [79]. c. Researchers from the University of Science & Technology in China are 'successful in the free-space distribution of entangled-photon pairs in a noisy city environment with a distance beyond the effective thickness of the aerosphere, making a significant step towards the satellite-based global quantum

	communications' [80]. d. A Japanese team including NEC successfully built world's fastest continuous QC key generation at the rate of 13Kbps. The system continued to work over 14 days in a 16km-long commercial optical network [81].
June 2005	Lo *et al.* [25] proposed a practical implementation of QKD using quantum decoy states introduced by Hwang in 2002 [24].
October 2005	Ghernaouti-Hélie and Sfaxi [82] described a scenario of using QKD in secure bank transactions in Switzerland and proposed a solution that integrates QKD into IPSec.
November 2005	Zhao *et al.* [26] did the first experimental implementation of QKD using decoy state techniques.
December 2005	Physicists at Innsbruck University, Austria produced the first quantum byte (8-qubits) system that would lead to the construction of the first quantum computer [83]. The formal paper was published in Nature, December 1 2005.
February 2006	a. Scientists from LANL and NIST achieved QKD at telecom industry wavelength in a 50km optical fiber using new superconducting TES for QKD [18]. b. Using superconducting technology, BBN Technologies and NIST have built the first generation of ultra-fast single-photon detectors that allow highly secure and faster transmission of information over longer distances [84].
March 2006	Researchers at the University of Toronto described the first experimental proof of a quantum decoy technique to encrypt data over fiber optic cable [85].
April 2006	NIST scientists transmitted quantum-encrypted information at a throughput of 4Mbps across a 1 km-long optical fiber. The use of QKD in securing video streams becomes feasible at these transfer rates, possibly leading to the development of a QKD-secured surveillance network. Such a network would be applicable to military data transfer or the transfer of sensitive financial and healthcare information [86].
May 2006	Mitsubishi and NEC developed a QC network system for the first time in Japan and they made successful interconnection with the University of Tokyo [42].
September 2006	Researchers from LANL and NIST generated and transmitted secret quantum keys over 184.6km of fiber optic cable, the longest distance recorded for QKD compared to the previous distance 122km [87]. Their QKD systems were able to produce keys using single photons.
October 2006	Duligall *et al.* [88] recently built a low-cost and compact QKD system that was able to generate and transmit keys over a short distance. They aimed to incorporate this system in a smart card or mobile phone.
July 2007	Ursin *et al.* [19] experimentally demonstrated entangled-based QKD over 144km. One photon was measured locally at La Palma and the other was sent over an optical free-space link to Tenerife of the Canary Islands where it was received by the Optical Ground Station of the European Space Agency.
March 2008	Scientists from the University of Melbourne developed the world's smallest diamond ring of diameter 5μm and thickness 300nm, which could be used as the future quantum computer [89]. The purpose for using diamond is that it has interesting properties to produce "qubits", the quantum equivalent of bits on standard computers. These properties come from tiny impurities in diamond which are called nitrogen-vacancy centers. Single photons can be produced by beaming laser onto one of these vacancies.
June 2008	Researchers at Toshiba's European Lab in England developed a detector, known as avalanche photodiode that uses a semiconductor-based senor to detect photons [45].
October 2008	The first commercial communication network using secure encryption based on QC was demonstrated in Vienna, Austria. The encryption utilizes keys that are generated and distributed by means of QC technologies [46].
April 2009	IdQuantique, the University of Geneva, and the University of Applied Sciences of Western Switzerland deployed a QC network that has been running for more than six months [44]. This network, known as Swiss Quantum Network, distributes encryption keys to any of its three nodes. These keys are serving as 10GB Ethernet encryption for secure communication between CERN and the University of Geneva.
August 2010	A team of Norwegian and German researchers found security breaches in commercially available QKD systems, MagiQ QPN5505 and IdQuantique Clavis2 [90]. Using tailored bright light, the team demonstrated that these two QKD products are potentially vulnerable because most QKD systems use avalanche photodiodes to detect single photons. Their 'findings are crucial for strengthening the security of practical QKD'.
February 2011	Jofre *et al.* [91] built a single photon source based on an attenuated laser diode for QKD. To date, this is the fastest polarization encoded QKD system.
February	Researchers at LANL have 'developed a minitransmitter that encodes the encryption key on a single

2012	photon'. It is called the QKarD, short for Quantum Smart Card that will provide quantum cryptographic security to smart phones for online banking and mobile commerce [92].
April 2012	Physicists from Max Plunk Institute of Quantum Optics in Germany created the first universal quantum network prototype that links two separate labs by fiber-optic cable. Both labs were able to send, receive, and store quantum information on a single photon [93].

ACRONYMS

AES	Advanced Encryption Standard
APD	Avalanche Photodiode
CERN	Conseil Européen pour la Recherche Nucléaire (in French) (European Organization for Nuclear Research)
DARPA	Defense Advanced Research Projects Agency
DES	Data Encryption Standard
IPSec	Internet Protocol Security
LANL	Los Alamos National Laboratory
NIST	National Institute of Standards and Technology
NPL	National Physical Laboratory
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PNS	Photon Number Splitting
PPP	Point-to-Point Protocol
QC	Quantum Cryptography
QKD	Quantum Key Distribution
QKI	Quantum Key Infrastructure
Qnet	Quantum Network
QRNG	Quantum Random Number Generator
RSA	Rivest-Shamir-Adleman
SARG	Scarani-Acin-Ribordy-Gisin
TLS	Transport Layer Security