Quantum Cryptography: An Emerging Technology in Network Security

Mehrdad S. Sharbaf
Senior IEEE Member
msharbaf@ieee.org
Loyola Marymount University
California State University, Northridge
Sharbaf & Associates

1. Abstract

The uses of computer communications networks technologies have increased the incidents of computer abuse. Because of these incidents, most organizations facing pressure to protect their assets. Most digital networks generally rely on modern cryptosystems to secure the confidentiality and integrity of traffic carried across the network. The current modern cryptosystems based on mathematical model introduce potential security holes related to technological progress of computing power, the key refresh rate and key expansion ratio, the most crucial parameters in the security of any cryptographic techniques. For that reason efforts have been made to establish new foundation for cryptography science in the computer communications networks. One of these efforts has led to the development of quantum cryptography technology, whose security relies on the laws of quantum mechanics [1,2,3,20, 24]. This research paper concentrates on quantum cryptography, and how this technology contributes to the network security. The scope of this research paper is to cover the weaknesses, and the security pitfalls in modern cryptography, fundamental concepts of quantum cryptography, the real –world application implementation of this technology, finally the future direction in which the quantum cryptography is headed forwards.

Keywords: Network Security; Quantum Cryptography; Quantum Key Distribution; Photon Polarization

2. Introduction

Most security breaches involve accessing unauthorized data or accessing a network illegally [12]. For the recent years, the intruders have demonstrated increased technical knowledge, developed new ways to exploit network vulnerabilities, and created advanced software tools to automate attacks [18]. A primary concern is that many attacks involve secret manner access to information resources, and organizations are often unaware of unauthorized access to their information systems. For example, an illegally installed optical tap was discovered by U.S. security personnel in a major carrier's optical digital network servicing an important financial institution just prior to their scheduled earning release in 2003. In fact, the 2003 CSI/FBI computer and security survey reports that 80% of respondents lost money because of computer breaches. For that reason, cryptography is a vital of today's computer and communications networks, protecting everything from business e-mail to bank transactions and internet shopping While classical and modern cryptography employ various mathematical techniques to avoid eavesdroppers from learning the contents of encrypted messages, but there are limitations on modern cryptosystems based on hard mathematical problem, vulnerability to the progress in computation (supercomputers) and algorithms, and also vulnerability to future quantum computation protocols. For that reason, in modern cryptography an absolute security of information not be guaranteed. In quantum mechanics the information is protected by the laws of physics. The security of quantum cryptography maintains in its ability to exchange the encryption key with absolute security. By sending the key encoded at the single photon level on a photon-by photon basis, quantum cryptography guarantees that the act of an eavesdropper intercepting a photon, even if it just to observe or to read it, irretrievable changes the information encoded on that photon [1,2,3]. The quantum cryptography network joins a variety of quantum key distribution (QKD) techniques to well established internet technology in order to build a secure network [10, 11]. The security of quantum key distribution relies on the inviolable laws of quantum mechanics, and the impossibility of perfect cloning of non-orthogonal states implies the security of this protocol [2]. Also, quantum cryptography technology makes extensive use of the Heisenberg uncertainty principle for ensuring secure cryptography. Quantum cryptography exploits the laws of quantum physics to guarantee in an absolute fashion the confidentiality of data transmission. Quantum cryptography constitutes a revolution in the field of network security. The purpose of this research paper is to explore the quantum cryptography technology in network security.

3. Historical Overview, and Limitation of Modern Cryptography

Secret writing for the transmission of messages has been practiced for nearly 4,000 years. According to [15], the great historian of cryptology, the first example of an intentionally altered message can be traced to a tomb in ancient Egypt dated about 1900 B.C. Cryptography has its origin in the ancient world. According to [21], the Julius Caesar used simple cryptography to hide the meaning of his messages. According to [21], The Caesar cipher is a mono-alphabetic cryptosystem, since it replaces each given plain text letter, wherever in the original message it occurs, by the same letter of the cipher text alphabet. However the concepts of source and receiver, and channel codes are modern notions that have their roots in the information theory.

This important discipline (information theory) was invented in 1940 by Claude Shannon at Bell Labs. Claude Shannon, in the 1948 provided the information theory basis for secrecy, which defines that the amount of uncertainty that can be introduced into an encoded message can't be greater than that of the cryptographic key used to encode it [25]. Claude Shannon presented this concept of security in communications in 1949, it implies that an encryption scheme is perfectly secure if, for any two messages M_1 and M_2, any cipher-text C has the same probability of being the encryption of M_1 as being the encryption of M_2 [6]. Shannon's coding channel theorem, which says that there exist codes that make it possible to transmit information through a noisy channel with any desired reliability, as long as the transmission rate (the number of bits transmitted per second) does not exceed a limit called the channel capacity [23].When the transmission rate exceeds the channel capacity, it is impossible to achieve reliable transmission. Shannon was developed two important cryptographic concepts: confusion and diffusion. According to Salomon [23], the term confusion means to any method that makes the statistical relationship between the cipher-text and the key as difficult as possible, and diffusion is a general term for any encryption technique that expands the statistical properties of the plaintext over a range of bits of the cipher-text. In general cryptosystems are taxonomies into two classes, symmetric or asymmetric, depending only on whether the keys at the transmitter and receiver are easily computed from each other [28]. In the simple symmetric encryption, Alice and Bob can share the same key (K), which is unknown to the attacker, and uses it to encrypt and decrypt their communications channel [6,28]. These secret keys are applied in the process of the encryption to present uncertainty to the unauthorized receiver, which can be removed in the process of decryption by an authorized receiver using his copy of the key [6, 28]. This indicates, of course, that if the key is exposed, further secure communications are impossible. Popular symmetric cryptography algorithms include the old Data Encryption Standard (DES) and the new Advanced Encryption Standard (AES). [22] argue that the AES system suffers from an obvious weakness: the key must be known to both parties. Thus the problem of confidential communication reduces to that of how to distribute these keys securely. The new class in cryptosystem is an asymmetric cryptography algorithm. In asymmetric cryptography algorithm a different key is used for encryption and decryption. This means, a party posses a pair of keys- a public key (pk), and an associated secret key (sk-private key)- with the public key for encryption and the private key for decryption. In 1976 Whitfield Differ, and Martin Hellman introduced the most popular public-key cryptosystem (Diffie, & Hellman, 1976), and in the early 1977, several research scientist such as Whitfield Diffie, Martin Hellman Ralph Merkel, Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) invented cryptography techniques based on computational complexity [6]. Today, these public-key cryptosystems are well known by Diffie-Hellman key-exchange and RSA prime-factor algorithms. Public-key techniques assume that certain mathematical functions are one way-easy to do in one direction, but too difficult for an adversary to undo in a reasonable time [21].However, classical schemes for key distribution rely on the unproven computational assumptions, and if someone discovers a fast technique for factoring large integers, the RSA cryptosystem will not survive anymore . Also the higher amount of computation in the process of encryption and decryption significantly reduces the channel capacity bits per second of message information . The other vulnerability is susceptible to the future of quantum computation protocols. For example: Shor's Algorithm [27], allows for factoring large numbers on a quantum computer in polynomial time, theoretically breaking RSA encryption. The same argument [30] demonstrate that classical cryptosystem provides no mechanism for detecting eavesdropping. Moreover, once scholars able to build a feasible quantum computer, Shor's algorithm could beak RSA easily in polynomial time.

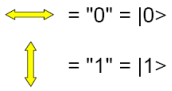
In general the amount of computational power used to subvert a particular cryptosystem determines the expected time it takes to recover an encryption message [32]. This determines that it takes much longer to subvert highly sophisticated systems such as AES today than it will take in a couple of decades. Therefore, encrypted messages in this system can only be considered secure for a limited period of time. For this reason, many efforts have been made by scientists to develop a new cryptosystem mechanism

to resolve this issue. One of these efforts has led to the development of quantum cryptography.

4. Quantum Cryptography and Theory Concept behind it

Quantum cryptography concept developed by Charles H. Bennett and Gilles Brassard in 1984 (BB84) as part of research study between physics and information at IBM lab [9].This is the first known quantum distribution scheme. The quantum system is based on the distribution of single particles or photons, and the value of a classical bit encodes by the polarization of a photon [1,2,3] . A photon is an elementary particle of light, carrying a fixed amount of energy. Based on physical law, light may be polarized; polarization is a physical property that emerges when light is regarded as an electromagnetic wave. According to [1,2] the direction of a photon's polarization can be fixed to any desired angle (using a polarizing filter) and can be measured using a calcite crystal. In fact, the quantum cryptography relies on two important elements of quantum mechanics-the Heisenberg Uncertainty principle and the principle of photon polarization. According to [24], the Heisenberg Uncertainty principle states that, it is not possible to measure the quantum state of any system without distributing that system. This means, the polarization of a photon or light particle can only be known at the point when it is measured. This principle plays an important role in preventing the attempts of eavesdroppers in a cryptosystem based on quantum cryptography. Secondly, the photon polarization principle explains how light photons can be polarized in a specific direction. In addition, an eavesdropper can not copy unknown qubits i.e. unknown quantum states, due to no-cloning theorem which was first presented by [31] in 1982.

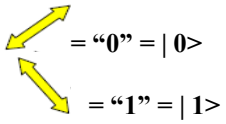
The quantum cryptography allows a bit string to be agreed between two communications parties without having two parties to meet face to face, and yet that two parties can be sure with a high confidence that the agreed bit string is exclusively shared between them. BB84 allows two parties, conventionally "Alice" and Bob", to establish a secret common key sequence using polarized photons. Each of these photons is in a state denoted by one of the four following symbols:



Rectilinear

$$\theta = 0^{\circ} \Rightarrow \text{state } |0\rangle$$

$$\theta' = 90^{\circ} \Rightarrow \text{state } |1\rangle$$



Diagonal

$$\theta = 45^{\circ} \Rightarrow \text{state } |0\rangle$$

$$\theta' = 135^{\circ} \Rightarrow \text{state } |1\rangle$$

—, |, ⁄, \,. According to[1], the first two photon states are emitted by a polarizer which is set with a rectilinear orientation and the other two states are emitted by a polarizer which is set with a diagonal orientation. For example: +(0)= — , +(1)= | , x(0)= ⁄, x(1)= \

If Alice sends random sequence of photons:

++xx++xxx++xx

the binary number represented with these states is

1110010110010

Now, if Bob wants to obtain a binary number sent by Alice, he needs to receive each photon in the same basis (Figure 1).

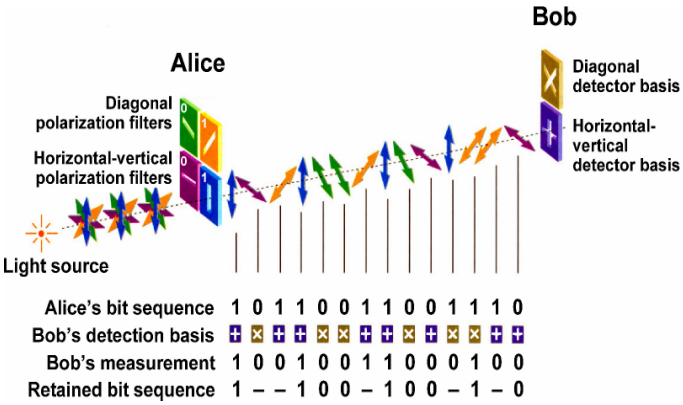


Figure 1

For each conventional bit to be transmitted in the QKD protocol Alice will set differently oriented polarizes + or x uniformly random. [2,3,9] stated that because a photon is an indivisible elementary particle, the QKD communications can not be passively tapped in the conventional sense so adversaries would need to undertake far more risky active attacks. However, the Heisenberg Uncertainty Principle ensures that any active attack will not permit an attacker to faithfully read the key transmission [9,24]. In another word, as Eve intercepts Alice's photons, she has to measure them with a random basis and send new photons to Bob. The photon states cannot be cloned (no-cloning theorem which was first presented by Wootters and Zurek in 1982.

Eve's presence is always detected: measuring a quantum system irreparably alters its state **(**The Heisenberg Uncertainty principle**).** For that reason
If an eavesdropper Eve tries to tap the channel, this will automatically show up in Bob's measurements.
In those cases where Alice and Bob have used the same basis, Bob is likely to obtain an incorrect measurement(Error Rate). Eve's measurements are bound to affect the states of the photons. The concept of QKD protocol implementation is based on figure 2 (key distillation).
Sifting is the process whereby Alice and Bob window away all the obvious "failed qubits" from a series of pulses. Sifting allows Alice and Bob reconcile their "raw" secret bit streams to remove the errors.
Error detection and correction allows Alice and Bob to determine all the "error bits" among their shared, sifted bits, and correct them so that Alice and bob share the same sequence of error-corrected bits. The process of error detection allows Alice and Bob to estimate the current Quantum Bit Error Rate (QBER) on the quantum channel between them, which can then be used as input for privacy amplification.
Privacy Amplification is the process whereby Alice and bob reduce Eve's knowledge of their shared bits to an acceptable level.

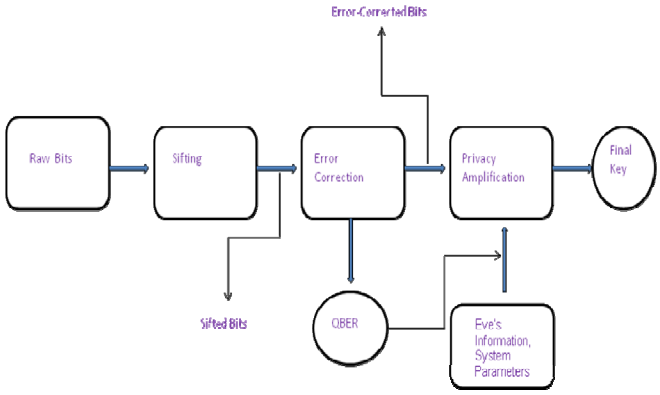


Figure 2

6. Vendor Product for QKD

There are currently four companies offering commercial quantum cryptography products; id Quantique/Deckpoint (Geneva), Cavium Networks (California), MagiQ Technologies (New York), and Quintessence Labs (Australia). MagiQ's solution is called the Navajo QPN security gateway. The quantum-key distribution hardware box is claimed by MagiQ [16]. to be the first commercially available quantum key distribution (QKD) system (Figure 3-excerpted from www.magiqtech.com).

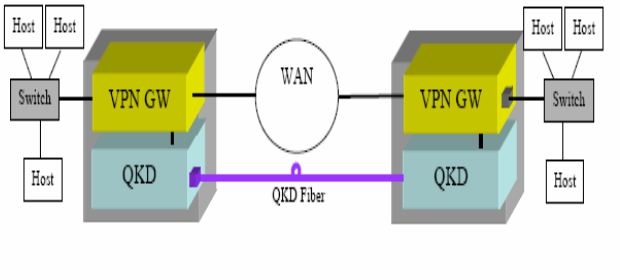


Figure 3.

Another product from MagiQ is QPN8505 to support external, customer-supplied encryption engines. The QPN7505 supports the notion of splitting a secure LAN into physically separate network segments by inserting QPN7505s between the SONET Multi Service Switch (MSS) and the Ethernet Switch (Figure 3 excerpted from www.magiqtech.com**).**

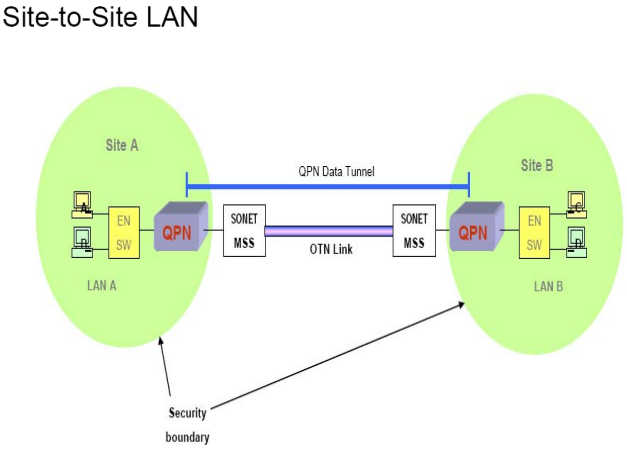


Figure 4.

QPN systems are hybrid component that contain an encrypted communication channel and quantum cryptography capability [16]. The QPN is an embedded systems that contains hardware and software developed by MagiQ Technologies, Inc.(Figure 4-excerpted from

www.magiqtech.com)

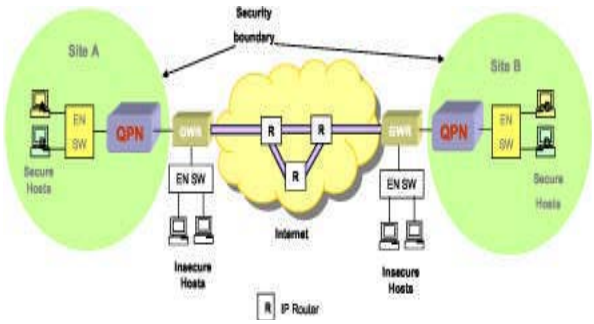


Figure 5. Quantum Private Network (QPN)

IDQ's Cerberis solution offers a radically new approach to network security, by combining the
sheer power of high-speed layer 2 encryption appliances with the unconditional security of
quantum key distribution (QKD) technology to secure point-to-point backbone and storage networks (Figure 4- excerpted from www.idquantique.com).

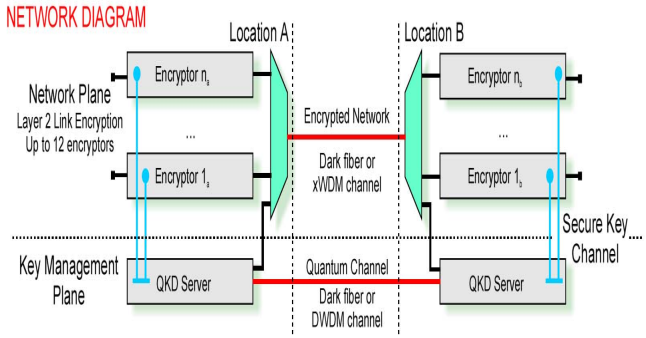


Figure 6.

QuintessenceLabs QKD link encryption operates in real time and is transparent to all higher layer communications protocols. Link encryption is necessary when the security of a transmission channel cannot be assured, and it is not possible or desirable to modify existing communications protocols and equipment. Quintessence Labs QKD provides ultrasecure communications over: (excerpted from http://www.quintessencelabs.com/index.php

- optical fibre metropolitan area networks
- direct point to point coverage up to 20 km
- extended range possible using relay stations

- optical local area networks (LANs) for in-house high performance security

7. Technical Challenges of QKD

One of the challenges for the researchers, is to develop optical device capable of generating, detecting and guiding single photons; devices that are affordable within a commercial environment. [18] present that a particular problem for QDK is selling technology based on quantum mechanics to clients who often know little about physics and are used to traditional cryptography. Another issue is the lack of a security certification process or standard for the equipment. Also [32] argue that, users need reassurance not only that QKD is theoretically sound, but also that it has been securely implemented by the vendors.

8. Conclusion

An important and unique characteristic of quantum cryptography is the ability to detect the presence of any third party between two communicating users. The security of quantum cryptography depends on the foundation of quantum mechanics, and that can revolutionize the network security.QKD techniques can be married to standard internet technology in order to provide highly secure communications for practical use.
While there have been substantial advancements in the field of quantum cryptography in the last decade, there are still challenges ahead before quantum cryptography can become a widely deployed key distribution system for governments, businesses, and academics.Basically, these challenges include developing more advanced hardware to enable higher quality and longer transmission distances for quantum key exchange. The advances in computer processing power and the threat of limitation for today's cryptography systems will remain a driving force in the continued research and development of quantum cryptography. The technology has the potential to make a valuable contribution to the network security among government, businesses, and academic environment.

9. References

[1] Bennett, Ch. H., & Brassard, G., "Quantum cryptography: public key distribution and coin tossing", *IEEE Conference on Computer, Systems, and Signal Processing,* 1984, pp. 175-90.

[2] Bennett, C. H., "Quantum cryptography using any two non-orthogonal states". *Physics Review Letter, 68*, 1992 p. 3121-3124.

[3] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J., "Experimental quantum cryptography". *Journal of Cryptology, 5(*1), 1992 p. 3-28.

[4] Bruss, D., Erdelyi, G., Meyer, T., Riege, T., & Rothe, J., " Quantum cryptography: A survey". *ACM Computing Surveys, 39(*2), 2007, p. 1-27.

[5] Buchmann, J., May, A., & Vollmer U., "Perspective for cryptographic long-term security". *Communications of ACM. 49(*9), 2006, p. 50-56.

[6] Coron, J. S., " What is cryptography?", *IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73.*

[7] Curcic, T., Filipkowski, M. E., Chtchelkanova, A., D'Ambrosio, P. A., Wolf, S. A., Foster, M., & Cochran, D., "Quantum Networks: From Quantum Cryptography to Quantum Architecture", *ACM SIGCOMM Computer Communication Review*, Vol.34, No.5, 2004, pp. 3-8.

[8] Davis, J., "Information Systems Security Engineering: A critical Components of the Systems Engineering Lifecycle", *ACM SIGAda,* 2004, pp.13-17.

[9] Elliot, C., "Quantum Cryptography", *IEEE Security & Privacy Journal*, 2004, pp. 57-61.

[10] Elliot, C., "Building the quantum network", *New Journal of Physics,* Vol. 46, No. 4, 2002, pp. 1-12.

[11] Elliot, C., Pearson, D., & Troxel, G., "Quantum cryptography in practice", *ACM SIGCOMM, Proceeding of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, 2003,* pp. 227-238.

[12] Farahmand, F., and Navathe, S. "A management perspective on risk of security threats to information systems". *Information Technology and Management,* 6(2), 2005, p. 203-225.

[13] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2008). Quantum Cryptography. *Review Moderns Physics, arXiv: quantum-ph/0101098v2*, p. 1-57.

[14] Hrg, D., Budin, L., & Golub, M.,"Quantum cryptography and security of information systems", *IEEE Proceedings of the 15th Conference on Information and Intelligent System*, 2004, p. 63-70.

[15] Kahn, D., "*The Cods Breakers: The Comprehensive History of Secret Communications from Ancient Times to the Internet".* New York, NY: Enigmas Books.1996.

[16] Internet Resources:
http://www.magiqtech.com
www.idquantique.com
http://www.quintessencelabs.com/index.php

[17] Li, X., & Zhang, D., "Quantum information authentication using entangled states", *IEEE Computer Society, International Conference on Digital Telecommunications*, 2006, pp. 64.

[18] Liu, S., Sullivan, J., & Ormaner, J. "A practical approach to enterprise IT security". *IEEE IT Professional Journal, 9(*3), 2001, p. 35-42.

[19] Myler, E., & Broadbent, G., "ISO 17799: Standard for Security", *Information Management Journal,*Vol.40, No.6, 2006, pp. 43-52.

[20] Papanikolaou, N., "An introduction to quantum cryptography", *ACM Crossroads Magazine,* Vol.11 No.3, 2005, pp. 1-16.

[21] Pfleeger, C. P., & Pfleeger, S. L.," *Security in Computing",* Upper Saddle River, NJ: Prentice Hall.2003.

[22] Rothe, J. (2002). Some facets of complexity theory and cryptography: A five-lecture tutorial. *ACM Computing Surveys, 34(*4), p. 504-549.

[23] Salomon, D., " *Coding for Data and Computer Communications",* New York, NY: Spring Science and Business Media. 2005.

[24] Sharbaf, M. S., (2009). " Quantum Cryptography: A new generation of information technology security system". *Published by IEEE Computer Society, Proceeding of the international conference on information technology: New Generation*., p. 1644-1648.

[25] Shannon, E. C., "Communication theory of secrecy system", *Bell System Technical Journal,* Vol.28, No.4, 1949, pp.656-715.

[26] Shields, A., & Yuan, Z., "Key to the quantum industry", *Physics World, 12*, 2007, p. 24-29.

[27] Shor, P. W. (1997). Polynomial-time algorithm for prime factorization and discrete logarithm on a quantum computer. *SIAMJ. Computing, 26,* p. 1484

[28] Simmon, G. J. ,"Symmetric and asymmetric encryption", *ACM Computing Surveys, 11(*4), 1979, p. 305-330.

[29] Steane, M. A., & Rieffel, G. W., "Beyond bits: The future of quantum information processing", *IEEE Computer,* 2000, pp. 38-45.

[30] Teja, V., Banerjee, P., Sharma N. N., & Mittal, R. K. (2007). Quantum Cryptography: State-of-art , challenges, and future perspective, *Proceeding of the 7th IEEE International Conference on Nanotechnology*, p. 1296-1301.

[31] Wootters, W. K., & Zurek, W. H., "A single quantum cannot be cloned". *Nature,* 299, 1982, p. 802.

[32] Young, A., "The future of cryptography: Practice and theory", *IEEE IT Professional Journal,* 2003, pp. 62-64.