A Comparative Study of Classical and QuantumCryptography Approaches: Review and Critical Analysis

Ruwayda Q. Alharbi and Soha S. Zaghloul

King Saud University, Faculty of CISC-CS Dept.

KSU, Al-Malaz Campus, Riyadh

432203422@student.ksu.edu.sa,smekki@ksu.edu.sa

ABSTRACT

Maths-based cryptography has prevailed for years in the world of information security. Although this approach has succeeded till now, but it still has its drawbacks such as loopholes and life expectancy problem. Researchers found that Quantum Cryptography, which is based on the laws of physics, might be a good alternative. Therefore, we were motivated to analyze a number of research papers in the field. This paper studies both approaches, their advantages, disadvantages, and their expected future. Moreover, it exposes the basic principles of Quantum Cryptography as well as its protocols. It explains why Quantum Cryptography is considered as an alternative to the Classical Cryptography. In addition, it highlights the status of Quantum Cryptography in research nowadays. Finally, we predict which approach will dominate the world of information security in the far future.

KEYWORDS: Classical cryptography, Quantum cryptography, Quantum protocols, BB84, B92, Quantum key distribution, QKD

1INTRODUCTION

Internet and networking technology play a central role in people's life nowadays.There is a large amount of personal, commercial, military, and government sensitive information to be transmitted worldwide. Therefore, it is important to design techniques that offer a secure, reliable and practical transmission. In fact, after the incident of a computer-related crime committed by Kevin Mitnick which costed U.S. companies a lot, the network security came into focus to attract people's attention [1]. Many defense and detection mechanisms are developed in order to prevent similar attacks.

One essential technique for secure communications is the Cryptography: the art of hiding message information and making it unintelligible to any unauthorized party. Cryptography referred almost to encryption which is the operation of converting a normal text (called plain text) into coded text (called cipher text). Decryption is the inverse operation: the operation of converting ciphertext into plaintext [2]. A cryptographic algorithm, or cipher, is a mathematical function used in encryption and decryption process which works along with a secret parameter "key". This key is actually a sequence of symbols which are known only to communicants. So, nobody else can decrypt and read cipher text [3]. Cryptosystems may use the same key in encryption and decryption process: this is known as Secret (Symmetric) Key Cryptography. Alternatively, two different keys may be used: a public key for encryption and another private one for decryption: this is known as Public (Asymmetric) Key Cryptography [4].

In fact, the security of an encrypted message relies on two main factors; namely, the reliability of the cryptographic algorithm and the secrecy of the key [3]. Shannon statement [5] deals with the first factor: a message being transmitted cannot be decoded if it is encoded by a random one-shot key whose length equals to the message length. However, the core problem is how to transport the key to legitimate users while keeping it secret.

In other words, the major problem in cryptography is that of key distribution. There are two main solutions to this problem, each of which has its own pros and cons. The first solution is the Classical Cryptography (CC) which is based on mathematics. It relies heavily on the computational difficulty of factoring large integers. The second solution is Quantum Cryptography which is based on physics. It depends on the universal laws of quantum mechanics [6].

The following sections of the paper are organized as follows: Section 2 discusses Classical Cryptography. Section 3 explains the principles of Quantum Cryptography. Section 4 explores the protocols of QC. Section 5 compares both techniques. Section 6 analyzes the two approaches. The paper concludes with Section 7.

2 CLASSICAL CRYPTOGRAPHY (CC)

Classical cryptosystems come in two types: symmetric systems and asymmetric systems [7]. Symmetric systems require a secure channel for key distribution. The security of the public key cryptography is based on computational complexity. Its idea is to use mathematical objects, known as one-way functions: these make the reverse process of finding the key or plaintext an almost impossible job. However, it relies on the unproven computational assumptions. In other words, if someone discovers a fast technique for factoring large integers, the algorithms will not survive anymore [6]. The most common approach that comes under asymmetric key cryptography is the RSA algorithm. The name of the algorithm represents the initials of its inventors: Rivest, Shamir and Adleman.

3 PRINCIPLE OF QUANTUM CRYPTOGRAPHY (QC)

Quantum Cryptographyis based on the unchanged laws of quantum mechanics. It relies on two important principles in quantum mechanics which are the Heisenberg Uncertainty and that of photon polarization. The Heisenberg Uncertainty principle states that it is not possible to measure the quantum state of any system without disturbing it. As a result, the QC-based cryptosystems are able to thwart the attempts of eavesdroppers. On the other hand, the photon polarization principle describes how light photons can be polarized in specific directions. Moreover, a polarized photon can only be detected by a photon filter with the correct polarization; otherwise, the photon will be destroyed [8]. In addition, quantum mechanics forbid the creation of identical copies of unknown quantum state: this is known as the no-cloning theorem [9].

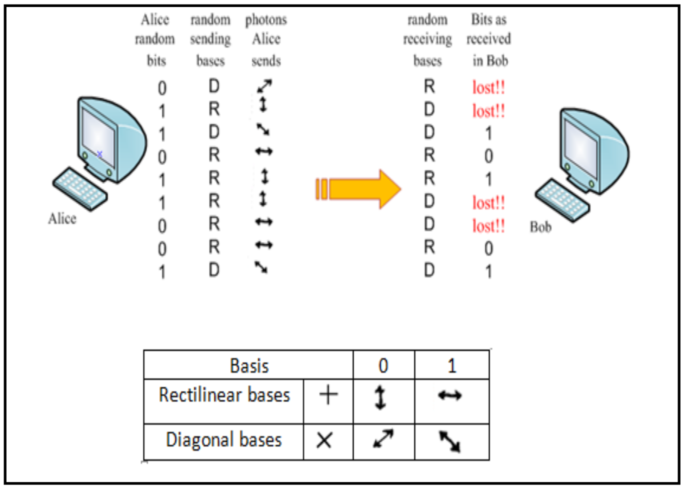
Quantum mechanics has multiple cryptographic applications [10]. The best known is the Quantum Key Distribution (QKD) the target of which is to create the key that will be used in the encryption algorithm. Two main relevant protocols are known in QKD: BB84 and B92 proposed by Bennett and Brassard in 1984 and 1992 respectively [11], [12], [13].

4 QUANTUM CRYPTOGRAPHY PROTOCOLS

As previously mentioned, there are two main protocols applied in QC: the BB84 and the B92 protocols. BB84 protocol [14] simply states that a photon may be polarized in one of four states. The horizontal (h) and the left circle (lc): these represent the zero value; the vertical (v) and the right circle (rc) represent the one value.

On the other hand, the B92 protocol [15] uses only two of the four states of polarization. The only imposed restriction on the two states is that they should not be orthogonal. For example, horizontal (h) may be used for zero value, and right circle (rc) for the one value. Figures 1 and 2 describe the sequence of operations to generate a secret key using the BB84. The process starts from the sender "Alice" selects a random binary key, converts it into polarized photons and sends it through a communication channel to the receiver "Bob". The latter reconverts the photons back into binary key.

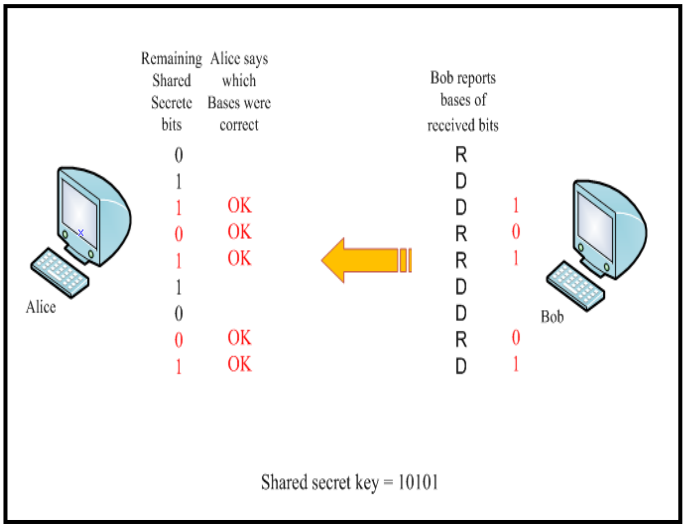
It may happen that some bits are lost or are subject to changes during transmission. These are excluded, and the rest of the bits constitute the communication shared key.



Alice random bits	random sending bases	photons Alice sends	random receiving bases	Bits as received in Bob
0	D	↗	R	lost!!
1	R	↕	D	lost!!
1	D	↘	D	1
0	R	↔	R	0
1	R	↕	R	1
1	R	↕	D	lost!!
0	R	↔	D	lost!!
0	R	↔	R	0
1	D	↘	D	1

Basis		0	1
Rectilinear bases	+	↕	↔
Diagonal bases	×	↗	↘

Figure 1. Step1: Quantum Transmission



Remaining Shared Secrete bits	Alice says which Bases were correct	Bob reports bases of received bits	
0		R	
1		D	
1	OK	D	1
0	OK	R	0
1	OK	R	1
1		D	
0		D	
0	OK	R	0
1	OK	D	1

Shared secret key = 10101

Figure 2. Step 2: Extraction of Shared Key

5 CC vs. QC

Classical Cryptography has many points of strength: it is independent of the transmission medium. Moreover, since the transmission distance does not rely on the algorithm, the CC is able to provide secure communication over millions of kilometers. In addition, CC is flexible in the sense that the algorithms may be implemented in software, hardware or a hybrid of both. Most importantly,CC does not require special specifications regarding the courier; therefore CC is not considered expensive.

On the other hand, the main drawbacks of the Classical Cryptography lie in three main points. First, the existence of some loopholes in the algorithm: these may be exploited by the hackers to break the system's security. The algorithm short life expectancy is also a major problem in CC. Therefore, it is necessary to increase the key size in order to extend the life expectancy time. Finally, CC algorithms require higher amount of computation to be effective.

On the other hand, QC suffers from many points of weaknesses [16]. These are mentioned below:

- During transmission, the photon may change its polarization. This may happen as a result of non-homologous transmission media or the intentional intervention of a hacker.
- Algorithms are not easily implemented in QC. Therefore, engineers usually sacrifice many vital features such as the digital signature. This renders the algorithm more vulnerable.
- Sensational design requirements of the photons emitter are too sensitive to be met.
- QC is not suitable for long distances: the probability for both absorption and depolarization of the photon increases proportionally with the length of the cable. This makes it impossible toapply on far transmissions such as satellite.
- The technique is vulnerable to hacking by time-shift attack.
- The possibility to generate perfect copies of an unknown quantum state by using stimulated emission or bunching properties of light.

- It is practically inapplicable to multiplex in a quantum channel; therefore, each single photon needs a dedicated channel of high quality which makes it very expensive.

Moreover, the technical challenges of QKD specifically include additional obstacles. First, the optical devices that deal with photons are too expensive. Second, the complexity of using the system since the user should have a background about physics. Third, the lack of security standards for the equipment; users shouldbe assuredthat it has beenimplemented in asecureQKDby sellers. Finally, QKD is practical only for short transmission distances: this is actually considered the main obstacle against spreading this technology widely.

In short, there are many issues pertaining to QC that the laws of physics cannot take care of. Therefore, there is still a long way off before excluding the CC and relying on QC in the world of information security.

6ANALYSIS

In our study of the QC, we found some contradictions in the literature. In this section, we list these encountered conflicts.

As previously mentioned, one of the main points of strength of QC is the no-clone theory, which means the impossibility of copying the polarization states [9]. However, the authors in [17] claim that it is possible to copy photons using amplified single-photon inputs.

Another conflict is about the communication channels in QC: while it is stated that it cannot be applied to send to satellites [16], new researches emerged that apply QC in mobile wireless networks [18]. Here, the authors integrate the BB84 protocol in 802.11 networks; they accordingly update the 4-way handshake protocol into what they called Quantum Handshake protocol.

In listing the limitations of QC, [16] mentioned that it lacks digital signature features. However, the authors in [19] present a quantum digital signature scheme that can sign general quantum states. Therefore, this is not considered a drawback anymore in QC.

In addition, the authors in [20] used laser pulses, instead of a single photon source, to overcome the problem of limited transmission distance.

Finally, the authors in [21] proposed a solution to overcome the tolerable errors limitation caused by a quantum repeater.

On the other hand, we have to highlight that theoretically speaking, QC is considered an absolutely secure way of communication. However, the use of imperfect devices may create security loopholes. Therefore, this should be taken into consideration when designing a secure communication.

Obviously, Quantum Cryptography is a worthwhile technique. From our point of view, it would be more useful if we considered a combination of both approaches: CC and QC. This will allow us to get the advantages of both of them, rather than totally replacing an approach by the other. In fact, there are many researches built on this concept. Secured Quantum Cryptography Algorithm (SQCA) [22] combined the fast speed privilege of Quantum Cryptography Algorithm (Shor's algorithm) with Classical Cryptography Algorithm (RSA). This resulted in an efficient, secure and faster algorithm. The experiments showed that the SQCA algorithm is more secure and faster than any CC algorithm known until now. Table 1shows a comparison between Classical Cryptography (RSA), Quantum Cryptography (Shor's) and SQCA.

Table1. Comparison between Classical Cryptography and Quantum Cryptography [22]

Property	RSA	Shor's	SQCA
Complexity	$O(N_k)$	$O((\log N)^3)$	$O(\log N)$
Key Size	512	512	1024
Random Attack	2.2 months	<1 second	Not Possible

7CONCLUSION

Classical Cryptography have the advantages of the provision of secure communication over long distances, the possibility of hardware/ software implementation, and the inclusion of a number of efficient algorithms. Despite the strength of Classical Cryptography and its effectiveness, it still depends on unproven computational assumptions. This motivated the researchers to look for other solutions to solve security problems. One of these efforts led to the birth of Quantum Cryptography. QC is marked by its high speed, and absolute secure communication channel. However, QC is still considered an immature technology; it involves many technical challenges such as the inadvertent change in polarization, the limited transmission distance, and the need of a dedicated channel.

In our opinion, one of the main reasons that delays the wide spread of QC approach is its adoption from physics laws. Researchers in Computer Science have to well understand these laws in order to make QC simpler and therefore more commonly used.

ACKNOWLEDGMENT

This research project was supported by a grant from the “Research Center of the Center for Female Scientific and Medical Colleges”, Deanship of Scientific Research, King Saud University.

REFERENCES

1. Daya B.: Network Security: History, Importance, and Future. University of Florida Department of Electrical and Computer Engineering.
2. Kahn D.: The Codebreakers: the story of secret writing. The MacMillan Company, 1st Ed. (1967); Reprint Ed. (1976).
3. Ayushi: A Symmetric Key Cryptographic Algorithm. International Journal of Computer Applications, Vol. 1, No. 15, pp. 1—4 (2010).
4. Sharbaf, M.S.:Quantum Cryptography: An Emerging Technology in Network Security. In: Proc. 2011 IEEE International Conference on Technologies for Homeland Security (HST),pp. 13—19, Los Angelos, CA (2011).
5. Shannon, C.E: Communication Theory of Secrecy System. Bell System Technical Journal, pp. 656—715 (1949).
6. Goel, R, Garuba M., and Girma A.: Research Directions in Quantum Cryptography. In: Proc. Fourth International Conference on Information Technology (ITNG '07), pp. 779—784 (2007).
7. Gottesman,D. and Lo, H.-K: From Quantum Cheating to Quantum Security.Physics Today, Vol. 53,Issue 11, p. 22 (2000).
8. Sharma, A., Ojha, V. and Goar, V.: Security Aspect of Quantum Key Distribution. International Journal of Computer Applications (IJCA),No. 2 (2010).
9. Wooters, W.K. and Zurek, W.H.: A Single Quantum Cannot be Cloned. Nature, Nature Publishing Group, Vol. 299, pp. 802—803 (1982).
10. Singh, S.: The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor Books (2000).
11. Heisenberg, W.: ŰberDen AnschaulichenInhaltder QuantentheoretischenKinematic und Mechanic. ZeitschriftfűrPhysik, Vol. 43, Issue 3-4, pp. 172--198 (1927).
12. Biham, Ȅ., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer Verlag(1993).
13. Ferguson, S., Schroeppel, R. and Whiting, D.: A Simple Algebraic Representation of Rijandel. In: Proceedings of Selected Areas in Cryptography (SAC), 8th Annual International Workshop, Toronto, Ontario, Canada, pp. 103—111, Springer Verlag (2001).
14. Bennett,Ch., and Brassard G.: Quantum Cryptography: Public Key Distribution and Coin Tossing. In: Proc. of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175—179 (1984).
15. Bennett, Ch., and Brassard, G.: Quantum Cryptography Using Any Two Non-Orthogonal States. Physical Review Letters, Vol. 68, Issue 21, pp. 3121—3124 (1992).
16. Vignesh, R.S,Sudharssun,S., Kumar, K.J.J.: Limitations of Quantum and the Versatility of Classical Cryptography:A Comparative Study.In: Proc. Second International Conference on Environmental and Computer Science (ICES), pp. 333—337 (2009).
17. Hofmann, H.F. and Ide, T.: Optimal Cloning of Single-Photon Polarization by Coherent Feedback of Beam Splitter Losses. New Journal of Physics, Vol. 8 (2006).
18. Falahati, A., and Meshgi, H.: Using Quantum Cryptography for Securing Wireless LAN Networks. In Proc. of IEEE International Conference on Signal Processing Systems, pp. 698—701 (2009).

19. Lű, X., and Feng, D.-G.: Quantum Digital Signature Based on Quantum One-Way Functions. In: Proc. of the 7th International Conference on Advanced Communication Technology (ICACT'05), pp. 514—517 (2005).
20. Los Alamos National Laboratory,http://www.physorg.com/news86020679.html, 2006.
21. Briegel, H.-J., Dừr, W., Cirac, J.I., and Zoller, P.:Quantum Repeaters: The Role of Imperfect Local Operations in QuantumCommunication.Physical Review Letters, Vol. 81, Issue 26 (1998).
22. Kaur, N., Singh,A., and Singh, S.: Enhancement of Network Security Techniques Using Quantum Cryptography. International Journal on Computer Science and Engineering, Vol. 3, Issue 5, pp. 1960—1964 (2011).