International Journal of Computer Systems (ISSN: 2394-1065), Volume 02– Issue 06, June, 2015
Available at http://www.ijcsonline.com/

Quantum Cryptographic Protocols: A Review

Es-said Chanigui[A], Abdelmalek Azizi[B]

[A]Dept. of Mathematics & Computer Science FSO, Mohamed I University, Oujda, Morocco
[B]Hassan II Academy of Sciences & Technology, Rabat, Morocco

Abstract

Quantum cryptography has solved a major problem of key distribution of conventional cryptography by using proven secure laws of quantum mechanics. The purpose of this paper is to give a brief overview of quantum cryptography and most prominent quantum key distribution protocols.

Keywords: *Quantum cryptography, Quantum key distribution, Quantum state transmission, Conventional post processing.*

I. INTRODUCTION

In this global high tech world where huge information travels so fast, securing data has become one of paramount concern in networks, commerce, military and strategic use. Various methods are being adopted to achieve the goal of transmitting information securely between two legitimate parties namely Alice and Bob. Cryptography is playing an important role to meet these requirements. One of the mechanisms to secure exchanged information in cryptography is encryption through which the information remains hidden for all except those who are allowed to decrypt the message. Cryptographic algorithms provide authentication, confidentiality, integrity, availability and no-repudiation [1]. Cryptography began thousands of years ago and a number of techniques start from basic shifting of alphabetical letters and go to complex mechanical and electronic encryption methods. Historical ciphers used substitution and transposition methods to encrypt/decrypt data. In conventional cipher, a key plays primordial role to encrypt/decrypt data. This key is exchanged secretly between parties involved in communication (the sender and the receiver).

Conventional ciphers may be categorized according to the type of key used. Symmetric key cipher, also called secret key cipher, use the same key for encryption and decryption. The key must be preserved secret by the parties of a communication. So in a network of n people wanting to communicate in a confidential way with a symmetric key cipher, it is necessary that the keys are distinct. Precisely, it is necessary to create and distribute $n\times(n-1)/2$ keys which are distinct and secret. As we can remark, the symmetric key cipher suffers from the problem of creation and distribution the keys. In asymmetric key cipher [2], known as public key cipher, two different but correlated keys are used: secret and public. Each participant diffuses a public key with his name. If one wishes to communicate with another participant, it is necessary to recover his public key and cipher the message with it, and send the ciphered message to this participant which is the only person who knows the secret key which makes possible to decipher the received messages. Public key ciphers are usually based on hard computational problems: RSA cipher relies on the difficulty of factorization [3]. Elliptic curve cryptography, which is also a public key cipher, offers a comparable security with shorter key length. Hybrid cryptographic system is used to exchange messages more efficiently and securely. In this system, key is exchanged using a public key cipher and the message is encrypted using a secret key cipher.

With increase in computer power, more complex techniques are adopted to encrypt data but at the same time it becomes convenient for attackers to decrypt it by using the high computational power. The conventional ciphers such us RSA [3], Diffie-Hillman [4] and AES [5], protect data based on the computational difficulty techniques. These ciphers neither provide secrecy proof nor detect eavesdropping. RSA algorithm, mainly used for key distribution, rely on the unproven computational assumptions and if someone discovers a fast technique for factoring large integers the amount of computation time to decrypt message information reduces significantly. Also in the near future, as expected, with the birth of quantum computers the conventional cryptographic techniques may become insecure and short key encrypted message would be decrypted by applying brute-force or key might be broken easily in the presence of high computational power. Peter W. Shor proposed an algorithm in 1994 which would run on quantum computer and allow to reverse a one-way functions [6]. This problem is generally considered hard on a traditional computer and has been used as the basis of several proposed cryptosystems. Kirckhoff's principle says that the security of cryptosystem should not rely on the secrecy of the algorithm but only on the secrecy of the key [7]. The key distribution is a major problem in conventional cryptography. Thus quantum key distribution (QKD) or quantum cryptography, while using with secret key cipher, provides acceptable levels of secure communications. Various quantum cryptographic protocols have been proposed to afford a solution to the key distribution problem.

The remaining part of the paper is organized as follows: In section II, we present secrecy principles used in quantum cryptography and working flow of quantum cryptography.

The description of quantum key distribution steps and a survey on the most prominent quantum key distribution protocols is given in section III. Finally, conclusion is shown in section IV.

II. Quantum Cryptography

Quantum cryptography is a relatively recent arrival in the information security world. It employs quantum physics, specifically the laws of quantum mechanics, to encrypt information on the physical level [8]. The amount of information that can be transmitted using the QKD protocol is not very large, but is provably very secure. Quantum cryptography warrants the secure data transmission by using laws of quantum mechanics; the Heisenberg uncertainty principle and the principle of photon polarization. The Heisenberg uncertainty principle implies that it is not possible to measure the quantum state of any system without disturbing that system [9][10]. Thus the polarization of photon or light particle can only be known at the point when it is measured. This principle play a critical role in thwarting the attempts of eavesdroppers in a cryptosystem based on quantum cryptography.

These laws make quantum cryptography secure because of the following principles:

- A single photon cannot be cloned to measure its state.
- It is impossible to split or to divide a quantum photon to make measurements secretly.
- An eavesdropper (Eve) will produce errors and can be detected if he tries to measure the bit value of the photon directly.

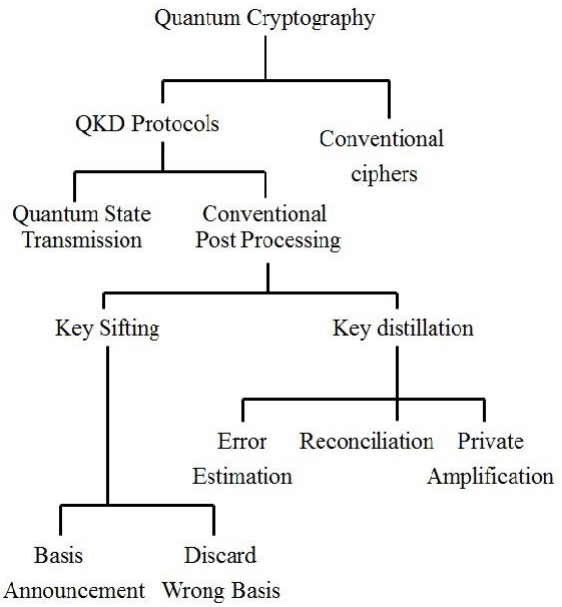


Fig. 1. A working-flow of Quantum Cryptography.

A QKD protocol comprises of two phases, namely quantum state transmission and conventional post processing. In quantum state transmission phase key is generated between Alice and Bob using quantum carriers (photons). In conventional post processing phase these key are distilled to mend a common secret key. A working-flow of quantum cryptography is shown in Fig. 1.

III. Quantum Key Distibution Protocols

In general, quantum key distribution protocols work in two phases, in the first phase quantum state transmission is carried out through quantum channel while post processing is done using public channel in the second phase [11] Fig. 2.

A. Quantum State Transmission

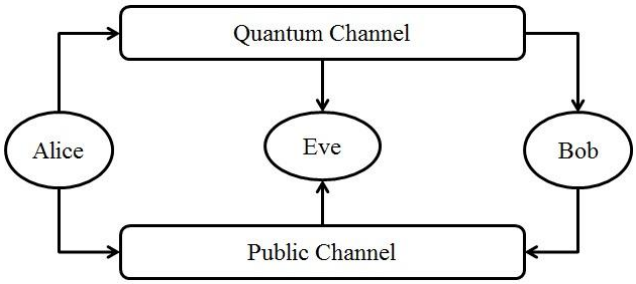


Fig. 2. A Block Diagram of Quantum Key distribution.

In quantum state transmission, Alice selects a basis and transmits it to Bob. Upon receiving the quantum state, Bob randomly chooses one of the bases and measures the incoming state using a measurement specific for that basis. He then records his measurement outcome. This is known as raw key generation process and the generated key is called raw key.

B. Post Processing

After completion of quantum state transmission process, Alice and Bob proceed to a conventional post processing step where the raw key is distilled [12] by passing through processes of sifting, error estimation, reconciliation and privacy amplification. The key distillation is achieved by exchanging messages through public channel to obtain a common-secret key. The reconciliation process removes the errors in the shared key to have a common key between Alice and Bob, while privacy amplification compresses the common key to produce a secret key.

C. Protocols of Quantum Cryptography

1) BB84 Protocol

The BB84 protocol described using Photon polarization state to transmit the information. It was developed by Charles Bennett and Gilles Brassard in 1984 [13], in the light of a paper written by Stephen Wiesner in early 1970s [14], It is known as BB84 after its inventors and year of publication. It is based in its design on Heisenberg's Uncertainty Principle. This protocol is surely the most famous and most realized Quantum Cryptography protocol. The security proof of this protocol against arbitrary eavesdropping strategies was first proved by Mayers [15] and a simple proof was later shown by Shor and Preskill [16]. Below are the steps of the BB84 protocol for exchange the secret key in the BB84 protocol [3], Alice and Bob must do as follow:

STAGE 1: *Communication over quantum channel*

- Alice creates two random binary strings X = $(x_1,x_2,...,x_n)$ and A = $(a_1,a_2,...,a_n)$. Bob also creates a random binary string B = $(b_1, b_2,\ldots, b_n)$.
- With the knowledge of X and A, Alice prepares a qubit (quantum bit) string $|\varphi x_i,a_i\rangle$ and each qubit is one of the four states: $|\varphi_{0,0}\rangle = |0\rangle$, $|\varphi_{1,0}\rangle = |1\rangle$, $|\varphi_{0,1}\rangle = |+\rangle$, $|\varphi_{1,1}\rangle = |-\rangle$ where $|+\rangle = 1/\sqrt{2}\times(|0\rangle+|1\rangle)$ and $|-\rangle = 1/\sqrt{2}\times(|0\rangle-|1\rangle)$, that is to encode $x_i \in X$ $(\subset\{0,1\}^n)$ in the rectilinear basis $B_\oplus = \{|0\rangle,|1\rangle\}$ or the diagonal basis $B_\otimes = \{|+\rangle,|-\rangle\}$ if $a_i = 0$ or $a_i = 1$, respectively. The association between the information bit and the basis are described in **Table I**. Then, Alice sends the qubit string to Bob.
- After receiving these n qubits, Bob measures them in the basis $B_\oplus$ or $B_\otimes$ according to the binary string B. Bob doesn't know which of the measurement are deterministic, i.e. measured in the same basis as the one used by Alice. Half the time Bob will be lucky and chose the same basis as Alice. In this case, the bit resulting from his measurement will agree with the bit sent by Alice. However the other half time he will be unlucky and choose the alphabet not used by Alice. In this case, the bit resulting from his measurement will agree with the bit sent by Alice only 50% of the time. After all these measurement, Bob now has in hand a binary sequence.

TABLE I. QUBIT PREPARATION ACCORDING TO THE CHOICE OF BASIS AND CBIT VALUE

	0	**1**
$\mathbf{B_\oplus}$	$\|\varphi_{0,0}\rangle$	$\|\varphi_{1,0}\rangle$
$\mathbf{B_\otimes}$	$\|\varphi_{0,1}\rangle$	$\|\varphi_{1,1}\rangle$

Alice and Bob now proceed to communicate over the public two-way channel using the following steps.

STAGE 2: *Communication over a public channel*

Phase1. Raw Key extraction

- Over the public channel, Bob communicates to Alice which base he used for each of his measurements (value of b_i).
- In response Alice communicate to Bob over the public channel which of his measurement was correct ($a_i=b_i$).

Alice and Bob then delete all bits for which they used incompatible basis ($a_i\neq b_i$) to produce their resulting raw keys. If Eve has not eavesdropped on their communication in STAGE 1, then their resulting keys will be the same. If she has eavesdropped on it, this key will not be in total agreement. delete the disclosed bits from their raw keys to produce their tentative final keys. If through their public disclosures Alice and Bob find no errors (i.e., R=0), then they know that Eve was not eavesdropping and that their tentative keys must be the same final key. If they discover at least one error during their public disclosures (i.e., R>0), then they know that Eve has been eavesdropping. In this case, they discard their tentative final keys and start all over again.

Phase2. Error estimation

Over the public channel, Alice and Bob compare small portion of their raw keys to estimate the error-rate R, and then

2) B92 Protocol

After BB84 protocol was published, Charles Bennett realized that it was not necessary to use two orthogonal basis for encoding and decoding. It turns out that a single non-orthogonal basis can be used instead, without affecting the security of the protocol against eavesdropping. This idea is used in the B92 protocol [17], which is otherwise identical to BB84 protocol. The key difference in B92 is that only two states are necessary rather than the possible 4 polarization states in BB84 protocol. Like the BB84 protocol, Alice transmit to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses dictates which bases Bob must use. Bob still randomly chooses a basis by which to measure but if he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure. Bob can simply tell Alice after each bit Bob sends whether or not he measured it correctly [18].

3) Ekert Protocol (B92 protocol)

In [19], Artur Ekert has elaborated a quantum protocol based on the properties of quantum-correlated particles. He uses a pair of particles called pair EPR: refers to Einstein, Podolsky and Rosen, which presented a famous paradox in 1935 in their article [20].

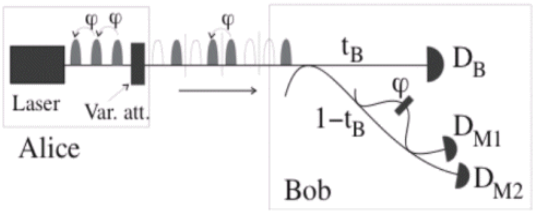
Unlike BB84 and B92 protocols, this protocol uses Bell's inequality to detect the presence or absence of Eve as a hidden variable. The EPR quantum protocol is a 3-state protocol and there are two phases to the Ekert protocol, the first phase over a quantum channel and the second over a public channel.

4) SARG04 Protocol

The SARG04 protocol is built when researchers noticed that, by using the four states of BB84 with different information encoding, they could develop a new protocol which would be more robust when attenuated laser pulses are used instead of single-photon sources. SARG04 protocol was proposed by Scarani et al. in 2004 [21]. SARG04 is equivalent to BB84 when viewed at the level of quantum processing [22]. SARG04 is intended to use in situations where the information is originated by a Poissonian source producing weak pulses and received by an imperfect detector. The authors Tamaki and Lo were successful in proving security for one and two-photon pulses using SARG04. SARG04 protocol in single-photon implementations was theorized to be equal with BB84, but experiments shown that it is inferior [22].

5) COW Protocol

Coherent One-Way protocol (COW protocol) is elaborated by Nicolas Gisin and al in 2004 [23]. It tailored for an implementation with weak coherent pulses. In the description of this protocol, the key is obtained by a very



simple time-of-arrival measurement on the data line and also an interferometer is built on an additional monitoring line. This line allows communicating parties to monitor the presence of an eavesdropper who would break coherence by her attack. The setup of this system is experimentally simple and it is tolerant to reduced interference visibility and to photon numbers splitting attacks, thus resulting in a high efficiency in terms of distilled secret bits per qubit (Fig. 3).

In their paper [23], the authors propose possible variations of this protocol. They also present two attacks that introduce errors on the monitoring line: the coherent attack on two subsequent pulses and the intercept-resend attack. There are many other protocols in existence, both prepare-and-measures (single photon) and entanglement based. The following table provides a list of the protocols already mentioned in the previous section, as well as other important protocols while citing the names of the authors and year of publication.

TABLE II. LIST OF THE MOST IMPORTANT QKD PROTOCOLS ACCORDING TO THEIR RESPECTIVE YEARS OF PUBLICATION

No	Name of protocol	Priciples	Authors	Year	Ref.
1	BB84	Heisenberg Uncertainty Principle	C.H. Bennett and G.Brassard	1984	[13]
2	E91	Quantum Entanglement	Ekert A.K.	1991	[19]
3	B92	Heisenberg Uncertainty Principle	C.H. Bennett	1992	[17]
4	Hwang98	Heisenberg Uncertainty Principle	W. Y. Hwang I.G. Koh and Y.D. Han	1998	[24]
5	SSP	Heisenberg Uncertainty Principle	Bechmann P.H. and Gisin N.	1999	[25] [26]
6	DPS	Quantum Entanglement	K.Inoue, E.Waks and Y.Yamanoto	2003	[27] [28]
7	SARG04	Heisenberg Uncertainty Principle	Scarani.V, A.Acin, Ribordy G , Gisin.N	2004	[21]
8	COW	Quantum Entanglement	Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N and ScaraniV	2004	[23]
9	KMB09	Heisenberg Uncertainty Principle	M. M. Khan, M. Murphy and A. Beige	2009	[29]
10	LL12	Heisenberg Uncertainty Principle	S. Lin and X.F. Liu	2012	[20]
11	S13	Heisenberg Uncertainty Principle	E. Esteban H. Serna	2013	[31]

IV. CONCLUSION

Quantum cryptography protocols are based on combinations of principles from quantum physics and information theory. Quantum cryptography cipher is considered as absolute secure cryptographic method because of eavesdropping detection. It is regarded as unbreakable until the validity of quantum mechanics laws exist. The combination of quantum key distribution with conventional secret key cryptographic algorithms allows raising the confidentiality of information transmission to an unprecedented level. Quantum cryptography has a bright future and is getting its necessary attention with its robust security potential. The MIT technology Review and Newsweek magazine wrote in 2013 quantum cryptography as one of the "ten technologies that will change the world".

REFERENCES

[1] M.A. Nielsen and I.L Chuang. Quantum computation and quantum information. Cambridge University Press, 2000.

[2] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, Oct. 1996.

[3] RL Rivest, A Shamir, L Adleman , "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM 21 (2), 120-126, 1978.

[4] Diffie, W., Hellman, M., "New directions in cryptography". IEEE Transactions on Information Theory 22 (6): 644–654, 1976.

[5] US NIST, "Federal Information Processing Standards Publication 197", November 26, 2001.

[6] P.W. Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM Journal on Computing, pp. 1484-1509, 1997.

[7] G. V. Assche, "Quantum Cryptography and Secret-Key Distillation", 6th ed. New York, Cambridge University Press, 2006.

[8] R. Alléaume,"SECOQC White Paper on Quantum Key Distribution and Cryptography", Secoqc-Wp-V5, White Paper, Ver. 5.1, 2007.

[9] D. Hrg, L. Budin, M. Golub. Quantum Cryptography and Security of Information Systems. Proceedings of the 15th International Conference on Information and Intelligent Systems, IEEe, pp. 63-70, 2004.

[10] N. Papanikolaou, "An Introduction to Quantum Cryptography", In ACM Crossroads Magazine, vol. 11,No.3, pp.1-16, 2005.

[11] M. Sharbaf, "Quantum Cryptography: A New Generation of Information Technology Security System", IEEE Computer Society, ITNG, page 1644-1648, 2009.

[12] M. van Dijk and H. van Tilborg, "The art of distilling [secret key generation], Proc. of the ITW'98, Killarney, 1998, pp. 158-159, 1998.

[13] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Proc. of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179, 1984.

[14] S.J. Wiesner, "Conjugate Coding", SIGACT News 15, pp. 78–88, 1983. (manuscript written circa 1970).

[15] D. Mayers, "Unconditional security in quantum cryptography," Journal of the ACM, vol. 48, no. 3, pp. 351–406, May 2001.

[16] Shor P.W. and Preskill J., Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. Physical Review Letters, vol. 85, pp. 441-444, 2000.

[17] C.H. Bennett Quantum cryptography using any two non orthogonal states, Physical Review Letters 68 (21) (1992) 3121-3124.

[18] M. Haitjema, "A Survey of the Prominent Quantum Key Distribution Protocols", "http://www.cs.wustl.edu/~jain/cse571-07/ftp/quantum/index.html#b92

[19] Ekert, K. Artur, "Quantum cryptography based on Bell's theorem", Physical Review Letters, Vol. 67, No. 6, 5 August 1991, pp 661 - 663.

[20] A. Einstein, B. Podolsky, N. Rosen, "Can quantum mechanical description of physical reality be considered complete?" Physical Review 47 (1935) 777–780.

[21] V. Scarani, A. Ac´ın, G. Ribordy, N. Gisin, Phys. Rev. Lett. 92, 057901 (2004).

[22] Chi-Hang Fred Fung, Kiyoshi Tamaki, Hoi-Kwong Lo, "On the performance of two protocols: SARG04 and BB84", Phys. Rev. A 73, 012337 (2006).

[23] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner and V. Scarani, "Towards practical and fast quantum cryptography", 2004.

[24] W. Y. Hwang, I.G. Koh and Y.D. Han, 1998. Quantum cryptography without public announcement of bases. Phys. Lett., A244: 489-494.

[25] N.Gisin. talk presented at the workshop on Quantum Computation, Torino. July 1997; D.bruss. Physical review letter. Vol 81.no3018 (1998).

[26] Bechmann-Pasquinucci, H and Gisin.N "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography." Physical Review Letter A59, 4238-4248; (1999).

[27] K.Inoue, E.Waks and Y.Yamanoto." Differential-phase-shift quantum key distribution using coherent light." Phys.Rev. A 68.022317 (2003).

[28] E.Waks, H.Takesue and Y. Yamamoto, "Security of differential-Phase-Shift quantum key distribution against individual attacks." Phys.Rev.A 73,012344 (2006).

[29] M. M. Khan et al. "High error-rate quantum key distribution for long distance communication" New J.Phys. 11 063043 http://iopscience.iop.org/1367-2630/11/6/063043/

[30] S. Lin and X.F. Liu, "A modified quantum key distribution without public announcement bases against photon-number-splitting attack". Int. J. Theor. Phys., 51, pp. 2514-2523, 2012.

[31] Eduin H.Serna, "Quantum Key Distribution from a random seed" arXiv: 1311.1582v2 quant-ph 12th Nov 2013.