Quantum Key Distribution (QKD) Protocols: A Survey

1st Ali Ibnun Nurhadi
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
ain@students.itb.ac.id

2nd Nana Rachmana Syambas
School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia
nana@stei.itb.ac.id

***Abstract*—The security strength of key distribution of most conventional cryptography is relied on mathematical complexity and the irrational time needed to break the algorithm. But it will be ineffective if the secret key distribution procedure is weak. In 1994 Peter Shor proposed an algorithm that can factorize great integer number efficiently by using principle of quantum computer, this algorithm poses a threat to some of the conventional cryptography. Recently, Quantum Key Distribution (QKD) is drawing much attention of researcher as a solution of that problem of key distribution. Theoretically, QKD have been proven can be provide unconditionally secure communication based on quantum mechanics laws. In this article we survey the QKD protocols. Also, we present a little experiment of some QKD protocols that we discussed on this paper.**

Keywords—QKD Protocols, Quantum Cryptography, Quantum Key Distribution

I. Introduction

Quantum key distribution (QKD) is a new security technology that depend on the laws of quantum mechanics to share the secret key and provide unconditionally security. By using quantum mechanics law, QKD has new ability that is not owned by conventional cryptography technique namely ability to detect the presence of eavesdropper. All of eavesdropper activities can be detected as error. The security that provide by QKD system have been proven robust to adversary attack, even with unlimited computational power. The first protocol of QKD was proposed in 1984 by Bennett and Brassard [1] and the first successful implementation of QKD deployed in 1989 [2]. Besides that, there are some great successfully projects of QKD network implementation such as DARPA Quantum Network [3], SECOQC QKD Network in Vienna [4], and Tokyo QKD Network [5].

II. Quantum Key Distribution

QKD is an emerging technology in quantum cryptography world. Unlike conventional cryptography algorithm which depend on complexity of mathematics as its security strength basis, the QKD uses quantum mechanics laws as its security strength basis and theoretically it has been proven can provide unconditionally security by combining three factors namely exploit the law of quantum mechanics, implemented by using one-time-pad and hashing scheme. The basic block diagram of QKD is illustrated by figure 1.

In figure 1 illustrated that QKD system has two channels i.e. quantum channel and public channel. Quantum Channel is used to transmit and share the information of secret key in the form of polarized photon, called as quantum bit (qubit). Meanwhile the public channel is used to discusses the process of qubits transmission and make a deal about the shared secret key. Generally, there are two medium types of quantum channel which is implemented on QKD system i.e. optical fiber and free space. There are some popular identity terms that used in QKD system namely Alice as the sender, Bob as receiver, and Eve as eavesdropper.

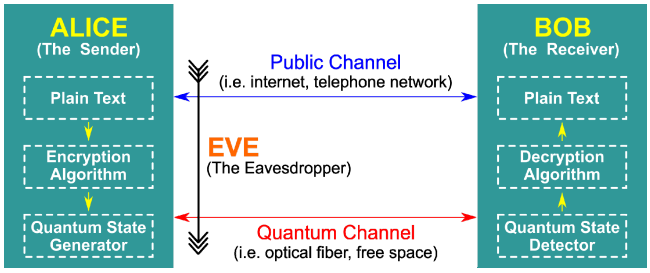

Fig. 1. Basic Block Diagram of QKD System

Furthermore, QKD implementation can be broken to four main procedures i.e. Raw key exchange, Key sifting, Key distillation, and Usable key size. These procedures explained by flowchart in figure 2.

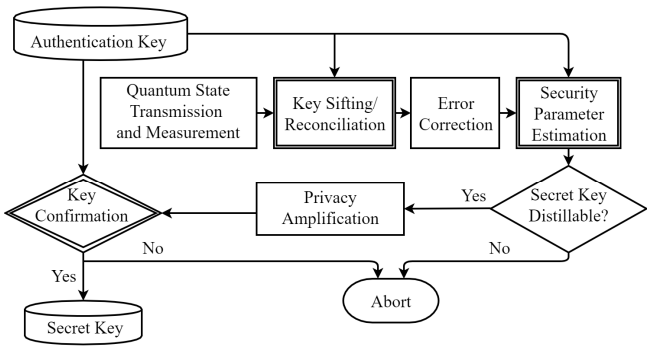

Fig. 2. Basic Flowchart of QKD Procedure

III. QKD Protocols

Basically, there are two types of QKD protocol schemes, the first scheme is prepare-and-measure-based QKD protocol, and the second scheme is entanglement-based QKD protocol. It was called as prepare-and-measure because in this protocol type, the sender (Alice) must "prepare" the information in the form of polarized photon and then the receiver (Bob) "measure" that photons sent.

Prepare-and-measure-based QKD protocol using Heisenberg's uncertainty principle, in which according to this principle, it is impossible to measure the quantum state in a system without disturbing its original quantum state. As explained in no-cloning theorem [6], stated that the quantum bit (qubit) is cannot be copied or amplified without

978-1-5386-6163-5/18/$31.00 ©2018 IEEE

disturbing them. This mechanism enabling the QKD system to detect the presence of eavesdropper by using the error parameter measurement that appear during the transmission process of photons from Alice to Bob. Meanwhile, in entanglement-based QKD protocol, Alice and Bob use entanglement photons principle to distribute the secret key.

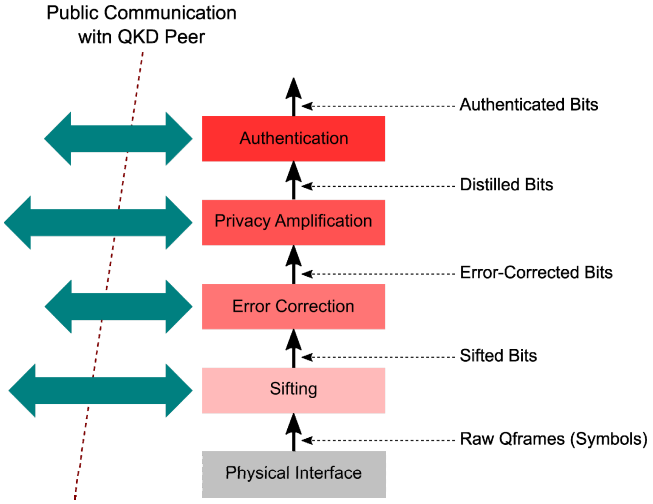

Fig. 3. Full Stack of QKD Protocol

Figure 3 describe the full stack diagram of QKD protocol, consisting of five mechanism i.e. raw q-frame, bits sifting, bits error correction, bits distillation, and bits authentication. In this section, there are nine protocols discussed, consisting of five prepare-and-measure-based QKD protocols and four entanglement-based QKD protocols. The discussion of these protocols is sorted by the year of its release.

A. BB84 Protocol

In 1984 [1], two researchers Bennett and Brassard proposed a protocol to share secret key between two parties using quantum mechanics principles, i.e. Heisenberg's uncertainty principle. It was the first quantum cryptography protocol that explained how to use photon polarization state to transmit the information of secret key through a quantum communication channel. This protocol well-known as BB84 protocol and categorized as prepare-and-measure-based QKD protocol.

BB84 protocol using single photon to transmit and distribute random bits of secret key. The single photon is polarized in one of four polarization states and selected using one of two conjugate bases namely rectilinear basis for vertical and horizontal polarization, and diagonal basis for diagonal and its anti-diagonal polarization, these bases polarization is illustrated by figure 4.

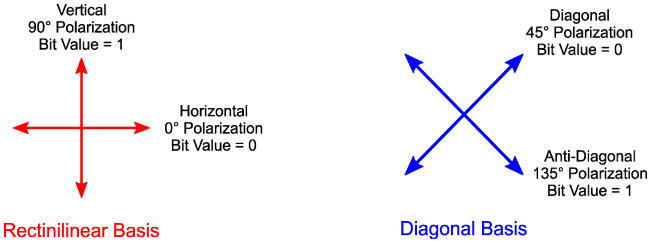

Fig. 4. Polarization Base of BB84 Protocol

The BB84 protocol implementation process can be divided into four main steps: Quantum Exchange, Key Sifting, Information Reconciliation, and Privacy Amplification. These four steps mechanism illustrated by figure 5 and explained in more detail steps by figure 6.

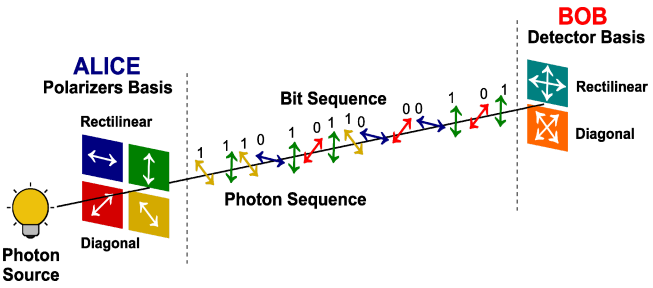

Fig. 5. Quantum Exchange Illustration of BB84 Protocol

Quantum Exchange															
Alice's random bit	1	0	1	1	0	0	0	1	1	0	1	0	0	1	1
Alice's random basis selection	R	D	R	R	D	D	R	D	R	R	R	D	R	D	D
Polarized photon sent by Alice	↕	↗	↕	↕	↗	↗	↔	↘	↕	↔	↕	↗	↔	↘	↘
Bob's random basis selection	D	R	D	R	D	D	D	D	R	R	R	R	D	D	D
Bob's measured received bits	0	0	1	1	0	0	0	1	1	1	1	1	1	1	1
Bob's basis and Alice's basis agreement?	N	N	N	Y	Y	Y	N	Y	Y	Y	Y	N	N	Y	Y
Public Discussion															
Bob reports basis of received bits	D	R	D	R	D	D	D	D	R	R	R	R	D	D	D
Alice says which basis were correct				√	√	√		√	√	√	√			√	√
Sifted key				1	0	0		1	1	1	1			1	1
Bob reveals some key bits randomly					0						1				
Alice confirm them					√						√				
Outcome															
Remaining Shared Secret Bits				1		0		1	1	1				1	1

Fig. 6. Detail Steps of BB84 Protocol Implementation

Theoretically BB84 protocol have been proven to provide unconditionally security by [7], [8], and discussed in detail in some research publications [9], [10], [11].

B. E91 Protocol

In 1991, Ekert [12] developed a QKD protocol that designed using entangled pairs of photons. By using the photon entanglement principle, the photons source can be created either by Alice or Bob. Entanglement-based QKD model can be illustrated by figure 7.

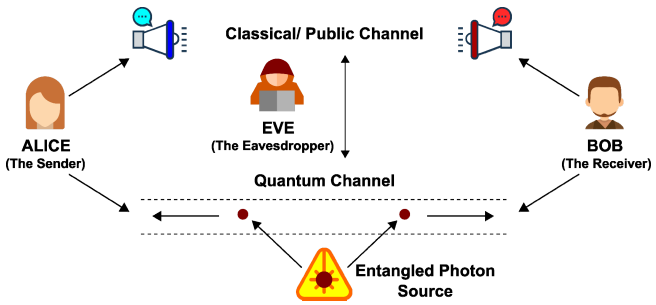

Fig. 7. Basic Concept of Entanglement-Based QKD Protocol

In figure 7 is illustrated that entangled photon source releases a pair of entangled photon/ particle which either Alice or Bob receive one particle from each pair. Same with the BB84 procedure, in E91 protocol Alice and Bob choose a random basis for measurement and discussing them in classical channel. If Alice and Bob use the same basis, then according to the quantum principle they should get opposite results. E91 protocol using Bell's Inequality test to detect

the presence of eavesdropper. E91 protocol classified as entanglement-based QKD protocol.

C. BBM92 Protocol

The basic concept of BBM92 protocol is similar with BB84 protocol such as raw key exchange mechanism, key sifting, and privacy amplification are basically the same. BBM92 can be said as entanglement-based version of BB84 protocol. This protocol proposed by Bennett, Brassard, and Mermin in 1992 [13] shortly after Ekert proposed his E91 protocol. BBM92 classified as entanglement-based QKD protocol.

D. B92 Protocol

B92 protocol is simplified version of BB84 protocol that proposed by Bennett in 1992 [14]. B92 protocol only use one of two polarization states while in BB84 use one of four photon polarization states. It is become the key difference between B92 and BB84 protocol. In B92 protocol 0-bit value encoded as 0 degrees in the rectilinear basis, and 1-bit value encoded as 45 degrees in the diagonal basis. Bennett realized that a single non-orthogonal basis can be used for encoding and decoding QKD protocol without affecting the ability to detecting the presence of eavesdropper. Another difference between B92 and BB84 protocol is in B92 protocol if the receiver (Bob) select the wrong basis, then he will not measure anything. In quantum mechanics, this condition is known as an erasure [15]. B92 is classified as prepare-and-measure-based QKD protocol.

E. Six-State Protocol (SSP)

In 1999, six-state protocol was proposed by Pasquinucci and Gisin [16]. This protocol using 6 polarization states and 3 measurement bases. Essentially, six-state protocol can be regarded as BB84 scheme with an additional basis, become 3 measurement bases.

Figure 8 is the Poincare sphere illustration, BB84 protocol can be represented on the Poincare sphere makes use of four spin-1/2 polarization states which corresponding to ±x and ±y direction. While the 6 state protocols have two extra polarization states correspond to ±z, become 6 states, they are ±x, ±y, and ±z on the Poincare sphere. Six-state protocol has higher symmetry compared to the BB84 protocol, and it is become his advantage. SSP is classified to prepare-and-measured-based QKD protocol.

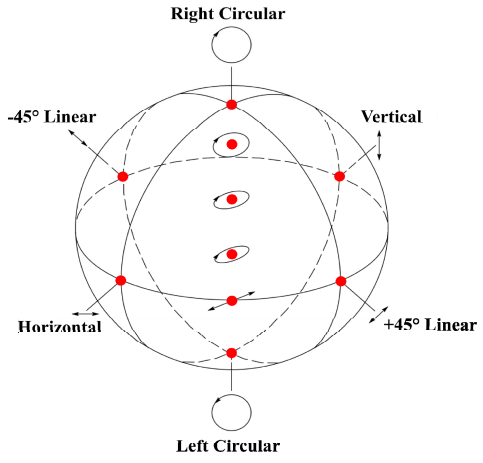

Fig. 8. Poincare Sphere

F. DPS Protocol

Differential-Phase-Shift QKD (DPS-QKD) protocol was proposed by K. Inoue et al. [17] in 2003. The setup and protocol scheme of the DPS-QKD l is illustrated by figure 9.

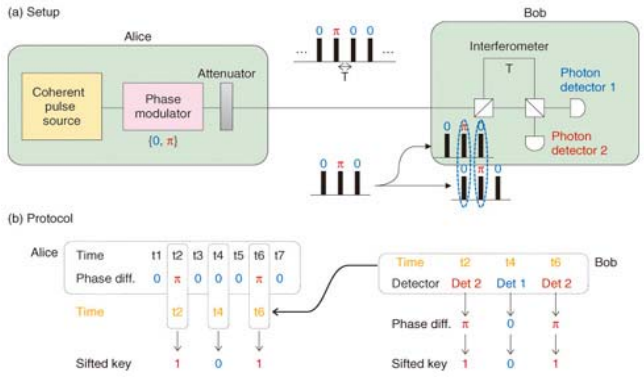

Fig. 9. Schematic diagram of DPS protocol [18]

This protocol designed by using the quantum entanglement principle. This protocol has some advantageous i.e. robust to photon number splitting (PNS) attack [17], [19], has simple configuration, and using domain time efficiently. DPS protocol is classified as entanglement-based QKD protocol.

G. SARG04 Protocol

The SARG04 protocol was proposed by Scarani, et al. [20] in 2004. This protocol designed by using attenuated laser pulse as photon source instead of single photon source. SARG04 and BB84 protocol has identical scheme first phase of these protocol. But it differs for the second phase, the sender, Alice use one of her pair of non-orthogonal state to encode her bit rather than she announces her bases directly. If Bob use appropriate basis, he will measure the exact state, but if he chooses wrong basis then he will not get the bit. For no errors assumption/ measurement, the length of the key remaining after the sifting stage is 0.25 of the raw key sent. SARG04 protocol is classified as prepare-and-measured-based QKD protocol.

H. COW Protocol

Coherent One-Way protocol (COW protocol) was proposed by Nicolas Gisin et al. in 2004 [21]. COW protocol designed by using the photon entanglement principle. This protocol has some advantages namely has high efficiency on distilled secret bits per qubit, robust to photon number splitting (PNS) attack and tolerant to reduced interference visibility. The COW protocol scheme is illustrated by figure 10. In COW protocol, the information is encoded in time function. This protocol is classified as entanglement-based QKD protocol.

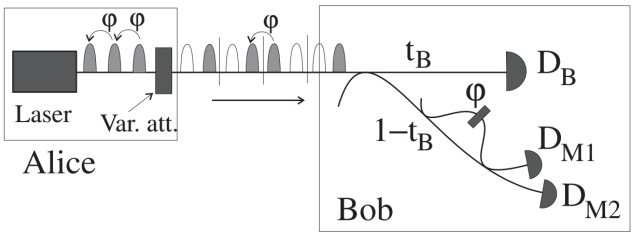

Fig. 10. Scheme of the COW protocol [21]

I. *S13 Protocol*

S13 protocol was proposed by Eduin H. Serna [22]. This protocol is identical to the BB84 protocol for all the quantum mechanism. The difference is by using private reconciliation from a random seed and asymmetric cryptography.

The resume of all protocols discussed in this paper is presented in table 1.

TABLE I. LIST OF QKD PROTOCOLS

No.	Year	Name of Protocol	Principle Base
1	1984	BB84	Heisenberg's Uncertainty Principles
2	1991	E91	Quantum Entanglement
3	1992	BBM92	Quantum Entanglement
4	1992	B92	Heisenberg's Uncertainty Principles
5	1999	SSP	Heisenberg's Uncertainty Principles
6	2003	DPS	Quantum Entanglement
7	2004	SARG04	Heisenberg's Uncertainty Principles
8	2004	COW	Quantum Entanglement
9	2013	S13	Heisenberg's Uncertainty Principles

IV. SIMULATIONS AND RESULTS

In this section the authors simulated three QKD protocols consisting of two prepare and measure-based protocols (BB84 and B92), and an entanglement-based protocol (BBM92). This simulation is done by using a quantum simulator that is QuVis [23]. The experiment setup are as follows:

- There are three protocols involved in this simulation namely BB84, B92, and BBM92 protocol.
- The testing scheme is conducted by involving the passive eavesdropping.
- Alice and Bob use a random basis to send polarized photon for each protocol experiments.
- Eavesdropper between Alice and Bob is also uses random base to translate the polarization base of Alice.
- This experiment conducted by activating "fast forward 100 photons" feature.
- The experiments are done by sending 100 photons to 2000 photons.
- Parameters measured in this experiment are value of N Key (Nk), N Error (Ne), and N error/ N Key (Np) for each protocol.

The result data of these simulations is presented in table 2. The value of N Key (Nk) for each protocol is presented in figure 11, the value of N Error (Ne) is presented in figure 12, and the value of N Error/ N Key (Np) is presented in figure 13. In Figure 11 is shown that the most number key generated is 1004 keys for 2000 photons sent using BBM92 protocol, while the least number key generated is 16 keys for 100 photons sent using B92 protocol. The more number of keys generated, the better.

TABLE II. KEY AND ERROR SIMULATIONS RESULTS

Photon Number	BB84			B92			BBM92		
	Nk	*Ne*	*Np*	*Nk*	*Ne*	*Np*	*Nk*	*Ne*	*Np*
100	52	12	0.231	16	4	0.25	47	12	0.255
200	95	25	0.263	43	11	0.256	99	20	0.202
300	140	39	0.279	68	16	0.235	146	39	0.267
400	192	56	0.292	90	23	0.256	201	53	0.264
500	249	78	0.313	117	26	0.222	250	69	0.276
600	249	88	0.301	146	29	0.199	288	78	0.271
700	292	99	0.289	178	35	0.197	344	91	0.265
800	342	112	0.289	214	44	0.207	395	100	0.253
900	388	126	0.287	239	49	0.205	444	116	0.261
1000	439	139	0.281	265	58	0.219	498	132	0.265
1100	495	159	0.288	288	65	0.226	545	147	0.27
1200	552	171	0.284	310	74	0.239	601	161	0.268
1300	603	180	0.277	334	82	0.246	653	171	0.262
1400	700	187	0.267	361	92	0.255	705	184	0.261
1500	744	200	0.269	394	103	0.261	752	198	0.263
1600	792	209	0.264	416	108	0.26	800	218	0.273
1700	845	226	0.267	443	112	0.253	854	233	0.273
1800	901	237	0.263	470	120	0.255	910	246	0.27
1900	939	246	0.262	491	122	0.248	958	262	0.237
2000	999	257	0.257	511	125	0.245	1004	272	0.271

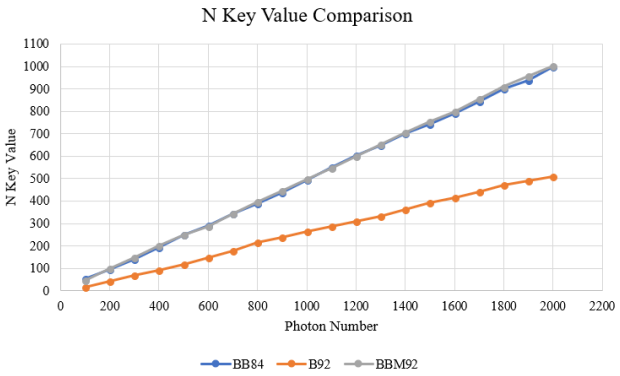

Fig. 11. N Key Value Comparison of BB84, B92, and BBM92 Protocol

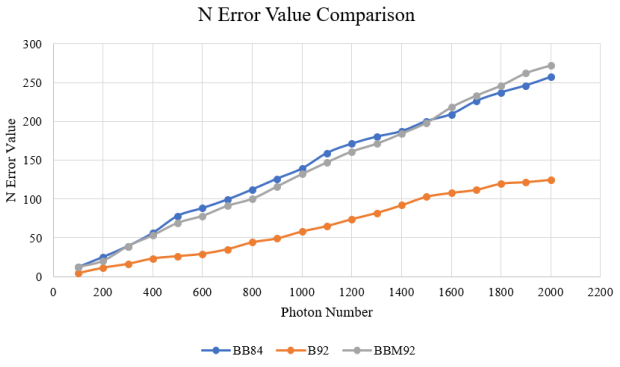

Fig. 12. N Error Value Comparison of BB84, B92, and BBM92 Protocol

In figure 12 is shown that the most number error obtained is 272 errors for 2000 photons sent using BBM92, while the least number error obtained is 4 errors for 100 photons sent using B92 protocol. The fewer number of errors obtained, the better.

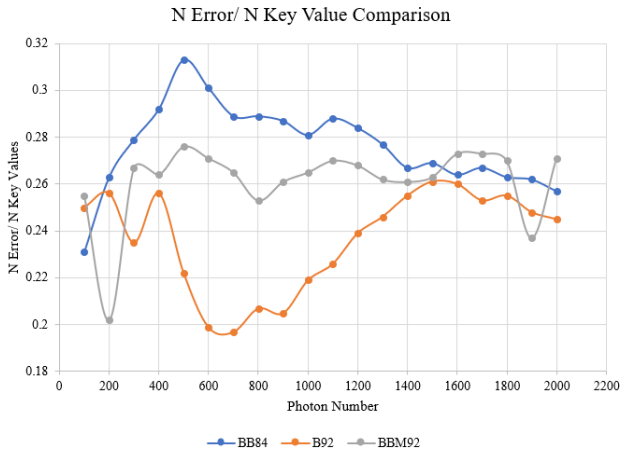

Fig. 13. N Error/ N Key (Error Probability) Value Comparison of BB84, B92, and BBM92 Protocol

In figure 13 is shown that B92 potocol has the smallest probability of error, ranged from 0.199 (19.9%) to 0.256 (25.6%). Theoritically, the maximum error value of B92 protocol is 25%. Non ideal condition of apparatus setup, environment, or design can be affected to the result. Instead, the largest probability of error is obtained by using BB84 protocol, ranged from 0.231 (23.1 %) to 0.313 (31.3%). Theoritically the maximum error value of BB84 protocol is 0.5 (50%). Meanwhile the probability of error of BBM92 is tend to be between of BB84 and B92 error probabilities, it's ranged from 0.202 (20.2%) to 0.276 (27.6%).

V. Conclusion

Quantum key distribution (QKD) is a new security technology that depend on the laws of quantum mechanics to share the secret key. QKD provide unconditionally security and an ability to detect presence of eavesdropper. This cryptography technology is drawing much attention of researcher as a solution of that problem of key distribution. There are tens of QKD protocol has been proposed, but basically, there are two main types of QKD protocol namely prepare and measure-based QKD protocol and entanglement-based QKD protocol. Prepare-and-measure-based QKD protocol using Heisenberg's uncertainty principle and entanglement-based QKD protocol using entanglement photons principle to distribute the secret key.

Based on experiment result of prepare and measure-based protocol (BB84, B92) and entanglement-based protocol (BBM92) that presented in table 2, figure 11, 12, and 13, the value of N error/ N key of B92 is the smallest, it's mean the error probability of this protocol (B92) is the smallest. If referring to error parameter, B92 protocol is the best than two other protocols (BB84 and BBM92), but in the implementation of QKD network there are some factors which must be considered such as secret key rate, distance, setup cost, robustness, etc.

References

[1] C. H. Bennett, and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theor. Comput. Sci. 560, pp. 7-11, 2014.

[2] C.H. Bennett, and Gilles Brassard, "Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working," ACM SIGACT News 20, pp. 78-82, 1989.

[3] C. Elliott *et al*., "Current status of the DARPA Quantum Network," 2005.

[4] M. Peev *et al*., "The SECOQC Quantum Key Distribution Network in Vienna," 2009 35th European Conference on Optical Communication, pp. 1-4, 2009.

[5] M. Sasaki et al. "Field test of quantum key distribution in the Tokyo QKD Network," Optics express vol. 19, pp. 10387-10409, 2011.

[6] W.K. Wootters, and W. H. Zurek, "A single quantum cannot be cloned," Nature 299, pp. 802-803, October 1982.

[7] S. Singh, "The Code Book: The Secret History of Codes and Code-breaking," Fourth Estate, London, 1999.

[8] S. Vittorio, "Quantum Cryptography: Privacy though Uncertainty," CSA Discovery Guides, 2002.

[9] E. Biham, M. Boyer, P. Boykin, T.Mor, V Roychowdhury, "A Proof of the Security of Quantum Key Distribution," Journal of Cryptology vol. 19, pp. 381-439, 2006.

[10] D. Mayers, "Unconditional security in quantum cryptography," J. ACM 48, pp. 351-406, May 2001.

[11] P. W. Shor, and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Phys. Rev. Lett., 85, pp. 441-444, July 2000.

[12] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Physical review letters vol. 67, pp. 661-663, August 1991.

[13] C. H. Bennett, G. Brassard, and N.D. Mermin, "Quantum cryptography without Bell's theorem," Physical review letters. 68. Pp. 557-559, February 1992.

[14] C. H. Bennett, "Quantum Cryptography using any two Nonorthogonal Sates," Physical review letters vol. 68, pp.3121-3124, June 1992.

[15] D. Bruss, G. Erdelyti, T. Meyer, T. Riege, and J. Rothe, "Quantum Cryptography: A Survey," ACM Computing Surveys, Vol. 39, No. 2, Article 6, June 2007.

[16] H. B. Pasquinucci,and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," Physical Review Letter A59, pp. 4238-4248, 1999.

[17] K. Inoue, E. Waks, Y. Yamanoto, "Differential-phase-shift quantum key distribution using coherent light," Phys.Rev. A 68, 2003.

[18] Y. Tokura, and T. Honjo, "Differential phase shift quantum key distribution (DPS-QKD) experiments," NTT Basic Research Laboratories, Vol. 9, September 2011.

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

[20] V. Scarani, A. Acin, G.Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Physical Review Letters, vol. 92. February 2004.

[21] N. Gisin *et al*., "Towards practical and fast quantum cryptography," 2004, unpublished.

[22] E. H. Serna, "Quantum Key Distribution from a random seed," November 2013, unpublished.

[23] A. Kohnle *et al*., "Quvis, the quantum mechanics visualisation project," [Online]. Available: https://www.st-andrews.ac.uk/physics/quvis/, accessed on: May 2018.