Analysis of Quantum Key Distribution Protocols

Myat Su Win
Faculty of Computer Systems and Technologies
University of Computer Studies,
Yangon, Myanmar
myatsuwin@ucsy.edu.mm

Thet Thet Khin
Faculty of Computer Systems and Technologies
University of Computer Studies,
Yangon, Myanmar
thetthetkhin@ucsy.edu.mm

Abstract-Essential role of Internet-based communication is the security of information. Classical Cryptography is based on mathematical models and computational complexity to compute the secret key. It does not provide enough security because finding a fast method to calculate the secret key will compromise the security of the system. Quantum Key Distribution is one of the most promising methods which provide unconditional security. Quantum Key Distribution (QKD) uses a quantum property in exchanging information called photons, as carriers of information in security systems, and QKD cannot separate from protocols BB84, B92 and BBM92. In this paper, we are testing the probability error comparison of BB84 protocol, B92 protocol, and BBM92 using QuVis simulator software. The results show that the B92 protocol is more relevant in detecting eavesdropping in lower error rates than the other two protocols.

***Keywords*— BB84, B92, BBM92, QuVis**

I. INTRODUCTION

Information security is growing more and more important field due to the widespread use of the internet, Wi-Fi, and Bluetooth. Classical cryptography is based on mathematics, and it relies on the computational difficulty of a factorizing large number. The security of classical cryptography is based on the high complexity of the mathematical problem, for instance, the factorization of the large number [1]. Confidentiality of information is important in communication between sending and receiving entities. By using encryption and decryption algorithms, secure message transmission will be achieved. So, an unauthorized person cannot access the messages, and it is known as cryptography. Message transmission involves the sender and receiver are named Alice and Bob, and the eavesdropper is named Eve [2]. For the confidentiality of information, encrypt the message before it is sent to the recipient with the secret keys known by Alice and Bob who are involved in the communication. The problem is how the secret keys are ensured to be safe, that during the classical exchange process, there is no way to ensure the key exchange process is completely secure. To overcome this issue, there is quantum mechanics as a method of securing the keys distribution [3].

Quantum Cryptography is based on physics, and it relies on the laws of quantum mechanics. It is arising technology that emphasizes the phenomena of quantum physics in which two parties can have secure communication based on the invariability of the laws of quantum mechanics. It allows two parties to generate a key with special characteristics and use it for secure communication between them [4].

II. RELATED WORKS

Nowadays, security is more and more important in communication between entities. To get a secure data transmission process, the encryption key needs to improve and secure every time. So, many researchers test the security of quantum key distribution protocols using different simulator environments to acquire a secure key distribution.

Omer K and Safia Abbas [5] presented the alternative quantum key distribution protocol different from the traditional key distribution protocols. Using two distinct modes, with or without eavesdropper, implemented with a standard simulator that is programmed using Visual Studio Ultimate 2012 (VC#) for QKD-BB84 protocol.

Manish Kalra and Ramesh C [6] proposed a protocol for quantum key distribution and simulation of BB84 protocol. They have presented the simulation process of BB84 protocol and proposed protocol in C++ using an object-oriented protocol approach. According to their simulation results, the average error rate of the proposed protocol is 50% less than the average error rate of the BB84 protocol. There are only two entities, one is the sender, and another one is the receiver; the eavesdropper does not present in their system. Using different security configurations for the efficiency of BB84 protocol validation and results are presented. According to their results, the QKD is susceptible to corporate with different security applications and achieves the key availability for such applications.

Beatrix Rambu Hada Nuhamara and Nana Rachmana Syambas [7] analyzed the probability error of the BB84 protocol and the probability error of the B92 protocol by sending range from 100 photons to 1000 photons and then compared these two protocols by using QuVis simulation software. According to their results, the BB84 protocol is more error rate than the B92 protocol.

In this paper, we tested photon sending range from 100 photons to 3000 photons and compared the probability errors of BB84 protocol, B92 protocol and BBM92 protocol to get more experiment result for future research.

III. QUANTUM KEY DISTRIBUTION

Quantum Key Distribution (QKD) is a secure communication method that implements a cryptographic protocol involving components of quantum mechanics. In quantum cryptography, Quantum Key Distribution is a fundamental technique for the secure key generation process. QKD does not use to transmit any message data and only used to generate and distribute a secure key. Then this key can be used with any chosen encryption algorithm to encrypt and decrypt a message. When data transmission from sender to receiver, quantum computing uses a stream of photons that have a property called a 'spin', and there are four types of spins: Horizontal and vertical, +45° diagonal,

and -45° diagonal. The horizontal and +45° represent the binary value 1 and the vertical and -45° represent the binary value 0 respectively [8,14]. The following Fig. 1 shows the process of Quantum Key Distribution.

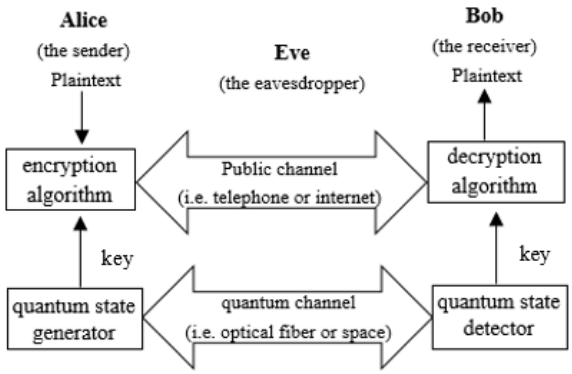

Fig. 1. Quantum Key Distribution

A. *BB84 Protocol*

One of the Quantum Key Distribution protocols is the BB84 protocol that was proposed by Bennett and Brassard in 1984. This protocol is based on photon polarization and uses two bases, the rectilinear (+) base and the diagonal (x) base. The rectilinear (+) base has two polarization, horizontal representing bit 0 and vertical representing bit 1. The diagonal (x) base also has two polarization, +45° representing bit 0 and -45° representing bit 1[9,13]. The following Fig. 2 shows the BB84 protocol quantum key exchange processes.

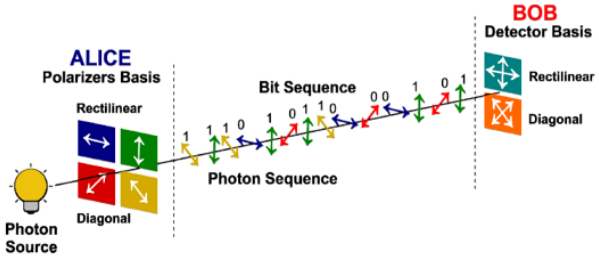

Fig. 2. Example of BB84 protocol key exchange

B. *B92 Protocol*

The B92 protocol was proposed by Bennett, Brassard, Salvail, and Smolin as a simplification of the BB84 protocol in 1992. The bases used in these protocols are different, BB84 protocol uses four bases and B92 protocol uses only two bases (+45° and -45°) [9]. Alice transmitted a number of photons encoded with randomly selected bits to Bob as well as the BB84 protocol. Likewise, Bob selects a random basis for measuring bits sent by Alice, but if the base used by Bob is the wrong base there is no measurement. Alice and Bob communicate using quantum channel. Alice sends bits of information in the form of photons and randomly selects a vertical base with bit value '1' in encoding with 45° polarization or horizontal base with '0' bit value encoded with 0° polarization [10]. The following Fig. 3 shows the B92 protocol quantum key exchange processes.

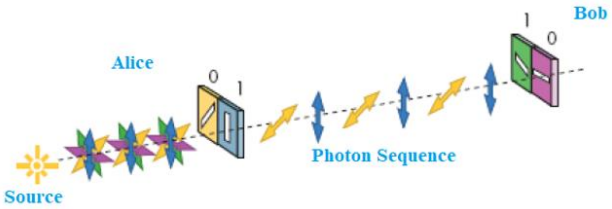

Fig. 3. Example of B92 protocol key exchange

C. *BBM92 Protocol*

Bennett, Brassard, and Mermin proposed the BBM92 protocol in 1992 that implements Quantum Key Distribution by using polarized-entangled photon pairs for communication between the sender and receiver [11]. A source produces polarization-entangled photon pairs and then these pairs are split into two photons, one photon from each pair being sent to Alice and one to Bob. Alice and Bob each randomly choose to measure each photon they receive in one of two non-orthogonal complementary bases, the horizontal/vertical basis (H = 0° and V = 90°) or +/- basis (+ = +45° and − = −45°). After a measurement run, where Alice and Bob have been measuring incoming photons for a certain time, they communicate publicly over a classical channel which basis they measured in for each photon they received. If they measured in the same basis, they each save their measurement result and they discard measurement result when their basis is different. Next Alice and Bob convert their measurement results to bit values by assigning the measurement results H and '+' to the bit value '0' and V and '-' to the bit value '1' [12].

IV. Experiment Setup

In this experiment, the QuVis software environment has been used as a simulator. Three protocols have been implemented in the simulation environment that is part of QKD and Eve will be added as an eavesdropper to develop the experiment. We tested the probability error comparison of BB84 protocol, B92 protocol, and BBM92 protocol.

In each testing, Alice (sender) and Bob (receiver) use a random basis to send photon polarization. Eve as eavesdropper between Alice and Bob also uses a random basis for translating the sender basic sent to the receiver. Using a "fast forward 100 photons" option to send polarized photons to Bob. Sending 100 photons to 3000 photons for this experiment and comparing the error probability ratio of each photon.

A. *Testing for BB84 Protocol*

In this protocol testing, Alice generates a secure key using polarized photons from 100 photons to 3000 photons. Alice randomly uses each photon polarization in one of two bases, either vertical or horizontal, and +45 or -45 using one of these four polarization directions. The vertical and -45 basis are assigned value '1' and the horizontal and +45 basis are assigned value '0' respectively [3].

By using the Intercept-Resend attack, Eve can interrupt the quantum channel and measure each quantum state send by Alice to Bob and then Eve will choose randomly one of the polarization bases and resend the photon to Bob. If Eve chooses incorrect polarized bases, means the infeasibility to measure the quantum state and if Eve chooses correctly, means the feasibility to measure and change the quantum

states and then resend the sequence of the quantum states to Bob. To overcome this vulnerability, the solution is monitoring the percentage of errors acquired between the sender and receiver communication at the end of the transmission [3].

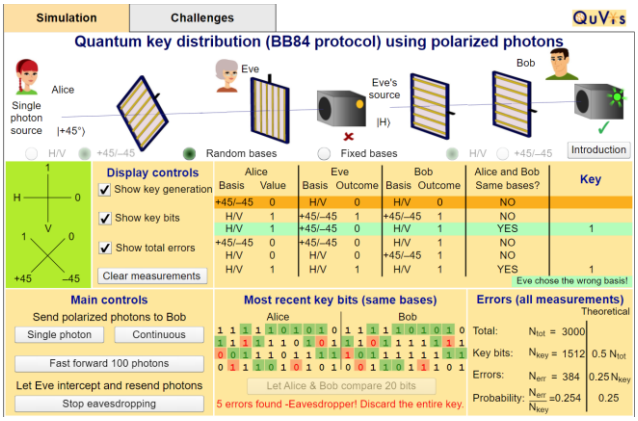

Fig. 4. Experiment testing of BB84 Protocol (QuVis)

Experiment testing for BB84 protocol is depicted in Fig. 4. Bob will be randomly selected as a base to detect each photon sent by Alice. According to these experimental results, it can be concluded:

- Alice and Bob use the same base but different values, and Eve uses a different base but the value is the same as Alice or Bob do not generate key and error occur.
- Alice and Bob use the same base, and Eve uses a different base, but all three values are the same, generate a key agreed between Alice and Bob.
- All three base and value are the same, generate a key agreed between Alice and Bob.
- Alice and Bob's base is different, but Eve uses the same base as Alice or Bob, and all three values are the same, do not generate a key agreed between Alice and Bob.
- All three values are the same and Alice and Bob use the same base but Eve uses a different base, generate a key agreed between Alice and Bob.
- The four bases used to filter the polarization of 3000 with compare 20 bits resulted in 5 error keys removed by the Eavesdropper effect.

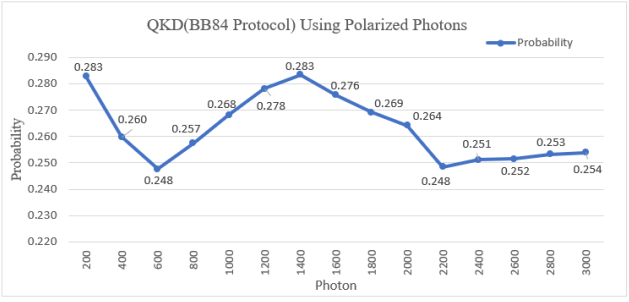

Fig. 5. Experimental result 100 photons to 3000 photons

The test results of 30 experiments shown in Fig. 5, the probability error key produces from the number of keys (N_{key}) and the number of key errors (N_{err}), the formula is:

$$P = N_{err}/N_{key} \quad (1)$$

The probability error key results that can be filtered by Bob does not exceed the supported limit of 0.5 (N_{tot}) so that the QuVis simulator correctly provides the theory of BB84 protocol.

B. Testing for B92 Protocol

In this protocol testing, Alice generates a secure key using polarized photons from 100 photons to 3000 photons. Alice randomly uses 0° (Horizontal) for value 0 or +45 for value 1 and Bob randomly uses 90° (Vertical) for value 1 or -45 for value 0 respectively.

The intercept-resend attack that occurs in the B92 protocol is a few different from the attack occurs in the BB84 protocol. Eve intercepts the quantum channel between Alice and Bob and alter every photon sent from Alice and measure its polarization and then passing the altered photons to Bob. If Eve randomly chooses the same polarized base as Alice, means the feasibility to measure the quantum state and no error occurred. If Eve randomly chooses a different polarized base as Alice, means the infeasibility to measure and change the quantum states and measurement error occur by Bob [3, 11].

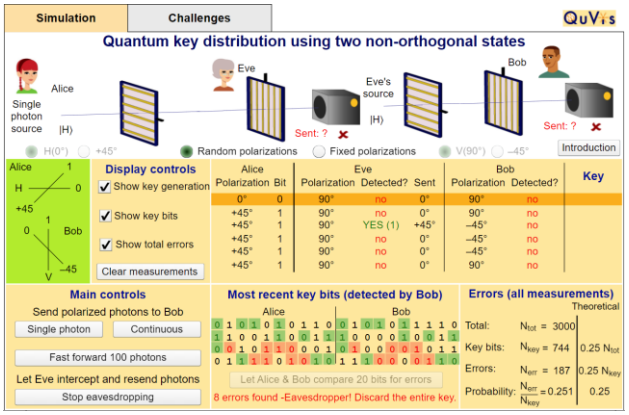

Fig. 6. Experiment testing of B92 Protocol (QuVis)

Experiment testing for the B92 protocol is depicted in Fig. 6. Bob will be randomly selected as a base to detect each photon sent by Alice. According to these experimental results, it can be concluded:

- Alice sends base +45° for value 1 that can be detected by Bob on base 90° although Eve sends the same base as Alice.
- Alice sends base 0° for value 0 that can be detected by Bob on-base -45° although Eve sends the same base as Alice.
- Alice sends base 0° for value 0 that cannot be detected by Bob on base 90°.
- Alice sends base +45° for value 1 that cannot be detected by Bob on-base -45°.
- The two bases used to filter the polarization of 3000 with compare 20 bits resulted in 8 error keys removed by the eavesdropper effect.

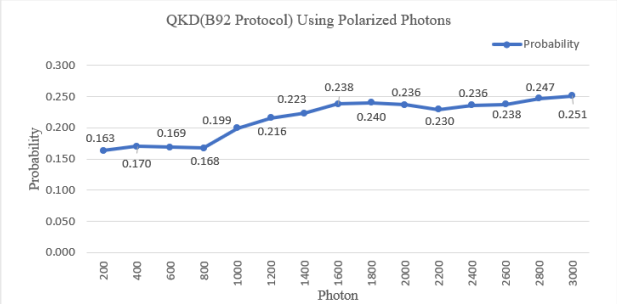

Fig. 7. Experimental result 100 photons to 3000 photons

The test results of 30 experiments shown in Fig. 7, the probability error key produces from the number of keys (N_{key}), and the number of key errors (N_{err}), the formula is N_{err}/N_{key}. The probability error key results that can be filtered by Bob does not exceed the supported limit of 0.25 (N_{tot}) so that the QuVis simulator correctly provides the theory of B92 protocol.

C. *Testing for BBM92 Protocol*

In this protocol testing, Alice generates a secure key using polarized photons from 100 photons to 3000 photons. For entangled spin ½ particles, the particles separate into two discrete streams, one deflected is outcome 1 when the direction is positive and one deflected is outcome 0 when the direction is negative.

Alice and Bob measure the quantum state independently, and two orthogonal axes are denoted X and Z and measurement outcome (0 or 1) and base (X or Z) for each pair [11].

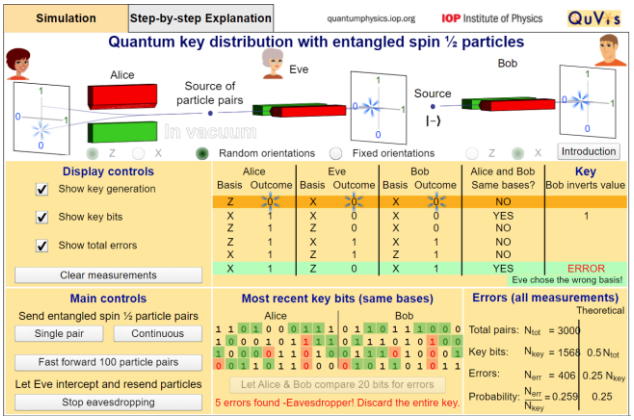

Fig. 8. Experiment testing of BBM92 Protocol (QuVis)

Experiment testing for the BBM92 protocol is depicted in Fig. 8. Bob will be randomly selected as a base to detect each photon sent by Alice. According to these experimental results, it can be concluded:

- Alice and Bob use the same base (X or Z) but different outcomes and Eve uses a different base but the value is the same as Alice or Bob, generate a key agreed between Alice and Bob.
- Alice and Bob use the same base but Eve uses a different base but all three outcomes are the same, do not generate key and error occur.
- Alice and Bob use a different base, do not generate a key agreed between Alice and Bob.
- Alice and Bob have the same outcome, do not generate a key agreed between Alice and Bob.
- The two bases used to filter the polarization of 3000 with compare 20 bits resulted in 5 error keys removed by the Eavesdropper effect.

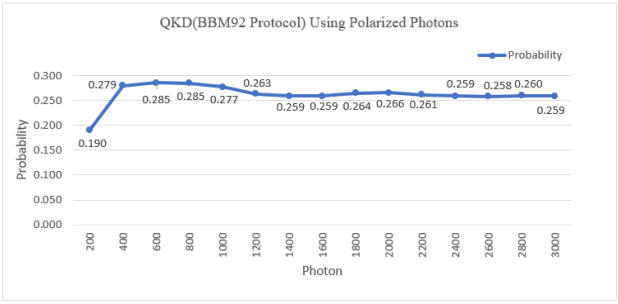

Fig. 9. Experimental result 100 photons to 3000 photons

The test results of 30 experiments shown in Fig. 9, the probability error key produces from the number of keys (N_{key}), and the number of key errors (N_{err}), the formula is N_{err}/N_{key}. The probability error key results that can be filtered by Bob does not exceed the supported limit of 0.5 (N_{tot}) so that the QuVis simulator correctly provides the theory of BBM92 protocol.

D. *Comparison Probability Error for BB84, B92, BBM92*

Using the same scheme for three different protocols generate probability error is shown in the following Table 1 and Table 2.

TABLE 1. COMPARISON PROBABILITY ERROR

Photon (N_{tot})	BB84			B92		
	N_{key}	N_{err}	N_{err}/N_{key}	N_{key}	N_{err}	N_{err}/N_{key}
100	47	13	0.277	26	4	0.154
200	99	28	0.283	49	8	0.163
300	154	43	0.279	69	13	0.188
400	204	53	0.260	88	15	0.170
500	254	62	0.244	110	21	0.191
600	311	77	0.248	136	23	0.169
700	356	91	0.256	160	29	0.181
800	408	105	0.257	191	32	0.168
900	458	116	0.253	250	37	0.148
1000	511	137	0.268	236	47	0.199
1100	563	151	0.268	256	54	0.211
1200	615	171	0.278	278	60	0.216
1300	667	187	0.280	300	65	0.217
1400	720	204	0.283	318	71	0.223
1500	771	214	0.278	342	81	0.237
1600	827	228	0.276	361	86	0.238
1700	873	240	0.275	388	94	0.242
1800	918	247	0.269	412	99	0.240
1900	976	261	0.267	437	103	0.236
2000	1026	271	0.264	461	109	0.236
2100	1041	261	0.251	520	119	0.229
2200	1099	273	0.248	549	126	0.230
2300	1150	290	0.252	572	132	0.231

Photon (N_{tot})	BB84			B92		
	N_{key}	N_{err}	N_{err}/ N_{key}	N_{key}	N_{err}	N_{err}/ N_{key}
2400	1198	301	0.251	593	140	0.236
2500	1246	312	0.250	617	147	0.238
2600	1296	326	0.252	640	152	0.237
2700	1350	342	0.253	669	163	0.244
2800	1398	354	0.253	697	172	0.247
2900	1456	371	0.255	718	180	0.251
3000	1512	384	0.254	744	187	0.251

TABLE 2. COMPARISON PROBABILITY ERROR

Photon (N_{tot})	BBM92		
	N_{key}	N_{err}	N_{err}/ N_{key}
100	51	7	0.137
200	100	19	0.190
300	154	39	0.253
400	204	57	0.279
500	256	72	0.281
600	319	91	0.285
700	369	102	0.276
800	411	117	0.285
900	464	129	0.278
1000	519	144	0.277
1100	560	152	0.271
1200	608	160	0.263
1300	653	167	0.256
1400	699	181	0.259
1500	746	191	0.256
1600	799	207	0.259
1700	847	219	0.259
1800	904	239	0.264
1900	953	252	0.264
2000	1001	266	0.266
2100	1099	288	0.262
2200	1156	302	0.261
2300	1203	311	0.259
2400	1254	325	0.259
2500	1314	340	0.259
2600	1363	352	0.258
2700	1416	368	0.260
2800	1463	380	0.260
2900	1519	397	0.261
3000	1568	406	0.259

TABLE 3. AVERAGE PROBABILITY ERROR RATE

Protocol	Photon (N_{tot})	Probability
BB84	3000	0.263
B92	3000	0.214
BBM92	3000	0.259

Table 3 shows the average probability error rate of BB84 protocol, B92 protocol, and BBM92 protocol. According to simulation results, the B92 protocol is the lowest probability key error than BB84 and BBM92 protocols. It is also illustrated in Fig. 10.

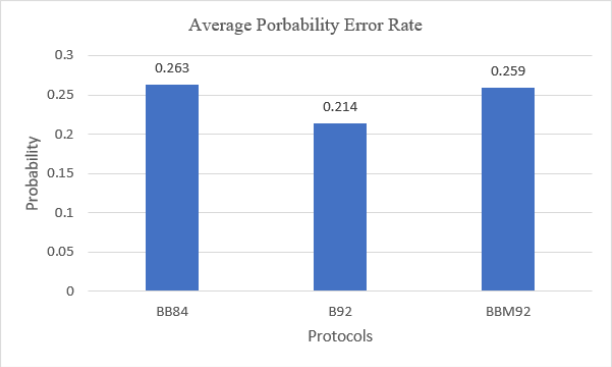

Fig. 10. Average Probability Error Rate of (BB84, B92, BBM92)

V. CONCLUSION AND FUTURE WORK

In this paper, we compared the probability key error between BB84 protocol, B92 protocol, and BBM2 protocol by using the QKD simulation software QuVis. The results show that the B92 protocol is the lowest probability key error than the BB84 protocol and BBM92 protocol. BB84 is the highest probability key error than the other two protocols. According to our experimental results, the B92 protocol is more relevant in detecting eavesdropping in lower error rates than the other two protocols.

In the future research, the experiment can be done by using a large number of photons and compare probability key error for another protocols in quantum key distribution.

REFERENCES

[1] N. Gisin, G.Ribordy, W.Tittel, and H. Zbinden, "Quantum Cryptography', Rev. Mod. Phys. 74 (1), 145 {190 (2002)}.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.

[3] A. Kohnle and A. Rizzoli, "Interactive simulations for quantum key distribution", European Journal of Physics, vol. 38, no. 3, 2017.

[4] M. I. Khan and M. Sher, "Protocols for secure quantum transmission: a review of recent developments," Pakistan Journal of Information and Technology, vol. 2, pp. 265-276, 2003.

[5] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty, and Abdel-Badeeh M.Salem, "Quantum Key Distribution: Simulation and Characterizations", International Conference on Communication, Management and Information Technology (ICCMIT 2015) 701-710.

[6] Manish Kalra and Ramesh C. Poonia (2018) Simulation of BB84 and proposed protocol for quantum key distribution, Journal of Statistics and Management Systems, 21:1, 661-666.

[7] Beatrix Rambu Hada Nuhamara and Nana Rachmana Syambas, "An Evaluation Of Quantum Key Distribution In QuVis Simulation Software", (2018) IEEE.

[8] Alekha Parimal Bhatt and Anand Sharma, "Quantum Cryptography for Internet of Things Security", Journal of Electronic Science and Technology, vol 17, No. 3, September 2019.

[9] J. –Y Wang et al., "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution", Nature Photon. 7 (5), 387{393 (2013).

[10] R.Etengu, F.M. Abbou, H.Y. Wong, A.Abid, N.Nortiza and A. Setharaman, " Performance comparison of BB84 and B92 Satellite-Based Free Space Quantum Optical Communication Systems in the

Presence of Channel Effects", Journal of Optical Communications, vol. 32, no. 1, pp. 37-47, 2011.

[11] Mart Haitjema, "A Survey of the Prominent Quantum Key Distribution Protocols", available online at http://www.cse.wustl.edu/~jain/cse571-07/index.html.

[12] Chris Erven, "On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source", University of Waterloo, Ontario, Canada, April 2007.

[13] Singh, H., Gupta, D., & Singh, A. (2014). Quantum key distribution protocols: a review. *IOSR Journal of Computer Engineering (IOSRJCE)*, 16.

[14] A. I. Nurhadi and N. R. Syambas, "Quantum Key Distribution (QKD) Protocols: A Survey," 2018 4th International Conference on Wireless and Telematics (ICWT), Nusa Dua, 2018, pp. 1-5, doi: 10.1109/ICWT.2018.8527822.