Polytechnic Journal. 2020. 10(1): 88-92
ISSN: 2313-5727
http://journals.epu.edu.iq/index.php/polytechnic

POLYTECHNIC JOURNAL

RESEARCH ARTICLE

Intercept-Resend Attack on SARG04 Protocol: An Extended Work

Ali H. Yousif*, Omar S. Mustafa, Dana F. Abdulqadir, Farah S. Khoshaba

Department of Information System Engineering, Erbil Technical Engineering College, Erbil Polytechnic University, Erbil, Kurdistan Region, Iraq

***Correspondence author:**
Ali H. Yousif,
Department of Information System Engineering,
Erbil Technical Engineering College, Erbil Polytechnic University, Erbil, Kurdistan Region, Iraq,
E-mail: ali.yousif@epu.edu.iq

Received: 28 October 2019
Accepted: 05 February 2020
Published: 30 June 2020

DOI
10.25156/ptj.v10n1y2020.pp88-92

ABSTRACT

In this paper, intercept/resend eavesdropper attack over SARG04 quantum key distribution protocol is investigated by bounding the information of an eavesdropper; then, the attack has been analyzed. In 2019, simulation and enhancement of the performance of SARG04 protocol have been done by the same research group in terms of error correction stage using multiparity rather than single parity (Omar, 2019). The probability of detecting the case in the random secret key by eavesdropper is estimated. The results of intercept/resend eavesdropper attack proved that the attack has a significant impact on the operation of the SARG04 protocol in terms of the final key length.

Keywords: Eavesdropper; Intercept-resend; IR; Quantum; SARG04

INTRODUCTION

Nowadays, the information security is the most important concern of people and entity. One of the main issues of practical quantum communication is the information security under the impact of disturbances or quantum noise. Cryptography is essential for secure communication in the digital era which is used to transfer the data from one party to another Anqi, 2018. First of all, from the sender side, the data are encrypted using a key, and then on the receiver side, the data are decrypted using the same or another key. The used key is the main part of the whole procedure. The key should be efficient to safe the data from any eavesdropper. However, the main issue of cryptography is the key distribution.

Quantum cryptography is used to implement the cryptographic system by implementing the concept of quantum mechanics. The quantum techniques are used to solve the key's issue of eavesdropping detection. The photons are used to communicate over the quantum channel. When eavesdropping occurs, the principles of quantum can be used to detect it. The state of the photon in quantum cryptography cannot be measured, and there is no error detected in photon transmission. The secret key can be exchanged at a distance depending on the principles of quantum mechanics. Quantum cryptography promises to revolutionize secure communication using the key distribution.

Quantum key distribution (QKD) enables two parties to establish a secure random secret key depending on the principles of quantum mechanics. The first proposed QKD is the BB84 protocol published by Bennett and Brassard in 1984 (BB84) (Bennett and Brassard, 1984). A new protocol introduced by Scarani et al. (2004) called SARG04 which is similar to BB84. Both protocols BB84 and SARG04 are sharing the same quantum state transmission phase and measurement phase. In addition, they use the same experimental measurement and the same four quantum states. The SARG04 protocol is the same at the level of quantum processing as the BB84 protocol; it differs only in the classical post-processing making it perfectly feasible to evaluate the experiment so far with the same data for SARG04 (Tobias, 2016). The SARG04 protocol provides almost identical security to BB84 in perfect single-photon implementations: If the quantum channel is of a given visibility (i.e., with losses), then the quantum bit error rate (QBER) of SARG04 is twice that of BB84 protocol and is more sensitive to losses (Hitesh et al., 2014). The SARG04 protocol in practice has a higher key rate than the BB84 protocol (Branciard et al., 2005).

In security studies, an investigation of the effect of collective rotation noise has been done on the security of the six-state QKD. The intercept-resend attack is approached on the quantum communication channel (Garapo et al., 2016). Another study found that the quantum error rate decreases when increasing the depolarizing parameter characterizing the noise of the channel after applying the disturbance effect of a depolarizing channel on the security of the QKD of the four-state BB84 protocol has been applied (Dehmani et al., 2012). Another paper presents a novel analytical model to investigate the eavesdropping attacks in wireless net of things; the results indicate that the probability of eavesdropping attacks heavily depends on the shadow fading effect, the path loss effect, Rayleigh fading effect, and the antenna models (Li et al., 2016).

Several attacks have to be applied against the QKD for security testing. We suppose that signals are transmitted and received between two honest parties of a quantum channel, and an eavesdropper can interact with the channel. One of the simplest strategies that eavesdropper follows is the intercept/resend attack (Hiroo and Ban, 2019). In intercept/resend attack, eavesdropper makes a strong projective measurement on the photon coming from the sender in an arbitrary basis and sends a new one to receiver, depending on the result eavesdropper obtains. The packets should be sent at random time to protect against the intercept-resend attack. On the other hand, the acceptable QBER must be under 25%. An eavesdropper could achieve an arbitrary low QBER by attacking just a fraction of the bits. Therefore, a non-zero QBER means that eavesdropper may have some information about the key.

THE PROPOSED MODEL OF KEY EXCHANGE

Estimate Intruder's Information

The intruder can apply the intercept/resend attack on the raw key to get the information. Therefore, both the sender and receiver should estimate the intruder information about the raw key. This information should be removed from the final key to prevent the intruder to get any information about it. Through the use of intercept-resend attack, the number of bits that are leaked to the intruder can be calculated as "(1)" (Jabbar and Ahmed, 2013):

$$W = N_s\left(\frac{4}{\sqrt{2}}\right) * QBER + 5\sqrt{N_s\left(4+2\sqrt{2}\right) * QBER} \tag{1}$$

Where *Ns* represent number of success pluses.

Strategies of Intercept-resend Attack on the SARG04 Protocol

In this attack, the eavesdropper intercepts the qubits coming from the sender. Eavesdropper does not have any knowledge about the basis used by the sender and receiver, so it chooses a random basis either to be rectilinear (+) ± or diagonal (X) H/V. The result is sent to the recipient, and eavesdropper listens to the public channel at the sifting stage. In case the sender wants to send "0", it will be encoded either ("V = 90" or "+ = 45") with equal probability. The eavesdropper independents on sender encoding, so it randomly selects one of the two bases (rectilinear or diagonal). The eavesdropper gets a correct result if it uses the rectilinear base, and the sent photon was encoded by vertical polarization (V), so erroneous result would not be created. Otherwise, the eavesdropper would get either a polarized photon at an angle of 45 or −45 (+ or −) with equal probability. The decision tree, "Figure 1," shows the scheme followed by an eavesdropper.

Intercept-resend Attack on SARG04

The significant difference caused by intercept-resend attack on the SARG04 protocol is the key length after the sifting stage. The value of key length is changed to 5/12 of raw key length. The probability of detecting cases is changed due to the changes caused by the intruder in the key which, in turn, will increases the probability of detecting cases from the sender.

All status has been represented for the "0" bit and all the probabilities that can be measured by the intruders and recipient for the "0" status, as shown in Table 1. Moreover, for status "1" bit, the probabilities are exactly identical the "0" bit status. For example, in the first column, the sender randomly sends a "0" bit using rectilinear (+) base, while the sender state is (↑). The intruder randomly used the same rectilinear (+) base, so the intruder's possible measurement will be (↑), which will be passed to the receiver. However, the receiver should use both rectilinear (+) and diagonal (X) basis to detect the bit state.

It is from Table 1 that:

The probability of detecting the case sent in column (1) is (P1 = 2/6 = 1/3) because two out of six cases are detected. However, the probability of detecting the case sent in column (2) is (P2 = 6 /12= 1/2) because six out of twelve cases are detected. In addition, the probability of detection in column (3) is (P3 = 1/3), and the probability of detection in column (4) is (P4 = 1/2).

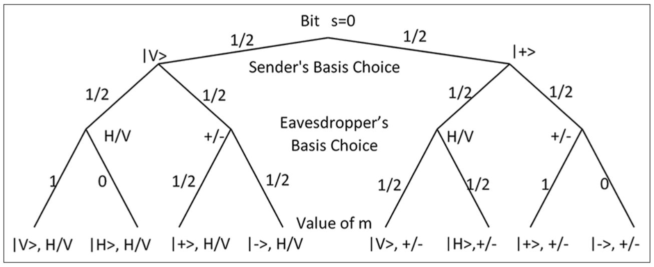
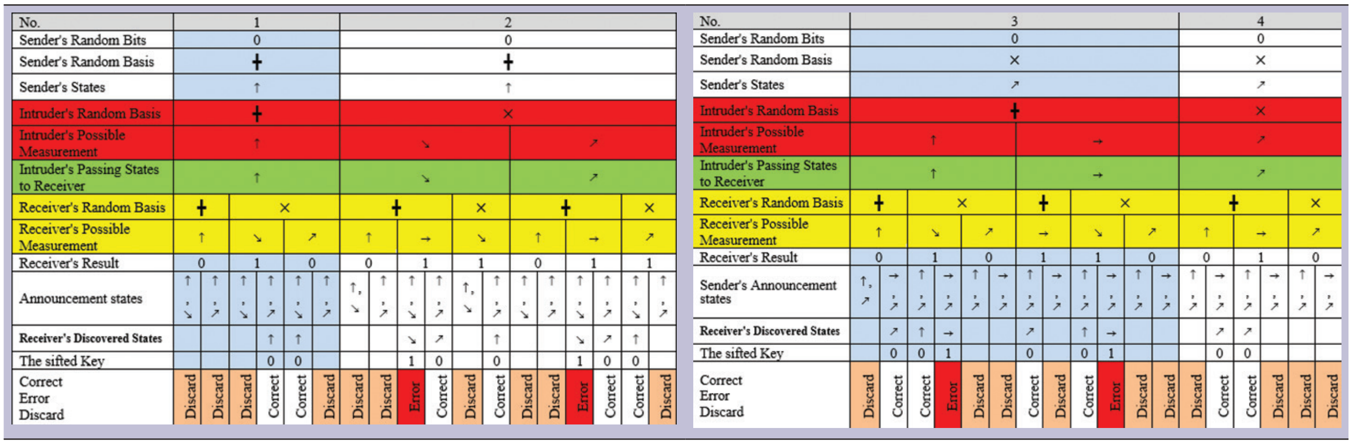


Figure 1: Decision tree for strategies of intercept-resend attack

Table 1: All cases where "0" in SARG04 can be sent and the process measured by the recipient after the apply intercept-resend attack



No.	1						2											
Sender's Random Bits	0						0											
Sender's Random Basis	+						+											
Sender's States	↑						↑											
Intruder's Random Basis	+						×											
Intruder's Possible Measurement	↑						↘						↗					
Intruder's Passing States to Receiver	↑						↘						↗					
Receiver's Random Basis	+		×				+				×		+				×	
Receiver's Possible Measurement	↑		↘		↗		↑		→		↘		↑		→		↗	
Receiver's Result	0		1		0		0		1		1		0		1		1	
Announcement states	↑, ↘	↑, ↗	↑, ↘	↑, ↗	↑, ↘	↑, ↗	↑, ↘	↑, ↗	↑, ↘	↑, ↗	↑, ↘	↑, ↗	↑, ↘	↑, ↗	↑, ↘	↑, ↗	↑, ↘	↑, ↗
Receiver's Discovered States				↑	↑				↘	↗		↑			↘	↗	↑	
The sifted Key				0	0				1	0		0			1	0	0	
Correct Error Discard	Discard	Discard	Discard	Correct	Correct	Discard	Discard	Discard	Error	Correct	Discard	Correct	Discard	Discard	Error	Correct	Correct	Discard

No.	3												4					
Sender's Random Bits	0												0					
Sender's Random Basis	×												×					
Sender's States	↗												↗					
Intruder's Random Basis	+												×					
Intruder's Possible Measurement	↑						→						↗					
Intruder's Passing States to Receiver	↑						→						↗					
Receiver's Random Basis	+		×				+		×				+				×	
Receiver's Possible Measurement	↑		↘		↗		→		↘		↗		↑		→		↗	
Receiver's Result	0		1		0		1		1		0		0		1		0	
Sender's Announcement states	↑, ↗	→, ↗	↑, ↗	→, ↗	↑, ↗	→, ↗	↑, ↗	→, ↗	↑, ↗	→, ↗	↑, ↗	→, ↗	↑, ↗	→, ↗	↑, ↗	→, ↗	↑, ↗	→, ↗
Receiver's Discovered States		↗	↑	→			↗		↑	→				↗	↗			
The sifted Key		0	0	1			0		0	1				0	0			
Correct Error Discard	Discard	Correct	Correct	Error	Discard	Discard	Correct	Discard	Correct	Error	Discard	Discard	Discard	Correct	Correct	Discard	Discard	Discard

So, the total probabilities of detecting the case "0" will be:

$$P\,total\ discover\ states\ intercept - resend = \frac{1}{4} * \left(P_1 + P_2 + P_3 + P_4\right)$$

$$= \frac{1}{4} * \left(\frac{1}{3} + \frac{1}{2} + \frac{1}{3} + \frac{1}{2}\right) \quad = \frac{1}{4} * \frac{5}{3} \quad = \frac{5}{12} \tag{2}$$

This means (5/3 = 1.67) cases can be detected out of four cases which indicate the possibility of disclosure of SARG04 protocol when applying an intercept-resend attack. The key length after the sifting process is 5/12 of the transmitted key length which is consider the maximum value of key after sifting. However, without intruders, the length of the key after the sifting process is 1/4 of the length of the transmitted key (Omar, 2019). In more precise, the key length is between (5/12 and 1/4) when the intercept-resend applied.

Photon Source

Two types of photon sources are used in the simulation program: The perfect single-photon source and weak coherence pulse WCP. Indeed, there is no perfect photon source in the real world. However, the WCP from the laser source is used widely spread. The out coming radiation is described by a single-mode coherent state:

$$p(n) = \frac{\mu^n}{n!} e^{-\mu} \tag{3}$$

This equation describes a Poisson distribution, where (μ) represents the mean photon number (Pulse Intensity) and (n) represent number of photons (0,1,…. n).

Figure 2 shows the probability of sending photons according to Poisson distribution and the number of photons. As shown in the figure, the probability of sending zero photon is very high, while the probability of sending a single photon is about 10%. However, the probability of sending two photons is <1% when the (μ =0.1). In the case of an increase in the number of photons (μ = 0.6), the probability of sending zero photon has decreased and became about 55% while the probability of sending a single photon has increased to 35%, whereas the probability of sending two photons or more has become about 10%.

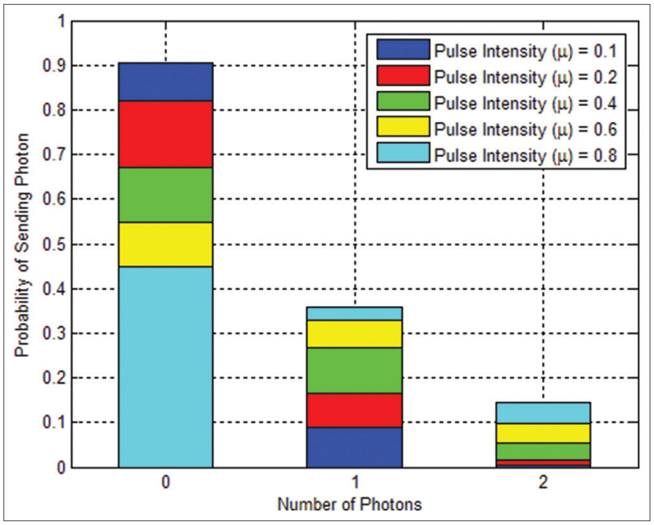


Figure 2: The relationship between the probability of sending photon and number of photons for different values of (μ)

SIMULATION AND RESULTS OF INTERCEPT-RESEND ATTACK ON SARG04

Simulation of Intercept-Resend Attack on SARG04

Visual Basic and MATLAB are used to build a simulation of SARG04 protocol and analyze the results. The intercept-resend attack programmed according to the following assumptions:

1. Two photons sources are used; the first generates single photons and the second generates a weak coherence pulse.
2. The attacker deals with the output of both sources based on a single entity and intercepts the pulses between the parties.
3. Intruders use one of the rules of measurement (V/H or 45°/135°); randomly, he/she also has the ability to generate the same pulse and then sends it to the other party.

Results of Intercept-Resend Attack on SARG04

The intercept-resend attack is applied to the SARG04 protocol where the key's length after sifting is between (5/12 and 1/4) of the total raw key length. The information gotten by eavesdropper is insignificant because there is no exchange of transmission basis between sender and receiver. The following results are obtained after implementing the attack:

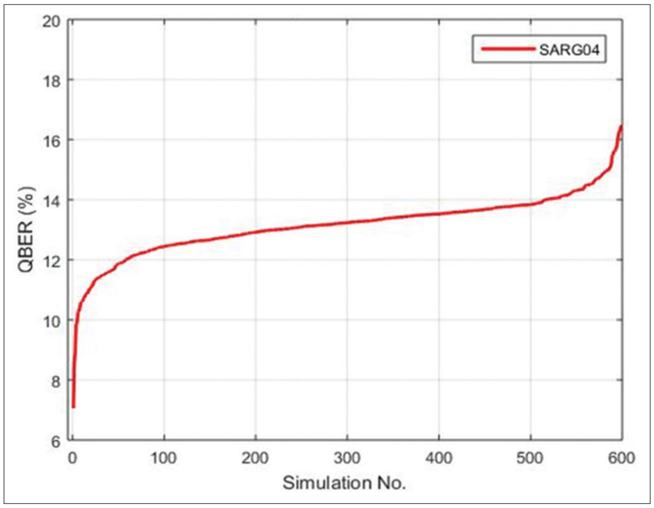


Figure 3: The relationship between QBER and the number of repeated simulation

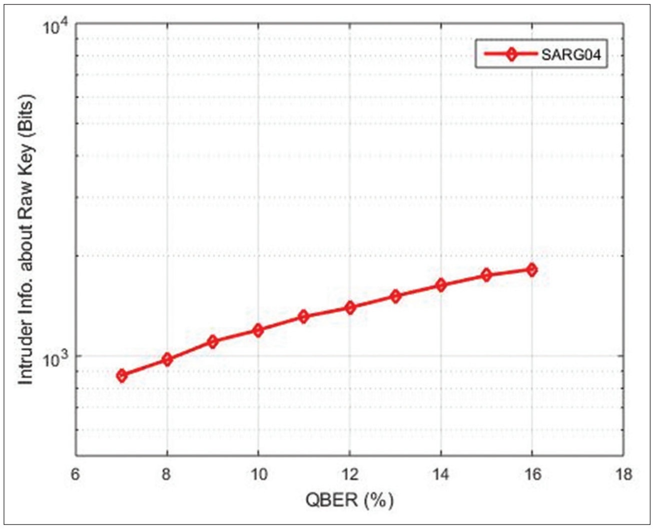


Figure 4: The relationship between the amount of obtained information by the intruder from the raw key and the QBER at *μ* = 0.1 in the case of the Intercept-resend attack

- Figure 3 shows the relationship between the QBER and the number of repeated simulation on SARG04 protocol in case of an Intercept-resend attack (Max. and Min. QBER in intercept-resend attack).
- Figure 4 shows the relationship between the amount of obtained information by the intruder from the raw key and the QBER at μ = 0.1 in the case of the intercept-resend attack.
- Figure 5 shows the ratio between the information obtained by the intruder to the raw key length when (μ = 0.1 and QBER = 16%).
- Figure 6 shows the relationship between final key length and QBER at values (μ = 0.1 and Raw Key = 10000 bits) during the intercept-resend attack.
- Figure 7 shows a bar of the final key for specific values of the raw key lengths when SARG04 protocol is attacked by the Intercept-resend at values (μ = 0.1 and QBER = 16.5%).

Finally, Table 2 shows the results of using the Stream ciphering for key expansion under intercept-resend attack

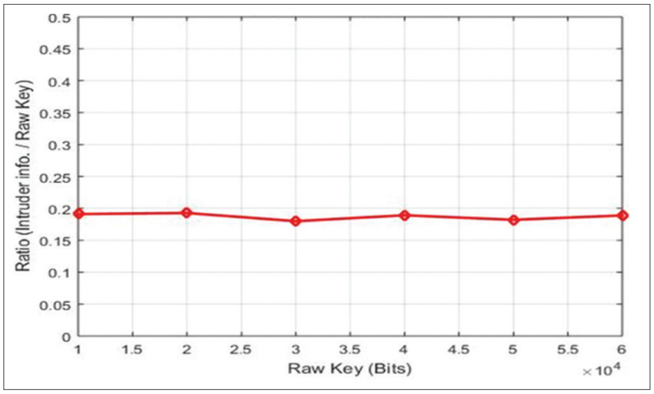


Figure 5: The ratio between the information obtained by the intruder to the raw key length when (*μ* = 0.1 and QBER = 16%)

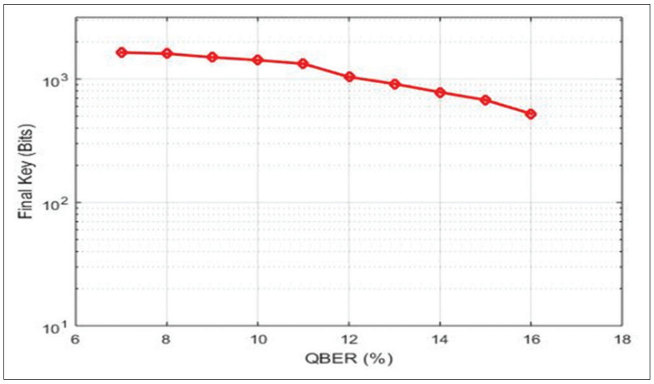


Figure 6: The relationship between final key length and QBER at values (*μ* = 0.1 and raw key = 10000 bits) during the intercept-resend attack

Table 2: The results of using the Stream ciphering for key expansion under intercept-resend attack

QBER (%)	Safety parameter (Bits)	Number of sent photons (Raw Key)	Sifted key length (Bits)	Key length after error correction (Bits)	Key length after privacy Amplification (Bits)	Key length after stream cipher Expanding (Bits)	Intruder's info. about raw key (Bits)
11.48	160	10,000	3379	2595	729	4374	1706
12.32	175	10,000	3456	2645	637	3822	1833
13.01	185	10,000	3374	2651	600	3600	1866
14.71	207	10,000	3408	2627	357	2142	2063
15.69	222	10,000	3435	2640	234	1404	2184
16.73	245	10,000	3522	2739	147	882	2347

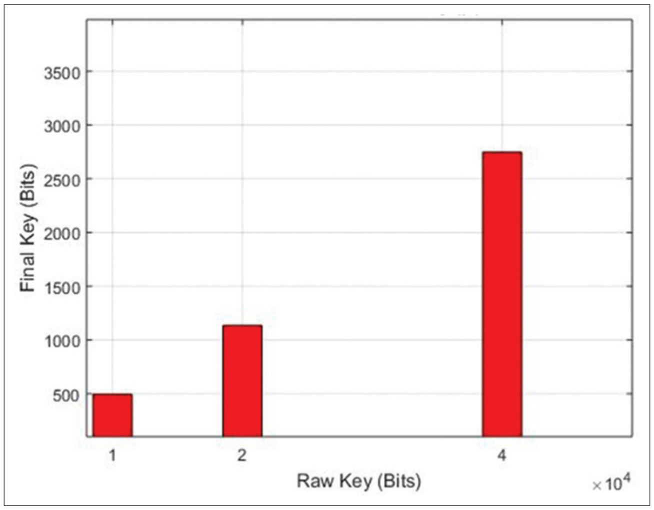


Figure 7: A bar of the final key for specific values of the raw key lengths when SARG04 protocol is attacked by the intercept-resend at values (μ = 0.1 and QBER = 16.5%)

CONCLUSION

The intercept-resend attack is more effective in terms of the information amount that will be subtracted from raw key length. On the other hand, it causes a lot of errors that affect the key and making the detection process much easier than the rest of other types. We investigate the security against the intercept/resend attack and the total probabilities of detecting one case "0" or "1" will equal to 5/12. The key length after the sifting process is 5/12 of the transmitted key length, which is represented the maximum value that the key can reach after sifting. In more precise, the key length is between (5/12 and 1/4) when the intercept-resend is applied.

REFERENCES

Anqi, H. 2018. Quantum Hacking in the Age of Measurement Device-Independent Quantum Cryptography. PhD Thesis, UWSpace.

Bennett, C. H. and G. Brassard. 1984. Quantum Cryptography: Public Key Distribution and Coin Tossing. Vol. 1. Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing. p175-179.

Branciard, C., N. Gisin, B. Kraus and V. Scarani. 2005. Security of two quantum cryptography protocols using the same four qubit states. Phys. Rev. A. 72(3): 032301.

Dehmani, M., M. Errahmani and A. Benyoussef. 2012. Quantum key distribution with several intercept-resend attacks via a depolarizing channel. Phys. Script. 86: 015803.

Garapo, K., M. Mafu and F. Petruccione. 2016. Intercept-resend attack on six-state quantum key distribution over collective-rotation noise channels. Chin. Phys. B. 25: 070303.

Hiroo, A. and M. Ban. 2019. The intercept/resend attack and the delayedmeasurement attack on the quantum key distributionprotocol based on the pre and post-selection effect. Quantum Phys. 26: 07282v3.

Hitesh, S., D. L. Gupta and A. K Singh. 2014. Quantum key distribution protocols: A review. IOSR J. Comput. Eng. 16(2): 1-9.

Jabbar, I. A. and I. A. Ahmed. 2013. Proposed a new method for error correction using Multi-Parity instead of single parity in BB84 protocol under different types of attacks. Al-Rafidain Eng. 21: 34-52.

Li, X., H. Wang and Q. Zhao. 2016. An analytical study on eavesdropping attacks in wireless nets of things. Mob. Inf. Syst. 2016: 4313475.

Omar, S. M., A. H. Yousif and D. F. Abdulqadir. 2019. Improving error correction stage and expanding the final key using dynamic linear-feedback shift register in sarg04 protocol. Polytech. J. 9: 1-6.

Scarani, V., A. Acín, G. Ribordy and N. Gisin. 2004. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. 92: 057901.

Tobias, V. 2016. Mobile Free Space Quantum Key Distribution for Short Distance Secure Communication. Master Thesis.