RESEARCH ARTICLE

Photon-number Splitting Attack on SARG04 Protocol: An Extended Work

Dana F. Abdulqadir*, Omar S. Mustafa, Ali H. Yousef

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

***Corresponding author:**

Dana F. Abdulqadir,
Department of Information
System Engineering, Erbil
Technical Engineering
College, Erbil Polytechnic
University, Erbil, Kurdistan
Region – F.R. Iraq.
E-mail: dana.farhad@epu.
edu.iq

Received: 28 August 2019
Accepted: 16 January 2020
Published: 30 June 2020

DOI

10.25156/pj.v10n1y2020.pp157-162

ABSTRACT

Network protection, an essential interest has migrated within this area particularly with the development of hacking, the strategies, as well as the penetration of the most effective blanketed networks. It can be stated that all the methods and protocols applied failed to forestall the intruder's attacks, consequently many researches grew to favor quantum mechanics over create non-intrusive methods. Many scientists and researchers have introduced other cryptographic subjects in quantum computing which is known as quantum key distribution protocol. In this paper, which is an extension to our preceding work (Mustafa et al., 2019), the simulation of the overall performance of SARG04 protocol had been examined in opposition to the most time-honored attack: Photon-number splitting (PNS) assault in the quantum channel. The data received showed results that obtained high resistance against PNS attack, due to the method that was used in the sifting stage.

Keywords: Attack; Photon-number splitting; Quantum key distribution; Quantum; SARG04

INTRODUCTION

Quantum key distribution (QKD) technology had been established in providing security levels which are required to withstand the threats realizable by future computing technologies, including quantum computers (Banerjee et al., 2017). In practical QKD, weak coherent state is often used and the channel transmittance can be very small; therefore, the protocol could be totally insecure under the PNS attack (Wang, 2005). However, when using attenuated coherent states, the relatively high rate of multi-photon pulses introduces vulnerabilities that can be exploited by the PNS attack to break the quantum key. Some QKD protocols have been developed to be resistant to the PNS attack (Lizama-Pérez et al., 2014). BB84 protocol is often established in weakening coherent states in preparation states, which give a reasonable chance to be attacked by PNS. The SARG04 protocol is built when researchers noticed that using the four states of BB84 with a 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 (Singh et al., 2014). However, SARG04 protocol provides more security than BB84 in the presence of PNS attack, in both the secret key rate and distance the signal can be carried (limiting distance) (Haitjema, 2007).

Many papers have investigated this subject, for example: Proposed a new method for error correction using multiparity instead of single parity in BB84 protocol Under Different Types of Attacks (Jabbar and Ahmed, 2013). Their work presented a method to estimate parameters of the decoy state method based on one decoy state protocol for SARG04 (Ali et al., 2012). They developed a new QKD protocol, called ack-QKD, which is resistant to the PNS attack (Lizama-Pérez et al., 2014). They provide the exact relations between the secure key rate and the bit error rate in a six-state SARG04 protocol with single-photon, two-photon, three-photon, and four-photon sources (Yin et al., 2016). Proposed a novel QKD protocol that uses AES to expand an initial secret, allows to individually authenticate every qubit, with tags that are efficient to construct (Price et al., 2017). The photon-number splitting (PNS) attack is studied in a specialized QKD modeling and simulation framework with a detailed treatment of the PNS attack which was provided with emphasis on practical considerations and ideal and non-ideal variations of the PNS attack were studied to measure the eavesdropper's information gain on the QKD-generated secret key bits and examine the detectability of PNS attacks with respect to both quantum bit error rate and the decoy state protocol (Mailloux et al., 2016). The cryptographic robustness of QKD with phase-time coding against a PNS attack

is analyzed by guaranteed the line length up to which a secret key distribution to determine both the protocol itself and the efficiency of error correction in raw keys (Sinil'shchikov and Molotkov, 2019). Proposed a family of sifting-less quantum-key-distribution protocols which use reverse reconciliation, and are based on weak coherent pulses (WCPs) polarized along different directions and also the physical part of the protocol is identical to most experimental implementations of BB84 and SARG04 protocols and they differ only in classical communications and data processing (Grazioso and Grosshans, 2013). The performance analysis of SARG04 and KMB09 protocols was presented with respect to protocol efficiency, Quantum Bit Error Rate (QBER), and robustness against eavesdropping (Lopes and Sarwade, 2015).

The protocol performance was improved as indicated in our previous work (Mustafa et al., 2019). In this paper, PNS attack has been applied to see the extent of its impact on SARG04 protocol. The data received showed results that obtained high resistance against PNS attack, due to using multi-parity rather than single parity in error correction stage and extend the size of final key using dynamic linear-feedback shift register circuits.

THE PROPOSED MODEL OF KEY EXCHANGE

Estimate Intruder's Information

In the simulation program, two types of photon sources were used: The perfect single photon source and the weak coherence pulse WCP. Through the use of PNS attack, the number of bits that are leaked to the intruder can be calculated as in Eq. (1) (Jabbar and Ahmed, 2013):

$$W = N_s \mu + 5\sqrt{N_s \mu(1-\mu)} \quad (1)$$

Where μ represents the pulse intensity (Number of photons in pluses) and N_s represents the number of success pluses (key length after sifting stage).

The μ is consider as (if condition) because the μ determine the pulse intensity of photon source.

Indeed, there is no perfect photon source in real world. However, the WCP from laser source is used widely spread. The out coming radiation is described by a single mode coherent state:

$$P(n) = \frac{\mu^n}{n!} e^{-\mu} \quad (2)$$

This equation describes a Poissonian distribution where (μ) represents the mean photon number (Pulse Intensity) and (n) represent number of photons (0, 1, 2, ..., n). Figure 1 shows the probability of sending photons

Figure 1: The relationship between the probability of sending photon and number of photons for different values of (μ)

according to Poissonian 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 ($\mu = 0.1$). In the case of an increasing in the number of photons ($\mu = 0.6$), 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%.

PNS Attack on SARG04 Protocol

Let's assume, the sender was sending pulses containing more than one photon according to Table 1. In this protocol, there is no exchange of basis, the sender does not reveal the basis but the pairs of non-orthogonal signal states in ways were one of these states becomes one of the ones being sent. The receiver can have a higher probability of predicting small parts once a discovered state orthogonal is found to one of two declared non-orthogonal states. This scenario shows that the intruder does not know which of the cases he has perfectly detected between two non-orthogonal states, because there is no exchange of basis in this protocol. Furthermore, the intruder does not know the basis that the recipient used to measure his states, which can be used by intruder to guess the key. In each state detected by the recipient will remain anonymous for the intruder and will be in two possibilities, for example, ($\uparrow$ and $\searrow$), meaning that there is no disclosure of any state in this protocol. It is worth mentioning that the sender also does not know the basis discovered by the recipient whether it is detected correctly or not, until the stage of errors correction.

Table 1: An implemented example of the PNS attack on SARG04 protocol for quantum states that sent between two parties (all pulses containing more than one photon)

The bits	1	2	3	4	5	6	7	8	9	10
Sender's Random Bits	1	0	0	0	1	0	1	0	0	1
Sender's Random Basis	+	+	x	+	x	x	x	+	+	+
Sender's States	→→	↑↑	↗↗	↑↑	↘↘	↗↗	↘↘	↑↑	↑↑	→→
Intruder's Random Basis (sniff off one photon and let the other pass)	+	x	x	+	x	+	+	x	+	x
Intruder's measurement Result	→	↗	↗	↑	↘	→	→	↗	↑	↘
Receiver's Random Basis	+	x	x	x	+	x	+	+	x	x
Receiver's measurement Result	→	↗	↗	↘	→	↗	→	↑	↗	↗
Sifting stage										
Sender's Announcement sets	→↗	↑	→	↑	→	→	↑	↑	↑	↘
Receiver's Discovered States. then announcing it to Sender		✓					✓		✓	✓
Receiver's new states after Discovering		↑					↘		↑	→
Intruder's will apply	x	?	x	x	x		?	x	?	?
Remaining key after sifting										
Sender's Key		↑					↘		↑	→
Receiver's Key		↑					↘		↑	→
Intruder's Key		Guessing				Guessing			Guessing	Guessing

Flowchart 1: The quantum stages in proposed model

SIMULATION RESULTS

- Visual Basic and MATLAB are used to build a simulation of SARG04 protocol and analyze the results, to validate the proposed algorithm, it is required first to simulate the protocol SARG04, which is simulated according to the following Flowcharts 1-6:

The encoding is done using the following algorithm:

If Evasdrop = "PNS" Then

 If Len(Qubit_StateB) > 2 Then

 Polarazation_Type = Mid(Qubit_StateB, 1, 1)

 Select Case Polarazation_Type

 Case "X"

Flowchart 2: The steps of receiving quantum states in detail

Qubit_StateB = Mid(Qubit_StateB, 2, Len(Qubit_StateB) - 1)

 Case "H"

Qubit_StateB = Mid(Qubit_StateB, 2, Len(Qubit_StateB) - 1)

 Case "V"

Qubit_StateB = Mid(Qubit_StateB, 2, Len(Qubit_StateB) - 1)

 Case "Z"

 Qubit_StateB = Mid(Qubit_StateB, 2,
 Len(Qubit_StateB) - 1)

 End Select

End If

End If

The simulation of PNS attack on SARG04 protocol is simulated according to the following assumptions:

- Using two photons sources (single photons and weak coherence pulse).

Flowchart 3: Represents sending the basis that used to measure the sent stats

Flowchart 4: How to check the basis that used in the measurement

Flowchart 5: The sifting stage

Flowchart 6: How to encoding the quantum stats to equivalent bits

Figure 2: The GUI of SARG04 simulator under PNS attack ($\mu = 0.1$)

Figure 3: The relationship between the pulse intensity and the intruder information about the raw key

Figure 4: The ratio between raw key and intruder information in PNS attack when ($\mu = 0.1$, QBER = 0%)

Table 2: The implementation results of SARG04 protocol under PNS attack (Raw key = 10,000 bits, $\mu = (0.1, 0.2, 0.4, 0.6, \text{ and } 0.8)$) with stream cipher

QBER (%)	Safety Parameter (Bits)	No. 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 Info. About Raw key (Bits)
Pulse Intensity = 0.1							
0	0	10000	2424	2231	1915	28725	316
0	0	10000	2441	2246	1928	28920	318
0	0	10000	2459	2263	1943	29145	320
0	0	10000	2434	2240	1923	28845	317
Pulse Intensity = 0.2							
0	0	10000	2418	2223	1642	24630	581
0.5	6	10000	2512	2296	1688	25320	602
0.51	6	10000	2484	2282	1680	25200	596
1.52	18	10000	2478	2280	1667	25005	595
Pulse Intensity = 0.4							
0	0	10000	2466	2264	1156	17340	1108
0.51	6	10000	2464	2264	1151	17265	1107
0.52	6	10000	2420	2227	1133	16995	1088
1.47	18	10000	2552	2348	1186	17790	1144
Pulse Intensity = 0.6							
0	0	10000	2512	2310	681	10215	1629
0.49	6	10000	2575	2369	694	10410	1669
0.5	6	10000	2523	2319	677	10155	1636
2.45	31	10000	2559	2355	665	9975	1659
Pulse Intensity = 0.8							
0	0	10000	2569	2364	208	3120	2156
0.49	6	10000	2586	2345	169	2535	2170
1.51	18	10000	2491	2281	171	2565	2092
2.42	31	10000	2598	2376	165	2475	2180
6.4	80	10000	2548	2328	109	981	2139

Figure 5: The relationship between raw key and key length after sifting stage in PNS attack when ($\mu = 0.1$, QBER = 0%)

- The WCP may contains (No photon, single photon, and more than one photon) and the WCP use Poissonian distribution to generate pulses.
 - The intruder should apply the following steps for each pules coming from the sender's:

Figure 6: The sifted key length in comparison with Raw Key when ($\mu = 0.1$, QBER = 0%)

- All pulses that contain zero photon will be ignored.
- All pulses that contain multi-photons it will attacked by taking one photon and pass the other to the receiver.
- The pulses that contain one photon it will pass without attack.

Figure 7: The relationship between length of Final Key with the length of sifted key after sifting stage in PNS attack

Figure 8: The effect of raw key size on intruder info under PNS attack when ($\mu = 0.1$, QBER = 0%)

- The following results are obtained after implementing the attack:

Figure 2 shows the implementation of PNS attack on SARG04 protocol. It is noted from the figure that the QBER = 0 because in SARG04 protocol intrusion is not detected, while making the information of the intruder useless, and this is done during the sifting stage [Table 2].

Figure 3 shows the effect of changing pulse intensity on the amount of intruder information when applying the PNS attack on SARG04 protocol and note that the values of SARG04 protocol are always lower due to the difference in key length after sifting stage as shown in Figures 4-8.

CONCLUSION

Overall, in this paper, it has come to conclusion that the PNS attack should not be taken lightly, because the sender and receiver failed to expose any errors. Intruders will significantly fail to smear an attack with pulses being no more than one photon even, especially if they use perfect single photon sources.

Furthermore, this paper establishes that the PNS attack has less impact on SARG04 protocol, because it does not affect

the state of hacked pulses which cannot be perceived by sender and receiver. Therefore, this attack is dangerous if all the pulses contain more than one photon while it could be the least dangerous in the case of a single photon source, due to the impartiality of applying this attack on the pulses. Since the source comprehends the photons that are applied are not 100% ideal (if omitting pulses, the number of photons is not as ideal according to Poissonian distribution) as a result of the pulses comprising of a single photon in addition to others containing more than one photon.

REFERENCES

- Ali, S., S. Mohammed, M. S. H. Chowdhury. and A. A. Hasan. 2012. Practical SARG04 quantum key distribution. *Optic. Quant. Electron.* 44(10-11): 471-482.
- Banerjee, A., A. Prabhakar. and R. M. Mathias. 2017. Quantum key distribution-technology review. *Defcom India J. Def. Inform. Commun. Technol.* 3(1): 1-13.
- Grazioso, F. and F. Grosshans. 2013. Photon-number-splitting-attack Resistant Quantum Key Distribution Protocols Without Sifting. *arXiv Preprint arXiv:1306.6061*. Cornell University, United States.
- Haitjema, M. 2007. A survey of the Prominent Quantum Key Distribution Protocols. Available from: <https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum.Mart> Haitjema, mart.haitjema@wustl.edu.
- Jabbar, A. I. A. and Ahmed, I.A. 2013. Applying multi-parity code to the quantum security protocol BB84 under different types of attacks-ENG. *AL Rafdain Eng. J.* 21(5): 34-53.
- Lizama-Pérez, L., J. López, D. Carlos-López. and S. Venegas-Andraca. 2014. Quantum flows for secret key distribution in the presence of the photon number splitting attack. *Entropy.* 16(6): 3121-3135.
- Lopes, M. and N. Sarwade. 2015. On the performance of quantum cryptographic protocols SARG04 and KMB09. In: 2015 International Conference on Communication, Information and Computing Technology (ICCICT). IEEE, United States. p1-6.
- Mailloux, L. O., D. D. Hodson, M. R. Grimaila, R. D. Engle, C. V. McLaughlin. and G. B. Baumgartner. 2016. Using modeling and simulation to study photon number splitting attacks. *IEEE Access.* 4: 2188-2197.
- Mustafa, O., A. Yousif. and D. Abdulqadir. 2019. Improving error correction stage and expanding the final key using dynamic linear-feedback shift register in sarg04 protocol. *Polytech. J.* 9(1): 1-6.
- Price, B. A., G. J. Rarity. and C. Erven. 2017. Quantum Key Distribution Without Sifting. 7th International Conference in Quantum Cryptography (QCRYPT), Cambridge, UK.
- Singh, H., D. L. Gupta. and A. K. Singh. 2014. Quantum key distribution protocols: A review. *J. Comput. Eng.* 16(2): 1-9.
- Siniil'shchikov, I. V. and S. N. Molotkov. 2019. Decoy states and low-density parity-check error-correcting codes in quantum cryptography with phase-time coding. *J. Exp. Theor. Phys.* 129(2): 168-196.
- Wang, X. B. 2005. Beating the PNS Attack in Practical QKD. Cornell University, New York.
- Yin, H. L., Y. Fu, Y. Mao. and Z. B. Chen. 2016. Security of quantum key distribution with multiphoton components. *Sci. Rep.* 6: 29482.