SCITECH
RESEARCH ORGANISATION|
Volume 4, Issue 3
October 12, 2015

Journal of Information Sciences and Computing Technologies
www.scitecresearch.com/journals

Improving BB84 in Quantum Encryption

Elaheh Golzardi
Department of Electrical and Electronic Engineering, Kurdistan PNU, Iran

Abstract.

Today, information security plays a key role in communications and exchanges.Until now Various approaches including: Quantum encryption and Quantum key Distribution (QKD), have been utilized for information security, that act based on Quantum Mechanic principles, so that if one tries to hear the information, it will be detected via increasing error rate in receiver part.

BB84 is one of secure algorithms in quantum encryption area, bearing less error rate in comparison to other quantum algorithms. The goal of the paper is to improve the algorithms as much as possible in order to defend the attacks. We use a hybrid key to accomplish the task in which we add authentication and time limit beside the QKD key.

Keywords: Quantum Cryptography (QC); Quantum Key Distribution (QKD); Hybrid Key.

1. Introduction

Numerous approaches have been developed for data encryption in order to generate a safe connection. Main challenge of the secure connections is generating the best data encryption via various algorithms introduced in the area.

BB84 algorithm has better error vulnerability feature than others. This is one of the QKD protocols proposed by Bennett and Brassard in 1984, although it has less error rate than other quantum algorithm, it suffers from attacks such as MITM،PNS etc. Thus this paper proposes an algorithm to defend such attacks, particularly MITM, as much as possible.

2. Related Works

Encryption originated through Wister`s work, in which he proposed unit quantum states for forged paper money and published his idea in 1983. Bennett and Brassard used unit quantum for data storing and they succeed to use them for data transmission and the first quantum encryption called BB84 registered in 1984 [2].

Quantum encryption theory advanced more in 1991, when it was proposed that two-particle state can be used in quantum encryption and it`s security was based on Bell inequality. Bent et al. 1991 approved that that quantum key potential distribution has applied distribution and it is accomplished by creating an initial system via polarizing the photons. Bennett and Brassard published BB84 in 1992 through which proposed that the protocol can be used via individual photon connection and with photon distribution for long distances in optical fibers [1].

After introduction of first encryption protocol, key distribution system which was based on optical photon polarization could transfer information in a distance about 30 cm [13].

Since then, data transfer`s distance increased in favor of optical fiber and many examinations carried on various key distribution instruments based on optical fiber transmission. The result of the researches was increasing transmission

distance to 24 km then it increased up to 48 km by developing the researches. Since then, many approaches proposed to increase transmission distance, currently transmission distance exceeds 100 km [19].

Researchers of the paper investigated the effect of polarized quantum channels on quantum encryption protocols BB84&SARG04 and the results are presented here [6].

A new approach was proposed for parameter selection via main elements analysis [5].

Researchers of the paper developed an approach to generate key using biometric developed (the images). The key generation is one of face characteristics, and limitation of key production process in this research, is a complex & long process one, although secure [14].

In this paper, researchers developed a new approach, based on the sessions, to generate key [18].

Since then, quantum key distribution was introduced and they developed basis of secure channels based on quantum key distribution sets, the goal of these experiments was to indicate plausible imaginations of quantum key distribution and achieving quantum encryption applications. Thus, it is expected that the experiment improve quantum key distribution states [8].

The concept of symmetric key distribution is a controversial issue in data encryption area. Many algorithms have been proposed of which, quantum encryption known as quantum key distribution, can detect Eve or attacker. An unconditional security is established in BB84 protocol, but it`s vulnerable to MITM attack, thus a solution is proposed to oppose it. In the proposed approach, calculation algorithms are used to cope with the attack. Indeed a key selection algorithm selected then both were mixed and they were introduced as hybrid key [17].

The paper deals with an efficient Key Distribution Technique based on Quantum Mechanics. The concept of Heisenberg's Uncertainty Principle and quantum indeterminacy property are used to detect the presence of eavesdropper and secure the process of Key Distribution [3].

In another paper it`s proposed enhancing the performance of the privacy amplification phaseby introducing message digests (MD) hash functions combined with truly random functions. The resulting Hash-Mod and Hash- Div functions are used to compress reconciled keys resulting from the error correction phase . Experiments were conducted using three different simulators to assess the performance of these combined functions using entropy and information measures [12].

3. Simulation

3.1.Quantum Key Distribution (QKD)

Due to specific capabilities and thing-oriented characteristics of JAVA in comparison to the other languages, we used JAVA for simulation and proposed algorithm experiment. The language comprises packages, classes and security relations which can be used for transmission and key generate. The algorithm comprises three parts, thus the simulation carried based on three components: Alice, Bob and Eve.

- Operators Description

We use following operators for simulation:

" + & x" present base operators and " | , - , / & \" indicate four directions. At the end the results presented binary.

Transmitter (Alice) using photon production source, transmits photons with one of four states: 0˚ (equals binary zero), 45˚ (equals binary zero), 90˚ (equals binary one) 135˚ (equals binary one) to receiver (Bob). However, a receiver instrument is used to measure polarization. Transmitter of the protocol transmits the photons in one of polarized states randomly.

Receiver (Bob) utilizes particular filters for measuring received photons randomly. The filters, called polarization bases, are either diagonal or rectilinear. Each polarization base composed of two polarization bases i.e. rectilinear base includes 0˚ and 90˚ of polarization states, diagonal base includes 45˚ and 135˚ of polarization states. According

to quantum mechanics, if polarization is horizontal or vertical, measurement of vertical/horizontal bases results in a correct horizontal/vertical angle.

But measurement of diagonal bases results in vertical or horizontal one randomly. After measurement, polarization state with measured state and all information of primary polarization will be eliminated [4].

3.2. Using Digital Signature to Generate Key

Using digital signature via abstracter function has numerous advantages as follow:

1) Converting individual input into an output with fixed length.
2) One directional.
3) Defending Incidences, etc.

The characteristics cause message integrity, increases efficiency and the speed of signed plans consequently, increases the security. Due to it`s higher security, we adapted the technology to generate identifying key and finally hybrid key.

- One-Time Signature

Digital signature has various categories including: Blind signature, Undeniable signature and etc; from which the users, based on their conditions, should choose one of them for their identity authorization.

In this paper, one-time signature is used to improve quantum encryption and the reason is it`s approvable security. However, we should generate a general key on every transmission; meaning that this category is used for more than one signature and it increases security significantly.

4. Proposed Theory Description

1) Generate Basic and values

Alice encrypts her selected Bit via random selection basis (rectilinear/ diagonal) and generates polarized photon, then transmits it to Bob via quantum channel, finally stores the combination of basis and values in the memory. Bob measures polarized photon in one of the two set basis (rectilinear/diagonal)

- If Bob selects the very Alice`s basis, the result will be true, unless the result is random.

2) Comparison

- Bob will be verified via Alice public key and classic channel, then he replies Alice whether his basis are encrypted ones, or not.

- Alice will be verified via Bob public key and classic channel, then he replies Bob whether his basis are encrypted ones, or not.

- Both compare the basis and keep values used with similar basis then removes remaining Bits.

3) Transfer Challenge

Alice encrypts the message and sends it to Bob.

Bob decrypts the message with his private key then, re-encrypts the message and sends back to Alice. Alice will investigate both of them to see whether they are same. If yes, she continues the message transmit, unless nothing.

4) Generate Identification Key

Alice & Bob generate their signatures and contact with each other through authentication.

Here, Alice & Bob can share the signature before / after quantum key generate.

- One-Time Signature

Due to approvable security, this category is used to generate key.

5) Generate Hybrid key

Both keys (QKD, signature key) repeat until their length becomes equal i.e. desired length. Final key will be generated via XOR operation.

- Implementing Time Limitation

One can implement time limitation on 4 or 5 stage, i.e. should key generation and transmission lasts more than allocated time, the process will resumes.

6) *Encryption & Decryption*

Alice encrypts the message via Bob`s public key and retransmits it to Bob. Bob can decryption the message via his private key.

5. Comparison and Evaluation

We compared proposed algorithms with BB84 then we concluded that:

- In proposed approach, in comparison to BB84, the number of basis transfer decreases below the half.
- The number of retransmit chances increases in comparison to BB84
- If the number of transmitted photons increases, it will cause hears with higher probability. Thus attacker power and/or channel noise increases, detection probability increases proportionally.
- Proposed approach has higher flexibility as it uses particular signature each time and this is due to one-time signature characteristics, i.e. each time, key generation accomplished by unique signature, and it`s regular replacement increases system security.
- The results prove that proposed approach is safer than old encryption ones.

6. Conclusion

Eve can get QKD key in most of present attacks such as MITM, PNS (photon number splitting), Intercept-Resend, thus we proposed the algorithm in order to increase security and to decrease penetrability probability. The proposed algorithm comprises a hybrid key plus time constraint probability in which QKD key combines with combined digital key in hybrid operation. Thus Eve can decrypt the messages if he gets QKD key, since he isn`t informed about conditional contract between the parties and identification key.

Providing the fact that Eve doesn't know about the conditional contract, we succeed, using the system, to address identification authentication. Designing the algorithm increased attacks` defend capability, however, it helped key distribution process for a reliable & trustable connection between transmitter and receiver.

7. References

[1] Bennet, C, Bessette, F, Brassard, G, Salvail, L, Smolin, J (1992). Experimental quantum Cryptography. Journal of cryptography.

[2] Bennet, C, Brassard, G (1992). Quantum cryptography.*IEEE. International Conference on computer. System and processing*. Bangalore. India. N.Y, p175.

[3] Chetty, N.V, Abhijith, B,Nihar, G, Raj Vincent P.M.D (2013). Modified Novel Quantum Key Exchange using BB84 Algorithm.*International Journal of Engineering and Technology*. 5(3)2451-2454.

[4] Elliot, C, Pearson, D (2003). Quantum Cryptography in Practice.*IEEE*.vol. 91, NO.6, PP 35-40.

[5] Fengxi, S,Zhongwei, G,Dayong, M (2010). Feature Selection Using Principal Component Analysis.*ICSEM*. 1: 27-30.

[6] Jeong, Y (2010). Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols. *Department of Physics, Pohang University of Science and Technology (POSTECH)*. 790-784, Korea. February 11.

[7] Kai-zhi, Y, Ying-lei, C, Liu, J (2011). A method for extracting the text feature of SAR image based on co-occurrence matrix.*4th International Congress on Image and Signal Processing (CISP),*Telecommun. Eng. Inst., Air Force Eng. Univ., Xi'an, China, 4: 2038-2043.

[8] Kartheek, D.N,Kumar, O.P,Srujan, S (2012). Security Using BB84 Quantum Key Distribution Protocols. *IJARCSSE All Rights Reserved.*

[9] Katz, J (2010). Digital Signatures.*1st ed, 2nd Printing*, pp. 3-33 & 87-119.

[10] Kollmitzer, C,Pivk, M (2010). Applied Quantum Cryptography. *Springer*.

[11] Lifang, W, Xingsheng, L, Songlong, Y, Peng, X (2010). A novel key generation cryptosystem based on face features. *IEEE 10th International Conference on Signal Processing*. pp. 1675-1678.

[12] Mahmoud Abbas, A,Goneid, A, El-KassasSh (2014).Privacy Amplification in Quantum Cryptography BB84 using Combined Univarsal2-Truly Random Hashing.*International Journal of Information and Network Security (IJINS).* 3(2)98-115.

[13] Marrand, P, Townsend, D (1995). Quantum key distribution over distance as long as 30km. vol. 20, no.15, pp. 1695-1697.

[14] Ogiela, M.R,Ogiela, L (2011). Image based cryptobiometric key generation. *Third International Conference on Intelligent Networking and Collaborative Systems (INCoS),* Sci. Technol, Krakow, Poland, pp. 673-678.

[15] Santhi, B,Ravichandran, K.S,Arun, A.P,Chakkarapani, L (2012). A Novel Cryptographic Key Generation Method Using Image Features.*Research Journal of Information Technology*, 4(2), pp. 88-92.

[16] Schildt, H (2007). The Complete Reference Java.*Seventh Edition, McGraw-Hill*.

[17] Shaikha, A. M, Shah, P. D (2012). BB84 and Identity Based Encryption (IBE) Based a Novel Symmetric Key Distribution Algorithm. *Elsevier journal*.

[18] Tanmay, B, Sirshendu, H,Ayan, M, BhadraChaudhuri S.R (2011). A novel data encryption technique by genetic crossover of robust biometric key and session based password.*International. J. Network Secur. Appl. (IJNSA).* 3(2), pp. 111-120.

[19] Ursin, R (2007). Entanglement-based quantum communication over 144km. *Nature Physics.* pp. 481-486.