The Goals of Parity Bits in Quantum Key Distribution System

Omer Abd Alkareem Jasim
Head of Computer Science department
Alma'arif University College – Iraq

Anas Ayad Abdulrazzaq
Deputy Head of Computer Science Department
Alma'arif University College - Iraq

ABSTRACT
The basic foundation behind cryptography as a discipline was to research how valuable data, information can be protected from unauthorized parties, such as adversaries. Quantum cryptography is one of the recent advancement occurred within that discipline. However, this cryptographic algorithm still at its early stages, where there is no wide implementation can be seen. Many research papers have been done to develop this algorithm, while others, to propose new implementations of this algorithm to tackle a specific problem.

This research paper studies and examines the relationship between the QKDS (Quantum Key Distribution System) and the parity bits. Hence, explore how the use of parity bits can improve the final resolved key.

Keywords
Quantum Cryptography, parity bits, BB84 protocol simulation, QKDS.

1. INTRODUCTION
From studying the history of cryptography, one can conclude that quantum cryptography is one of the recent approaches proposed to solve security issues related to data encryption in general, and secret key distribution in particular. And since this approach is still at its early stages, many researches and developments have been proposed and some had been implemented to improve it. The objective of this research paper is concentrated on studying the relation between the algorithm and the parity bits, then, conclude whether the use of it can improve the final resolved key. Thus, we proposed and developed a simulation software providing thorough simulation of how quantum algorithm works. Hence, results will be combined and a conclusion will be drawn. Moreover, the software offers different parameters to be configured and tuned, and photons transmission and results are visually available.

The paper will briefly explain the theoretical concepts behind the quantum cryptography, BB84 protocol and its phases. It also provide a tabulated information about the different simulated experiments are presented, results, and a conclusion based on these results will be made.

1. BACKGROUND

1.1 Quantum Cryptography
Quantum mechanics is a branch of physics describes basic phenomenons as related to multiple polarization state of a single photon [1]. As described by Muhammed and Nicolas, the foundation of quantum cryptography was based on the concepts of quantum mechanics. Such that, quantum bit can exists in four deferent states (horizontal, vertical, right and left diagonals polarization), quantum bit's state can't be measured (it will be detailed further), and quantum bit can't be duplicated (based on the quantum mechanics law known as the quantum "no-cloning" theorem) [1, 2]. Within the discipline of quantum cryptography, quantum bit is a unit of quantum information, and usually referred to as the qubit [5].

1.2 QKDS
Quantum cryptography suggests various possibilities which are beyond the abilities of classical cryptography. Arguably, the QKDS (Quantum Key Distribution System) [5]. The QKDS is merely used to negotiate secret quantum keys among parties (usually called Alice and Bob) through a communication channel, like fiber optics. QKDS came as an alternative to the existing "public/secret key distribution system". The QKDS solve(d) the well known problems existed within the current scheme [3]. Within the discipline of Quantum cryptography, the communication channel is known as Quantum Channel.

2. BB84 QUANTUM PROTOCOL
BB84 protocol describes the use of photon polarization states to transmit classical information over a quantum channel [1, 4]. Both sender and receiver sides must have devices that can generate and detect pulses of light in different polarization.

The first phase of BB84 protocol is quantum bits generation. Alice generates two random bits, A1 and A2. A1 selects the basis and A2 represents the polarization within that base (rectilinear or diagonal). Alice prepares a photon where its polarization state depends on both A1 and A2 and sends it over the quantum channel. Bob generates a random bit B3 and sets his polarization detector to that basis. He reads bit B4. Bob and Alice tell each other about B3 and A1 over a public and authenticated channel. If they agree, they add A2 and B4 to their bit sequence [6].

Table 1 depicts BB84 bits generation using | = \ = 1 and - = / = 0:

Table 1. The process of quantum bits generation

Actions	Photons, bases, and their states												
Alice randomly generates photons bases	+	X	+	+	X	X	+	+	X	X	+	+	X
Alice sends photons	|	/	|	-	/	\	|	-	\	\	-	|	/
Bob measures with	+	X	X	+	+	X	+	X	X	+	X	+	X
Bob's results	|	/	/	-	|	\	|	\	\	-	\	|	/
Valid data	|	/		-		\	|		\			|	/
Translated and added to their key sequences	1	0		0		1	1		1			1	0

***Note: X=diagonal base, += rectilinear base**
/ = right diagonal, \ = left diagonal
↑ = vertical state = 1, ← = horizontal stat = 0.

The strong privacy of the BB84 protocol stemmed from encoding the classical information in non-orthogonal states. Thus, the photon polarization state can't be measured without discarding or disturbing the original state (based on the quantum mechanics theorem: No-cloning) [2, 5].

Receiving bits sequences by both sides represents the end of this phase (i.e. bit transmission), and the starts of the second phase of BB84 protocol, see figure 1.

2.1 Raw Key Extraction (KE)

Raw key extraction step represents the start of the second phase of BB84 protocol. The main purpose of raw key extraction phase is to eliminate all possible errors occurred during bits discussion (generation and transmission) over quantum channel. Negotiated parties (i.e. sender and receiver) compare their filter types used for each photon; unmatched type of filter for any transmitted photon, the corresponded bit will be eliminated, otherwise, the bit will be considered [5, 6].

For BB84, sharing the type of filters used in reading/sending process over a public channel does not reveal any side's bit sequence. Because by using both filter types, polarized photons with any qubit value can be produce quantum key distribution decision steps after Raw Key Extraction as shown at the next figure.

2.2 Error Estimation (EE)

The negotiation process to resolve a quantum key might occur over a noisy-unsecured quantum channel. Such channel can cause a partial key damage or unmet conditions due to physical noise of transmission medium. For example, the sending and the receiving sides might not get the same qubit value even if they have used the same type of filter [5, 6].

To avoid such attacks, both sides determine an error threshold value "Rmax" when they are sure that there is no eavesdropping on transmission medium. Then after each

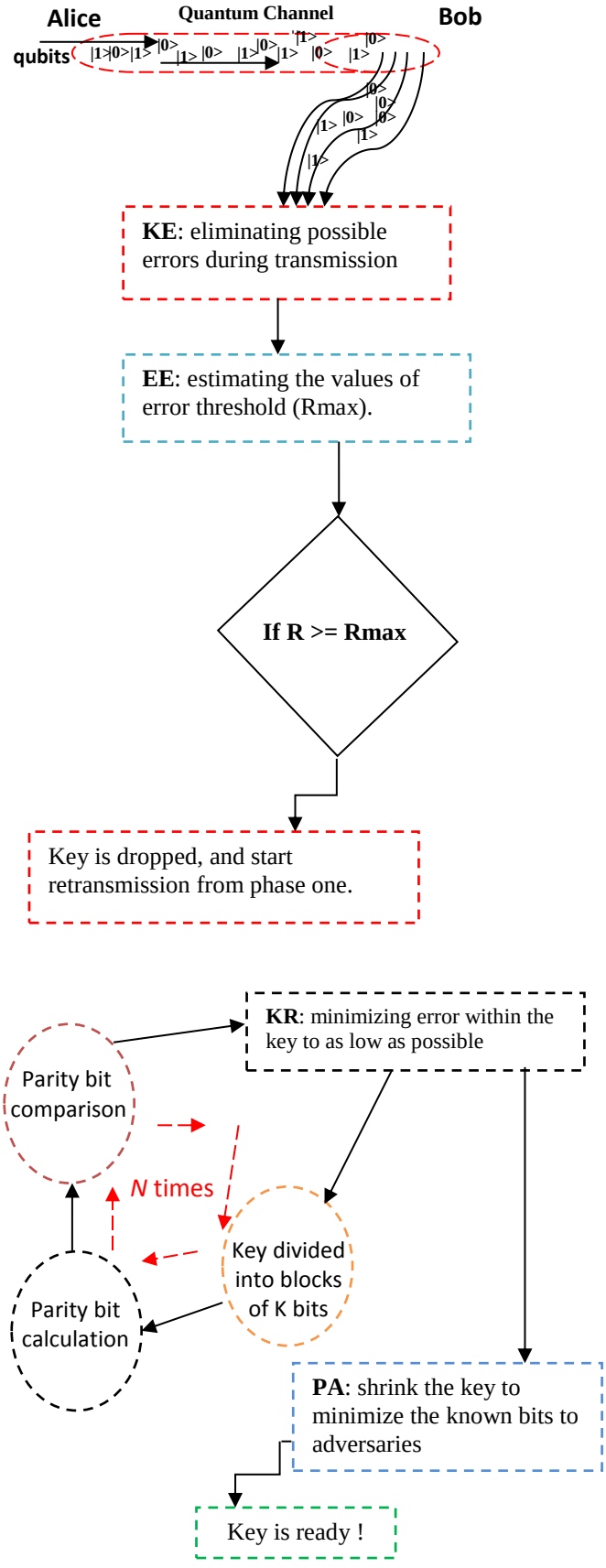

Figure 1: BB84 protocol phases

QKD session, they compare (sacrifice) some bits of their raw keys in order to calculate a transmission error percentage "R". By that way, for R > Rmax case they can be sure about existence of an eavesdropper.

2.3 Key Reconciliation (KR)

Even for R ≤ Rmax cases, errors might/can be found within the an uncompared parts of the raw key. Error reconciliation is implemented to minimize those errors within the key as possible. This step consists of number of sub-steps such as dividing the raw key into blocks of K bits, parity calculations for each block, and parity comparison which are all beyond the topic of this paper. More detailed is provided in [6, 7].

Furthermore, those sup-steps are repeatedly executed by Alice and Bob for N number of rounds, where the value of N is completely negotiated by Alice and Bob.

2.4 Privacy Amplification (PA)

Privacy Amplification is the fourth and the final step in quantum key extraction. Applied to minimize the number of bits that an eavesdropper might know in the raw resolved key from step three [7, 8]. Sending and receiving sides apply a shrinking method to their bit sequences in a way that renders it difficult for the eavesdropper to properly-apply it on his/her captured bit sequence [8].

If we assume that an n bits sequence was the result from the last three steps, and he/she (eavesdropper) knows m bits (m is a value derived from Rmax); then, n-m-s (s is a constantly chosen security parameter) sub-blocks are extracted. The parity values of these sub-blocks' union form the final key [9, 10].

3. PARITY BITS AND QUANTUM CRYPTOGRAPHY

A parity bit is a bit that is added to ensure that the number of bits with value of one in a given set of bits is even or odd. An even parity bit is set to 1 if the number of ones in a given set of bits is odd (making the "total" number of ones, including the parity bit, even). An odd parity bit is set to 1 if the number of ones in a given set of bits is even (making the "total" number of ones, including the parity bit, odd) [10].

Parity bits are used in P.A. step to resolve the final key, and as an error detection code in K.R. step (see 3 and 4 from section 2. BB84 quantum protocol). However, parity bits are an error detection code, but not an error correction code, neither as a way to determine which particular bit is corrupted [11].

Table 2. Parity bit calculation

Raw binary	Odd/Even	Binary+Parity (8 bits)	Odd/Even
1000001	E	0 1000001	E
1000010	E	0 1000010	E
1000011	O	1 1000011	E
1000100	E	0 1000100	E
1000101	O	1 1000101	E

*Note: E = even parity, O = Odd parity.

4. PARAMETERS AND NORMAL OPERATION

In this section, the proposed system and it's different parameters will be explained.

4.1 The Proposed System

To observe and examine the relation between the parity bits and the QKDS. The developed software shown below in Figure 2 simulates the BB84 quantum protocol: that means simulating the two phases of QKDS; quantum bits generation and key extraction (see section 2. BB84 Quantum Protocol).

The developed simulator exposes us with number of crucial-adjustable parameters wherein those are important to understand and adjust. The availability of these parameters in our simulator is to give the tester an insight look and experience of BB84 protocol work. Since controlling such environment will help to understand what would happen if this occur.

As an example of these parameters, the total number of bits to be transmitted, rate of photons that will change polarization due to channel's noise, delay of bits transmission in quantum channel, and eavesdropping rate. Aside from that, the photons transmission and results will be visually available to observe during the simulation.

5. TESTS AND RESULTS

The conducted test scenarios using the simulator was carried out on Core i3 (2.4GHz) with 2GB of RAM. Through adjusting the number of photons to be transmitted, starting from 5000 up-to 20000, the simulator reflects the following results shown below in Table – 3. It shows in details the number of bits resolved at each phase of the quantum key extraction phases (see section 2. BB84 Quantum Protocol), and the final key length - in bits - gained by Alice and Bob (the negotiated parties) without the use of parity bits.

When we applied the same scenarios again (i.e. the same number of bits were used) with parity bit in use, we were able to reflect the results shown in Table 4. The Rmax threshold values was set to 0.5 during both tests, thus, if the value of error percentage (R) exceeded the threshold value, the key will be ignored and a new transmission must start from the beginning (see section 2. BB84 Quantum Protocol, Error Estimation).

At the third time, we enabled the quantum channel time delay feature. If the its value set to 0.5, from the 4400 bit (first case, Table 3) we received 4000 bit only. And from 2500, we received 2000. And 2800, 1700, and 600 respectively. Moreover, we tested the system with greater time delay values, no bits were received and sometimes the simulator crippled and crash.

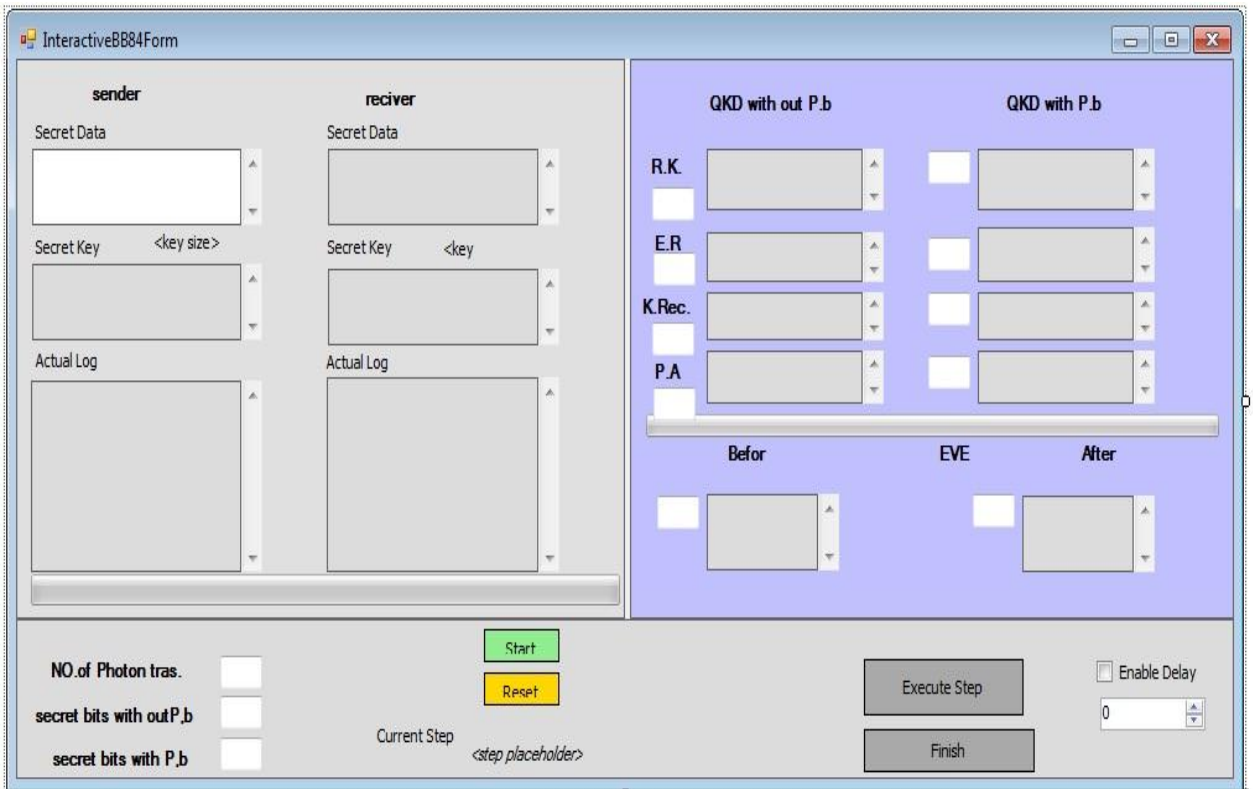

Figure 2: BB84 protocol simulator overview

Table 3. Quantum keys resolved from BB84 simulator

No. of photons transmitted at different negotiation sessions		No. or bits extracted at each phase				
Session No.	**Bits**	**Raw Key Extraction**	**Error Estimation**	**Key Reconciliation**	**Privacy Amplification**	**Finally Resolved Secret Key**
1	**20000**	**12000**	**7000**	**4500**	**2300**	**2300**
2	**10000**	**6100**	**3800**	**1700**	**730**	**730**
3	**15000**	**10000**	**5100**	**3000**	**1400**	**1400**
4	**9000**	**5000**	**2000**	**1000**	**500**	**500**
5	**5000**	**2900**	**1100**	**560**	**310**	**310**

Table 4 . Quantum keys resolved from BB84 simulator (with parity bits)

No. of photons transmitted at different negotiation sessions		No. or bits extracted at each phase				
Session No.	**Bits**	**Raw Key Extraction**	**Error Estimation**	**Key Reconciliation**	**Privacy Amplification**	**Finally Resolved Secret Key**
1	**20000**	**12000**	**9000**	**7000**	**4400**	**4400**
2	**10000**	**6100**	**5000**	**3800**	**2500**	**2500**
3	**15000**	**10000**	**7000**	**5200**	**3200**	**3200**
4	**9000**	**5000**	**3500**	**2500**	**2000**	**2000**
5	**5000**	**2900**	**2500**	**1600**	**800**	**800**

6. CONCLUSION

Quantum cryptography is a mature cryptographic algorithm and still at its early phases. Many research works have been recognized to develop this algorithm, while others to propose new implementations such as quantum computing and quantum programming [12, 14].

In this research, we examined the relation between QKDS and parity bits and successfully proved how the resolved final key would be different from the one without. Some of the resolved keys (see Table 4) are bigger by almost one-third from the one without in Table 3. As related to our results, another approach published Sofyan and Omar suggested using Universal Hashing Function instead, such as (Wegman_Carter, Taylor Code) [13]. Arguably, our approach is about how can we enhance the QKDS from within the algorithm itself and without using a second or third party Hashing/encryption algorithm.

Even more, the first phase of BB84 protocol suggests using any classical-based encryption algorithm such as DES encryption algorithm, that is to generate a completely randomized with no relation-between bits to be transmitted. The main purpose of this method is to make sure that if those bits are partially exposed to an adversary, he/she can't guess the rest of them. In the proposed simulation software, we randomly generate these bits without using such algorithm. Thus, this is an advantage to the proposed work, since if such algorithm was used, the final resolved key-with-parity would have been much bigger in length.

7. REFERENCES

[1] Muhammad Musharraf Ishtiaq Khan, "Protocols for Secure Quantum Transmission: A Review of Recent Developments", Pakistan Journal of Information and Technology 2 (3): 265-276, 2003, ISSN 1682-6027.

[2] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden , "Quantum Cryptography", REVIEWS OF MODERN PHYSICS, VOLUME 74, JANUARY 2002 , pp. 145 – 195.

[3] Matt Blumenthal , "Encryption: Strengths and Weaknesses of Public-key Cryptography ", Proceedings of the 1st Villanova University Computer Science Research Symposium , 2007.

[4] Branciard, Cyril; Gisin, Nicolas; Kraus, Barbara; Scarani, Valerio, "Security of two quantum cryptography protocols using the same four qubit states". Physical Review, 2005, A 72 (3).

[5] N. Axvig, K. Morrison, E. Psota, D. Dreher, L.C. P erez, and J. L. Walker, "´ Analysis of connections between pseudocodewords" , IEEE Transactions on Information Theory, vol. IT-55, no. 9, pp. 4099–4107, September 2009.

[6] P. O. Vontobel, "Symbolwise graph-cover decoding: Connecting sum- product algorithm decoding and bethe free energy minimization", in Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing, September 2008.

[7] D. Changyan, D. Proetti, I. E. Telatar, T. J. Richardson, and R. L. Urbanke, "Finite length analysis of low-density parity-check codes on the binary erasure - channel," IEEE Transactions on Information Theory, vol. 48, pp. 1570–1579, June 2002.

[8] Ergün GÜMÜŞ and CRYPTOGRAPHY AND DISTRIBUTION G.Zeynep AYDIN M.Ali AYDIN, "quantum comparison of quantum protocols", STANBUL UNIVERSITY, 2008 KEY (503-510) , JOURNAL OF ELECTRICAL & ELECTRONICS ENGINEERING VOLUME: 8.

[9] Vittorio, S., "Quantum Cryptography: Privacy Through Uncertainty" , 2002, http://www.csa.com/discoveryguides/crypt/overview.php

[10] Id Quantique White Paper, "Understanding Quantum ", 2005, http://www.idquantique.com/products/files/vectis-understanding.pdf

[11] Chip Elliott, David Pearson, MAGregory Troxel, "Quantum Cryptography in Practice", Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communications, ACM NY, 2003, pp. 227-238.

[12] Matteo Mariantoni, H. Wang, T. Yamamoto, M. Neeley, Radoslaw C. Bialczak, Y. Chen, M. Lenander, Erik Lucero, A. D. O'Connell, D. Sank, M. Weides, J. Wenner, Y. Yin, J. Zhao, A. N. Korotkov, A. N. Cleland, John M. Martinis, "Implementing the Quantum von Neumann Architecture with Superconducting Circuits", Cornel University Library, Journal Reference: Science 334, 61-65 (2011).

[13] F.T.Sufyan and K. Jasim.Omer , "Reducing the Authentication bits lost in Quantum Cryptography", The International Conference on Digital Information and Communication Technology and its Applications (PGNET'2011) , Jemors University , Liverpool.

[14] PETER SELINGER , "Towards a Quantum Programming Language ", Math. Struct. in Comp. Science 14(4):527-586, 2004 .