Increasing the Protocol Gain of Quantum Cryptography

Dr. Firas Ali Sabir Al-Juboori
Computer Engineering Department, University of Baghdad/ Baghdad
Email:firasaljuboori@yahoo.com
Noor Kareem Juma'a Al-Mandilawi
Computer Engineering Department, University of Baghdad/ Baghdad

Received on:20 /5/2012 & Accepted on: 9/5/2013

ABSTRACT

Quantum cryptography is a technique to distribute a sequence of truly random and unconditionally secure bits over a secure communication by applying the phenomena of quantum physics. The distributed secret bits perform the secret key which is used later to encrypt messages with an encryption algorithm, usually the One-Time-Pad is used. Quantum Key Distribution solves the security problem in classical cryptography by depending on the laws of physics which is focusing on the physics of information. Quantum protocol gain usually is low due to the quantum channel noise and the difference between the photon polarization at the sender and receiver side; in this research, a method is proposed to increase the protocol gain without decreasing the security level of quantum key. BB84 quantum key distribution algorithm is implemented and simulated with MATLAB R2010a simulation; and a comparison is made with A. Singh and N. Sharma [14] results.

Keywords: Quantum cryptography, BB84, Quantum channel, Quantum Key Distribution (QKD).

زيادة المكسب لبروتوكول التشفير الكمي

الخلاصه

الكتابة المشفره الكميه هي تقنية لتوزيع سلسلة مرالقطعِ العشوائيةحقاً والآمنة بدون شرط, على إتصال آمن بتطبيق ظواهر فيزياء الكم. القطعالموزعه سرياً تمثل المفتاح السري الذي يستعمل لاحقاً لتشفير الرسائل بخوارزمية تشفير، عادة ون-تايم-باد تستعمل. يحل التوزيع الرئيسي الكمي مشكلة الأمن في الكتابة المشفرة الكلاسيكية بالإعتماد على قوانين الفيزياء التي تركز على فيزياء المعلومات. مكسب النظام الكهِ عادة منخفض بسبب ضوضاء القناة الكمية والإختلاف بين إستقطاب الفوتون في جانب المستلم والمرسل؛ في هذا البحث, تم اقتراح طريقة لزيادة مكسب النظام بدون ان ينقص مستوىأمنالمفتاحِ الكهِ . طبقت خوارزمية التوزيع الكمي الـ بي بي 84 و مثلت بمحاكاة الماتلاب R2010a؛ وقورنت النتائج مع نتائج بحث المصدر [14].

INTRODUCTION

In classical cryptography, the two authorized persons are communicated by using either symmetric key cryptography or asymmetric key cryptography. In symmetric key cryptography, both of the sender and the receiver use the same key; in asymmetric key cryptography or public key cryptography, two pair of keys

is used a private key which is keep secret and a public key which is known publicly. When the sender (Alice) wants to send an encrypted message to the receiver (Bob), she encrypts the message with Bob's public key which could be decrypted only by Bob since he is the only one know his private key which decrypts the message [1,2,3].

Symmetric key cryptography uses the same key in both encryption and decryption of the message; which is requires a beforehand secure key. Thus, both sender and receiver should be met to handover the secret key to each other, or they could exchange the secret symmetric key over a secret channel which can not be achieved and the attacker could easily capture the key by monitoring the channel passively [4,5].

Asymmetric key cryptography uses the public key to encrypt the message and the private key to decrypt the message. The attackers are enabled to extract the private key from the public key, and this is based on mathematical assumption, for example: RSA algorithm which its large numbers are difficult to be factorize and its security can be cracked through renders messages insecure retroactively [3,5,6,7].

The problems of symmetric key and asymmetric key cryptography are known as key distribution problem ; quantum cryptography is used to solve this problem [1,3].

Quantum cryptography solves the security problems mentioned above by enabling the two authorized parity to share an unconditionally secure key in the presence of an eavesdropper since its security is guaranteed by the principles of quantum mechanics which make the eavesdropper unable to catch a just right copy of the unknown quantum state [8, 9].

The main usage of the Quantum Key Distribution (QKD) is to produce a truly random unconditionally secure key and distribute it over a secure (quantum) channel [10].

The quantum secret key is used in a chosen encryption algorithm to encrypt and decrypt messages which can be distributed over any standard (public) channel [11].

In [3], N. Kaur et al. made a comparison between classical cryptography and quantum cryptography and proved that the security level of quantum cryptography (quantum key distribution) is higher than classical cryptography.

In [12], Devi V. Anusuya and Raj T. Sampradeep have implement a quantum cryptography system based on BB84 protocol and proved that BB84 protocol has a Quantum Bit Error Rate (QBER) lower than other quantum cryptography protocols.

In [13], several parameters of the quantum gain are discussed and several ideas are listed to increase the protocol gain.

In [14], A. Singh and N. Sharma have proposed a mechanism which combines BB84 protocol at two levels, at the sender-receiver level and at the receiver-sender level to increase key length; both levels are based on logic gates to reduce the probability of eavesdropping and both levels are based on base probability with 0.5.

The rest of this paper is organized as follows: the next section summarizes quantum cryptography and QKD, BB84 protocol discussed under section BB84 protocol, the base probability is discussed under protocol gain section, A. Singh

and N. Sharma section contain the results of [14] which this research results are compared with. the implementation of BB84 and its simulation in MATLAB are discussed under section design and implementation and the results are discussed in section proposed system results and the last section contains the conclusions.

QUANTUM CRYPTOGRAPHY AND QKD

Quantum cryptography goal is to provide a secret key which is truly random and unconditionally secure and as long as the message between two authorized parities whose are never met before and they do not need to meet [15].

Quantum cryptography security mainly depends on two quantum mechanics, the principle of photon polarization and the Heisenberg Uncertainty principle. The photon polarization principle describes how the photons of light can be polarized in an exact direction which prevents the eavesdropper from truly measured the quantum states [7].

Heisenberg uncertainty principle states that without disturbing the system, pairs of quantum properties cannot be exactly deliberated simultaneously; for example, position and momentum thus it is impossible to calculate the quantum states of that system and the horizontal-vertical and diagonal polarization of photons are two such pairs [7,8].

Because of the previous two quantum principles, quantum cryptography prevents the eavesdropper from knowing the values of key bits. When the eavesdropper tries to measure the polarization of a photon, the choice of what direction is used affects all subsequences measurements; this means that the polarization of a photon of light partially can only be known at the point when it is measured. This principle is an important role in preventing the attempts of eavesdroppers in a cryptosystem based on quantum cryptography [7,8,16].

When the sender wants to send a sequence of random bits, these bits are polarized before sending; the polarization will be in one of the following four states is shown in Table (1) [10].

Table (1) Polarization of quantum bits.

State	Basis	Value	Polar angle
|0>	+	0	0 º
|1>	+	1	90 º
|0>+ |1>	x	0	45 º
|0>- |1>	x	1	-45 º

In the rectilinear (+) base, the photon is sending in either horizontal base with 0 º which is 0 or in vertical base with 90 º then it performs 1. In the diagonal (x) base, the photon sent with 45 º it will be 0 or with -45 º then it will be 1 [7, 10].

For example: if the sender (Alice) wishes to send random sequence of photon as follows: +××+×+++

The binary number represented with these states is:

11010110

Now, if the receiver (Bob) wants to obtain a binary number sent by Alice, he needs to receive each photon in the same basis as shown in Table (2) below.

Table (2) Quantum Key Generation.

Alice's random bits	1	1	0	1	0	1	1	0
Alice's random sending basis	+	×	×	+	×	+	+	+
Photon polarization Alice sends	|	\	/	|	/	|	|	—
Bob's random measuring basis	+	+	×	+	×	+	×	×
Photon polarization Bob measure	|	|	/	|	/	|	\	\
Bob's random bits	1	1	0	1	0	1	1	1
Shared secret key	1	—	0	1	0	1	—	—

BB84 PROTOCOL

BB84 is the most widely used protocol nowadays, which is the first QKD protocol invented by Charles Bennett and Gilles Brassard in 1984 [17].

In BB84 protocol coding scheme, four non-orthogonal polarization states (0º, 90º, 45º and -45º) are used that will polarize each of the photon that will be send. The communication in this protocol requires two channels, quantum channel (e.g.: optic fiber or free space) and public channel (e.g.: Internet). Alice and Bob have to communicate within channels, quantum channel and public channel to share a secret key as shown in Figure (1). First, Alice and Bob have to communicate (one way communication) via quantum channel, and then they both will create a public connection over the public channel (two way communication) [9,17]. BB84 protocol works as follow:

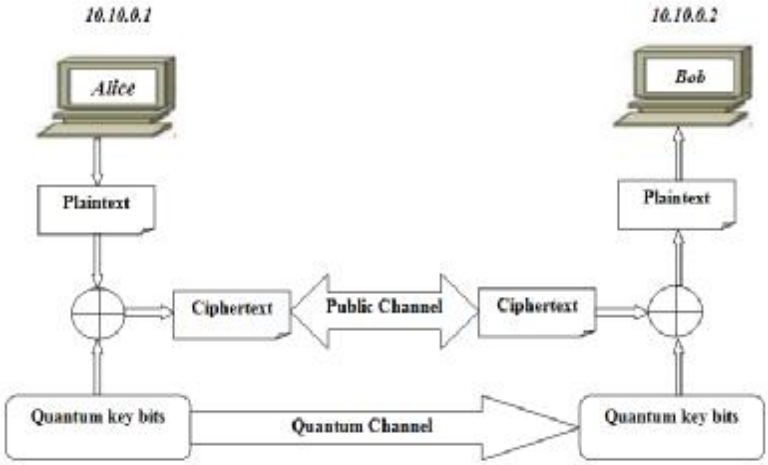
a. Over Quantum Channel:

1. Alice will send polarize photons (measure as bit) to Bob using the Quantum channel.
2. After all the photon has been transmitted; Bob will measure the bits he has received by using the rectilinear or diagonal basis.

b. Over Public Channel:

1. Both Alice and Bob will establish a connection to communicate over a public channel. Bob will proclaim his measurements (states) at the public channel with or without the presence of eavesdropper.
2. Alice will retort the correct measurements that Bob have measured with or without presence of eavesdropper.
3. Now, Alice and Bob share a raw key, which is considered not fully secret, bits may be tampered by eavesdropper during the transmission.
4. Then both Alice and Bob will continue communicate via public channel to find and correct the bits that they have by the following four phases: [9] as shown in Fig. (2).

- Sifting Raw Key.
- Error Estimation.
- Error Correction.
- Privacy Amplification.



Figure(1) Overall quantum system processes.

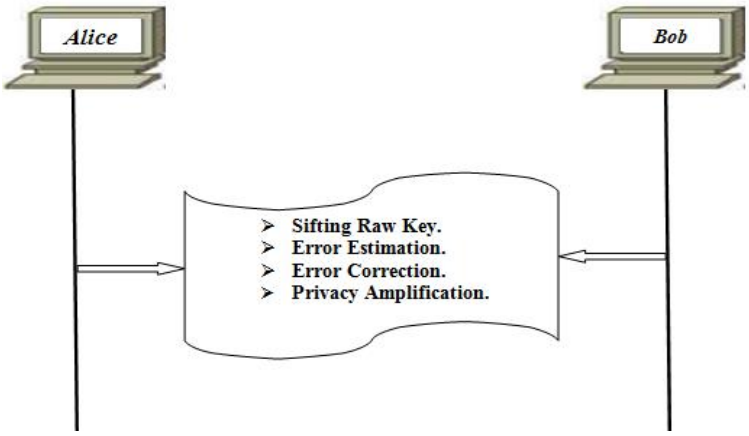


Figure (2) Public channel processes.

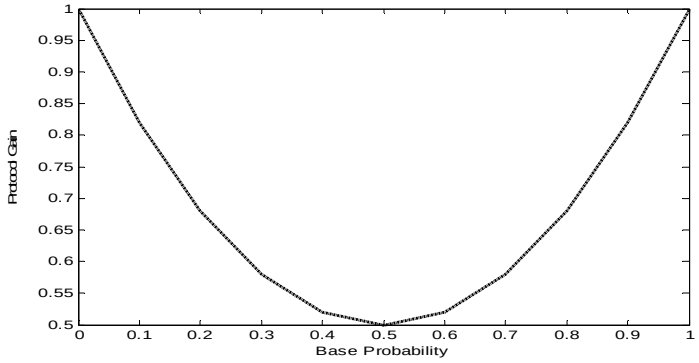


Figure (3) Protocol Gain P_g of Equation. (1).

Protocol Gain

In [13], refer that protocol gain of a quantum cryptography system is depends on the probabilities of the bases used in photon polarization. Protocol gain can be obtained by Eq. (1):

$$P_g = \delta . \delta + (1- \delta). (1+ \delta) = 2 \delta^2 - 2 \delta + 1 \quad \ldots(1)$$

Where δ is the probability of bases and $\delta \in [0,1]$. Figure (3) shows the probability gain against base probability.

From the above Fig. it is clear that the protocol gain will be in its worst case when $\delta=0.5$ and the enhancement starts from $\delta=0.6$.

A. SINGH AND N. SHARMA METHOD

In [14], researchers proposed a double BB84 protocol with a logic gate to encode the bits before sending in order to increase the security against the attacker. Their proposed system, a double BB84 protocol is choosing with 0.5 base probabilities to each stage which decrease the protocol gain of the whole system and that was the problem in [14] because the resulted sifted key was slightly short, since a lot of the bits was lost in the channel or discarded due to the same less base choosing between Alice and Bob due to the double BB84 protocol stages. Table (3) below, shows the results of [14].

Note: the measurements of [14] are measured after their system has been build by the researchers of this research.

Table (3) Sifted key length of A. Singh and N. Sharma method.

No. of bits send by Alice	Total key length received by Bob
256 bit	192 bits
512 bit	384 bits
1024 bit	758 bits
2048 bit	1541 bits
4096 bit	2175 bits

DESIGN AND IMPLEMENTATION

In this research, a method is proposed to increase the protocol gain without decreasing the security level of quantum cryptography which stays constant. Fig. (4) shows the proposed method structure and the flowchart of the 1st QKD system is shown in Fig. (5) and the 2nd QKD system is shown in Figure (6).

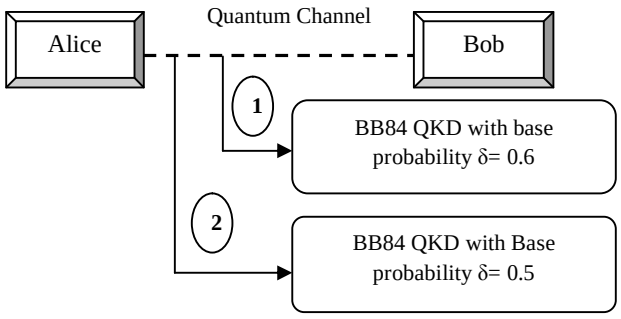


Figure (4) proposed method structure.

This research implement BB84 protocol with δ=0.5 and δ=0.6 and compare between the results and extracts the research proposed technique with a CNOT gate to encode the bits before sending in order to increase the security level.

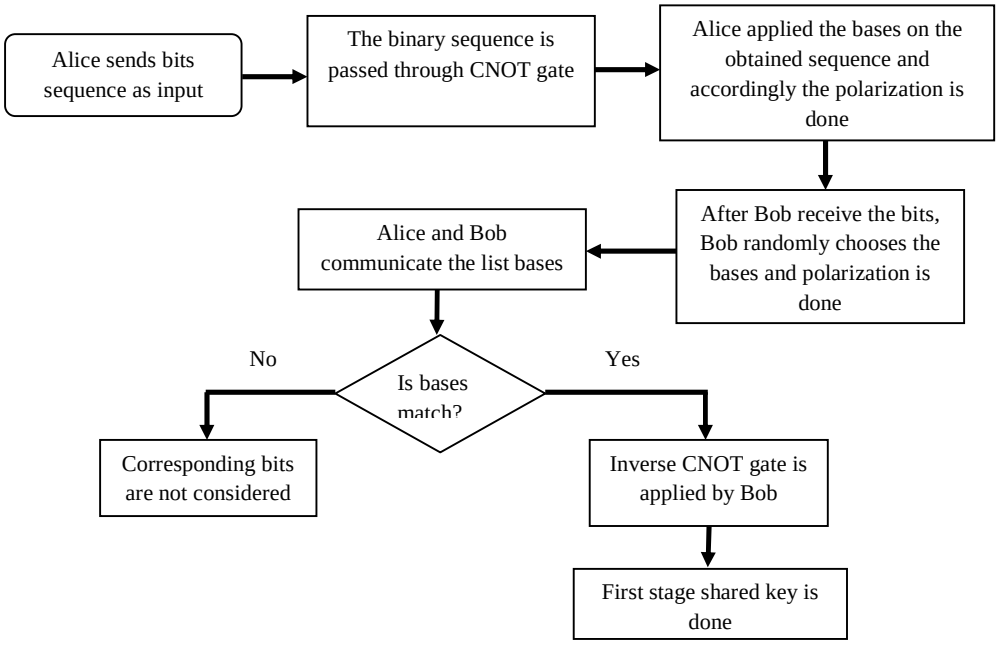


Figure (5) First stage QKD flowchart.

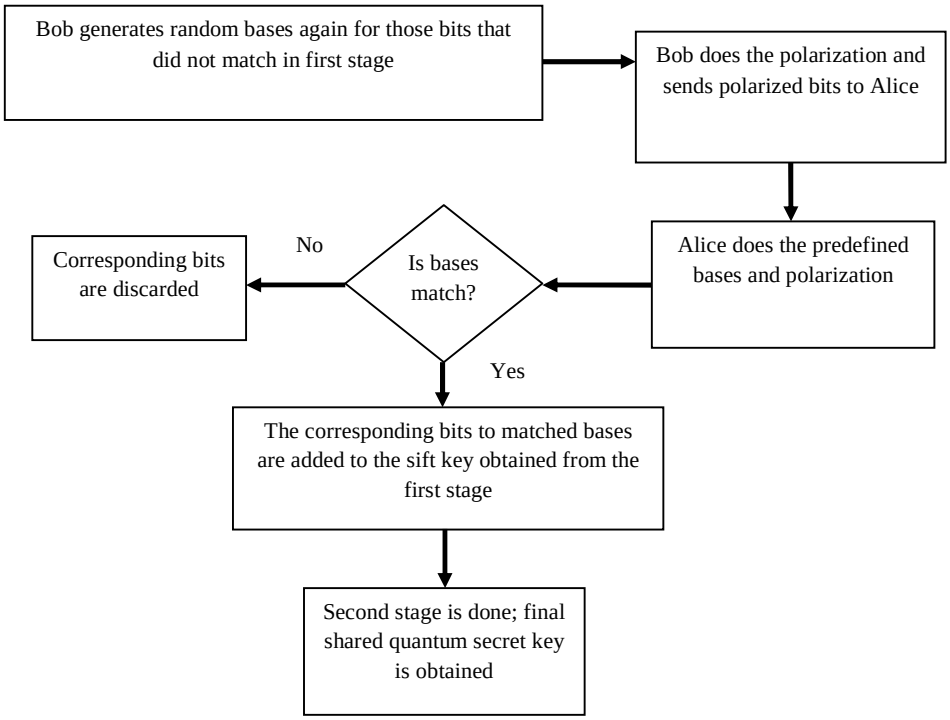


Figure (6) Second stage QKD flowchart.

1. BB84 with δ=0.5

When δ=0.5, this mean that the polarizing bases are used with equal probability i.e. 50% of the photons are polarized with rectilinear base and 50% with diagonal base.

In [13], the bases are presents with binary states where logic 0 is the rectilinear base and logic 1 is the diagonal base. Thus, in this research the LFSR random binary bits generator is used to generate the bases with δ=0.5 because in LFSR number of ones= number of zeros+1.

The results of sifting key -which is the key presented from the sifting key public stage- with δ=0.5 are shown in Table (4).

From Fig. (3) previously, it could be seen that the protocol gain of δ=0.5 is at its worst case but the security level of δ=0.5 is higher than other probabilities and this is proven in [12,13].

Table (4) Sifting key results with 0.5 base probabilities.

No. of bits send by Alice	No. of bits received by Bob
256 bit	125 bit
512 bit	242 bit
1024 bit	502 bit
2048 bit	973 bit
4096 bit	2070 bit

2. BB84 protocol with δ=0.6

In this section the probability of the rectilinear base is increased to 0.6 while the probability of the diagonal base is decreased to 0.4. When the probability δ goes to 1 the number of received bits at Bob's side with right base is increased, Table (5) shows the results of the received quantum bit after sifting phase against the photons sends by Alice.

In [13], they mentioned that when the probability δ becomes higher, the eavesdropper chance to catch the data without being detected becomes higher too. 'Alice and Bob must negotiate at least which bases to use with higher probability and Eve can use this information' [13].

Thus, in this section the results have been taken with 0.61 to 0.69 and do not go higher due to the eavesdropping.

In δ=0.6, the protocol gain here is increased but the security level is decreased as proved in [12,13].

Table (5) Sifting key results with 0.6 base probabilities.

No. of bits send by Alice	No. of bits received by Bob
256 bit	152 bit
512 bit	300 bit
1024 bit	597 bit
2048 bit	1280 bit
4096 bit	2427 bit

Table (6) below shows a comparison between δ=0.5 and δ=0.6.

Table (6) comparison between 0.5 and 0.6 base probabilities.

Base probabilities	0.5	0.6
security	More secure	Less secure
Protocol gain	worst case	increase
Percent of information catched by attacker	≈ < 25% [13]	≈ < 75% [13]

Thus, in the proposed system, the first BB84 stage is implemented with 0.6 base probability and this will solve the sifted key length problem in [14], and the second BB84 is implemented with base probability of 0.5 to solve the security problems with the first stage as mentioned before in 0.6 base probabilities problem. Figure (7) shows a comparison between Table (4) and Table (5) results.

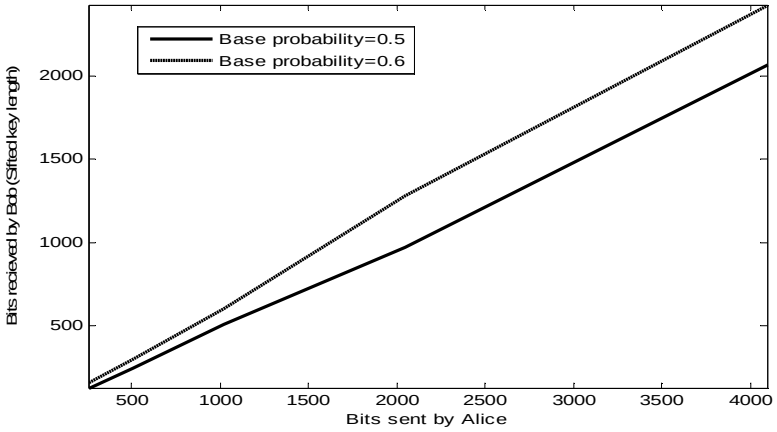


Figure (7) A comparison between δ=0.5 and δ=0.6 sifted key length.

From Figure (7), it could be seen that the sifting key length in case of δ=0.6 is higher that sifting key length in case of δ=0.5; but, as discussed previously, the security level of δ=0.6 is lower than of δ=0.5 and to solve this problem a CNOT quantum gate is added to decrease the attacker chance to 25%. For example if a |00> state is encode using the CNOT gate, the attacker has four probabilities which are |00>, |01>, |10>, or |11> to catch.

PROPOSED SYSTEM RESULTS

The proposed system is based on two stages: first one, BB84 with δ=0.6 and the second stage is BB84 with δ=0.5 this will increase the sifted key length and keep the security level high.

Table (7) shows the proposed system sifted key length and Fig. (8) shows a comparison between Table (3) and Table (7) results.

Table (7) Double BB84 proposed system results.

No. of bits send by Alice	Total key length received by Bob
256 bit	219 bits
512 bit	446 bits
1024 bit	881 bits
2048 bit	1743 bits
4096 bit	3469 bits

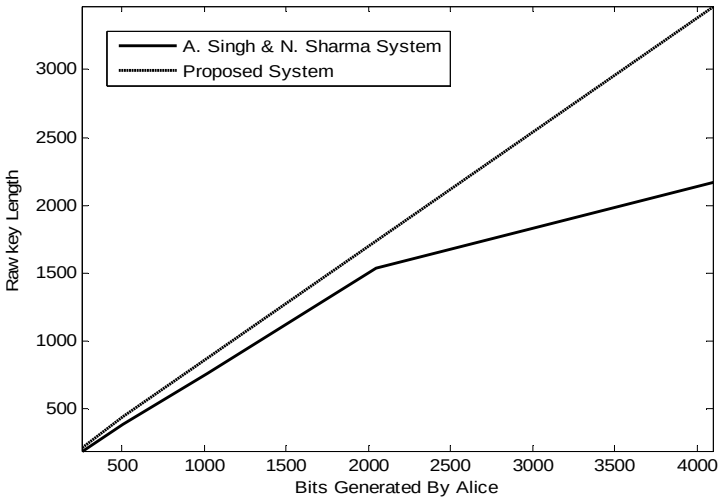


Figure (8) A comparison of the proposed system results with [14] results.

Figure (8) shows the results of A. Singh and N. Sharma and this research proposed system results, it is clearly that the gain of this research proposed system is the better than A. Singh and N. Sharma gain since the sifted key length of the proposed system is higher than the one of [14].

CONCLUSIONS

By increasing the QKD steps, the raw key length increases. In the increment in the base probability factor δ, matching basis at both sender and receiver sides raise will increase the raw key length and the protocol gain. By adding a quantum gate to the transmitting system, maximum probability of catching bits by eavesdropping will decrease to $\frac{1}{4}$ if two bits quantum gate is used; this increases the security level.

REFERENCES

[1]. Hrg, D. L. Budin and M. Golub, "Quantum Cryptography and Security of Information Systems", Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb, 2002.

[2]. Xue , Y. "Classical Cipher", lectures 5-6, *https://tao.truststc.org/Members/yuan**xue**/cyptography.../**lecture**5.pdf*.

[3]. Kaur, N. Dr. A. Singh and S. Singh, "Enhancement of Network Security Techniques using Quantum Cryptography", International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397, Vol. 3 No. 5, 2011.

[4].Protocol using Finite Sample Bits", Department of Communications and Integrated Systems, Tokyo Institute of Technology, Tokyo, Japan, October 2010.

[5]. Schneier, B. "Applied Cryptography, Protocols, Algorithms, and Source Code in c", ISBN: 0471128457, 2nd Edition, (John Wiley & Sons, Inc., 1996).

[6]. William,S. "Cryptography and Network Security Principles and Practices", Prentice Hall**,** 4th Ed. 2005.

[7]. Goel, R. M. Garuba and A. Girma, "Research Directions in Quantum Cryptography", Howard University, Washington, 2007.

[8]. Sharbaf, M. "Quantum Cryptography: A New Generation of Information Technology Security System", IEEE, Nova Southeastern University, 2009.

[9]. Muhammad, N. Z. Zukarnain, "Implementation of BB84 Quantum Key Distribution Protocol's with Attacks", European Journal of Scientific Research, Department of Communication Technology and Network Faculty of Computer Science and Technology, UPM, Selangor, Malaysia, 2009.

[10]. Jha,S. P. Chatterjee, A.Falor and M. Chakraborty, "A Matlab realization of Shor's Quantum Factoring Algorithm", IEEE, Department of Information Technology Institute of Engineering & Management, Kolkata, India, Jan, 2011.

[11].10 Minutes with a Quantum Cryptography Expert, Innovation magazine, Vol. 9 No. 2, 2010. www.innovationmagazine.com.

[12].Devi, V. Anvsuya, Raj, T. Sampradeep, "Quantum Cryptography Based Email Communication through Internet", International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462, Vol. 3 No. 1, 2011.

[13]. Kollmitzer , C. M. Pivk (Eds.), "Applied Quantum Cryptography", Lect. Notes Phys. 797 (Springer, Berlin Heidelberg 2010), DOI 10.1007/978-3-642-04831-9.

[14]. Singh, A. N. Sharma, "DEVELOPMENT OF MECHANISM FOR ENHANCING DATA SECURITY IN QUANTUM CRYPTOGRAPHY", Department of Computer Science & Engineering and Information Technology BPS Mahila Vishwavidyalaya, India, 2011.

[15]. Bone, S. M. Castro, "A brief history of quantum computing". http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/.

[16]. Papanikolaou,N. "An introduction to quantum cryptography", ACM Crossroads Magazine, Vol.11, No.3, 2005, pp. 1-16.

[17]. Hughes, R. G. Morgan and C. Peterson, "Practical quantum key distribution over a 48-km optical fiber network", Physics Division, Los Alamos National Laboratory, Los Alamos, No. 87545, LA-UR-99-1593, 1999.