VOL. 15, NO. 22, NOVEMBER 2020 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A SIMULATIVE COMPARISON OF BB84 WITH B92 QUANTUM CRYPTOGRAPHY PROTOCOL

Hasanain Abdulhasan Alsreeh[1], Duaa Hakem Alabeedy[2] and Saif Uldun Mostfa Kamal[3]
[1]Departement of Computer Engineering, Iraq University College, Basra, Iraq
[2]Departement of Communication Engineering, Iraq University College, Basra, Iraq
[3]Departement of Computer Technology Engineering, Iraq University College, Basra, Iraq
E-Mail: saif.kamal@iuc.edu.iq

ABSTRACT

Quantum cryptography is a novel technology in which two parties can secure network communication by applying the phenomena of quantum physics. In this research, a comparison between BB84 and B92 protocols will be explained. The simulation results indicate that the B92 protocol is half efficient the BB84 protocol in the key rate produce with and without eavesdropping.

Keywords: QKD protocols comparison, BB84 protocol, B92 protocol, final key length.

1. INTRODUCTION

Cryptography is the art of encoding and decoding messages and has existed as long as people have distrusted each other and sought forms of secure communication [1]. Today's most common encryption methods are threatened by the potential creation of the quantum computer. But quantum cryptography has been developed which promises more secure communication than any existing technique and can't be compromised by quantum computers. All classical encryption schemes do not provide unconditional security (expect the one-time pad algorithm) because, it depends on the principles of classical physics, it is impossible to reveal possible eavesdropping, because information encoded into classical signals can be gained, copied or monitored passively and without changing the state of the object [2]. Quantum cryptography solves the problems of conventional cryptographic schemes by providing away for two users who are in different locations to securely establish a secret key and to detect if eavesdropping has occurred [3]. The security of quantum key exchange is based on two physical theorems they are the uncertainty principle and the no- cloning theorem [4]. Various implementations for quantum key distribution protocols have been proposed, such as BB84, B92 and E91 [5, 4]. Our research is related to BB84 and B92 protocol.

2. BB84 PROTOCOL

BB84 protocol was invented by Bennett and Brassard [5]. It uses four non-orthogonal polarization states (0^{o}, 90^{o}, 45^{o}, 135^{o}) for each polarized photon that will be transmitted. BB84 protocol works as follows:

- Alice sends to Bob a sequence of randomly polarized photons.
- After all the photon transmission finished, Bob will measure the bits he received using the rectilinear or diagonal basis.
- Bob announces to Alice his polarization bases (but not results).
- Alice tells Bob which measurements are done in compatible bases.
- Alice and Bob will discard all the bits that were measured in incompatible bases and gained the sifted keys which in ideal conditions must be the same if no eavesdropping has occurred during the transmission.

3. B92 PROTOCOL

B92 is a two state protocol and was presented to the community in 1992 by Charles Bennett [5]. This protocol exploits two non-orthogonal basis and only one polarization state per basis so then the polarizations are two non-orthogonal quantum states. For example, the 0 bit is encoded $|\rightarrow\rangle$and decoded $|\nwarrow\rangle$and the 1 bit is encoded $|\nearrow\rangle$ and decoded $|\uparrow\rangle$.

The key point of the protocol is that when the transmitting and receiving bases are the same the detector will never click (the photon will be absorbed since the two polarizes are orthogonal). In the other case, when the bases are different, there is a chance for the detector to click and a chance to stay still, because the photon at the receiver side will jump suddenly in either of two states. If the photon jumps to a state that is perpendicular to the polarizer then the photon will be absorbed and no click will occur, otherwise; if it jumps to a state that is parallel to the polarizer then the photon will pass the polarizer and the click will occur. After that Bob will send a message to Alice, in a public classic channel, where there are the positions in his string where he got the clicks. Alice will discard all her bits except the ones corresponding to the message coming from Bob. Finally, Alice and Bob will share the same sub-string. The steps of the protocol can be illustrated in the following table:

Table-1. Step by step description of the B92 protocol.

1)	Alice's bit	0	1	1	0	0	1	1	1
2)	Alice sends	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\rightarrow\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$
3)	Bob's random switching	$\|\uparrow\rangle$	$\|\nwarrow\rangle$	$\|\nwarrow\rangle$	$\|\nwarrow\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$
4)	Click?	no	no	no	yes	no	no	yes	no
5)	Sifting				√			√	
6)	Sifted key				0			1	

4. ERROR CORRECTION AND PRIVACY AMPLIFICATION

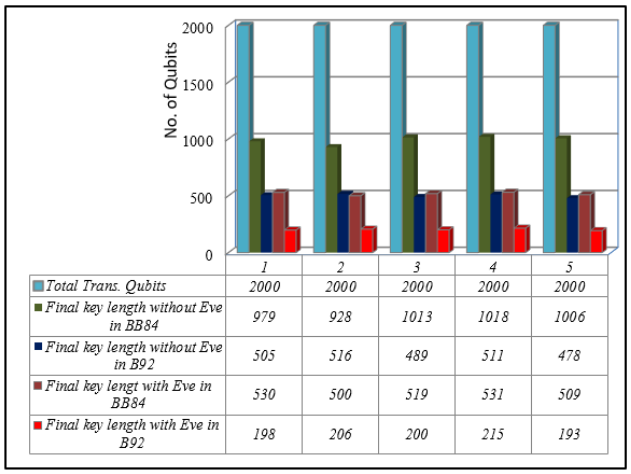
The sifted key that is gained from the BB84 protocol or the B92 protocol is not secure, because of the presence of Eve. First of all, Alice and Bob have to calculate the estimated bits error rate ($BER_{estimate}$). They selected random bits from their strings to compare them on the public channel, then they compute the number of errors found in these sampled positions to be divided on the total number of the sampled positions. If they found that their error rate is higher than maximum bits error rate (BER_{max}), they will suspend the communication and start all over again (BER_{max} has predetermined value).

If the error rate estimated is less than the threshold value, Alice and Bob will discard the sampled they used in estimation and start with an error correction protocol (such as the CASCAD protocol that is used in this simulation) to produce errors frey keys called the reconciled Keys.

The size of the reconciled keys will be reduced by discarding number of bits equal to the number of bits that Eve obtained from eavesdropping on the quantum and public channels in the privacy amplification stage.

5. SIMULATION RESULTS

Figure-1 illustrates the length of the final secret key with and without eavesdropping using BB84 protocol and theB92 protocol. The figure uses an error rate (2%) and the total number of the transmitted bits is (2000 bits). The figure explains the results of executing the simulation program five times.



	1	2	3	4	5
Total Trans. Qubits	2000	2000	2000	2000	2000
Final key length without Eve in BB84	979	928	1013	1018	1006
Final key length without Eve in B92	505	516	489	511	478
Final key lengt with Eve in BB84	530	500	519	531	509
Final key length with Eve in B92	198	206	200	215	193

Figure-1. Total transmitted qubits from Alice and successful received qubits from Bob without and with Eve existent versus number of attempts using both the BB84 and B92 protocols with (N=2000 qubits, error rate=2%).

Figure-2 shows the number of parity revealed during the error correction process (using CASCADE protocol) with respect to different error rates in both BB84 and B92 protocols. For total transmitted bits (N=2000), the figure shows that as the error rate increases the number of parity revealed also increases.

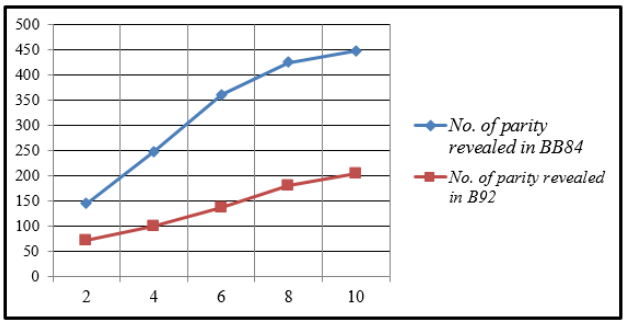


Figure -2. No. of parity revealed versus the actual error rate (N=2000).

Figure-3 shows that the estimated Eve's information I_{max} that she obtained from the intercept-resend attack is always greater than the actual Eve's information I_{actual} and they are near each other in both BB84 and B92 protocols and simulation had been done for different values of BER_{actual} that is inputted to the program and for total transmitted bits (N=2000).

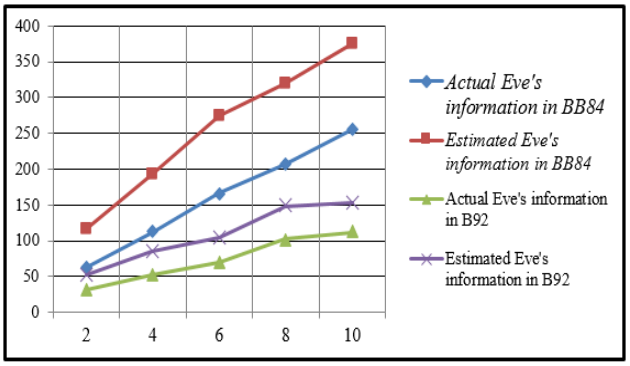


Figure-3. Expected and actual Eve's information on the sifted key versus actual bit error rate inputted to the program for both BB84 and B92 protocols (N=2000).

6. CONCLUSIONS

- In BB84 the successfully received bits are about 50% when there is no eavesdropping. If the eavesdropper (Eve) uses the intercept/resend strategy for all the transmitted qubits, the successfully received bits are reduced to about 25%, while in B92 protocol the ratio is 25% when there is no eavesdropping and 12.5% when Eve eavesdrops on all the transmitted bits. Thus B92 is half efficient the BB84 protocol in the key rate produced.
- The CASCADE error correction protocol requires the revealing of some parity bits which represent information that have been leaked to Eve. In B92 protocol the number of parities revealed is less comparing with the number of parities revealed in BB84 protocol, since the length of the sifted keys in B92 is half of the length of the sifted keys in BB84 protocol and that will lead to less number of iterations in the error correction process using the CSCADE protocol.
- The length of the final secret key depends on both the original transmitted data and the quantum bit error rate caused by Eve. With constant error rate, the final key length increases as the original transmitted bits increase at both of the protocols.

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden. 2002. Quantum Cryptography. Reviews of Modern Physics. 74: 145-195.

[2] Ajit Singh. 2007. An Efficient Quantum Cryptography's Algorithm for Data Security. Indian Journal of Engineering & Materials Sciences. 14: 346-351.

[3] C. H. Bennett and G. Brassard. 1984. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India.

[4] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone. 1996. Handbook of Applied Cryptography. CRC Press.

[5] S. Imre and F. Balazs. 2005. Quantum Computing and Communications: An Engineering Approach. John Wiley & Sons Ltd.