IMPLEMENTING BB84 WITHOUT THE CLASSICAL CHANNEL TO IMPROVE THE SECURITY OF THE QKD PROTOCOL.

Fardeen Hasan (UIN: 669660474)

Abstract: As Quantum computing has emerged and has showed a higher computation power when compared to classical computers using qubits, with an increase in computation power the need for more secure cryptography was needed, this was done by introducing BB84, This protocol for key distribution is proven to be unconditionally secure by No cloning of qubits and Heisenberg's uncertainty theorem. But the high bit error level of BB84 for quantum key distribution makes it slower. Since all the possible attacks on BB84 by the eavesdropper are on the classical channel, a model is proposed that modifies the BB84 protocol to eliminate the original high bit error and still being unconditionally secure.

Keywords – Quantum computing, qubits, No cloning theorem, Heisenberg's Uncertainty, unconditionally secure, BB84.

I. INTRODUCTION

Quantum key exchange utilizes principles of quantum mechanics to be unconditionally secure that allows an exchange of random keys which are qubits, this key can be used for encryption and decryption. This project deals with reducing or eliminating the high bit error rate of BB84 protocol whilst still not compromising of its security and the proposed model will still be unconditionally secure.

Current trends in Qkd protocol are to increase its bit rate and to increase the distance the key exchange could take place; the proposed model will surely increase the bit rate of key exchange of the Quantum key distribution protocol.

Discarding the use of classical channel increases the bit rate while still being unconditionally secure, but this can lead to decreasing the distance through which the key distribution can be sent over as using the classical channel was the means of increasing the distance and qubits over a quantum channel can't stay stable for a longer period of time. It can only remain stable for 10km which makes this proposed protocol obsolete to be used in real world, as communication over long distances is a viable requirement of a cryptosystem.

The paper is organized as follows, section 2 will give the theoretical background, section 3 will deal with the actual implementation and section 4 will deal with the summary of the project.

II. THEORITICAL BACKGROUND

The cryptosystems used widely rely on the difficulty of prime number factorization, we see in [2] how the computation power of quantum computers can prime factorize large polynomials. BB84 was introduced it demonstrated how a Quantum key exchange using quantum mechanics can be performed [1] and it was proven to be unconditionally secured [3]. However, even though its unconditionally secure the number of agreed bits is one fourth of the total number of bits which opens the possibility for attacks. A better understanding of the BB84 protocol is required to understand the possible attacks it may face.

Table 1. BB84 protocol [1]

Alice's random bits	0	1	1	0	1	0	0	1
Sending basis randomly from Alice	+	+	x	+	x	x	x	+
Produces photon	↑	→	↘	↑	↘	↗	↗	→
Measuring basis randomly from Bob	+	x	x	x	+	x	+	+
Produce photon Bob measures	↑	↗	↗	↘	→	↗	↑	→
Bits as received by Bob			1					1
Bob basis	+	x	x	x	+	x	+	+
Bob decision on the correct bits	T		T			T		T
Shared bits without Eve	0		1			0		1
Randomly Bob detect some key bits			1			0		
Alice conforms them			T			T		
Shared secret bits	0							1

BB84: The Sender Alice choses random bits using a random bit generator and then chooses random basis which produces photons this is sent over to Bob, Bob chooses random basis to measure, if the basis chosen by Bob is same as the basis of eve then the bits received are accurate, Bob sends the basis he chose over classical channel, Alice relays the information of the chosen bits being correct or incorrect then Bob sends few of the correct bits to Alice and Alice acknowledges this. Then the remaining of the correct bits becomes the Distribution key.

Sender 's random bit	0	1	1	0	1	0	0	1
Sender random sending basis	+	+	x	+	x	x	x	+
Photon polarization Sender sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	x	+	+	x	+	x	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Receiver random measuring basis	+	x	x	x	+	x	+	+
Photon polarization Receiver measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✘			✓		✓

Table 2. BB84 protocol [2]

If an eavesdropper Eve intercepts this information in between it can choose a random basis and decrypt the bit received from Alice then based on this Eve will generate a bit and sends it to bob and if Eve gets the basis right and bob choses the same basis then they both get the correct bit, if eve chooses the wrong basis and bob chooses the correct basis as Alice then he get the right bit and even gets the wrong bit; an error in the key is 50%x50%=25% so the probability that they find disagreement and identify the presence of Eve is $P_d=1-(0.75)^n$, the only part were Eve can know about the bits being correct or not is from the classical channel if this is eliminated, the interception by Eve will be eliminated from the protocol. The working of BB84 needs a calculation of Qber = Number of bits error by Total number of bits. The calculation of Qber will also be avoided by eliminating use of a classical channel.

III. THE PROPOSED PROTOCOL:

Alice Randomly generates bits and choses basis randomly which generates photons like before then sends it to Bob over a quantum channel where Bob chooses a random basis and encrypts the bits and sends it over to Alice using quantum channel eve notices which basis bob did not choose correctly and makes changes in her key because now Alice would know what key bob has and this becomes the key for cryptography .

Even if Eve intercepts bits from Alice she has no way to know what bits are correct since the classical channel does not exist.

Sender bits	0	1	0	0	1	1
Basis	x	+	+	+	x	x
Photon Polarization	↗	→	↑	↑	↘	↘
Receiver Basis	x	+	+	+	x	x
Photon Polarization	↗	→	↑	↑	↘	↘
Shared key	0	1	0	0	1	1
Shared key	0	1	0	0	1	1

Table 3. Proposed BB84

As it is shown from Table 3 without using classical channel key can be shared, eliminating classical channel will eliminate interception of Eve

Sender bits	0	1	0	0	1	1
Basis	x	+	+	+	x	x
Photon Polarization	↗	→	↑	↑	↘	↘
Receiver Basis	+	x	+	+	x	x
Photon Polarization	↑	↗	↑	↑	↘	↘
Bob's key	1	0	0	0	1	1
Shared key	1	0	0	0	1	1

Table. 4 Proposed BB84 with a wrong basis

Even with a wrong basis the key shared is can be worked out by Alice as she knows the basis Bob chooses.

This Protocol does not need the calculation of Qber.

IV. SUMMARY AND CONCLUSION

The Proposed BB84 surely will be faster as it does not have to compute Qber and Since there is no classical channel there will be no attacks from any eavesdropper. But the discarding of classical channel would mean the distance of the channel is reduced. So although the bit rate is increased the distance the key can be sent over is reduced.

REFERENCES

[1] Bennett, G., Charles H & Brassard (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, pp. 175–179, New York.

[2] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM journal on computing, 26, 1484–1509.

[3] Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. Physical review letters, 85(2), 441.

[4] Wootters, W.K. and Zurek, W.H. (1982) A Single Quantum Cannot Be Cloned. Nature, 299, 802-803.

[5] Bennett, C. H., Bernstein, E., Brassard, G., & Vazirani, U. (1997). Strengths and weaknesses of quantum computing. SIAM journal on Computing, 26(5), 1510-1523.

[6] Bennett, Charles h., and David p. Divincenzo. "quantum information and computation." nature 404.6775 (2000): 247.

[7] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 560, 7-11.

[8] Bennett, C. H., Brassard, G., Breidbart, S., & Wiesner, S. (1983, January). Quantum cryptography, or unforgeable subway tokens. InAdvances in Cryptology (pp. 267-275). Springer US.

[9] pan, w. D., and f. T. Sheldon. "a short survey on quantum computers y. Kanamori,∗ s.-m. Yoo." international journal of computers and applications 28.3 (2006).

[10] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (1992). Experimental quantum cryptography. Journal of cryptology, 5(1), 3-28.

[11]Nan-Run, Z., Zhou & Gui-Hua (2005). A realizable quantum encryption algorithm for qubits. Chinese Physics, 14, 2164.