Approaching Secure Protocol from Quantum Perspective

,Abdalraouf Hassan, Wesam Batrafi, and Khaled Elleithy
Department of Computer Science Engineering
University of Bridgeport
Bridgeport, CT, 06604, USA
(abdalrah, wbatarfi)@my.bridgeport.edu, elleithy@bridgeport.edu

***Abstract*— The aim of quantum cryptography is to overcome the everlasting problem of unrestricted security in private communication. The usage of the quantum principles protects the privacy of the user data during the time it is in the transmission process over the telecommunication channels. The sophisticated algorithm we have developed will make the data meaningless to eavesdroppers. The security of modern cryptographic systems has been accomplished by using a long key that will require many years to launch a brute force attack. Therefore, we designed an efficient algorithm that is developed based on BB84 and B92 techniques. In this paper, we utilized the classic features of quantum mechanism, such as superposition and uncertainty principle. We present the underlining mechanisms of quantum cryptography that enhances the security of data transmission in three stages with valid results that promise a low rate of errors that leads to a strong consistent key by raising the constraint of the security concept.**

***Keywords*—** *Quantum, Cryptography, Security, BB84, B92.*

I. INTRODUCTION

The revolution of Quantum mechanism occurred early in the 20th century. Therefore, every time we use electronics devices or transmit and receive information unconsciously, we utilize our knowledge of the nature of quantum. Yet, in information, technology there is still enough room for developing quantum properties [1]. During the early 80, scientists have acknowledged quantum aspects as a supply for identifying with protocols banned by traditional laws of physics. Furthermore, in modern computers, the increase in performances goes hand in hand with decrease in size. Consequently, more rapidly, a single transistor will be so modest that it will be essential to account for quantum effects to understand fully and to predict decisively its behavior [2].

The theory of quantum cryptography was developed in 1984 (BB84) by Charles H. Bennett and Gilles Brassard as part of a research study between physics and information at IBM. It was known at that time as quantum distribution scheme [1].

The fundamental concept of the quantum system relies on the distribution of single particles or photons and the value of a classical bit encodes by the polarization of a photon [2]. Actually, the quantum cryptography is based on two important elements of quantum mechanics: The Heisenberg Uncertainty principle and the principle of photon polarization. Based on physical law, a photon is an elementary particle of light carrying a fixed amount of energy, light may be polarized; polarization is a physical property that comes forward when light is observed as an electromagnetic wave [3]. The direction of a photon's polarization can be fixed to any desired angle (using a polarizing filter) and can be measured using a calcite crystal.

II. PROBLEM IDENTIFICATION

While genuine algorithms have fulfilled the markets for a practical secure system, the search for a provable secure algorithm is still searched by scientists. Furthermore, security of RSA, the mainly used crypto protocol today, resides on the not disproven fact that no efficient factorization algorithm that is able to break it in logical times is known.

We now know that if quantum computers will be ever available, RSA could be broken by Shor's quantum Algorithm [4] a quantum computer could factorize large numbers in a very efficient manner exploiting entangled states. The open traditional problem was essentially the key distribution process. Identical shared keys will be given to Alice and Bob by QC protocol. Then to categorize the approximate communication error level, the two parties have to compare their strings [5]. The third party Eve interceptions could be the reasons for the error, channel flaws (as losses) and detectors' inefficiencies and/or dark counts, to make it more difficult to differentiate among these types of errors is physically impossible. For that reason, we assume all the errors are due to eavesdropping. QC tries to answer the following question: Is it actually possible to produce and distribute a sequence of truly strings random numbers of bits to form a shared trusted key in a provably secure way?

III. RELATED WORK

The Heisenberg Uncertainty principle states that, it is not possible to measure the quantum state of any system without disturbing that system. This means that polarization of a photon or light particle can only be known at the point when it is measured [9]. This principle plays an important role in preventing the attempts of eavesdroppers in a cryptosystem based on quantum cryptography [6].

Secondly, the photon polarization principle explains how light photons can be polarized in a specific direction. In addition, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to the no-cloning theorem which was first presented by [8] in 1982. The quantum cryptography allows a bit string to be agreed between two communications parties without having two parties to meet face to face, and yet these two parties can be sure with a high confidence that the agreed bit string is exclusively shared between them.

A. One Time Pad

In cryptography, a one-time pad (OTP) is an encryption technique that cannot be broken if used correctly [10]. In this technique, a plaintext is paired with a random, secret key (or pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition [4]. If the key is truly random and at least as long as the plaintext and never reused in whole or in part and kept completely secret, the resulting cipher text will be impossible to decrypt or break [7]. It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys. However, practical problems have prevented one-time pads from being widely used.

Despite Shannon's proof of its security, the one-time pad has serious weakness in practice; it requires perfectly unpredictable random one-time pad numbers, which is a non-trivial software requirement [5].

Secure generation and exchange of the one-time pad material must be at least as long as the message [9]. The security of the one-time pad is only as secure as the security of the one-time pad key-exchange. Careful treatment must make sure that it continues to remain secret from any adversary

Key distribution is needed bcause the pad, like all shared secrets, must be passed and kept secure, and the pad has to be at least as long as the message, once a very long pad has been securely sent (e.g., a computer disk full of random data), it can be used for numerous future messages until the sum of their sizes equals the size of the pad [12]. Quantum key distribution also proposes a solution to this problem.

Distributing very long one-time pad keys [11] is inconvenient and usually poses a significant security risk. The pad is essentially the encryption key but unlike keys for modern ciphers, it must be extremely long and is much too difficult for humans to remember [8]. Storage media such as thumb drives, DVD-Rs, or personal digital audio players can be used to carry a very large one-time-pad from place to place in a non-suspicious way, but even so the need to transport the pad physically is a burden compared to the key negotiation protocols of a modern public-key cryptosystem. Finally, the effort needed to manage one-time pad key material scales very badly for large networks of communicants [7].

The number of pads required increase as the square of the number of user's increase freely exchanging messages. For communication between only two persons or a star network topology, this is less of a problem [14]. The key material must be securely disposed of after use to ensure that key material is never reused and to protect the messages sent. Because the key material must be transported from one endpoint to another and persist until the message is sent or received, it can be more vulnerable to forensic recovery than the transient plaintext it protects [13].

IV. CRYPTOGRAPHY

Cryptography came to use thousands of years ago, and since then, it has been constantly developing along with human civilization [11]. The significantly influenced human society and some time even the course of history. Today cryptography has become important technology in the internet society that each individual relies on [9].

One typical example is the RSA [7] crypto scheme; it is often used in online shopping: The net shop prepares a public key containing the product (N) of p and q prime numbers. A net shop published this product (N) for its customers and keeps the values of p and q secret [8].

The costumers encrypted their credit card information with the purchase information with public key and sent the encrypted data to the net shop; the net shop derives the private key from the two primes by simple calculation to decrypt this data [10]. Let us assume the malicious hacker knows the public key but has no idea of the private key. For decryption, the hacker needs to factorize (n) to find the prime p and q. The factorization of this prime numbers is a time consuming task when (n) is large [8].

In the end of the last century, it was said even the most powerful computer would take thousands of years to factorize 200 digit numbers [12]. Since then rapid progress has been made in both software and hardware.

In December 2009, an international team of researchers succeeded in cracking 786-bit RSA key in only two years using a novel encryption algorithm and cluster of personal computers [15]. If military intelligence had a method of breaking longer keys, it would never announce this fact. For this reason, RSA scheme today employs a public key with at least 1024-bit key.

In recent years, the fiber tapping device [13] became available in the market, making it easy for hacker to tap signal for a fiber. It has been actually reported that fiber networks in some U.S. investment firms and Frankfort airport were intercepted in the past. Therefore, encryption is necessary to guarantee safe transmission to sensitive data.

A. BB84

The first QKD protocol was introduced in 1984 [6], labeled as BB84. It used two polarization bases, rectilinear (R) basis and diagonal (D) basis, and the single photon that may be polarized with four states: |h›, |v› |lcp›, and |rcp›. Polarization state |h› (|v›) in R-basis reveals “0” (“1”) and polarization state |lcp› (|rcp›) in D-basis reveals “0” (“1”). The italic letters h mean horizontal, v vertical, lcp left circle polarized, and rcp right circle polarizes [10].

Alice and Bob would like to send an encrypted message to each other so their message securely can be made private [12]. To do this, they need a cryptographic key that is only known to them that they will use to encrypt their message [15]. In addition, there is Eve; she tries to intercept their message, BB84 will allow them to come up with secret key both can use and trust.

To follow the BB84 protocol, Alice and Bob need to use two communication channels [11], classical channel and quantum channel. The classical channel allows them to send individual bits of information back and forth. As the bits travel among the classical channel, it is possible for Eve to intercept them. Eve can observe the bits and send a copy of them to their regular destination. When communicating through a classical channel, Alice and bob have no way to detect Eve.

The quantum channel [8] behaves differently. Instead of transferring bit, it transfers qubits. The qubits represent bit, and either of two processes can generate them. Let us call them (A) and (B). The BB84 takes advantage of some properties of qubits. Qubits cannot be copied and it is not possible to determine whether if qubits were generated by process (A) or (B). When qubits represent zero in machine (A), it will produce a zero and when qubits represent one, the machine will produce one [10]. In both cases the qubits will be destroyed in the process, on the other hand, if machine (A) is fed with qubits that were produced by machine (B), the output will be randomly half the time is zero and half the time is one, and the qubits is still be destroyed [9]. Likewise, a special machine exists to observe qubits produced by process (B). Let us call it machine (B). When it gives qubits produced by process (B), a machine (B) will out put the correct bit, but when is fed a qubits produced by process (A), machine (B) output will be random and just as machine (A) qubits will be destroyed. Therefore, when Bob receives a qubit over the quantum channel, he will not know which machine to use to observe it. He will decide by a coin toss [5]. Half the time he will feed qubits to machine (A) and half the time, he will feed it to machine (B) [9].

The protocol began [11] when Alice sent Bob a very large number of qubits over the quantum channel. Bob recorded all the output he received as he fed the qubits randomly to his qubits measuring machine. He will pick the right machine half the time; an average 50 percent of his measuring will be correct for the remaining qubits. He will still end up half the time just by chance. This means 75% of Bob measurement will be correct [5].

However, if Eve intercepted [9] the qubits before they reach Bob, she will also need to make random guesses as to which machine to use. Thus because Eve intercepted half of the qubits, therefore half of the qubits she will send to Bob. Half has been generated correctly and half of them incorrectly [5]. This means only 75% of the qubits that will reach Bob will represent what Alice intended [9]. Now when Bob receives the qubits, he will have to make random guesses. This will give Bob a new accuracy of 62.5%. Bob however does not know that yet, so he and Alice will have to communicate some information to each other to work out what accuracy Bob is getting. Once Bob finished measuring all the qubits he received, he will open the classical channel and send Alice a stream of bits that indicates to her which machines he used to measure each of her qubits. Once she received that message from Bob, she will review the personal record and send to Bob telling him which of the qubits he ended up measuring correctly [11]. Now Bob can throw away the wrong qubits and Alice can do the same. Now they are in possession of a string of bits that is only known to them and no one else.

If the observation accuracy [10] is below 100%, they will know Eve intercepted some of their Qubits and the communication is not secure. Proved that Eve was attempting to confound their effort, they should now be in possession of string of bits that is known only to them. They have very large sequence of bits so they can afford to sacrifice a random subset of them in order to determine whether Eve was listening to them over the classical channel [7]. They need to choose a subset of bits and compare them, and if they are satisfied they are secure, then they can use the reaming bit to form a secret cryptographic key. If they observe an accuracy of 100 %, they can be reasonably confident that their share key is secure. Now they can use them to encrypt further communications, using this protocol allow Alice and Bob to generate a cryptographic key and they can determine whether secrecy has been compromised or not.

Table 1.A 8-bit sample of Alice (A) and Bob (B) for BB84

Sequence of bits	1	2	3	4	5	6	7	8
A’s bit	1	0	1	0	0	1	0	0
A’s source basis	D	R	R	D	R	D	D	D
A’s polarization	|rcp›	|h›	|v›	|lcp›	|h›	|rcp›	|lcp›	|lcp›
B’s detector basis	D	D	D	R	R	D	R	D
B’s measurement	|rcp›	|rcp›	|lcp›	|v›	|h›	|rcp›	|h›	|lcp›
B’s bit	1	1	0	1	0	1	0	0
A’s response	Y	N	N	N	Y	Y	N	Y
Shared secret key	1	_	_	_	0	1	_	0

B. *Protocol B92*

In the B92 protocol [4], two states can be regarded as “half” of the BB84 protocol. Alice and Bob first have to agree that Alice uses |h›-photon and |rcp›-photon to represent “0” and “1”. Bob uses |lcp›-basis and |v›-basis as “0” and “1”. Table 1 and Table 2 show BB84 and B92 in detail.

Based on B92 only two states are more important than the possible four polarization states in BB84 protocol [16], and this is the main difference in B92. “0” can be encoded as “0” degree in the (R) rectilinear basis and “1” can be encoded by “45” degrees in the diagonal basis (D). Just like the BB84, Alice transmits to Bob a random string of photons encoded with randomly chosen bits, however now, Alice dictates which bases she must use [1]. Bob still randomly chooses a basis by which to measure, but if he chooses the wrong basis, he will not measure anything (a condition in quantum mechanics that is known as an erasure). Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.

Table 2.A 8-bit sample of Alice (A) and Bob (B) for B92

Sequence of bits	1	2	3	4	5	6	7	8
Alice’s bit	1	1	0	0	1	0	0	1
A’s polarization	|rcp›	|rcp›	|h›	|h›	|rcp›	|h›	|h›	|rcp›
B’s detector	|lcp›	|v›	|v›	|v›	|lcp›	|lcp›	|v›	|lcp›
Bob’s bit	0	1	1	1	0	0	1	0
Bob measurement	N	Y	N	N	N	Y	N	N
Shared secret key	_	1	_	_	_	0	_	_

For instant, in Table 2, only two bits are shared by Alice and Bob (2, 6) as the secret key, the efficiency is 2/8= 25%.

For protocol B92 [4, 17, 18], the ideal efficiency is 25%. To analyze the +efficiency in properly way is shown in Figure 2. Assume that Alice sent |h›-photon, i.e., “0” (Figure 2(a)). Bob will choose randomly |lcp› -basis or |v›-basis. If Bob selects the wrong basis, i.e., |v›-basis, he cannot detect the photon. If Bob selects the correct basis, i.e., |lcp›-basis, he has 50% probability to detect the photon; however, even if he chooses the correct basis, he still has the probability of 50%. Finally, Bob will have idealized maximum efficiency of 25% to share the correct bits [16, 17, 18].

V. Proposal Algorithm to Improve security

In this protocol, we introduced the three stages process. The first stage convention is similar to the BB84 protocol. Alice will choose random strings bits through the four bases according to the BB84 protocol and send them to Bob through Quantum channel. Bits “0” can be encoded as |v› state in (R) basis and as |lcp› degrees in the (D) basis and bits “1” can be encoded as |v› state in (R) and |rcp› (D) basis [11].

A. *In the first stage Bob will make his guess and use random basis to measure Alice’s Qubits; then Bob will open a classical channel to communicate with Alice and announce what basis he used to measure his bits. Alice will compare their bases and find out which is the wrong measurement and then discard the wrong basis from the strings that she received from Bob, and she will save what resulted from this process.*

a) In the second stage Alice will repeat the first step again and generate another random sequence of photon using the same polarization basis from stage one and send it to Bob through quantum channel.

b) Bob will detect each photon that is represented in the binary sequence using random basis from |lcp›, |rcp›-basis or |h›, |v›-basis to measure Alice string.

c) Alice and Bob will share the results of Bob’s measurement through classical channel. Alice will analyze Bob’s result and proceed to the final stage.

d) Alice compares both Bob’s result with her string, and discards the correct matched Bob’s result from his measurement.

e) Finally, Alice will combine the first stage result and second stage result string together to generate the final shared secret key. It will be a strong sophisticated key that will provide more security and reliability to their information transaction.

These key will be developed from the result of deriving the two keys represented as one strong Encryption key, so both user can use now to transmit their data safely.

First stage for producing the key works exactly according to BB84 protocol

Table 3.A 8-bit sample of Alice (A) and Bob (b) 1st stage

Sequence of bits	1	2	3	4	5	6	7	8
A’s bit	1	0	1	1	0	1	0	1
A’s basis	D	D	R	D	R	D	R	R
A’s polarization	|rcp›	|lcp›	|v›	|rcp›	|h›	|rcp›	|h›	|v›
B’s detector	R	D	R	R	R	D	D	D
B’s measurement	|h›	|lcp›	|v›	|h›	|h›	|rcp›	|rcp›	|lcp›
Bob’s bit	0	0	1	0	0	1	1	0
Bob reports basis	R	D	R	R	R	D	D	D
A’s response	N	Y	Y	N	Y	Y	N	N
1st shared secret key	_	0	1	_	0	1	_	_

B. The Second stage for producing the secret key

Alice will generate another random string through the quantum channel to Bob. Bob will measure the string randomly and compare his measured bits through classic channel with Alice. Alice here will discard the correct basis that is matched Bob’s measurement from her string.

C. The Third stage Alice will compare both keys from first and second stage together and combine them as one strong secret key that will be used to transfer data between both parties through the classic channel.

Table 3.B 8-bit sample of Alice (A) and Bob (b) 2nd stage

Sequence of bits	1	2	3	4	5	6	7	8
A’s bit	0	0	1	0	1	1	1	0
A’s basis	D	R	D	R	R	R	R	D
A’s polarization	|lcp›	|h›	|rcp›	|h›	|v›	|v›	|v›	|lcp›
B’s detector	D	R	D	R	R	D	R	D
B’s measurement	|lcp›	|v›	|lcp›	|h›	|v›	|rcp›	|h›	|lcp›
Bob’s bit	0	1	0	0	1	1	0	0
Bob reports	D	R	D	R	R	D	R	D
A’s response	N	Y	Y	N	N	Y	Y	N
2nd Shared secret key	_	1	0	_	_	1	1	_

Final stage to combine 1st and 2nd secret key to finalized the shared secret key.

Table 3.C 8-bit sample of Alice (A) and Bob (b) final stage

1st key	0	_	1	0	1	_	_	_	_
2nd key	_	1	0	_	_	1	_	1	_
Final Shared Secret key	0	1	0	1	0	1	1	1	_

VI. ANALYSIS

In figure 3.A, if Bob chooses the correct basis, he will detect the correct polarized photon. However, if Bob chooses the wrong basis, he knows that his result is inconclusive. Therefore, the idealized maximum efficiency is 50% for BB84. It also shows that Alice used R-basis sending |h›-photon and |v›-photon. In B92, the efficiencies are 25% and for BB84 its 50% and this is the price that two QKD protocol must pay for secrecy. Here we proposed two-way transmission over the quantum channel (Alice →Bob and Alice→ Bob) instead of one-way transmission. Our enhanced QKD protocol has three stages. In the first stage, Alice sends random sequence of photon according to BB84; in the second stage Alice will use a modified version of BB84 to send another large sequence of photon, and in the final stage Alice will generate a cryptography key that resulted from previous stages.

Our enhanced protocol enhances the efficiency to 43.8% with the average complexity order 2.76 when using BB84 in the first stage. In addition, when using the modified version in the second stage the idealized maximum efficiency can reach 28.9% with average complexity of 2.4.

VII. CONCLUSION

Quantum cryptography is a fascinating illustration; the uncertainty principle imposes restrictions on the capacity of certain types of communication channels. It is not possible for hackers to determine whether the qubits were generated by R-basis or D-basis. Furthermore, by taking advantages of transmitting the qubits over the quantum channel, that will increase the security by developing strong cryptographic key and use it to exchange data between two parties. However, in our proposed protocol, we take advantages of the properties of quantum qubits twice to generate a secret key that can be generated without any interference from an eavesdropper. By increasing the restriction of the security. Therefore, we develop a strong reliable key by adding more security demands without being worrying about any guesses from intruder who might be present. Even if the guess of the attacker in the first case was 25%, we enforced this error to be decreased to 15% to 18%. This is because of` the principles of quantum mechanics that ensure that no eavesdropper can successfully measure the quantum state while it is being transmitted without disturbing the state in some detectable way. Using this protocol allows Alice and Bob to generate secure a cryptographic key, and they can determine whether or not their secrecy has been compromised.

REFERENCES

[1] Shor, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on. IEEE, 1994.

[2] Porzio, Alberto. "Quantum cryptography: Approaching communication security from a quantum perspective." Photonics Technologies, 2014 Fotonica AEIT Italian Conference on. IEEE, 2014.

[3] Brief histories of crypto techniques and machinerie http://en.wikipedia. org/wikilHistory _ oC cryptography ;

[4] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring" in Proceedings of the 35th Annual Symposium on Foundations of Computer Science (ed. Goldwasser, S.) pp. 124-134 (IEEE Computer Society Press, 1994), see also SIAM J. Com put. 26:1484 (1997);

[5] Carl W. Helstrom, "Quantum Detection and Estimation Theory", (Academic Press Inc., New York, 1976, ISBN 0123400503); J. A. Wheeler and W. H. Zurek, "Quantum Theory and Measurement", (Princeton Univ. Press, Princeton,1984, ISBN 0691083169);

[6] W. K. Wootters, e W. H. Zurek, "A single quantum cannot be cloned", Nature, vol. 299, pp. 802-803, Oct 1982;

[7] Kitaev, Alexei Yu, Alexander Shen, and Mikhail N. Vyalyi. Classical and quantum computation. Vol. 47. Providence: American Mathematical Society, 2002.

[8] Trojek, Pavel, et al. "Compact source of polarization-entangled photon pairs." Optics express 12.2 (2004): 276-281.

[9] Li, Xiaoyu. "A quantum key distribution protocol without classical communications." arXiv preprint quant-ph/0209050 (2002).

[10] Kuhn, D. Richard. "Vulnerabilities in Quantum Key Distribution Protocols." arXiv preprint quant-ph/0305076 (2003).

[11] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, December 1984, pp.175-179 (1984);

[12] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States", Phys. Rev. Lett., vol. 88,n. 5, pp. (057902) 1-4, Jan 2002;

[13] G Nocerino, D Buono, A Porzio and S Solimeno, "Survival of continuous variable entanglement over long distances", Phys. Scr., vol. TI53, pp. (014049)1-6, Mar. 2013;

[14] C. H. Bennett, D. P. DiVincenzo, J. A. SmolinandW. K.Wootters, “Mixed state entanglement and quantum error correction,”Phys. Rev. A54, 3824–3851(1996), arXive e-print quant-ph/9604024.

[15] N.J. Cerf, S. lblisdir, and G. Van Assche, "Cloning and cryptography with quantum continuous variables", Eur. Phys. J. D, vol. 18, n. 2, pp. 211-218, Feb. 2002;

[16] T. C. Ralph, "Continuous variable quantum cryptography", Phys. Rev. A, vol. 61, n. I, pp. (010303)1-4, Jan 1999;

[17] Kartalopoulos, Stamatios V. "Identifying vulnerabilities of quantum cryptography in secure optical data transport." Military Communications Conference, 2005. MILCOM 2005. IEEE. IEEE, 2005.

[18] Gisin, Nicolas, et al. "Quantum cryptography." Reviews of modern physics 74.1 (2002): 145.