IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Quantum Cryptography Enhancement of QKD EPR Protocol & Identity Verification

Rambabu Saini[*1], Shavita Shiwani[2]
Gyan Vihar School of Engineering and Technology, Jaipur, India
rambabusaini@outlook.com

Abstract

Today secure communications is increasingly more important to the intended communicators without being intercepted by eavesdroppers. Quantum cryptography promises to revolutionize secure communication which solves the key distribution problem in cryptographic system by providing a secure communication channel between two parties with high security guaranteed by the fundamental lows of the physics. Quantum cryptography provides the solution that uses property of polarization to ensure that transmitted data is not disturbed. Basic protocols for QKD provide maximum 25% (B92 protocol) and 50% (BB84 and EPR) idealized efficiency receptively, which is not enough for secure transmission of shared key. This work provides the mechanism that enhances the data security in quantum cryptography during exchange of information by increasing the size of shared key up to 75%. The identity verification mechanism tries to provide maximum success for user authentication. At the starting point detailed explanation of Quantum key distribution's EPR protocol is given. Using the EPR method, Alice and Bob could potentially store the prepared entangled particles and then measure them and create the key just before they were going to use it, eliminating the problem of insecure storage. In the Next phase, proposed mechanism is described. The proposed mechanism combines EPR protocol at two stages, (1) from sender to receiver and then (2) from receiver to sender. Doubling EPR protocol enhances information reconciliation as well as privacy amplification. In future the proposed mechanism will be very beneficial where unconditional security is required during key and other secret information exchange.

Keywords: Quantum cryptography, Quantum key distribution, BB84 algorithm, EPR algorithm, Identity verification.

Introduction

Quantum cryptography allows one to distribute a secret key between two remote parties using the fundamental principles of quantum mechanics. Quantum Cryptography is the composition of two words: Quantum and Cryptography. Quantum is the smallest and individual discrete unit of some physical property that a system can possess and Cryptography is the science, which enables to store private data or transmit it across insecure communication channel. The purpose of quantum cryptography is to transmit information such that only the intended recipient receives it. So, Quantum Cryptography is the mechanism, which uses quantum for doing cryptographic process. Quantum Cryptography uses conventional cryptographic approaches or methods and enhances these through the use of quantum effects of particular entity. Quantum Key Distribution (QKD) is used in quantum cryptography for producing a secure key, which is shared between two parties using a quantum channel, and an authentication is done by classical channel. The private/secure key obtained and used to cipher messages that are sent over an insecure classical channel.

Conventional Cryptographic security depends upon how complex a mathematical problem is to solve. In today's high performance computers era with the advent of reliable technologies these complex mathematical problems can be easily estimated. As the result security level reduces. Modern cryptosystem uses Quantum Cryptography, which provides unmatchable security of the key using quantum mechanics. For example: Heisenberg's Uncertainty Principle, Wave/Particle duality, Qubits and No cloning theorem. Heisenberg's Uncertainty principle states that the more precisely one property is measured, the less precisely the other can be

measured. Using this principle Quantum Cryptography successfully provides unconditional security. The concept of Wave/Particle duality is being used in photon polarization. A qubit or quantum bit is a smallest unit of quantum information. Like a bit, a qubit can have values 0 or 1, a qubit can retain supEPR osition state of these two bits. The no cloning theorem implies that a possible eavesdropper cannot intercept measure and reemit a photon without introducing a significant and detectable error in the reemitted signal. Thus, it is possible to build a system that allows two parties, the sender and the receiver, commonly called "Alice" and "Bob", to interchange information and detect where the communication channel has been tempered. The key obtained using quantum cryptography can then be used with any chosen encryption algorithm to encrypt a message, which can be transmitted over a standard communication channel. Once the secret key using Quantum Cryptography is established, it can be used together with classical cryptographic techniques such as the one-time-pad to allow the parties to communicate meaningful information in absolute secrecy.

Quantum Key Distribution

Light waves are electromagnetic waves which can show the phenomenon of polarization, in which the direction of the electric field vibrations is constant or varies in some definite way. A polarization filter is a material that allows only light of a specified polarization direction to pass. Information about the photon's polarization can be determined by using a photon detector to determine whether it passed through a filter. In other words photon is a quantum object, and in the quantum world an object can be considered to have a property only after you have measured it, and the type of measurement impacts the property that you find the object to have. In quantum key distribution, any attempt of an eavesdropper to obtain the bits in a key not only fails, but gets detected as well. Specifically, each bit in a key corresponds to the state of a particular particle, such as the polarization of a photon – named quantum bit (qbit).

The sender of a key has to prepare a sequence of polarized photons - qbits, which are sent to the receiver through an optical fiber channel. In order to obtain the key represented by a given sequence of photons, the receiver must make a series of measurements using a set of polarization filters.
A photon can be polarized rectilinear (0^o, 90^o), diagonal (45^o, 135^o) and circular (left - spinL, right - spinR).

The process of mapping a sequence of bits to a sequence of rectilinearly, diagonally or circularly polarized photons are referred to as conjugate coding**,** while the rectilinear, diagonal and circular polarization is known as conjugate variables. Quantum theory suggests that it is impossible to measure the values of any pair of conjugate variables simultaneously due to Heisenberg's principle of uncertainty. The same impossibility applies to rectilinear, diagonal and circular polarization for photons. For example, if someone tries to measure a rectilinearly polarized photon with respect to the diagonal, all information about the previous "property" of rectilinear polarization of the photon vanished.

BB84 Algorithm of QKD

BB84 is the first known quantum key distribution scheme, named after the original paper by Bennett and Brassard, published in 1984. It allows two parties; as standard convention that Alice as sender and Bob as receiver, to establish a secret shared key using polarized photons - qbits. Eve is presented as eavesdropper. The steps of the algorithm are explained below:

1. Alice generates a random binary sequence *S*.
2. Alice chooses which type of photon to use (rectilinearly polarized, "R", or circularly polarized, "X") in order to represent each bit in S. Let b denotes the sequence of each polarization base.
3. Alice uses specialized equipment, including a light source and a set of moralizer's to create a sequence p of polarized photons - qbits whose polarization directions represent the bits in *S*.
4. Alice sends the qbits p to Bob over an optical fiber.
5. For each qbit received, Bob makes a guess of which base is polarized: rectilinearly or diagonally, and sets up his measurement device accordingly. Let b' denote his choices of basis.
6. Bob measures each qbit with respect to the basis chosen in step 5, producing a new sequence of bits *S*'.
7. Alice and Bob communicate over a classical, possibly public channel. Specifically, Alice tells Bob the choice of basis for each bit, and Bob tells Alice whether he made the same choice. The bits for which Alice and Bob have used different bases are discarded from *S* and *S'*.
8. They convert the remaining data to a string of bits using a convention such as:

Left-circular = 0, Right-circular = 1
Horizontal = 0, vertical = 1

EPR Algorithm of QKD

Another protocol proposed by Einstein, Podolsk, and Rosen (EPR) is EPR protocol for Quantum Key Distribution. In their proposal they challenged the foundations of quantum mechanics by pointing out a paradox to take advantage of EPR correlations. According to the paradox, particles are prepared in such a way that they are "entangled". This means that although large distances in space may separate them, they are not independent of each other. Their states are associated in such a way that the measurement of a chosen variable *A* of one automatically determines the result of the measurement of *A* of the other. Suppose the entangled particles are photons. If one of the particles is measured according to the circular basis and found to have a left-circular polarization, then the other particle will also be found to have a left-circular polarization if it is measured according to the circular basis. If however, the second particle is measured according to the rectilinear basis, it may be found to have either vertical or horizontal polarization. Using the EPR correlation of "entangled" photons a protocol for developing secret key is explained below:

1. Alice generates a random binary sequence *S*.
2. Alice creates EPR pairs of polarized photons for each bit, keeping one particle for herself and sending the other particle of each pair to Bob.
3. Alice randomly measures the polarization of each particle she kept according to the rectilinear (+) or circular (X) basis. She records each measurement type and the polarization measured.
4. Bob randomly measures each particle he received according to the rectilinear (+) or circular (X) basis. He records each measurement type and the polarization measured providing a new sequence *S'*.
5. Alice and Bob tell each other which measurement types were used, and they keep the data from all particle pairs where they both chose the same measurement type form *S* and *S'*.
6. They convert the matching data to a string of bits using a convention such as:
   Left-circular = 0, Right-circular = 1
   Horizontal = 0, vertical = 1

Related work

A research paper published by Ching-Nung Yang and Chen-Chin Kuo, Department of Computer Science & Information Engineering, National Dong Hwa University, Republic of China which shows the combined BB84 protocol and B92 protocols and B92 and B92 protocols twice for improving the efficiency and performance. A brief description of their research work is given as follows:

In that well known paper they introduced two new enhanced protocols using base protocols of QKD as:

1. First Enhanced Quantum Key Distribution protocol (FEQKD) in which one four state BB84 protocol and the other two states B92 protocol is combined (BB84 + B92).
2. Second Enhanced Quantum Key Distribution protocol (SEQKD) in which both two state protocols i.e. B92 is combined with B92 protocol during transmission from Alice to Bob and then from Bob to Alice.

They calculated the idealized maximum efficiency 42.9% and the complexity order 2.86 for FEQKD. It has better efficiency and a little complexity than B92 protocol, but when compared with BB84 protocol it has simpler complexity and a little less efficiency. For SEQKD protocol they used B92 protocol and were successful in enhancing the efficiency for B92 protocol by adding extra steps. For FEQKD and SEQKD protocols they use the information when Bob chooses the wrong detector's basis; however the information is discarded in original BB84 protocol.

I have forwarded this concept of combining or doubling QKD EPR protocol to enhance the security level.

Proposed technique

In the proposed technique I am taking EPR protocol as the base and the technique using the EPR protocol two times (1) from Alice to Bob and (2) Bob to Alice.

First stage (data transmission is done from Alice to Bob)

1. Alice generates a binary string (1011010110101101) that is to be sent to Bob as secret key.
2. Alice prepares EPR pairs of polarized photons for each bit of string. She keeps one particle for herself and sends other particle to Bob of each pair.
3. Alice randomly measures the polarization of each particle she kept according to the rectilinear (+) or circular (X) basis. She

records each measurement type and the polarization measured.

4. Bob randomly measures particle he received according to the rectilinear (+) or circular (X) basis. He records each measurement type and the polarization measured.
5. Alice and Bob tell each other which measurement types were used, and they keep the data from all particle pairs where they both chose the same measurement type.
6. They convert the matching data to a string of bits using a convention such as:

   Left-circular = 0, Right-circular = 1
   Horizontal = 0, vertical = 1

Here the first stage of EPR protocol is over. As the result Alice and Bob gets a shared key that is common for both of them. Below table shows all the steps involved in the first stage.

First stage (Transmission from Alice to bob)																
Binary sequence from Alice	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**1**
Alice measurement types at random choice	**X**	**+**	**X**	**+**	**X**	**X**	**+**	**+**	**+**	**X**	**X**	**X**	**+**	**X**	**+**	**+**
Polarization of photon's measured by Alice	**R**	**H**	**R**	**H**	**L**	**R**	**V**	**V**	**H**	**R**	**R**	**L**	**H**	**L**	**V**	**H**
Measurement made by Bob	**X**	**+**	**+**	**+**	**+**	**X**	**X**	**X**	**+**	**X**	**+**	**+**	**X**	**X**	**X**	**+**
Polarization of photon's measured by Bob	**R**	**H**	**V**	**H**	**V**	**R**	**L**	**R**	**H**	**R**	**V**	**V**	**R**	**L**	**R**	**H**
Bob publicly tells Alice which type of measurement he made on each photon	**X**	**+**	**+**	**+**	**+**	**X**	**X**	**X**	**+**	**X**	**+**	**+**	**X**	**X**	**X**	**+**
Alice publicly tells Bob which measurements were the correct type	**Y**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**N**	**Y**	**Y**	**N**	**N**	**N**	**Y**	**N**	**Y**
Alice and Bob each keep the data from correct measurements and convert to binary	**1**	**0**		**0**		**1**			**0**	**1**				**0**		**0**

Figure 1: The string of bits owned by Alice and Bob is: 1 0 0 1 0 1 0 0. This string of bits will be used in next stage to form a perfect secure key. In practice, the number of photons sent and the resulting length of the string of bits would be much greater. The idealized maximum efficiency provided by 1st stage is 50% for EPR protocol.

Second stage (data transmission is done from Bob to Alice)

With the Completion of first stage Bob gets 8 bits matched out of 16 bits. As the proposal of the new technique if we want to enhance security of the shared key, need to increase the number of bit in matching. So in second stage EPR protocol is used for information reconciliation, which increases the

size of shared key. There for only those bits that did not match are processed in second stage as follows:

1. Bob randomly measures the polarization of each bit those were canceled at first stage, according to the rectilinear (+) or circular (X) basis. He records each measurement type and the polarization measured.
2. Alice randomly measures each bit he received according to the rectilinear (+) or circular (X) basis. She records each measurement type and the polarization measured.
3. Alice and Bob tell each other which measurement types were used, and they keep the data from all particle pairs where they both chose the same measurement type.
4. They convert the matching data to a string of bits using a convention such as:
   Left-circular = 0, Right-circular = 1
   Horizontal = 0, vertical = 1

Below table shows all the steps involved in the 2nd stage.

Second stage (Transmission from Bob to Alice)																
Bob's measurement types at random choice only for each bit those were canceled at first stage			+		+		X	+			X	X	+		X	
Polarization of photon's measured by Bob			H		V		R	V			R	L	H		R	
Measurement made by Alice at random choice			+		X		X	X			X	+	+		+	
Polarization of photon's measured by Alice			H		R		R	L			R	V	H		H	
Alice publicly tells Bob which type of measurement he made on each photon			+		X		X	X			X	+	+		+	
Bob publicly tells Alice which measurements were the correct type			Y		N		Y	N			Y	N	Y		N	
Alice and Bob each keep the data from correct measurements and convert to binary			0				1				1		0			

Shared Key through 1st round	**1**	**0**		**0**		**1**			**0**	**1**				**0**		**0**
Final shared Key	**1**	**0**	**0**	**0**		**1**	**1**		**0**	**1**	**1**		**0**	**0**		**0**

Figure 2: After completion of second stage the matching bits are added with the 1st stages shared key. So finally Alice and Bob get a shared key of 12 bits, which is larger then the first stage. Here probably 12 bits are matched out of 16 bits. The 2nd stage provides 25% ideal efficiency of the total photons transferred. Finally String of bits owned by Alice and Bob is: 10 0 0 1 1 0 1 1 0 0 0. This string of bits forms the secret key.

Identity Verification

Even though every quantum key distribution protocol (mostly BB84 and EPR) provides more secure exchange of shared secret key but still communicators needs to be authenticated. Indeed, authentication is much demanded to the security of QKD otherwise it is easy to perform a man-in-the-middle attack. Authentication may be achieved by public key authentication and symmetric key authentication. Symmetric key authentication can provide unconditionally secure authentication, but at the cost of needing to have pre-established pairs of symmetric keys. Public key authentication, on the other hand, is simpler to deploy, and provides extraordinarily convenient distributed trust when combined with certificate authorities (CAs) in a public key infrastructure (PKI). Public key authentication cannot itself be achieved with information theoretic security.

A third method for authentication is to use trusted third parties which actively mediate authentication between two unauthenticated parties, but there has been little interest in adopting these in practice. Certificate authorities, who are used in public key authentication, are similar to trusted third party authentication but do not actively mediate the authentication: they distribute signed public keys in advance but then do not participate in the actual key authentication protocol. The difference in trust between trusted third parties and certificate authorities for authentication in QKD is smaller than in the purely classical case since the key from QKD is independent of the inputs.

In this proposed protocol, I am highlighting symmetric key authentication with enhanced mechanism, which potentially can provide unconditionally secure authentication during quantum key distribution. Two steps involved in the proposed technique, those are as follows-

Initial phase

Assuming the information center is legitimate and believable. The information center is responsible neither for mutual authentication nor for the generation of quantum keys. The role of this center is to simply help the legitimate user to obtain the authenticated quantum channel by registering themselves with the information center. Here, I assume that both the communicators are registered with the information center with their unique ID's. Initial phase involves few steps as follows:

1. Alice and Bob send their ID's, making a request to establish secure connection between them. (ID_A for Alice and ID_B for Bob were assigned by information center at the time of registration)
2. The information center applies public key authentication scheme to validate them as legal users using public key infrastructure. If public key authentication successes, information center generates a random numbers different unique KEY POOL encrypted by user's private key and sends to Alice and Bob. KP_A belongs to Alice and KP_B belongs to Bob.
   (A) If it is first time communication ever between Alice and Bob, information center exchanges a copy of these KEY Pools to each other. (It means Alice knows about KP_B and Bob knows about KP_A after KEY POOL exchange) and establishes quantum communication channel between then.
   (B) Else establishes quantum communication channel without KEY POOL exchange between then.

Mutual Authentication

Mutual authentication phase involves few stages as follows-

1. Alice publicly asks to Bob a key from POOL $KP_{B.}$ Bob matches it in $KP_{A,}$ if key not found transmission is discarded.
2. Bob asks to Alice a key from POOL KP_A. Alice matches it in KP_B, if key not found transmission is discarded.
3. Again Alice asks to Bob another key from POOL $KP_{B.}$ Bob matches it, if key not found transmission is discarded else it comes to know that there is no eavesdropper in between them. Mutually 100% user authentication is done because only Alice and Bob know keys from their respective POOL.
4. Alice and Bob must discard copy of KEY POOL which was exchanged between them. Refresh the original KEY POOL with new quantum distributed keys those were generated by (first half, second half and addition of these keys) proposed protocol (EPR+EPR). Alice and Bob only know those keys; mutual authentication may be achieved with higher success in next transmission.

Security Analysis

Conventional communication channel may be intercepted by eavesdroppers and may reveal Alice's signal correctly and can resend the same copy of signal to Bob. It is, however, probably impossible to intercept/resend the communication in quantum channel. If Eve tries to intercepts the quantum channel, there will be a large bit error rate in their shared key. In that case Alice and Bob need to discard their shared key.

In 1st stage, the security remains as the same as EPR protocol. If Bob chooses the correct basis, then he will detect the correct polarized photon. However, if Bob chooses the wrong basis, he knows that his result is inconclusive. So the idealized maximum efficiency is 50% for EPR protocol. It means 50% of the shared key is known by Eve. The proposed technique works here to enhance idealized maximum efficiency about to 75% (50% from 1st stage +25% from 2nd stage) of the total photons transferred for establishing shared secret key, which is good enough. In 2nd stage, Eve does not know which source bases Bob chooses in the positions where his measurement results are "N" in 1st stage, because Bob may detect nothing when choosing the wrong or even correct bases. The proposed identity verification mechanism can easily authenticate valid communicators. We can also add error detecting and correcting codes into our enhanced QKD protocols.

Conclusion

The proposed technique uses EPR protocol in two stages to improve EPR protocol. The new protocol has the idealized maximum efficiency near about to 75%, which is better than previous EPR protocol. This proposal uses the information when Bob chooses the wrong detector's basis; however the information is discarded in the original EPR protocol.Security analysis shows that original EPR protocol provides 50% maximum idealized efficiency but the enhanced technique comparatively provides 75% maximum ideal efficiency which means proposed technique increases the ideal efficiency to 25%.

References

[1] C.H. Bennet and G. Brassard, "*Quantum cryptography: public key distribution and coin tossing*", Proceedings of *IEE International Conference on Computers*, Systems and Signal Processing, Bangalore, India, pp.175-179, Dec. 1984.

[2] C.H. Bennet, "*Quantum cryptography using any two non-orthogonal states*", Physical Review Letters, Vol. 68, pp.3121-3124, May 1992.

[3] C.H. Bennet, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "*Experimental quantum cryptography*", Journal of cryptology, Vol. 5, pp. 3-28, 1992.

[4] G. Brassard and L. Salvail "*Secret key reconciliation by public discussion*" Advances in Cryptology: Eurocrypt 93 Proc. pp 410-23, 1993.

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "*Quantum cryptography*," Rev. Mod. Phys.74, pp145–195, 2002.

[6] C. Gobby, Z. L. Yuan and A. J. Shields, "*Quantum key distribution over 122 km telecom fiber*," Appl. Phys. Lett. 84, pp 3762–3764 2002.

[7] D. Gottesman, H. K. Lo, N. L¨utkenhaus and J. Preskill, "*Security of quantum key distribution with imperfect devices*," Quant. Inf. Comput. 4,pp 325–360, 2004.

[8] Ching-Nung Yang, Chen-Chin Kuo, "*Enhanced Quantum Key Distribution Protocols Using BB84 and B92*".

[9] Gerald Scharitzer, "*Basic Quantum Cryptography*" Vienna University of Technology, Institute of Automation.

[10] A. K.Ekert, "*Quantum cryptography based on Bell's theorem*", Physical Review Letters, vol. 67, no. 6, 5 August 1991, pp. 661 - 663. A.K.Ekert,

J.G.Rarity, P.R.Tapster, and G.M.Palma, Practical quantum cryptography based on two-photon interferometry, Phys. Rev. Lett. 69, 1293(1992).