(IJIASE) 2018, Vol. No. 4, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

QUANTUM CRYPTOGRAPHY – EXPLORING THE APPLICABILITY OF BB84 AND EPR ALGORITHMS IN ENHANCING THE QKD

Divyashi Agrawal
Bhartiyam Vidya Niketan, Gwalior

ABSTRACT

Today secure communications are increasingly more important to the intended communicators without being intercepted by eavesdroppers. Quantum cryptography promises to revolutionize the key distribution problem in cryptographic system by providing a secure communication channel between two parties with high security guaranteed by the fundamental laws 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 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 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 enables one to disseminate a mystery key between two remote gatherings utilizing the key standards of quantum mechanics. Quantum Cryptography is the creation of two words: Quantum and Cryptography. Quantum is the littlest and individual discrete unit of some physical property that a framework can have and Cryptography is the science, which empowers to store private information or transmit it crosswise over uncertain correspondence station. The reason for quantum cryptography is to transmit data with the end goal that just the planned beneficiary gets

it. In this way, Quantum Cryptography is the system, which utilizes quantum for doing cryptographic process. Quantum Cryptography utilizes traditional cryptographic methodologies or techniques and improves these through the utilization impacts of specific substance. Quantum Key Distribution (QKD) is utilized in quantum cryptography for delivering a safe key, or, in other words two gatherings utilizing a quantum channel, and a validation is finished by established channel. The private/secure key acquired and used to figure messages that are sent over an unreliable established channel. Customary Cryptographic security relies on how complex a numerical issue is to illuminate. In the present elite PCs period with the appearance of solid advancements these complex numerical issues can be effectively assessed. As the outcome security level diminishes. Current cryptosystem utilizes Quantum Cryptography, which gives unmatchable security of the key utilizing quantum mechanics. For instance: Uncertainty Principle, Wave/Particle duality, Qubits and No cloning hypothesis. Heisenberg's Uncertainty standard expresses that the more decisively one property is estimated, the less definitely the other can be estimated. Utilizing this rule Quantum Cryptography effectively gives unqualified security. The idea of Wave/Particle duality is being utilized in photon polarization. A qubit or quantum bit is a littlest unit of quantum data. Like a bit, a qubit can have values 0 or 1, a qubit can hold dinner position condition of these two bits. The no cloning hypothesis infers that a conceivable meddler can't block measure and reemit a photon without presenting a huge and recognizable blunder in the reemitted flag. Along these lines, it is conceivable to fabricate a framework that permits two gatherings, the sender and the recipient, normally called "Alice" and "Bounce", to exchange data and recognize where the correspondence channel has been tempered. The key acquired utilizing quantum cryptography would then be able to be utilized with any picked encryption calculation to scramble a message, which can be transmitted over a standard correspondence channel. When the mystery key utilizing Quantum Cryptography is set up, it tends to be utilized together with traditional cryptographic systems, for example, the one-time-cushion to enable the gatherings to impart important data in supreme mystery.

QUANTUM KEY DISTRIBUTION

Light waves are electromagnetic waves which can show the phenomenon of polarization, in which the course of the electric field vibrations is consistent or fluctuates in some distinct way. A polarization channel is a material that permits just light of a predefined polarization course to pass. Data about the photon's polarization can be controlled by utilizing a photon finder to decide if it went through a channel. At the end of the day, the photon is a quantum question, and in the quantum world a protest can be considered to have a property simply after you have estimated it, and the kind of estimation impacts the property that you discover the question have. In quantum key conveyance, any endeavor of a meddler to get the bits in a key flops, as well as gets recognized also. In particular, each piece in a key compares to the condition of a specific molecule, for example, the polarization of a photon – named quantum bit (qbit). The sender of a key needs to set up a succession of captivated

photons - qbits, which are sent to the recipient through an optical fiber channel. With the end goal to acquire the key spoken to by a given succession of photons, the recipient must make a progression of estimations utilizing an arrangement of polarization channels. A photon can be energized rectilinear (0o, 90o), askew (45o, 135o) and roundabout (left - spinL, right - spinR). The way toward mapping a succession of bits to a grouping of rectilinearly, corner to corner or circularly energized photons are alluded to as conjugate coding, while the rectilinear, askew and round polarization is known as conjugate factors. Quantum hypothesis recommends that it is difficult to quantify the estimations of any match of conjugate factors at the same time because of Heisenberg's guideline of vulnerability. A similar difficulty applies to rectilinear, corner to corner and round polarization for photons. For instance, in the event that somebody attempts to quantify a rectilinearly enraptured photon as for the slanting, all data about the past "property" of rectilinear polarization of the photon vanished. BB84 Algorithm of QKD BB84 is the principal known quantum key appropriation plot, named after the first paper by Bennett and Brassard, distributed in 1984. It permits two gatherings; as standard tradition that Alice as sender and Bob as beneficiary, to build up a mystery shared key utilizing captivated photons - qbits. Eve is introduced as spy. The means of the calculation are clarified underneath:

1. Alice creates an irregular parallel arrangement S.
2. Alice picks which sort of photon to utilize (rectilinearly enraptured, "R", or circularly captivated, "X") with the end goal to speak to each piece in S. Let b indicates the arrangement of every polarization base.
3. Alice utilizes particular gear, including a light source and an arrangement of moralizer's to make a grouping p of captivated photons - qbits whose polarization bearings speak to the bits in S.
4. Alice sends the qbits p to Bob over an optical fiber.
5. For each qbit got, Bob makes a figure of which base is enraptured: rectilinearly or corner to corner, and sets up his estimation gadget appropriately. Give b' a chance to signify his decisions of premise.
6. Bounce estimates each qbit as for the premise picked in stage 5, delivering another grouping of bits S'.
7. Alice and Bob impart over a traditional, conceivably open channel. In particular, Alice discloses to Bob the decision of reason for each piece, and Bob reveals to Alice whether he settled on a similar decision. The bits for which Alice and Bob have utilized diverse bases are disposed of from S and S'.
8. They convert the rest of the information to a series of bits utilizing a tradition, for example,

Left-round = 0, Right-roundabout = 1

Even = 0, vertical = 1

EPR ALGORITHM OF QKD

Another convention proposed by Einstein, Podolsk, and Rosen (EPR) will be EPR convention for Quantum Key Distribution. In their proposition, they tested the establishments of quantum mechanics

by indicating out a conundrum exploit EPR connections. As per the mystery, particles are set up so that they are "trapped". This implies albeit substantial separations in space may isolate them, they are not autonomous of one another. Their states are related so that the estimation of a picked variable An of one naturally decides the aftereffect of the estimation of An of the other. Assume the entrapped particles are photons. In the event that one of the particles is estimated by the roundabout premise and found to have a left-roundabout polarization, at that point the other molecule will likewise be found to have a left-round polarization on the off chance that it is estimated by the roundabout premise. Assuming, be that as it may, the second molecule is estimated by the rectilinear premise, it might be found to have either vertical or even polarization. Utilizing the EPR relationship of "ensnared" photons a convention for creating mystery key is clarified underneath:

1. Alice produces an arbitrary paired grouping S.

2. Alice makes EPR sets of enraptured photons for each piece, keeping one molecule for herself what's more, sending the other molecule of each combine to Bob.

3. Alice arbitrarily measures the polarization of every molecule she continued as indicated by the rectilinear (+) or round (X) premise. She records every estimation composes and the polarization estimated.

4. Sway haphazardly measures every molecule he got by the rectilinear (+) or roundabout (X) premise. He records every estimation compose and the polarization estimated giving another succession 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 = 1Horizontal = 0, vertical = 1

RELATED WORK

An examination paper distributed by Ching-Nung Yang and consolidated BB84 convention and B92 conventions and B92 and B92 conventions twice to enhance the productivity and execution. A concise portrayal of their examination work is given as pursues: In that outstanding paper they presented two new improved conventions utilizing base conventions of QKD as:

1. First Enhanced Quantum Key Distribution convention (FEQKD) in which one four state BB84 convention and the other two states B92 convention is joined (BB84 + B92).

2. Second Enhanced Quantum Key Distribution convention (SEQKD) in which both two state conventions i.e. B92 is joined with B92 convention amid transmission from Alice to Bob and after that from Bob to Alice. They ascertained the glorified most extreme proficiency 42.9% and the multifaceted nature arrange 2.86 for FEQKD. It has better proficiency and a little multifaceted nature than B92 convention, however when contrasted and BB84 convention it has less difficult intricacy and somewhat less effectiveness. For SEQKD convention they utilized B92 convention and were fruitful in upgrading the proficiency for B92 convention by including additional means. For FEQKD and SEQKD conventions they utilize the data when Bob picks the wrong indicator's premise; be that as it may, the data is disposed of in unique BB84 convention.

PROPOSED TECHNIQUE

In the proposed method I am accepting EPR convention as the base and the procedure utilizing the EPR convention 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 arbitrarily measures molecule he got by the rectilinear (+) or round (X) premise. He records every estimation composes and the polarization estimated.
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 = 1Horizontal = 0, vertical = 1Here 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. By and by, the quantity of photons sent and the subsequent length of the series of bits would be substantially more noteworthy. The glorified most extreme proficiency given by first stage is half for EPR convention.

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 arbitrarily measures the polarization of each piece those were dropped at the first stage, as per the rectilinear (+) or round (X) premise. He records every estimation composes and the polarization estimated.

(IJIASE) 2018, Vol. No. 4, Jan-Dec **e-ISSN: 2454-9258, p-ISSN: 2454-809X**

2. Alice arbitrarily measures each piece he got by the rectilinear (+) or round (X) premise. 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 = 1Horizontal = 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			

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 12bits, which is larger than 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 series of bits shapes the mystery 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 open key verification and symmetric key validation. Symmetric key validation can give unequivocally anchor confirmation, yet at the expense of needing pre-built up sets of symmetric keys. Open key validation, then again, is less complex to send, and gives remarkably helpful conveyed trust when joined with declaration experts (CAs) in an open key framework (PKI). Open key verification can't itself be accomplished with data theoretic security.

A third technique for validation is to utilize confided in outsiders which effectively intercede verification between two unauthenticated parties, however there has been little enthusiasm for embracing these by and by. Endorsement experts, who are utilized out in the open key confirmation, are like confided in outsider verification however don't effectively intervene the validation: they disperse marked open keys ahead of time yet then don't take an interest in the genuine key confirmation convention. The distinction in trust between confided in outsiders and endorsement specialists for confirmation in QKD is littler than in the simply traditional case since the key from QKD is free of the information sources. In this proposed convention, I am featuring symmetric key confirmation with upgraded component, which conceivably can give unequivocally anchor verification amid quantum key circulation. Two stages engaged with the proposed method, those are as per the following-

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 job of this middle is to just assist the real client with obtaining the confirmed quantum channel by enrolling 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. (IDA for Alice and IDB 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. KPA has a place with Alice and KPB has a place with Bob. (An) If it is first-time

correspondence ever among Alice and Bob, data focus trades a duplicate of these KEY Pools to one another. (It implies Alice thinks about KPB and Bob thinks about KPA after KEY POOL trade) and sets up quantum correspondence channel between at that point. (B) Else sets up quantum correspondence channel without KEY POOL trade between at that point.

Mutual Authentication

Mutual authentication phase involves few stages as Follows

1. Alice publicly asks to Bob a key from POOL KPB. Bob matches it in KPA, if key not found transmission is discarded.
2. Bob asks to Alice a key from POOL KPA. Alice matches it in KPB, if key not found transmission is discarded.
3. Again Alice asks to Bob another key from POOL KPB. Bob matches it; if key not found transmission is discarded else it comes to know that there is no eavesdropper in between them. Commonly 100% client confirmation is done on the grounds that just Alice and Bob know keys from their particular POOL.
4. Alice and Bob must discard copy of KEYPOOL which was exchanged between them.

Revive the first KEY POOL with new quantum circulated keys those were created by (first half, second half and expansion of these keys) proposed convention (EPR+EPR). Alice and Bob just know those keys; shared verification might be made with higher progress in next transmission.

SECURITY ANALYSIS

Customary correspondence channel might be caught by busybodies and may uncover Alice's flag effectively and can resend a similar duplicate of flag to Bob. It is, be that as it may, most likely difficult to capture/resend the correspondence in quantum channel. In the event that Eve endeavors to blocks the quantum channel, there will be a substantial piece mistake rate in their mutual key. All things considered Alice and Bob need to dispose of their common key. In first stage, the security stays as the equivalent as EPR convention. In the event that Bob picks the right premise, at that point he will recognize the right captivated photon. Nonetheless, if Bob picks the wrong premise, he realizes that his outcome is uncertain. So the romanticized most extreme proficiency is half for EPR convention. It implies half of the common key is known by Eve. The proposed strategy works here to improve admired most extreme productivity going to 75% (half from first stage +25% from second stage) of the aggregate photons exchanged for setting up shared mystery key, or, in other words. In second stage, Eve does not know which source bases Bob picks in the positions where his estimation results are "N" in first stage, since Bob may distinguish nothing while picking the wrong or even right bases. The proposed personality confirmation component can without much of a stretch validate substantial communicators. We can likewise include blunder recognizing and adjusting codes into our upgraded QKD conventions.

CONCLUSION

The proposed technique uses EPR protocol in two stages to improve EPR protocol. The new protocol has the idealized maximum efficiency near about to75%, 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 provides75% maximum ideal efficiency which means proposed technique increases the ideal efficiency to25%.

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*", PhysicalReview Letters, Vol. 68, pp.3121-3124, May1992.

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

[4] G. Brassard and L. Salvail "*Secret keyreconciliation 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 kmtelecom fiber*," Appl. Phys. Lett. 84, pp3762–3764 2002.

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

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

[9] Gerald Scharitzer, "*Basic QuantumCryptography*" Vienna University ofTechnology, Institute of Automation.

[10] A. K.Ekert, "*Quantum cryptography based on Bell's theorem*",Physical Review Letters, vol. 67, no. 6, 5August 1991, pp. 661 - 663. A.K.Ekert,J.G.Rarity, P.R.Tapster, and G.M.Palma,
Practical quantum cryptography based ontwo-photon interferometry, Phys. Rev. Lett.
69, 1293(1992).

[11]R.Saini, Shavita ShiwaniIJESRT[Quantum Cryptography][432-439].