RESEARCH ARTICLE OPEN ACCESS

Third-Party Authentication Using Quantum Key Distribution Protocols

Kunal Mishra[1], Ashish Upadhyay[2], Prerna Gaur[3]

Department of Instrumentation & Control Netaji Subhas Institute of Technology India.

Abstract:

By using quantum motorized systems, Quantum key distribution (QKD) promises safe key conformity. For the opportunity cryptographic infrastructures, we argue that QKD will be an important part. Without reliance on computational assumptions QKD can give long-term discretion in favor of encrypted in cycle. QKD can make use of each information-theoretically confined symmetric key verification or computationally make safe public key confirmation, it still requires validation to prevent man-in-the-middle attacks; we argue that QKD still offers stronger refuge than classical key concurrence even when it uses public key certification. Secure group announcement could began speedily by Dynamic peer group. By establishing a collaborative assembly key for a disseminated dynamic peer group that provides a elementary understanding is the foremost aspect. The third party regarding the validation part were trusted by the Participants of the etiquette. The network systems which deal with highly sensitive in sequence, such as military, hospitals, research conveniences were preferred by the planned set of rules. In superposition states for authentication and key circulation which provides high security against many attacks were our protocol utilizes polarized photons.

Keywords :- **Third-Party ,Quantum Key ,Protocols.**

I. INTRODUCTION

Since its advance, the field of quantum cryptography — and in finicky, quantum key distribution (QKD) — has garnered regular technical and trendy concern. The promise of "unconditional security" has bring public notice, but the often uncontrolled brightness expressed for this ground has also spawned analysis and analysis. quantum key distribution protocols (QKD) to look after security in large p2p networks, with in new commands in classical cryptography and quantum cryptography. Two conciliator protocols, one with natural user certification and the other with explicit mutual certification, are proposed to present the merits of the new arrangement. The purpose of key delivery is for two users "Alice" and "Bob" , who break up no secret in sequence initially, to agree on a random key, which remains furtive from an adversary "Eve", who eavesdrops on their interactions. In classical cryptography, it is full for granted that transportation can always be without interest monitored, so that the eavesdropper learns their entire stuffing, without the sender or receiver person aware that any eavesdropping has taken place.

II. RELATED WORK

Quantum key delivery mainly depends on three algorithms; BB84, B92, E91, and EPR. Those protocols trade qubits over quantum direct and then apply probabilistic procedures to change the key bits succession. BB84 uses rectilinear and transverse bases to pass numbers from sender to recipient. The used bases are shown in equation B92 employs non-orthogonal bases to throw qubits to the receiving side. EPR uses one of the out of the ordinary quantum properties which is embarrassment to transfer data between parties. Two entangled states are shown in equation.

BB84:

It is a quantum key circulation scheme industrial by Charles Bennett and Gilles Brassard in 1984. It is the primary quantum cryptography practice. The protocol is provably secure, relying on the quantum possessions that in sequence gain is only possible at the outflow of disconcerting the signal if the two states one is trying to distinguish are not orthogonal (see no cloning theorem). It is usually explain as a method of strongly communicate a private key from one celebration to another for utilize in one-time pad encryption.

In the BB84 scheme, Alice requirements to send a private key to Bob. She begins with two string of bits, a and b, each n bits long. She then encodes these two string as a string of n qubits,

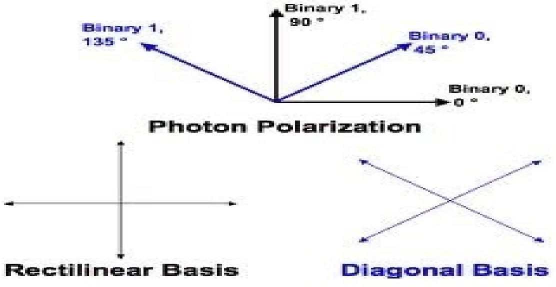
$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_ib_i}\rangle.$$

a_i and b_i are the i^{th} bits of a and b, respectively. Together, a_ib_i give us an index into the following four qubit states:

$$|\psi_{00}\rangle = |0\rangle$$
$$|\psi_{10}\rangle = |1\rangle$$
$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Note that the bit b_i is what decides which basis a_i is determined in (either in the computational basis or the Hadamard basis). The qubits are now in states which are not together orthogonal, and thus it is impracticable to distinguish all of them with confidence without knowing b.

Alice sends $|\psi\rangle$ over a public quantum channel to Bob. Bob receives a state $\varepsilon\rho = \varepsilon|\psi\rangle\langle\psi|$, where ε represents the effects of noise in the direct as well as eavesdropping by a third party we'll call Eve. After Bob receives the sequence of qubits, all three parties, namely Alice, Bob and Eve, have their own states. However, since only Alice knows b, it makes it virtually without a solution for either Bob or Eve to distinguish the states of the qubits. Also, after Bob has received the qubits, we know that Eve cannot be in ownership of a copy of the qubits sent to Bob, by the no cloning theorem, unless she has made dimensions. Her measurements, however, risk disturbing a particular qubit with probability ½ if she guesses the wrong basis.



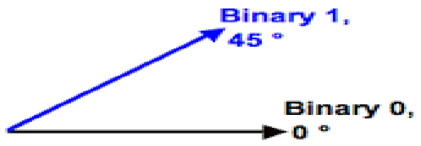
Photon Polarization
BB84 4 State Encoding

Bob earnings to generate a string of arbitrary bits b' of the same length as b, and then measures the string he has customary from Alice, a'. At this point, Bob announces in public that he has conventional Alice's communication. Alice then knows she can now safely announce b. Bob communicate over a community channel with Alice to agree on which b_i and b'_i are not equal. Both Alice and Bob now thrust aside the qubits in a and a' where b and b' do not equivalent.

From the remaining k bits where both Alice and Bob considered in the same basis, Alice accidentally chooses $k/2$ bits and discloses her choice over the community channel. Both Alice and Bob pronounce these bits freely and run a prove to see if more than a certain come to of them agree. If this check passes, Alice and Bob proceed to use privacy amplification and information reconciliation technique to create some number of shared secret keys. Otherwise, they cancel and create over.

B92:

B92 is essentially a easy version of BB84.In this practice quantum cryptography is apply using any two on on-orthogonal state. The key difference in B92 is that it only requirements two states rather than the four divergence states required in BB84. Like the BB84, Alice transmit a string of photons to Bob which she encoded with accidentally special bits. Now the bits chosen by Alice find out the base she has to use. Bob still accidentally chooses a basis by which to measure the bits but right basis selection absolutely remove the information and he will not measure any readings because of a provision in quantum mechanics called as an erasure. Bob simply informs Alice after being paid each bit, if he measured the bit acceptably or not. In this way they both find out the key to be used in secretly encoding the messages.



Photon Polarization
B92 2 State Encoding

E91 protocol:

The Ekert scheme uses knotted pairs of photons. These can be produced by Alice, by Bob, or by some resource detach from both of them, include eavesdropper Eve. The photons are strewn so that Alice and Bob each end up with one photon from each join up The scheme relies on two properties of embarrassment. First, the entangled states are faultlessly interconnected in the sense that if Alice and Bob both evaluate whether their particles have vertical or horizontal polarizations, they always get the same answer with 100% prospect. The same is true if they both evaluate any other pair of corresponding (orthogonal) polarizations. This necessitates that the two distant parties have exact directionality management. However, the finicky results are completely random; it is impossible for Alice to predict if she (and thus Bob) will get vertical polarization or horizontal divergence. Second, any attempt at eavesdropping by Eve destroys these correlation in a way that Alice and Bob can detect.

Similarly to BB84, the protocol involve a private measurement protocol before detecting the presence of Eve. The height stage involves Alice measuring each photon she receives using some basis from the set $Z_0, Z_{\frac{\pi}{8}}, Z_{\frac{\pi}{4}}$ while Bob chooses from $Z_0, Z_{\frac{\pi}{8}}, Z_{-\frac{\pi}{8}}$ where Z_θ is the $\{|\uparrow\rangle, |\downarrow\rangle\}$ basis rotated by θ. They keep their series of basis choices private until dimensions are finished. Two groups of photons are made: the first consists of photons considered using the same basis by Alice and Bob while the second contain all other photons. To detect eavesdropping, they can multiply the test statistic S using the correlation coefficients between Alice's bases and Bob's similar to that shown in the Bell test experiments. Maximally entangled photons would result in $|S| = 2\sqrt{2}$. If this were not the case, then Alice and Bob can conclude Eve has introduced local realism to the system, violate Bell's Theorem. If the protocol is successful, the first group can be used to breed keys since those photons are completely anti-aligned between Alice and Bob.

III. PROPOSED ALGORITHM

In this paper, we intend a three-party key supply protocol. Alice and Bob want to steadily correspond with each other and require a secret key to secure their communicate channel from a trust third party. In protocol such as BB84 and B92, the correspondent and the beneficiary are not able to know the furtive key until the last step when they finish the link of their bases. When a third party is introduce, BB84 and B92 cannot be applied since there is no machinery to precisely give out the same key to various parties. In our projected protocol we are in view of how to involve three or more parties in the key delivery process.

<u>User Authentication and Quantum Bases distribution</u>

1- Alice requests to have a connection with Bob

$$Alice \rightarrow QKD: E_{PR\text{-}Alice}\,(ID_{Alice} \,||\, ID_{Bob})$$

QKD will register the connection request status in log file and check the ID of Alice for user Authentication. Moreover, QKD checks Bob's ID status (Busy, Free). If Bob is free, QKD moves to step 2.

2- QKD sends to Bob a connection request containing Alice's request

$$QKD \rightarrow Bob: E_{PU\text{-}Bob}\,(ID_{Alice} \,||\, ID_{Bob})$$

3- When Bob reply by accepting the connection with Alice, Bob will send to QKD a confirmation message

$$Bob \rightarrow QKD: E_{PR\text{-}Bob}\,(ID_{Alice} \,||\, ID_{Bob})$$

QKD decrypts the message and adds connection's status Between Alice and Bob and both of them are authenticated to send and receive data.

4- QKD starts distributing quantum bases (+,X) in some Sequence to encode the message to Alice and Bob in an encrypted message using their public keys.

4. 1 $QKD \rightarrow Alice: E_{PU\text{-}Alice}(ID_{Alice} \,||\, ID_{Bob} \,||\, QB).$

4. 2 $QKD \rightarrow Bob: E_{PU\text{-}Bob}(ID_{Alice} \,||\, ID_{Bob} \,||\, QB).$

<u>Data Transfer over Quantum channel</u>

5- After Alice and Bob receive the quantum bases from QKD, Alice sends an encrypted message using the quantum bases to Bob

$$Alice \rightarrow Bob: E_{PR\text{-}Alice}(E_{QB}(M)||E_{PU\text{-}Bob}(ID_{Alice}))$$

6- Bob and Alice send a random part of the message to QKD by using Private Key of sender(Alice, Bob).

$$Bob \rightarrow QKD: E_{PR\text{-}Bob}(E_{QB}(M)||E_{PU\text{-}QKD}(ID_{Bob}))$$
$$Alice \rightarrow QKD: E_{PR\text{-}Alice}(E_{QB}(M)||E_{PU\text{-}QKD}(ID_{Alice}))$$

QKD can decrypt the messages and compare between them. If there are any mismatching bits, then QKD concludes that there is an intruder.

7- QKD sends notification messages to Alice and Bob to *inform them there is an intruder or not.*

$$QKD \rightarrow Bob: E_{PU\text{-}Bob}(E_{QB}(Notify))$$
$$QKD \rightarrow Alice: E_{PU\text{-}Alice}(E_{QB}(Notify))$$

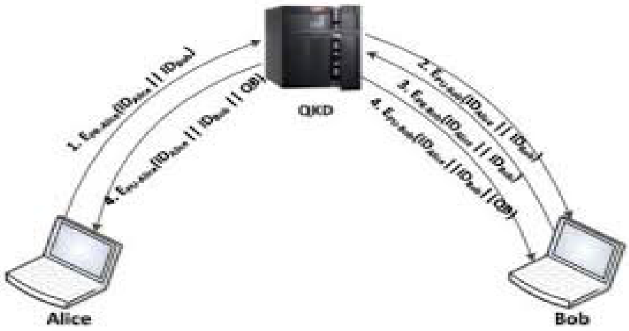
Our specific aim is to progress key distribution organism by apply some classical concepts and quantum techniques. By apply public key concept, we can enhance addict authentication and data reliability process. The anticipated algorithm achieves a high percentage of the approved bases. Moreover, we don't need the material channel to check the Qubits string where the quantum bases are mutual by using asymmetric key distribution centre.

The proposed algorithm consists of two phases:

1. User Authentication & Quantum Bases distribution

2. Data Transfer over the Quantum channel

In order for Alice and Bob to obtain a conference key, they perform more than steps take place involving the three parties.



User Authentication and Quantum Bases distribution

If the Notify communication is Okay, the relation will be alive until QKD sends any error announcement or Alice stops sending. In the wished-for protocol, we improve protection over the quantum channel. Each message is legitimate by the sender using its private key. Moreover, data substantiation enhancement is achieved when parties send random pieces to QKD center and notify them. By apply this protocol we remove the guessing theory applied in early protocol such as BB84, B92, and EPR. We have improved the facility to identify if there is an prowler or not.

Security of the Proposed Protocol

The protocol is impervious to man- in- the-middle attack, because the participant is authenticated both implicitly and explicitly. Even TC cannot intercept the data transmit between the participants because the assembly key is only known to Alice and Bob.
An eavesdropper Eve cannot copy the transmitted data in our protocol. Because in order to check Eve from doubling the data, our practice uses polarized photons in Quantum superposition states. Hence, by transmit data as a superposition of state, no one can make a copy of the transmit data without errors.

IV. ALGORITHM ANALYSIS

Our proposed algorithm consists of two common phases and seven steps. In this division we question our algorithm and compare it with other algorithms. Table I shows a relationship with respect to used bases, established channel and user substantiation. Table II, illustrates a comparison in regards to amount of used phase and the use of cryptography.
In protocols BB84, B92 and EPR there is a prospect of mismatching bases. Taking into kindness this possibility, the length of bases will be comparatively smaller to the original piece. If there is an attacker, the percent will be 50%, which means that half of key will be unnecessary. In our protocol, we can transport the meaning by using the whole key length. By using public key encryption algorithm, we can send the quantum bases succession from QKD to Alice and Bob. In addition, we improve user's confirmation where the above three algorithms do not supply it.
On the other hand, earlier protocols use classical channel to match up to between the correspondent and the recipient bases. In our algorithm, the sender and the receiver send random parts from the message to QKD to check if there is an intruder or not.

V. CONCLUSION

This paper planned a Quantum authenticated key supply procedure. The objectives of this practice are to let participant share a special conference key after each session while provided that certification, both completely and plainly. To hide transmit figures from not permitted user; this protocol uses quantum superposition state instead intertwined states.

This practice consisted of three phase. In the primary phase, the participants are utterly authenticated via the trusted centre.
In the second stage, a session key is customary between the two participant. Even the trusted centre cannot listen to the secure letter between the participant because the session key shared between the participant is hidden from the trust centre.
In the third phase, the participant of the announcement is communally authentic to each other.

Quantum key distribution protocols BB84, B92 and EPR communicate using a typical channel to compare the bases. This draw near facilitates eliminate the incorrect qubits. In this paper we introduce a novel security quantum algorithm that employs public key encryption algorithm to 85 generate keys to improve defense over quantum announcement channel. additionally, the introduced algorithm enhances user's certification and data privacy.

REFERENCES

1. M. Elboukhari, M. Azizi, and A. Azizi, "Analysisof the Security of BB84 by Model Checking,"*arXiv preprintarXiv:1005.4504,* 2010.

2. T. Hwang, K.-C. Lee, and C.-M. Li, "Provably secure three-party authenticated quantum key distribution protocols," *Dependable and Secure Computing, IEEE Transactions on,* vol. 4, pp. 71-80, 2007.

3. Y. Kanamori, S.M. Yoo, D.A. Gregory, and F. Sheldon, "Authentication Protocols using Quantum Superposition States," to appear in *International Journal of Network Security.*

4. https://en.wikipedia.org/wiki/Quantum_key_distribution#BB84_protocol:_Charles_H._Bennett_and_Gilles_Brassard_.281984.29

5. D. R. Kuhn, "A hybrid authentication protocol using quantum entanglement and symmetric cryptography," quant-ph/0301150, 2003.

6. Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283(5410):2050–2056, 1999.

7. P.D. Townsend, "Secure Key Distribution System Based on Quantum Cryptography," Electronics Letters, vol. 30, pp. 809- 811,1994.

8. Muneer Alshowkan , Khaled Elleithy ,Ammar Odeh, Eman Abdelfattah, "A New Algorithm for Three-Party Quantum Key Distribution" DOI: 10.1109/INTECH.2013.6653692 Conference: 2013 Third International Conference on Innovative Computing Technology (INTECH).

9. Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah" Quantum Key Distribution by Using Public Key Algorithm(RSA)" Third International Conference on Innovative Computing Technology (INTECH 2013)

10. Douglas Stebila , Michele Mosca, Norbert Lütkenhaus "The Case for Quantum Key Distribution" arXiv:0902.2839v2 [quant-ph] 2 Dec 2009