International Journal of Emerging Engineering Research and Technology
Volume 3, Issue 7, July 2015, PP 5-12
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Quantum Key Distribution by Exploitation Public Key Cryptography (ECC) In Resource Constrained Devices

Sneha Charjan, D. H. Kulkarni

[1]*Department of Computer Engineering, SKNCOE, Pune, India*
[2]*Department of Computer Engineering, SKNCOE, Pune, India*

ABSTRACT

Quantum Cryptography uses the laws of quantum physics for communication, offers an unconditionally secure solution to the key distribution problem. Moreover quantum mechanics also provides the ability to detect the presence of eavesdropper who is trying to learn key. But there is a problem of user authentication in quantum cryptography which can be overcome by using advantages of both public and quantum cryptography. By using ECC (Elliptic Curve Cryptography), which provides equivalent security level as RSA (Rivest-Shamir-Adleman) in less key size that is 160 bit key size of ECC provides equivalent security level as 1024 bit key size of RSA which is advantageous for resource constrained devices like cellular phone, personal digital assistants (PDAs), embedded systems, sensors and smart cards. At the same time in typical quantum cryptography there is an overhead and inefficiency caused due to number of rounds required to measure the correct bases which can be overcome using the system.

Keywords: Quantum Cryptography, Quantum Key Distribution (QKD), Network security, Photon Polarization, Three Party Communication.

INTRODUCTION

The uses of computer communications networks technologies have increased the incidents of computer abuse. On account of these episodes, most organizations confronting weight to secure their benefits. Most digital networks generally large depend on cutting edge cryptosystems to secure the confidentiality and integrity of movement conveyed over the network. The current modern cryptosystems focused around scientific model acquaint potential security openings related with mechanical advancement of computing power, the key refresh rate and key expansion ratio, the most pivotal parameters in the security of any cryptographic strategies. Therefore efforts have been made to create new establishment for cryptography science in the machine communication systems. One of these endeavors has prompted the improvement of quantum cryptography innovation, whose security depends on the laws of quantum mechanics.

Key distribution is the capacity that conveys a key to two parties who wish to communicate. Key distribution is the strength of any cryptographic system as the security of any communication is totally depends on the secret key. Therefore, it is important to have secure key distribution system because if the key get compromised then whole system will get compromised.

Classical cryptography is based on a combination of guess work and mathematics. Security depends on the difficulty of computational complexity which is not enough as the fast growing methods to calculate the secret key will compromise the security. There are two approaches in classical cryptography for key distribution: Symmetric cryptography and asymmetric cryptography. [1]

In symmetric cryptography there is same secret key shared between two parties who want to communicate whereas in asymmetric cryptography communicating parties must have pair of key called public and private key; the private key is kept secret with each party and public key is used for encryption of data is known to everyone who wants to communicate.

Whereas quantum key distribution provides the most secure way to distribute or exchange secrete keys as quantum cryptography uses the laws of quantum mechanics for communication which offers

Address for correspondence:

snehjan10@gmail.com

an unconditionally secure solution. Moreover quantum mechanics also provides the ability to detect the presence of eavesdropper who is attempting to learn the key as the quantum state on the transmitted data will collapse to single state and therefore, get disturbed. [2]

A problem of user authentication in quantum cryptography which can be overcome by using advantages of both public and quantum cryptography. By using ECC, which provides equivalent security level as RSA in less key size which is advantageous for resource constrained devices like cellular phone, personal digital assistants (PDAs), embedded systems, sensors and smart cards. At the same time in typical quantum cryptography there is an overhead and inefficiency caused due to number of rounds required to measure the correct bases which can be overcome using the system.

This paper is organized as follows: Section II Related work gives brief information about existing system. Section III Problem Statement and Proposed System describe the overview of system proposed. Section IV gives detail about simulated experimental result and section V summarizes and concludes the proposed system.

RELATED WORK

In quantum key distribution system, two parties who want to communicate are allowed to create secret key based on random function. Many protocols have been introduced to solve a problem of communication using quantum cryptography. The first protocol was introduced by Charles H. Bennett and Gilles Brassard in 1984 named as BB84 [2]. It was focused around Heisenberg's Uncertainty principle. All other Heisenberg's Uncertainty principle (HUP) based protocols are essentially variants of the BB84 idea. The essential thought for all these conventions then is that Alice can transmit a random secrete key to sway by sending a series of photons where the secrete key's bits are encoded in the polarization of the photons. Heisenberg's Uncertainty principle can be used to guarantee that an eavesdropper cannot measure these photons and transmit them on to Bob without disturbing the photon's state in a detectable way thus revealing eavesdropper's presence. Also the non-cloning theorem assures that eavesdropper cannot replicate a particle of unknown state. BB84 uses two phases, in first phase Alice will communicate to Bob over a quantum channel. Alice begins with choosing random strings. Bob will notify over any insecure channel that what bases he used to measure each photon. BB84 uses four polarization states [3]. In 1992 Charles Bennett proposed a simplified version of BB84, in which only two polarization states are necessary, named as B92.

While there are a number of other BB84 variants one of more recent was propose by Scarani, Acin, Ribordy, and Gisin named as SARG04. The protocol shares the exact same phase as BB84. In the second stage when Alice and Bob focus for which bits their bases matched, Alice does not straightforwardly report her bases. Rather she affirms a couple of non-orthogonal states, one of which is utilized to encode her bit. In the event that Bob utilized the right basis, he will gauge the right state. In the event that he picked mistakenly, he won't measure both of Alice's states and he won't have the capacity to focus the bit. . This convention has a particular preference when utilized as a part of functional equipment [4].

Four state quantum key distributions (QKD) protocol BB84 and two state QKD protocol B92 can let Alice and Bob share the secret key with idealized maximum efficiencies 50 % and 25 % over quantum channel, respectively. In [3], two enhanced QKD protocols are proposed. One is to enhance the idealized maximum efficiency to 28.6 % with the average complexity order 2, and the other has the efficiency 42.9 % and the average complexity order 2.86.

To compensate the loss in the signal the assumption are made while designing BB84 like weak signal source, near perfect transmission line, sensitive and fast quantum detectors, amplifiers, repeaters that are needed. These assumptions might not be practical in many situations. It uses highly attenuated lasers as source of quantum signals which can produce signals that contain more than one photon leads to new attack known as Photon Splitting Attack [5].

In [6], Decoy state quantum key distribution (QKD) has been proposed as a novel approach to enhance both the security and the performance of practical QKD setup. In this author report the first experiments on decoy state QKD, thus bridging the gap. Two protocols of decoy state QKD are implemented: one decoy protocol over 15 km of standard telecom fiber, and weak + vacuum protocol over 60 km of standard telecom fiber. The standard security proof give a zero key generation rate at the distance the decoy state QKD is performed. Therefore decoy state QKD is necessary for long distance secure communication which explicitly shows the power and feasibility of decoy method.

A QKD protocol over a two way quantum channel, this protocol does not require any classical channel instead two communicating parties are required to be connected by two way quantum channel. It reduces overhead due to key shifting and key reconciliation over classical channel and also the operational overhead and increase the speed with which keys can be exchanged [7].

Quantum cryptography can provide long term confidentiality for encrypted information without reliance on computational assumptions. Although QKD still requires authentication to prevent man-in-the-middle attacks. In [8], the vulnerability in existing models are reviewed like no authentication of participant, lack of pre process, no estimation of attackers information and the improved QKD protocol is proposed in which they have used both classical and quantum channels and included nine steps that are authentication of participant , initialization, quantum transmission, shifting, error reconciliation, estimating attacker's information, decision on continuation, privacy amplification, getting error free key which enhance the security.

In an entanglement-based quantum key distribution [9], authors have used a modified version of Cabello's definition of efficiency of QKD protocols to do comparison between their protocol and BB84. A sequence of qubit pairs is gained by dividing the stream of qubits. The protocol reveals less information about the key bit than BB84 because before the beginning of the protocol the participants get agreed publically on two 2-qubit unitary transformations, U_1 and U_2 and all transmitted qubits are useful unlike BB84 that half of qubits are discarded on average. In this one classical bit is used to acknowledge receiving each qubit and one classical bit is used for determining the basis of each group of qubits. It provides advantage against eavesdropper under an intercept resent attack.

Multiple-Access quantum key distribution networks addresses multi –user QKD networks, there is no need of any other node except the two communicating parties, they can mutually exchange a secret key. In this the idea of switching is used instead of full mesh network in wavelength division multiplexing (WDM) network. Certain wavelength is assigned to two nodes who want to exchange the key and wavelength router links them together. Same network is used for both classical and quantum signals by assigning them two different wavelength bands. The hybrid setup is formed by combining time/code division multiple access (TDMA/CDMA) QKD networks with WDM routing setup, in which each WDM node serves as a hub through multiple TDMA/CDMA users can be supported. In this to get the advantage of both TDMA and CDMA, a listen-before-send (LSB) protocol is proposed which supports multiple users [10].

In [11], the comparison of commercial and next generation quantum key distribution is given. Till date, most of the QKD systems have utilized a discrete variable (DV) binary approach. In this discrete information is encoded onto a quantum state of single photon and binary data are measured using single photon detectors. Recently, continuous variable (CV) QKD system has been developed, in which randomly generated continuous variables are encoded on coherent state of weak pulses of light and continuous data values are measured with homodyne detection methods. CV-QKD offers higher secret key exchange rate for short distances, lower cost, and compatibility with telecommunication technologies. In CV-QKD, unlike DV-QKD, Alice and Bob do not have the same values during key shifting process, they only have correlated data and therefore, key generation, error correction are more tedious in this approach. For short distance CV-QKD system can generate higher secret key rate than DV-QKD system as it uses detector with higher quantum efficiency but at the same time it is very challenging for CV-QKD for long distance as secret key generation rate is strongly dependent on the vacuum noise which increases with distance. On the other hand in DV-QKD system, the QBER is typically not impacted by vacuum noise. For long range distance in fiber and free space, DV-QKD appears to have a competitive edge while CV-QKD systems hold a promise for more economic fiber usage by allowing a higher number of systems to coexist on a single fiber.

In [5], authors have proposed a novel secure quantum key distribution algorithm in which their main objective is to overcome the deficiencies found in BB84 and B92 protocols by eliminating the need for two communicating parties to confirm their used basis over a public channel. Session key is the strength of any cryptography communication. So in this session key is exchanged over the most secure channel that is quantum channel. Before that using public key cryptography the users are authenticated and confidentiality is maintained by exchanging random basis and nonce. It eliminates the inefficiency caused due to requirement of many rounds just to agree on a basis for the quantum communication.

In [1], a new model for QKD is introduced between three parties where there is a trusted center providing the clients the necessary secret information to securely communicate with each other. In this there is no need of physical channel to check qubits sequence. The proposed algorithm consists of two phases: 1. User Authentication and quantum bases distribution. 2. Data Transfer over the quantum channel. When Alice wants to communicate with Bob, Alice sends requests with its ID to QKD, QKD check for authentication and asks to Bob. When both the parties get agreed on communication, QKD starts distributing quantum bases in some sequence to encode the message to Alice and Bob in encrypted message using Alice and Bob's public keys. It improves the efficiency by eliminating the rounds required to check the quantum bases and provide authentication.

A new algorithm for three party quantum key distribution [12] provides new mechanism to establish trust between different parties. The trusted third party forms an agreement on the secret key and establishes a trust between them. The specific aim is to allow the parties to agree on the basis and not the final secret key. This protocol requires three quantum channels between parties along with classical channel. QKD selects random classical bits and orthogonal bases to generate qubits. Qubits are transmitted to Alice and Bob through quantum channel. Then Alice and Bob must select random bases to measure received qubits and transfer them to classical bits. They send these classical bits to QKD. After receiving qubits from Alice and Bob, QKD measures it using original bases and transfer result to classical bits and compare bits with received bits and maintain record to indicate correct and incorrect positions of the received bits. All steps are repeated several times depending on key size then determine correct position to get final key. It is also useful to determine the presence of eve.

PROBLEM STATEMENT AND PROPOSED SYSTEM

Problem Statement

Authentication and resource usage problem: It is defined as designing an algorithm to authenticate the user in QKD without using classical channel with the use of Public Key Cryptography with ECC to reduce the usage of resources in resource constrained devices and also overcome the overhead caused due to number of rounds required to measure the correct bases and final key.

Proposed System

The proposed system is the hybridization of three party algorithm given in [1] and using ECC instead of RSA. Three party algorithm which removes the problem of user authentication and overcome the overhead and inefficiency caused in typical QKD due to number of rounds required to measure correct key bases and final key. While the advantage of using ECC is, it provides equivalent security level as RSA in less key size. Due to which any system will require less power for computation which is useful for resource constrained devices. The comparative table for key size of RSA and ECC is given below [13].

Table1. *Comparison*

Comparison	
RSA Key size in bits	***EC Key size in bits***
1024	160
2048	224
3072	256
7680	384
15360	512

Algorithm:

Algorithm includes two phases:

1. User Authentication and Quantum Bases Distribution
2. Data Transfer over Quantum Channel

In this, in first phase ECDSA (Elliptic Curve Digital Signature Algorithm) is used for user authentication. And after word all the communicating parties will use their public and private keys for communication over quantum channel.

Consider Alice and Bob as the users of the system where Alice is the sender and Bob is the receiver. QKD is the trusted third party who distributes the quantum bases.

P_A- Alice's Private Key

P_B- Bob's Private Key

Pu_A- Alice's Public Key

Pu_B-Bob's Public Key

Pu_{QKD}- QKD's Public Key

ID_A-ID of Alice

ID_B-ID of Bob

E_{QB}- Encrypted using Quantum Bases (QB)

Phase 1: User Authentication and Quantum Bases Distribution

1. Alice requests to have a connection with Bob

   Alice -> QKD: P_A (ID_A |ID_B)

QKD will register the connection request status in log file and check the ID of Alice for authentication. Also, 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 -> Bob: Pu_B (ID_A|ID_B)

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

   Bob -> QKD: P_B (ID_A|ID_B)

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.

   QKD -> Alice: Pu_A (ID_A|ID_B|QB)

   QKD -> Bob: Pu_B (ID_A|ID_B|QB)

Phase 2: Data Transfer over Quantum Channel

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

   Alice -> Bob: P_A (E_{QB}(M)|Pu_B(ID_A))

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

   Bob -> QKD: P_B (E_{QB}(M)|Pu_{QKD}(ID_B))

   Alice -> QKD:P_A (E_{QB}(M)|Pu_{QKD}(ID_A))

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 -> Bob: Pu_B (E_{QB}(notify))

   QKD -> Alice: Pu_A (E_{QB}(notify)).

   ECC- Elliptic Curve Cryptography [14],[15],[16]

The equation of an elliptic curve is given as,

$$y^2 = x^3 + ax + b$$

E- Elliptic Curve

P- Point on the curve

n- Maximum limit (prime number)

Key Generation:

$Q = d * P$

d-The random number selected within the range of (1 to n-1)

P-The point on the curve

Q- Public key

d- Private key

Encryption:

Let 'm' be the message that is to be send

Consider 'm' has the point 'M' on the curve 'E'

Randomly select 'k' from [1-(n-1)].

Two cipher texts will be generated let it be C1 and C2

EXPERIMENTAL RESULTS

Proposed system assures that there can't be man-in-middle attack as in quantum cryptography man-in-middle attack is possible only when users are not authenticated and in proposed system, it's first authenticating user and then only allowing him/her to communicate with other users. The authentication is provided by using public key cryptography and quantum channel. In this public key cryptography is implemented using both RSA and ECC to verify which algorithm is going to consume more amount of resources. From the results, it is conclude that ECC is far better than RSA for resource constrained devices.

Simulation results are generated by implementing proposed system in Java, which shows the comparison between RSA and ECC by exploitation in the proposed system using different parameters that are key generation time, key encryption time, key decryption time.

Following graphs (Fig. 1,2,3,4) shows the comparison that proves that time required for system to execute using ECC is very less than RSA, so the power consumption is less for computation of key. System also provide authentication and overcome the problem of overhead which causes due to large number of rounds require to finalize the secrete key.

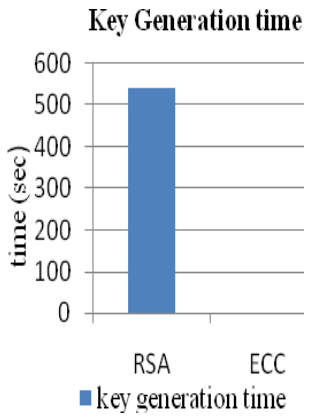

Figure1.*Comparison in Key generation Time*

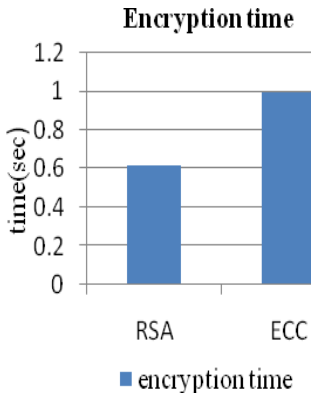

Figure2. *Comparison in Encryption Time*

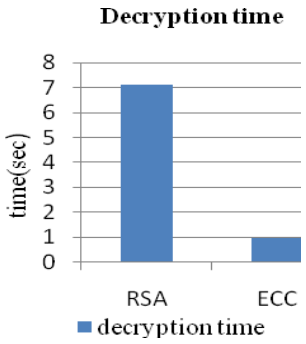

Figure3. *Comparison in Key Decryption Time*

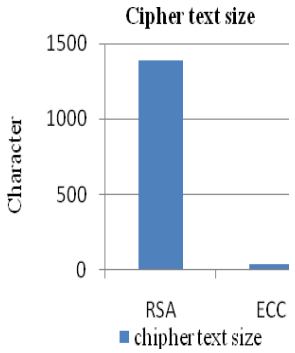

Figure4. *Comparison in Cipher Text Size*

CONCLUSION

Quantum cryptography is that the most secure system of communication however suffers from the matter of users authentication and conjointly inefficiency caused attributable to range of rounds needed to measure the proper bases and final key which might be overcome victimization classical cryptography that is public key cryptography. Planned system overcomes the problem of user authentication victimization the general public key cryptography within the quantum key distribution system. As in the algorithmic rule the QKD (trusted third party), distributes the quantum base before communication start between two parties, the overhead get removed that is cause due to the amount rounds needed to induce the error free key. And at same time public key cryptography is victimization Elliptic curve Cryptography that provides same security level as RSA algorithmic rule in terribly less key size that consumes less power for computation thus it's helpful in resource constrained devices. Combination of each classic and quantum cryptographies removes downside and provides the most secure communication.

ACKNOWLEDGEMENT

I thank my guide Prof. D. H. Kulkarni for her valuable guidance and support. Also I would like to thank Prof. Pathan for his generous help in all queries. I would like to thank all staff members who have assuredly helped me a lot and my friends and parents for their motivated support in this work.

REFERENCES

[1] Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah, "Quantum Key Distribution by Using Public Key Algorithm (RSA)", London, United Kingdom: third International Conference on Innovative Computing Technology (INTECH),IEEE, August 2013.

[2] Charles H. Bennett, Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", International Conference on Computers, Systems and Signal Processing Bangalore, India, December 10-12, 1984.

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

[4] M. Haitjema, "A Survey of the Prominent Quantum Key Distribution Protocols", December 2007.

[5] Abdulrahman Aldhaheri, Khaled Elleithy, Majid Alshammari, Hussam "A Novel Secure Quantum Key Distribution Algorithm", University of Bridgeport.

[6] Y. Zhao, B. Qi, X. Ma, H. Lo. L. Qian, "Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber", ISIT, Seattle, USA, July 2006.

[7] Farnaz Zamani, P. K. Verma, "A QKD Protocol with a Two-way Quantum Channel", in Advanced Networks and Telecommunication systems (ANTS), 5th International Conference IEEE, pp 1-6, 2011.

[8] R. D. Sharma, A, De, "A New Secure Model for Quantum Key Distribution Protocol", Industrial and Information system (ICIIS), 6th IEEE International Conference, pp 462-466, 2011.

[9] M. Houshmand and S. Hosseini-Khayat, "An Entanglement-base Quantum Key Distribution Protocol ",in Information Security and cryptology (ISCISC), 8th International ISC Conference on. IEEE, pp. 45-48, 2011.

[10] M. Razavi, "Multiple-Access Quantum Key Distribution Networks", IEEE Transactions on Communication, vol. 60, no. 10, October 2012.

[11] L. Osterling, D. Hayford, G. Friend, "Comparison of Commercial and Next Generation Quantum Kay Distribution: Technologies for secure communication of information", in Homeland Security (HST), IEEE Conference on Technologies for, pp. 156-161, 2012.

[12] M. Alshowkan, K. Elleithy, A. Odeh, e. Abdelfattag, "A New Algorithm for Three –Party Quantum Key Distribution", 3rd International Conference on Innovative Computing Technology (INTECH), London, United Kingdom, August 2013.

[13] Mohsen Bafandehkar, Sharifah Md Yasin, Ramlan Mahmod, Zurina Mohd Hanapi, "Comparison of ECC and RSA Algorithm in Resources Constrained Devices", IEEE, 2013.

[14] Ikshwansu Nautiyal, Madhu Sharma, "Encryption using Elliptic Curve Cryptography using Java as Implementation tool", IJARCSSE, vol. 4, Issue 1, January 2014.

[15] Anoop MS, "An Elliptic curve cryptography", An implementation guide.

[16] Avi Kak, "Elliptic Curve Cryptography", Lecture notes on "Introduction Computer Security", March 2007.

[17] Sneha Charjan, D.H. Kulkarni, "Quantum Key distribution using different Techniques and algorithms", IJERT, vol. 3, Issue 11, November 2014

AUTHORS' BIOGRAPHY

Sneha Charjan received Bachelor degree in Computer Technology from the RTMNU, Nagpur, Maharashtra, India in 2012. She is pursuing Master degree in Computer Networks from the Savitribai Phule Pune University, Pune, Maharashtra, India.

Prof. D.H. Kulkarni received Master degree in Computer Engineering. She is Assistant Professor in Computer Engineering Department, SKNCOE, Pune, Maharashtra, India.