Journal of Theoretical and Applied Information Technology
10th July 2013. Vol. 53 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SOLVING HEURISTIC ATTACKS USING ELLIPTIC CURVE CRYPTOGRAPHY IN QUANTUM COMPUTER

[1]G. ALOY ANUJA MARY, [2]C.CHELLAPPAN

[1] ANNA UNIVERSITY,Department of Computer Science & Engineering, Guindy,Chennai-55
[2] ANNA UNIVERSITY, Department of Computer Science & Engineering, Guindy,Chennai-55

E-mail:[1] aloyanujamary@gmail.com ,[2] drcc@annauniv.edu

ABSTRACT

Quantum Secret Sharing (QSS) is one of the important branch in Quantum Cryptography which combines Quantum with classical mechanics. The main objective of this paper is to propose elliptic curve cryptography (ECC) for solving heuristic attacks. The QSS and ECC methods has been tested in the following three quantum algorithms like Genetic Algorithm (GA), Tabu search algorithm (TS), Cuckoo search algorithm (CS). By considering the error rate, ECC method has higher error rate than the existing QSS method and secrecy also has been improved. The proposed ECC method is implemented and tested for 50 iterations and also comparison is made with QSS.

Keywords: *Quantum Secret Sharing, Genetic Algorithm, Tabu Search Algorithm, Cuckoo Search Algorithm , Elliptic Curve Cryptography.*

1. INTRODUCTION

In modern world, secure communication has twisted into one of the most favorable fields. This field is the highly required field for every organization and entity [1], and their developments are rising considerably [2]. In public environment cryptography is broadly used to keep the data secure [3] [4] by means of Encryption and Decryption process. Here, using some key at the transmitter side the original message or plaintext is encrypted. Then the encrypted data is decrypted with the identical or an additional key at the receiver side as per the accepted protocol between the two parties [1] [5]. Broadcast, network communication and also electronic transactions such as Internet, e-mail, and cell phones are the application areas of cryptography [5]. To control eavesdroppers from learning the contents of encrypted messages most classical cryptosystems is based on the computational difficulty of certain mathematical functions and employs different mathematical techniques [6]. However, it was revealed that this sort of security might be vulnerable for the strong ability of quantum computation [4] and in addition the conservative cryptography can't offer any guarantee for key security [6].

Secure communication link is established by using these keys over an insecure public networks. However, a malicious attacker might obtain the session key from the key distribution method [7]. Now, there has been a excellent deal of research of a latest cryptographic method called quantum cryptography [8]. Unlike the classical cryptography, quantum cryptography is based on the laws of quantum physics. These laws ensure that nobody can measure the state of an arbitrary polarized photon carrying information without introducing disturbances, which will be detected by legal users. As all eavesdropping can be detected, quantum cryptography is considered as a promising key distribution over long term unconditionally secure cryptosystems [9].Quantum cryptography includes quantum key distribution (QKD), quantum secure direct communication (QSDC), quantum secret sharing (QSS), quantum identity authentication (QIA), and so on [10].

Quantum Key Distribution has the capability to communicate between two users to discover the existence of any third party trying to gain knowledge of the key [6].The security of the key is unconditionally guaranteed by quantum mechanics [11], [12]. Different from it, another appealing branch of quantum communication is quantum secure direct communication (QSDC), in which additional classical bit transmission is needed to transmit the secure information [13]. On the other hand, with quantum mechanics, quantum secret sharing (QSS) task can be realized. In which, the sender's secret message is distributed through quantum mechanical method among n shares and in such a way that the shares can retrieve the secret message by their cooperative operation [15]. The quantum secret sharing (QSS) scheme is better than the classical approaches in detecting the error caused by an eavesdropper [14] and also it has attracted a great deal of attention in many theoretical and practical aspects [15].

2. RELATED WORKS

A handful of research works available in the literature deals about the quantum mechanics. A few of the most recent literature works in this topic are reviewed in this section.

In 2009, Majid Safari *et al.*, [16] have proposed a terrestrial relay-assisted scheme for a free-space quantum key distribution (QKD) system based on BB84 protocol. To forward the qubits to the next relay node or to the receiver without performing any measurement or discovery process they have considered the operation of passive relays. They have derived an upper bound on quantum bit error rate (QBER) of the relay-assisted QKD system based on a near-field analysis. Also, experimental results have exposed that for long link ranges in which turbulence effects are particularly degrading, the relay-assisted proposal was able to outperform point-to-point direct transmission.

In 2010, Pradeep Kumar *et al.,* [17] have discussed the use of spin wave optical interactions to apply the BB84 and B92 quantum key distribution (QKD) protocols. Spin waves combine the transverse magnetic (TM) and transverse electric (TE) optical modes of a waveguide. To establish the time evolution of quantized TM and TE modes, they have derived the interaction Hamiltonian to illustrate the coupling, and to solve the resulting equations. A set of four non orthogonal states which were corresponding to the set of polarization states of a single photon can be generated based on the choice of coupling coefficient. These states form a conjugate basis suitable as a QKD basis set. Several medium-induced polarization fluctuations can be moderated by their scheme. To execute the BB84 protocol using frequency-coded coherent optical states the spin wave–optical interactions can be used.

In 2010, Fei Gao *et al.*, [4] have discussed the security analysis of two three-party quantum key distribution protocols (QKDPs). These protocols were vulnerable to the dense-coding attack. It was revealed that the eavesdropper Eve obtained the session key by distributing entangled qubits as the fake signal to Alice and performing combined measurements following Alice's encoding. The attack process was just similar to a dense-coding communication between Eve and Alice. In addition, to the transmitted information this attack did not initiate any errors and which was not discovered by Alice and Bob. At last, in their work, the root of that uncertainty and a possible way to develop these protocols were described.

In 2010, Gan Gao [18] has discussed the cryptanalysis of four party quantum secret distribution protocol in which the collective eavesdropping-check was employed. In four party QSS protocol, simply one boss named Alice wants to execute Bell state measurement and the other agents were requisite to execute a solitary qubit process. In this protocol, to avert eavesdropping they have used the collective eavesdropping-check for quantum channels. Due to the dishonest agents in the QSS protocol eavesdropping can be formed without introducing any error on Alice's secret messages.

In 2011, Ananda Rao *et al.*, [7] have proposed a system by grouping both implicit quantum key distribution protocol (3AQKDP) and explicit quantum key distribution protocol (3AQKDPMA). The attacks like eavesdropping, man-in-the-middle, and replay can be prevented by their establishment of secure connection. The communication rounds have been reduced by their approach. In addition a long term secret key has been used and shared among two parties frequently. The joint approach of both classical and quantum cryptography has the capability to identify the existence of passive attack such as eavesdropping.

In 2011, K.Sathi Reddy *et al.*, [19] have discussed a Quantum authenticated key distribution protocol to execute key allocation. It is also developed to ensure that the participants of the communication were authenticated implicitly and explicitly. Only for authentication part the Participants of their protocol depend on third party. Therefore the proposed protocol has been implemented in network systems which deal with highly sensitive information like military, hospitals, and research facilities. For authentication and key distribution they have utilized polarized photons in superposition states which provide high protection against several attacks. The structure of the paper is organized as follows: A brief review of the researches related to the quantum methods is given in Section 2. The analysis of Quantum algorithms with heuristic attacks are given in section 3. ECC based Key Generation, its Encryption and Decryption is given in section 4. Security Evaluation, Objective model and Comparison results are presented in section 5.Conclusion of the existing and proposed approach is presented in Section 6.

3. PROPOSED METHODOLOGY

The main aim is to offer a better multiparty quantum secret sharing protocol to solve the drawbacks that currently exist in the literary works. In this work, four party quantum secret sharing protocol will be used and also the analysis of attacks against the robustness of the protocol will be performed. Thus very popular and most recent heuristic attacks will be implemented on the four party quantum secret sharing protocol to validate the robustness of the protocol. The popular heuristic algorithms such as Genetic Algorithm, Tabu Search Algorithm, as well as the recent Cuckoo search algorithm will be utilized for cryptanalysis. But these QSS protocols not have any security process when the information is shared between parties. The lack of security process in information sharing makes the performance insufficient. Thus the drawbacks in the existing QSS protocol have to overcome by introducing an ECC based security method. Here an ECC based private and public keys are created to the four parties in quantum system. Based on the created keys, the information is shared between the parties and also the security checking process is performed on the shared information.

4. HEURISTIC ATTACKS

To analyze the robustness of the four party QSS protocol very popular heuristics attacks are implemented. These heuristics attacks are fashioned by three popular heuristics algorithms such as Genetic Algorithm (GA), Tabu Search algorithm (TS), Cuckoo Search Algorithm (CSA).

4.1 Attack Generation by Genetic Algorithm (GA)

Genetic Algorithms (GAs) are adaptive heuristic search algorithm based on the evolutionary ideas of natural selection and genetics.Inorder to solve optimization problems random search method is used.

GAs simulates the survival of the fittest among individuals over consecutive generation for solving a problem. Each generation has a population of character strings that are analogous to the chromosome. Each individual represents a point in a search space and a possible solution. The processes of evolution are then made by each individual in the population. By exploiting GA, the heuristic attack will be generated for analyzing the QSS protocol. The steps involved in the QSS protocol analyzer process with GA attack is described below.

Step 1: Generate random solutions of chromosomes in the form of matrix as similar to the Bob, Charlie and David solutions.
Step 2: Evaluate the fitness function using the formula, which is given in equation.(14).
Step 3: After that, genetic operations like crossover and mutation are performed for generate new solutions. Here we carry out the single point crossover and mutation operations.
Step 4: The process is repeated until the maximum number iterations are reached.
Subsequently, we find the minimum error rate $Er_{\min}$. The process is concluded that if evaluated minimum error rate $Er_{\min}$ does not exceeds the threshold function (λ), the QSS protocol is secure i.e. the information is not hacked by any one otherwise, it is not secure.

4.2 Attack Generation by Tabu Search Algorithm (TS)

Tabu search (TS) is an iterative procedure designed for the solution of optimization problems. It is used to solve a wide range of hard optimization problems such as job shop scheduling, graph coloring (related), the Travelling Salesman Problem (TSP) and the capacitated arc routing problem.

Tabu search algorithm initially generates a initial solution as input, where tours are added to Adaptive Memory Procedure (AMP) .During each consecutive iterations tours are selected from the AMP in a biased manner to construct a new solution. Non-Tabu feasible solutions are generated in an attempt to escape minima. Two memory based strategies that form a fundamental principles of TS is Intensification and Diversification. With the use of Intensification strategy regions around attractive solutions are thoroughly searched, and typically operates by restarting a search from a solution previously found to yield good results. Steps involves in QSS analyses with TS based heuristic attack which is described below,

Step 1: Generate initial solution as heuristic attacker and tours are added to the Adaptive Memory Procedure (AMP)

Step 2: Evaluate the fitness function (Error rate) by Bell state Measurement

Step 3: For iterations tours are selected from the AMP in a biased manner to construct new solutions

Step 4: Repeat step 2 for the newly generated solutions

Step 5: If the error rate evaluated in Step 4 is less than the error rate evaluated in the Step 2 the newly generated solution is move to the Tabu list. If not the solution is discarded.

Step 6: Iteration continues to evaluate the minimum error rate.

If the evaluated error rate does not exceeds the threshold function (λ) i.e. $E_{R_{\min}} < \lambda$ which is mentioned in the equation (16) eavesdropper eve does not exists. If not the communication is hacked.

4.3 Attack Generation by Cuckoo Search Algorithm (CSA)

In Cuckoo search (CS), each egg in a nest represents a solution, and a cuckoo egg represents a new solution [20]. The aim is to use the new and potentially better solutions (cuckoos) to replace a not-so-good solution in the nests. In the simplest form, each nest has one egg. The algorithm can be extended to more complicated cases in which each nest has multiple eggs representing a set of solutions [21]. The procedure of QSS analyses process with CSA based heuristic attack is given below,

Step 1: Consider the Objective function as threshold error rate (λ)

Step 2: Generate initial population as solution generated as heuristic attacker

Step 3: Perform error rate evaluation using Bell state measurement

Step 4: Perform Levy flights to generate new solutions and evaluate the fitness function

Step 5: Iterations continues till the $E_R \alpha \lambda$

Step 6: Find the error rate probability factor, $P_a \in [0,1]$

Whereas best solutions can be find and minimum error rate $E_{R_{\min}}$ is evaluated. If the evaluated error rate does not exceeds the threshold function (λ) then eve does not exists. If not the communication is hacked.

5. ECC based Key Generation

In the proposed method, we generate keys to the four parties in the quantum system by the elliptic curve cryptography. In public key cryptography each user generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations[22]. The mathematical operations of ECC is defined over the elliptic curve

$$y^2 = x^3 + ax + b \tag{1}$$

Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number.

Key Generation: The operations of elliptic curve cryptography are defined over two finite fields: Prime field and Binary field. The suitable field is selected with finitely huge number of points for cryptographic operations. Here, we have used prime field operations by choosing a prime number P, and finitely large numbers of basic points are generated on the elliptic curve, such that the generated points p are between 0 to P. Then, we randomly select one basic point $p_i(x_i, y_i)$ for cryptographic operations and this point satisfies the equation of the elliptic curve on a prime field, which is defined as,

$$y^2 \bmod P = x^3 + ax + b \bmod P \tag{2}$$

In Equ. (1), a and b are the parameters that defining the curve, and x and y are the coordinate values of the generated points p. We randomly select one basic point p_i that satisfies the aforementioned Equ. (1). To perform the cryptography, we need to select a private key p_v on the sender side, which is a randomly selected integer less than P and generate a public key

$$p_u = p_v * p_i \tag{3}$$

By using the aforementioned key generation operations, we generate public and private keys to the four parties like Alice, Bob, Charlie and David. Thus the created private and public keys to the parties is defined as,

$$\text{Alice}=\{V_A,U_A\} \quad (4)$$

$$\text{Bob}=\{V_B,U_B\} \quad (5)$$

$$\text{Charlie}=\{V_C,U_C\} \quad (6)$$

$$\text{David}=\{V_D,U_D\} \quad (7)$$

From Equ.(4) to (7) illustrates the created private and public keys of the four parties. By exploiting these keys the parties perform the information sharing in the quantum system. The generated keys by ECC provide more security in the information sharing because the keys are not easily find out by any other users or hackers.

5.1 ECC based Encryption

The encryption process is performed over the information which is send by the Alice. The original message is encrypted by the Alice private key and sends to the parties. The encryption process is used to avoid the information hacking by eavesdroppers. In quantum system, the information each bit is represented by using a basis consisting of two Eigen states, denoted by $|0\rangle$ *and* $|1\rangle$, respectively. Similar to classical bits, a qubit may be in the $|0\rangle$ state, in the $|1\rangle$ state, or in any superposition of both states. In quantum machines, the qubit $|0\rangle$ and $|1\rangle$ is represented as a vector form is stated as follows,

$$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix},|1\rangle=\begin{bmatrix}0\\1\end{bmatrix} \quad (8)$$

In our proposed method encryption process, the qubits vector representation value is taken as a binary value and this binary value is given to the encryption process. The Alice all qubits are transformed to the binary value and the encrypted message is in the form of

$$M_e=\{C_i,C_j\} \quad (9)$$

$$C_i=M_o*p_i \quad (10)$$

$$C_j=(x,y)+M_o*(V_A*p_i) \quad (11)$$

In Equ. (9), M_e is encrypted message is comprised of two parts which is computed by Equ. (10) and (11). The value of C_i is calculated by multiplying the original message M_o with the basic point p_i and C_j is computed by using the Alice private key V_A which is given in Equ. (11). This encrypted message M_e is send to the receiver (i.e. parties). In quantum system Alice want to send her information to the three parties like Bob, Charlie and David. So Alice spilt her information into three parts and sends it to her parties. Here, the Alice sends the message is an encrypted message by ECC procedure.

5.2 ECC based Decryption

After the Alice send the message to the receiver (i.e. parties), they want to decrypt the message. The encrypted message is decrypted by using the formula is given as,

$$M_d=C_j-(V_B*C_i) \quad (12)$$

The above Equation describes that the encrypted information is decrypted by the party Bob. The other two parties Charlie and David decrypt their messages by their private keys V_C and V_D by using the same formula as given in Equ. (12).

6. SECURITY EVALUATION

The security evaluation process is performed by the heuristics attacks in the Quantum Secret sharing process. Similarly in the proposed method we randomly generates parties public keys to hack the Alice information. In this situation the hacker receives encrypted information only, but they can't decrypt the received messages without knowing the corresponding party private key. Alice performs the security evaluation process by measuring the received information from their parties. The error rate is calculated for compute the security level of the proposed method.

6.1 Objective Model

The developed objective model basic steps for the four party QSS analyses process is given below.

Step 1: Let M_e is the matrix randomly generated with 0's and 1's by the eavesdroppers.

Step 2: Let M_a be the matrix generated by Alice, the generated matrix is in the state of

$$|\Psi\rangle_{123} = \frac{1}{2}\Big[|\Psi^-\rangle_{13}(|0\rangle)_2 + |\Psi^+\rangle_{13}(-|0\rangle)_2 + |\phi^-\rangle_{13}(|1\rangle)_2 + |\phi^+\rangle_{13}(|1\rangle)_2\Big]$$

Or

(13)

$$|\Psi'\rangle_{123} = \frac{1}{2}\Big[|\Psi^-\rangle_{13}(|1\rangle)_2 + |\Psi^+\rangle_{13}(|1\rangle)_2 + |\phi^-\rangle_{13}(|0\rangle)_2 + |\phi^+\rangle_{13}(-|0\rangle)_2\Big]$$

Step 3: Error Rate Calculation: The both matrices M_e and M_a are compared by calculating an error rate. The higher Error Rate shows that the matrix M_e from the eavesdropper does not match with Alice matrix M_a . The error rate calculation is defined as,

$$E_R = M_a - M_e \qquad (14)$$

M_a → Matrix generated by Alice

M_e → Matrix generated by eavesdropper.

Step 4: Minimum Error Rate: The eavesdropper continuously generates a random matrix to obtain the Alice information. At every time we compute an error rate, along with we find a minimum error rate. Minimum error rate is the average error rate calculated with the number of iterations.

$$E_{r_{\min}} = \frac{\sum_{m=0}^{M} (M_a - M_e)}{M} \qquad (15)$$

M is the number of iterations.

Step 5: Objective Model: Afterward, the minimum error rate $E_{r_{\min}}$ from the M number of iterations is compared with the user defined threshold value λ .

$$\xi = \underset{M_e}{\arg} E_{r_{\min}} :< \lambda \qquad (16)$$

If ξ is the observation random variable, M_e is the parameter used for the minimization of error, which is used as an argument here. $E_{r_{\min}}$ and λ is the minimum error rate and threshold rate value respectively.

6.2 Comparison Results

The performance of the QSS system is evaluated by changing the matrix size under 10 experiments and the results are compared against the GA, TSA, and CSA with the proposed ECC System. The results under each condition are tabulated below and the minimum error value hold algorithm is put forward to further analysis.

Table I: Error Rate Of Proposed & Existing Methods For GA, TSA And CSA Attacks At Iteration 10

ERROR RATE						
Iteration=10	**Proposed Technique**			**Existing Technique**		
No. of rounds	GA	CS	TS	GA	CS	TS
1	0.8	0.733333	0.8	0.625	1	0.5
2	0.8	0.733333	0.733333	0.75	0.25	0.25
3	0.8	0.733333	0.866667	0.625	0.5	0.25
4	0.8	0.6	0.6	0.25	0.25	0.25
5	0.8	0.6	0.6	0.625	0.25	0.25
6	0.8	0.6	0.733333	0.5	0.25	0.25
7	0.8	0.6	0.666667	0.625	0.25	0.25
8	0.8	0.6	0.8	0.5	0.5	0.5

9	0.8	0.6	0.733333	0.625	0.25	0.5
10	0.8	0.6	0.666667	0.25	0.5	0.5
Average	0.8	0.64	0.72	0.5375	0.4	0.35
Standard Deviation	1.17028E-16	0.064406	0.087771	0.158607	0.229129	0.122474

Table II: Error Rate Of Proposed & Existing Methods For GA, TSA And CSA Attacks At Iteration 20

ERROR RATE						
Iteration=20	**Proposed Technique**			**Existing Technique**		
No. of rounds	GA	CS	TS	GA	CS	TS
1	0.8	0.8	0.8	0.625	0.5	0.25
2	0.733333	0.8	0.8	0.25	0.25	0.25
3	0.733333	0.8	0.6	0.25	0.25	0.25
4	0.733333	0.8	0.733333	0.5	0.25	0.25
5	0.666667	0.733333	0.733333	0.5	0.5	0.25
6	0.666667	0.733333	0.733333	0.25	0.25	0.25
7	0.666667	0.733333	0.666667	0.375	0.25	0.25
8	0.666667	0.733333	0.733333	0.5	0.5	0.25
9	0.666667	0.733333	0.6	0.375	0.25	0.25
10	0.666667	0.733333	0.6	0.375	0.5	0.5
Average	0.7	0.76	0.7	0.4	0.35	0.275
Standard Deviation	0.047140	0.034427	0.078567	0.122474	0.122474	0.075

Table III: Error Rate Of Proposed &Existing Methods For GA, TSA And CSA Attacks At Iteration 30

ERROR RATE						
Iteration=30	**Proposed Technique**			**Existing Technique**		
No. of rounds	GA	CS	TS	GA	CS	TS
1	0.8	0.8	0.8	0.5	0.25	0.25
2	0.8	0.8	0.8	0.25	0.25	0.25
3	0.8	0.8	0.733333	0.25	0.25	0.25
4	0.8	0.8	0.733333	0.5	0.25	0.25
5	0.8	0.8	0.733333	0.5	0.5	0.5
6	0.733333	0.733333	0.733333	0.5	0.25	0.25
7	0.733333	0.733333	0.733333	0.375	0.5	0.25
8	0.733333	0.733333	0.6	0.25	0.25	0.25
9	0.666667	0.733333	0.733333	0.5	0.25	0.25
10	0.6	0.733333	0.666667	0.25	0.5	0.5
Average	0.746667	0.766667	0.726667	0.3875	0.325	0.3
Standard Deviation	0.068853	0.035136	0.058373	0.117925	0.114564	0.1

Table IV: Error Rate Of Proposed & Existing Methods For GA, TSA And CSA Attacks At Iteration 40

ERROR RATE						
Iteration=40	**Proposed Technique**			**Existing Technique**		
No. of rounds	GA	CS	TS	GA	CS	TS
1	0.8	0.8	0.8	0.375	0.25	0.25
2	0.8	0.8	0.733333	0.25	0.25	0.25
3	0.733333	0.8	0.8	0.25	0.25	0.25
4	0.733333	0.8	0.666667	0.5	0.25	0.25
5	0.733333	0.8	0.733333	0.5	0.5	0.5
6	0.733333	0.8	0.733333	0.5	0.25	0.5
7	0.733333	0.733333	0.733333	0.25	0.25	0.25
8	0.733333	0.733333	0.733333	0.25	0.25	0.25
9	0.733333	0.733333	0.666667	0.25	0.25	0.25
10	0.733333	0.733333	0.733333	0.625	0.5	0.5
Average	0.746667	0.773333	0.733333	0.375	0.3	0.325
Standard Deviation	0.028109	0.034427	0.044444	0.136931	0.1	0.114564

Table V: Error Rate Of Proposed &Existing Methods For GA, TSA And CSA Attacks At Iteration 50

ERROR RATE						
Iteration=50	**Proposed Technique**			**Existing Technique**		
No. of rounds	GA	CS	TS	GA	CS	TS
1	0.8	0.666667	0.8	0.25	0.25	0.25
2	0.8	0.666667	0.733333	0.5	0.25	0.25
3	0.8	0.666667	0.733333	0.5	0.25	0.25
4	0.8	0.666667	0.6	0.25	0.25	0.25
5	0.8	0.666667	0.666667	0.5	0.5	0.5
6	0.666667	0.466667	0.733333	0.5	0.25	0.25
7	0.666667	0.466667	0.733333	0.25	0.25	0.25
8	0.666667	0.466667	0.733333	0.25	0.25	0.25
9	0.666667	0.466667	0.8	0.5	0.25	0.25
10	0.666667	0.466667	0.733333	0.25	0.5	0.5
Average	0.733333	0.566667	0.726667	0.375	0.3	0.3
Standard Deviation	0.070273	0.105409	0.058373	0.125	0.1	0.1

5.3.1 Comparison Graph Results

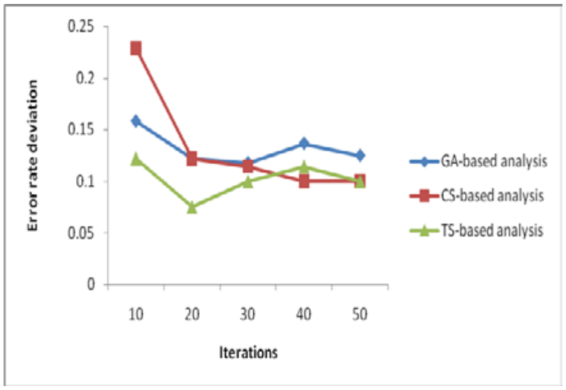

Figure 1: Performance Of Error Rate Deviationvs Iterations In Existing Method

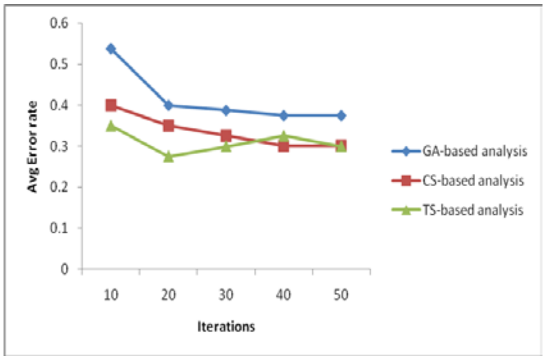

Figure 2: Performance Of Average Error Rate Vs Iterations In Existing Method

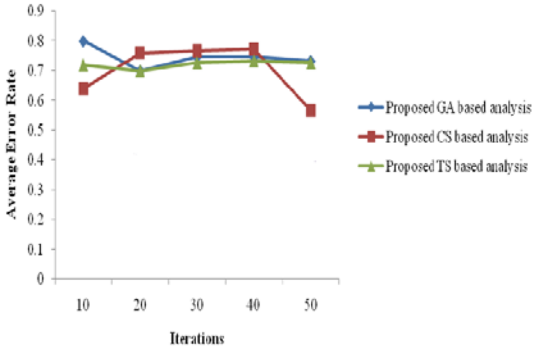

Figure 3: Performance Of Average Error Rate Vs Iterations In Proposed Method

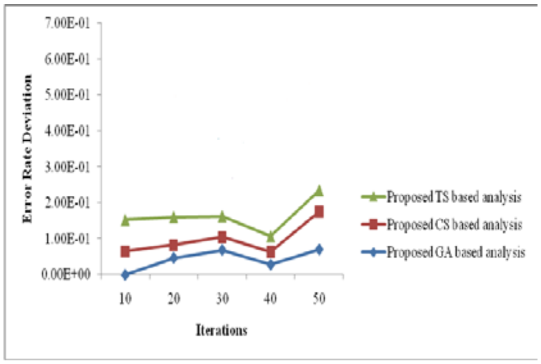

Figure 4: Performance Of Error Rate Deviation Vs Iterations In Proposed Method

DISCUSSION:

Table 1 and 3 indicate that TS has minimum error rate. But in case of Table 2 TS has minimum error rate. And the Table 4 it is observed that CS has minimum error rate. But from the Table5 it is observed that CS and TS has minimum error rate.

From the figure 1 it is observed that GA and CS has 3.6% and 10.6% error rate higher than TS in 10thiteration respectively. In 20thiteration GA and CS has error rate deviation as 4.7% higher than TS. In 30thiteration GA and CS has error rate deviation as 1.7% and 1.4% respectively higher than TS. But in case of 40thiteration CS has lower error rate deviation than GA (3.6%) and CS (1.4%).whereas in case of 50th iteration CS and TS has same error rate value and GA has more deviation of 2.5% than GA and TS. From this it is concluded that by performing more number of iterations CS will have better performance than GA and TS.

From the figure 2 it is observed that average error rate value of GA is more than CS, TS in 10th iteration. And the deviation difference between GA and CS is 13.7% in 10th iteration and is reduced to 0.5% in 20th iteration and goes to the same extent of same value for other iterations. So GA will perform poor. As CS has a higher error rate value, the deviation difference between CS and TS is 7.5% in the 20thiteration. But in case of 30th iteration the deviation difference reduced to 1.4%. And TS increases to 1.4% above CS in 40th iteration. In the 50th iteration TS deviates to the same level of CS and both performs better. But for further iterations there is a chance for TS to deviates higher but CS is stable for some extent and so CS performs better.

From the figure 3, proposed method heuristic technique analysis has given higher error rate than the existing method. The higher the error rate shows the information sharing without loss the information. In Proposed method, the average error rate value of GA based analysis has attained 80% which is 18% and 6% higher than the CS and TS methods at the iteration value is 10. When increasing the iteration value 20, 30 and 40 the GA and TS average error rate performance is in same level but the CS error rate is slightly deviated from other two methods. At the 50th iteration, the average error rate value of CS method has decreased at 56% but the GA and TS has acquired same level average error rate performance. In existing technique, the heuristic method analysis has given low average rate performance it shows the loss of information between the parties. From the figure 4, Proposed technique error rate deviation is low than the existing technique. The low error rate deviation shows the reliable average error rate within the heuristic methods i.e. the error rate is change at minimum level. The higher the error rate deviation in the existing methods shows that the error rate is not in the specified level.

7. CONCLUSION

From the analysis it is observed that in the QSS protocol, GA algorithm based heuristic attack ensures that communication is secure. But in case of TS and CS algorithm based heuristic attacks QSS protocol has no robustness. To improve the robustness of QSS protocol using such attacks, elliptic curve cryptography is used. The comparison result shows that Proposed ECC based QSS protocol has given more secure information sharing than the existing approach. Hence, it is proved that

Proposed ECC based four party QSS protocol is more secured than the existing method.

REFERENCES:

[1]Rahul Aggarwal, Heeren Sharma and Deepak Gupta, "Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol", International Journal of Computer Applications (0975 – 8887), Vol.20, No.8, pp.28-31, 2011

[2]Nur Atiqah Muhammad and Zuriati Ahmad Zukarnain, "Implementation of BB84 Quantum Key Distribution Protocol's with Attacks", European Journal of Scientific Research, Vol.32 No.4, pp.460-466, 2009.

[3] Muhammad Mubashir Khan and Jie Xu, "Quantum Cryptography with Generalized Bases and Dimensions of Photon States", International Journal of Security and Its Applications, Vol. 6, No. 1, pp. 49- 56, 2012.

[4]Fei Gao, Su-Juan Qin, Fen-Zhuo Guo, and Qiao-Yan Wen, "Dense-Coding Attack on Three-Party Quantum Key Distribution Protocols", IEEE journal of quantum electronics, Vol. X, No. X, pp. 1-6, 2010.

[5] Mohamed Elboukhari, Abdelmalek Azizi, and Mostafa Azizi, "Integration of Quantum Cryptography in the TLS Protocol: Reality and Perspectives", MICS'10 International conference, Ensias, Rabat Morocco, Nov 2-4, 2010

[6]Rishi Dutt Sharma, "Quantum Cryptography: A new approach to information security", International Journal of Power System Operation and Energy Management (IJPSOEM), Vol.1, No. 1, pp.11-13, 2011

[7]G.Ananda Rao, Y.Srinivas, J.Vijaya Sekhar and Ch.Pavan Kumar, "Three Party Authentication Key Distributed Protocols Using Implicit and Explicit Quantum Cryptography", Indian Journal of Computer Science and Engineering, Vol. 2, No. 2, pp. 143-145, 2011.

[8]T.Rubya N. Prema Latha and B.Sangeetha, "A Survey on Recent Security Trends using Quantum Cryptography", (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, No. 09, pp. 3038-3042, 2010.

[9]Thi Mai Trang Nguyen, Mohamed Ali Sfaxi and Solange Ghernaouti-Helie, "802.11i Encryption Key Distribution Using Quantum Cryptography", Journal of networks, Vol. 1, No. 5, pp.9-20,2006

[10] Zhang Xing LAN, "One-way quantum identity authentication based on public key", Chinese Science Bulletin, Vol.54, No.12, pp.2018-2021, 2009.

[11] Veronica Fernandez, Robert J. Collins, Karen J. Gordon, Paul D. Townsend, and Gerald S. Buller , "Passive Optical Network Approach to Giga Hertz-Clocked Multiuser Quantum Key Distribution", IEEE journal of quantum electronics, Vol. 43, No 2, pp.1-9,2007

[12] Kyo Inoue, "Quantum Key Distribution Technologies", IEEE journal of selected topics in quantum electronics, Vol. 12, No. 4, pp.888-896, 2006.

[13] Xiao-Ming Xiu ,Li Dong, Ya-Jun Gao, Feng Chi, Yuan-Peng Ren and Hui-Wei Liu, "A revised controlled deterministic secure quantum communication with five-photon entangled state",Journal Optics Communications, Vol.283,No. 2, pp. 344–347, 2010.

[14] I-Ching Yu, Feng-Li Liny and Ching-Yu Huangz, "Quantum secret sharing with multilevel mutually (un)biased base", Phys. Rev letters, Vol.78, No.1, pp.1-5, 2008.

[15]Zhang Zhan Jun and Man zhong xiao, "Multiparty quantum secret sharing of key using practical faint laser pulses", Chin.Phsy.Letters, Vol.22, No.7, pp.1588-1591, 2005.

[16] Majid Safari and Murat Uysal, "Relay-Assisted Quantum-Key Distribution over Long Atmospheric Channels", Journal of light wave technology, Vol. 27, No. 20, pp.4508-4515, 2009.

[17]Pradeep Kumar and Anil Prabhakar, "Quantum Key Distribution using Spin Wave–Optical Interactions", IEEE journal of quantum electronics, Vol. 46, No. 11, pp.1542-1548,2010.

[18] Gan Gao, "Cryptanalysis of multiparty quantum secret sharing with collective eavesdropping-check", Journal Optics Communications, Vol. 283, No.14, pp.2997–3000, 2010.

[19]K. Sathi Reddy and Raja Kumar Medapati, “Three Party Quantum Authenticated Key Distribution Protocol Using Superposition States”, Int. J. Comp. Tech. Appl., Vol 2,No.5, pp.1589-1594,2011.

[20] Gaige Wang, Lihong Guo, Hong Duan, Luo Liu, Heqi Wang and Jianbo Wang, ” A Hybrid Meta-heuristic DE/CS Algorithm for UCAV Path Planning”, Journal of Information & Computational Science,Vol. 9,No. 16,pp. 4811–4818,2012.

[21]Ehsan Valian, Shahram Mohanna and Saeed Tavakoli,” Improved Cuckoo search algorithm for feed forward neural network training”, International Journal of Artificial Intelligence & Applications (IJAIA), Vol.2, No.3,pp.36-43, 2011.

[22]Honxia Shi, Yi ouyang,” A Novel Fast η - Adapt Slide Window Elliptic Curve Cryptography Algorithm”, Network Computing and information security, Vol.345, pp.56-62, 2012.