Quantum Secret Sharing Protocol using the heuristic Attacks

[1]Rajaram Jatothu,[2]Dr. R P Singh
[1]Research Scholar, 2 Research Guide
[1]SSSUTMS, Sehore, India, [2]SSSUTMS, Sehore, India

***Abstract*— In this work to dissect the power of the four party QSS protocol exceptionally well known heuristic attack are executed. This heuristic attack is molded by three prevalent heuristics calculations, for example, Quantum motivated Genetic Algorithm (GA), and Tabu Search Algorithm (TSA) and Cuckoo Search Algorithm (CSA) .The mobile ad-hoc network (MANET) is one of the self-configuring infrastructures less network, of mobile terminals associated by wireless. Quantum cryptography is the science of exploiting quantum mechanical properties to achieve cryptographic perform tasks. The best known example of quantum cryptography quantum key distribution is which offers and information secure solution.**

***IndexTerms*— Heuristic attacks, MANET, Cuckoo Search Algorithm, Quantum Secret Sharing Protocol**

I. INTRODUCTION

Mystery sharing is a common issue in the excellent cryptography which is a system for part of a message into a few sections so that the whole set is expected to read thoroughly the message. QSS (Quantum Secret Sharing) is the imperative branch in quantum cryptography consolidates quantum standards with established cryptography. A four gathering QSS protocol is utilized for sharing quantum state data between parties in the quantum framework is broke down also, examined here. One of the real issues in traditional figuring is Backpack (or) Rucksack issue and this issue has been settled effectively by methods for Quantum Inspired traditional hereditary, cuckoo look also, tabu hunt calculations. The real issue in executing quantum cryptographic convention is quantum bit mistake. Heuristic assault is created utilizing hereditary, cuckoo hunt and tabu inquiry calculation. Along these lines this section concentrates on breaking down the security in multiparty correspondence with the execution parameters, for example, calculation time and mistake rate. The nuts and bolts of established mystery sharing are examined in the beneath segment.

CLASSICAL SECRET SHARING PROTOCOL

A secrecy sharing plan is identified with key foundation. The unique inspiration for mystery sharing is to shield cryptographic keys from misfortune; it is attractive to make reinforcement duplicates. The more noteworthy the quantity of duplicates made, the more noteworthy the danger of security presentation; the littler the number, the more prominent the danger of losing. The possibility of mystery sharing is to begin with a mystery, what's more, partition it into pieces called shares which are dispersed among clients with the end goal that the pooled offers of particular subsets of clients permit reproduction of the first mystery. The general model for mystery sharing is appeared in the Figure 1.

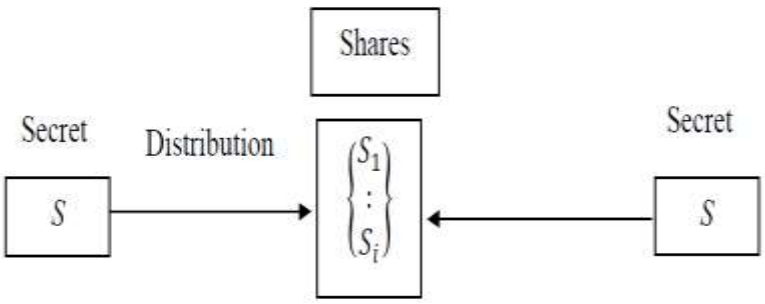

Figure 1 The general model for secret sharing

QUANTUM SECRET SHARING (QSS) PROTOCOL

Exhibition of four-party quantum secrecy sharing by means of four photon entrapment was executed here. In any case, the subsequent mystery key is new. There is no unique key which must be reproduced. In other words, the plan isn't a mystery sharing plan as it claims. Normally, it is a key foundation. Decisively, it is a variety of BB84 plot. The gathering A comprises of any client from the four clients. The gathering B comprises of the other three clients. In like manner, the plans are not mystery sharing plans as guaranteed. Alice, Bob, Claire and David each offer a photon from the following four-photon polarization-entrapped state.

$$|\psi\rangle = \frac{1}{2\sqrt{3}}[2|HHVV\rangle - |HVHV\rangle - |HVVH\rangle - |VHHV\rangle - |VHVH\rangle + 2|VVHH\rangle]_{abcd} \quad (4.1)$$

Where H and V indicates horizontals, vertical polarization of photons in the four spatial modes a, b, c, and d. In the accompanying, we accept that Alice is the merchant. Each gathering picks haphazardly between two correlative estimation bases. To swap over the estimation comes about into a key grouping; every member recognizes his outcome with a bit estimation of 0 or 1. The estimations will be rehashed until the point when they set up a crude key of wanted length. For key filtering, every member reports freely at whatever point he has enrolled a photon and which estimation premise he has utilized, yet not the outcomes. After key filtering, all members need to check for outer spying. At long last get a typical secure key; they need to perform key compromise and security intensification. The accompanying segment will talk about the proposed four gathering QSS protocol with developmental calculations.

II. FOUR PARTY QSS PROTOCOL

The QSS protocol is created to share the quantum state data amongst parties and the strength of the convention is approved by misusing the heuristic assaults. This strategy shares the quantum data among parties by creating EPR combines in the trapped states. The QSS protocol considered four gatherings in the quantum state to share the data also, is called as four gathering quantum mystery sharing. The fundamental strategies of four gathering QSS protocols are described below.

- Assume that Alice (A) as boss to share the information between the parties Bob (B), Charlie (C) and David (D).
- Initially Alice at random generate particles to the parties Bob, Charlie and David on the starting point of (| 0|>,|1|>) . By utilizing these quantum states Alice prepares N EPR pairs in the entangled states.

$$|\psi^-\rangle_{A_iB_i} = \frac{1}{\sqrt{2}}(|0\rangle_{A_i}|1\rangle_{B_i} - |1\rangle_{B_i}|0\rangle_{B_i})$$

$$|\psi^-\rangle_{A_iC_i} = \frac{1}{\sqrt{2}}(|0\rangle_{A_i}|1\rangle_{C_i} - |1\rangle_{B_i}|0\rangle_{C_i})$$

$$|\psi^-\rangle_{A_iD_i} = \frac{1}{\sqrt{2}}(|0\rangle_{A_i}|1\rangle_{D_i} - |1\rangle_{B_i}|0\rangle_{D_i})$$

- The number of established particles Rn approved by the receivers B, C, and D are N, Alice goes to the next step or else, Alice terminates the QSS protocol.
- Then Bob, Charlie and David randomly select a set of particles from their received particles and make Bell measurements on them in the measurement bases (|0>,|1>) and then notify Alice the order and the measurement basis of their chosen particles.
- According to the measurement result from Bob, Charlie and David, Alice performs Bell measurements on the same particle of Bob, Charlie and David and Alice compares his measurement result with Bob, Charlie and David results to detect eavesdropping.
- If their resulting bits are compared with a certain threshold Value α, the error rate Er does not exceed a certain threshold (α)the communication is secure, otherwise the QSS will not be in a secure state. The process of QSS protocol process is illustrated in the following Figure,

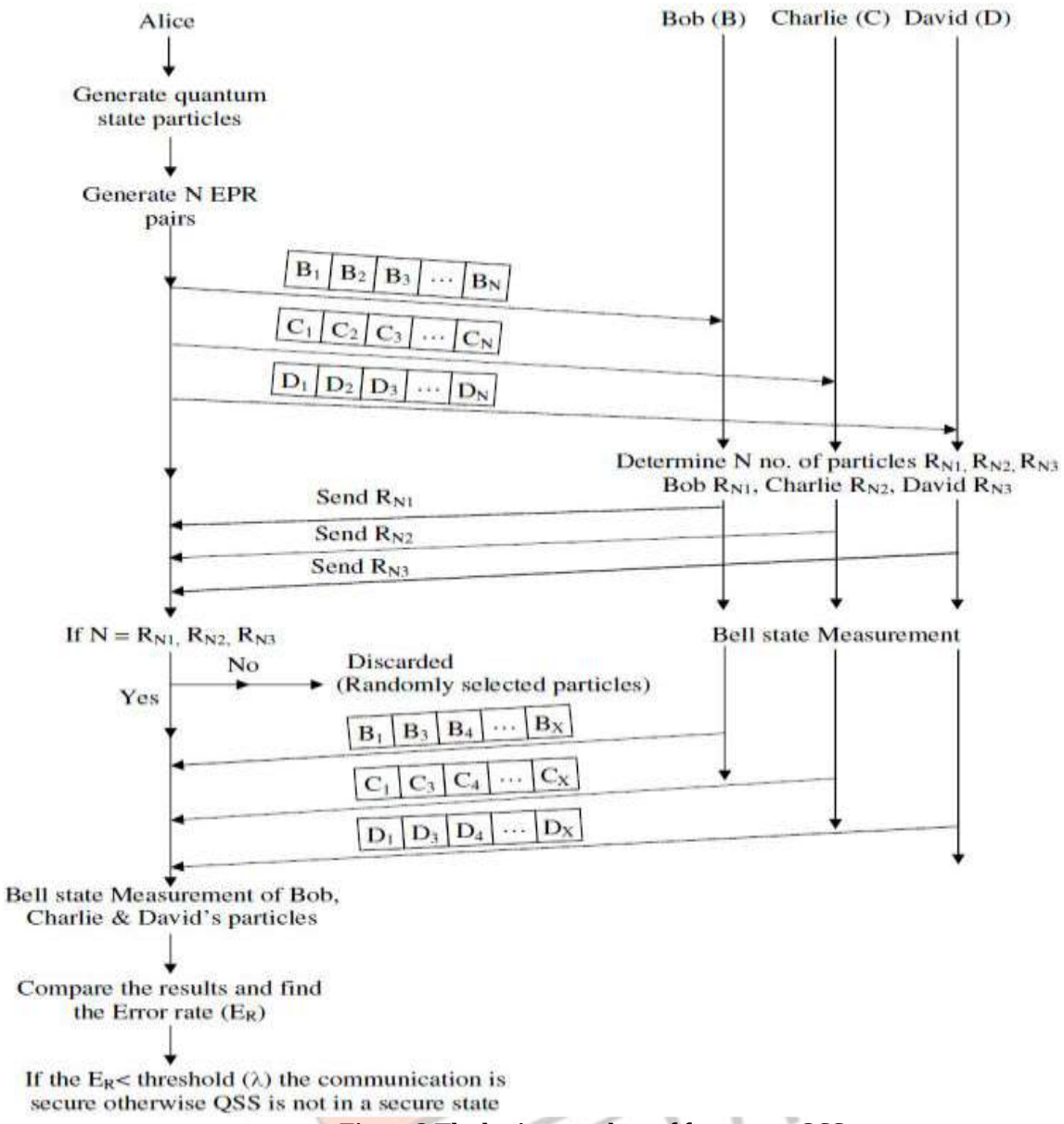

Figure 2 The basic procedure of four party QSS

III. QUANTUM SECRET SHARING WITH HEURISTIC ATTACK

To dissect the power of the four party QSS protocol exceptionally well known heuristic attack are executed. This heuristic attack is molded by three prevalent heuristics calculations, for example, Quantum motivated Genetic Algorithm (GA), Tabu Search Algorithm (TSA) and Cuckoo Search Algorithm (CSA).

Attack Generation by Quantum Inspired Genetic Algorithm (QIGA)

Genetic Algorithms (GAs) are versatile heuristic inquiry calculation in view of the transformative thoughts of normal choice and hereditary qualities. All things considered they speak to a clever abuse of an arbitrary hunt used to tackle advancement issues. Albeit randomized, GAs are in no way, shape or form arbitrary, rather they abuse recorded data to coordinate the pursuit into the locale of better execution inside the inquiry space. GAs reenacts the survival of the fittest among people over back to back age for tackling an issue. Every age comprises of a populace of character strings that are similar to the chromosome. Every individual speaks to a point in a hunt space and a conceivable arrangement. The people in the populace are then made to experience a procedure of development. By abusing GA, the heuristic assault will be produced for breaking down the QSS convention.

Attack Generation by Quantum Inspired Tabu Search Algorithm (QITSA)

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 an 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 principle of TS are 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.

Attack Generation by Quantum Inspired Cuckoo Search Algorithm (QICSA)

In Cuckoo search (CS), each egg in a nest represents a resolution, and a cuckoo egg represents a new solution. The plan 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.

IV. RESULT AND DISCUSSION

In this four gathering QSS protocol some heuristic assaults based QIGA, QITSA and QICSA are produced to assess the power of the data sharing. The normal blunder rate figuring, mistake rate deviation, normal computational time, time deviation count are made and arranged underneath in this segment. From the tables 1 and 2, it is watched what calculation performs with less computational time for more number of emphases. Likewise least blunder rate should observed to be not as much as the edge esteem (ʎ) though the correspondence is secure generally isn't secure i.e. the data is hacked by busybody. In this investigation heuristic assaults are produced for cryptanalysis enquiry. This could be performed utilizing the Matrix arrangement of the heuristic assaults .The execution of the proposed framework is assessed by changing the network estimate under 10 tests and the outcomes are analyzed against the QIGA, QITSA, and QICSA. The outcomes under each condition are organized underneath and the base mistake esteem hold calculation is advanced to advance examination.

Iterations	Average error rate			Average computation time(sec)		
	QIGA (proposed)	QICSA (proposed)	QITSA (proposed)	QIGA (proposed)	QICSA (proposed)	QITSA (proposed)
10	0.5375	0.4	0.35	0.018162	0.012237	0.014621
20	0.4	0.35	0.275	0.019874	0.014943	0.010203
30	0.3875	0.325	0.3	0.021312	0.011617	0.013204
40	0.375	0.3	0.325	0.022683	0.010491	0.014435
50	0.375	0.3	0.3	0.023986	0.01065	0.010167

Table 1 Average error rate and average computation time of QIGA, QICSA& QITSA for iterations =10, 20, 30, 40 & 50

Iterations	Error rate deviation			Computation time deviation(sec)		
	QIGA (proposed)	QICSA (proposed)	QITSA (proposed)	QIGA (proposed)	QICSA (proposed)	QITSA (proposed)
10	0.158607	0.229129	0.122474	0.004236	0.00342	0.006892
20	0.122474	0.122474	0.075	0.001454	0.009629	0.000887
30	0.117925	0.114564	0.1	0.002176	0.003505	0.008579
40	0.136931	0.1	0.114564	0.003372	0.000816	0.011351
50	0.125	0.1	0.1	0.004663	0.000629	0.001296

Table 2 Error rate deviation and computation time deviation of QIGA, QICSA& QITSA for iterations =10, 20, 30, 40 & 50

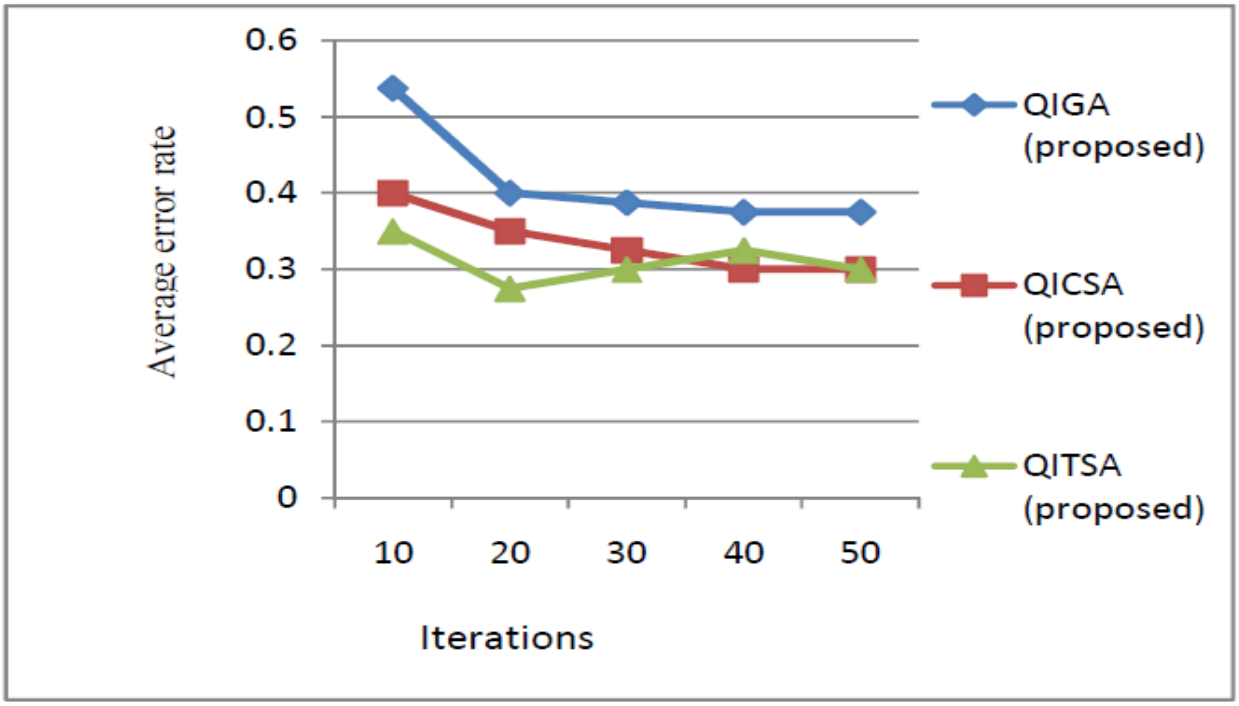

Figure 3 Number of iterations vs average error rate for the proposed QSS based heuristic search algorithms

From the Figure 3, it is observed that QIGA and QICSA has 3.6% and 10.6% error rate higher than QITSA in 10thiteration respectively. In 20th iteration QIGA and QICSA has error rate deviation as 4.7% higher than QITSA. In 30thiteration QIGA and QICSA has error rate deviation as 1.7% and 1.4% respectively higher than QITSA. But in case of 40thiteration QICSA has lower error rate deviation than QIGA (3.6%) and QICSA (1.4%).whereas in case of 50th iteration QICSA and QITSA has same error rate value and QICSA has more deviation of 2.5% than QIGA and QITSA. From this it is concluded that by performing more number of iterations QICSA will have better performance than QIGA and QITSA.

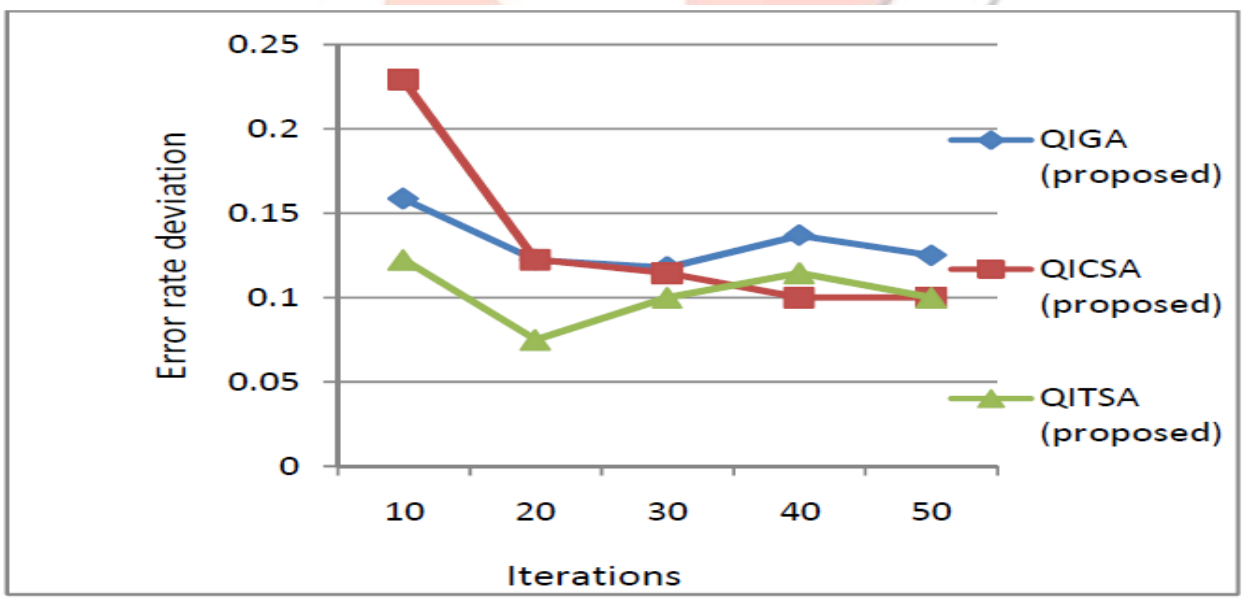

Figure 4 Number of iterations vs error rate deviation for the proposed QSS based heuristic search algorithms

From the Figure 4, it is observed that average error rate value of QIGA is more than QICSA, QITSA in 10th iteration. And the deviation difference between QIGA and QICSA 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 QIGA will perform poor. As QICSA has a higher error rate value, the deviation difference between QICSA and QITSA is 7.5% in the 20thiteration. But in case of 30th iteration the deviation difference reduced to 1.4%. And QITSA increases to 1.4% above QICSA in 40th iteration. In the 50th iteration QITSA deviates to the same level of QICSA and both performs better. But for further iterations there is a chance for QITSA to deviates higher but QICSA is stable for some extent and so QICSA performs better.

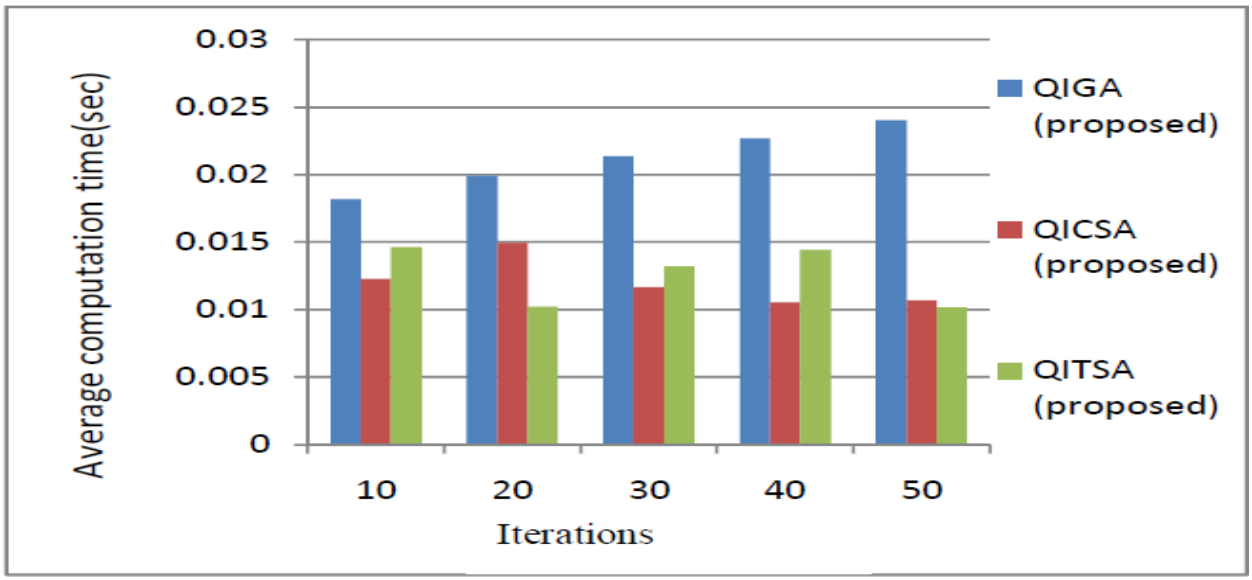

Figure 5 Number of iterations vs averge computation time for the proposed QSS based heuristic search algorithms

From the Figure 4.5, it is found that QICSA algorithm performs better than QIGA and QITSA. The encircled spots in the above representation infer that they are not hacked. From the analysis it is also concluded that QICSA will perform better by increasing number of iterations.

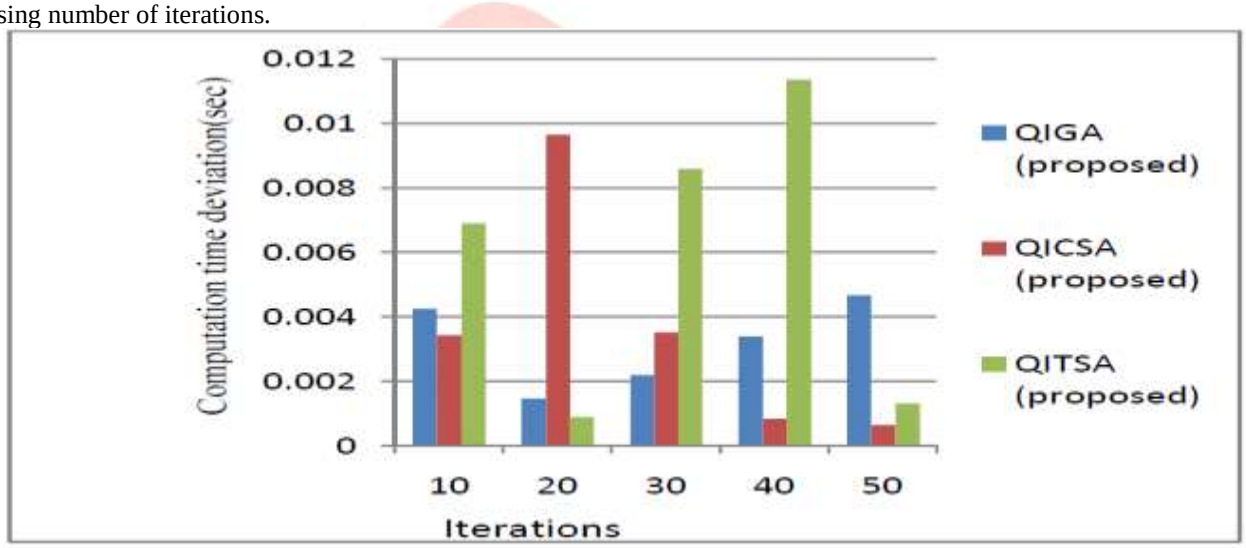

Figure 6 Number of iterations vs Computation time deviation for the proposed QSS based heuristic search algorithms

From the Figure 6 it is found that QICSA performs better than QIGA and QITSA. The evaluation result under the circumstance of different iterations for QICSA is found to be better than other two algorithms. The experimental results indicate that QICSA takes more iteration to analyze the robustness of the protocol. Thus compared to classical algorithms Quantum inspired evolutionary algorithms performs better because of Quantum superposition, Quantum entanglement and Quantum gates.

V. Conclusion

This section has featured the highlights of quantum propelled algorithms, for example, QIGA, QICSA and QITSA and contrasted their execution and the traditional calculations, for example, GA, CSA and TSA. Four gathering quantum mystery sharing are executed and dissected. Heuristic assaults are created utilizing Quantum enlivened hereditary, cuckoo inquiry and tabu pursuit calculations. Exhibitions are assessed regarding calculation time and mistake rate. From the correlation, the Quantum propelled heuristic inquiry calculations performs better as far as both blunder rate and calculation time on account of the Quantum standards, for example, Quantum superposition, Quantum entanglement, Heisenberg's vulnerability rule and no-cloning hypothesis.

References

[1] T. ElGamal, ―A public-key cryptosystem and a signature scheme based on discrete logarithms,‖ IEEE Trans. Inf. Theory, vol. IT-31, no. 4, pp. 469–472, Jul. 1985. 125

[2] M. Abadi and B. Blanchet. Secrecy types for asymmetric communication.In Foundations of Software Science and Computation Structures (FoSSaCS 2001), volume2 pp20-30

[3] Cheminod, M.; Cibrario Bertolotti, I.; Durante, L.; Sisto, R.; Valenzano, A.;‖ Experimental Comparison of Automatic Tools for the Formal Analysis of Cryptographic Protocols‖ Dependability of Computer Systems, 2007. DepCoS-RELCOMEX '07. 2nd International Conference on 14-16 June 2007 Page(s)153 - 160

[4] Markovic, M ‖ Data Protection Techniques, Cryptographic Protocols and PKI Systems in Modern Computer Networks‖ Systems, Signals and Image Processing, 2007 and 6th EURASIP Conference 27-30 June 2007 Page(s):13 - 24
[5] G. R. Blakley and D. Chaum, Eds., Advances in Cryptology Proceedings of Crypto '84. Berlin, Germany: Springer-Verlag, 1985.
[6] Gura, N., Patel, A.,Wander, A., Eberle, H., Shantz, S. C.: Comparing elliptic curve cryptography and RSA on 8-bit CPUS , ESAS 04, Lecture Notes in Computer Science, Vol. 3156, pp. 119- 132, August 2004.
[7] I. Blake, G. Seroussi, N. Smart, ―Elliptic Curves in Cryptography,‖ London Mathematical Society, Lecture Note Series 265, Cambridge University Press, 1999.
[8] Standard Specifications for Public Key Cryptography, IEEE1363, 2000 126
[9] M. Hasler, ―Synchronization of chaotic systems and transmission of information,‖ Int. J. Bifurc. Chaos, vol. 8, no. 4, Apr. 1998.
[10] M. J. Ogorzalek, ―Taming chaos—Part I: Synchronization,‖ IEEE Trans. Circuits. Syst. I, Fundam. Theory Appl., vol. 40, no. 10, pp. 693–699, Oct. 1993.
[11] T. Yang,―A survey of chaotic secure communication systems,‖ Int. J.Comput. Cogn. 2004 [59] J. L. Massey, Contemporary Cryptology: An Introduction, G. J. Simmons, Ed. New York: IEEE Press, 1992.
[12] W. Bagga and R. Molva. Policy-based cryptography and applications. In Proceedings of Financial Cryptography and Data Security (FC'05), volume 3570 of LNCS, pages 72–87. SpringerVerlag, 2005
[13] J. Holt, R. Bradshaw, K. E. Seamons, and H. Orman. Hidden credentials. In Proc. of the 2003 ACM Workshop on Privacy in the Electronic Society. ACM Press, 2003.
[14] S.S. Al-Riyami, J. Malone-Lee, and N.P. ―Smart. Escrow-free encryption supporting cryptographic workflow‖. Cryptology ePrint Archive, Report 2004/258, 2004. http://eprint.iacr.org/.
[15] David Williams ―A new information science Quantum information processing is based on quantum mechanical principles 127 and includes quantum computing and cryptography‖ materials today July-August 2007 Volume10
[16] Fred Piper ―Some trends in research in cryptography and security mechanisms‖ Research in cryptography and security mechanisms Elsevier Science Ltd March 2003 pp 23-26
[17] Michael P. Howarth, Sunil Iyengar, Zhili Sun, Member, IEEE, and Haitham Cruickshank, Member, IEEE‖ Dynamics of Key Management in Secure Satellite Multicast‖ IEEE Journal On Selected Areas In Communications, Vol. 22, No. 2, February 2004 pp 308-319
[18] Vengatesan K., and S. Selvarajan: Improved T-Cluster based scheme for combination gene scale expression data. International Conference on Radar, Communication and Computing (ICRCC), pp. 131-136. IEEE (2012).
[19] Kalaivanan M., and K. Vengatesan.: Recommendation system based on statistical analysis of ranking from user. International Conference on Information Communication and Embedded Systems (ICICES), pp.479-484, IEEE, (2013).
[20] K. Vengatesan, S. Selvarajan: The performance Analysis of Microarray Data using Occurrence Clustering. International Journal of Mathematical Science and Engineering, Vol.3 (2) ,pp 69-75 (2014).