ANALYSIS OF SOME QUANTUM BASED ALGORITHMS WITH GKM APPROACH FOR E-COMMERCE APPLICATIONS

[1] UDAYABHANU N P G RAJU [2]Dr. R VIVEKANANDAM
[1]Research Scholar, SSSUTMS SEHORE, MP
[2]Research Guide, SSSUTMS, SEHORE, MP

ABSTRACT

We present several quantum based schemes that are relevant to the security factors of E-commerce applications. To achieve an efficient use of QKD mechanisms to secure E-Commerce applications,we propose to integrate quantum key distribution into main group key protocols. It gives some benefits and contributions of the use of quantum Key Distribution to enforce security level. A few practicality approaches to actualize arrangements in light of quantum key distribution are proposed to accomplish proficient correspondence among the E-trade applications.

Keywords: Quantum Key Distribution, Security, Group Key management, Cryptographic computations

INTRODUCTION

Utilizing the progress from the Internet and in addition advancement of information innovations, various regular disconnected administrations for instance banking, sending and government undertakings have a tendency to relocate to on-line composes. As of now, making data arranged association comes to end up plainly mechanical innovation as well as moreover business procedure to secure contending power. Web based business, which treats business activities by on the web, is the most outstanding case and furthermore personally identified with our genuine life. In any case, people are as yet mindful about using such helpful devices. This truly is started from worries on security of their points of interest. Characteristic feeble purposes of the Web and exchange offs between general execution and assurance expands clients' doubt. Vast quantities of interchanges that contains client's private data are gone up against by pernicious activities. In this way it truly is clear that individuals ought to submit ourselves to have the capacity to outlining safe E-business programs however not reducing effectiveness.

LITERATURE REVIEW

Sun et al., proposed modified access polynomial based self-healingkey management schemes that used broadcast authentication to reduce collusion attacks in E-commerce applications. Two attacks were introduced to interrupt the security of accesspolynomials. The collusion resistance was defined according to the sessioninterval. The security was achieved and the packet losses were tolerated with thehelp of the sliding window and modified access polynomial. The resourceconsumption was reduced and the errors in the access polynomials were avoided.The results showed that the proposed scheme attained forward and backwardsecrecy as well as avoided the collusion attack.

Sumalatha and Sathyanarayanan, proposed an Enhanced IdentityBased Cryptography (EIBC) for managing group keys in the E-commerce cellular network. The exchange ofpublic key certificates were eliminated and publicly known identity was enabled.Further, a mathematical model was formulated for multicast group keymanagement. The results proved that the EIBC scheme was highly secure.Suganthi and Sumathy proposed an energy efficient keymanagement scheme to secure the data in the NETWORK. Further, the suggestedalgorithm established three keys, namely, pair wise key, individual key and agroup key. The BSs and the neighbor nodes shared the individual keys and thepair-wise keys respectively, whereas all the nodes shared the group key. The keyswere calculated using the polynomial function at the time of initialization,membership change and key compromise. When compared with the existingmethods, the proposed scheme achieved low computation, communication andstorage overhead.

PROPOSED WORK

The fabulous assurance of quantum PCs is to enable new computations (called quantum counts), that offer responses for issues requiring exorbitant resources for their answer on a built up PC. Two wide classes of quantum figurings are known which fulfill this certification. The highest point of the line of figurings relies upon Shor's quantum Fourier changes and consolidates extraordinary computations for understanding the considering and discrete logarithm issue. These counts give a striking exponential quicken over the best known built up estimations. The mediocre of count relies upon Grover's estimation for performing quantum chasing. These give an essential quadratic quicken over the best conventional estimations. The quantum look for figurings get its noteworthiness from the wide use of interest based techniques in customary estimations which in numerous events allow a reasonable change of the output for the given issue.

Most present theoretical quantum computations rely upon quantum property called quantum parallelism. Quantum parallelism rises up out of the limit of a quantum memory enroll to exist in a superposition of base

states. A quantum memory enlist can exist in a superposition of states, each fragment of this superposition may be thought of as a single dispute to a limit. A limit performed on the enlist in a superposition of states is subsequently performed on each of the fragments of the superposition, yet this limit is simply associated one time. Since the amount of possible states is 2n where n is the amount of qubits in the quantum enlist, we can perform in one activity on a quantum PC what may take an exponential number of tasks on a built up PC. This is mind blowing, yet as the amount of superposed states increases in the quantum select, the probability of estimating a particular one will decrease.

Quantum look computations have various potential applications. Specific parts of quantum look for figurings can be associated with various issues in programming designing to quicken computations for a couple of issues in NP especially, those issues for which a straight search for an answer is the best count known. Quantum mechanics can immensely quicken looking strategy over unstructured database or discretionarily passed on data. In a quantum look for process, the evaluation of interest space require not be finished picking one thing at any given minute from the chase space rather the request can be associated direct to social events of things superposed together. Quantum enrolling requires to make programs in an absolutely new way some of which are absolutely inconsequential with a customary PC e.g. superposition. An essential accomplishment happened with LovGrover‟s snappy count that is ended up being the speediest workable for looking for through unstructured databases. The count is productive to the point that it requires for the most part √N (where N is the total number of segments in the interest space) request to find the pined for thing, rather than chase in conventional figuring, which all things considered requires N/2 looks. The quantum look computation offers only a quadratic speedup, instead of the more awesome exponential speedup offered by estimations in light of the quantum Fourier change.

Grover's count has another extraordinarily accommodating application, in the field of part encoded data. Quantum PCs can break DES (Data Encryption Standard) for the most part used system to secure data. A careful interest by customary means would take a long time (substantially finished a year). Regardless, Grover's computation could find the DES enciphering key in not long after couple of endeavors when diverged from customary figuring. Grover states that "A web crawler could investigate every nook and corner of the Internet in thirty minutes, a savage power decoder could unscramble the DES transmission in five minutes". These numbers are stunning stood out from the speediest conventional estimation's number of today.

Estimation get ready for quantum PCs isn't basic. Fashioners go up against issues, not looked in the advancement of counts for customary PCs. The issue is that our human nature is built up in the customary world. In case we use that impulse as a manual for the advancement of figuring, by then the algorithmic

contemplations we consider will be conventional considerations. To plot incredible quantum figuring's one must execute one's built up sense for at any rate some part of the arrangement methodology. At precisely that point we can achieve the pined for algorithmic end.

QKD WITH GKM BASED ALGORITHMS FOR E-COMMERCE APPLICATIONS

Quantum Parallelism Hadamard Transformation

Quantum parallelism is fundamental feature of many quantum algorithms. Quantum parallelism allows quantum computers to evaluate a function f (x) for many different values of x simultaneously. Let us explain how quantum parallelism works, and some of its limitations.

Suppose f (x): {0,1}→{0,1} is a function with a one bit domain and range. A convenient way of computing this function on a quantum computer is to consider a two qubit quantum computer which starts in the state |x, y>. With an appropriate sequence of logic gates it is possible to transform this state into |x, y ⊕f (x)>, where ⊕ indicates addition modulo 2; the first register is called the „data" register, and the second register the „target" register. It give the transformation defined by the map |x, y>→|x, y ⊕f (x)>a nameUf, and note that it is easily shown to be unitary. If y=0, then the final state of the second qubit is just the value f (x).Consider the function shown in Figure 1, which applies Uf to input not in the computational basis. Instead, the data register is prepared in the superposition (|0>+|1>)√/2, which can be created with a Hadamard gate acting on |0>. Then apply Uf resulting in the state,

$$(|0, f(0)\rangle + |1, f(1)\rangle)/\sqrt{2}$$

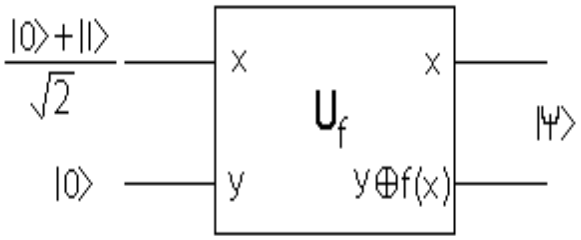

Figure 1: Quantum circuit for evaluating f (0) and f (1) simultaneously

The diverse terms contain data about f (0) and f (1) it is practically as though we have assessed f (x) for two estimations of x at the same time, an element known as quantum parallelism. Not at all like traditional parallelism, where numerous circuits each worked to process f (x) are executed all the while, here is a solitary f

(x) circuit utilized to assess the capacity for various estimations of x at the same time, by abusing the capacity of a quantum PC to be in super positions of various states.

The Deutsch- Jozsa Algorithm

This prophet sums up the Deutsch prophet to a capacity f: {0,1}n → {0,1}. The capacity is steady or adjusted in every one of the stages. Here adjusted implies that the capacity is 0 on half of its contentions and 1 on the other half. Obviously for this situation the capacity might be neither steady nor adjusted. For this situation the prophet doesn't work. It might state yes or no yet the appropriate response will be useless. Likewise here the calculation enables one to assess a worldwide property of the capacity in one estimation in light of the fact that the yield state is as upper position of adjusted and steady states with the end goal that the adjusted expresses all lie in a subspace orthogonal to the consistent states and can in this manner be recognized from the last in a solitary estimation. Conversely, the best deterministic established calculation would require 2n/2+1 inquiry to the prophet with a specific end goal to take care of this issue.

Heisenberg Uncertainty Principle Algorithm

In 1984 Charles Bennett and Gilles Brassard distributed the primary QKD convention. It depended on Heisenberg's Uncertainty Principle and is basically known as the BB84protocol after the author‟s names and the year in which it was distributed. It is as yet a standout amongst the most unmistakable conventions and one could contend that the greater part of the other HUP based conventions are basically variations of the BB84 thought. The fundamental thought for these conventions at that point is that Alice can transmit a randomsecret key to Bob by sending a series of Photons where the mystery key's bits are encoded in the polarization of the photons. Heisenberg's Uncertainty Principle can be utilized to ensure that an Eavesdropper can't quantify these photons and transmit them on to Bob without aggravating the photon's state perceivably in this way noteworthy their quality.

Adiabatic Algorithms

Over 10 years has gone since the disclosure of the primary quantum calculation, yet so far little advance has been made regarding the "Blessed Grail" of taking care of aNPcomplete issue with a quantum circuit show. As worried over, Shor's calculation remains solitary in its exponential "accelerate", yet while no proficient established calculation for figuring is known to exist, there is likewise no confirmation that such a calculation doesn't or can't exist. In 2000 a gathering of physicists from MIT and Northeastern University proposed a novel worldview for quantum processing that varies from the circuit demonstrate in a few intriguing ways. Their objective was to attempt to settle with this calculation an occurrence of satisfiability choosing whether a

recommendation in the propositional math has a delightful truth task which is a standout amongst the most renowned NP finish issues.

BB84 Six-State Protocol (SSP) Algorithm

Another variation of BB84 is the Six-State Protocol (SSP) proposed by Pasquinucci and Gisin in 1999. SSP is indistinguishable to BB84 aside from, as its name suggests, instead of utilizing two or four states, SSP utilizes six states on three orthogonal bases by which to encode the bits sent. This implies a spy would need to pick the correct premise from among 3 potential outcomes. This additional decision makes the spy deliver a higher rate of mistake along these lines getting to be noticeably less demanding to distinguish. Brus and Micchiavello demonstrated in 2002 that such higher-dimensional frameworks offer expanded security. While there are various other BB84 variations, one of the later was proposed in 2004 by Scarani, Acin, Ribordy, and Gisin..

The SARG04 convention shares precisely the same stage as BB84. In the second stage, when Alice and Bob decide for which bits theirbases coordinated, Alice Does not specifically report her bases. Or maybe she reports a couple of non orthogonal states, one of which she used to encode her bit. In the event that Bob utilized the right premise, he will gauge the right state. In the event that he picked erroneously, he won't quantify both of Alice's states and he won't have the capacity to decide the bit. BB84 was the primary proposed QKD convention and it depended on Heisenberg's Uncertainty Principle. An entire arrangement of conventions took after which based on the thoughts of BB84. Probably the most remarkable of these were B92, SSP, and **SARG04**.

Shor's Algorithm

The prophet simply depicted, despite the fact that exhibiting the potential predominance of quantum PCs over their traditional partners, by and by manage evidently immaterial computational issues. Without a doubt, it is farfetched whether the exploration field of quantum processing would have pulled in so much consideration and would have developed to its present status if its legitimacy could be exhibited just with these issues. In any case, in 1994, subsequent to understanding that Simon's prophet can be bridled to fathom a significantly more fascinating and critical issue, in particular considering, which lies at the core of ebb and flow cryptographic conventions, for example, the RSA , Peter Shor has transformed quantum figuring into a standout amongst the most energizing exploration areas in quantum mechanics.

Shor's calculation misuses the smart number theoretic contention that two prime components p,q of a positive whole number N=pq can be found by deciding the time of a capacity $f(x) = yx \bmod N$, for any $y < N$ which has

no normal elements with N other than 1. The period r of $f(x)$ relies upon y and N. When one knows the period, one can factor N if r is even and $yr/2 \neq -1 \bmod N$, which will be together the case with likelihood more noteworthy than 1/2 for any y picked arbitrarily (if not, one picks another estimation of y and tries once more). The variables of N are the best normal divisors of $yr/2 \pm 1$ and N, which can be found in polynomial time utilizing the outstanding Euclidean calculation.

Shor's outcome is the most sensational case so far of quantum "accelerate" of calculation, despite the way that considering is accepted to be just in NP and not in NP finish. To confirm whether n is prime makes various strides which is a polynomial in log2n (the paired encoding of a characteristic number n requires log2n assets). Be that as it may, no one knows how to consider numbers into prime's polynomial time, not even on a probabilistic Turing machine, and the best traditional calculations we have for this issue are sub-exponential. This is yet another open issue in the hypothesis of computational unpredictability. Current cryptography and Internet security conventions such open key and electronic mark depends on these realities: It is anything but difficult to discover extensive prime numbers quick, and it is difficult to consider huge composite numbers any sensible measure of time. The revelation that quantum PCs can fathom calculating in polynomial time has had, consequently, an emotional impact. The execution of the calculation on a physical machine would have monetary, and additionally logical outcomes.

Grover's Algorithm

Expect we have met someone who kept the name riddle, however revealed her telephone number. Would we have the capacity to find her name using her number and a phone index? In the most cynical situation, if there are n entries in the inventory, the computational resources required will be immediate in n. Grover (1996) demonstrated how this errand, to be particular, looking through an unstructured database, ought to be conceivable with a quantum count with multifaceted nature of the demand $\sqrt{n}$. Agreed, this "quicken" is more unpretentious than Shor's since looking through an unstructured database has a place with the class P, yet rather than Shor's case, where the built up diserse nature of figuring is so far dark, here the predominance of the quantum estimation, however unassuming, is certainly provable. That this quadratic "quicken" is in like manner the perfect quantum quickens doable for this issue.

Notwithstanding the way that the inspiration driving Grover's computation is by and large delineated as "looking through a database", it may be more correct to depict it as "altering a capacity". Grover's estimation demonstrates that in the quantum show looking for ought to be conceivable speedier than this; in assurance its shot unusualness O (N1/2) is asymptotically the fastest doable for looking through an unsorted database in the immediate quantum show. It gives a quadratic speedup, not at all like other quantum estimations, which may

give exponential, quicken over their built up accomplices. In any case, even quadratic speedup is huge when N is huge. Unsorted interest paces of up to relentless time are achievable in the nonlinear quantum show if we have a limit y=f(x) that can be evaluated easily on a quantum PC according to Grover's observation which empowers us to figure x when given y. Altering a limit is related to looking through a database since we could devise a limit that makes a particular estimation of y if x organizes a desired area in a database, and another estimation of y for various estimations of x. The uses of this count are broad. For example, it can be used to choose capably the amount of answers for a N thing look for issue, accordingly to perform intensive journeys on a class of answers for a NP complete issue and altogether decrease the computational resources required for clarifying it.

CONCLUSION

From this analyzing work, we have studied on secure and efficient designs ofE-commerce applications using Quantum cryptographic primitives. For the concrete design, we reviewed previous related works and pointed out their problems and weaknesses. And then we have suggested two improved protocols to address those problems and weaknesses considering other requirements. Through our analysis in terms of security and performance, we have explained that some other proposed algorithms are used to secure and efficient andhave more advantages compared to other algorithm of works.

References

[1] W.-d. Qiu, Y.-w. Zhou, B. Zhu, Y.-f. Zheng, and Z. Gong, "Key-insulated encryption based group key management for wireless sensor network," Journal of Central South University, **20**, 2013, 1277-1284.

[2] A. E. El-Din, R. A. Ramadan, and M. B. Fayek, "VEGK: Virtual ECC group key for wireless sensor networks," in Computing, Networking andCommunications (ICNC), 2013 International Conference on, 2013, 364- 368.

[3] G. Indra and R. Taneja, "An ECC-time Stamp based mutual authentication and key management scheme for WSNs," in Advanced InformationNetworking and Applications Workshops (WAINA), 2013 27th InternationalConference on, 2013, 883-889.

[4] C. Alcaraz, J. Lopez, R. Roman, and H.-H. Chen, "Selecting key management schemes for WSN applications," Computers & Security, **31**, 2012, 956-966.

[5] Y. Zhou, T. Wang, and Y. Wang, "A novel WSN key pre–distribution scheme based on group–deployment," International Journal of SensorNetworks, **15**, 2014, 143-148.

[6] A. H. Sodhro, Y. Li, and M. A. Shah, "Novel Key Storage and Management Solution for the Security of Wireless Sensor Networks," TELKOMNIKAIndonesian Journal of Electrical Engineering,**11**, 2013, 3383-3390.

[7] R. S. Reddy, "Key Management in Wireless Sensor Networks Using a Modified Blom Scheme," arXiv preprint arXiv:1103.5712, 2011, 1-9. [38] L. Yun, W. Chunying, and Z. Yiying, "A secret-sharing-based key management in Wireless Sensor Network," in Software Engineering andService Science (ICSESS), 2013 4th IEEE International Conference on, 2013, 676-679.

[9] Z. Zhiming, J. Changgen, and D. Jiangang, "A Novel Group Key Agreement Protocol for Wireless Sensor Networks," in MeasuringTechnology and Mechatronics Automation (ICMTMA), 2010 InternationalConference on, 2010, 230-233.

[10] E. K. Wang, Y. Ye, and X. Xu, "Location-Based Distributed Group Key Agreement Scheme for Vehicular Ad Hoc Network," International Journalof Distributed Sensor Networks, 2014.

[11] W. Gang, W. Tao, G. Quan, and M. Xuebin, "An Efficient and Secure Group Key Management Scheme in Mobile Ad Hoc Networks [J]," Journalof Computer Research and Development,**47**, 2010, 911-920.

[12] S. Gong, X. Zuo, L. Mei, and R. Zhao, "Enhanced Key Management Scheme Based on Random Key Pre-distribution for Wireless Sensor Networks," in Future Information Technology, ed: Springer, 2014, 343-348.

[13]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).

[14]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).