A Novel Technique to modify the SHOR'S Algorithm –Scaling the encryption scheme

Nitesh Chouhan, Hemant Kumar Saini
Dept. of Information Technology
M.L.V. Textile Engineering College
Bhilwara, Rajasthan, India
niteshchouhan_9@yahoo.com,
hemantrhce@rediffmail.com

Dr. S. C. Jain
Dept. of Computer Science Engineering
University College of Engineering, RTU
Kota, Rajasthan, India
scjain1@gmail.com

***Abstract*—This paper involves the study of traditional facts about the classical model of cryptography and also surveyed the security protests of encryption schemes. Not only stick to this also gives the computing understanding of the quantum computing schemes of traditional SHORS computation with the old technique demonstration in mathematical view. Here also proposed a novel technique which resembles the shors scheme and also copared the results to prove its scalabilty.**

Keywords-Quanutm; Qubits; modular exponentiation; scaling;shor's algorithm.

I. INTRODUCTION

Today when the world of security protests the encryption scheme with new paradigms the time has come where the end starts to scale the new encryption techniques with the classical computing. Since the classical computer depend on the prime factors or multipliers because factoring large statistics is so devilishly hard, this "factoring problem" is the root for many encryption schemes for shielding credit cards, government secrets, and other intimate data. It's assumed that a single quantum supercomputer may easily crack this problem, by using atoms, essentially in parallel, to quickly factor huge numbers.

However with the Applied Mathematics, derived through a quantum algorithm that calculates the prime elements of a excessive quantity, enormously more professionally compared to traditional system. Though, the algorithm's success is contingent on a computer with a large amount of quantum bits. While others have tried to tool Shor's algorithm in numerous quantum schemes, none have been gifted to do so by additional than a few quantum bits, in a mountable way.

In standard calculating, statistics are indicated by also 0s or 1s, and panels are approved out rendering to an algorithm's "orders," whose function these 0s and 1s to alter participation to a harvest? In difference, quantum computing faiths on atomic-scale components, or "qubits," that can be alongside 0 and 1 — a national documented as a superposition. In this state-run, a solitary qubit can fundamentally transmit out two separate waterways of pedals in comparable, formation calculations far more effective than a standard computer.

Chief Quantum computing is the capsule assumed by SHORS which is a procedure which issues integers' trendy polynomial period scheduled a quantum system. If unique stabs to track it on a classical computer, solitary turns into the problematic that the state-run vector that is existence functioned on is of exponential size, so it cannot be track professionally.

II. SHOR'S EXPERIMENTATION

Initially, it is thoughtful an outmoded factoring method, conceited that the amount essential to subject is M = 15. Let's choice a chance quantity x∈ [2; M – 1](the base)—say, x = 7 which measure whether the greatest common divisor gcd (x, N) = 1; whilst with none, issue is previously resolute. This is the circumstance for a= {3, 5, 6, 9, 10, 12}. Following, estimate the sectional x^a mod N for a=0, 1, 2…and find its period r: the first value of x > 0 such that x^a mod M = 1. Assumed s, consequence features of M needs tricky the gcd of a s/2 ±1 and i.e. is skillfully likely through a outdated approach— such as, by Euclid's procedure. With concept with M=15, X=7, the prefabricated exponentiation vintages 1, 7, 4, 13, 1, having epoch of 4. The highest common divisors of a s/2 ±1=74/2 ±1= {48, 50} besides M=15 are {3, 5}, the important aspects of M. Here, the circumstances x= {4, 11, 14} consume epoch s = 2 and need "a" only upsurge stage (x^2 mod N=1), that is cautious "informal" circumstance [8]. Reminder that the historically for a selected "a" might not predict. In what way this formula is applied in a Quantum Computer? A Quantum computer too compute ax mod N trendy a calculative record for a = 0, 1, 2… in addition formerly excerpt s. By the quantum Fourier transform (QFT) practical toward epoch list, the epoch of ax mod N may be mined since a quantity list of capacities decreasing till the factorized extent [1].

978-1-5090-3239-6/17/$31.00©2017IEEE

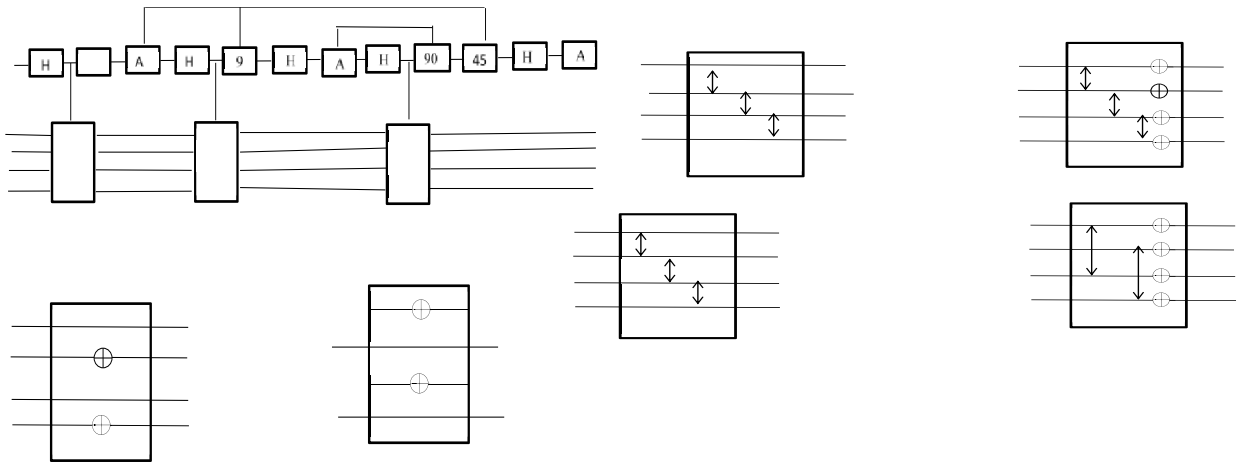

Fig. 1. (a) real factorization for 15 to base11 in left (b) right side show the mod multiplier od a mod N for a=2,7,8,11

III. CHALLENGES

A. *Focusing on Modulor Exponentiation*

Initially emphasis on the epoch list and then the address exponentiation is performed over the modulus in divisional list. Factoring M, an m = $\lceil \log_2(M) \rceil$-bit quantity , needs least of m qubits in the multiplicative register and usually about 2m qubits with passage of (9, 10). Consequently, even though a factoring 15 (an m = 4-bit number), needs 3m = 12 qubits. These qubits then have to be operated with great reliability gate processes. Assumed present condition regulator over new computer quantum bits, viz. method shall perhaps harvest an inacceptable performance. Though, a occupied quantum application of such an algorithm might not required. As depicted in Kitaev [2], when the classical QFT data (such as the period s) is 2m qubits focused to a QFT can be traded by a qubit alone.

B. *Maintaining Qubit Recycling*

Still, such approach needs qubit reprocessing (explicitly, continuously single-qubit data and formal initialization) balancing and manage to recompense aimed at abridged scheme scope.

The instant key element to Shor's procedure— and a particularly additional stimulating feature compared to the QFT—is exponentiation over modulus, that acknowledges the next overall interpretations: the effort state 1(in floating illustration) is substance to a provisional proliferation founded on the higher order bit k in epoch list. As a maximum, here shall be two outcomes after this formerly step as certain in Fig 1(a) It trails that, for the very first stage, it is satisfactory to device an augmented operation that tentatively charts $1 \rightarrow a^{2k} \bmod N$. Since the position of a great loyalty growth (with its act being nourished advancing toward altogether following qubits), such well-organized clarification recovers the general routine of inexperienced recognitions.

Succeeding multipliers can correspondingly be swapped with plots by since only probable yields of the former multiplication subsequently n periods, 2m > M conceivable consequences shall be measured, a arithmetical task as puzzling as divisioning M by standard resources. Therefore, measured complete modular multipliers should be applied.

Figure 1(b) demonstrates the trial found truth bench aimed at the modular multiplier 2 mod15.These quantum routes can be proficiently derived from conventional measures by a range of normal methods for revocable mathematics and native optimization (17, 18). , the latter generator only has to make the precise quantity of associations amid the epoch list and the computation register. Native processes after the temporary (interweaving) tasks may be unwanted to ease the absolute growth. Aimed at important totaling, accretion stages 1, 3, and 4 slightly touch the act of the employment. These steps signify only a minor subsection of the whole calculation, which mostly contains of the complete measurable integrators. Therefore, the understanding of the measurable integrators is prerequisite in scalable Shor algorithm implementation.

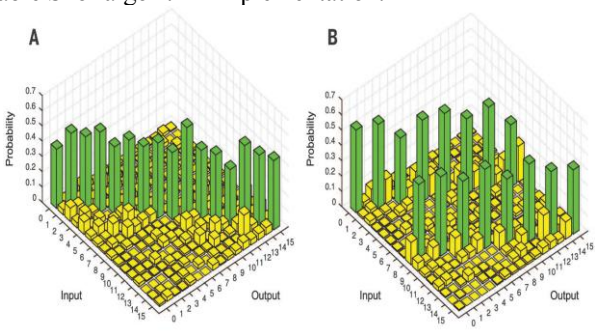

Fig. 1(b). Experimentally obtained the 2mod 15 multiplier at state qubit 0 in part A and proving the operation in part B

IV. Proposed Novel Approach

Unique noticeable difficulty by such a method is that the unitary conditions in Shor's algorithm include multifaceted statistics, so they cannot be stochastic matrices. Likewise, the l2 standard, not the l1 standard, of the columns of the unitary mediums in Shor's algorithm equivalent one. (Also, the unitary matrices in Shor's algorithm are all dissimilar; consequently it is not smooth near to a Markov Chain)[3]

Nonetheless why must this halt? Here is how it remained rational.it could possibly dose this tricky: Initially, adapt the unitary matrices jumble-sale in Shor's algorithm to orthogonal matrices so that each entrance a+ib grows renewed to the matrix.

$$\begin{matrix} a & b \\ -b & a \end{matrix}$$

Nevertheless novel matrices be stochastic, meanwhile they include negative numbers. To hit this difficulty as depicted in [4], alter individually passes a in the orthogonal matrix to the matrix of only nonnegative entries.

$$\begin{matrix} a & 0 \\ 0 & a \end{matrix} \quad \text{if a } >0$$

$$\begin{matrix} 0 & a \\ -a & 0 \end{matrix} \quad \text{if a}<0$$

The design here such to the matrix act just on vectors of figure (a,0)t when a>0 with (0,−a)t whilst a<0.) Thus it will have quadrupled the feature and file scope of the unitary matrices in Shor's algorithm. Subsequently, stabilize the file of the novel matrices in order that the entire append to single.

Consequently quadrupled feature and file size of the unitary matrices in Shor's algorithm. After that, standardize the file of the novel matrices, in order that append to single. Since, standardize the columns of the novel matrices might potentially chaos up the algorithm, except the thought was to facilitate in view of the fact that in Shor's imaginative paper [5] the quantum gates worn to construct up the Fourier transform are much amazingly easy.

proviso such deception connecting the Fourier transform, and not winning benefit of particular assets of multiplication modulo n, worked, then it would offer a speedy traditional algorithm not just for factoring except for the supplementary universal abelian hidden subgroup dilemma - e.g. recognize the epoch of an arbitrary sporadic progression excluding no rapid standard algorithm for the abelian concealed subgroup dilemma, while if assess the significance of a utility $Z \rightarrow \pm 1$ at n integers, at that time we have not ruled out the possibility of the function being intervallic with epoch a amount of prime p that does not split the dissimilarity of a few two of statistics. Numerous primes of size roughly n2 essentially survive, thus contain no anticipate of outline the era in instance fewer than the square root of the amount of the epoch.

V. Contribution

In this a new approach to modify the Shor's algorithm Has been discussed which not only provides a new door to transform the encryption scheme in a quantum computing of Quantum computers which is intelligent to estimate the prime factors of a large integers. This will be a new door in the mathematics filed of Applied Quantum Theory of computers which is also seen by the compared result which depicts the best realization of the qubit operations.

VI. Results and Discussion

Quantum computers are clever to smash traditional algorithms. It was simply in 1994 that Peter Shor come up with an process that is intelligent to estimate the prime factors of a big integer immensely added efficiently than branded achievable with a usual system[6]. This paradigmatic algorithm inspired the flourishing research in quantum in sequence dealing out and the seek for an genuine execution of a quantum computer. in excess of the last fifteen years, by clever optimizations, numerous example of a Shor algorithm have been apply on a variety of raised area and obviously establish the viability of quantum factoring [7][8][9][10][11]. In support of universal scalability, although, a dissimilar approach has to be follow [12]. At this time, the understanding of a completely ascendable Shor algorithm as planned depicted in Kitaev [13]. intended for this, it is surveyed in our paper the factoring the number 15 by successfully utilize 7 qubits and 4 "cache-qubits", mutually with the completion of comprehensive mathematics process, known as modular multipliers.

In this paper it is offered the awareness of Kitaev's idea of Shor's algorithm bottom on ascendable construction chunks with three-digit resolution of aspect M= 15, using basis {2, 7, 8, 11, 13} toward to-do this, it is productively in employment a partially conventional QFT mutual with sole qubit announce, forward looking behavior, and qubit reusing .in contrast with the usual procedure, it is awareness of Shor's algorithm trim down the mandatory amount of qubits by practically a reason of 3. Additionally, the total quantum register have been focus to "black-box" technique. Utilize the equal of a quantum supply via spectroscopic decoupling with a kind thinkable derivation of the required pulse progression to attain great loyal values. This envisage that ascendable procedure conclude that scalable entrap design and quantum error rectifies the arbitrary extended quantum calculation.

Acknowledgment

It springs us huge preference to direct our genuine gratefulness to Dr. S. C. Jain, who is functioning as a professor at University College of Engineering at Rajasthan Technical University, Kota (Rajasthan), India for his priceless supervision. In spite of his chaotic agenda he was continuously amicable and spared his time to appear our difficulties and spring us suitable guidance.

References

[1] Thomas Monz, Daniel Nigg, Esteban A. Martinez, Matthias F. Brandl, Philipp Schindler, Richard Rines, Shannon X. Wang, Isaac L. Chuang, Rainer Blatt, "Realization of a scalable Shor algorithm", American Association for the Advancement of Science, vol. 351, pp. 1068-1070, April 2016.

[2] Christopher M. Dawson and Michael A. Nielsen, "The Solovay-Kitaev algorithm". Journal Quantum Information & Computation, vol.6, pp. 8195, January 2006.

[3] http://statweb.stanford.edu/~cgates/PERSI/papers/MCMCRev.

[4] Dr. S.C. Jain, Nitesh Chouhan and Hemant Kumar Saini. "A Survey on Different Visions with Contrasting Quantum and Traditional Cryptography", International Journal of Computer Applications, vol.134, no.-8, pp.33-38, January 2016.

[5] Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM J.Sci.Statist.Comput.,pp.1-25,Jan 1996.

[6] P. W. Shor, "Algorithm for Quantum Computation:Discrete Logarithm and factoring", Foundations of Computer Science, Proceedings., 35th Annual Symposium on pp. 124–134 ,1994.

[7] Alberto Politi, Jonathan C. F. Matthews, Jeremy L. O'Brien, "Shor's Quantum Factoring Algorithm on a Photonic Chip", Vol. 325, Issue 5945, pp. 12-21, Science , 04 Sep 2009.

[8] Enrique Martin-Lopez, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou, Jeremy L. O'Brien, "Experimental realisation of Shor's quantum factoring algorithm using qubit recycling", Journal of Nature Photonics,pp.773-776, Nov 2011.

[9] E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, DSank, A. Vainsencher, J. Wenner, T. White Y. Yin, A. N. Cleland, J. M. Martinis, "Computing prime factors with a Josephson phase qubit quantum processor", Nature Physics 8, 719-723, 2012. doi:10.1038/nphys2385.

[10] Lanyon, B. P. and Weinhold, T. J. and Langford, N. K. and Barbieri, M. and James, D. F. V. and Gilchrist, A. and White, A. G, "Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement", vol.-99, issue-25, pp. 2505(1)-2505(4), Dec 2007.

[11] Vandersypen, Lieven M. K., Steffen, Matthias, Breyta, Gregory, Yannoni, Costantino S., Sherwood, Mark H., Chuang, Isaac L.,"Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance", journal of Nature, Phys. Rev. Lett. 99, 250505, 19 December 2007.

[12] J. A. Smolin, G. Smith, and A. Vargo, "Pretending to factor large numbers on a quantum computer," Jan. 2013, arXiv:1301.7007.

[13] A.Yu.Kitaev, "Quantum measurements and the Abelian Stabilizer Problem",pp.1-22,quant-ph/9511026.