Comparison of time complexity in factorizing large bi prime numbers using Grover's and Shor's algorithm

Preprint · August 2020

DOI: 10.13140/RG.2.2.23597.51680/1

3 authors:

Sahil Parvez
University of Bologna
3 PUBLICATIONS **2** CITATIONS

SEE PROFILE

Bikash K. Behera
Bikash's Quantum (OPC) Pvt. Ltd.
202 PUBLICATIONS **1,478** CITATIONS

SEE PROFILE

Prasanta K. Panigrahi
Indian Institute of Science Education and Research Kolkata
688 PUBLICATIONS **6,993** CITATIONS

SEE PROFILE

Comparison of time complexity in factorizing large bi prime numbers using Grover's and Shor's algorithm

Sahil Parvez , Bikash K. Behera & Prasanta K. Panigrahi

***Abstract*—Factorizing large bi prime integer numbers using quantum computers illuminates quantum advantage over classical computers. Finding the prime factors on classical computers would require sub exponential time period, however due to optimization its done in polynomial time by optimizing and solving it using quantum computers. Recently there are a number of works revolving around it. However our work is based on generalized Grover's algorithm, by Liu and Shor's algorithm. We will be comparing time-complexity of factorization on various quantum computers and also discuss the shortfalls in Shor's algorithm. Here we will be experimentally factorizing 12794893 using IBM's different 5 qubit and 15 qubit quantum processors utilizing phase-matching property making it the largest number being factorized on a quantum computer. We will be statistically comparing data sets for different open access quantum computers. By the principles we can factorize large integers with minimum time and resources.**

I. Introduction

Factorization is the core of data cryptography like in the RSA [13] technique for secure data communication. Hence it is an integral part of the security system. With Shor's and Grover's algorithm it could be done in a jiffy, making the RSA cryptography system obsolete or an old school technique. Till now with Shor's algorithm [9] [10] [11] the largest number factorized experimentally is 21. With Grover's algorithm the larges number factorized experimentally is 4088459 in 2018, [14] using 2 qubits. The phase matching property [12] is used which finds quantum advantage [3][4] over classical computers.

In our work, optimization of the circuit [5] [6] is done using adiabatic approach, the pre-processing required has been minimized. With exact search we can replace the dynamically evolving system Hamiltonian with an exponential function of the non-unitary Hamiltonian used in the adiabatic case. The basis states can be encoded to get the required solutions, then can be separated out using an exact quantum search algorithm [8].

II. Grover's Algorithm

We strive to factorize a biprime number N [1] [2] into prime factors p and q, such that, N = p × q. If the number to be factorized is even, then we keep dividing it by two until an odd composite number is reached.

The factors p and q can be denoted in binary form as $\{1p_mp_{m-1}...p_2p_11\}$ and $\{1q_nq_{n-1}...q_2q_11\}$ respectively, where

$$p = 2^{m+1} + \sum_{i=1}^{i=m} p_i + 1$$

and a similar expression would be applied for q. Our first target is to optimize the problem into set of equation in variable form p_i and $q_j (i \in [1, m] \cap N, j \in [1, n] \cap N)$, which is subjected to the condition that

$$p_{bin} \times q_{bin} = N_{bin}$$

(the subscript denotes binary notation) [6, 7, 11, 12]. It has been recently shown that the set of equations in m + n variables is reducible to a smaller number of variables [11]. This is because, if

$$p_i + q_j = z$$

for some i,j, where z ∈ 0, 2, then

$$p_i = q_j = 0$$

if z = 0 and

$$p_i = q_j = 1$$

if z = 2. Hence, the set of equations is reduced to only those variables $p_i and q_j$ such that the index i takes values from the set $I_p = \{i \in [1, m] \cap N : p_i + q_j = 1$ for some j$\}$ and similar scenario goes well for index j also. In cases where m = n, the optimization of the set of equations in variables $p_i and q_i$ leads to a smaller set of equations where

$$p_i + q_i = 1$$

and $Pi < jp_iq_j + p_jq_i = z$ $(z \in 0, 1, i, j \in I \subseteq [1, n] \cap N)$. Hence, the set I such that

$$p_i + q_i = 1$$

and

$$p_i = q_i = 0$$

Sahil Parvez is from the Department of Physics, Aligarh Muslim University, Aligarh 202002, Uttar Pradesh, India.
E-mail: sahilparvez999@gmail.com
Corresponding author.
Bikash K. Behera and Prasanta K. Panigrahi are from the Department of Physical Sciences, Indian Institute of Science Education and Research Kolkata, Mohanpur, 741246, West Bengal, India
E-mail: bikash@bikashsquantum.com
Bikash K. Behera is also at Bikash's Quantum (OPC) Pvt. Ltd., Balindi, Mohanpur, 741246, Nadia, West Bengal, India
Corresponding author.
E-mail: pprasanta@iiserkol.ac.in

$(\forall i \in I)$. Considering N = 12794893. It is known that the prime factors of this number have the same number of digits. Hence, m = n in this case. The prime factors p and q are denoted in binary as $\{1p_{10}p_9...p_2p_1 1\}_{bin}$ and $\{1q_{10}q_9...q_2q_1 1\}_{bin}$ respectively. The factorization problem reduces to the set of equations:

$$p_2 + q_2 = 1$$

$$p_3 + q_3 = 1$$

$$p_2 q_3 + p_3 q_2 = 0.....(1)$$

As for the rest of the variables, upon optimization we obtain:

$$p_i = q_i = 0; i \in \{9\}$$

$$p_i = q_i = 1; i \in \{1, 4, 5, 6, 7, 8, 10\}.....(2)$$

Since $q_i = 1 - p_i$ for $i \in 1, 3$, the set of equations(Eq. (1)) is further reduced to:

$$q_2 + q_3 - 2q_2 q_3 = 0.......(3)$$

The values of q1 and q3 satisfying Eq.(3), represents the solution to our factorization problem that are encoded in the ground state of the 2-qubit Hamiltonian,

$$\widehat{H} = (\widehat{a_1} + \widehat{a_2} - 2\widehat{a_1}\widehat{a_2})^2$$

where $\widehat{a_i} = \frac{I - \sigma_z^i}{2}$, I stands for the 1-qubit identity operation and σ_z^i denotes the Pauli Z operator acting on the ith qubit. Since q_2, q_3 satisfy Eq. (3), the two qubit z basis eigenstate $|q_2\rangle|q_3\rangle$ satisfies $H|q_2\rangle|q_3\rangle = 0.|q_2\rangle|q_3\rangle$ (note that for any $b \in 0, 1, \widehat{a_i}|b\rangle = b|b\rangle$, thus yielding the above result), while for any other two qubit state (in z-basis) the corresponding eigenvalue of H is some positive value (non-zero). It is to be noted that, for a case in which two factors need to be found, H can have two and only two ground state eigenstates (whose eigenvalue is zero). Upon simplifying, we obtain

$$\widehat{H} = \frac{1}{2}(I_2 - \sigma_z^1 \otimes \sigma_z^2)......(5)$$

where we have used the fact that $\widehat{a_i^2} = \widehat{a_i}$. I_2 denotes the 2-qubit identity operation. It can be shown that $\widehat{H}$ has eigenvalues 0 and 1. One can verify that the unitary operator $e^{-i\widehat{H}\theta}$ (equivalent to the operation $(e^{-i\theta} - 1)\widehat{H} + I$) induces a relative phase change of θ in the 2-qubit z-basis eigenstates that correspond to the eigenvalue 0 for the operator $\widehat{H}$. If$|b_1\rangle|b_2\rangle$ is such a state $(b_1, b_2 \in \{0, 1\})$, then $(q_2, q_3) = (b_1, b_2)$. Hence, the operator $e^{-i\widehat{H}\theta}$ performs a conditional phase shift $e^{i\theta}$ which marks the required "solution" states. Firstly, we take the equal superposition state in a two qubit system, i.e. the state given by $|\psi_0\rangle = \frac{1}{2}\sum_{i=0}^{i=3}|i\rangle$. We pass $|\psi_0\rangle$ through the operator $e^{-i\widehat{H}\theta}$, which marks our required solution states. Our next aim is to separate out these "marked" states which we wish to obtain by some means. To achieve this, the generalized Grover's search algorithm is used, which searches any number of marked states from an arbitrary quantum database with certainty [8]. We have already achieved the first step of this algorithm, viz. we have introduced a conditional phase shift to the marked states.Secondly, we apply the 2 qubit operator U† , where U transforms $|00\rangle$to $|\psi_0\rangle$. In our case, U† = U = $H^{\otimes 2}$(H denotes the Hadamard operation). The next step involves the conditional phase shift $e^{i\theta}$ to $|\ 00\rangle$state, whereas all the other basis states remain unchanged. Finally, we perform the operation U (in our case U = $H^{\otimes 2}$). The result is that the final state should contain only the solution states. The value of the phase shift angle θ for the exact quantum search algorithm to work is found to be equal to $\frac{\pi}{2}$ [8], with only a single iteration being required. Detailed calculations along with the overall quantum circuit have been presented in Supplementary material. We experimentally realized the factorization problem at hand using IBM's 5-qubit and 1 5-qubit quantum processor. The tomographical results have been presented below.

A. IBMQ Circuit Implementations

IBM Quantum provides a provision to access their open access quantum processors. For factorizing 12794893, the reduced circuit diagram, transcribed script circuit, density matrix, state vectors and measurement probability are as follows:

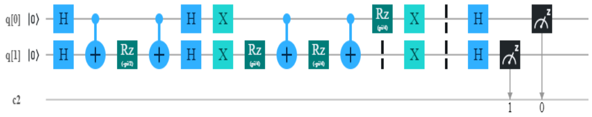

Figure 1. Circuit diagram (reduced). In this circuit we are performing Grover's exact search for biprime number 12794893

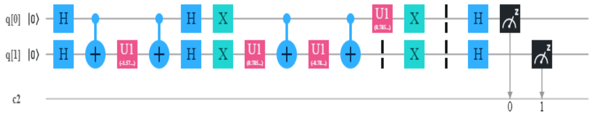

Figure 2. Transcribed circuit diagram of the above circuit performing the exact search for the number 12794893

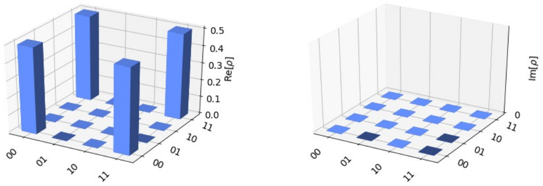

Figure 3. Theoretical Density Matrix as expected by running the circuit. The result is generated by IBMQ. The theoretical density matrix is accordance with the formulated density matrix.

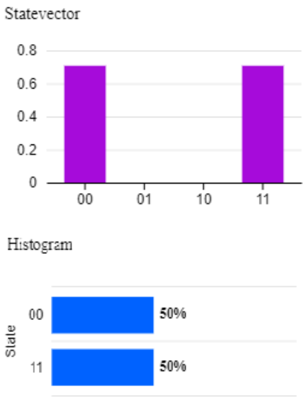

Figure 4. Theoretical State Vector and Measurement probabilities of the corresponding circuit, showing the possible outcome states and their measurement probabilities. These are generated by IBMQ showing the ideal outcome based on the circuit implementation

These are the data that we ideally expect. However it slightly differs from the actual data. Hence in the following sections we will going through the resulting data of simulation, IBMQX2,IBMQ Melbourne, IBMQ London and IBMQ Rome.

1) IBMQ X2 Yorktown Results:

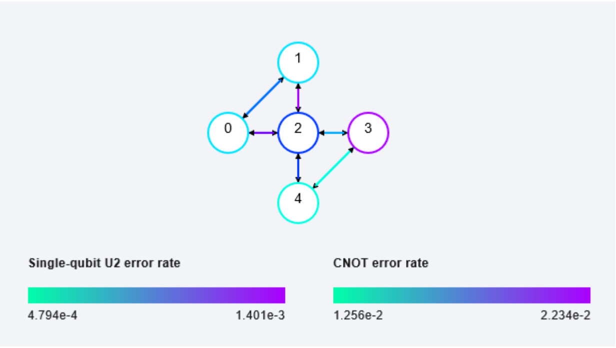

Figure 5. IBMQX2 Circuit Diagram. It is a 5 qubit quantum processor with the following connectivity. It shows the error rates in each qubit and CNOT errors. Retrieved from IBMQ Experience.

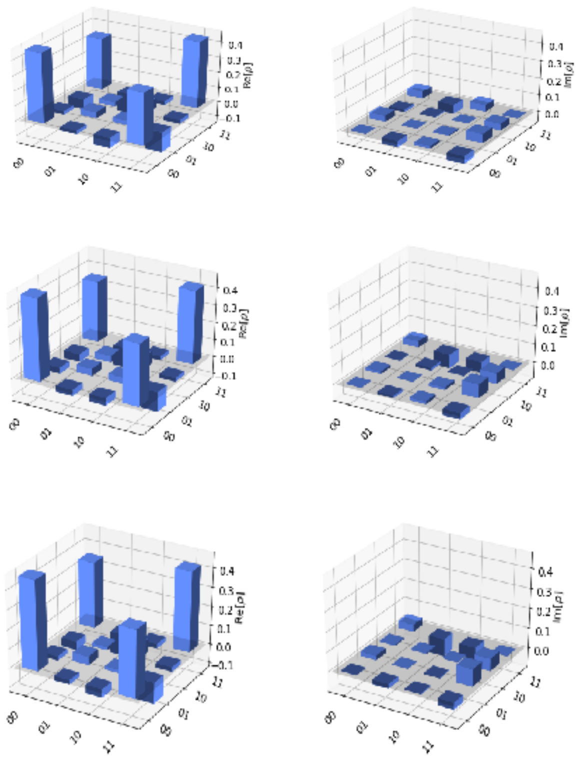

Figure 6. Experimental Density Matrix for 1024, 4096 and 8192 shots respectively. The density matrix has been experimentally determined by IBMQX2 and tomography done by phthon.

The following results shows the measurement probabilities of IBMQ X2. We can notice that the states $\mid 01 \rangle$and $\mid 10 \rangle$has possible probabilities. This is because of the errors in the chips.

Qubits	Frequency
Q0	5.286396567
Q1	5.238258986
Q2	5.030502806
Q3	5.295630999
Q4	5.084389602

The table shows the qubit frequency of each qubit in IBMQ X2

2) IBMQ London Results:

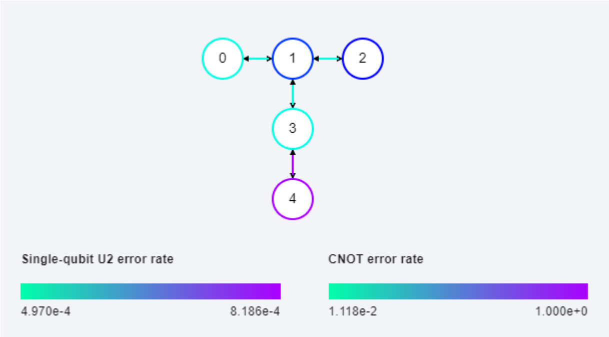

Figure 7. IBMQ London Circuit. It is a 5 qubit quantum processor with the following connectivity. It shows the error rates in each qubit and CNOT errors. Retrieved from IBMQ Experience.

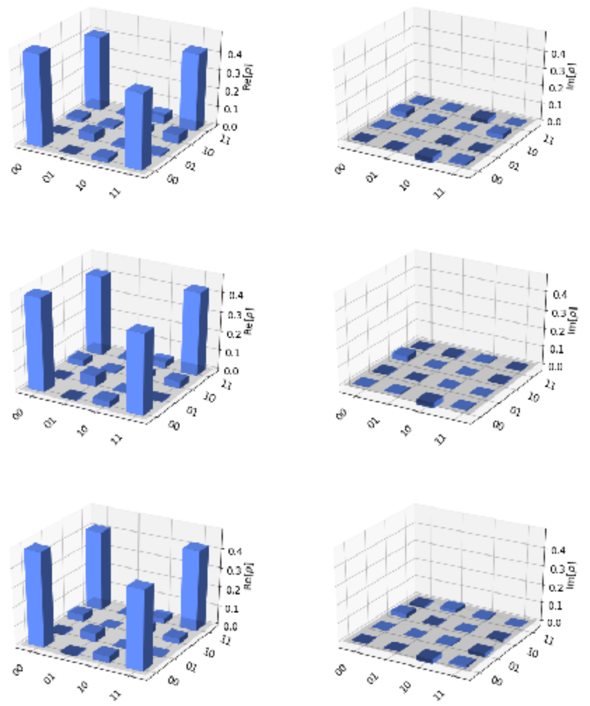

Figure 8. Experimental Density Matrix for 1024, 4096 and 8192 shots respectively. The density matrix has been experimentally determined by IBMQX2 and tomography done by phthon.

Qubits	Frequency
Q0	5.253961305
Q1	5.048630713
Q2	5.230574157
Q3	5.20094217
Q4	5.065789099

The table shows the qubit frequency of each qubit in IBMQ London

3) IBMQ Melbourne Results:

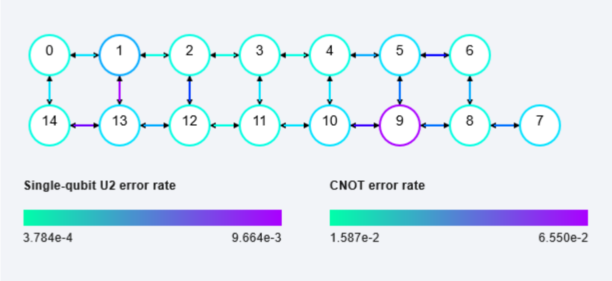

Figure 9. IBMQ Melbourne Circuit. It is a 15 qubit quantum processor with the following connectivity. It shows the error rates in each qubit and CNOT errors. Retrieved from IBMQ Experience.

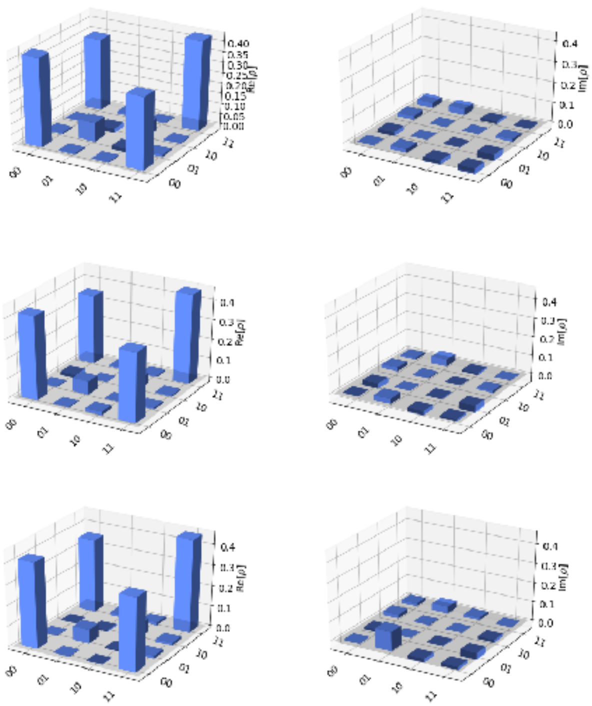

Figure 10. Experimental Density Matrix for 1024, 4096 and 8192 shots respectively. The density matrix has been experimentally determined by IBMQX2 and tomography done by phthon.

Qubits	Frequency
Q0	5.100161789
Q1	5.238397128
Q2	5.032824716
Q3	4.896090996
Q4	5.026230627
Q5	5.066890488
Q6	4.924042694
Q7	4.974509588
Q8	4.740668071
Q9	4.96328594
Q10	4.945211141
Q11	5.004959172
Q12	4.759999116
Q13	4.96832728
Q14	5.001476368

The table shows the qubit frequency of each qubit in IBMQ Melbourne. It has 15 qubits.

B. *Time Comparison*

We have gone through the measurement probabilities, which highlights their errors and accuracy of the system. Now lets check out the Running time of the different quantum devices and compare them.

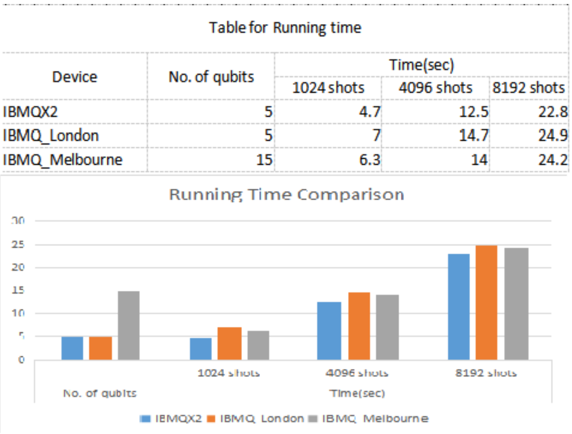

Table for Running time

Device	No. of qubits	Time(sec)		
		1024 shots	4096 shots	8192 shots
IBMQX2	5	4.7	12.5	22.8
IBMQ_London	5	7	14.7	24.9
IBMQ_Melbourne	15	6.3	14	24.2

Figure 11. Table and the Chart shows the Time Comparison between different IBMQ devices. The running time is taken for processing the Circuit in IBMQ.

C. *Mathematical Information about Phase*

Let us discuss the necessary mathematics for obtaining the value of the phase shift angle θ for the exact quantum search algorithm to work. Since there are two different factors, the Hamiltonian $\widehat{H}$ (Eq. (5)) has two and only two eigenstates whose corresponding eigenvalue is zero. Hence, two basis states represent the solution to our problem. These two states are marked with the relative phase shift $e^{i\theta}$. If considered from the quantum database $|\psi_0\rangle, |x_0\rangle$ represents the normalized sum over the two marked states. Let $|x_0^\perp\rangle$ represent the normalized sum over the other two states (non-marked states). Hence, in the two dimensional vector space, $|x_0^\perp\rangle$ represents the hyperplane perpendicular to $|x_0\rangle$, and the vector space is spanned by $\{|x_0\rangle, |x_0^\perp\rangle\}$. The state $|\psi_0\rangle$ can be expressed as:

$$|\psi_0\rangle = \sin\phi|x_0\rangle + \cos\phi|x_0^\perp\rangle$$

In our case, $\phi = \frac{\pi}{4}$. The relation between θ and ϕ is given as [15]

$$\theta = 2\sin^{-1}\left(\frac{\sin\frac{\pi}{4j+2}}{\sin\phi}\right) ....(6)$$

where j is the minimum number of iterations after which the marked states can be separated with certainty. Eq. (6) has real solutions for

$$j \geq \frac{\pi}{4\phi} - \frac{1}{2}$$

Hence, the value of j is given as [15]

$j = \{\frac{\pi}{4\phi} - \frac{1}{2}$, if $(\frac{\pi}{4\phi} - \frac{1}{2})$ is an integer, INT$(\frac{\pi}{4\phi} - \frac{1}{2}) + 1$, otherwise$\}$

The formulation of the theoretical and experimental density matrices for the purpose of carrying out quantum state tomography [18] shall now be discussed. For a two qubit system, the experimental density matrix is given by

$$\rho^E = \frac{1}{4}\sum_{i,j=0}^{3}(S_i \times S_j)(\rho_i \otimes \rho_j)$$

S_0, S_1, S_2 and S_3 are known as Stokes parameters. $\{\sigma_i\}$ is the set of single qubit operations I, $\sigma_X, \sigma_Y, \sigma_Z$ for i = 0, 1, 2, 3 respectively. The Stokes parameters are calculated as

$$S_0 = 1$$

$$S_1 = P_{|0_X\rangle} - P_{|1_X\rangle}$$

$$S_2 = P_{|0_Y\rangle} - P_{|1_Y\rangle}$$

$$S_3 = P_{|0_Z\rangle} - P_{|1_Z\rangle}$$

where $P_{|i_j\rangle}$ denotes the probability of obtaining the eigenstate —ii upon measurement in the basis denoted by j. To perform a measurement on any qubit in X-basis, H gate is applied to the qubit before measurement and $S^\dagger$H gate is used for the same in Y -basis. Our task is to check whether the experimental density matrix is in good agreement with the theoretical one. The theoretical density matrix is given by

$$\rho^T = |\Psi\rangle\langle\Psi|$$

A measure of the overlap between two density matrices is given by fidelity, which quantifies the closeness of the experimentally obtained quantum states to the final state of the system in the ideal case. This quantity is calculated as

$$F(\rho^T, \rho^E) = T_r\left(\sqrt{\sqrt{\rho^T}\rho^E\sqrt{\rho^T}}\right)$$

In theory, the final state obtained after the circuit is executed should be

$$\left|\Psi\right\rangle = \frac{1}{\sqrt{2}}[\left|00\right\rangle + \left|11\right\rangle]$$

. Hence,

$$\rho^T = \frac{1}{2}\begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 1\end{bmatrix}$$

III. Shor's Algorithm

This is an algorithm to factorise an number N on quantum device. It was devised by Peter Shor, in 1994. Shor's algorithm factorizes a number in polynomial time [7] in the order of log N, and takes quantum gates in the oreder of $O((logN)^2(loglogN)(logloglogN))$. [16] In 2012, the largest number factorized by this algorithm is 21. [10] It required 10 qubits to solve it.

For factorizing 12794893 it would require 48 qubits and 24 entangled state qubits, hence requiring a total of 72 qubits. It becomes impossible on a practical processor, hence becoming one of the drawbacks of Shor's algorithm.

A. *Quantum Period Finding*

In this part another arbitrary number a, is chosen which is coprime to the number N. It can be done by taking gcd(a,N)=1. Then finding the remainder by Chinese remainder theorem and then finding the period by quantum Fourier transformation. The period gives the prime factor. As we can see in the diagram below, 2n represents 48 qubits and the n are 24 entangled qubits.[17] The quantum function applied:

$$f(x) = a^x modN$$

.

$$Q = 2^q, N^2 \leq Q < 2N^2$$

$$U_f\left|x, 0^q\right\rangle = \left|x, f(x)\right\rangle$$

$$U_f\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}\left|x, 0^q\right\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}\left|x, f(x)\right\rangle$$

$$U_{QTF}(\left|x\right\rangle) = \frac{1}{\sqrt{Q}}\sum_{y=0}^{Q-1}\omega^{xy}\left|y\right\rangle$$

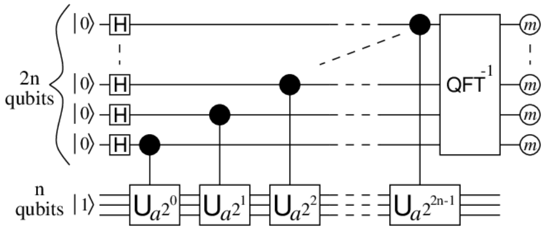

Figure 12. Diagram for Shor's circuit using 2n+n qubits. The n qubits represent the entangled states. The QFT^{-1} represents the Inverse Quantum Fourier Transformation. This image is taken from an arXiv paper by S. Beauregard. [17]

References

[1] C. H. Bennett, and D. P. DiVincenzo, Quantum information and computation. Nature 404, 247–255 (2000).

[2] B. E. Kane, A silicon-based nuclear spin quantum computer. Nature 393, 133–137 (1998).

[3] S. Bravyi, D. Gosset, and R. K¨onig, Quantum advantage with shallow circuits. arXiv preprint quant-ph/9511026 (1995).

[4] D. Rist´e, et al. Demonstration of quantum advantage in machine learning. npj Quantum Inf. 3, 16 (2017).

[5] Chris J.C. Burges, Factoring as Optimization. Microsoft Research MSR-TR-200 (2002).

[6] Nanyang Xu,et al. Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance Sysytem. Phys. Rev. Lett. 108, 130501 (2012).

[7] Y. Wang, H. Zhang, and H. Wang, Quantum Polynomial Time Fixed-Point Attack for RSA. China Commun. 15, 25–32 (2018).

[8] Y. Liu, An exact quantum search algorithm with arbitrary database. Int. J. Theor. Phys. 53, 2571–2578 (2014).

[9] L. M. K. Vandersypen, et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature 414, 883–887 (2001).

[10] E. Mart´ın-L´opez, et al. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. Nat. Photon. 6, 773–776 (2012).

[11] A. Bocharov, M. Roetteler, and K. M.Svore, Factoring with qutrits: Shor's algorithm on ternary and metaplectic quantum architectures. Phys. Rev. A 96, 012306 (2017).

[12] X. Li, K. Song, , N. Sun, and C. Zhao, Phase matching in grover's algorithm. Proc. 32nd Chin. Control Conf. , 7939–7942 (2013).

[13] R. L. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-key Cryptosystems. Commun. ACM 21, 120–126 (1978).

[14] "Exact search algorithm to factorize large biprimes and a triprime in IBM quantum computer", arXiv:1805.10478.

[15] Y. Liu, An exact quantum search algorithm with arbitrary database. Int. J. Theor. Phys. 53, 2571–2578 (2014).

[16] Beckman, David; Chari, Amalavoyal N.; Devabhaktuni, Srikrishna; Preskill, John (1996). "Efficient Networks for Quantum Factoring" (PDF). Physical Review A. 54 (2): 1034–1063.arXiv:quant-ph/9602016 .Bibcode:1996PhRvA..54.1034B .doi:10.1103/PhysRevA.54.1034 .PMID 9913575 .

[17] Beauregard, Stephane (2003). " Circuit for Shor's algorithm using 2n+3 qubits" (PDF). arXiv:quant-ph/0205095.

[18] P.K. Vishnu, D. Joy, B.K. Behera, P.K. Panigrahi, Experimental Demonstration of Non-local Controlled-Unitary Quantum Gates Using a Five-qubit Quantum Computer, Quantum Inf. Process. 17,274 (2018), doi:10.1007/s11128-018-2051-2, arXiv: 1709.05697