Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 123 (2019) 102-113 EISSN 2392-2192

Quantum Factorization of Integers 21 and 91 using Shor's Algorithm

Poornima Ardhyamath[1], N. M. Naghabhushana[2], Rohitha Ujjinimatad[3]

[1]Research Scholar, Department of Physics, RYM Engineering College, Ballari, India
E-mail address: ampoornima@gmail.com

[2]Department of Physics, RYM Engineering College, Ballari, India
E-mail address: naghabhushananm@gmail.com

[3]Department of Electronics, Proudhadevaraya Institute of Technology, Hosapete, India
E-mail address: rohitha_ujjini@rediffmail.com

ABSTRACT

In this paper we focused on the factorization of integer in detail using well known Shor's algorithm and its quantum part realization. The algorithm finds prime factors any integer more efficiently than any known classical algorithm. It is based on prior knowledge of the answer to the factorization problem. Algorithm includes finding gcd using polynomial time Euclidean algorithm, determination of unknown period from quantum computer and continued fraction expansion approach. Factorization of two integers 21 and 91 are shown in this paper with all steps. Quantum part of the factorization described mathematically.

***Keywords*:** Shor's Algorithm, Quantum Fourier Transform, GCD, Euclidean Algorithm, Factorization

1. INTRODUCTION

Shor's Algorithm was named after its creator Peter Shor, who first published the algorithm in 1994. Quantum computers had already been discussed for many years by researcher and popular media, but it with Shor's discovery that the potential of quantum

(Received 12 February 2019; Accepted 02 March 2019; Date of Publication 03 March 2019)

computers was beginning to be understood. Shor's algorithm has awoken a curiosity among physicists, mathematicians and computer scientists alike. After all, could other problems that are classically very difficult, or require an excessive amount of resources. Researchers say that these problems can be easily solvable on a quantum computer.

The factorization of large numbers on classical computers is extremely resource demanding. Theoretical concepts of shor's algorithm allow a quantum computer to factor the same number with lesser operations. However Shor's algorithm has not gone so far in terms factoring large integers [1]. Shor's algorithm is one of the few quantum algorithms that solves a computational problem with real-world applications: to efficiently find a factor q in a composite number N, which is otherwise thought to be hard. In fact, the hardness of finding the integer factorization of a composite number, is one of the most widely believed conjectures in computer science, and cryptographic applications that we all use in our daily life are built upon this [2]. Several experimental realizations of Shor's algorithm for small numbers have been presented [3–9]. These are all very impressive demonstration of quantum optimal control, but experimental realization of Shor's algorithm with the currently available technology is demanding, and this has led to the need for vast simplifications in the algorithm.

Until now the largest number 143 factored on quantum computer device [10]. Only 4 qubits at 300K are used to perform this computation. Shor's algorithm implemented so far using 4 qubits for factorization do not need prior knowledge of the answer [11-17]. Until 2012 the largest number factored using Shor's algorithm was 15, and today the largest is still only 21.

Since these factorizations are relied on Prior knowledge of the answer, the shor's algorithm implementations were not genuine to the factorization problem. The idea of transforming factorization problem into optimization problem using quantum mechanics was introduced by Burges in 2001 [18], and further it was improved in 2010 by Schaller and Schutzhold [19].

2. FACTORIZATION PROBLEM

Finding prime factors of a given odd composite positive integer 'n'. The problem of factoring integer 'n' can be reduced by choosing a random integer in relatively prime to n and finding smallest positive integer P such that

$$m^P = 1\ mod\ n \tag{1}$$

Shor developed the algorithm in polynomial time to solve the factorization problem. It consists of five steps. Among these steps the step 2 requires the use of quantum computer. Remaining steps of the algorithm can be performed in classical computer.

3. STEPS OF SHOR'S ALGORITHM

Step 1: Choose a random positive integer $x < n$. Compute the greatest common divisor gcd(x, n) using Polynomial time Euclidean algorithm. If $gcd(x, n) \neq 1$, then proceed to next step.

Step 2: Determine the unknown period P using quantum computer of the function $f(a) = x^a \; mod \; n$. Quantum computer is very efficient at period finding.

Step 3: If P is an odd integer, then go back to step 1. The probability of P being odd is $\left(\frac{1}{2}\right)^K$, where K is the number of distinct prime factors of n. If P is even, then proceed to step 4.

Step 4: Since P is even, $\left(x^{P/2} - 1\right)\left(x^{P/2} + 1\right) = x^P - 1 = 0 \; mod \; n$. If $\left(x^{P/2} + 1\right) = 0 \; mod \; n,$ then go to step 1. If $\left(x^{P/2} + 1\right) \neq 0 \; mod \; n$ then proceed to step 5. It can be shown that the probability that $\left(x^{P/2} + 1\right) = 0 \; mod \; n$ is less than $\left(\frac{1}{2}\right)^{K-1}$ where k denotes the number of distinct prime factors of n.

Step 5: Using Euclidean algorithm compute $d_1 = gcd\left(x^{P/2} - 1, n\right)$. Since $\left(x^{P/2} + 1\right) \neq 0 \; mod \; n$, it can be easily shown that, d_1 is a non trivial factor of n. Get another factor, $d_2 = {}^{n}/_{d_1}$.

In the step 2 two quantum registers are initialized. The size of the register 1 is L qubits such that $n^2 \leq q = 2^L \leq 2n^2$. This register holds values $\{0, \; 1, \; 2, \; . \; . \; . \; . \; q - 1\}$ and is used at the quantum fourier transform. Register 2 holds function values of $f(a) = x^a \; mod \; n$. The size of the register 2 is $M = floor(\log_2 n) + 1$.

$$|Reg\ 1 > |Reg\ 2 > \; = |a > |f(a) > = |a > |b >$$

$$= |a_0, \; a_1, \; a_2, \; . \; . \; . a_{L-1} > |b_0. \; b_1, \; b_2, \; . \; . \; . b_{M-1} >$$

The step 2 of the shor's algorithm is as follows.

Step 2.1: Initialize Register 1 and Register 2

$$|\psi_0 > =| \; Reg\ 1 > | \; Reg\ 2 > =|0 > |0 > = |0\,0\,0\,0 . \; . \; . \; 0 > |0\,0\,0\,0 . \; . \; . \; 0 >$$

Step 2.2: Apply the Q-point Fourier transform to register 1.

$$|\psi_0 > \xrightarrow{QFT} |\psi_1 > = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a > |0 >$$

Register 1 holds all the integers $0, 1, \; 2, \; . \; . \; . q - 1$ in superposition.

Step 2.3: Let U_f be the unitary transformation that $|a > to \; |a > |f(a) >$ Apply the linear transformation U_f to the two registers. The result is

$$|\psi_1 > \xrightarrow{U_f} |\psi_2 >$$

$$|\psi_2> = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a> \ |f(a)>$$

$$|\psi_2> = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a> \ |x^a \ mod \ n>$$

The state of two registers is now more than a superposition of two states. In this step we have quantum entanglement of the two registers.

Step 2.4: Measure register 2. It will create a periodic superposition in register 1. Then $|f>$ must collapse into some value $f(a_0)$. The state of $|a>$ will also collapse into the reimage of $f(a_0)$. As f is periodic, the reimage of $f(a_0)$ is $\left\{a_0, \ a_0 + P, \ a_0 + 2P, \ . \ . \ . \ . + \left(\frac{n}{r} - 1\right) P\right\}$.

We get,

$$|\psi_3> = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a> \ |f(a)> \xrightarrow{measure\ register\ 2}$$

$$|\psi_4> = \sqrt{\frac{p}{q}} \sum_{i=0}^{q-1} |a_0 + ip> \ |f(a_0)>$$

Step 2.5: Apply quantum Fourier transform to register 1.

$$|\psi_4> = \sqrt{\frac{p}{q}} \sum_{i=0}^{q-1} |a_0 + ip> \xrightarrow{QFT}$$

$$|\psi_5> = \frac{1}{\sqrt{p}} \sum_{i=0}^{q-1} |i \ \frac{q}{p} > \emptyset_i$$

Here, $\emptyset_i$ is some unimportant phase associated with each term due to linear shift a_0.

Step 2.6: Measure register 1. Measured value is a multiple of $^q/_p$. Save this value.
Go back to step 2.1. Repeat the algorithm several times to get distinct multiples of $^q/_p$. Once enough values are found, calculate the gcd to retrieve $^q/_p$. As q is known, p is easily achieved.

4. FACTORING COMPOSITE NUMBER $n = 21$

1) Choose x

2) Determine q
3) Initialize first register (r_1)
4) Initialize second register (r_2)
5) Take QFT on first register
6) Measurement
7) Continued Fraction Expansion $\rightarrow$ Determine r
8) Check $r \rightarrow$ Determine factors.

- If it is not co-prime with n, for example $x = 7, \rightarrow gcd(x,\ n) = gcd(7,\ 21) = 7 \rightarrow \frac{21}{7} = 3 \rightarrow done,$ Factors are 7 and 3
- If it is co-prime with n, for example $x = 11, \rightarrow gcd(x,\ n) = \mathrm{gcd}(11,\ 21) = 1$
- Choose q such that $n^2 \leq q \leq 2n^2 \rightarrow\ n^2 = 21^2 = 441\ ,\ 2n^2 = 882,\quad q = 2^L$

Table 1. Selecting Appropriate $\boldsymbol{q}$ value.

L	0	1	2	3	4	5	6	7	8	9	10
q	1	2	4	8	16	32	64	128	256	512	1024

The number between 441 and 882 is 512. Hence $q = 512 = 2^9$.

- Initialize registers 1 and 2. Thus the state of the two registers becomes

$$|\psi_0> = |0>_{r_1}\ |0>_{r_2}$$

$$|\psi_0> = \frac{1}{\sqrt{512}} \sum_{a=0}^{511} |a>|0>$$

This corresponds to $\frac{1}{\sqrt{2}}(|0> + |1>)$ on all bits.

- Initialize the 2nd register with superposition of all states $x^a\ mod\ n$.

$$|\psi_1> = \frac{1}{\sqrt{512}} \sum_{a=0}^{511} |a>|11^a\ mod\ 21>$$

Table 2. Finding Period P.

a	0	1	2	3	4	5	6	7	8	9	. . .
$11^a\ mod\ n$	1	11	16	8	4	2	1	11	16	8	. . .

Period $P = 6$

$$|\psi_1> = \frac{1}{\sqrt{512}}\{\,|0>|1>+|1>|11>\;+|2>|16>\;+|3>|8>\;+\;....|511>|11>\}$$

- Apply quantum Fourier transform on first register. The QFT is

$$X(k) = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} x(n)\;{W_N}^{kn}$$

Put $n = m \quad and \quad N = 512$ in the above equation.

$$|\psi_2> \;\; QFT\{|\psi_1>\}$$

$$|\psi_2> = \frac{1}{\sqrt{512}}\sum_{m=0}^{511}|\psi_1>\;{W_N}^{km}$$

$$|\psi_2> = \frac{1}{\sqrt{512}}\sum_{m=0}^{511}\frac{1}{\sqrt{512}}\sum_{a=0}^{511}|a>|11^a\;\;mod\;21>{W_N}^{km}$$

Interchange the order of summation

$$|\psi_2> = \frac{1}{512}\sum_{a=0}^{511}|a>\sum_{m=0}^{511}{W_N}^{am}\;\;|11^a\;\;mod\;21>$$

For $= 2$,

$$|\psi_2> = \frac{1}{512}\;\;|2>\sum_{m=0}^{511}{W_{512}}^{2m}\;\;|16>$$

Approximate result of above equation is 427. i.e C= 427.

- Continued Fraction Expansion:

$$\frac{C}{q} = \frac{427}{512} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + ...}}}$$

$$d_0 = a_0 \qquad d_1 = 1 + a_0 a_1 \qquad d_n = a_n d_{n-1} + d_{n-2}$$
$$r_0 = 1 \qquad r_1 = a_1 \qquad r_n = a_n r_{n-1} + r_{n-2}$$

$$\frac{427}{512}=0+\cfrac{1}{\cfrac{512}{427\ mod\ 512}}=0+\cfrac{1}{\cfrac{512}{427}}=0+\cfrac{1}{1+\cfrac{85}{427}}=0+\cfrac{1}{1+\cfrac{1}{\cfrac{427}{85}}}=0+\cfrac{1}{1+\cfrac{1}{5+\cfrac{2}{85}}}$$

$$=0+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{\cfrac{85}{2}}}}=0+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{42+\cfrac{1}{2}}}}$$

$$d_0=0 \qquad d_1=1+0\,, \qquad r_0=1, \quad r_1=a_1=1$$

$$d_2=a_2d_1+d_0=5\times1+0=5$$

$$r_2=a_2r_1+r_0=5\times1+1=6$$

$$d_3=a_3d_2+d_1=42\times5+1=211$$

$$r_3=a_3r_2+r_1=42\times6+1=253$$

$$d_4=a_4d_3+d_2=2\times211+5=427$$

$$r_4=a_4r_3+r_2=2\times253+6=512$$

Table 3. Finding $\boldsymbol{r}$ through Continued Fraction Expansion.

n	0	1	2	3	4	$\frac{d_1}{r_1}=1,\ \frac{d_3}{r_3}=\frac{211}{253},\ \frac{d_4}{r_4}=\frac{427}{512}$
a_n	0	1	5	42	2	$\frac{d_2}{r_2}=\frac{5}{6}\rightarrow r=6\rightarrow This\ works$
d_n	0	1	5	211	427	
r_n	1	1	6	253	512	

First Factor of 21 is $d_1=gcd\left(x^{P/2}-1,n\right)=gcd\left(11^{6/2}-1,21\right)=gcd(1330,\ 21)=7$

Second factor of 21 is $\qquad d_2=\frac{n}{d_1}=\frac{21}{7}=3$

5. FACTORING COMPOSITE NUMBER OF $\boldsymbol{n}=\mathbf{91}$

Choose q such that $n^2\le q\le 2n^2$. $\quad 8281\le q\le 16562,\quad Let\ q=2^{14}=16384$

Step 1: Choosing random positive integer $x=3$, Since $gcd(91,\ 3)=1$, proceed to step 2 to find the period P.

$$f(a)=x^a\ mod\ n=3^a\ mod\ 91$$

Table 4. Selecting Period P.

a	0	1	2	3	4	5	6	7	. . . . .
$f(a)$	1	3	9	27	81	61	1	3	. . . . .

Period P = 6

Step 2: Initialize registers 1 and 2. Thus the state of the two registers becomes

$$|\psi_0>=|0>|0>$$

$$|\psi_0>=\frac{1}{\sqrt{16384}}\sum_{a=0}^{16383}|a>|0>$$

This corresponds to $\frac{1}{\sqrt{2}}(|0>+|1>)$ on all bits. Initialize the 2nd register with superposition of all states $x^a\ (mod\ \ n)$.

$$|\psi_1>=\frac{1}{\sqrt{16384}}\sum_{a=0}^{16383}|a>|3^a\ (mod\ \ n)>$$

$$|\psi_1>=\frac{1}{\sqrt{16384}}\sum_{a=0}^{16383}|a>|3^a\ (mod\ \ 91)>$$

$$|\psi_1>=\frac{1}{\sqrt{16384}}\{|0>|1>+|1>|3>+|2>|9>+|3>|27>+|4>|81>+|5>|61>+|6\ >|1>+|7>|3>+|8>|9>+|9>|27>+|10>|81>+|11>|61>+|12>|1>+|13>|3>+\ .\ .\ .\ .\ .\ .\ .\ +|16380>|1>+|16381>|3>+.\ .\ .\ .|16383>|27>\}$$

Step 3: The quantum Fourier transform on the 1st register
The QFT is

$$X(k)=\frac{1}{\sqrt{N}}\sum_{m=0}^{N-1}x(n){W_N}^{km}$$

$$|\psi_2>=\frac{1}{\sqrt{16384}}\sum_{m=0}^{16383}\frac{1}{\sqrt{16384}}\sum_{a=0}^{16383}{W_N}^{am}|a>|3^a\ (mod\ 91)>$$

Consider,

$$\sum_{a=0}^{16383}{W_N}^{am}|a>|3^a\ (mod\ 91)>=|1>+{W_N}^{m}|3>+{W_N}^{2m}|9>+{W_N}^{3m}|27>+{W_N}^{4m}|81>+{W_N}^{5m}|61>+.\ .\ .\ .+{W_N}^{16380m}|1>+{W_N}^{16381m}|3>+.\ .\ .\ .{W_N}^{16383m}|27>$$

The result of $|\psi_2>=C=13453.$

- Continued Fraction Expansion:

$$\frac{C}{q}=\frac{13453}{16384}=0+\cfrac{1}{\cfrac{16384}{13453}}=0+\cfrac{1}{1+\cfrac{2931}{13453}}=0+\cfrac{1}{1+\cfrac{1}{\cfrac{13453}{2931}}}=0+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1729}{2931}}}$$

$$=0+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{\cfrac{2931}{1729}}}}=0+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1202}{1729}}}}=0+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{\cfrac{1729}{1202}}}}}$$

$$=0+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{527}{1202}}}}}=0+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{\cfrac{1202}{527}}}}}}$$

$$=0+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{148}{527}}}}}}=0+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{\cfrac{527}{148}}}}}}}$$

$$=0+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{3+\cfrac{83}{148}}}}}}}$$

$$=0+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3}}}}}}}}}}}}}$$

Table 5. Finding r through Continued Fraction Expansion.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
a_n	0	1	4	1	1	2	3	1	1	3	1	1	1	1
d_n	0	1	4	5	9	23	78	101	179	638	817	1455	2272	3727
r_n	1	1	5	6	7	20	67	87	154	549	703	1252	1955	3207

$d_0 = a_0 \qquad d_1 = 1 + a_0 a_1 \qquad d_n = a_n d_{n-1} + d_{n-2}$

$r_0 = 1 \qquad r_1 = a_1 \qquad r_n = a_n r_{n-1} + r_{n-2}$

First Factor of 91 is $d_1 = gcd\left(x^{P/2} - 1, n\right) = gcd\left(3^{6/2} - 1, 91\right) = gcd(26,\ 91) = 13$

Second factor of 21 is $d_2 = \frac{n}{d_1} = \frac{91}{13} = 7$

6. EUCLIDEAN ALGORITHM

Euclidean algorithm is an efficient method for computing the greatest common divisor (gcd). Algorithm steps are as follows:

Step 1: Let a and b are the integers such that $a > b$ and r be the remainder when a is divided by b. Assume $r \neq 0$ and q is the quotient.

Step 2: $a = bq + r,\ r = a - bq$. Whatever divides a and b must also divide r and also divide b. Similarly any divisor of b and r must also be divisor of a and also divide b. Thus $gcd(a,\ b) = gcd(b,\ r)$. When $r = 0$, $a = bq$ then $gcd(a,\ b) = b$.
Algorithm works by repeatedly using $gcd(a,\ b) = gcd(b,\ r)$. If $a > b$ then compute remainder $r\ of\ a \div b$. If this is zero, then $gcd(a, = b) = b$. If $r \neq 0$, take b and r, compute the remainder $r_1 = b \div r$. If $r_1 = 0$ then using $gcd(a,b) = gcd(b,r) = gcd(r,\ r')$. Continue until the remainder is zero.

7. CONCLUSIONS

Mathematical description on factorization of composite numbers $n = 21$ and $n = 91$ are cleared explained with all steps using shor's algorithm. Quantum part in the factorization problem is shown with approxiamte results. This helps in finding the value of r. Using this value factors compoiste numbers are determined with the help Euclidean algorithm. The mathematical description explained in this paper can be used to factorize the larege integers.

References

[1] Nikesk S Dattani and Nathaniel Bryans, Quantum factorization of 56153 with only 4 qubits, *Quantum Physics*, 27th November 2014. arXiv:1411.6758

[2] Niklas Johansson and Jan Ake Larsson, Realization of Shor's Algorithm at Room Temperature, *Quantum Physics*, 10th January 2017. arXiv:1706.03215

[3] T. Monz et al., Realization of a scalable Shor algorithm, *Science* 351, 1068–1070 (2016).

[4] E. Lucero et al., Computing prime factors with a Josephson phase qubit quantum processor. *Nature Physics* 8, 719-723 (2012).

[5] E. Martin-Lopez et al., Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nature Photonics* 6, 773–776 (2012).

[6] Politi, J. C. Matthews, and J. L. O'Brien, Shor's quantum factoring algorithm on a photonic chip. *Science* 325, 1221–1221 (2009).

[7] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits. *Physical Review Letters* 99 (2007) 10.1103/PhysRevLett.99.250504

[8] B. P. Lanyon et al., Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement. *Physical Review Letters* 99 (2007) 10.1103/PhysRevLett.99.250505

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

[10] N. Xu, J. Zhu, D. Lu, X. Zhou, X. Peng, and J. Du. Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System. *Physical Review Letters*, vol. 108, no. 13, p. 130501, Mar. 2012.

[11] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, vol. 414, no. 6866, pp. 883–7, Jan. 2001.

[12] B. Lanyon, T. Weinhold, N. Langford, M. Barbieri, D. James, A. Gilchrist, and A. White, Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement. *Physical Review Letters*, vol. 99, no. 25, p. 250505, Dec. 2007.

[13] C.-Y. Lu, D. Browne, T. Yang, and J.-W. Pan, Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits. *Physical Review Letters*, vol. 99, no. 25, p. 250504, Dec. 2007.

[14] Politi, J. C. F. Matthews, and J. L. O'Brien, Shor's quantum factoring algorithm on a photonic chip. *Science*, vol. 325, no. 5945, p.1221, Sep. 2009.

[15] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'Brien, Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nature Photonics*, vol. 6, no. 11, pp. 773–776, Oct. 2012.

[16] E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. 'Malley, D. Sank, A. Vainsencher, J. Wenner, T. White, Y. Yin, A. N. Cleland, and J. M. Martinis, Computing prime factors with a Josephson phase qubit quantum processor. *Nature Physics*, vol. 8, no. 10, pp. 719–723, Aug. 2012.

[17] J. A. Smolin, G. Smith, and A. Vargo, Oversimplifying quantum factoring. *Nature*, vol. 499, no. 7457, pp. 163–5, Jul. 2013.

[18] C J C Burges, Factoring as Optimization. *Microsoft Research*, Vol. MSR-TR-200, 2002

[19] G. Schaller and R. Schutzhold, The role of symmetries in adiabatic quantum algorithm. *Quantum Information and Computation*, vol. 10, no. 1, pp. 109-140. 2010.

Biography

Poornima Aradhyamath received B.Sc degree from Gulbarga University and M.Sc in Physics from Karnataka University Dharawad, Karnataka. She worked as assistant professor at BITM, for 10 years. Presently she is a regular research scholar in the Department of Physics at RYM Engineering College, Ballari. She has four research paper in international Journals and presented two papers in international conferences.

Nagabhushana N. M. received B.Sc, M.Sc and PhD degree from Gulbarga University, Karnataka. His area of research is Nuclear Physics, Material and Quantum Computing. He has Published 10 research papers in International journals and many papers in national and international conferences. Presently he is working as a professor and HOD of physics department at RYM Engineering College, Ballari, Karnataka. He has guided many M.Sc projects and guiding 8PhD students under VTU, Belagavi

Rohitha Ujjinimatad received B.E. degree in Electronics and Communication Engineering from Bangalore University, M.Tech. in Digital Electronics and Ph.D. from VTU, Belagavi, India. He is student member of IEEE and life member of ISTE and he is working as Professor in ECE Department at Proudadevaraya Institute of Technology, Hospete, India. His area of research is spectrum sharing and spectrum sensing in cognitive radio networks. He has guided many B.E. and M.Tech. Projects, and guiding five Ph.D. students. He has one national and 16 International Conference Papers to his credit. Also he has published papers in IET Communications, IET Journal of Engineering, Springer, IJCAand other reputed journals etc.