2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)
Galgotias University, Greater Noida, UP, India. Oct 30-31, 2020

An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm

Vaishali Bhatia
Chitkara University Institute of Engineering and Technology,
Chitkara University, Punjab India
vaishali.bhatia@chitkara.edu.in

K.R. Ramkumar
Chitkara University Institute of Engineering and Technology,
Chitkara University, Punjab India

***Abstract*—Quantum Computing is a prominent word in this era as it allows computation to be performed in no time. The motive of using Quantum Computing (QC) is that even exponentially large number of problems can be solved using it which was earlier difficult with the classical computing. Conventional methods are based on usage of bits which consist of 0's and 1's while QC works with qubits. The main issue is that conventional computing has issue of storage as well as computation even when parallel computation is performed on it. Concept of quantum parallelism allows the computation to be performed in exponentially very low time as compared to conventional method. This paper will discuss about Quantum Computing Algorithms and how Shor's algorithm is able to break RSA algorithms is discussed. Entanglement and superposition of qubits helps fast computation. The demonstration of the applicability has been evaluated based on Computation time, storage capacity, accuracy, confidentiality, efficiency, integrity, and availability. Among various algorithms Shor's technique is able to break various encryption algorithm with more supremacy as compared to conventional computing methods. In nutshell, paper will discuss about various QC algorithms and will illustrate how shor's algorithm is able to crack RSA.**

Keywords—Quantum Computing, Classical Computing, Entanglement, Superposition, Qubits, Computation time, Shor's Algorithm.

I. INTRODUCTION

Quantum Computing (QC) was started in 1980's and is based on the phenomenon of Quantum mechanics along with the techniques like Entanglement and superposition. The computation when performed using computers are known as quantum computers which came into existence in 1994. The first problem that was addressed by QC was game of sudoku which was solved using 16 qubits [1]. The conventional computing system it has two possible states which are 0 and 1 while QC consists of qubits where each bit consists of two possible states. In 2018 the largest possible quantum computer consists of 72 qubits [2].

The idea which leads to development of QC is that when large amount of data is available to the user so for processing it the task is to parallelize task in order to speed up computation but it led to large execution time even with large number of cores. With QC large amount of data can be handled parallelly using principle of Entanglement, Interference and superposition of qubits and running them parallelly [3]. Its advantage is that it not only helps in dealing with dynamic problems but also provide solution to hard and complicated problems in very less time.

There are basic terminologies that should clear while going deep into the quantum mechanics is that whenever any atom or particle processing magnetic properties are put into magnetic field then it is either deflected upward or downward are known as spins [4]. Fig 1 illustrates the **spin** movement in case of Quantum computers which consist of either upward and downward movement while in classical computers it consists of up, down, left and right.

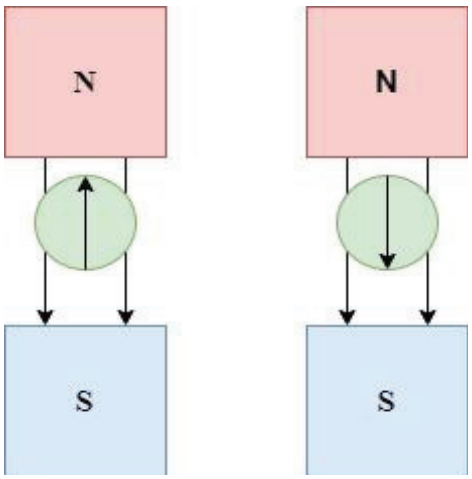

Fig. 1. Spin Movement in case of Quantum Computers

These are based on the principle of superposition which states that when two states are combines the resultant will also be a valid state is known as superposition principle [5]. The particle is represented by qubits which consits of states such as 00, 01,10 and 11. In this 0 represemts up spin while 1 represents down spin.

Here **|1 0>** means there are two bits one is in up spin while other is in down spin.

Figure 2 depicts spin movement in case of classical computers.

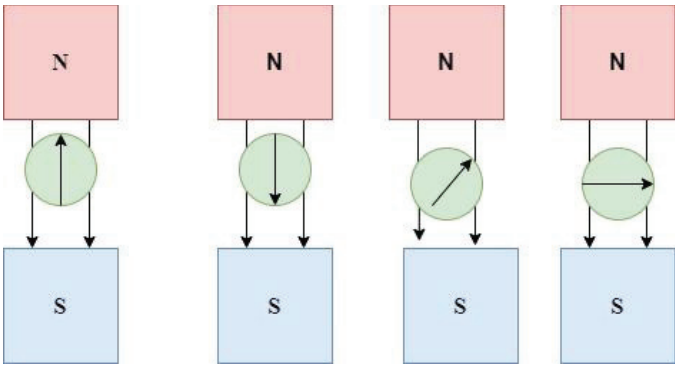

Fig. 2. Spin Movement in case of Classical Computers

It is different from classical computing as it is based on the trying all possibilties of amplitudes to give best results.

$$\varphi = \alpha|0> + \beta|1> \quad (1)$$

Here in the above equation φ represents quantum state while $\alpha|0> + \beta|1>$ represents **superposition** where the value of **|0> is [1 0]** and that of **|1> is [0 1].**

Matrix multiplication of |0 1> is 0 while that of |1 1> is 1. Similarly other superpsoition resuts are represented by the below equation [6].

$$|+> = |0> + |1>/2 \quad (2)$$

$$|-> = |0> - |1>/2 \quad (3)$$

The next relevant term in the field of QC is **Quantum Gates [7].** Just like classical computers use logical gates like AND, OR, NOT for operations similarly QC use quantum gates such as Pauli-X, Pauli-Y, Pauli-Z, Hadamard etc. for performing operations [8]. Below equation represents Hadamard matrix on which further operations like superposition with 0 and 1 qubits can be applied for performing operations [9].

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (4)$$

Interference of waves is performed by byproduct of superposition of qubits to get the desired result [10].

Entanglement is the process in which correlation is described between two or more states or in reference to other states is known as entanglement. It is considered to be the most prominent as it is very difficult to find correlation between particles in case of classical computers [11].

Figure 3 depicts basic fundamental of evolution of Quantum Computing which shows it started in 1970's [12] with the basic idea and further extended to commercial boom till now.

Fig. 3. Evolution in field of Quantum Computing

The paper is divided into various sections where section I contains detail about Introduction to Quantum Computing and its various terms as discussed above, Section II consists of various algorithms in QC, Section III consists of literature survey which illustrates work done by various researchers in this field, Section IV consists of proposed work which illustrates how Shor's Algorithm is able to crack RSA Algorithm, Section V consists of Results and Discussions.

II. Quantum Algorithms

This section will discuss about various Quantum Algorithms and how they are important.

A. Deutsch Jozsa Algorithm

It was the first algorithm which was developed in 1992 order to compete with the classical computers. It takes input as 0 or 1 and gives output as 0 or 1 [13].

$$f: \{0,1\} \rightarrow \{0,1\} \quad (5)$$

This algorithm is said to be balanced if it has equal number of 0's and 1's as output. It takes n digit binary number as input and gives result in either 0 or 1.

It was able to solve hard problems with exponentially low complexities in comparison to classical computing with $2^{n-1}+1$-time complexity in worst case [14]. It works on the principle is that it takes the input apply Hadamard operation then prepare all configuration in order to apply oracle function then grouping along with mapping is performed in order to give result in either 0 or 1. Oracle function states that if f(x)=0 apply I gate and if f(x)=1 then apply X gate [15]. Figure 4 depicts implementation of Deutsch Jozsa implemented using Qiskit for value of input n=3 bits.

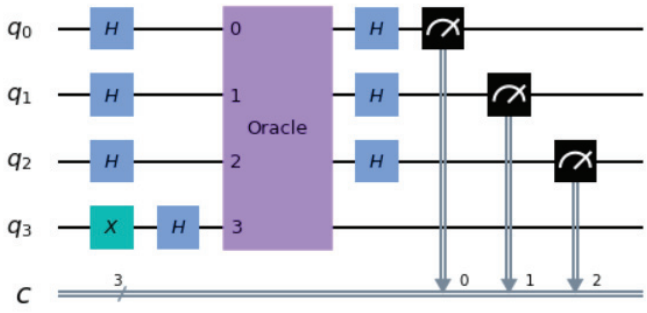

Fig. 4. Implementation of Deutsch Jozsa Algorithm using Qiskit

B. Grover's Algorithm

It works on the principle of parallelism which was developed in 1996 which has complexity of O(√N) as compared to O(N) [16]. It is basically used for searching database and works mainly with unstructured data [17]. For example: If we have n items and we need to look for any item then this algorithm can be used.

$$f(x): \{0 \; for \; u = x \; and \; 1 \; for \; u! = x\} \quad (6)$$

Figure 5 illustrates implementation of Grover's algorithm for input n=4 bits.

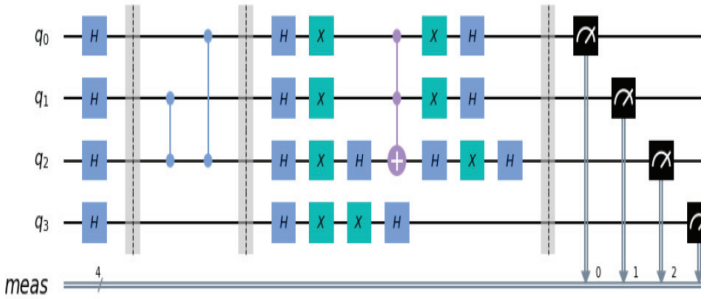

Fig. 5. Implementation of Grover's Algorithm using Qiskit

C. *Simon's Algorithm*

This algorithm was introduced in 1997 and is based on the principle of Discrete Fourier Transformation in this case it is known as Quantum Discrete Fourier Transformation [18]. Its function is to basically speed up the process of computation. It works on the method of one to one and two to mapping which consists of mapping one input with one output or mapping two inputs with one output [19]. Figure 6 shows the implementation of Simon's Algorithm using Qiskit

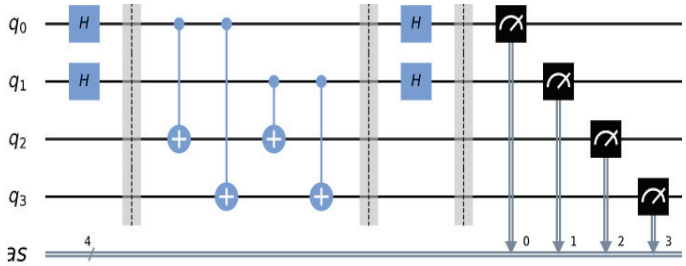

Fig. 6. Implementation of Simon's Algorithm using Qiskit

D. *Shor's Algorithm*

Shor's Algorithm was developed by Peter Shor in 1994 where the task is to find the factors of algorithm in polynomial time using Quantum computers [20]. Shor's Algorithm is also known as Shor's Factoring algorithm which is used when we want to find the prime factor in polynomial time. This is based on the concept that the factors of large numbers are very difficult to formulate. It uses technique of measuring periodicity of objects [21].

To find the factors of large number is believed to be Hard problem for classical computers. Let us suppose p and q are two large numbers where N=p*q so the task is to find the values of p and q if the value of N is known to us. It is possible to find these values but time that will be taken is not known if we try to find factors using Brute Force Algorithm. If we search in classical computing there is no other model which will perform better than brute force algorithm [22]. Task of Shor's algorithm is to find period of the periodic function. Encryption algorithm which is based this concept of factoring technique

The operator used for Shor's Algorithm is Quantum Fourier Transformation. It works well with the factoring algorithm and is till now able to find the factors of equation till 21 qubits [23]. The steps followed for implementation is that first registers are initialized in terms of superposition of Q states along with the tensor product [24]. Using the above states quantum function f(x) is created to these input registers Inverse Quantum Fourier Transformation is applied on it. Then other irreducible operations are performed on it [25]. Its task is mainly the reduction of the factorization problem.

Shor's Algorithm:

1. First step is to take two prime values from the user p and q.
2. Calculate n=p*q.
3. Check if n is even, prime or prime power.
4. Suppose x, where x<n calculate gcd (x, n)! =1 then find factors of n.
5. Suppose smallest value of q as power of 2 in such a way that $n^2 \leq q < 2n^2$.
6. Period of r is calculated using r of $x^a \bmod n$ this calculate will give result in variable c such that c/q = d/r.
7. Find gcd (d, r) =1 using continued fraction expansion.
8. If r is even then p, q = gcd ($x^{r/2} \pm 1$, n) else go to step 2.

RSA Algorithm:

1. Suppose two prime numbers p, q.
2. Calculate n, where n=p*q
3. Suppose value of e, such that $1<e<\phi(n)$
4. Here $\phi(n) = (p-1) * (q-1)$
5. Public key is e, n
6. $d = (k * \phi(n) + 1)/e$, k is some integer value
7. Private key, d, n

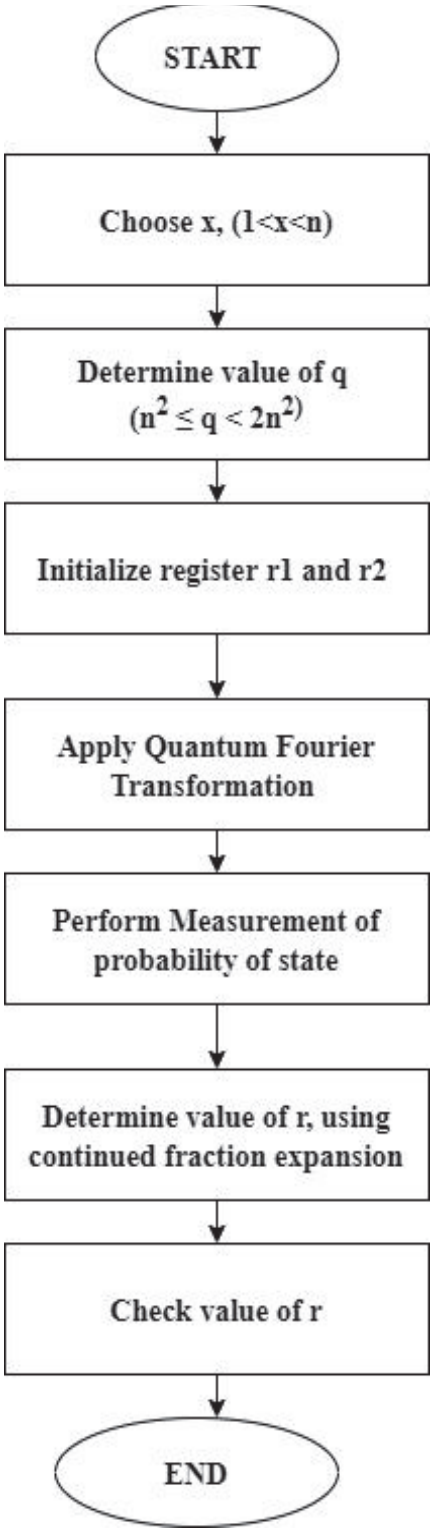

Fig. 7. Flow process of Shor's Algorithm

Figure 7 depicts the flow process of Shor's algorithm which shows how the algorithm works.

III. RELATED WORK

This section will give comparative analysis of work of various researcher in this field. This section will elaborate the work done by various researchers in breaking RSA and other encryption algorithms using RSA. Table 1 illustrates data in tabular format.

TABLE I. COMPARATIVE ANALYSIS OF DIFFERENT AUTHORS

Author	Proposed Model	Technique/ Advantage	Demerits
Seifert et. al. [26]	Diophantine approximation	Improved version than classical technique	Added more overhead
Bacon, D. et al. [27]	Discussed Quantum in different areas	Efficient Factoring algorithm	Lacks Accuracy
Chang et. al. [28]	Lemma 5-1 to Lemma 5-9	Breaking of DES algorithm	High time complexity
Bacnik et. al. [29]	Factoring method	Technique of breaking RSA	Lacks error correction
Eicher J et. al. [30]	Peter shor's algorithm	Used Shor's algorithm for analysis of Discrete Log cryptosystem and Elliptic curve cryptosystem	More Complexity
Casey J. Riggs [31]	Discussed various algorithms	RSA security along with Simon's and Shor's algorithm	Time Complexity
Lu, C. Y [32]	Photonic Qubits Technique	Real entanglement was performed in order to verify result of theory and experiments	Little Complex process
Fowler, A. G et. al.[33]	Nearest Neighbor Technique	Implemented Shor's algorithm using Quantum Gates	More usage of gates
Wang, Y et. al. [34]	Discussed security of RSA	Fixed point on attack on RSA in polynomial time is discussed in this paper.	Non periodic problems are yet not discovered in this model.
Nene, M et. al. [35]	MATLAB used for implementation of breaking RSA using Shor's Algorithm	Results obtained are accurate	Faces difficulties when the value of N increases.
Childs et. al. [36]	Working out on Algebraic problems	Speeding up of Super-polynomials are discussed	Lacks accuracy
Bernstein et. al. [37]	GEECM Technique	Technique which will generate prime numbers. Claims to be faster than Shor's algorithm in terms of security as well as finding factors of polynomials	Lacks efficiency

IV. METHODOLOGY

RSA is an efficient algorithm which is based on the concept of usage of two keys public key and private key where one key is used for encryption while other key is used for the process of decryption. A user is secure till these keys are secure.

This algorithm is based on the concept of prime factorization which are easy to crack if the message is of small size while as long as the number of bits in the message increases more harder is to crack it. To solve the problem of handling large number of bits in case of finding prime factorization introduction of Shor's Algorithm came to rescue in 1994 which can easily solve the problem of handling hard problem which were very difficult to compute in case of classical computers. Finding factors of two prime numbers is hard problem to handle in case of classical computes while it is easy to handle in case of Quantum computers.

Public key used in RSA algorithm is based on the prime factors which are used for the process of encryption if these factors are not known then it is difficult to decrypt these numbers. The complexity of finding factors of large number is exponentially large for bigger numbers which are solved by using Shor's Algorithm. Complexity of finding factors of polynomial is $O(\exp(3\sqrt{64}/9n(logn)$^2 in case of classical computers while it is O (n^3 log n) in case of quantum computers.

Let's take an example to illustrate the concept to find gcd of 21

and 15 we will use technique like: Gcd (21,15) so

1. 21 = 1*15 + 6
2. 15 = 2*6+3
3. 6 = 2*3 + 0

Since 3 is common to both so this is gcd of 21 and 15.

So, to break this factor in general we use formula:

x^a mod N where value of x will be tried and tested and stopped once it starts repeating. Let's illustrate this with example

1. 2^0 mod 15 = 1 mod 15
2. 2^1 mod 15 = 2 mod 15
3. 2^2 mod 15 = 4 mod 15
4. 2^3 mod 15 = 8 mod 15
5. 2^4 mod 15 = 1 mod 15

Since its repeating at value **r=4 so it is the period of function.**

So, we can say

$(\mathbf{2^2})^2$ mod 15 hence value of x=4, if value of x is even then it is considered for operation and if it is odd then other value of x is guessed.

In this technique we start with guessing value x so main difficulty is in finding the value period. Shor's algorithm is based on the concept of usage of Bounded-error probabilistic polynomial time (BPP) is based in solvable polynomial technique using which any problem can be solved with the complexity of O(n).

Since finding period was main issue which was solved using Quantum Computing. So, to compute period of equation we need to find it using Euclid Algorithm.

So as per our example value of x=4, N=15 so

gcd (15,4+1) = gcd (15,5) = 5 (i)

gcd (15,4-1) = gcd (15,3) = 3 (ii)

So, from (i) and (ii) we get 5*3 = 15 which was the value of N.

Step-wise procedure of breaking RSA using Shor's Algorithm:

1. First step is to take number n.
2. Choose a prime number m and then calculate value of gcd (n, m) =1
3. Find value of function f=m^amod n
4. Running Shor's algorithm with periodic function (p).
5. If value of p is even then follow step 4.
6. Apply Euclidean Algorithm
   d = gcd ($m^{p/2}$-1, n)

V. RESULTS AND DISCUSSIONS

As a result, it can be concluded that there are various models the number of bits wrt to execution time was plotted using qiskit and results obtained are shown in the graph below for the quantum model.

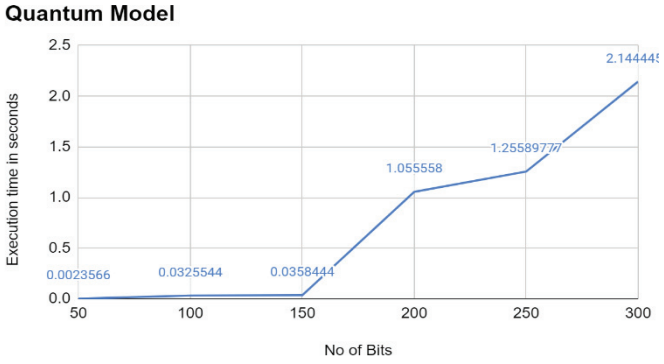

Fig. 8. Qunatum Model

The paper has discussed about Quantum Computing its various techniques along with this discussed about the shor's algorithm and how this algorithm is able to break RSA and explains how the above algorithm is better than another algorithm. In a nutshell in future this model can be used for breaking other encryption algorithms and dealing with large file size and increasing more accuracy in it.

REFERENCES

[1] Kubiatowicz, J. (2007, August). The future is Quantum Computing?. In *2007 IEEE Hot Chips 19 Symposium (HCS)* (pp. 1-5). IEEE.

[2] Bernhardt, C. (2019). *Quantum Computing for Everyone*. Mit Press.

[3] Sarkar, K., & Bhattacharyya, S. P. (2017). *Soft computing in chemical and physical sciences: a shift in computing paradigm*. CRC Press.

[4] Gershenfeld, N. A., & Chuang, I. L. (1997). Bulk spin-resonance quantum computation. *science*, *275*(5298), 350-356.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 19

[5] Neergaard-Nielsen, J. S., Nielsen, B. M., Hettich, C., Mølmer, K., & Polzik, E. S. (2006). Generation of a superposition of odd photon number states for quantum information networks. *Physical review letters*, *97*(8), 083604.

[6] Leuenberger, M. N., & Loss, D. (2001). Quantum computing in molecular magnets. *Nature*, *410*(6830), 789-793.

[7] Knill, E., Leibfried, D., Reichle, R., Britton, J., Blakestad, R. B., Jost, J. D., ... & Wineland, D. J. (2008). Randomized benchmarking of quantum gates. *Physical Review A*, *77*(1), 012307.

[8] Raychev, N. (2015). Quantum computing models for algebraic applications. *International Journal of Scientific and Engineering Research*, *6*(8), 1281.

[9] Song, X., Wang, S., El-Latif, A. A. A., & Niu, X. (2014). Dynamic watermarking scheme for quantum images based on Hadamard transform. *Multimedia systems*, *20*(4), 379-388.

[10] Bhambri, S. (2014). Quantum Clouds: A future perspective. *arXiv preprint arXiv:1410.6502*.

[11] Preskill, J. (2012). Quantum computing and the entanglement frontier. *arXiv preprint arXiv:1203.5813*.

[12] Shor, P. W. (2002, May). Introduction to quantum algorithms. In *Proceedings of Symposia in Applied Mathematics* (Vol. 58, pp. 143-160).

[13] Tesch, C. M., & de Vivie-Riedle, R. (2004). Vibrational molecular quantum computing: Basis set independence and theoretical realization of the Deutsch–Jozsa algorithm. *The Journal of chemical physics*, *121*(24), 12158-12168.

[14] Gulde, S., Riebe, M., Lancaster, G. P., Becher, C., Eschner, J., Häffner, H., ... & Blatt, R. (2003). Implementation of the Deutsch–Jozsa algorithm on an ion-trap quantum computer. *Nature*, *421*(6918), 48-50.

[15] Shi, F., Rong, X., Xu, N., Wang, Y., Wu, J., Chong, B., ... & Feng, M. (2010). Room-temperature implementation of the Deutsch-Jozsa algorithm with a single electronic spin in diamond. *Physical review letters*, *105*(4), 040504.

[16] Li, S. S., Long, G. L., Bai, F. S., Feng, S. L., & Zheng, H. Z. (2001). Quantum computing. *Proceedings of the National Academy of Sciences*, *98*(21), 11847-11848.

[17] Walther, P., Resch, K. J., Rudolph, T., Schenck, E., Weinfurter, H., Vedral, V., ... & Zeilinger, A. (2005). Experimental one-way quantum computing. *Nature*, *434*(7030), 169-176.

[18] Brassard, G., & Hoyer, P. (1997, June). An exact quantum polynomial-time algorithm for Simon's problem. In *Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems* (pp. 12-23). IEEE.

[19] Gay, S. J. (2006). Quantum programming languages: Survey and bibliography. *Mathematical Structures in Computer Science*, *16*(4), 581-600.

[20] Gershenfeld, N. A., & Chuang, I. L. (1997). Bulk spin-resonance quantum computation. *science*, *275*(5298), 350-356.

[21] Hayward, M. (2008). Quantum computing and shor's algorithm. *Sydney: Macquarie University Mathematics Department.*

[22] Lanyon, B. P., Weinhold, T. J., Langford, N. K., Barbieri, M., James, D. F., Gilchrist, A., & White, A. G. (2007). Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement. *Physical Review Letters*, *99*(25), 250505.

[23] Van Meter, R., Itoh, K. M., & Ladd, T. D. (2008). Architecture-dependent execution time of Shor's algorithm. In *Controllable Quantum States: Mesoscopic Superconductivity and Spintronics (MS+ S2006)* (pp. 183-188).

[24] Vandersypen, L. M., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., & Chuang, I. L. (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, *414*(6866), 883-887.

[25] Beauregard, S. (2002). Circuit for Shor's algorithm using 2n+ 3 qubits. *arXiv preprint quant-ph/0205095*.

[26] Seifert, J. P. (2001, April). Using fewer qubits in Shor's factorization algorithm via simultaneous diophantine approximation. In *Cryptographers' Track at the RSA Conference* (pp. 319-327). Springer, Berlin, Heidelberg.

[27] Bacon, D., & VAn DAm, W. (2010). Recent progress in quantum algorithms. *Communications of the ACM*, *53*(2), 84-93.

[28] Chang, W. L. (2010, September). Fast Quantum Algorithms of Breaking the Data Encryption Standard. In *International Symposium on Parallel and Distributed Processing with Applications* (pp. 520-527). IEEE.

[29] Bacnik, B. Breaking RSA with Quantum Computing.

[30] Eicher, J., & Opoku, Y. (1997). Using the Quantum Computer to Break Elliptic Curve Cryptosystems.

[31] Riggs, C. J., Lewis, C. D., Mailloux, L. O., & Grimaila, M. (2016). Understanding quantum computing: a case study using Shor's algorithm. In *Proceedings of the International Conference on Foundations of Computer Science (FCS)* (p. 25). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[32] Lu, C. Y., Browne, D. E., Yang, T., & Pan, J. W. (2007). Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits. *Physical Review Letters*, *99*(25), 250504.

[33] Fowler, A. G., Devitt, S. J., & Hollenberg, L. C. (2004). Implementation of Shor's algorithm on a linear nearest neighbour qubit array. *arXiv preprint quant-ph/0402196*.

[34] Wang, Y., Zhang, H., & Wang, H. (2018). Quantum polynomial-time fixed-point attack for RSA. *China Communications*, *15*(2), 25-32.

[35] Nene, M. J., & Upadhyay, G. (2016). Shor's Algorithm for Quantum Factoring. In *Advanced Computing and Communication Technologies* (pp. 325-331). Springer, Singapore.

[36] Childs, A. M., & Van Dam, W. (2010). Quantum algorithms for algebraic problems. *Reviews of Modern Physics*, *82*(1), 1.

[37] Bernstein, D. J., Heninger, N., Lou, P., & Valenta, L. (2017, June). Post-quantum RSA. In *International Workshop on Post-Quantum Cryptography* (pp. 311-329). Springer, Cham.

[38] Kumar M., Shenbagaraman V.M., Shaw R.N., Ghosh A. (2021) Predictive Data Analysis for Energy Management of a Smart Factory Leading to Sustainability. In: Favorskaya M., Mekhilef S., Pandey R., Singh N. (eds) Innovations in Electrical and Electronic Engineering. Lecture Notes in Electrical Engineering, vol 661. Springer, Singapore. https://doi.org/10.1007/978-981-15-4692-1_58