Quantum Computing and Post Quantum Cryptography

Manish Kumar[1]

[1]*Department of Information Technology, Delhi Technological University Delhi, India*

Email: mk13403@gmail.com

Abstract

The present knowledge we had in quantum computer and the most possible architecture of a quantum computer might be able to break RSA 2048 in future. In classical computer two bits represents any one of four bit information whereas in quantum due to superposition it can be represent all four states. For ‘n’ qubits system is analogous to 2n classical bits. Quantum teleportation, quantum entanglement and other makes it possible to break present cryptosystem. Shor’s Algorithm is used for integer factorization which is polynomial time for quantum computer. This can be threat for RSA security. In this paper matlab implementation of Shor’s algorithm is presented. Used classical way for getting period of function because classical computers not engage quantum phenomena. As numbers of iterations grow, probability of getting exact factor of ‘n’ acutely increased. This paper also discusses popular methods for making qubits like Silicon based Qubits in which electron is put inside nano material which is used as a transistor. In Superconducting circuit method insulator is used as a sandwich in between two metal layers. Used by Google, IBM, Intel, Microsoft. In Flux qubits method very small size loop of superconducting metal is used. This paper also discusses Quantum Proof Algorithm like Lattice-based cryptography used concept of good and bad base. In Learning with errors method if we have more equation then variable, it is over defined system. In Code based cryptography some matrixes allow for efficient error correction (good matrix) but most matrix’s does not (bad matrix) concept is used. In Hash based signatures scheme have long signatures or keys, but they are secure. Also discuss Multivariate Quantum proof algorithm. The abstract should contain maximum of 300 words. No abbreviation should be mentioned in the abstract. Give a brief summary of your research work.

Keywords: *qubit, quantum computer, cryptography, Shor’s algorithm, quantum proof algorithms*

1. Introduction

We have always in mind that is quantum computer is a replacement of classical computer in present scenario. Quantum computer is only faster in a special type of calculation. It done computation in parallel. It will not affect activity like browsing internet, writing documents, watching HD videos. Searching a particular detail of a number in a telephone directory, like find the person which number belongs to him. If the entry in the telephone dictionary is one million then in quantum computer required square root steps. In classical computer two bit can represent any one of four 00, 01, 10, 11. Four numbers but anyone can use i.e. two bits information. But in quantum mechanics it is possible to make superposition of each one of these four states. To find out state of two spin system four coefficients or numbers required, but in classical for two bits only two numbers. Two qubits hold four bits of information. For three qubits systems having eight different states. For ‘n’ qubits system is analogous to 2^n classical bits. Qubits exits any of the combination of states, but when we measured, it fall any one of the basis states. We cannot compute superposition; only compute basis states (up or down). The present knowledge we had, the most possible architecture of a quantum computer might be able to break RSA 2048 bits required about 20 million physical qubits. Because we need error correction, we can't do it with 50 or 100 qubits, because we lacking the ability to correct the error. We can do it with few thousand perfect qubits of zero error, but we never do it, because we always have errors. But tomorrow anyone can come with better quantum algorithm or better quantum error correction code. Then it possible with less number of qubits required to break RSA 2048. Both qubits and gates must be error free. But as on today, there is no perfect qubits. Number of qubits required to break RSA 2048. Quantum teleportation, quantum entanglement and other makes it possible to break present cryptosystem.

1.1 Quantum teleportation

If someone wants to send quantum information to other person. He cannot send quantum states as he cannot do copy of the quantum states. He can use entangled qubit and classical bits for transfer the stat that is called quantum teleportation. First party do some operation on his qubits and send to second party, after receiving results, second party do some operations on it. This way information is transported. Two particles (photons) which are entangled are shared in two different locations irrespective of distance between them, information can be teleported. This involves only transportation of quantum states not physical states. In today world teleportation upto 44 kilometres long with more than 90% accuracy is done in fiber optic network and 1200 km using satellite arrays.

1.2 Quantum entanglement

It is a quantum mechanical phenomenon where two or more object's quantum states relate to each other irrespective of distance between them. If we have two entangled particles (photons, electrons, molecules etc.) then if one is detect in one direction then other particle must be detect in opposite direction. If entangled particles have total spin zero, then if one particle's spin is in clockwise then other particle spin must be in anti-clockwise. Entangled photons are used in quantum holography also. At present a photon entangled with an ion is send 50 km long in optical fiber.

1.3 Quantum superposition

Separate unrelated quantum states exist in same time of a quantum system. It's a union of definite quantum states. Qubits may be in a superposition of both basis sates of |0> and |1>. 'n' qubits may be in a superposition of 2n states. At quantum level particles act like waves. Just like various waves overlap each other, quantum particles also do overlapping to form a unique wave.

2. Current Industry methods for making Qubits [12,13,14]

2.1 Silicon based Qubits

In this electron put inside Nano material is used as a transistor. By doping pure silicon with Group V elements such as phosphorus, extra valence electrons are added that become unbounded from individual atoms and allow the compound to be an electrically conductive. Using silicon-based CMOS (complementary metal-oxide-semiconductor) technology for making Quantum Qubits. Using silicon and phosphorus atom for making qubits. In silicon qubits it provides less noisy environment. More than 95% of Silicon that is available naturally have nuclear spin-0. Phosphorus impurities use as a doner. Crystalline silicon and with phosphorus atoms can be used, spin qubits can read by nuclear magnetic resonance techniques. Drain 'D' and source 'S' is made of modified silicon having impurities, Fig-3. When concentration is high more electrons are present. Highly metallic silicon electrode is used. When we apply voltage electrons accumulate at insulator surface which is in between two metallic silicon. Size can reduce to very small in nanometre that just hold few electrons.

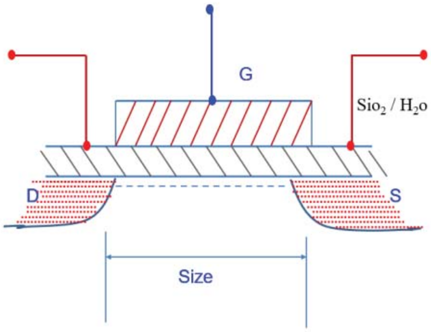


FIG 1. Drain and Source in silicon CMOS

2.2 Superconducting circuit

Superconducting circuit is used by Google, IBM, Intel, Microsoft. This is most advanced technology. Insulator is used as a sandwich in between two metal layers. It is called Josephson junction. This uses as a controller of energy level. As temperature decreased, electrical resistivity decreases in metallic conductors. At below critical temperature resistance of superconductor become zero. In a loop of superconducting wire, an electric current flow with no power source.

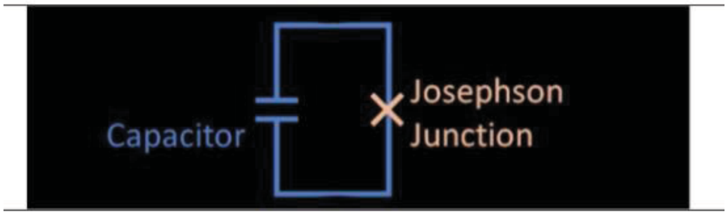


FIG 2. Capacitor with Josephson junction.

2.3 Flux qubits

Flux qubits is used by D wave company. In this code 0 and 1 is given as, current flow clockwise or anticlockwise direction. Current flowing in superposition of clockwise and anticlockwise. It's a very small size (micro meter) loop of superconducting metal. Operations are done by using microwave radiation on qubits and that energy is corresponding to the gap of the two basis states. Appropriately selected frequencies set qubit into quantum superposition. Flux qubit state is measured by superconducting quantum interference device (SQUID).

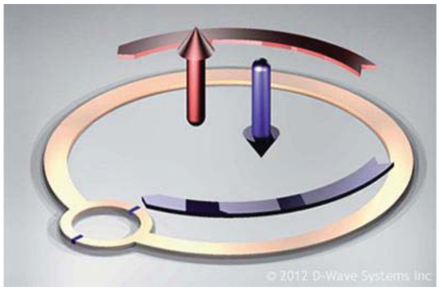


FIG 3. Superconducting Qubit

3. Shor's Algorithm [18,19]

With quantum mechanics it is possible for factorization of large number into its prime factors in polynomial time (O(log N)) using Peter Shor's factorization algorithm, previously it takes exponential time (O(log N)^{k}) in classical methods. This is big threat for data security. It consists of both classical part as well as quantum part. In classical part we convert the problem of factoring into finding the period problem, and for finding the period we use quantum Fourier transform which is in quantum part.

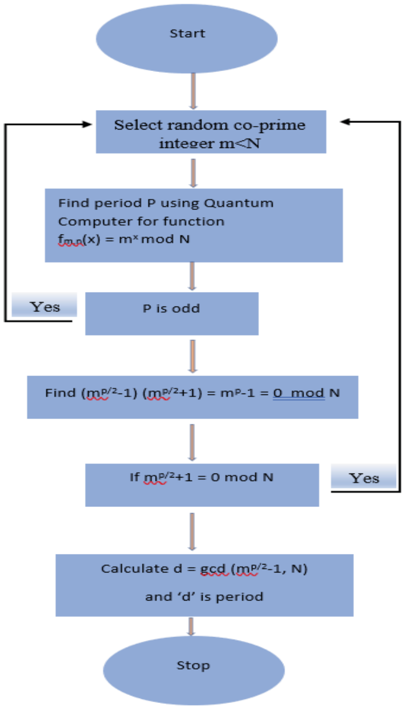

Start
Select random co-prime integer m<N
Find period P using Quantum Computer for function $f_{m,n}(x) = m^{x}$ mod N
Yes
P is odd
Find $(m^{p/2}-1)$ $(m^{p/2}+1) = m^{p}-1 = 0$ mod N
If $m^{p/2}+1 = 0$ mod N
Yes
Calculate d = gcd $(m^{p/2}-1, N)$
and 'd' is period
Stop

FIG 4. Flow chart of algorithm

Quantum part of Shor's algo. (Order finding)

Select a power of 2,

$Q = 2^{L}$ such that $N^{2} < Q < 2N^{2}$

'f' restricted to {0,1,2,…,Q-1}

Where $f(y) \ = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1} |f(x) > \omega^{xy}$

Initial state of Register1(R_1) and Register2(R_2)

$|\psi_0> \ = \ |R_1> |R_2> \ = \ |0> |1>$

$$|\psi_0 > \ = |0 > \ |1 > \ \xrightarrow{f \otimes I} |\psi_1 > \ = \ \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1} |x > \ |1 >$$

Applying Fourier transform to R_1

Applying unitary transformation Uf to R2

$$|\psi_1 > \ = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1} |x > \ |1 > \ \xrightarrow{Uf} |\psi_2 > \ = \ \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1} |x > |f(x) >$$

Applying Fourier transform to R_1

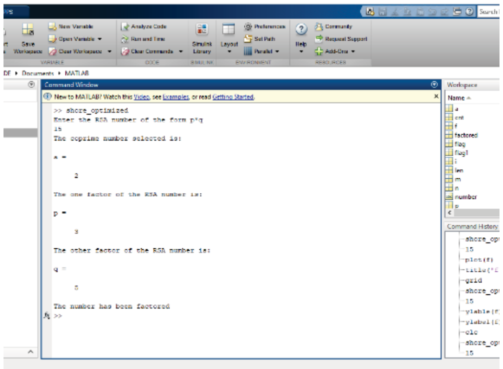
$$|\psi_2 > \ = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1} |x > \ |f(x) > \quad \xrightarrow{f \otimes I} \ |\psi_3 > \ = \frac{1}{Q}\sum_{x=0}^{Q-1} \sum_{y=0}^{Q-1} \omega^{xy} \, |y > |f(x) >$$

For 'y' we measure register 1 and using continued fractions for y/2L we get period P.

4. Results

Example for number 323 and 15

```
Enter the RSA number of the form p*q
323
The coprime number selected is:
a = 16
The one factor of the RSA number is:
P = 19
The other factor of the RSA number is:
q = 17
the number has been factored
```



```
>> shore_optimized
Enter the RSA number of the form p*q
15
The coprime number selected is:

a =

     2

The one factor of the RSA number is:

p =

     3

The other factor of the RSA number is:

q =

     5

The number has been factored
>>
```

FIG 5. Output for n=15

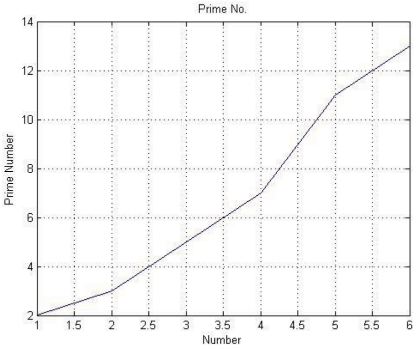


FIG 6. Prime number plot n=15

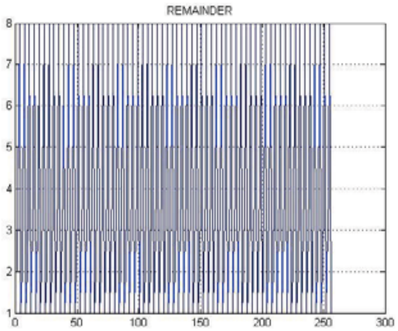
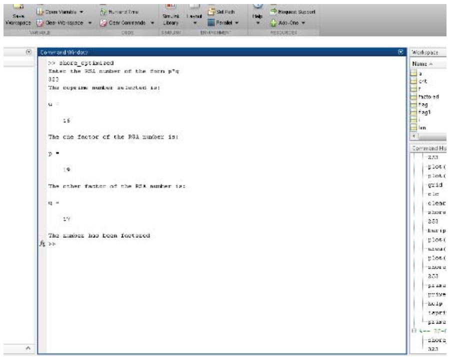


FIG 7. Remainder plot for n= 15



```
>> shore_optimized
Enter the RSA number of the form p*q
323
The coprime number selected is:

a =

    16

The one factor of the RSA number is:

p =

    19

The other factor of the RSA number is:

q =

    17

The number has been factored
>>
```

FIG 8. Output for n=323

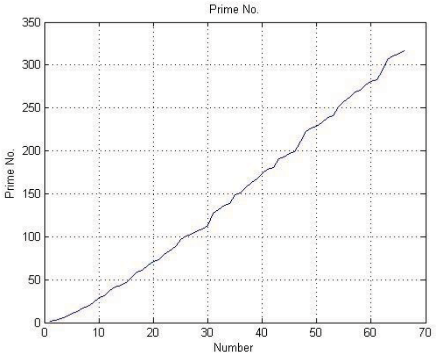


FIG 9. Prime number plot n=323

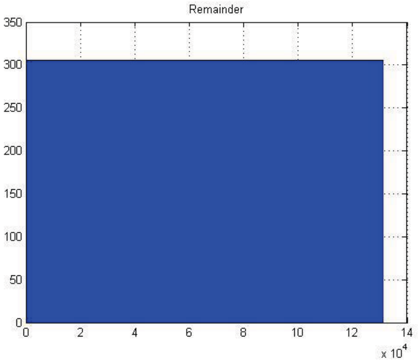


FIG 10. Remainder plot for n= 323

5. Quantum Proof Algorithm[10,11]

These families of crypto algorithm are considered quantum proof algorithms.

1. Lattice based
2. Code based
3. Hash based
4. Multi variate

5.1 Lattice-based cryptography

Lattice is set of intersection point in the space and these points are defined by parallel and equidistance lines going in two-dimensional space. Each intersection point is called lattice. Lattice field is defined by two vectors, called base vectors. Different bases can be used to define same lattice field.

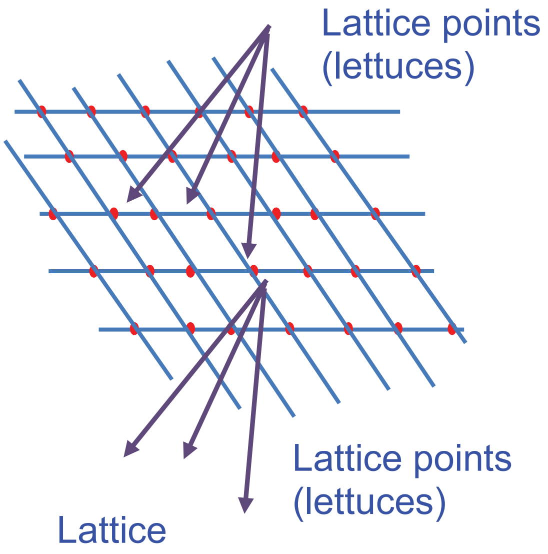


FIG 11. Lattice and Lattice points

Good base is almost orthogonal. Bad base is almost parallel. Good and bad base can be defined in same lattice field.

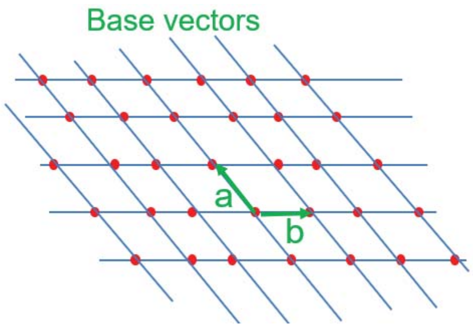


FIG 12. Good base vector

"Good" base
(almost orthogonal)

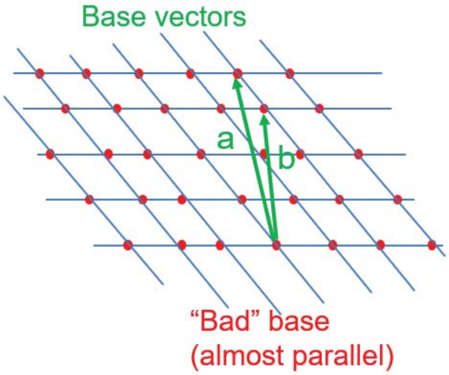


FIG 13. Bad base vector

Which lattice is closest from a given point in two-dimensional space, it is easy to get, but if the lattice field has 250 dimensions? It is extremely difficult to find closest lattice. Answer is easy if we have good base but it is difficult to answer if we have bad base. This is the concept behind lattice-based cryptosystem.

5.2 Goldreich- Goldwasser-Helevi Encryption (GGH)

Alice private key is a good base in a lattice field. Alice public key has bad base define in same lattice field. Encoding the message is not difficult but decoding is extremely difficult. Alice can decrypt because she knows good base, attacker cannot decrypt because he knows only bad base. this way (GGH) works, it is a quantum proof.

5.3 Learning with errors LWP method

We have system of equation; It can be solved by Gauss elimination method or by modular arithmetic. If we have more equation then variable, It is Over defined system. we are talking over defined system where a solution exists.

Table 1: System of equations

system of linear equations
294.x + 629.y + 321z = 38
701.x + 29.y + 91z = 462
613.x + 339.y + 201z = 636

Table 2: System of equations

system of linear equations	Modulo arithmetic
294.x + 629.y + 321.z = 38	(mod 797)
701.x + 29.y + 91.z = 462	(mod 797)
613.x + 339.y + 201.z = 636	(mod 797)

Table 3: System of linear equations

system of linear equations	Modulo arithmetic
294.x + 629.y + 321.z = 38	(mod 797)
701.x + 29.y + 91.z = 462	(mod 797)
613.x + 339.y + 201.z = 636	(mod 797)
256.x + 94.y + 115.z = 522	(mod 797)
704.x + 629.y + 322.z = 477	(mod 797)
391.x + 23.y + 743.z = 213	(mod 797)
290.x + 620.y + 201.z = 40	(mod 797)
211.x + 339.y + 381.z = 510	(mod 797)

In this Alice's private key is solution of the equation. In right side of the equation we add errors like + 1 - 2 - 1 + 2 adding very small errors and hide this error. We can find errors without knowing X, Y and Z but is a very laborious work. This leads to a trapdoor function, it is easy to compute in one direction but difficult in other direction, this is called learning with errors trapdoor function. Adding Errors is easy but finding error is difficult unless we know X Y and Z (variables value). This is known as Regev encryption.

Table 4: Adding errors in equations

Adding errors in equations	
$294.x + 629.y + 321.z = 38 + 1$	(mod 797)
$701.x + 29.y + 91.z = 462 - 2$	(mod 797)
$613.x + 339.y + 201.z = 636$	(mod 797)
$256.x + 94.y + 115.z = 522 + 1$	(mod 797)
$704.x + 629.y + 322.z = 477$	(mod 797)
$391.x + 23.y + 743.z = 213 - 1$	(mod 797)
$290.x + 620.y + 201.z = 40 + 2$	(mod 797)
$211.x + 339.y + 381.z = 510 + 1$	(mod 797)

And have public key is equation system itself with incorrect solutions, added small errors on the right side.

New added equation can be used to encrypt one bit.

For Encrypt '0'

Add small errors to the result of equations.

For Encrypt '1'

Add big number (big error) to the result of equations. This way one bit is encoded. If Bob encrypt something, he selects some equations and left other equations. This is a random process, generally half of the equations are left, and then add all the equations we have. Alice known value of variable X, Y and Z. She can easily check whether there is a small or big error. A small error means 0 and big error is means it is 1.

Table 5: Added errors in equations

Added errors in equations	
$294.x + 629.y + 321.z = 39$	(mod 797)
$613.x + 339.y + 201.z = 636$	(mod 797)
$290.x + 620.y + 201.z = 42$	(mod 797)
$\mathbf{400.x + 791.y + 723.z = 717}$	**(mod 797)**

For attacker it's very difficult to decrypt because he needs to invert learning with errors trapdoor function. It's a quantum proof algorithm but only encrypt one bit at a time. They are more efficient variant of learning with errors.

5.4 Code based cryptography

Its start with error correcting codes. Parity bit (an error detecting code). Three-times code (its error connecting code but not very efficient). We need better error correcting code. For this linear error correcting codes are better alternative.

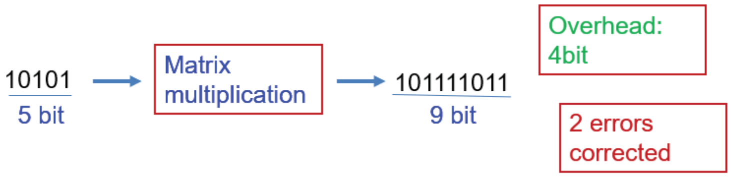


FIG 14. Code based cryptography

In general, overhead of 'n' bits, 'n/2' errors corrected. For error correction a error correction algorithm is used.

For multiplication different matrixes can be used. Some matrix's allow for efficient error correction (good matrix) but most matrix's does not (bad matrix). A good matrix can be changed into a bad metric if multiply by blend Matrix. This can be used for encryption and in this length of public key equal to 1 Mb, but in RSA public key 2 kb, but it is quantum proof.

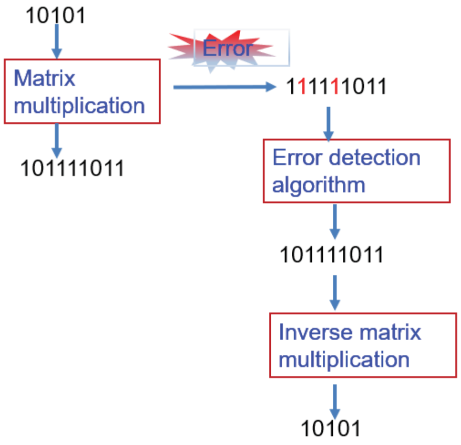


FIG 15. Code based cryptography

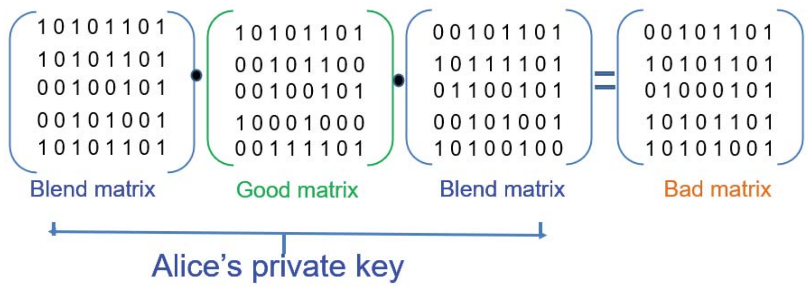


FIG 16. Encryption and Decryption

5.5 Hash methods[10,11]

Hash based signatures scheme have long signatures or keys, but they are probably secure. One of the schemes is Lamport Signature [15]. We use RSA, digital signature algorithm for sign messages. But after quantum computers these scheme are not safe. One method that is quantum robust is Lamport signature given by Leslie B. Lamport. In this

- We make two sets A and B of 256 random 256-bit numbers. The private key value is 512.
- Taking hash of every numbers. The public key is 512 hashes.
- Using SHA-256 we hash the message. For 0 we take from set A, for 1 we take set B for ith number.
- Then 256 random numbers is the signature. And public key is 512 hashes.

Lamport method is use single time for signing. Using hash tree we can do multiple time signing.

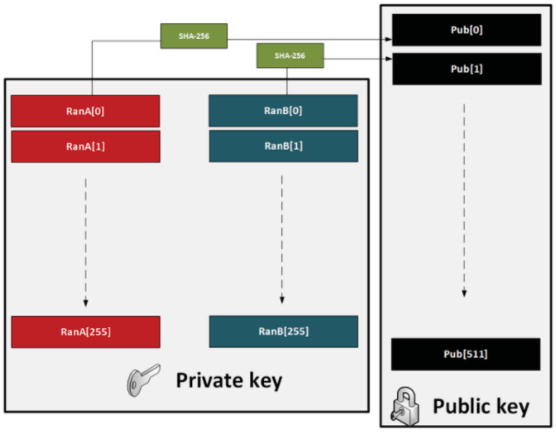


FIG 17. Encryption & Decryption in Lamport

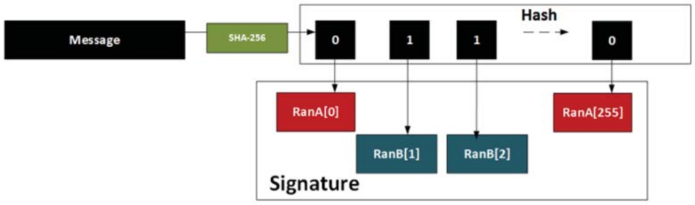


FIG 18. Encryption & Decryption in Lamport

5.6 Multivariate algorithm[10,11]

In multivariate public key cryptosystem, public key are set of multivariate polynomials. Complexity to solve system of multivariate equations is idea behind this. It’s used for signatures. One of the schemes is unbalanced oil-and-vinegar scheme. Unbalanced oil and vinegar scheme is used for digital signature. Its security based on NP-hard problem. Finding solution of ‘m’ equations with ’n’ variables is NP-hard problem. If m is larger or smaller than n, its easy comparable when both m and n are equal.

To make an effective signature, solution of these equations required.

$$y1 = f1\ (x1\ ,\ldots,\ xn)$$

$$y2 = f2\ (x1\ ,\ldots,\ xn)$$

$$\vdots$$

$$ym = fm\ (x1\ ,\ldots,\ xn)$$

here y = (y1, y2,…, ym) is message that is signed.

The effective signature is x = (x1, x2 ,…, xn).

First message is change to suited in equation system. Each single equation has form

$$yi = \sum \gamma ijk\ aj\ a'k + \sum \lambda ijk\ a'j\ a'k + \sum \xi ij\ aj + \sum \xi'ij\ a'j + \delta i$$

each coefficients γijk, λijk, ξij, δi taken in secret.

Vinegar variable a'j is selected randomly.

Solution of derive linear system of equation give us ai.

Signature validation is done by public key

$$y1 = f^*1\ (x1\ ,\ldots,\ xn)$$

$$y2 = f^*2\ (x1\ ,\ldots,\ xn)$$

.

.

.

ym = f*m (x1 ,…, xn).

Attacker not access to the coefficients, oil and vinegar variables. Each equation has to solve for signature verification.

6. Conclusion

Quantum computing is a fascinate area of research. An overview of quantum phenomena and quantum computer is here. Quantum computer is not a replacement of classical computer. It will not affect activity like browsing internet, writing documents, watching HD videos. In Quantum computer number of operations required to arrive at result is exponentially small. Improvement is not in speed of individual operation, it is the total number of operations is needed for arrival at result. It's only useful in arrival of results only in some particular type of cases. Implemented Shor's algorithm in matlab is done. We used classical methods for getting few results because classical computers not engage quantum phenomena. Modification also done to put in Fast Fourier Transform for getting period of function. As number of iterations grow, probability of getting exact factor of 'n' acutely increased. Getting non trivial factor of 'n' and random variable selected both are not correlated to each other. Many new ideas and innovation are arriving daily; many modifications of Shor's original algorithm are present that required less run on quantum computer. Quantum computer with number of qubits increasing daily, we have 72 qubits quantum computer today but in near future it cross thousands of qubits and possible to factor large composite numbers or break RSA 2048. For safeguard from quantum computer effect we have many quantum safe algorithms. In future we will see these quantum proof algorithms are widely used in every field, where security is concern.

REFERENCES

[1] Mavroeidis, Vasileios, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang. "The impact of quantum computing on present cryptography." *arXiv preprint arXiv:1804.00200* (2018).

[2] Curcic, Tatjana, Mark E. Filipkowski, Almadena Chtchelkanova, Philip A. D'Ambrosio, Stuart A. Wolf, Michael Foster, and Douglas Cochran. "Quantum networks: from quantum cryptography to quantum architecture." *ACM SIGCOMM Computer Communication Review* 34, no. 5 (2004): 3-8.

[3] Chen, Lily, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. *Report on post-quantum cryptography*. Vol. 12. US Department of Commerce, National Institute of Standards and Technology, 2016.

[4] Mavroeidis, Vasileios, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang. "The impact of quantum computing on present cryptography." *arXiv preprint arXiv:1804.00200* (2018).

[5] Chuang, Isaac L., and Yoshihisa Yamamoto. "Simple quantum computer." *Physical Review A* 52, no. 5 (1995): 3489.

[6] Barenco, Adriano. "Quantum physics and computers." *Contemporary Physics* 37, no. 5 (1996): 375-389.

[7] McClean, Jarrod, Nicholas Rubin, Kevin Sung, Ian David Kivlichan, Xavier Bonet-Monroig, Yudong Cao, Chengyu Dai et al. "OpenFermion: the electronic structure package for quantum computers." *Quantum Science and Technology* (2020).

[8] Gheorghiu, Alexandru, Theodoros Kapourniotis, and Elham Kashefi. "Verification of quantum computation: An overview of existing approaches." *Theory of computing systems* 63, no. 4 (2019): 715-808.

[9] Gidney, Craig, and Martin Ekerå. "How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits." *arXiv preprint arXiv:1905.09749* (2019).

[10] Chen, Lily, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. *Report on post-quantum cryptography*. Vol. 12. US Department of Commerce, National Institute of Standards and Technology, 2016.

[11] https://spectrum.ieee.org/tech-talk/telecom/security/how-the-us-is-preparing-for-quantum-computings-threat-to-end-secrecy

[12] McClean, Jarrod, Nicholas Rubin, Kevin Sung, Ian David Kivlichan, Xavier Bonet-Monroig, Yudong Cao, Chengyu Dai et al. "OpenFermion: the electronic structure package for quantum computers." *Quantum Science and Technology* (2020).

[13] Duan, Lu-Ming, and Guang-Can Guo. "Reducing decoherence in quantum-computer memory with all quantum bits coupling to the same environment." *Physical Review A* 57, no. 2 (1998): 737.

[14] Duan, Lu-Ming, and Guang-Can Guo. "Preserving coherence in quantum computation by pairing quantum bits." *Physical Review Letters* 79, no. 10 (1997): 1953.

[15] Lamport, Leslie. *Constructing digital signatures from a one-way function*. Vol. 238. Technical Report CSL-98, SRI International, 1979.

[16] J. O'Gorman and E. T. Campbell, "Quantum computation with realistic magic-state factories," Physical Review A 95, 032338(1–19) (2017)

[17] V. Gheorghiu and M. Mosca, "Quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes," arXiv preprint arXiv:1902.02332 (2019).

[18] Shor, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." In *Proceedings 35th annual symposium on foundations of computer science*, pp. 124-134. Ieee, 1994.

[19] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." *SIAM review* 41, no. 2 (1999): 303-332.