A New Approach towards Quantum Resistant Cryptography

Ravikar Srivastava
National Informatics Centre, New Delhi

----------ABSTRACT----------

Quantum computing is another developing innovation which is going to impact whole computing process and especially cryptography. Most of the cryptosystems will fail when quantum computing becomes a reality. In such situation cryptography through lattice and mersenne primes is a ray of hope. In this paper, we investigate the impact of quantum computing on cryptography and possible solution to provide a secure system.

KEYWORDS**: Cryptography, Quantum Computing, Lattice, Mersenne Primes**

1. INTRODUCTION

Dependence on computers and its wide application in the cutting edge world have constrained the specialists to enhance and produce a small, fast and a robust computer. This target can be realized by Nanotechnology [1-3]. Nanotechnology can plan and fabricate electronic segments that can be utilized to make it a reality. Nanotechnology is an extensively characterized term that is not limited to a single discipline but the shared factor is very high in all areas including medical or engineering. There are new hopes in terms of response type and response time. With the help of devices of nanometer size there is a scope of radically new form of technology [4-5]. As a result of the extent of the gadgets included a great part of the work included with nanotechnology requires working at the nuclear level, changing and controlling atoms and molecules. Due to the enabled technology at this level there is a big scope of practical implementation of quantum computers. It has turned into a hotspot for high contention. It will be a big mistake, if we ignore the impact of quantum computing on cryptography. New methods (using other platforms) [6] needs to be developed on regular basis in order to avoid potential threat of quantum computing [7-8]. The development of new protocols will also give an added benefit that they can be useful in variety of situations like Electronic Health Records (EHR) systems, wireless communication or various defense related applications [9-12]

2. PRELIMINARIES

2.1Quantum computing:

There is a difference in computation process between quantum computers and binary digital computer. Digital computer uses data in the form of binary digits (0&1) while quantum computers [13] uses quantum bits which can be superposition of various states. A quantum computer with m qubits can be in any random superposition of up to 2^m different states simultaneously**.** We will explain it through a simple example. Suppose we have 3 bits then it can represent various 8 unique combinations in binary as given in figure 1 where every position can have only 0 or 1. But if 0 and 1 also have 2 states each then various combinations will increase to 64 i.e. 8 times.

Decimal number	0	1	2	3	4	5	6	7
Binary number	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**

Fig 1: **Possible combination of 0 and 1 for 3 bits.**

Thus we can say there will be huge increase in speed of computation and it will affect whole technology.

2.2Cryptography:

Modern cryptography is not limited to encryption and decryption only while it is associated with the process of developing a cryptosystem which can provide information security by using various mathematical techniques, methods and algorithms. Some of the security services [14-17] are as given follows (shown in figure 2 below).

- **Confidentiality**: It is a process to prevent the information from an unauthorized person. It can be enabled by using various algorithms for encrypting the data.
- **Data integrity**: Integrity service refers to protect the data alteration. It assures that whether data is exactly same or not since it was last communicated or stored by an authorized entity. This service does not stop data alteration while it can identify it.
- **Authentication**: This service verifies that the data received is from an authorized resource and it has two parts. First part is message authentication. It identifies the source of the message. Second is Entity authentication. It provides assurance that received data is from a particular specified entity.
- **Non-repudiation:** This service assures that in future sender will not be able to deny for his action.
- **Access control:** It is the service to prevent unauthorized use of a resource.

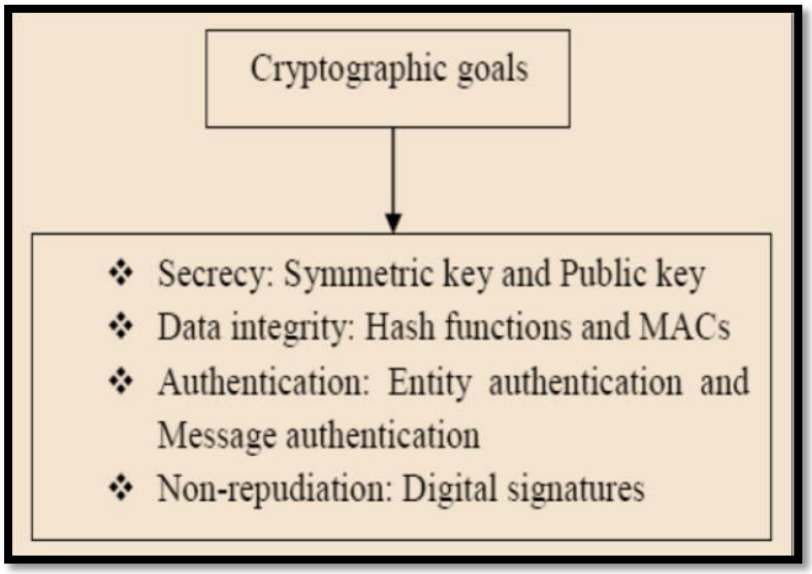

Fig.2: **Denoting security objectives with corresponding applications.**

Modern day cryptography is moving towards batch cryptography which is performing batch decryption, batch key agreement and batch verification. In batch cryptography decryption, key agreement and verification is done in a batch of various tasks (not one by one). Here we are going to show an example of aggregate signature [18] and batch verification. Suppose there are t signatures given for t different messages, which are given by t different users. In batch processing, these signatures $s_1, s_2, s_3, \ldots \ldots s_t$ can be combined into a common signature which is used to verify that all the t users signed the original messages in a batch where k^{th} user has signed the message m_k for $k = 1,2, \ldots . . t$. Signatures are generated as follows

$$s_1 + s_2 \rightarrow s_{12}$$
$$s_{12} + s_3 \rightarrow s_{123}$$
$$s_{123} + s_4 \rightarrow s_{1234}$$
$$s_{1234} + s_5 \rightarrow s_{12345}$$
$$s_{1234\ldots n-1} + s_n \rightarrow s_{12345\ldots n}$$

First batch verification [19] came in 1994 for DSA signature after that various improvements came in successive years. Now day's cloud computing is available easily and cost of infrastructure is decreasing for an individual. All trusted third party can use cloud so use of batch processing will enhance in near future and all computing may transfer to a common platform .In such situation there will be a requirement of new techniques and algorithms to shift whole cryptographic system to a new dimension.

3. IMPACT OF QUANTUM COMPUTING ON CRYPTOGRAPHY

Quantum computing will result to the end of almost all the cryptographic schemes based on number theoretic or discrete logarithm problem because factoring will become an easy problem. Currently available quantum computers are not capable to perform factoring large numbers or solving discrete log problem in an efficient way. But in the presence of useful quantum computers which can involve more than a million bits, (qubits) all cryptographic algorithms which are in use today will become of no use. Quantum bit innovation is a barrier for the realization of quantum computers. The fundamental requirement is the generation of quantum bits (qubit). While current processing works by exchanging between two states, quantum bit enables multiple states to exist simultaneously. In view of this a quantum PC would have the capacity to do in days what a conventional PC may take a huge number of years to perform. It will be a big challenge for the security. Most of the cryptographic schemes will become vulnerable to attacks. It will be of great concern not only to secure data but also the physical security of the devices. Any cryptosystem consists of four components encryption/decryption, digital signature, authentication and key agreement. All will be affected by the evolution of quantum computers. Currently used standards for encryption whether DES, Triple DES and AES are considered as secure, with AES being the current government standard providing 128-bit, 192-bit, and 256-bit key sizes [20]. On one side Nanotechnology provides a way to improve on these encryption standards but on another side, it is also a threat for them to remain secure. Quantum cryptography can provide an encryption system which will be impossible to decode. This encryption process uses the nature of photons. Photons are encoded in one of four positions, one horizontal, one vertical and two diagonal. If anyone tries to intercept, the transmission will not only tip off but the intrusion attempt but will also invalidate the code. Security of any encryption system is heavily dependent on keys and if the key is hacked then the data is hacked as well. In case of Quantum encryption, keys can be altered several times, which makes them almost infeasible to compromise.

Authentication is also a very important part in the security of a network and will also be affected with the advent of quantum cryptography. On one side accuracy associated with authentication schemes will increase while on another side it will make existing schemes vulnerable to attack.

4. HOW TO OVERCOME CHALLENGES FACED BY CRYPTOGRAPHY VIA QUANTUM COMPUTING

Traditional cryptographic algorithms [21-22] are based on factorization or elliptic curves which are not looking resistant against quantum algorithms. Possible solutions can be cryptography through lattices and mersenne prime numbers.

4.1Lattice Cryptography.

In 1996, Ajtai discovered [23] that there are mathematical problems in the area of lattices that have some desirable properties with respect to cryptography. Since then, lattices have been used to construct several crypto systems and other cryptographic applications [24-28]. Lattice-based cryptography is the generic term for asymmetric cryptographic primitives based on lattices. To develop a cryptosystem first requirement is to search a hard problem. Any problem is said to be computationally hard if no algorithm can solve it efficiently. For a lattice of n dimension there are two hard problems: Shortest Vector Problem (SVP) and Closest Vector Problem (CVP). In case of SVP, problem is to find shortest vector in lattice L. It looks easy in case of 2 or 3 dimensions but it is a hard problem if this dimension is increases up to 500 or more. In case of CVP one vector t is given which is not in L. Hard problem is to find a vector which is closest to t. Another variation of this hard problem is to find approximate closest vector. Most of the functions based on lattices is quadratic or linear, which is a attractive feature for the construction of a cryptosystem and a revolutionary advantage over number theoretic algorithms in cryptography [29]. Some of the available cryptosystems [30-34] and its practical implementations include NTRU Encryption, NTRU key exchange and NTRU authentication. Lattice cryptographic systems are fully homomorphic [35], very much resistive against key leakage and efficient also. These features [36-38] making it quantum resistant.

4.2 Cryptography through mersenne prime:

It is a latest area of work in which cryptosystem is based on mersenne prime numbers [39]. Till date only fifty mersenne primes are known. $2^{77232917}-1$ is the largest mersenne prime till date. Mersenne prime numbers are of the form $q=2^n-1$ where n is a prime. These numbers have a very unique property that for any number $y\ modulo\ q$ and $t=2^z$ where t is a positive integer, $y\times t$ is a cyclic shift of y by z positions and thus the number of $1's$ remain unchanged in y. In other words we can say that hamming weight of y remains unaffected. The process of encryption is as follows: Let us take an expression $R=S/T(mod\ q)$ where S and $T(mod\ q)$ are having low hamming weight and it is very difficult to distinguish R from a random integer modulo q. In order to encrypt a bit $x=\{0,1\}$, the encryption algorithm choses two random numbers n_1, n_2 of low hamming weight and then the output $C=(-1)^x(n_1R+n_2)$ where R is the public key and T is the private key.

5. CONCLUSION

Cryptographic systems enhance security features and guarantees efficient and powerful message security mechanism. Today's Cryptographic systems are under way and can only be seen as an amendment to traditional procedures. In the future when quantum computing will take place in reality, we have to rely on new cryptosystems which are resistant against quantum computers. In future, lattice cryptography and cryptography using mersenne prime can play vital role in the area of security.

REFERENCES

1. J.R. Heath, P.J. Kuekes, G.S. Snider, R.S. Williams, A defect-tolerant computer architecture: opportunities for nanotechnology, Science, volume 280, number 5370, 1998, 1716-1721, DOI: 10.1126/science.280.5370.1716
2. S. Lokhande, R. Pate, Role of nanotechnology in shaping the future of mobile and wireless devices, International journal of science and research, volume 3, issue 1, 2014, 212-215, available at https://www.ijsr.net/get_abstract.php?paper_id=15011403
3. V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6, DOI: 10.1680/jnaen.18.00006
4. G. P. Nair, Nanocore - a review on 5G mobile communications, International journal of computer science and mobile computing, 2013, 124-133, available at https://ijcsmc.com/docs/papers/ICMIC13/ICMIC13S14.pdf
5. Nanomaterials, American elements report, available at https://www.americanelements.com/nanomaterials-nanoparticles-nanotechnology.html
6. V. Shukla, A. Chaturvedi, M.K. Misra, On authentication schemes using polynomials over non commutative rings, Wireless personal communications, volume 118, 2021, 185-193, DOI: https://doi.org/10.1007/s11277-020-08008-4

7. A. Chaturvedi, V. Shukla, M.K. Misra, Three party key sharing protocol using polynomial rings, IEEE international conference on electrical, electronics and computer engineering , 2018, 1-5, DOI: 10.1109/UPCON.2018.85969054.3
8. A. Chaturvedi, V. Shukla, M.K. Misra, A random encoding method for secure data communication: an extension of sequential coding, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1189-1204, DOI:https://doi.org/10.1080/09720529.2021.1932902
9. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451, DOI: 10.1080/09720529.2019.1692450
10. V.Shukla, A.Chaturvedi, N.Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21, DOI: 10.5120/cae2015651903
11. V. Shukla, N. Srivastava, A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical, computer and electronics engineering , 2016, 83-86, DOI: 10.1109/UPCON.2016.7894629
12. A. Chaturvedi, M.K. Misra, S.P. Tripathi, V. Shukla, An authenticated key agreement protocol using artin's braid group, International journal of computer sciences and engineering, volume 5, issue 12, 2017, 233-236, DOI: https://doi.org/10.26438/ijcse/v5i12.233236
13. Z. Ullah, Nanotechnology and its impact on modern computer, Global journal of researches in engineering general engineering, volume 12, issue 4, 2012, 1-6, available at https://globaljournals.org/GJRE_Volume12/6-Nanotechnology-and-Its-Impact-on-Modern-Computer.pdf
14. A. J. Menezes, P. C. V. Oorschot, S. A. Vanstone, Handbook of applied cryptography, 5th edition, CRC Press Inc., USA, ISBN: 9780849385230, 2001
15. W.Stallings, Cryptography and network security, principles and practices, seventh edition, Prentice Hall, ISBN-13:978-0134444284, ISBN-10:0134444280, 2005
16. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed networks, Wireless personal communications, volume 110, 861-872, 2019, DOI: https://doi.org/10.1007/s11277-019-06760-w
17. V. Shukla, M.K. Misra, A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1241-1256, DOI: https://doi.org/10.1080/09720529.2021.1932908
18. D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and verifiably encrypted signatures from bilinear maps**,** International conference on the theory and applications of cryptographic techniques (Part of the lecture notes in computer science book series (LNCS, volume 2656)), 2003, 416-432, DOI: https://doi.org/10.1007/3-540-39200-9_26
19. D. Naccache, D.M. RaÏhi, S. Vaudenay, D. Raphaeli, Can D.S.A. be improved? — complexity trade-offs with the digital signature standard**,** Workshop on the theory and application of cryptographic techniques (Part of the lecture notes in computer science book series (LNCS, volume 950)), 1994, 77-85, DOI: https://doi.org/10.1007/BFb0053426
20. M.B. Nathanson, Elementary methods in number theory, Graduate texts in mathematics, Springer, 2000, eBook ISBN 978-0-387-22738-2, DOI: 10.1007/b98870
21. R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, volume 21, issue 2, 1978 , 120–126, DOI**:** https://doi.org/10.1145/359340.359342
22. M. Bellare, R. Canetti, H. Krawczyk, Keying hash functions for message authentication**,** Annual international cryptology conference (Part of the lecture notes in computer science book series (LNCS, volume 1109)), 1996, 1-15, DOI: https://doi.org/10.1007/3-540-68697-5_1
23. M. Ajtai, Generating hard instances of lattice problems (extended abstract), Proceedings of the twenty-eighth annual ACM symposium on theory of computing, 1996, 99–108, DOI: https://doi.org/10.1145/237814.237838
24. Y. Chen, P.Q. Nguyen, BKZ 2.0: Better lattice security estimates**,** International conference on the theory and application of cryptology and information security (part of the lecture notes in computer science book series (LNCS, volume 7073)), 2011, 1-20,

DOI: https://doi.org/10.1007/978-3-642-25385-01

25. L. Ducas, V. Lyubashevsky, T. Prest, Efficient identity-based encryption over NTRU lattices, IACR cryptology e print archive, 2014, 1-20, DOI: 10.1007/978-3-662-45608-82
26. W. Diffie, M. Hellman, New directions in cryptography, IEEE transactions on information Theory, volume 22, issue 6, 1976, 644-654, DOI: 10.1109/TIT.1976.1055638
27. O. Goldreich, S. Goldwasser, S. Halevi, Public-key cryptosystems from lattice reduction problems**,** Annual international cryptology conference, (Part of the lecture notes in computer science book series (LNCS, volume 1294)), 1997, 112-131, DOI: https://doi.org/10.1007/BFb0052231
28. C. Gentry, C.J. Peikert, V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, Proceedings of the fortieth annual ACM symposium on theory of computing, 2008, 197-206, DOI: https://doi.org/10.1145/1374376.1374407
29. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A secure peer to peer entity authentication scheme using lattice cryptography, volume 10, issue 6, 2018, 1874-1880, available at https://www.jardcs.org/backissues/abstract.php?archiveid=5737
30. J. Hoffstein, N. H. Graham, J. Pipher, J. H. Silverman, W. Whyte, NTRUSign: digital signatures using the NTRU lattice, Cryptographers' track at the RSA conference (part of the lecture notes in computer science book series (LNCS, volume 2612)), 2003, 122-140, DOI: https://doi.org/10.1007/3-540-36563-X_9
31. J. Hoffstein, J. Pipher, J. H. Silverman, NTRU: A ring-based public key cryptosystem, International algorithmic number theory symposium (Part of the lecture notes in computer science book series (LNCS, volume 1423)), 1998, 267-288, DOI: https://doi.org/10.1007/BFb0054868
32. D. Micciancio, C. Peikert, Trapdoors for lattices: simpler, tighter, faster, smaller**,** Annual international conference on the theory and applications of cryptographic techniques, (Part of the lecture notes in computer science book series (LNCS, volume 7237)), 2012, 700-718, DOI: https://doi.org/10.1007/978-3-642-29011-441
33. C. A. Melchor, X. Boyen, J.C. Deneuville, P. Gaborit, Sealing the leak on classical NTRU signatures, International workshop on post-quantum cryptography, 2014, 1-21, DOI: https://doi.org/10.1007/978-3-319-11659-41
34. E. Alkim, N. Bindel, J. Buchmann, Q. Dagdelen, P. Schwabe, TESLA: tightly-secure efficient signatures from standard lattices, Cryptology e print archive: report 2015/755, 2015, 1-24, available at https://eprint.iacr.org/2015/755/20150730:095248
35. C. Gentry, Fully homomorphic encryption using ideal lattices, Proceedings of the forty-first annual ACM symposium on theory of computing, 2009, 169–178, DOI: https://doi.org/10.1145/1536414.1536440
36. P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proceedings 35th annual symposium on foundations of computer science, 1994, 124-124, DOI: 10.1109/SFCS.1994.365700
37. Y. Yuan, C.M. Cheng, S. Kiyomoto, Y. Miyake, T. Takagi, Portable implementation of lattice-based cryptography using javascript, Third international symposium on computing and networking, 2015, 58-67, DOI: 10.1109/CANDAR.2015.36
38. A. Schmidt, Quantum algorithm for solving the discrete logarithm problem in the class group of an imaginary quadratic field and security comparison of current cryptosystems at the beginning of quantum computer age, International conference on emerging trends in information and communication security (Part of the lecture notes in computer science book series (LNCS, volume 3995)), 2006, 481-493, DOI: https://doi.org/10.1007/11766155_34
39. D. Aggarwal, A. Joux, A. Prakash, M. Santha, A new public-key cryptosystem via mersenne numbers, Annual international cryptology conference (Part of the lecture notes in computer science book series (LNCS, volume 10993)), 2018, 459-482, DOI: https://doi.org/10.1007/978-3-319-96878-0_16