National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

The Need For Quantum – Resistant Cyber Security : A Review

Subhashree K, Kavitha S, Sanjay K
M.Sc. Department of Mathematics (M.Sc.), Guru Nanak College, Chennai, Tamil Nadu, India

ABSTRACT

Conventional cyber security, especially public key cryptosystems depend upon the difficulty of solving large integer factorization and discrete log problems. The most straightforward way to solve these problems is to try all possible keys, which would be far too difficult for conventional computers. But the speed in which quantum computing is growing has posed a great threat to the conventional cryptosystems. This paper reviews how conventional public key cryptosystems might crumble under quantum computing and the need for quantum – safe cryptography.

Keywords : RSA, Shor's Algorithm, IFP, DLP, Quantum-resistant cryptography

I. INTRODUCTION

The two types of modern cryptography are symmetric and asymmetric key (Public key) cryptography. Secure Sockets Layer (SSL) and Transport Layer Security (TLS), cryptographic protocols that provide authentication and data encryption between servers, machines and applications operating over a network use combinations of symmetric and asymmetric cryptography. The most popular asymmetric cryptographic schemes used today are

- ✓ Rivest-Shamir-Adleman (RSA)
- ✓ Elliptic Curve Digital Signature Algorithm (ECDSA)
- ✓ Digital Signature Algorithm (DSA)
- ✓ Diffie-Hellman key agreement protocol

The use of these algorithms essentially depends upon the fact that the Integer Factorization Problem (IFP) and Discrete Logarithm Problem (DLP) are very hard to solve. But, the Shor's algorithm, created by Peter Shor, in the year 1994, can break these algorithms, if run on a quantum computer. Even though quantum computers are not commercial yet, they are speculated to be available for extensive use in a decade or so. Thus, security through the above mentioned algorithms, which are still in wide use today, will become obsolete after the advent of quantum computers. So, research is being carried out to create algorithms which are quantum resistant, to replace the conventional asymmetric cryptosystems.

II. INTEGER FACTORIZATION PROBLEM

Since the time of Euclid, it has been known that every positive integer n can be uniquely (up to order) factored into the product of primes.

Integer factorization, especially prime factorization is the problem of finding the prime factors of a given composite number. Factorizing large numbers is a very hard task for classical computers. It is computationally easy (polynomial time) to determine whether or not n is a prime or composite number. But if n is a product of two large prime numbers, then it is extremely hard to compute the factors of such n. This is the concept behind the RSA algorithm, which is the most popular one in use now. Researchers have estimated that a 1024 bit RSA modulus (which is the bit size commonly used now), would take thousands of years to crack using classical computers.

III.DISCRETE LOG PROBLEM

If a is an arbitrary integer relatively prime to n and g is a primitive root of n, then there exists among the numbers 0, 1, 2, ..., Φ(n) - 1 , where Φ(n) is the totient function, exactly one number such that

$$a \equiv g^{\mu} \ (mod\ n)$$

The number μ is then called the discrete logarithm of *a* with respect to the base *g* modulo *n* and is denoted

$$\mu \equiv indga(mod\ n)$$

It is very hard to find μ, given a and g. This concept is at the heart of Diffie-Hellman, Elliptic Curve Cryptography algorithms etc.

IV.SHOR'S ALGORITHM AND THE INTEGER FACTORIZATION PROBLEM

The Shor's algorithm tackles the integer factorization problem through the following steps: For a given integer n

Step 1: Determine if *n* is even, prime or a prime power. If so, we will not use Shor's algorithm as there are many effective classical methods to factorize such numbers.

Step 2: Pick a random integer $x < n$ and calculate *gcd(x,n).* If this is not 1, then we have obtained a factor of *n*.

Step 3: This step is to be performed on a quantum computer. Pick *q* as the smallest power of 2 with $n^2 \leq q < 2n^2$. Find period *r* of $x^a \ mod\ n$. Measurement gives us a variable *c* which has the property $c/q \approx d/r$ where $d \in$N.

Step 4: Determine *d ,r* via continued fraction expansion algorithm. *d,r* only determined if *gcd(d,r)*= 1(reduced fraction).

Step 5: If *r* is odd, go back to *Step 2*. If $x^{r/2} \equiv -1$ mod *n* go back to *Step 2*. Otherwise the factors *p* or *q*= $gcd(x^{r/2 \pm 1},n)$. [15]

The best known algorithms (including probabilistic ones) which deliver a factor of *n*, all require a super-polynomial number of classical steps in *n*. For example, the Schnorr-Seysen- Lenstra probabilistic algorithm factorizes $n<2^a$ in $exp(O((aloga)^{1/2}))$ classical steps. In contrast, Shor's algorithm delivers (with positive probability) a factor of $n < 2^a$ in $O(n^2 lognlog\ logn)$ quantum steps [17].Thus, the Shor's algorithm, with the help quantum computers can break RSA and similar algorithms which rely on the difficulty of factorizing large numbers (1024 bit, 2048 bit etc.)

V. SHOR'S ALGORITHM AND THE DISCRETE LOG PROBLEM

The discrete logarithm problem in Z*p, *p* prime as well as in the group of points of an elliptic curve over a finite field, is considered unbreakable by classical computers. The Shor's algorithm can solve the problem on *n*- bit inputs in $O(n^3)$ time, while the most efficient algorithm for this problem, for classical computers, called Gordon's algorithm will take as long as $exp(O((logp)^{1/3}(log\ logp)^{2/3}))$ where *p* is the prime. [15]

VI. CONCLUSION

The monumental growth of quantum computing during the recent years has brought the need for quantum – resistant cryptography a bit closer. While many symmetric key algorithms are quantum safe, it is the asymmetric algorithms which would face a big blow in the quantum era. There have already been significant advances in research towards post –

quantum cryptography. On January 2019, National Institute of Standards and Technology has published 17 public-key encryption and key-establishment algorithms, which are considered strongest candidates for post-quantum cryptography standardization. They are BIKE, Classic McEliece, CRYSTALS-KYBER, FrodoKEM, HQC, LAC, LEDAcrypt (merger of LEDAkem/LEDApkc), New Hope, NTRU (merger of NTRU Encrypt/NTRU- HRSS-KEM), NTRU Prime, NTS-KEM, ROLLO (merger of LAKE/LOCKER/Ouroboros-R), Round5 (merger of Hila5/Round2), RQC, SABER, SIKE, and Three Bears. A continued analysis on the performance of the above mentioned algorithms will prove to be fruitful to get ready for the post- quantum era.

VII. REFERENCES

[1]. Weedbrook, C., Pirandola, S., Lloyd, S. and Ralph, T.C., 2010. Quantum cryptography approaching the classical limit. Physical review letters, 105(11), p.110501.

[2]. Gajbhiye, S., Karmakar, S., Sharma, M. and Sharma, S., 2017, December. Paradigm shift from classical cryptography to quantum cryptography. In 2017 International Conference on Intelligent Sustainable Systems (ICISS) (pp. 548-555). IEEE.

[3]. Farik, M. and Ali, S., 2016, December. The Need for Quantum-Resistant Cryptography in Classical Computers. In 2016 3rd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE) (pp. 98-105). IEEE.

[4]. Häner, T., Roetteler, M. and Svore, K.M., 2016. Factoring using 2n+ 2 qubits with Toffoli based modular multiplication. arXiv preprint arXiv:1611.07995..

[5]. Buchanan, W. and Woodward, A., 2017. Will quantum computers be the end of public key encryption?. Journal of Cyber Security Technology, 1(1), pp.1-22.

[6]. Amico, M., Saleem, Z.H. and Kumph, M., 2019. Experimental study of Shor's factoring algorithm using the IBM Q Experience. Physical Review A, 100(1), p.012305.

[7]. Coles, P.J., Eidenbenz, S., Pakin, S., Adedoyin, A., Ambrosiano, J., Anisimov, P., Casper, W., Chennupati, G., Coffrin, C., Djidjev, H. and Gunter, D., 2018. Quantum algorithm implementations for beginners. arXiv preprint arXiv:1804.03719.

[8]. Martín-López, E., Laing, A., Lawson, T., Alvarez, R., Zhou, X.Q. and O'brien, J.L., 2012. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. Nature Photonics, 6(11), p.773.

[9]. Chen, L., Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R. and Smith- Tone, D., 2016. Report on post-quantum cryptography. US Department of Commerce, National Institute of Standards and Technology.

[10]. Brands, G., Roellgen, C.B. and Vogel, K.U., 2015. QRKE: Quantum-Resistant Public Key Exchange. arXiv preprint arXiv:1510.07456.

[11]. Ioannou, L.M. and Mosca, M., 2011, November. A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys. In International Workshop on Post-Quantum Cryptography (pp. 255-274). Springer, Berlin, Heidelberg.

[12]. Chen, L., 2017. Cryptography Standards in Quantum Time: New wine in old wineskin?. IEEE security & privacy, 15(4), p.51.

[13]. Mavroeidis, V., Vishi, K., Zych, M.D. and Jøsang, A., 2018. The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200.

[14]. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing,26(5),1484-26. doi:http://dx.doi.org/10.1137/S0097539795293 1 72

[15]. Shor, Peter W. “Polynomial-time algorithms for prime factorization and discretelogarithms on a quantum computer.”SIAM journal on computing26.5 (1997):1484-1509.

[16]. Ekera, M., 2016. Modifying Shor's algorithm to compute short discrete logarithms. IACR Cryptology ePrint Archive, 2016, p.1128.

[17]. Christophe Pittet. Mathematical aspects of Shor’s algorithm. 3rd cycle. Shillong - Inde, 2013, pp.15.

Cite this article as :

Subhashree K, Kavitha S, Sanjay K, "The Need For Quantum - Resistant Cyber Security : A Review", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 09-12, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT19472