International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
International Conference on Technological Emerging Challenges (ICTEC-2019)
Available online at www.ijrat.org

Concert And Enforcement Of A Security Processor For Satellite Communications Using Rlwe-Kex

[1]M.Tulasi , [2]M.Gagan Kumar, [3]K.S.V.L.Prasanna.T
[1]Dept of ECE, Student III ECE , [2]Dept of ECE, Student, II ECE, [3]Asst professor, Dept of ECE, Gandhiji Institute of Science & Technology,Krishna district, Andhra pradesh.

Abstract: In communication systems data security plays a very important role in order to counteract the more and more numerous security threads. Particularly, in satellite communication systems, security is based on cryptographic schemes that must remain indestructible for significant amount of time as in satellite's durable cycle, upgrading and shielding is not an easy process .This process highlights the need for upgrading the post quantum implementations to protect from quantum based attacks .The encryption and decryption implementations are based on key exchange algorithm. The goal of the author is to protect the hardware from quantum attacks, increase the speed to match the requirements of satellite communication and reducing the consuming resources when compared to the similar works.

KEYWORDS: Satellites, quantum attacks, cryptography, RLWE, key exchange algorithm

1. INTRODUCTION:

We know that communication refers to the exchanging or sharing of information between two or more entities through any medium or channel. If this communication takes place between any two earth stations through a satellite then it is called satellite communication. In communication, satellite systems are the main means of communication because of their long distance connection and connections of points with terrestrial means which is extremely difficult. And also they are preferable in cases where sensitive information like information about national security, important deals with other companies where incase of business sector, e.t.c…,

So in wireless communications the data transmission process is becoming very difficult due to the intruder. We are unable to transmit the information in a secure way and also cyber attacks become more advanced .So too must our satellite communication infrastructure, we make a mission to keep our satellite communications safe on our secure way. These networks are preferable for data transmission over a long distances due to the advantages like global availability, reliability & flexibility & also to provide message confidentially.

For this reason, satellites are provided with highly secure cryptography algorithms .and also considering the satellite life expectancy is very long . In this field reprogramming becomes very difficult .Taking this into consideration the installation and implementations should be made very carefully.

In this framework, appreciable research has been invested that recent years in the advancement of computing system based on quantum mechanics. Eventually we acheive a machine which made stunningly fast capabilities for parallel computations will be able to solve many of hard mathematical problems. Here , we are introducing a modern cryptography, which elevate perception and motivation towards post-quantum cryptography algorithms. Now a days cyber attacks on satellite devices are active. It is necessary to improvement of cryptographic algorithm into satellite communication systems that is adaptable to quantum attacks.

To resist in quantum computer's attack, we mostly referred the post-quantum cryptography and this cryptographic researches are based on five different cryptographic schemes.

(1)**Lattice Based Cryptography:**

An example is LWE cryptosystem. It is based on Schorr's algorithm. It is also resistant to quantum based attacks.

(2)**Code Based Cryptography:**

It is based on error correcting codes and in the hardness of decoding a message with random errors .An example is MC Eliece's cryptosystem.

(3)**Hash Based Cryptography:**

It uses hash function to maintain the security based on collision resistance of hash function.

(4)**Multi Varient Cryptography:**

It is used to solving a set of non – linear equations over a finite field.

(5)**Super Singular Elliptic Curve Cryptography:**

It is a Diffie-Hellman type scheme. It is based on the difficulties of finding isogenies between super singular elliptic curves.

But here we are using key exchanging algorithm which is used to share secret between two parties and to protect the hardware from quantum attacks. Example for key exchange algorithm is Diffie-Hellman algorithm .This implementation is proposed on Ring Learning With Errors-Key Exchanging (RLWE-KEX).

The goal of this implementation is to applicable this domain where high security is necessary especially in satellite communication. The main concept is to reduce the effectiveness of mass surveilliance programs.

we've afforded background information on satellite communication security and using ring learning with errors key exchange algorithm. we have discussed about designing of proposed systems. Implementation results are presented and comparisons with other works are made. Finall section gives the conclusion of this paper.

2. BACKGROUND:

a. Satellite Communication:

In this communication electro-magnetic waves are used as carrier signals. These signals carry the information such as voice , audio, video or any other data between group and space and vice versa. It collects various kind of information, like sensor ,image and control data. These are propogated to the satellites computer which turns the data into binary based packets and transmits them to transpoder (converts binary digits to radio signals) which is known as repeater. Repeater is nothing but circuit which increases the strength of receiver signal.

Here we have two types of frequency ,i.e uplink and downlink frequency. The process of satellite communication begins at earth station. Here an installation is designed to transmit and receive the signal from a satellite in an orbit around the earth.

Generally, cryptographic methods are two types , symmetric and asymmetric cryptography which are used to solve the problems which are raised against the transmitting sensitive data confidentially. Cryptographic satellites such as DES, 3DES , IDEA, AES, LWE. Although due to the threatening of quantum computers, the enlargement and concatenation of a quantum resistant algorithm on satellite is essential.

Key exchange based cryptography through RLWE-KEX algorithm can allocate a solution to this difficulty.

b. RLWE-KEX :

In cryptography, a public key exchange algorithm allows two parties to create and share a secret key, this is important because now a days some public key algorithms are used which is easily broken by a quantum computer. RLWE-KEX is one of post quantum cryptographic algorithms which faces difficulty in solving certain mathematical problems involving lattices. Unlike older lattice based cryptographic algorithms , the RLWE-KEX is provably reducible to a known hard problem in lattices.

Since 1980's the security of cryptographic key exchanges and digital signatures over the internet has been particularly based on a small number of public key algorithms. The security of these algorithms is hard in classical computing. There is difficulty in factoring the product of two choosen prime numbers and to compute discrete logarithms in a carefully choosen finite field. These problems are solved on a classical computer by relatively small quantums using 5 to 10 thousand bits of memory .There is hope in the comnputer industry that large scale quantum computers will be available around 2030 .Cryptography which is not perceptivity to attack by a quantum safe or post quantum cryptography .

One class of quantum resistant cryptographic algorithm is based on a concept called LWE(learning with errors).LWE operates within the ring of polynomial over a finite field. This specialized form is called Ring Learning With Errors (RLWE), which can readily be extended to an actively secure version and an authenticated version. The key exchange consists of one transmission from one end of the line and one transmission from the other end of the link .Diffie-Hellmann and Elliptic curve Diffie-Hellmann are two most popular key exchange algorithms which areused to secure the establishment of secret keys over untrusted communication channels . Like Diffie-Hellmann and Elliptical Diffie Hellmann , the RLWE-KEX Pprovides a property called "forward secrecy", the aim of which is to reduce effectiveness of mass survillance programs. The best method to estimate the practical security of a given set of lattice parameters is the BKHZ 2.0 lattice reduction algorithm. According to the BKZ algorithm the key exchange parameters listed above will provide greater than 128 (or) 256 bits of security , respectively.

RLWE-KEX works in the ring of polynomials modulo a polynomial $\emptyset(x)$ with coefficients in the field of integers mod q (i.e., the ring $R_q:=Z_q[x]/\emptyset(x)$) where q is prime integer .Multiplication and addition of polynomials will work in the usual fashion which results of a multiplication reduced mod $\emptyset(x)$.In 2014, Peikert presented a key transport skill based on Ring-LWE.For some what greatyer than 128 bits of security, Singh presents set of parameters which have 6956 bit public keys for the Piekert's scheme. The private key allows 14000 bits. An RLWE version of the classic MQV variant of Diffie-Hellmann key exchange was discussed by Zhang et al . in 2014. The representation of a typical polynomial is expressed as :

$$a(x)=a_0+a_1x+a_2x^2+----------+a_{n-2}x^{n-2}+a_{n-1}x^{n-1}$$

Another concept necesary for the RLWE problem is the idea of "small" polynomials with respect to some norm. The typical norm used in the RLWE problem is known as infinity norm (also called as uniform norm). This norm of a polynomial is simply the largest coefficient of the polynomial when these coefficients are viewed as integers.

Parameter choices:

RLWE-KEX has two sets of parameters:

- For 128 bits of security, n=512,q=25601, and $\emptyset(x)=x^{512}+1$
- For 256 bits of security, n=1024,q=40961,and $\emptyset(x)=x^{1024}+1$

If we assume that the Gaussian parameter σ is $8/\sqrt{(2\pi)}$ and the uniform sampling bound (b)=5 , then the probability of key agreement is less than 2^{-71} for the 128-bit secure parameters and less than 2^{-91} for the 256-bit secure parameters.

3. PROPOSED SYSTEM DESIGN:

In this work , a RLWE-KEX cryptographic scheme implementation is proposed , based on Zhang et al. work.From this scheme we are providing high computation speed .The proposed implementation consists of two independent systems named as encryption and decryption systems.

An encryption scheme based on the ring-LWE problem has been proposed by Peikert. The steps are described below.

1. **Key Gen() :** Generate a polynomial $a \in Rq$ with coefficients chosen uniformly in Zq. Next sample two polynomials r1, r2 ∈ Rq from X and compute $p = r1 - a \cdot r2 \in Rq$. The public key is (a, p) and the private key is r2.

2. **Enc (a, p, m)** : First encode the message m to a polynomial $\bar{m} \in Rq$. Sample three polynomials e1, e2, e3 ∈ Rq from X . The ciphertext is the pair of polynomials $c1 = a \cdot e1 + e2$ and $c2 = p \cdot e1 + e3 + \bar{m} \in Rq$.
3. **Dec (c1, c2, r2) :** Compute $m0 = c1 \cdot r2 + c2 \in Rq$ and decode the coefficients of m0 to either 0 or 1.

The basic arithmetic operations are polynomial multiplication, addition, subtraction, and generation of error polynomials from a discrete Gaussian distribution. For around 100 bit security, the implementations use a parameter set with n = 256, a 13-bit modulus q, and a narrow discrete Gaussian distribution with standard deviation σ around 4.5. The polynomial multiplication is the costliest one. To perform fast polynomial multiplication, number theoretic transform (NTT) is used over fast Fourier transform (FFT) .

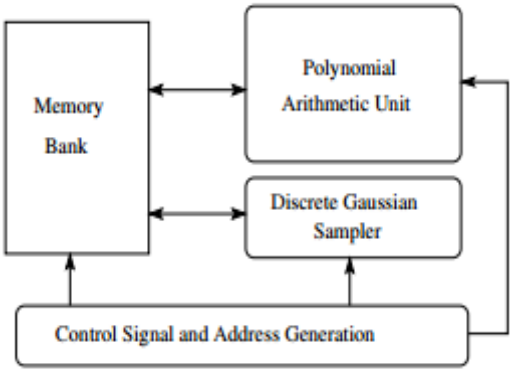

Fig: Architecture Of Ring Lwe Encryption

The architecture uses its polynomial arithmetic unit to perform polynomial addition and multiplication, and the discrete Gaussian sampler to generate the error polynomials. To achieve fast computation time, the architecture uses an efficient memory access scheme.

4. CONCLUSION :

In this paper, we presented a cryptographic scheme for satellite communications is used in Ring Learning With Errors – Key Exchange Cryptography. This architecture provides high speed in satellite communications and also achieve fast computation time. It uses memory banks for data storage. In recent trend there is a great progress in security in telecommunications field. In future security schems can also extended there applications in fields such as cloud Computing, Mobile Computing and the Internet of Things in addition to satellite communication systems.

REFERENCES:

[1] R. Overbeck, N. Sendrier, “Code-based cryptography”, In Post-Quantum Cryptography, pp 95-146, 2009.
[2] J. Buchmann, E. Dahmen, M. Szydlo, “Hash-based Digital Signature Schemes”, In Post-Quantum Cryptography, pp 35-94, 2009.
[3] J. Ding, B. Yang, “Multivariate Public Key Cryptography”, In Post-Quantum Cryptography, pp 193-242, 2009.
[4] L. De Feo, D. Jao, J. Plut, “Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies”, Journal of Mathematical Cryptology 8(3). pp 209-247, 2014.
[5] D. Micciancio, O. Regev, “Lattice-based Cryptography”, In Post-Quantum Cryptography, pp 147-192, 2009.
[6] J. Howe, C. Moore, M. O’Neill, F. Regazzoni, T. Güneysu and K. Beeden,“Lattice-based Encryption Over Standard Lattices in Hardware”, DAC '16, proceedings of the 53rd Annual Design Automation Conference (162), Austin, 2016.
[7] JSAT International, “Satellite Components”, 2018.
[8] W. Stallings, “Cryptography and Network Security”, 6th edition, Upper Saddle River, Pearson, ISBN: 0133354695, 2014.
[9] S. Bai and S. D. Galbraith. An Improved Compression Technique for Signatures Based on Learning with Errors, pages 28–47. Springer, Cham, 2014.
[10] BBC News. NSA ‘developing code-cracking quantum computer’. January 2014. http://www.bbc.com/news/technology-25588605.
[11] A. Boorghany, S. B. Sarmadi, and R. Jalili. On Constrained Implementation of Lattice-based Cryptographic Primitives and Schemes on Smart Cards. Cryptology ePrint Archive, Report 2014/514, 2014.
[12] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from lwe. Cryptology ePrint Archive, Report 2016/659, 2016.
[13] N. Sklavos, I. D. Zaharakis, A. Kameas, A. Kalapodi, “Security & Trusted Devices in the Context of Internet of Things (IoT)”, Euromicro Conference on Digital System Design (DSD), Vienna, Austria, 2017. [16] N. Sklavos, I. D. Zaharakis, “Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and

Implementations", IEEE proceedings of the 8th IFIP International Conference on New

[14] Technologies, Mobility and Security (NTMS'16), Larnaca, Cyprus, November 21-23, 2016. [17] T. Pöppelmann and T. Güneysu, "Area optimization of lightweight latticebased encryption on reconfigurable hardware", In ISCAS, pp 2796-2799, 2014. [18] I. D. Zaharakis, N. Sklavos, A. Kameas, "Exploiting Ubiquitous Computing, Mobile Computing and the Internet of Things to Promote Science Education", IEEE proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS'16), Larnaca, Cyprus, November 21-23, 2016

[15] N. Sklavos, "On the Hardware Implementation Cost of Crypto-Processors Architectures", Information Systems Security, The official journal of (ISC)2, A Taylor & Francis Group Publication, Vol. 19, Issue: 2, pp 5360, 2010.