ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Analysis and Implementing the NTRU and Braid Group Cryptosystem Algorithms in IoT Devices

[1] M.Jeyanthi, [2] S.Parameswaran
[1] Final Year PG Computer Science Student, [2] Asst. Prof of CSE
[1][2] Sree Sowdambika College of Engineering

***Abstract* – In this paper we give an overview of public-key cryptographic schemes based on non-commutative groups with special consideration to braid groups and we have to analysis several commonly used light weight algorithm public key-exchange protocols with the aim of establishing the best algorithms for lightweight cryptography in critical infrastructure and emergency scenarios. Most of the method currently in use are based on arithmetic over finite field. The potential advent of quantum computer is very troubling because all of these cryptosystem are easily broken by such machine. Braid group based on non-commutative algebraic structure over infinite field .Braid group have certain properties that make them easily amenable to digital computation. The main contributions of this paper are: 1.Performance analysis of several state-of-the-art public-key cryptographic algorithms like NTRU Encryption, Braid groups etc. In order to find those that are most suitable for low power computing platforms 2.Implementing security framework based on the analyses public-key key-exchange cryptographic algorithms in IOT devices. Internet of Things (IoT) enables physical things to communicate, compute and take decisions based on any network activity.**

***This calls for a secure solution for communication among heterogeneous devices.**

***In heterogeneous environment motive of each user in IoT can be different in form of communication and computation and is difficult to be judged.**

Index Terms— NTRU-Number theory research unit, Public key cryptography, Braid Group cryptosystem, Wireless communications,Dehornoy's algorithm.

1. INTRODUCTION

methods for secure correspondence within the sight of outsiders (called enemies). All the more for the most part, it is tied in with developing and dissecting conventions that beat the impact of enemies and which are identified with different viewpoints in data security, for example, information secrecy, data integrity, and authentication . The earliest secret writings have been found in 4000-year-old Egyptian hieroglyphics. These do not seem to have been a serious attempt to hide information, but rather a puzzle for readers to solve.

The Romans used a substitution cipher, the Caesar cipher. In this scheme each letter of the alphabet is replaced with another. By today's standard this is almost a trivial scheme to crack. A stronger version of a substitution cipher was developed in the 16th Century, the Vigen`ere cipher. By the 20th Century machines like Enigma made ciphers that were extremely difficult for a human to break. All of the older cryptosystems were "private key".

In other words, the same secret key is used to decrypt as it is to encrypt. This poses the problem of transmitting the key securely itself. In 1976 the first "public key" protocol was developed by Diffie and Hellman. This was an important development, as now secrets can be kept hidden without ever physically sharing keys. Today, security is more important than it has ever been. The internet has left us vulnerable in ways that did not exist before. Everything is potentially out in the open. There is banking information, business secrets, health-care records, credit-card purchases, emails, telephone calls, national security, your secrets – all of that subject to attack. It is projected that eCommerce will hit 1.5 trillion dollars! There are hackers, criminals, extortionists, and others with malicious intent that want your information. The good news is that cryptography is keeping us safe. The NTRU Encrypt public key cryptosystem, also known as the NTRU encryption algorithm is based on the shortest vector problem in a lattice. Operations are based on objects in a truncated polynomial ring R=Z[X]/(XN-1) with convolution multiplication and all polynomials in the ring have integer coefficients and degree at most N-1.a=a0+a1X+a2X2+…+aN-2XN-2+aN-1XN-1

2. BRAID GROUPS

The braid cluster Bn is AN infinite, nonabelian cluster of n braids. A member of the braid cluster Bn encompasses a easy geometric interpretation. Visualize n strings connection n points at the highest to n points at very cheap, not essentially vertically. Keeping the ends of the strings fixed, imagine crossing these strings zero or additional times. AN example is shown in Figure one. Braids may be delineate victimization the generators i (Figure 2) of the cluster Bn. The braid cluster Bn is given by the (Artin) presentation

Bn = {σ1, . . . , σn−| σiσj = σjσi for |i − j| ≥ 2 , σiσjσi = σjσiσj for |i − j| = 1}

A property of braid group elements that makes them easy to digitize is that they can be uniquely represented in a convenient form. We will need to define a few notions to describe this unique representation.

Consider the monoid Bn+ (a monoid satisfies all the requirements of a group except the existence of inverses). Elements of Bn+ can be written as words in only the i+1 (not thei 1) under the same relations as the group Bn shown in Eq. (1). These elements are called positive braids and are used to define an order relation between braids:

x ≤ y if y = axb, with x, y ∈ Bn and a, b ∈ B + n (2)

We next define the fundamental braid Δ of Bn:

Δ = (σ1 • • • σn−1)(σ1 • • • σn−2)• • • σ1 (3)

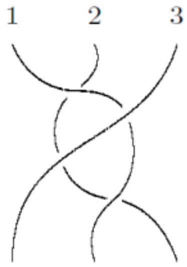


Figure 1: The 3-braid σ1-1 σ2 σ1 σ2= σ2 σ1

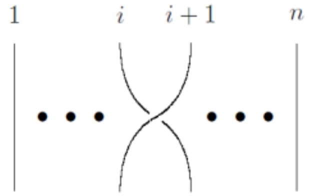


Figure 2: The generator _i

2.1 Conjugacy search problems

A difficult issue is the supporting of any open key cryptosystem. There are a few (evidently) difficult issues in mesh gatherings. We will center around variations of the conjugacy look issue, around which all the twist assemble cryptosystems proposed to date are constructed.

2.1.1 Conjugacy Search Problem

Given x, y ∈ Bn such that y = a −1xa for some a ∈ Bn. Find b ∈ Bn such that y = b −1xb.

2.1.2 Generalized Conjugacy Search Problem

Given x, y ∈ Bn such that y = a −1xa for some a ∈ L Bn. Find b ∈ L Bn such that y = b −1xb. (This problem can also be stated with a, b ∈ U n)

2.1.3 Diffie - Hellman type Generalized Conjugacy Search Problem

Given x, yA, yB ∈ Bn such that yA = a −1xa and yB = b −1xb for some a ∈ LBn and b ∈ UBn. Find b −1yAb(= a −1yBa = a −1 b −1xab).

2.2 Commutator based key agreement

Key agreement protocol that's supported the multiple synchronic conjugacy search drawback. This protocol is termed the Arithmetica key exchange.

2.2.1. Public information

(a) The braid index n is published.

(b) A(lice) publishes the subgroup GA = hx1, . . . , xsi ⊆ Bn
by specifying the generators x1, . . . , xs.

(c) B(ob) publishes the subgroup GB = hy1, . . . , yti ⊆ Bn by specifying the generators y1, . . . , yt

2.2.2. Key agreement

(a) A selects a secret word a = W(x1, . . . , xs) ∈ GA and sends a −1y1a, . . . , a −1yta to B.

(b) B selects b = V (y1, . . . , yt) ∈ G B and sends b −1x1b, . . , b −1xsb to A.

This protocol works because the product of conjugates is the conjugation (by the equal element) of products: (a −1xa)(a −1ya)=a−1xya. Anshel et al cautioned the usage of n= 80 and s=t=20 turbines for every subgroup.

2.3 Diffie-Hellman type key agreement

In 2000, Ko et al proposed a key agreement protocol based on the Diffie-Hellman type Generalized Conjugacy Search Problem. 1. Public information (a) A sufficiently complicated braid x ∈ Bn is published, along with the braid index n. 2. Key agreement (a) A(lice) selects a ∈ LBn (A's private key) and sends yA = a −1xa (A's public key) to B. (b) B(ob) selects b ∈ UBn (B's private key) and sends yB = b −1xb (B's public key) to A. (c) B receives yA and computes the shared key K = b −1yAb = a −1 b −1xab. There are strong parallels between this key

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

agreement and the Diffie-Hellman key agreement. The braid x is analogous to the integer g and conjugation a −1xa replaces exponentiation g a . Ko et al suggested a few instances of the security parameters,

2.4 Dehornoy's algorithm

Dehornoy's algorithm for the phrase problem is an handy to implement and environment friendly algorithm. A word w is stated to be decreased if for any i such that w is of the form:

w1 ai w0 ai-1w2 (or) w1 ai-1 w0 ai w2

Where w1 ,w2 ,w0 are the substring there exists some j < i such that two ai ai-1 is in w0

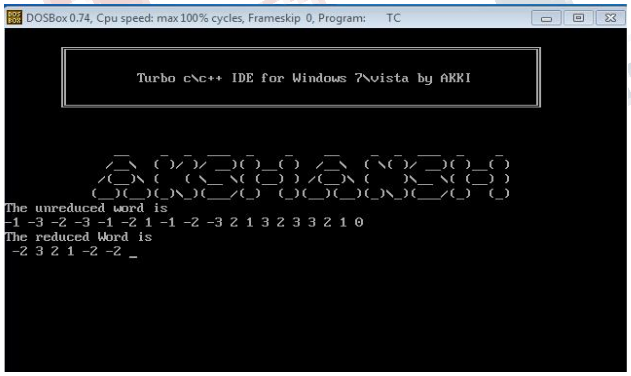
2.4.1 Handle Reduction

In the handle reduction technique we consider two main concept they are permitted handle and handle reduction

A allowable handle of a braid word w may be a sub word of the shape h = σ±11 V0σε2V1σε2• • • σε2Vkσ∓11 where ε ∈ {±1} and Vi is a word containing no σ1±1, σ2±1.

- Handle discount could in addition produce new handles (and the scale of phrases may increase) – thus it's uncertain whether or not manage reduction makes braid 2 in a very higher kind. ar we tend to drawing near σ-positive/negative word
- Nevertheless, handle reduction eventually yields a σ-positive or σ-negative word

The reduced word using handle reduction method in dehornoys algorithm was shown below


DOSBox 0.74, Cpu speed: max 100% cycles, Frameskip 0, Program: TC

```
Turbo c\c++ IDE for Windows 7\vista by AKKI

The unreduced word is
-1 -3 -2 -3 -1 -2 1 -1 -2 -3 2 1 3 2 3 3 2 1 0
The reduced Word is
 -2 3 2 1 -2 -2 _
```

3. NTRU ENCRYPTION ALGORITHM

NTRU is while not a doubt a parameterized social unit of cryptosystems; each system is precise with the helpful resource of 3 number parameters (N, p, q) that signify the highest degree N-1for all polynomials within the truncated ring R, alittle modulus and an outsized modulus, severally, the section it's assumed that N is prime, letter of the alphabet is unceasingly massive than p, and p and letter of the alphabet area unit coprime; and four sets of polynomials radio frequency, Lg, lumen and Lr (a polynomial a part of the non-public key, a polynomial for technology of the general public key, the message and dazzling worth, respectively), all of credentials at the most N-1.Sending a secret message from Alice to Bob needs the generation of a public and a personal key.

The public key is known by both Alice and Bob and the private key is only known by Bob. To generate the key pair two polynomials f and g, with coefficients much smaller than q, with degree at most N-1and with coefficients in {-1,0,1} are required. They can be considered as representations of the residue classes of polynomials modulo XN-1 in R.

Alice, who wants to send a secret message to Bob, puts her message in the form of a polynomial m with coefficients {-1,0,1}. In modern purposes of the encryption, the message polynomial can be translated in a binary or ternary representation.

After creating the message polynomial, Alice chooses randomly a polynomial r with small coefficients (not restricted to the set {-1,0,1}), that is meant to obscure the message. With Bob's public key h the encrypted message e is computed: e= pr.h+m (mod q) anybody knowing r could compute the message m; sor must not be revealed by Alice. In addition to the publicly available information, Bob knows hisown private key.

Here is how he can obtain m: First he multiplies the encrypted message e and part of his private key f, the NTRU Encryption algorithm's security is based on modulo two unrelated moduli, and its correctness is based on clustering properties of the sums of random variables. In "CS attack" we tend to follow lattice foundation discount ways to cryptanalyze the theme, to get each the authentic secret key, or an alternate secret key that is equally helpful in cryptography text. what is more, a variety of attacks use the similar standards of metal attack. thence we discover out regarding and gift new techniques exchanging the non-public key on a unconquerable channel.

4. EXISTING AUTHENTICATION PROTOCOL

The formal novel mutual authentication and key settlement protocol based on the number principle research unit (NTRU) public key cryptography for

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 5, Issue 3, March 2018

wireless communications proposed by way of Jiang Jun and HeChen, is inclined lattice based totally attack. “CS attack”, new lattice based totally assault new hybrid meet in the middle and lattice discount assault are some of the assaults that work. The present mutual authentication and key agreement protocol for wireless communication makes use of NTRU encryption for the key trade between the user and server. The complete manner is carried out in two phases

- Initialization stage.
- Real-Time alternate stage.

During the initialization stage, the certificates are distributed from CA to customers and network authentication servers. In the preliminary stage the person chooses two random polynomial equations SKu and gu. PKu is the public key that is computed according to NTRU key era algorithm. Thus the person holds each public and non-public key. Now the consumer sends his public key alongside with his ID to CA.

$$PK_u + ID \longrightarrow CA$$

The CA the use of his non-public key applies NSS Algorithm to generate has cost of PKu which is used as signature. A transient ID is assigned to consumer denoted as TIDu and a timestamp Tu. The CA sends a certificate along with its public key PKca. The certificate consists of hash (PKu), TIDu and Tu. The identical data is sent to AS also. From now the 2d stage starts.

$$Hash\ (PK_u)+TID_u+T_u+PK \longrightarrow User$$

Here, the use of CS attack in the manner of man-in-the-middle assault the first stage can be penetrated through the attacker. It is defined as follows. When the person sends his public key along with ID, the attacker captures the records from being delivered to CA, and CS attack is utilized to find the user’s personal key or an choice key that works as personal key. Now the attacker forwards the public key along with the victim’s user ID to CA. Then CA sends user’s certificates alongside with its public key. The attacker captures the facts and prevents it from being delivered to the user. Now the attacker has victim’s public key, personal key and user certificate.

5. THE MODIFIED PROTOCOL

The proposed machine would additionally work in two stages,

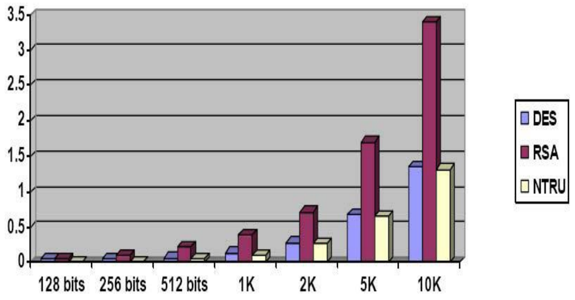
Stage 1: Initialization stage
Stage 2: Real time alternate stage

In the initialization stage the polynomial is ring is form. A random polynomial equation is chosen which belongs to the ring as the session’s non-public key. The corresponding public key is generated. The public key is again encrypted using DES encryption algorithm. The key used for the decryption is only acknowledged to the person and network AS. The encrypted public key is despatched over the tightly closed conversation channel. The key is exchanged over the conversation channel safely.

Hence the proposed device would accomplish the following tasks:

•Able to communicate the public key in secure manner.
•Increased security than the current system.
•Implement new approach for communicating the session key between the consumer and the network AS.

The under plan explains the performance analysis for DES, RSA and NTRU strategies



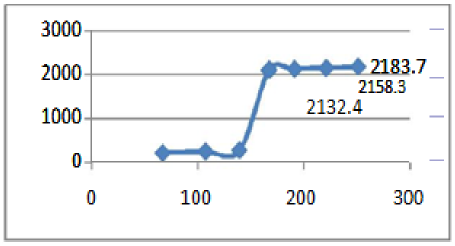
Performance analysis on encryption for DES, RSA and NTRU methods

6. PERFORMANCE EVALUATION

The experiments of the CS attack on NTRU encryption algorithm have been implemented on Pentium IV 2.04GHz PC.

N : Degree of the polynomial
Q : Randomly selected integer
T : Time taken to compute the public key from the chosen private key
Tint : Time for Initialization of lattice
Tred : Time for the lattice reduction
Tone : Time taken fo initialization of lattice lattice + Time taken for the lattice reduction
Ttot : Total time taken to cryptanalyze the private key form the public key

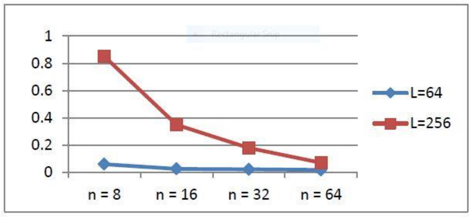
The most average time to cryptanalyze NTRU encryption algorithm and the maximum common time for cryptanalyzing the DES encryption algorithm for a number of parameter sets and found the effects and introduced them in the following graphs



Degree of polynomial (N) on X-axis; Time in sec on Y-axis

Figure 1:Graph showing the relation between the time taken to cryptanalyze the private key to the degree of the polynomial.

In this work, we analyse the feasibility of using the Braid Key Reduction scheme, in aid restrained devices such as those used for Internet-of-Things endpoints. We present an evaluation of Braid Key Reduction blessings over different cryptosystems for use in such devices. We existing some data on the wide variety of discount steps and the common time wished to decrease a random braid in terms of the braid index. Furthermore, to the first-class of our knowledge, in this work we current the first time independent implementation of Braid Key Reduction.



Entity Authentication Schemes Using Braid Word Reduction

CONCLUSION

Braid groups grant an elegant framework for designing new public key cryptosystems that can be efficiently implemented on a digital computer. These cryptosystems suffer but a minor drawback: they are no longer secure! Even inside the confines of braid groups, it might also still be possible to assemble a impenetrable cryptosystem through an splendid desire of the security parameters; in addition investigation is needed. In addition, there are problems except the conjugacy search problems that ought to be used to diagram a secure cryptosystem.

The advantages of NTRU

- more efficient encryption and decryption, in both hardware and software implementations;
- much faster key generation allowing the use of “disposable" keys (because keys are computationally “cheap" to create).
- low memory use allows it to use in applications such as mobile devices and Smart-cards.

If an software is required with the perfect decryption priority DES is greater appropriate - An asymmetric key cryptographic device gives high security in all ways. Encryption, decryption and complexity are excessive in NTRU - The RSA gives the best safety to the business application.

ACKNOWLEDGMENT

This paper was supported by the Sree Sowdambika College of Engineering, Final Year PG Computer Science student M.Jeyanthi (Reg.no:921816405005) guided by S.Parameswaran, Assistant Professor of Computer Science and Engineering. The authors thank to their colleagues for their help and support at different stages of the system development. Finally, we would like to thank the anonymous reviewers for their helpful comments.

REFERENCES

1. Hoffstein J., Lieman D., Pipher J., Silverman J. “NTRU: A Public Key Cryptosystem”, NTRU Cryptosystems, Inc.
2. Parasitism C, Prada J. “Evaluation of Performance Characteristics of Cryptosystem Using Text Files”, Journal of Theoretical and Applied Information Technology.
3. Hoffstein J., Pipher J., Silverman J. An Introduction to Mathematical Cryptography, New York,2008
4. Hoffstein J., Pipher J., Silverman J. “ NTRU – A ring based public key cryptosystem”
5. Andrea Pellegrini, Valeria Bertacco and Todd Austin (2010), “Fault-Based Attack of RSA Authentication”
6. Anoop MS (2007),“Public Key Cryptography Applications Algorithms and Mathematical Explanations”.
7. Aydos, M., Sunar, B., Koç, Ç.K., (1998), “An Elliptic Curve Cryptography Based Authentication and

Key Agreement Protocol for Wireless Communication”. 2nd Int. Workshop Discrete Algorithms (DIAL M’98), Dallas, TX.

8. Neal Koblitz and Alfred J. Menezes, A survey of public-key cryptosystems, SIAM Re-view 46 (2004) 599-634.

9. Iris Anshel, Michael Anshel, and Dorian Gold feld, An algebraic method for public-key cryptography, Mathematical Research Letters (6) (1999) 287-291.

10. Iris Anshel, Michael Anshel, and Dorian Goldfeld, Method and apparatus for crypto-graphically secure algebraic key establishment protocols based on monoids, United States Patent 6,493,449 2002).

11. Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park, New Public-Key Cryptosystem Using Braid Groups, CRYPTO 2000, 166-184, Springer Lecture Notes in Computer Science (2000).

12. Patrick Dehornoy, Braid-based cryptography, Contemporary Mathematics 360 (2004) 5-33.

13. Jae Choon Cha, Ki Hyoung Ko, Sang Jin Lee, Jae Woo Han, and Jung Hee Cheon, An efficient implementation of braid groups, AsiaCrypt 2001, 144-156, Springer Lecture Notes in Computer Science 2048 (2001).

14. J. A. Stankovic, “Research directions for the internet of things,” IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3–9, Feb 2014.

15. K. Akpinar, K. A. Hua, and K. Li, “Thingstore: A platform for internetof-things application development and deployment,” ser. DEBS ’15. New York, NY, USA: ACM, 2015, pp. 162.

16. D. Bonino, M. T. D. Alizo, A. Alapetite, T. Gilbert, M. Axling,H. U. andJose Angel Carvajal Soto, and M. Spirito, “Almanac: Internet of things for smart cities,” 2015 3rd International Conference on, Aug 2015, pp. 309–316.

17. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22–32.

18. C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, “A survey on internet of things from industrial market perspective,” IEEE Access, vol. 2, pp.1660–1679, 2014.

19. F. A. Garside, The braid group and other groups, Quart. J. Math. Oxford 20 (1969),no. 78, 235–254.

20. M. Garzon and Y. Zalcstein, The complexity of Grigorchuk groups with application to cryptography, Theoretical Computer Sciences 88 (1991) 83–98.

21. O. Goldreich, S. Goldwasser and S. Halevi, Public-key cryptosystems from latticereduction problems, Advances in Cryptology, Proceedings of Crypto ’97, Lecture Notes in Computer Science 1294, ed. B. Kaliski, Springer-Verlag (1997), 112–131.

22. E. S. Kang, K. H. Ko and S. J. Lee, Band-generator presentation for the 4-braidgroup, Topology Appl. 78 (1997), 39-60.

23. K. Komaya, U. Maurer, T. Okamoto and S. Vanston, Newpublic-key schemes baseson elliptic curves over the ring Zn, Advances in Cryptology, Proceedings of Crypto’91, Lecture Notes in Computer Science 576, ed. J. Feigenbaum, Springer-Verlag(1992), 252–266.

24. N. Koblitz, Algebraic aspects of cryptography, Algorithms and Computations in Mathematics 3 (1998) Springer-Verlag, Berlin.

25. J. C. Lagarias, Knapsack public key cryptosystems and Diophantine approximation, Advances in Cryptology: Proceedings of Crypto ’83, ed. by D. Chaum, Plenum Publishing (1984), 3–24.