Improving the Security in Wireless Network System Using NTRU

Myat Mon Tin; Kalyar Myo San
University of Computer Studies, Yangon
myatmon.tin27@gmail.com; kalyar.myosan@gmail.com

Abstract

Reliable technology is not enough to ensure the security for the many application systems. Such several reliability deficiencies become the vital part of the security level in today wireless technology. Efficient cryptographic techniques are necessary to endow the security level in wireless network system. NTRU becomes the fastest and smallest public-key security solutions for wireless technologies and applications. In Advanced Number Theory Research Unit (NTRU) Public key Cryptosystem (PKCS) is composed with mainly three parameters: N is the polynomials of the truncated polynomial ring have degree N-1, p is small modulus which can reduce the coefficient of the message at the decryption process and q is large modulus which can reduce the coefficient of the truncated polynomial. In this paper, we analyze to improve the security in wireless network system by applying four security levels such as moderate, standard, high, and highest of Advanced NTRU.

Keywords: Advanced NTRU, PKCS, wireless, security level

1. Introduction

The growth of lightweight mobile devices is growing as the time goes by. Therefore, wireless communications which are used by these mobile devices are the essential part of the daily life of human being. This is a convenient way to stay connected with family members or business clients anytime of the day. Significantly, a wireless network is of great advantage compared to wired network. Wired network usually consumes a lot of time in order to set up in a building or house. In some instances, there is a need to route wires through thick wall or ceilings. Wireless network can be deployed easily and is less expensive. More clients can be added to the network without the necessity for extra materials. Now, with this growing adoption of wireless network, security has become a focal point regarding the decision to deploy the wireless network.

To protect against attackers for wireless communication, one of the solutions of wireless network security is using PKCS. Among them, NTRU PKCS is more suitable than any other PKCS because of its greater security and speed. In fact, NTRU PKCS has ordinary type and optimization for this ordinary type. Both of these two types offer various security levels for wireless network. On account of greater security, NTRU becomes popular in today wireless networks. In this paper, Advanced NTRU is applied in wireless network system for online library system by encrypting password of the register users to secure their data. Furthermore, the experimental results demonstrate by analyzing the four security levels of registered users' passwords.

2. Related Work

Johannes Buchmann [1] presented a new algorithm for enhancing the performance of NTRU a variety of methods that may be used to increase the speed and efficiency of the NTRU public key cryptosystem. The author also presented a highly efficient implementation of NTRU within the Java Cryptography. Krishnapriya Kadati [5] compared the capabilities and performance of a pure Java JCE implementation, a JNI based C/C++ native implementation and a pure Visual C++ implementation of NTRU PKCS. Narasimham Challa [2] stated about that NTRU confirms its cryptography and delivers encryption, decryption and authentication at speeds of multiple times faster than RSA. NTRU is ideally suited for applications where high performance, high security and low power consumption are required. NTRU has its unprecedented performance advantages open up new options for security. JIANG Jun [4] presented a novel mutual authentication and key agreement protocol based on NTRU public key cryptography. The symmetric encryption, hash and "challenge-response" techniques were adopted to build their protocol. Since the lightweight NTRU public key cryptography is employed, their protocol can not only overcome the security flaws of secret-key based authentication protocols such as those used in Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS).

3. PKCS

The development of public-key cryptography [6] is the greatest and perhaps the only true revolution in the entire history of cryptography. It is also called asymmetric algorithm which has two keys: public key and private key. Anyone knowing the public key can encrypt messages or verify signatures, but cannot decrypt messages or create signatures. To decrypt the encrypted message, private key is used.

3.1 NTRU: Advanced Topics

NTRU public-key algorithm is a lightweight one which can be used for cryptographic public-key scheme in wireless network because of its greater security, speed and lower computational complexity. Both encryption and decryption process of NTRU are extremely fast compared to other asymmetric encryption scheme. The fundamental operation of NTRU involves convolution polynomial rings and addition of small numbers. Although the key length of NTRU and other asymmetric algorithms are the same, the key generation in NTRU is fast and easy.

3.2 Parameters of Advanced NTRU

NTRU PKCS [7] is parameterized by three values N, p and q. All objects are univariate polynomials of degree N which are multiplied using the convolution product rule. For getting faster speed, assigned p as 2+X. q is using as modulus; multiplication and addition are generally followed by reduction mod q.

This table shows the various security levels of NTRU.

Table (1) Security levels of NTRU

Security levels	N	q
Moderate	167	128
Standard	251	128
High	347	128
Highest	503	256

3.3 Polynomial Multiplication of Advanced NTRU

All operations of advanced NTRU are based on the objects in a truncated polynomial ring with convolution multiplication and all polynomials in the ring have integer coefficients and degree at most N-1.

3.3.1 Polynomial Ring (R)

An algebraic structure is a polynomial ring in which addition and multiplications are defined. It has to be communicative for ring addition (i.e, a+b = b+a) but it doesn't has to be communicative for ring multiplication (i.e, a.b = b.a).

3.3.2 Polynomial Multiplication of Advanced NTRU

The operation of polynomial multiplication is as follows:

$a = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + \ldots + a_{N-2} X^{N-2} + a_{N-1} X^{N-1}$

$b = b_0 + b_1 X + b_2 X^2 + b_3 X^3 + \ldots + b_{N-2} X^{N-2} + b_{N-1} X^{N-1}$

$c = c_0 + c_1 X + c_2 X^2 + c_3 X^3 + \ldots + c_{N-2} X^{N-2} + c_{N-1} X^{N-1}$

$$c_k = \sum_{i=0}^{k} a_i . b_{k-i} + \sum_{i=k+1}^{N-1} a_i . b_{N+k-i} \quad (1)$$

3.4 Key Generation of Advanced NTRU

As a public-key cryptosystem, NTRU have to generate not only public key but also private key for encryption and decryption process. First of all, a small random polynomial **(F)** has to be generated for getting private key **(f)** with p=2+X. After getting the private key, it has to be inversed to generate **(fq)** as a part of a public key **(h)**. By generating a full public key, a small random polynomial **(g)** is also needed. The process of Key Generation is as follows:

$$\text{private key } (f) = 1 + p*F \quad (2)$$

$$\text{public key } (h) = p*fq*g \pmod q \quad (3)$$

3.5 Encryption Process of Advanced NTRU

Encryption process is implemented by using with public key **(h)** and a small random polynomial **(r)** and original message **(m)**. The operation of encryption process is shown in below.

$$c = r*h + m \pmod q \quad (4)$$

3.6 Decryption Process of Advanced NTRU

Because of asymmetric algorithm, the public key is used to encrypt the original message. On the other hand, the private key is used to decrypt the encrypted message. To get the original message, the following equations are used.

$$a = f*e \pmod q \quad (5)$$

$$d(-2) = a(-2) \pmod{2^N + 1} \quad (6)$$

To get the decrypted ciphertext polynomial d, the above equations are used. Besides, it can also show that the decrypted ciphertext is whether true or not by equality.

3.6.1 Centering the polynomial a

All the coefficient of p*r*g + f*m are normally lie between the range of -q/2 and +q/2. On account of using binary polynomials **f** to have form 1 + p*F, the values of r, g, m and f will not be centered at zero. In spite of involving the values of polynomials are small, they won't lie within the range of -q/2 and +q/2.

Moreover, it can't be identified the total number of 1's and 0's which is included in original message before it can be decrypted. But it can be extracted from using the following method.

1. Set $I = fq(1) . (a(1) - p(1) . r(1) . g(1)) \pmod q$

2. Set $Avg = (p(1) . r(1) . g(1) + I f(1)) / N$

3. The expected range of the coefficients will be between Avg - q/2 and Avg + q/2. Avg will generally not be an integer, so the actual expected range will be the q integers that lie between Avg - q/2 and Avg + q/2.

3.6.2 HuffMan Encoding

There is a way to assign binary codes to symbols that reduces the overall number of bits used to encode a typical string of those symbols. This is called Huffman encoding**.** Huffman coding [8] is an entropy encoding algorithm for lossless data compression. The term refers to the use of a variable-length code table for encoding a source symbol (such as a character in a file) where the variable-length code table has been derived in a particular way based on the estimated probability of occurrence for each possible value of the source symbol.

3.6.3 Generating a HuffMan Tree

For getting an optimum code, a given message code length can more than the length of a more portable message code [3]. If this requirement were not met, then a reduction in average message length could be obtained by interchanging the codes for the two messages in question in such a way that the shorter code becomes associated with the more portable message. Moreover, if there are several messages with the same probability, it is possible that the codes for these messages may differ in length. However, the codes for these messages may be interchanged in any way without affecting the average code length for the message ensemble.

4. Proposed System

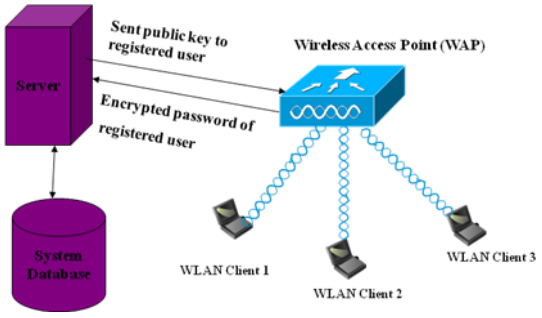

Figure (1) Proposed System Design

When a visited user wants to register as a member of the website, server has to generate public key for him/her to encrypt the password while the related private key will be stored at the server. The encrypted password will be sent to the server and then the pre-stored private key will be used to decrypt it. If the decrypted data is same to the pre-stored data which is at the server, the registered user will be granted to the wireless network and also has rights to access the services.

4.1 Key Generation from Server Side

Algorithm 1

generateKey(pubKey, priKey)

1. invertable = false;
2. randPolyBinaryP(g, DG)
3. while not invertable
4. do
5. randPolyBinaryP(priKey, DF)
6. priKey = priKey + 1
7. invertable = inversePoly2(temp, priKey)
8. end do
9. inversePolyQr(Fq, priKey, temp, Q)
10. multN(pubKey, Fq, g, Q);

4.2 Generating a HuffMan Code from Client Side

If we have a set of numbers and their frequency of use, we can create a huffman tree by sorting the list of frequency. Parent node in this tree is created by combining the two lower element's frequencies and two-lowest elements are formed as leaves. We have to calculate until just only one element left in the list which will become the root of binary huffman tree. After getting the root element, we can take the value of huffman code due to cross the tree to the value we want. Ouput value of left-hand side is 0 and right-hand side is 1.

4.2.1 Example of HuffMan Tree*:*

The encoding for the value **4** (15:4) is **010**. The encoding for the value **6** (45:6) is **1.**

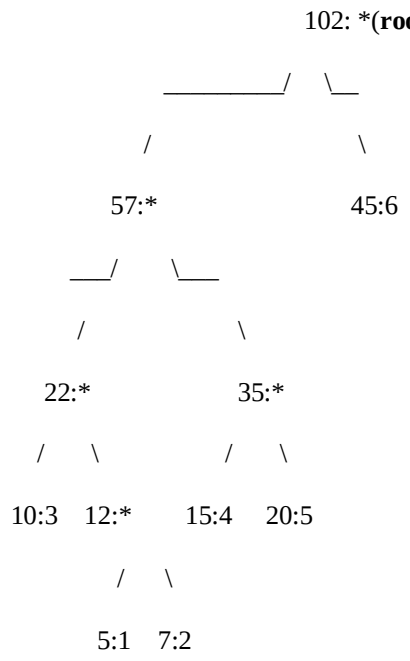

Figure (2) Structure of HuffMan Tree

4.3 Encryption process from Client Side

Algorithm 2

encryptPolyP(ciphertext, plaintext, key)

1. randPolyBinary(r, DR)

2. multN(ciphertext, key, r, Q)

3. for i = 0 to n-1 step 1

4. ciphertext[i] = (ciphertext[i] + plaintext[i]) mod Q

5. end loop

4.4 Decryption process from Server Side

Algorithm 3

decryptPolyP(plaintext, ciphertext, key)

1. mult(a, key, ciphertext, Q)

2. for i = 0 to n-1 step 1

3. if a[i] < 0 then

4. a[i] = a[i] + Q

5. else if a[i] > Q / 2 then

6. a[i] = a[i] - Q

7. end if

8. plaintext[i] = a[i]

9. end loop

10. reduceModP2(plaintext)

5. Experimental Result

When an existing user or a new user logs into the site, step by step procedures are performed as described in section 4. Performance analysis of the four security levels of NTRU PKCS is done by based on the same password length of a user. This system can allow from 6 password lengths to 14 for one user. Table (2) shows one of the sample records that are recorded by using same password length of the same user for four security levels. This example presents about the password length is six and testing is made ten times by using same password length for that user. According to the experimental results, the processing time (encryption and decryption and keygen time for password) is varying even it has the same password length. The processing time varies based on the generating the random numbers. Because the random number will be reproduce in every login transaction for one user to improve security.

The comparison result of these four types is as shown in the table and the graphical presentation is also shown in figure (3). According to the figure (3), the highest levels can ensure to be the best security level because it takes the maximum time for processing (encryption and decryption and keygen time). Sometimes, the processing time in four security levels may be

nearly same, the highest levels can ensure to improve the security in wireless network system among other security levels of NTRU PKCS.

Table (2) Result of Comparison

Moderate	Standard	High	Highest
15	0	31	62
0	15	16	47
0	15	31	62
31	0	31	31
16	15	32	63
16	16	31	62
15	16	32	63
0	16	31	62
0	15	16	46
0	0	31	47

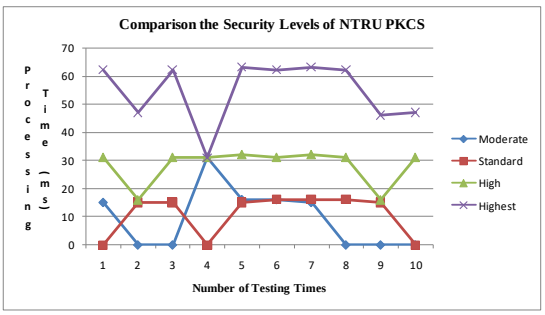

Figure (3) Comparison the Security Levels of NTRU PKCS

6. Conclusion

NTRU offers the first public key security solution that is specifically designed to operate efficiently and cost effectively in resource-constrained wireless environments. With NTRU technology, carriers, handset manufacturers and application developers are able to secure 2.5 and 3G wireless applications, while realizing increased system performance, fast deployment and critical scalability. Moreover, because of using advanced NTRU, the processing time is faster than NTRU and it can also improve the security by generating the random numbers. This paper analyzed the enhancement of the security in wireless network system by applying four security levels such as moderate, standard, high, and highest of Advanced NTRU. Among them, highest level can support better security than any other security levels of NTRU PKCS in wireless network system.

References

[1] J.Buchmann, M.Döring, R.Lindner, "Efficiency Improvement for NTRU", Sicherheit 2008, Lecture Notes in Informatics, Volume 128, pp. 163-17 8, Copyright Gesellschaft für Informatik, 2008.

[2] N.Challa, J.Pradhan, "Performance Analysis of Public key Cryptographic Systems RSA and NTRU", International Journal of Computer Science and Network Security (IJCSNS), VOL.7 No.8, August 2007.

[3] DAVID A. HUFFMAN, "A Method for the Construction of Minimum-Redundancy Codes", Proceedings of the Institute of Radio Engineers, Vol. 9, No. 40. (September 1952), pp. 1098-1101.

[4] J.Jun, H. Chen, "A novel mutual authentication and key agreement protocol based on NTRU cryptography for wireless communications", Journal of Zhejiang University Science (JZUS), ISSN 1009-3095, Vol.6A, Issue 5, p.399-404, 2005.

[5]K.Kadati, K.D.Bhimavarapu, G. Koodarappally, "Capabilites and Performance of a JCE Implementation of NTRU PKCS", Project Specification, ECE 646, Fall 2005, George Mason University.

[6] William Stallings, "Cryptography and Network Security ", Fourth Edition, Pearson Education, Inc.

[7] The NTRU Public Key Cryptosystem – A Tutorial. www.ntru.com/cryptolab/tutorials.htm.

[8] http://en.wikipedia.org/wiki/Huffman_coding.