International Journal of Computer Science and Network (IJCSN)
Volume 1, Issue 4, August 2012 www.ijcsn.org ISSN 2277-5420

MODIFIED MUTUAL AUTHENTICATION AND KEY AGREEMENT PROTOCOL BASED ON NTRU CRYPTOGRAPHY FOR WIRELESS COMMUNICATIONS

[1]Raj Kumar G.V.S.,[2]Naveen Kumar K, [3]Chandra Sekhar P, [4]Bhargav Nunna V. V. S., [5]Vinod Kumar B

[12345] Department of Information Technology, GIT,GITAM Univeristy,
Andhra Pradesh, Visakhapatnam-45, India

ABSTRACT

In this paper we implemented new methods of public keys exchange in the existing mutual authentication and key agreement protocol in wireless communication. The existing mutual authentication and key agreement protocol in wireless communications has been studied and the break points have been observed. We used "CS attack" to cryptanalyze the user's public key and obtain the private key. We overcame this break point by implementing DES encrypting algorithm along with NTRU encryption algorithm to improve the security. We also have studied the cryptanalyzation of NTRU encryption algorithm with various parameters and calculated the average window size to send and receive the public key.

Keywords: *NTRU-Number theory research unit, Public key cryptography, Lattice attacks, Wireless communications.*

1. Introduction

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. The key exchange problem is how to exchange whatever keys or other information are needed so that no one else can obtain a copy. Traditionally, this required trusted couriers, diplomatic bags, or some other secure channel.

Public-key cryptography refers to a cryptographic system requiring two separate keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the hypertext. Neither key will do both functions. One of these keys is published or public and the other is kept private. If the lock/encryption key is the one published then the system enables private communication from the public to the unlocking key's owner. If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key.

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 $R=Z[X]/(X^N-1)$ with convolution multiplication and all polynomials in the ring have integercoefficients and degree at mostN-1.$a=a_0+a_1X+a_2X^2+\ldots+a_{N-2}X^{N-2}+a_{N-1}X^{N-1}$.

2. NOTATIONS

AS: Authentication Server, CA: Certification Authority, PK_u: User's Public key, PK_{ca}: Certification Authority's Public key, TID_u: Temporary id of user, SK_u: Private keys of the user, N: Degree of the polynomial ring, K: No. of bits in a block used for

Cryptanalyzation, d_r: Degree of the random polynomial used to generate public key, CS attack: Copper Smith &Adi**S**hamir attack.

3.NTRU Encryption Algorithm:

NTRU is actually a parameterized family of cryptosystems; each system is specified by three integer parameters (N, p, q) which represent the maximal degree N-1for all polynomials in the truncated ring R, a small modulus and a large modulus, respectively, where it is assumed that N is prime, q is always larger than p, and p and q are coprime; and four sets of polynomials $\mathbf{L}_f$, $\mathbf{L}_g$, $\mathbf{L}_m$ and $\mathbf{L}_r$(a polynomial part of the private key, a polynomial for generation of the public key, the message anda blinding value,respectively),all of degree at most N-1.

Sending a secret message from Alice to Bob requires the generation of a public and a private 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 X^N-1 in *R*. The polynomial f, f ϵ L_f must satisfy the additional requirement that the inverses modulo q and modulo p (computed using the Euclidean algorithm) exist, which means that $f*f_p=1$(mod p) and $f*f_q=1$(mod q)must hold. So when the chosen **f** is not invertible, Bob has to go back and try another **f**. Both **f** and $\mathbf{f_p}$are Bob's private key. The public key **h** is generated computing the quantity $h= f_q*g$ (mod q).

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 applications 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**; so**r** must not be revealed by Alice. In addition to the publicly available information, Bob knows his own private key. Here is how he can obtain **m**: First he multiplies the encrypted message **e** and part of his private key **f,** the plain text **a** is obtained as a=f**.**e(mod q)

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 apply lattice basis reduction techniques to cryptanalyze the scheme, to discover either the original secret key, or an alternative secret key which is equally useful in decoding the cipher text. Furthermore, various attacks use the similar principles of CS attack. Hence we study and present new methods exchanging the private key on a secure channel.

4.TheExisting Authentication Protocol:

The formal novel mutual authentication and key agreement protocol based on the number theory research unit (NTRU) public key cryptography for wireless communications proposed by **Jiang Jun** and **HeChen**,is susceptible lattice based attack. "CS attack", new lattice based attack new hybrid meet in the middle and lattice reduction attack are some of the attacks that work.

The existing mutual authentication and key agreement protocol for wireless communication uses NTRU encryption for the key exchange between the user and server. The whole process is carried out in two phases

A) Initialization stage.
B) Real-Time exchange stage.

During the initialization stage, the certificates are distributed from CA to users and network authentication servers. In the initial stage the user chooses two random polynomial equations SK_u and g_u. PK_u is the public key that is computed according to NTRU key generation algorithm. Thus the user holds both public and private key. Now the user sends his public key along with his ID to CA.

$$PK_u + ID_u \longrightarrow \quad CA$$

The CA using his private key applies NSS Algorithm to generate has value of PK_u which is used as signature. A temporary ID is assigned to user denoted as TID_u and a timestamp Tu. The CA sends a certificate along with its public key PK_{ca}. The certificate consists of hash (PK_u), TID_u and T_u. The same information is sent to AS also. From now the second stage starts.

$$Hash(PK_u)+TID_u+T_u+PK_{ca} \longrightarrow User$$

Here, using CS attack in the procedure of man-in-the-middle attack the first stage can be penetrated by the attacker. It is explained as follows.

When the user sends his public key along with ID, the attacker captures the data from being delivered to CA, and CS attack is applied to find the user's private key or an alternative key that works as private key. Now the attacker forwards the public key along with the victim's user ID to CA.

Userattacker

$PK_u + ID_u$ PK_u+ID_u(fake) → CA

↓

SK_u

(find outs the private key)

Then CA sends user's certificate along with its public key. The attacker captures the data and prevents it from being delivered to the user. Now the attacker has victim's public key, private key and user certificate. With this, the attacker can pass the mutual authentication and get access to the network.

$$Hash(PK_u)+TID_u+T_u+PK_{ca} \not\rightarrow CA$$

Hence using CS attack algorithm in the man-in-the-middle attack procedure the attacker can get authenticated and get access to the network and other resources. Here not only CS attack but also other type of attacks new lattice based attack, new hybrid meet in the middle andlattice reduction attack can also be used as they are lattice based reduction attacks and promise to compromise the private key with their best results.

5. The Modified Protocol:

The proposed system would also work in two stages,

- **Stage 1:** Initialization stage
- **Stage 2:** Real-time exchange 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 private 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 known to the user and network AS. The encrypted public key is sent over the secure communication channel. The key is exchanged over the communication channel safely.

Hence the proposed system would accomplish the following tasks:

- Able to communicate the public key in secure manner.
- Increased security than the existing system.
- Implement new method for communicating the session key between the user and the network AS.

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.

T_{int}: Time for Initialization of lattice.

T_{red}: Time for the lattice reduction.

T_{one}: Time taken fo initialization of lattice lattice + Time taken for the lattice reduction.

T_{tot} : Total time taken to cryptanalyze the private key form the public key.

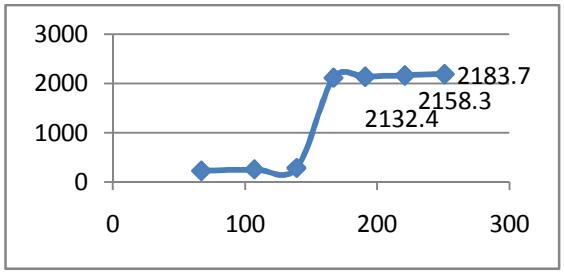
Table 1: Experimental Results

N	67	107	139	167	191	221	251
Q	61	101	131	157	181	211	239
d_r	19	31	40	48	55	63	72
T	24	49	75	102	124	151	177
T_{int}(sec)	5.2	73.8	352	1117.3	2499.7	5872	12287.6
T_{red}(sec)	1.9	17.9	57.9	144.1	195.4	317.2	460.8
T_{one}(sec)	7.1	91.7	409.9	1261.4	2695.1	6189.2	12748.4
T_{tot}(sec)	$2^{26.8}$	$2^{55.5}$	$2^{83.3}$	$2^{110.6}$	$2^{132.4}$	$2^{158.3}$	$2^{183.7}$

Table 2.The time taken for the cryptanalyzation of the DES encryption algorithm using Nomadic Genetic Algorithm

Expt. No	No. of keys found using NGA	Time taken forNGA in seconds
1	42	21
2	42	22
3	36	20
4	36	19
5	30	25
6	42	25
7	36	35
8	36	31
9	42	25
10	36	25

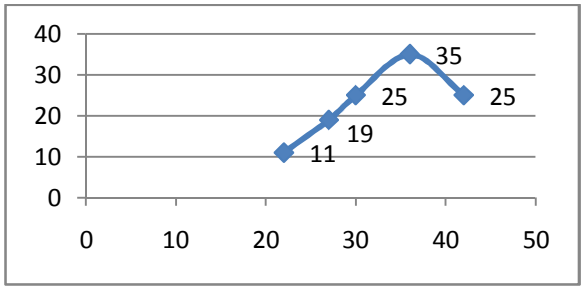
The maximum average time to cryptanalyze NTRU encryption algorithm and the maximum average time for cryptanalyzing the DES encryption algorithm for various parameter sets and observed the results and presented them in the following graphs.



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.

From the above graph, the maximum average time to cryptanalyze the NTRU Encryption algorithm is 2158.13 seconds, which is equal to $2^{11.07557}$ seconds. Let T_1 be the time required to cryptanalyze NTRU private key. i.e. $T_1 = 2^{11.07557}$.



Number of keys found on X-axis; Time in sec on Y-axis

Figure 2: Graph showing the relation between the time taken to cryptanalyze the number of keys used in DES encryption algorithm.

From the above graph the maximum average time to cryptanalyze DES encryption algorithm is 28.33 seconds, .i.e. $2^{4.82443}$ seconds. Let the average maximum time t_2 be the time taken to cryptanalyze DES encryption. Then $T_2 = 2^{4.82443}$ seconds.

T1+T2= 2186.63 seconds.

Thus the maximum time to cryptanalyze the modified mutual authentication and key exchange protocol for wireless communication is 2186.63 seconds. .i.e. the maximum time window to cryptanalyze is 2186.63 seconds that is equal to $2^{11.0945}$seconds.

Hence this window can be used as life time expiry for the connection request. If the user takes more than the window time, the session expires and the user has to communicate with the network AS once again.

7. Conclusion :

The formal mutual authentication and key agreement protocol can be compromised and the attacker can get access to the network in the disguise of a network user. The new system eradicated this by using DES encryption algorithm to encrypt the public key and send to the network AS and vice versa. Then it is decrypted by the receiver and hence the public key is exchange without

being exposed. Hence the possibility of the lattice based attack is reduced. And also by using the difference time stamp of time of the request to the time of exchange of the public key the attacked can be stopped. If the difference between the two timestamps is much larger compared to a threshold value then the request of the user is simply rejected as the time taken to cryptanalyze the des algorithm and then cryptanalyze NTRU encryption algorithm takes much time than just to cryptanalyze NTRU encryption. Hence the new mutual authentication and key agreement protocol for wireless networks is much more secure than the formal protocol.

8.Future Enhancement :

To increase the security by following this protocol, timestamp would be more useful. The window for the cryptanalyzing the NTRU public key and DES encryption key can be observed and the relation of the window required to find the public key is calculated and the efficient time limit can be found out for the session automatic expiry. Further new steps taken to authenticate the user if the user tries to reconnect to the network AS after the recent time out. For this purpose the details of recently visited and rejected user's data have to be saved.

References

[1] Abdullah M. Jaafar and AzmanSamsudin (2010), "A New Public-Key Encryption Scheme Based on Non-Expansion Visual Cryptography and Boolean Operation" IJCSI International Journal of Computer Science Issues, Vol 7, Issue 4, No 2, pp.1-10.

[2] Andrea Pellegrini, Valeria Bertacco and Todd Austin (2010), "Fault-Based Attack of RSA Authentication"

[3] Anoop MS (2007),"Public Key Cryptography Applications Algorithms and Mathematical Explanations".

[4] 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 and Methods for Mobility (DIAL M'98), Dallas, TX.

[5] Chunbo ma, Jun ao (2010), proposed "NTRU Based Group Oriented Signature and its Applications in RFID", Workshop Education Technology and Computer Science (ETCS), Vol 1, pp.166-169.

[6] Cohen A.E, Parhi, k.k, (2011), proposed "Architecture Optimizations for the RSA Public Key Cryptosystem" IEEE, Vol.11 , Issue 4, pp.24-34.

[7] Daewan Han, (2005), "A new lattice attack on NTRU Cryptosystem. Trends in mathematics, Information center for mathematical sciences", Vol.8, No 1, pp. 197-205.

[8] Dan boneh, Giovanni Di Crescenzo (2004), "Public Key Encryption With keyword Search", In proceedings of Eurocrypt 2004, LNCS 3027, pp. 506-522

[9] DavideAlessio, Marc Joye (2009),"A Simple Construction for Public-Key Encryption with Revocable Anonymity: The Honest-Sender Case" 9th ACM Workshop in Digital Rights Management, pp. 11-16.

[10] Don coppersmith, Adi Shamir, (1998), "Lattice attacks on NTRU ". In proceeding of Eurocrypt , LNCS, vol. 1233, Springer-verlag, pp. 52-61.

[11] Forsgren, H. Grahn, K. ; Karvi, T. ; Pulkkis, G (2010), proposed " Security and Trust of Public Key Cryptography Options for HIP", IEEE conference on Computer and Information Technology, pp.1079-1084.

[12] Hoffstein, J., Silverman, J.H., (2001), "NSS: The NTRU signature scheme". Proc. of Eurocrypt '01,Vol.2045, pp.211-228.

[13] Hoffstein, J., Silverman, J.H., (2001), "NTRU: A Ring-Based Key Cryptosystem".

[14] Hoffstein, J.,Silverman, J.H., (2002), "Optimizations for NTRU. Public-Key Cryptography and Computational Number Theory",DeGruyter.

[15] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Piper, Joseph H. Silverman. "Hybrid lattice reduction and meet in the middle resistant parameter selection for NTRU encrypt". NTRU Cryptosystems Inc.

[16] Jerry Crow (2003), "Prime Numbers in Public Key Cryptography",This is a paper from the SANS Institute Reading Room site.

[17] Jha R, sainiA.k, (2011), "A Comparative Analysis & Enhancement of NTRU Algorithm for Network Security and Performance Improvement". Conference in Communication Systems and Network Technologies, pp.80-84.

[18] Jiang Jun, HE Chen, (2004),"A novel mutual authentication and key agreement protocol base on NTRU cryptography for wireless communications", A Journal of Zhejiang University SCIENCE, ISSN 1009-3095,pp. 399-404.

[19] JohannesBuchmann, ChristophLudwig."Practical lattice basis sampling reduction". Proceedings ANTS'06 Proceedings of 7thInternational conference of Algorithmic Number Theory.

[20] Jon Callas (2005),"Identity-Based Encryption with Conventional Public-Key Infrastructure"

[21] MihirBellare, Alexandra Boldyreva, Silvio Micali (2000),"Public-key Encryption in a Multi-User Setting: Security Proofs and Improvements", A preliminary version of this paper appears in Advances in cryptology EUROCRYPT'00,Lecture Notes in Computer Sciences Vol.1087.

[22] Na Zhao, shenghuisu, (2011), "An Improvement and a New Design of Algorithms for Seeking the Inverse of an NTRU Polynomial".conferencce on CIS, pp. 891-895.

[23] Nick Howgrave-Graham (2007)."A hybrid lattice-reduction and meet-in-the-middle attack against NTRU",proceedings of 27th annual international cryptology conference on advances in cryptology.

[24] Ray A. Perlner, David A. Cooper (2009), "Quantum Resistant Public Key Cryptography", Proceedings of the 8th symposium on Identity and Trust on the Internet.

[25] Ronald Cramer, Victor Shoup (2003),"Design and Analysis of Practical Public Key Encryption Schemes Secure against Adaptive Chosen Cipher textAttack",SLAM Journal of computing Vol.33,pp. 167-226.

[26] Singh S (2005)**,"**Analysis and implementation Public Key Cryptosystem based on Boolean Satisfiability problem", IEEE 7th Malaysia International Conference on Communication.

[27] Whitfield Diffie and Martin Hellman (1976), "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol.22, No. 6, pp. 644-654.

[28] S.SivaSathya, T.Chithralekha and P.AnandaKumar (2010)," Nomadic Genetic algorithm for cryptanalyzation of DES 16". International Journal of Computer Theory and Engineering, Vol. 2, No. 3, June, pp.1793-8201.