Authentication Protocol using MYK-NTRUSign Signature Algorithm in Wireless Network Environment

Aihan Yin
School of Information Engineering, East China Jiaotong University, Nanchang 330013, China
Email: yinaihan@126.com

Hongchao Liang, and Ming Zhu
School of Information Engineering, East China Jiaotong University, Nanchang 330013, China
Email: {mr_lianghc, zhuming061104269}@163.com

***Abstract*—In this paper, we propose a new bidirectional authentication and key agreement protocol based on the MYK-NTRUSign signature algorithm. The AES encryption algorithm and hash techniques were adopted to build our protocol. To implement the mutual authentication and session key agreement, the proposed protocol includes two phases: namely initial phase and mutual authentication with key agreement phase. As the MYK-NTRUSign signature algorithm is applied, our protocol not only can overcome the security flaws of authentication protocols based on secret-key, but also support greater security attributes and lower computational complexity in comparison with currently well-known public key based wireless authentication schemes.**

***Index Terms*—MYK-NTRUSign Signature Algorithm; AES Encryption; Key Agreement; Bidirectional Authentication**

I. Introduction

Wireless communications is advancing rapidly in recent years. After 2G (e.g. GSM) widely deployed in the world, 3G mobile communication systems are spreading step by step in many areas. At present, some countries have already launched investigations beyond 3G (B3G) and 4G. Due to the openness of the wireless communication network, sharing of communication channels, network protocol security, the diversity of network attack means of incomplete, there is a huge security threat, which make the wireless communication security problem more and more attention.

To solve the security problems, cellular networks such as GSM and UMTS all employ the symmetric key algorithms (e.g. A5 and Kasumi) to implement the authentication and the session keys agreement before the subscriber is authorized to access the network. Because of wireless LAN (WLAN), the WEP (Wired Equivalent Privacy) protocol based on symmetric key algorithm RC4 is specified. However, some authentication mechanisms based on symmetric cryptosystem for wireless access control are adopted in consideration of the performance, the security flaws are obvious. For instance, the International Mobile Subscriber Identity (IMSI) used in cellular networks may be transmitted in plaintext during the authentication. It leads to a passive attacker in a position to eavesdrop the user's identity and locate the user easily. In addition, the shared secret key's management and maintenance will result in scalability problem when users increase in number [1].

Some public key based authentication protocols specifically designed for wireless networks have been proposed in recent years to overcome the security flaws mentioned above. Among them, the well-known authentication and key agreement protocol appropriate for wireless networks on the basis of elliptic-curve cryptography techniques was ASK-WAP [2] and UAP[3]. Even though the protocol reduces to some extent computational complexity on the user side by using elliptic curve cryptography (ECC) algorithm, the server just verify the user’s identity legitimacy and the server is not authenticated to the user. So it does not really achieve the bidirectional authentication.

NTRU (Number Theory Research Unit) public key cryptosystem is a kind of very promising public key cryptography scheme. The attractive advantages of NTRU are its encryption/decryption speed, signature/verification speed and the ease of creating public-private key pairs while providing high security level [4]-[7]. NTRU as a new public cryptosystem was first presented by Hoffstein [8]-[11]. It is a ring-based cryptosystem operating in polynomial ring Z[X]/(xN-1) where N is the security parameter. Then, researchers have proposed the NSS, R-NSS and NTRUSign algorithm [12]-[15]. However, NSS and R-NSS algorithm has been breached. In NTRUSign algorithm, Signers use the private key to generate plaintext closest vectors, the vectors are NTRU lattice, and the vector as plaintext signature. Min et al. [16] proposed a NTRUSign algorithm of ductility attack methods: an attacker by active eavesdropping, after receiving a message with the signature of the legal cases, able to forge a multiple legal signature of the message; At the same time give a repair

doi:10.4304/jnw.9.5.1139-1144

defects of ductility MYK-NTRUSign digital signature algorithm.[17] In this paper, we employed the MYK-NTRUSign signature algorithm [18][19] in combination with symmetric encryption algorithm (AES) and hash techniques (e.g. MD5 or SHA) to construct our new mutual authentication and session key agreement protocol appropriate for wireless communications.

The rest of this paper is organized as follows. Section 2 provides the description of MYK-NTRUSign signature algorithm and the proposed scheme is presented in Section 3. Security and performance analysis of our scheme is included in Section 4. Finally, we draw some concluding remarks in Section 5.

II. Description of MYK-NTRUSign Algorithm

In this section, we briefly describe the MYK-NTRUSign digital signature scheme. The security of MYK-NTRUSign scheme is based on the approximately closest vector problem in a certain lattice, called NTRU lattice. The basic idea is as follows: The signer's private key is a short basis for an NTRU lattice and his public key is a much longer basis for the same lattice.

The MYK-NTRUSign digital signature scheme works as follows:

A. System Parameters

1. *N*: a (prime) dimension.
2. *q*: a modulus, *df*, *dg*: key size parameters.
3. *NormBound*: a bound parameter of verification.

B. Key Generation

A signer creates his public key *h* and the corresponding private key (*f*, *g*, *F*, *G*) as follows:

1. Select binary polynomials *f* and g with *df* 1's and *dg* 1's, respectively.
2. Compute small polynomials (*f*, *g*) satisfying $f{*}G-g{*}F=q$.
3. Compute the public key $h = f^{-1}{*}g$ (mod q).

C. Signing Step

A signer generates his signature *s* on the digital document *D* as follows:

1. Obtain the polynomials (m_1, m_2) mod *q* for the document *D* by using the public hash function.
2. Compute

$$G{*}\mathrm{m}_1-F{*}\mathrm{m}_2=A+q{*}B \tag{1}$$

$$-g{*}\mathrm{m}_1+f{*}\mathrm{m}_2=a+q{*}b \tag{2}$$

where *A* and *a* have coefficients between -*q*/2 and *q*/2.

3. Compute:

$$s' \equiv f{*}B+F{*}b \pmod{q} \tag{3}$$

4. Compute:

$$t' \equiv g{*}B+G{*}b \pmod{q} \tag{4}$$

if $\|\mathrm{s}'-\mathrm{m}_1\|^2+\|\mathrm{t}'-\mathrm{m}_2\|^2 > \mathrm{Normbound}^2$,

$$\mathrm{s}=\mathrm{s}'+\sum_{\mathrm{i}=0}^{\mathrm{N}-1}\mathrm{x}^{\mathrm{i}} \pmod{q} \tag{5}$$

else

$$\mathrm{s}=\mathrm{s}'-\mathrm{s}'_{\mathrm{N}-1}\sum_{\mathrm{i}=0}^{\mathrm{N}-1}\mathrm{x}^{\mathrm{i}} \pmod{q} \tag{6}$$

5. The polynomial *s* is the signature on the digital document *D* for the public key *h*.

D. Verification Step

For a given signature *s* and document *D*, a verifier should do the following:

1. Hash the document D to recreate (m_1, m_2).
2. With the signature s and public key *h*, compute the corresponding polynomial.

$$t \equiv s{*}h \pmod{\mathrm{q}} \tag{7}$$

if $\|\mathrm{s}-\mathrm{m}_1\|^2+\|\mathrm{t}-\mathrm{m}_2\|^2 > \mathrm{Normbound}^2$, refuse to sign.

3. If $\mathrm{s}_{\mathrm{N}-1} \neq 0$, $\mathrm{s}' = \mathrm{s}-\sum_{\mathrm{i}=0}^{\mathrm{N}-1}\mathrm{x}^{\mathrm{i}} \pmod{\mathrm{q}}$ and if $||\mathrm{s}'-\mathrm{m}_1||^2+||\mathrm{t}'-\mathrm{m}_2||^2 \leq \mathrm{Normbound}^2$, refuse to sign.
4. Receive the signature.

A valid signature demonstration that the signer knows a lattice point that is within Normbound of the message digest vector *m*. The designers recommend that the suggested parameters (*N*, *q*, *df*, *dg*, *Normbound*) = (251, 128, 73, 71, 300) offers an equivalent security as 1024 bit RSA.

III. The Proposed Schemed

A. Notations

TABLE I. The meaning of symbolic in authentication process

Symbolic name	Symbolic meaning
E(X)	Encryption of X by using symmetric encryption algorithm
ID_X	X's actual identity
DID_X	Dynamic identity of X
a||*b*	Concatenation of a and b
PK_A	MYK-NTRUSign based public key polynomial in A
SK_A	MYK-NTRUSign based private key polynomial in A
K_{XY}	Symmetric secret key shared by X and Y
R_X	Random number generated by X
S_X	MYK-NTRUSign based signature generated by X
T_X	Expiration date of certificate X
h(X)	Hashed value of X
C_X	Certificate of X

In this paper, in order to enhance the safety of the network, a new mutual authentication and session key agreement scheme is introduced. Note that the certifying authority (CA) is responsible for creating and distributing certificates to the user and server in our protocol. The certificates contain the public key of user or server, the certificate's expiration date and the unique identification. Besides, the certificates should be signed by using his own private key. The proposed scheme has two phases: system initialization phase and mutual authentication with key agreement phase as described below.

B. System Initialization Phase

The CA first generates his public-secret key pair according to the MYK-NTRUSign signature algorithm. Thus the CA publishes his public key $PK_{CA}=h$, and stores private key SK_{CA}=(f_{CA}, g_{CA}, F_{CA},G_{CA}). For the user, the initialization process is as follows:

Step 1. The user send (ID_U, PK_U) to CA.

Step 2.CA selects a random value X_U and T_U, in which T_U is certificate expiration date. Then computes DID_U=$ID_U \oplus X_U$ and m =(PK_U||DID_U||T_U).

Step 3. CA generate the user's certificate C_U according to the MYK-NTRUSign signature algorithm and transmit message (C_U, DID_U, T_U, PK_{CA}) to user through the safe channel.

Like the initial process of user side mentioned above, server also gets his certificates C_S, DID_S, T_S and PK_{CA} from CA.

C. Mutual Authentication with Key Agreement Phase

After the initialization procedures are completed, the real authentication can be executed. Fig. 1 shows the detailed real-time execution procedure.

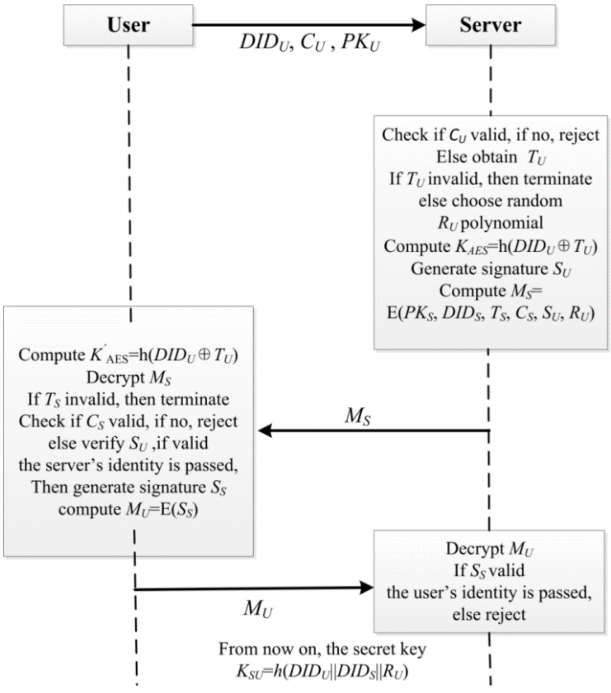
User
Server
DID_U, C_U , PK_U
Check if C_U valid, if no, reject
Else obtain T_U
If T_U invalid, then terminate
else choose random
R_U polynomial
Compute K_{AES}=h($DID_U \oplus T_U$)
Generate signature S_U
Compute M_S=
E(PK_S, DID_S, T_S, C_S, S_U, R_U)
Compute K'_{AES}=h($DID_U \oplus T_U$)
Decrypt M_S
If T_S invalid, then terminate
Check if C_S valid, if no, reject
else verify S_U ,if valid
the server's identity is passed,
Then generate signature S_S
compute M_U=E(S_S)
M_S
Decrypt M_U
If S_S valid
the user's identity is passed,
else reject
M_U
From now on, the secret key
K_{SU}=h(DID_U||DID_S||R_U)

Figure 1. Mutual authentication with key agreement protocol

Step1: Initially, the user U send his certificate C_U combined with public key PK_U, dynamic identity DID_U to the server.

Step2: After having received the messages in Step 1, the server S first verifies the U's certificate C_U according to MYK-NTRUSign algorithm. If this checks, the server can obtain T_U from the certificate C_U and checks whether T_U is valid or not. If it is not, the authentication process will be terminated. Otherwise, the server selects a random value R_U and computes temporary secret key K_{AES}=h($DID_U \oplus T_U$). The server S also computes m_U=h(PK_U||DID_U||T_U) and make modulo q arithmetic to get (m_1,m_2). Then S computes $G_s \oplus m_1$-$F_s \oplus m_2$=A+$q \oplus B$,-$g_s \oplus m_1$+$f_s \oplus m_2$=a+$q \oplus b$, where $-\frac{q}{2} \ll A, a \ll \frac{q}{2}$. Afterwards, the server calculates his signature S_U by using the MYK-NTRUSign algorithm. Subsequently, the server encrypts (PK_S, DID_S, T_S, C_S, S_U, R_U) as M_S through AES encryption algorithm. At last, the server sends M_S to user.

Step3: Upon receiving the message M_S from server, the user computes K_{AES}'=h($DID_U \oplus T_U$). Then it will decrypt M_S by using the secret key and checks the T_S. And if it is expired, the authentication will be terminated. And then he verifies the server's certificate C_S. If C_S is valid, the user verify sever's signature S_U. Then according to the MYK-NTRUSign, the user checks whether S_U is valid or not. If it is passed, he ensures the server is correct. In order to judge the correctness of user, the user calculates his signature S_S by using the MYK-NTRUSign algorithm, and sends the encrypted signature $\mathrm{S_S}$ with symmetric key $\mathrm{K'_{AES}}$ as M_U to the corresponding server.

Step4: After having received the encrypted data, the server decrypts M_U to obtain the U's signature S_S. Then, the server verifies the U's signature S_S through MYK-NTRUSign signature algorithm. If it is passed, the mutual authentication between the user and server is completed. Then on both sides, the secret session key K_{SU} can be achieved by computing the hashed value of the concatenation of DID_U, DID_S and R_U from the following equation.

$$K_{SU}= \mathrm{h}(DID_U||DID_S||R_U) \tag{8}$$

IV. Security and Performance Evaluation of the Proposed Scheme

In this section, we analyze that the proposed scheme can withstand all related security attacks and can work correctly. The security of our scheme is based on the hard problem of polynomial factorization in polynomial ring. In addition, the proposed scheme is more efficient in terms of Performance than the related schemes.

A. Security Analysis

Here we mainly discussed and analyzed the security attributes of the proposed scheme on various known cryptographic attacks and then provides a comparison of our scheme with the related schemes.

(1) Mutual authentication and session key agreement

The proposed scheme provides the mutual authentication to keep faith between the user and the server. In our scheme, it decrypts the received data by using the secret key K_{AES}, which is unknown to the attacker. First, the user authenticates the server and then server authenticates the user using the MYK-NTRUSign signature algorithm. After the authentication process, the user and the server possess the common session key, which is free from known session information attack. Therefore, the mutual authentication and session key agreement is done safely to the proposed scheme.

(2) The session key freshness

In the proposed scheme, the server and the user compute the session key K_{SU}=h(DID_S||DID_U||R_U). As the dynamic identity DID_U hides the user's real identity and is changed with different users. Besides, the random number R_U is randomly generated in a communication. So the session key K_{SU} is freshness.

(3) Perfect forward secrecy and Known key security

A protocol is called Perfect forward secrecy, if compromise of the two private keys of the participating entities does not affect the security of the previous session keys. Assume that the private key and public key of user and sever are leaked to an adversary. As the random value X_U is unknown to the adversary, it can't work out the legal signature. The adversary also cannot obtain the previous session keys because of the R_U is unknown to the adversary. Thus the perfect forward secrecy is preserved in the proposed scheme. At the same time, even if the secret key K_{AES} is leaked or cracked, but R_U is randomly generated in the authentication process, so it can't deduced the session key. Therefore, the protocol is known key security.

(4) Nonrepudiation

Our scheme is based on MYK-NTRUSign digital signature algorithm. It need to verify the server's signature S_S and the user's signature S_U. So the new scheme has the sign nonrepudiation.

(5) Confidentiality

In the communication process, our scheme will generate a secret key K_{AES}, which is used for encrypting the transmission data and the secret key K_{AES} is different with different users. In addition, the session key $K_{SU} = \mathrm{h}(DID_S||DID_U||R_U)$ and the hash function is one-way security. It can ensure the confidentiality during the process of communication.

(6) User anonymity

In our protocol, the user' dynamic identity DID_U hides the user's real identity. Therefore, our scheme has the identity anonymity.

(7) Meet-in-the-Middle Attack

As the proposed scheme preserves the identity anonymity, so the attacker cannot obtain the user's identity ID_U. Thus the proposed scheme can prevent all kinds of meet-in-the-middle attack.

Further, the security comparison of the proposed scheme with previous authentication schemes is summarized in Table 2 .From the Table 2, it is clear that the proposed scheme provides more security attributes than the other schemes. Therefore, the proposed scheme is more efficient, secure and practical for the users in wireless networks.

TABLE II. COMPARISON AGAINST DIFFERENT SECURITY PROPERTIES

SCHEMES			
Security attributes	ASK-WAP	UAP	PROPOSED
User anonymity	Yes	Yes	Yes
Nonrepudiation	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes
Meet-in-the-Middle Attack	No	Yes	Yes
Perfect forward secrecy	No	Yes	Yes
Known key security	No	Yes	Yes
Mutual authentication	No	No	Yes

B. Performance Analysis

In this section, we compare our scheme with the other schemes in terms of performance. First of all, MYK-NTRUSign digital signature algorithm is based on NTRUSign algorithm, which inherited the speed advantage. In the same security strength, three kinds of cryptographic algorithms performance comparison is as follows:

TABLE III. COMPARISON THE PERFORMANCE OF DIFFERENT SIGNATURE ALGORITHM.

Process	NTRUSign (251)	ECDSA (2^{162})	RAS (1024)
Key generated rate (μs)	9761	1624	2090509
Signature rate (μs)	500	1424	9090
Certification rate (μs)	303	2183	781

From Table 3, we can know that NTRUSign key generation algorithm is slower, and the signature verification faster speed. However, our proposed scheme is based on MYK-NTRUSign algorithm, the key generation is in the initialization phase, signature and verification are certified segment. Therefore, the scheme has the advantages of fast certification.

In order to make better analysis on the performance analysis, we have three algorithms (ASK-WAP, UAP, PROPOSED) simulated respectively. Simulation environment is STM8L151 sensor with ultra-low power consumption and super processor which is special good at processing a large of data, the matching simulation software is Tiny-OS system that can run automatically on the processor ROM.

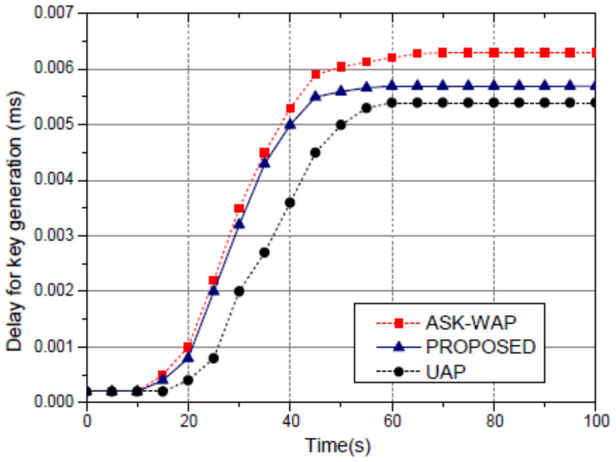

Figure 2. Comparison of key generation delay curve

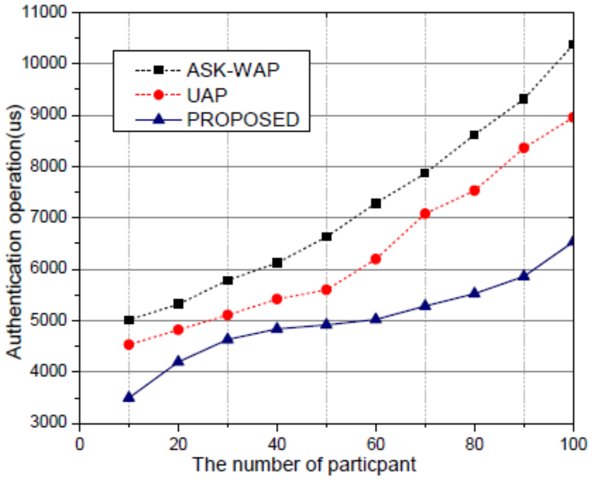

Figure 3. Comparison of authentication operation

Obviously, figure 2 shows the results of delay for key generation. This is because the MYK-NTRUSign public-private key pair of bytes is bigger than the number of bytes of ECDSA public-private key pair, need more in the process of transmission bandwidth, time delay is also relatively increase. Figure 3 has shown that with the increasing node scale the authentication operation for three schemes present rising tendency, the slope of curve we proposed scheme just has increase slightly relative to the other schemes. Moreover, the computation costs and number of communication rounds of our scheme is less than those of the other schemes.

Generally speaking, our scheme not only provides mutual authentication but also supports a session key agreement. Moreover, our protocol does not need to perform the certificate computation. From the above descriptions, we conclude that our protocol is more efficient and practical than the related schemes for wireless communication.

V. Conclusion

In this paper, we have proposed a new bidirectional authentication and key agreement protocol using the related signature algorithm. Combined with the symmetric secret key algorithm and hash techniques, we have shown that the proposed protocol offers key agreement and mutual authentication. According to the comparisons in Section 4, the proposed protocol is more efficient and practical than some recently proposed protocols. It can not only removed the security flaws of some recently proposed schemes, but also satisfy the request of wireless communication conditions. Thus, the proposed scheme is efficient and usable for wireless communication.

Acknowledgement

This work was partially supported by the National Science Foundation of China under grants 61262079 and Provincial Natural Science Foundation of Jiangxi under grants 20114BAB201026.

References

[1] JIANG Jun, HE Chen, "A novel mutual authentication and key agreement protocol based on NTRU cryptography for wireless communications," *Journal of Zhejiang University SCIENCE*, 6(2005) pp. 399-404.

[2] Mangipudi K, Malneedi N, Katti R, et al, "Attacks and solutions on aydos-savas-koc's wireless authentication protocol," *IEEE Communication Society, Golbecom*, 2004 pp. 2229-2234.

[3] Abdel Alim Kamal, Amr M. Youssef, "Fault analysis of the NTRUSign digital signature scheme," *Cryptography and Communications*, 4(2012) pp. 131-144.

[4] Hoffstein J, Silverman J H, "NTRU: a ring based public key cryptosystem," *Springer-Verlag*, 1998, pp. 267-288.

[5] Le, Xuan Hung, et al, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare." *Journal of Networks 6.3* (2011) pp. 355-364.

[6] Hoffstein J, Silverman J H, "NSS: the NTRU signature scheme," *Proc of Euroerypt'01*, 2045 (2000) pp. 211-228.

[7] Hoffstein J, Pipher J, Silverman J H, "Enhanced encoding and verification methods for the NTRU signature scheme [EB/OL]," [2009-12-16]. http://www.ntm.Com/technology/tech.technical.htm.

[8] Wang, Ding, et al, "Secure Password-based Remote User Authentication Scheme against Smart Card Security Breach," *Journal of Networks 8.1* (2013): 148-155.

[9] Hoffstein Jeff, Nick Howgrave-Graham, Jill Pipher, William Whyte, "Practical Lattice-Based Cryptography: NTRU Encrypt and NTRUSign," *The LLL Algorithm*, 2010, pp. 349-390.

[10] Junping Yao, Zefeng Dong, Xinshe Li, "A Novel Group Signature Scheme Based on NTRU," *Computational Intelligence and Security (CIS)*, 2011, pp. 861- 864.

[11] Krontiris, Ioannis, and Tassos Dimitriou, "Scatter–secure code authentication for efficient reprogramming in wireless sensor networks," *International Journal of Sensor Networks 10.1* (2011) pp. 14-24.

[12] Yanfang Wu, Zheng Huang, Jie Zhang .et.al. "A lattice-based digital signature from the Ring-LWE," *Network Infrastructure and Digital Content (IC-NIDC)*, 2012, pp. 646-651.

[13] Chunbo Ma, Jun Ao, "NTRU Based Group Oriented Signature and its Applications in RFID," *Education Technology and Computer Science (ETCS)*, 2012, pp. 166 - 169.

[14] Bu Shanyue, Chen Liqing, "A New Key Management Protocol for Wireless Sensor Network," *Computer Science & Service System (CSSS)*, 2012, pp. 991-994.

[15] Kamal, A.A, Youssef, A.M, "A Scan-Based Side Channel Attack on the NTRU Encrypt Cryptosystem," *Availability, Reliability and Security (ARES)*, 2012, pp. 402-409.

[16] Ron Steinfeld, San Ling, Josef Pieprzyk, et.al. "NTRU CCA: How to Strengthen NTRU Encrypt to Chosen-Cipher text Security in the Standard Model," 7293 (2012) pp. 353-371.

[17] Laiha Mat Kiah, "A novel peer-to-peer SMS security solution using a hybrid technique of NTRU and AES-Rijndael," *Scientific Research and Essays*, 22 (2010) pp. 3455-3466.

[18] Jha, R. Saini, A.K, "A Comparative Analysis & Enhancement of NTRU Algorithm for Network Security and Performance Improvement," *Communication Systems and Network Technologies (CSNT)*, 2011, pp. 80 - 84.

[19] Jingguo Bi, Qi Cheng, "Lower Bounds of Shortest Vector Lengths in Random NTRU Lattices," *Theory and Applications of Models of Computation*, 7287 (2012) pp. 143-155.

Aihan Yin is a Professor of Information Engineering department at East China Jiaotong University in Jiangxi, China, since 2003. She received the Bachelor's degree from TIANJIN University in 1984, and the Master's degree from the Nanjing University of Aeronautics and Astronautics in 2005, respectively. In 2011, she obtained her PhD at Huazhong University of Science and Technology. Her research focuses on Optic Communication Technology, Bandwidth Access Network, Communication Network Protocol, Wireless Communication Technology, Signal Processing and Optoelectronic Technique.

Hongchao Liang is a postgraduate student at East China Jiaotong University in Jiangxi, China. He received his bachelor

in Communication engineering department at East China Jiaotong University in Jiangxi, China. His interests include authentication and encryption technology in the wireless network.

Ming Zhu is a postgraduate student at East China Jiaotong University in Jiangxi, China. He received his bachelor in electronic information engineering department at Yangzhou University in Yangzhou, China. His interests include authentication and encryption technology in Optic Access network.