NTRU based group oriented signature

Chunbo Ma and Jun Ao
School of Information and Communication,
Guilin University of Electronic Technology, Guilin, Guangxi, 541004, P. R. China

***Abstract*—In order to prevent illegal tracking and stealing personal or cargo information, the authentication services should be provided for the tags to identify a Reader. A NTRU based signature scheme is proposed in this paper, which meets the demand for a group of tags to quickly and securely identify a Reader in RFID system. In our scheme, only the tag in specified group can verify the reader's message. Because of fast operation, easy key generation and limited source occupied, our signature is very suit for the RFID systems.**

Keywords- NTRU, group-oriented, RFID

I. INTRODUCTION

RFID is an auto and contactless authentication technique, which can be widely used in many engineering fields such as provision chain management, smart machine, and electronic paying system. However, the RFID technique has raised many serious privacy and security problems during the RFID technology provides us huge business and operation convenience. Currently, the security issues of RFID are manly manifested in illegal tracking, stealing personal or cargo information and forging RFID [2]. In the context of RFID it is very important for the system security that the tags can distinguish authorized readers from otherones.

Currently, many authentication algorithms used in RFID systems are based on symmetric crypto. Due to the severely constrained memory and processing capabilities in RFID, the public key cryptography has not been used for a long time. However, as the development of cryptography and the enhanced capability of storage and computing, some novel and more efficiency public key cryptography are attracting people's attention. NTRU is such a promising crypto system that its fast computing and small storage requirement make very different from any other public key crypto system. Hoffstein et al. [3] first proposed NTRU crypto system in 1996, and designed a very efficient signature scheme called NTRUSign [4] in 2003. This signature scheme can be used in authenticating for two communicating parties in NTRU based systems.

To withstanding stealing personal or cargo information, the Tags are been required to authenticate the readers. Assume that a reader will read the information of a volume of cargo, namely the reader will scan very tag and get tag's information. Considering the security issues, each tag will authenticate the reader and ensure that the reader is what it claims to be. Two methods can be used in above scenario. One method is that reader can sign a message for each tag to declare its identity. It means that the reader will generate amount of signatures to meet the requirement. Obviously, the efficiency of this method is very low. Of course, if a reader can sign a message for all the tags, then the reader's burden will alleviate a lot. Motivated by this method, an NTRU based group oriented signature is designed in this paper. This signature scheme is promising in providing efficient and fast authentication services in above scenario.

II. RELATED WORKS

RFID-based identification is an emerging technology which requires authentication as a cryptographic service [5]. This property can be achieved by symmetric as well as asymmetric primitives. Previously known work considered only symmetric-key algorithms e.g. AES [6]. The suitability of Public-Key (PK) algorithms for RFID is an open research problem as limitations in costs, area and power are quite severe. A few papers [7]discussed feasibility of ECC based PKC on RFID-tags.

NTRU [3] is one of the fastest public key crypto systems we have even know. Its security is based on the shortest vector problem (SVP). As we all know, R-NSS [9] and NTRUSign [4] are two typical signatures which are based on NTRU crypto system. R-NSS is vulnerable to the attack proposed by Gentry and Szydlo [10]. This attack integrating the GCD and statistical method can recover the private key with amount of valid signatures. The reason that their attack methods can success is that the values generated by R-NSS are the multiple of single private key. The signature of NTRU, however, is not the multiple of single private key, but the linear combination of two private keys. The coefficients of the combined polynomial approximately obey uniform distribution.

The designated verifier signature first proposed by Jakobsson, Sako and Impagliazzo in 1996 [11] and followed by many research results. Jakobsson et al. extended the designated signature to multiple designated verifier signature.

Ma et al. [12] designed a group-oriented encryption scheme. In such a scheme, anyone can encrypt a message using the group public key and distribute the ciphertext to the designated group.Any member in the group can independently decrypt the ciphertext via his private key. However, two valid users in this scheme can cooperate with each other to obtain a new and valid private key that can be used by any user. In other words, the scheme is vulnerable to colluding attack.

Ma et al. present the concept of group inside signature [13]. In their scheme, any one in the same group with the signer can verify the signature generated by the signer. This type of signature can be transmitted by broadcast on the Internet. Embedding a group tab in the private key is the key skill to construct this signature. With this method, the efficiency of signing a message is improved enormously. This signature is corresponding to the first model.

III. Background

NTRU is a public key crypto system which is based on a hard mathmetrical problem of finding short vectors in certain lattices. We then first define a Lattice as follows.

Definition1. Assume that $b_1, b_2, \cdots, b_n$ are n linearly independent vectors, then the lattice is defined as

$$L = \{b_1 \cdot x_1 + b_2 \cdot x_2 + \cdots + b_n \cdot x_n\} = \sum_{i=1}^{n} b_i Z .$$

Where x_j is random number. We say $b_1, b_2, \cdots, b_n$ is a base of lattice L, and n is the dimension or rank of the lattice. For the sake of simplicity, we define $B = [b_1, b_2, \cdots, b_n]$. The lattice L actually is a matrix that consists of row vector b_j. In addition, we denote B as the generator matrix of lattice L, and L(B) as lattice L.

The signature we proposed in this paper is based on approximating Closest Vector Problem (CVP). Here is the definition of CVP.

Definition2. CVP (the Closest Vector Problem) [14]. Let $\| \ \|$ is a norm. Given a lattice L(B) and the target $t \in R^m$, finding a vector x in the lattice such that $\|x - t\|$ is the minimal value. We therefore express the CVP as follows.

$$L - CVP = \left\{ \left(m, n, b_1, b_{2,} \cdots, b_n, t\right) \middle| \begin{array}{c} m, n \in N, b_1, b_{2,} \cdots, b_n \in Z^m, t \in R^m \\ \exists x \in L\left(b_1, b_{2,} \cdots, b_n\right) \setminus \{0\} : \|x - t\| \le \|\omega - t\|, \forall \omega \in L \end{array} \right\}$$

IV. Group Oriented Signature

A. The scheme

As we have mentioned above, our signature scheme is designed for a group of Tags to authenticate a Reader. We define a set $U = (Tag_1, Tag_2, \cdots, Tag_n)$. Then our scheme can be expressed as that to the signature signed by the Reader, nobody outside the specified group U can independently verify the signature. The proposed scheme consists of following steps.

1) *Key Extract*

- To produce a private key pair for $Tag_i \in U$, KGC (Key Generating Centre) chooses two small polynomials f_i and g_i whose degree is no more than N-1. The definition of f_i and g_i can refer to paper [14].
- KGC chooses a random polynomial $h \in Z_q[x]/(x^N - 1)$, and then computes ε_i for Tag_i such that

$$h = F_q^i * g_i * \varepsilon_i \quad (1)$$

- KGC produces f_0 and g_0 for the Reader as he has done for Tag_i, and then computes ε_0 to meet following equality.

$$h = F_q^0 * g_0 * \varepsilon_0$$

The private key pair of the Reader is (f_0, g_0), and the corresponding public key is ε_0.

Here F_q^i is the inverse of f_i in the ring $\mathbf{Z}_q[x]/(x^N - 1)$, and ε_i is the public key of Tag_i. In addition, h is a secret value and will be destroyed after finishing above steps.

2) *Signing*

- Assume the Reader will sign the massage M. The first he should to do is transform the massage M with cryptographic one-way function into two polynomials (m_1, m_2), such that $m_1, m_2 \in \mathbf{Z}_q[x]/(x^N - 1)$.
- Computing two polynomials G_0 and F_0 to meet following equality.

$$G_0 * g_0 - F_0 * f_0 = q \quad (2)$$

About the generation of G_0 and F_0, one can refer to the NTRUSign digital signatures proposed by Hoffstein.

- Computing four polynomials a, b, A and B to meet following equality.

$$\begin{cases} F_0 * m_1 + G_0 * m_2 = A + q * B \\ g_0 * m_1 + f_0 * m_2 = a + q * b \end{cases} \quad (3)$$

- Signer Reader produces s as follows

$$s = f_0 * B + G_0 * b \pmod q \quad (4)$$

The signature on message M produced by Reader is $\sigma = (M, s)$, and then the signature will be sent to the specified group U by broadcasting.

3) *Verification*

After receiving Reader's signature, each member in group U (e.g. Tag_j) can verify the signature as follows.

- Computing (m_1, m_2) by using public cryptography one-way function and the massage M.
- Computing

$$t = \varepsilon_q^0 * h * s = \varepsilon_q^0 * F_q^j * g_j * \varepsilon_j * (f_0 * B + G_0 * b) \pmod q$$
$$= \varepsilon_q^0 * F_q^0 * g_0 * \varepsilon_0 * (f_0 * B + G_0 * b) \pmod q$$
$$= g_0 * B + F_0 * b \pmod q \quad (5)$$

Here, ε_q^0 is the inverse of ε_0 in the ring $\mathbf{Z}_q[x]/(x^N - 1)$.

- Computing the distance between (s, t) and (m_1, m_2), and check if the following inequality holds.

$\| (m_1 - s), (m_2 - t) \| \le NormBound$

If above inequality holds, the signature is valid, other wise failed.

B. Why signature works

We get the following equality with (2)

$$\begin{pmatrix} F_0 & g_0 \\ G_0 & f_0 \end{pmatrix}\begin{pmatrix} f_0 & g_0 \\ G_0 & F_0 \end{pmatrix} = \begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix} \quad (6)$$

Then, the equality (3) can be described as follows.

$$(m_1, m_2)\begin{pmatrix} F_0/q & g_0/q \\ G_0/q & f_0/q \end{pmatrix} = (A/q + B, a/q + b)$$

$$(m_1, m_2) = (A/q + B, a/q + b)\begin{pmatrix} f_0 & g_0 \\ G_0 & F_0 \end{pmatrix} \quad (7)$$

After receiving Reader's signature (M, s), Tag$_j$ computes (m_1, m_2) and deduces s from t, since the one-way function is known to all. To (s,t), we have

$$(s,t) = (B,b)\begin{pmatrix} f_0 & g_0 \\ G_0 & F_0 \end{pmatrix} \quad (8)$$

With equalities (7) and (8), we have

$$(m_1 - s, m_2 - t) = (A/q, a/q)\begin{pmatrix} f_0 & g_0 \\ G_0 & F_0 \end{pmatrix} \quad (9)$$

Since the coefficients of A/q and a/q are randomly distributed in $(-\frac{1}{2}, \frac{1}{2})$, then their central norm meet $\|A/q\| \approx N/12$ and $\| a/q \| \approx N/12$. In addition, we have

$$\| f_i \| \qquad \| g_i \| = O(\sqrt{N})$$

$$\| F \| \approx \| f_i \| \sqrt{N/12} \qquad \| G \| \approx \| g_i \| \sqrt{N/12}$$

Then we can get the distance between (s,t) and (m_1, m_2), i.e. the NormBound

$$\|(m_1 - s), (m_2 - t)\|^2 =$$

$$\|((A/q) * f_0 + (a/q) * G_0), ((A/q) * g_0 + (a/q) * F_0)\|^2$$

$$= \frac{c^2 N^3}{72}(1 + \frac{1}{N})$$

As Hoffstein et al.[4] pointed out, $\frac{c^2 N^3}{72}(1 + \frac{1}{N})$ is a smaller value. Therefore, Tag$_j$ can verify the validity of Reader's signature.

C. Comparison with NTRUSign

NTRUSign in model is point to point, in other words, only two participants to communicating with each other. Furthermore, it is a public verifiable signature, that means anyone has ability to verify a NTRUSign signature. However, the participants in our group oriented signature are all the members in the specified group, and nobody outside the group can verify the signature.

Because NTRUSign in algorithm design has a public key h, each user can compute $t = h * s$ and decide if $\| (m_1 - s), (m_2 - t) \| \le NormBound$ holds. However, in our scheme, h is a secret value and destroyed after key extraction. It means that only the member in specified group can compute $F_q^i * g_i * \varepsilon_i$ with his private key (F_q^i, g_i) and the corresponding public key ε_i. Nobody outside the group can perform such computing.

V. Security

The equality $h = F_q * g$ is used in NTRUSign to describing the relation between public key h and private keys f and g. Here, F_q is the inverse of f in the ring R. If an attacker wants to break the scheme by finding private key via public key h, its difficulty is equal to solving the CVP. However, in our scheme, under the situation of known the public key ε, an attacker even can't perform brute attack, because h is a secret value in the equality $h = F_q * g * \varepsilon$ and it is very difficulty for the attacker to establish the relation between ε and $F_q * g$.

Given two vectors m_1 and m_2, computing s and t to meet $\| (m_1 - s), (m_2 - t) \| \le NormBound$ is a CVP. Actually, our scheme and NTRUSign both are based on approximating CVP, since the norm of (F, G) is not small enough. But Dinur [14] has proved that approximating CVP is also an intractable problem.

VI. Conclusion

The authentication technique is a crucial method to prevent Tag from been illegal stolen or forged in RFID system. Because of the constrained computing capacity, storage and power in RFID, some authentication techniques based on traditional public key can not be used. Currently, NTRU based crypto schemes are been considered as a promising method to protecting the information security in some source constrained scenarios. In this paper, we design a NTRU based group oriented signature for the broadcasting scenarios in RFID system. Actually, our scheme stems from NTRUSign, and the efficiency and security are similarly to it.

References

[1] W. Sean and L. Thomas. Automatic identification and data collection technologies in the transportation industry: BarCode and RFID. Technology report 2001.

[2] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda. RFID systems: A Survey on Secuirty Threats and Proposed Solutions. In Proceedings of International Conference on Personal Wireless Communication (PWCA06), LNCS 4217, 2006.

[3] Hoffstein J., Pipher J., Silverman J. H.. NTTU: A new high speed public key cryptosystem. In Proceedings of the algorithm number theory. LNCS 1423. Springer-Verlag, 1998: 267-288.

[4] Hoffstein J. Howgrave-Graham N, Pipher J., Silverman J. H., Whyte W.. NTRUSign: Digital signatures using the NTRU lattice. In Proceedings of the CT-RSA'03. LNCS 2612. Springer-verlag, 2003: 122-140.

[5] International Organization for Standardization. ISO/IEC 18000-3. Information Technology AIDC Techniques-RFID for Item Management. March 2003.

[6] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems using the AES Algorithm. In Proceedings of 6th International Workshop on Cryptographic Hardware in Embedded Systems (CHES), LNCS 3156, Springer-Verlag, 2004: 357-37.

[7] P. Tuyls and L. Batina. RFID-tags for Anti-Counterfeiting. Topics in Cryptology-CT-RSA 2006, LNCS 3860, Springer-Verlag, 2006:115-131.

[8] Coppersmith D., Shamir A..Lattice attacks on NTRU. In Proceedings of the Eurocrypt'97. LNCS 1233, Springer-Verlag, 1997: 52-61

[9] Hoffstein J., Phpher J., Silverman J. H..Enhanced encoding and verification methods for the NTRU signature scheme. Version 2, May30, 2001, Http://www.ntru.com

[10] Gentry C., Szydlo M.. Cryptanalysis of the revised NTRU signature scheme. In Proceedings of the advances in cryptology-Eurocrypt'02. LNCS 2332. Springer-Verlag, 2002: 299-320.

[11] M. Jakobsson, K. Sako, R. Impagliazzo: Designated Verifier Proofs and their Applications. Proc. of Eurocrypt'96, Springer LNCS Vol. 1070, 142-154 (1996)

[12] Chunbo Ma, Jun Ao. "Group-oriented encryption secure against collude attack". Journal of Convergence Information Technology. 2008, 3(4): 47-53. ISSN: 1975-9320. Also available at http://eprint.iacr.org/2007/371.

[13] Chunbo Ma, Faliang Ao, Dake He. "Certificateless Group inside Signature". Proceedings of ISADS'05 (7th International Symposium on Autonomous Decentralized Systems, Chengdu. P. R. China), pagers: 194~200.

[14] Dinur I., Kindler G. and Safra S. Approximating CVP to within almost polynomial factors in NP-hard. In 39th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, 1998: 99-109.