Discussion on Matrix NTRU

Xu-Ren Luo and Chen-Hui Jerry Lin,

Department of Electrical and Electronic Engineering, Chung Cheng Institute of Technology,
National Defense University, Taiwan (R.O.C.)

Summary
In recent years the study of cryptosystem has shifted noticeably from symmetric to asymmetric key encryptions. One of the more intriguing issues of the research is NTRU encryption system, which is based on ring theory. The security of NTRU always depends on the lattices. Several studies have suggested that it is very difficult to know whether a polynomial is invertible or not. Nayak et al. introduced a new method as a matrix solution to solve the problem. However, this method is not without its flaws. In this paper, we expose the weakness regarding network security in matrix NTRU cryptosystem of Nayak et al. (2008, 2010) conscientiously, and we also propose a novel solution to this weakness. Our approach is based on the fact that some new conditions for selection of keys can increase the size of domain compared to what was shown in the previous studies and improve the strength of security against different kind of network attacks. First, we use a counter example to point out the flaw in the theorem of inverse modulo q introduced in the previous studies. Second, we prepare a new approach for inverse modulo q. The purpose of this paper is to demonstrate that our twofold selection scheme is superior to the original matrix NTRU cryptosystem and will help cryptosystems function under a safer environment by creating one public key and two private keys.

Key words:
Private Key, Public Key, Encryption, Decryption, Modular Operation.

1. Introduction

Cryptography and network security are two of the more intriguing issues prevailing throughout the last few decades. The heart of the technique requires the use of complex algorithms to achieve better data security. With cryptographic algorithms, cryptographic keys are often manipulated to encrypt plaintext message into different cipher-ones and to decrypt the cipher-ones by inversing the process with the same corresponding key. One of the most import requirements when applying the technique to the Internet is confidentiality. Other important issues include integrity, non-repudiation, and authentication. Nowadays, however cryptography is paramount to the protection of the digital content, and as observed by practical experience, it provides a much more trustworthy means of constraining the senders and receivers of certain messages.

Manuscript received January 5, 2011
Manuscript revised January 20, 2011

The traditional role of cryptography is to hide the data in communications. Due to the fast emergence of the Internet and its potential for commercial transactions over public data networks, the urgent need for the development of a new type of cryptographic system has become evident. Classical cryptography uses a symmetric key scheme which requires the sender and recipient to share a common key. In 1976, Diffie and Hellman [1] introduced the concept of public key cryptography which used one key to encrypt and a different key to decrypt. As a result, the major problem of symmetric key cryptosystem is how to securely distribute the symmetric key. Since then, there has been increasing interest for researches in finding new and fast public key cryptosystems. New studies over NTRU follow group algebra over strictly non-commutative groups. It is expected that new lattice reduction technique will be discovered over time and will be able to reduce the number of arithmetic operations involved in it. Speed is the key property of NTRU cryptosystem. Therefore, it is interesting to study a new variant of NTRU only if it gives any speed improvement along with more security against lattice attack. We will show that the keys are chosen in papers by Nayak et al. [3, 4] through a non-commutative ring (matrix ring of polynomials) with the condition that the determinant is one or negative one, which will definitely provide a small selection range and therefore cryptosystem becomes more prone to different kind of attacks. We will introduce some new conditions for a selection of keys that increases the size of the domain compared to that which was shown in the paper of Nayak et al. [3, 4].

2. Review of previous results

We will use $Mat_{n\times n}(I)$ to denote $n\times n$ matrices with integer entries. In Nayak et al. [2, 3], they selected two natural numbers, say p and q, then they tried to find some conditions to ensure the selection of a matrix, say X that has inverse modulo p, say X_p and inverse modulo q, say X_q such that

$$X\left(X_p\right) = I_{n\times n} + pS\,, \tag{1}$$

and

$$X\left(X_q\right) = I_{n\times n} + qT\,, \tag{2}$$

where X_p, X_q, S and T are in $Mat_{n\times n}(I)$ and $I_{n\times n}$ is the identity matrix for $n\times n$ matrices. To simplify the expression, they denoted Eq. 1 as

$$X\left(X_p\right) = I \pmod p\,. \tag{3}$$

For the matrix NTRU cryptosystem [2], the public key is pX_qY and the two private keys are X and X_p. Consequently, the existence of X_p and X_q is crucial for the matrix NTRU cryptosystem.

In Nayak et al. [3], they assumed that

$$X_p = X^{-1} + pN\,, \tag{4}$$

where X^{-1} is the inverse of X and N is any matrix in $Mat_{n\times n}(I)$. They verified that $X\left(X^{-1}+pN\right)=I+p\left(XN\right)$ to imply $X\left(X^{-1}+pN\right)=I \pmod p$. However, they forgot to check whether $X^{-1}+pN$ is in $Mat_{n\times n}(I)$.

3. Counter example proposed by us

We will demonstrate that the theorem of Nayak et al. [3, 4] for inverse modulo p is false by the following counter example.

We assume that $X=\begin{pmatrix}2 & 1 & 0\\ 1 & 0 & 1\\ 0 & 2 & 0\end{pmatrix}$ such that $X^{-1}=\begin{pmatrix}0.5 & 0 & -0.25\\ 0 & 0 & 0.5\\ -0.5 & 1 & 0.25\end{pmatrix}$ with $\det A=-4$. It yields that for any matrix N in $Mat_{n\times n}(I)$, $X^{-1}+pN$ is not in $Mat_{n\times n}(I)$.

Let us recall that $X^{-1}=\frac{1}{\det X}\left(cofX\right)^T$, where $cofX$ is the cofactor matrix of X with the (i,j) entry of $cofX$ satisfying $(-1)^{i+j}\det\left[X \text{ detelt i row and j column}\right]$, and $(\ )^T$ is the transpose operation.

Since X is in $Mat_{n\times n}(I)$, the entries of $cofX$ are all integers. If $\det X=\pm 1$, it yields X^{-1} which is also in $Mat_{n\times n}(I)$.

The example in Nayak et al. [3, 4] for the modulo p inverse followed the rule Eq. 4 was based on the special condition that its determinant was -1 which accidentally derived that $X^{-1}+pN$ is in $Mat_{n\times n}(I)$.

If the selection of X is restricted to matrices whose $\det X=\pm 1$, the possible selection for X will be shrunk to a very small range that may allure hackers to attack the cryptosystem.

4. Our approach

In this section, we present a new method to solve the restriction of possible selection for X to achieve more secure cryptosystem. In our method, two matrices, say X and Y in $Mat_{n\times n}(I)$, and two positive numbers, say p and q are selected such that X has (1) X_p, the inverse modulo p, and (2) X_q, the inverse modulo q.

We selected a matrix X in $Mat_{n\times n}(I)$ with $\det X\neq 0$, and a matrix Y without any restriction.

The row vectors of X is denoted as $\{R_1,...,R_n\}$ where $R_j=\left(x_{j1},...,x_{jn}\right)$ for $j=1,...,n$ and $X=\left(x_{ij}\right)_{n\times n}$.

According to Gram-Schmidt Orthogonalization, for $R_2,...,R_n,R_1$ (the order is important, where R_1 is the last one), there is an orthogonal family, say $\{V_1,V_2,...,V_n\}$ with

$V_1=R_2$, $V_2=R_3-\frac{\langle R_3,V_1\rangle}{\langle V_1,V_1\rangle}V_1,\ldots,V_k=R_{k+1}-\sum_{j=1}^{k-1}\frac{\langle R_{k+1},V_j\rangle}{\langle V_j,V_j\rangle}V_j$, for $k=2,...,n-1$, and $V_n=R_1-\sum_{j=1}^{n-1}\frac{\langle R_1,V_j\rangle}{\langle V_j,V_j\rangle}V_j$, where $\langle\ ,\ \rangle$ means the inner product in R^n.

It implies that V_n is orthogonal with respect to $\{V_1, V_2, ..., V_{n-1}\}$ so that V_n is orthogonal with respect to $\{R_2, R_3, ..., R_n\}$.

Moreover, we will prove that $\langle R_1, V_n \rangle \neq 0$.

We assumed that $\langle R_1, V_n \rangle = 0$ then R_1 is in the orthogonal space of V_n. Hence, R_1 is in the span of $\{R_2, R_3, ..., R_n\}$ to imply that the determinant of X is zero, that is $\det X = 0$. It is a contradiction.

This is because the entries of R_j for $j = 1, ..., n$ are integers, and then the entries of V_j are rational numbers. Therefore, we can construct a row vector with integer coefficient, say W_1 that satisfies (1) $\langle R_1, W_1 \rangle \neq 0$ and (2) $\langle R_j, W_1 \rangle = 0$ for $j = 2, 3, ..., n$.

Similarly, for $R_1, R_3 ..., R_n, R_2$ (the order is important, where R_2 is the last one), we can find a row vector, say W_2, with integer coefficients, that satisfies (1) $\langle R_2, W_2 \rangle \neq 0$ and (2) $\langle R_j, W_2 \rangle = 0$ for $j = 1, 3, 4, ..., n$.

Following this trend, we can find W_j for $j = 1, 2, ..., n$ such that (1) $\langle R_j, W_j \rangle \neq 0$, for $j = 1, 2, ..., n$, and (2) $\langle R_k, W_j \rangle = 0$ for $k \in \{1, 2, ..., n\}$ with $k \neq j$.

Hence, we can construct a matrix in $Mat_{n\times 1}(I)$, say $C = (C_1, ..., C_n)$ with $C_j = W_j^T$ for $j = 1, 2, ..., n$.

We compute XC to derive a diagonal matrix, say $D = (d_{ij})$ with $d_{ij} = 0$, for $i \neq j$, and $d_{ii} = R_i C_i = \langle R_i, W_i \rangle \neq 0$, for $j = 1, 2, ..., n$.

We will select a natural number, denoted as q such that q is relative prime with respect to $R_1C_1, R_2C_2, ..., R_nC_n$.

From Euclidean Algorithm, there are values, say α_k and β_k (they are integers) that satisfy $\alpha_k R_k C_k + q\beta_k = 1$, for $k = 1, 2, ..., n$.

We define a matrix in $Mat_{n\times n}(I)$ as $[\alpha_1 C_1, \alpha_2 C_2, ..., \alpha_n C_n]$

Next, we will prove that

$$X[\alpha_1 C_1, \alpha_2 C_2, ..., \alpha_n C_n] = I_{n\times n} \pmod q. \quad (5)$$

$$X[\alpha_1 C_1, \alpha_2 C_2, ..., \alpha_n C_n] = \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} [\alpha_1 C_1, \alpha_2 C_2, ..., \alpha_n C_n]$$

$$= \begin{bmatrix} \alpha_1 R_1 C_1 & 0 & 0 & 0 \\ 0 & \alpha_2 R_2 C_2 & 0 & 0 \\ 0 & 0 & & 0 \\ 0 & 0 & 0 & \alpha_n R_n C_n \end{bmatrix}$$

$$= \begin{bmatrix} 1-q\beta_1 & 0 & 0 & 0 \\ 0 & 1-q\beta_2 & 0 & 0 \\ 0 & 0 & & 0 \\ 0 & 0 & 0 & 1-q\beta_n \end{bmatrix}$$

$$= I_{n\times n} \pmod q. \quad (6)$$

By the same argument, we can select a number, say p that is also relative prime to $R_1C_1, R_2C_2, ..., R_nC_n$. Furthermore, from the Euclidean Algorithm, there are values, say s_k and t_k (they are integers) that satisfy $s_k R_k C_k + pt_k = 1$, for $k = 1, 2, ..., n$. Consequently, we know that $[s_1 C_1, s_2 C_2, ..., s_n C_n]$ is an inverse modulo p.

5. Numerical example

For example, we recalled the previous one $X = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 2 & 0 \end{pmatrix}$, with $\det X = -4$.

From Gram-Schmidt orthogonalization for $R_2 = (1,0,1)$, $R_3 = (0,2,0)$, and $R_1 = (2,1,0)$, then $V_1 = (1,0,1)$, $V_2 = (0,2,0)$ and $V_3 = (1,0,-1)$ to imply that $\langle R_1, V_3 \rangle = 2 \neq 0$.

By Gram-Schmidt orthogonalization for $R_3 = (0,2,0)$, $R_1 = (2,1,0)$, and $R_2 = (1,0,1)$ then $V_1 = (0,2,0)$, $V_2 = (2,0,0)$ and $V_3 = (0,0,1)$ to imply that $\langle R_2, V_3 \rangle = 1 \neq 0$.

Using Gram-Schmidt orthogonalization for $R_1 = (2,1,0)$, $R_2 = (1,0,1)$, and $R_3 = (0,2,0)$ then $V_1 = (2,1,0)$, $V_2 = \left(\frac{1}{5}, \frac{-2}{5}, 1\right)$ and $V_3 = \left(\frac{-2}{3}, \frac{4}{3}, \frac{2}{3}\right)$ then

we select integer entries to imply $V_3 = (-1, 2, 1)$ and to imply that $\langle R_3, V_3 \rangle = 4 \neq 0$.

Next, we select $q = 37$ that is relative prime to $\{2, 1, 4\}$.

By the Euclidean Algorithm we derive that

$$(-18)\langle R_1, V_3 \rangle + 37 = 1, \quad (7)$$

$$(-36)\langle R_2, V_3 \rangle + 37 = 1, \quad (8)$$

and

$$(-9)\langle R_3, V_3 \rangle + 37 = 1, \quad (9)$$

so we know that

$$X_q = \begin{pmatrix} (-18)\begin{pmatrix}1\\0\\-1\end{pmatrix} & (-36)\begin{pmatrix}0\\0\\1\end{pmatrix} & (-9)\begin{pmatrix}-1\\2\\1\end{pmatrix} \end{pmatrix} = \begin{pmatrix} -18 & 0 & 9 \\ 0 & 0 & -18 \\ 18 & -36 & -9 \end{pmatrix}. \quad (10)$$

For completeness, we check that

$$X(X_q) = \begin{pmatrix} -36 & 0 & 0 \\ 0 & -36 & 0 \\ 0 & 0 & -36 \end{pmatrix}, \quad (11)$$

to confirm that $X(X_{37}) = I_{3\times 3} \pmod{37}$.

6. Conclusion

In this paper, we present a new matrix NTRU method to revise and improve the weak procedure proposed previously, and to locate an inverse modulo q. According to Nayak et al. [3, 4], they have only found the inverse modulo q for matrices with a determinant of ± 1. This is too restricted and may cause the one public key and the two private keys provided by the cryptosystem to be easily hacked. In our method, there are plenty of matrices with non-zero determinant which can be used, and will improve the security of the cryptosystem. The capabilities against lattice or other possible attacks and the comparison with other variants in terms of size of plain text block, size of encrypted text block, encryption speed, decryption speed, message expansion, private key length, public security, private key security and lattice security etc. may be of interest to future research to explored and to meet real-time application requirements.

References

[1] W. Diffie and M.E. Hellman, "New directions in cryptography," IEEE Trans. On Information Theory, vol. 22, pp.644-654, 1976.

[2] J. Hoffstein, J. Pipher and J.H. Silverman, "NTRU: A Ring based public key cryptosystem," Lecture notes in Computer Science, Springer-Verlag, Berlin, pp.267-288, 1998.

[3] R. Nayak, C. V. Sastry, and J. Pradhan, "A matrix formulation for NTRU cryptosystem," Proc. 16th IEEE International Conf. on Networks (ICON-2008), New Delhi, India, 12-14 December, 2008.

[4] R. Nayak, C. V. Sastry, and J. Pradhan, "Algorithmic Comparison between Polynomial Base and Matrix Base NTRU Cryptosystem," (IJCNS) International Journal of Computer and Network Security, vol.2, no.7, pp.58-63, July 2010.

Xu-Ren Luo was born in Hsinchu, Taiwan, Republic of China, on Dec. 5th, 1974. He received the B.S. degree in Computer Science and the M.S. degree in Electrical and Electronic Engineering, both from Chung Cheng Institute of Technology (CCIT), National Defense University, Taiwan, R.O.C., in 1997 and 2004, respectively. He is currently pursuing the Ph.D. degree in the area of information assurance at the Electrical and Electronic Engineering Department, CCIT. His research interests are focused on information security, data hiding, multimedia security, and image processing.

Chen-Hui Jerry Lin was born in 1960. He received the M.S. degree from the Department of Electrical Engineering, University of Missouri at Rolla in 1986. He then began his career of teaching computer programming at several colleges and universities of technology. He received the Ph.D. degree in electrical engineering from National Taiwan University in 1998. He has joined the faculty of National Defense University as an associate professor since 2002. His research interests include signal processing and computer programming.