Cryptanalysis of a Lattice-Knapsack Mixed Public Key Cryptosystem

Jun Xu[1,2,3], Lei Hu[1], Siwei Sun[1], and Ping Wang[4,5,6]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] University of Chinese Academy of Sciences, Beijing 100049, China
[3] School of Mathematical Science, Anhui University, Hefei 230601, Anhui, China
[4] Tian Jin Zhong Wei Aerospace Data System Technology Co., Ltd
[5] Space Star Technology Co., Ltd
[6] Institute No.503 of the fifth Research Academy, China Aerospace Science and Technology Corporation. Beijing 100086, China
{jxu,hu,swsun}@is.ac.cn

Abstract. Recently, a lattice based public key cryptosystem mixed with a knapsack was presented in the CANS 2011 conference. In this paper, we propose two message recovery attacks on this cryptosystem. The first one is a broadcast attack: a single message of m bits can be recovered if it is encrypted for $\lceil \frac{m+1}{2} \rceil$ recipients. The second attack is a multiple transmission attack in which a message can be recovered with a probability of $(1-2^{-l})^m$ if it is encrypted under a same public key for $l = \lceil \log_2 m + 2 \rceil$ times using different random numbers. The multiple transmission attack can be further improved with a linearization technique to that only $\lceil \frac{\log_2 m+1}{2} \rceil$ times of encryptions are required to recover the message. An open problem related to the message recovery attack using only one cipehertext is discussed.

Keywords: Public Key Cryptosystem, Lattice, Knapsack, Linearization.

1 Introduction

Ever since the discovery of the quantum algorithm [26] which can factor integers and compute discrete logarithms in polynomial time and hence can break RSA, DSA, and ECDSA efficiently, the necessity for new designs of public key cryptosystems immune to quantum algorithm attacks has become strong and urgent. Several new designs based on computational hard problems resistant to quantum algorithm attacks have been extensively studied, including hash based, code based, multivariate polynomial equation based and lattice based cryptography.

The first lattice based cryptosystem was proposed by Ajtai and Dwork [1] in 1997. However, to avoid Nguyen and Stern's heuristic attack [20], implementations of the Ajtai-Dwork cryptosystem would require very large keys, making

J. Pieprzyk, A.-R. Sadeghi, and M. Manulis (Eds.): CANS 2012, LNCS 7712, pp. 32–42, 2012.

it far from being practical. To increase the efficiency of the Ajtai-Dwork cryptosytem, Cai and Cusick [6] constructed a new cryptosystem by mixing the Ajtai-Dwork crytosystem with a knapsack. Unfortunately, Pan and Deng [23] presented an iterative method to recover the message encrypted by the Cai-Cusick cryptosystem under a ciphertext-only scenario.

With several known attacks in mind, Pan et al [24] proposed a new lattice-based public key cryptosystem which mixes with a knapsack in its design in the CANS 2011 conference. Unfortunately, it does not enjoy any security proof and is slower than state-of-the-art lattice-based encryption schemes (e.g., [11, 18, 27]), although its security was carefully evaluated against some lattice based attacks in [24]. One of such lattice based attacks, for example, is some attack similarly as that in [15–17] against NTRU [14] targeting at its cyclic structure, but the underlying lattice in this new cryptosystem has no special cyclic structure like in NTRU. Furthermore, the new cryptosystem hides the knapsack structure behind linear combinations. This strategy is very different from those knapsack based public key cryptosystems which hide their trapdoors by transforming a superincreasing knapsack into a generic one. Therefore, the existing successful attacks [21] against knapsack based cryptosystems seem to not be applicable to the new system.

In this paper we propose two feasible attacks on the cryptosystem of Pan et al [24]. The first one is a broadcast attack, it assumes a single message is encrypted by the sender directed for several recipients with different public keys, the message can be recovered by solving a system of nonlinear equations via linearization technique. The second one is a multiple transmission attack in which a single message is encrypted under the same public key for several times using different random vectors. In this situation, the message can be easier to recover.

The rest of this paper is organized as follows. Section 2 gives a description of the cryptosystem of Pan et al. Section 3 presents a broadcast attack and a multiple transmission attack on the crytosystem. In section 4, we further improve the multiple transmission attack by linearization technique. Section 5 is devoted to discuss an open problem related to the message recovery attack using only one cipehertext. The last section is a conclusion.

2 Description of the Cryptosystem of Pan et al.

In this section we describe the cryptosystem recently proposed by Pan et al [24]. For detailed information on its design rationale, please refer to their paper [24].

This cryptosystem is parameterized by a security parameter m. Let $n = 2m$.

Key Generation: Randomly choose a superincreasing sequence $\{N_1 = 1, N_2, \cdots, N_n\}$ and a permutation τ on $\{1, 2, \cdots, n\}$ such that $\tau^{-1}(1) \leq m$. For each $1 \leq i \leq m$, represent $N_{\tau(i+m)}$ as a linear combination of $\{N_{\tau(1)}, \cdots, N_{\tau(m)}\}$ with integer coefficients, namely,

$$N_{\tau(i+m)} = \sum_{j=1}^{m} b_{i,j} N_{\tau(j)}, \quad i = 1, 2, \cdots, m.$$

The absolute values of the coefficients $b_{i,j}$ $(1 \leq i, j \leq m)$ should be made reasonably small [24] and this can be done by employing Babai's nearest plane algorithm [3].

Use the above integer coefficients to form an $m \times n$ matrix

$$A = \begin{bmatrix} 1 & 0 & \cdots & 0 & b_{1,1} & b_{2,1} & \cdots & b_{m,1} \\ 0 & 1 & \cdots & 0 & b_{1,2} & b_{2,2} & \cdots & b_{m,2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & b_{1,m} & b_{2,m} & \cdots & b_{m,m} \end{bmatrix},$$

and let

$$l_{i,1} = \sum_{\substack{j=1,\cdots,n \\ A_{i,j}<0}} A_{i,j}, \quad i = 1, \cdots, m$$

$$l_{i,2} = \sum_{\substack{j=1,\cdots,n \\ A_{i,j}>0}} A_{i,j}, \quad i = 1, \cdots, m$$

$$q = \max_{i=1,\cdots,m} \{l_{i,2} - l_{i,1}\}.$$

Finally, randomly choose a permutation σ on $\{1, \cdots, n\}$ such that the matrix $S = [A_{\sigma(1)}, A_{\sigma(2)}, \cdots, A_{\sigma(m)}]$ is an invertible matrix over the field $\mathbb{F}_p$, where p is the smallest prime such that $p > q$ and A_j denotes the j-th column of A.

Public Key: The smallest prime p such that $p > q$, and $H = S^{-1}[A_{\sigma(m+1)}, \cdots, A_{\sigma(n)}]$.

Here the entries of the matrices are regarded as integers in the interval $[0, p-1]$ and identically regarded as elements of the field $\mathbb{F}_p$, and the matrices are operated modulo p.

Private Key: $N_2, \cdots, N_n, S, \tau, \sigma, l_{i,1}, l_{i,2}$ $(i = 1, \cdots, m)$.

Encryption: For any message $t \in \{0,1\}^m$, randomly choose a vector $r \in \{0,1\}^m$ and the ciphertext c is computed as follows

$$c = Ht + r \mod p.$$

Note that all vectors are written as column vectors in this paper as in [24].

Decryption: Let $v = (r^T, t^T)^T = (v_1, \cdots, v_n)^T$, and $d = Sc \mod p$. The message t and the random number r are recovered by solving the following superincreasing knapsack problem with unknown coefficients $x_i \in \{0, 1\}$

$$(N_{\tau(1)}, \cdots, N_{\tau(m)})\tilde{d} = \sum_{i}^{n} x_i N_i,$$

where $\tilde{d} = d \mod p$ with its entries $l_{i,1} \leq \tilde{d}_i \leq l_{i,2}$. It can be shown that $x_i = v_{\sigma^{-1}(\tau^{-1}(i))}$.

3 Two Attacks on the Cryptosystem of Pan et al.

In this section we present two attacks against the cryptosystem of Pan et al, one is a broadcast attack and the other is a multiple transmission attack, they can recover the encrypted messages with practical complexities, without any knowledge on the structure of the public and secret keys.

3.1 Broadcast Attack

The first broadcast attack was introduced in 1988 by Håstad in [13] to compromise the security of the RSA cryptosystem with low public key exponents. Broadcast attacks against lattice based encryption schemes have already been proposed by Plantard and Susilo [22]. In a broadcast attack, it is assumed that a single message is encrypted by the sender several times for multiple recipients with different public keys.

Below we will show that Pan et al's cryptosystem is insecure under this attack scenario. To be more specific, if the number of recipients exceeds $l := \lceil (m+1)/2 \rceil$, an attacker can derive the corresponding plaintext from the l ciphertexts.

Let $H = (h_{ij})_{m \times m}$. From $c = Ht + r \mod p$, we have

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{bmatrix} - \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1m} \\ h_{21} & h_{22} & \cdots & h_{2m} \\ & \cdots & \cdots & \\ h_{m1} & h_{m2} & \cdots & h_{mm} \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_m \end{bmatrix} = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{bmatrix} \mod p$$

Since $r_i \in \{0, 1\}$ for $1 \leq i \leq m$, we have

$$\left(c_i - \sum_{j=1}^{m} h_{ij} t_j\right) \cdot \left(c_i - 1 - \sum_{j=1}^{m} h_{ij} t_j\right) = 0 \mod p$$

Obviously, this results in m quadratic equations over $\mathbb{F}_p$ on m variables $t_1, \cdots, t_m$. These variables are binary, but we do not know how to exploit this feature to solve them out from a single encryption (see the discussion in Section 5). In a broadcast scenario, assume a same message $t = (t_1, \cdots, t_m)^T$ is encrypted under

$l = \lceil (m+1)/2 \rceil$ different public keys, say $H^{(k)} = (h_{ij}^{(k)})_{m\times m}$, $1 \le k \le l$, into the ciphertexts $(c_1^{(k)}, \cdots, c_m^{(k)})^T$, $1 \le k \le l$, then

$$\begin{cases} \Big(c_i^{(1)} - \sum\limits_{j=1}^{m} h_{ij}^{(1)} t_j\Big)\Big(c_i^{(1)} - 1 - \sum\limits_{j=1}^{m} h_{ij}^{(1)} t_j\Big) = 0, \quad 1 \le i \le m \\ \cdots \\ \Big(c_i^{(l)} - \sum\limits_{j=1}^{m} h_{ij}^{(l)} t_j\Big)\Big(c_i^{(l)} - 1 - \sum\limits_{j=1}^{m} h_{ij}^{(l)} t_j\Big) = 0, \quad 1 \le i \le m \end{cases} \tag{1}$$

This is a system of $m\lceil (m+1)/2 \rceil \ge m(m+1)/2$ quadratic polynomial equations in $t_1, \cdots, t_m$. Utilizing the known linearization technique [2, 4, 9] and regarding all quadratic monomials $t_i t_j$ as new variables, the system (1) become a linear system in $m(m+1)/2$ unknowns ($t_1, \cdots, t_m$ and the $\binom{m}{2}$ new variables), it can be solved in time complexity $(\frac{m^2}{2})^\omega$ by a naive or advanced linear equation solving method, where $\omega = 3$ for a naive Gaussian elimination and $\omega = 2.376$ for the method of Coppersmith and Winograd [7].

Complexity and Experimental Result: To demonstrate the feasibility of the broadcast attack, we have implemented the attack in the Magma computer algebra system on a PC with Intel(R) Core(TM) Quad CPU (2.83GHz, 3.25GB RAM, Windows XP). For $m = 100$, which is one of the parameter suggested by the designers [24], we can recover the unknown message in no more than one hour. We chose $p = 271$, our Magma experiment successfully obtained the corresponding message within 46 minutes assuming $l = 51$.

For other suggested parameters: $m = 200, 300, 400, 500$, our Magma experiment failed to recover the message due to un-optimized programming and large memory consumption, but in all these cases, the time complexity of the attack is still in an acceptable range since even for $m = 500$ and by using a naive method, it is roughly $(\frac{500^2}{2})^\omega \approx 2^{50.79}$, which can be done on a minicomputer like DELL PowerEdge 7250 [10] and it will output a desired result within a week for an optimized memory management.

3.2 Multiple Transmission Attack

As observed in [14], multiple NTRU encryptions of a single message under a single public key may compromise the security of the encrypted message of NTRU, and this method used to recover the secret message is named as Multiple Transmission Attack [17]. In this section, we show that a similar vulnerability exists in Pan et al's cryptosystem, and we propose an efficient attack targeting at this vulnerability.

Assume a single message t is encrypted using the same public key H for l different but uniformly and independent random m-dimensional vectors in the encryption. Let

$$c^{(j)} = Ht + r^{(j)} \mod p, \quad 1 \le j \le l$$

be the ciphertext under the random m-dimensional vectors $r^{(j)}$, and use them as columns to form $n \times l$ matrices C and R:

$$C = \begin{bmatrix} c_1^{(1)} & c_1^{(2)} & \cdots & c_1^{(l)} \\ c_2^{(1)} & c_2^{(2)} & \cdots & c_2^{(l)} \\ \vdots & \vdots & & \vdots \\ c_n^{(1)} & c_n^{(2)} & \cdots & c_n^{(l)} \end{bmatrix}, R = \begin{bmatrix} r_1^{(1)} & r_1^{(2)} & \cdots & r_1^{(l)} \\ r_2^{(1)} & r_2^{(2)} & \cdots & r_2^{(l)} \\ \vdots & \vdots & & \vdots \\ r_n^{(1)} & r_n^{(2)} & \cdots & r_n^{(l)} \end{bmatrix}.$$

Let u_k and $r_k^{(j)}$ be the k-th entries of Ht and $r^{(j)}$, respectively. It is clear that the j-th entry of the k-th row $(c_k^{(1)}, c_k^{(2)}, \cdots, c_k^{(l)})$ of C is equal to $u_k + r_k^{(j)}$, which is either u_k or $u_k + 1 \mod p$.

We determine each row of R as follows. We have assumed that $p \geq 3$. Thus, for any two elements in $\{0, 1, \cdots, p-1\}$ which differ by 1 modulo p, we define their cyclic minimum as $\min\{a, a+1\} = a$ if $a \in \{0, 1, \cdots, p-2\}$ and $\min\{p-1, 0\} = p-1$. For a fixed $1 \leq k \leq l$, since the entries $c_k^{(1)}, c_k^{(2)}, \cdots, c_k^{(l)}$ either take two values which differ 1 modulo p or take the same value, we can always find a value $\widetilde{u_k}$ as $\min\{c_k^{(1)}, c_k^{(2)}, \cdots, c_k^{(l)}\}$. $\widetilde{u_k}$ will be equal to u_k in almost cases except when $(r_k^{(1)}, r_k^{(2)}, \cdots, r_k^{(l)}) = (1, \cdots, 1)$. Therefore, we can obtain correctly the value of u_k with a probability of $1 - 2^{-l}$. Assuming the uniformness and independence of random vectors $r^{(j)}$, we correctly get the vector Ht with a probability of $(1-2^{-l})^m$. Consequently, we can successfully recover the message t by computing $\tilde{t} = H^{-1}\tilde{u}$ with a probability of $(1-2^{-l})^m$.

Let $l \approx \log_2 m + 2$, we have

$$(1-2^{-l})^m \approx ((1 + \frac{1}{2^l - 1})^{-2^l})^{2^{-2}} \longrightarrow e^{-1/4} \approx 0.78, \ when \ m \to \infty,$$

which means that roughly $l = \lceil \log_2 m \rceil + 2$ encryptions can be used to probably successfully recover the message t. This number $(\lceil \log_2 m \rceil + 2)$ of needed times of encryptions is greatly less than the corresponding number $(\lceil (m+1)/2 \rceil)$ in a broadcast attack. The concrete value of the probability $(1-2^{-l})^m$ for different pairs of m and l are listed in Table 1, which are verified in our experiment on multiple transmission attacks.

Table 1. Success probability of the multiple transmission attack

m \ l	7	8	9	10	11	12	13	14
100	0.4542	0.6649	0.8237	0.9034	0.9510	0.9746	0.9885	0.9935
200	0.2047	0.4583	0.6742	0.8203	0.9038	0.9525	0.9753	0.9886
300	0.0956	0.3080	0.5654	0.7461	0.8640	0.9281	0.9643	0.9841
400	0.0461	0.2109	0.4596	0.6753	0.8231	0.9051	0.9476	0.9766
500	0.0220	0.1413	0.3731	0.6235	0.7874	0.8901	0.9414	0.9709

4 Improved Multiple Transmission Attack

In this section we show that the number of transmissions needed to successfully recover the message in a multiple transmission attack can be halved with the help of linearization technique.

Suppose a single message t is encrypted using the same public key H for l times and let

$$\begin{bmatrix} c_1^{(k)} \\ c_2^{(k)} \\ \vdots \\ c_m^{(k)} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1m} \\ h_{21} & h_{22} & \cdots & h_{2m} \\ \vdots & \vdots & & \vdots \\ h_{m1} & h_{m2} & \cdots & h_{mm} \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_m \end{bmatrix} + \begin{bmatrix} r_1^{(k)} \\ r_2^{(k)} \\ \vdots \\ r_m^{(k)} \end{bmatrix} \mod p$$

be the k-th ciphertext, where $k \in \{1, 2, \cdots, l\}$.

According to Section 3.2, each row of R can be determined correctly with a probability $1 - 2^{-l}$, and can be correctly determined with a probability $1 - 2 \cdot 2^{-l}$ since we can correctly determine u_k when $c_k^{(1)}, c_k^{(2)}, \cdots, c_k^{(l)}$ are not the same, namely when $(r_k^{(1)}, r_k^{(2)}, \cdots, r_k^{(l)}) \neq (1, \cdots, 1)$ and $(0, \cdots, 0)$. Thus, about $(1 - 2^{1-l})m$ rows of R can be determined surely. Without loss of generality, we assume the remaining undetermined rows of R are the last $\rho = \lceil 2^{1-l} m \rceil$ ones.

Now from the first ciphertext and

$$\begin{bmatrix} c_1^{(1)} \\ c_2^{(1)} \\ \vdots \\ c_{m-\rho}^{(1)} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1m} \\ h_{21} & h_{22} & \cdots & h_{2m} \\ \vdots & \vdots & & \vdots \\ h_{m-\rho,1} & h_{m-\rho,2} & \cdots & h_{m-\rho,m} \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_m \end{bmatrix} + \begin{bmatrix} r_1^{(1)} \\ r_2^{(1)} \\ \vdots \\ r_{m-\rho}^{(1)} \end{bmatrix} \mod p,$$

we can linearly represent $m - \rho$ unknowns t_j by other ρ ones. Without loss of generality, we assume the ρ unknowns are $t_1, t_2, \cdots, t_\rho$ and the linear relations are

$$\begin{cases} t_{\rho+1} = L_{\rho+1}(t_1, t_2, \cdots, t_\rho) \\ \quad \vdots \\ t_m = L_m(t_1, t_2, \cdots, t_\rho) \end{cases}$$

Then from binary property of t_i, $i = 1, \cdots, m$, a system of quadratic polynomial equations with ρ unknowns can be built as follows:

$$\begin{cases} t_1^2 = t_1 \\ \quad \vdots \\ t_\rho^2 = t_\rho \\ L_{\rho+1}^2(t_1, t_2, \cdots, t_\rho) = L_{\rho+1}(t_1, t_2, \cdots, t_\rho) \\ \quad \vdots \\ L_m^2(t_1, t_2, \cdots, t_\rho) = L_m(t_1, t_2, \cdots, t_\rho) \end{cases} \tag{2}$$

It can be successfully solved by linearization technique provided $m \geq \binom{\rho}{2} + 2\rho$, or equivalently, provided $l \geq \lceil \frac{\log_2 m+1}{2} \rceil$. Thus, about $\lceil \frac{\log_2 m+1}{2} \rceil$ encryptions can be used to recover the secret message, which is about one half the number of the method proposed in Section 3.2. As an example, for $m = 500$, this number is 5, we need only 5 encryptions to recover the secret message.

5 Discussion and Open Problem

The broadcast and multiple transmission attacks presented in the previous two sections do not use the inherited information about the structure of the public key H except that it is invertible. A natural question to ask is that in the case of only assuming H is an invertible matrix, whether it is possible to recover the encrypted message with only one ciphertext, namely is there a ciphertext only attack on the cryptosystem in this case? Mathematically, this problem can be formulated as follows:

Problem: Let $n = 2m$, A be an $m \times n$ matrix of rank m over $\mathbb{F}_p$. Given $c \in \mathbb{F}_p^m$, find a binary vector $x \in \{0, 1\}^n$ (if any) such that $c = Ax \mod p$.

For most such matrices A, this problem has at most one solution for a general c, this is a requirement for cryptographic decryption scenario. We may further assume any m columns of A are linearly independent. Then, how to find the solution x efficiently?

The above problem can be viewed as a syndrome decoding of a linear code with parity check matrix A where the error noise vector is limited to be binary. A slightly general but essentially equivalent limitation is that each component of the error noise vector only takes two distinct values and the two values for different components may be different. This case can be translated to the case of binary noise vectors via an affine transformation. Here for the syndrome decoding, we do not limit the number of the errors (namely the Hamming weight) of the noise but limit the component of the noise to be binary. On the contrary in classical coding theory, the Hamming weight of the noise is limited but its component values are not restricted.

Another point of view is to look at the above problem as a knapsack problem on a vector space, that is, a subset sum problem on the column vectors of A.

In the encryption scheme of Pan et al [24], the corresponding A is chosen as (H, I), where I is identity matrix. This scheme is like the problem of Learning With Errors (LWE) [25]. It can be treated as the problem to solve a specific system of $2m$ quadratic equations over $\mathbb{F}_p$ in m variables of the form:

$$\begin{cases} x_1^2 - x_1 = 0 \\ \quad \vdots \\ x_m^2 - x_m = 0 \\ (c_1 - h_{11}x_1 - \cdots - h_{1m}x_m)^2 - (c_1 - h_{11}x_1 - \cdots - h_{1m}x_m) = 0 \\ \quad \vdots \\ (c_m - h_{m1}x_1 - \cdots - h_{mm}x_m)^2 - (c_m - h_{m1}x_1 - \cdots - h_{mm}x_m) = 0 \end{cases} \tag{3}$$

We do not know how to efficiently solve (if possibly) this seemingly very specific nonlinear system for large m. We have tried several methods such as XL [9], Fix-XL [4] and ElimLin [8] to solve (3), but failed to achieve an efficient solving method. We think this highly structured system of equations or knapsack problem on a vector space is an interesting pursuing topic and it may be a computational hard problem.

Finally, we point out that the cryptosystem of Pan et al is not secure under chosen plaintext attacks (CPA-secure) [12]. It is obvious that one can tell the difference between two messages $(0, \cdots, 0)^T$ and $(1, 0, \cdots, 0)^T$ by simply checking whether the ciphertext is close to the all zero vector or to the first column of H. However, this does not mean that this kind of observation can be directly utilized to launch an above-mentioned narrow-sense ciphertext-only attack, i.e., recovering a message given its only one ciphertext.

6 Conclusion

In this paper, we proposed two efficient attacks on a recently proposed cryptosystem that mixes the lattice and knapsack ideas in its design rational. Both attacks are capable of recovering the encrypted messages in practical time complexities under broadcast-like attack modes. The vulnerability of the new design is clearly due to the characteristic that the random vectors in its encryption process are chosen from a very limited set, namely the binary vectors.

We did not propose a ciphertext-only attack on this new cryptosystem, this type of attacks is equivalent to solve a knapsack problem on a vector space, which is an interesting research topic.

Acknowledgements. The authors would like to thank anonymous reviewers for their helpful comments and suggestions. The work of this paper was supported by the National Key Basic Research Program of China (2013CB834203), the National Natural Science Foundation of China (Grants 61070172 and 10990011), the Strategic Priority Research Program of Chinese Academy of Sciences under Grant XDA06010702, and the State Key Laboratory of Information Security, Chinese Academy of Sciences.

References

1. Ajtai, M., Dwork, C.: A public-key cryptosystem with worst-case/average-case equivalence. In: Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, pp. 284–293 (1997)
2. Arora, S., Ge, R.: New Algorithms for Learning in Presence of Errors. In: Aceto, L., Henzinger, M., Sgall, J. (eds.) ICALP 2011. LNCS, vol. 6755, pp. 403–415. Springer, Heidelberg (2011)
3. Babai, L.: On Lovász lattice reduction and the nearest lattice point problem. Combinatorica 6, 1–13 (1986)
4. Bard, G.V.: Algebraic Cryptanalysis. Springer, Heidelberg (2001) ISBN 978-0-387-88756-2

5. Bosma, W., Cannon, J., Playoust, C.: The Magma Algebra System I: The user language. Journal of Symbolic Computation 24, 235–265 (1997)
6. Cai, J.-Y., Cusick, T.W.: A Lattice-Based Public-Key Cryptosystem. In: Tavares, S., Meijer, H. (eds.) SAC 1998. LNCS, vol. 1556, pp. 219–233. Springer, Heidelberg (1999)
7. Coppersmith, D., Winograd, S.: Matrix multiplication via arithmetic progression. Journal of Symbolic Computation 9, 251–280 (1990)
8. Courtois, N.T., Bard, G.V.: Algebraic Cryptanalysis of the Data Encryption Standard. In: Galbraith, S.D. (ed.) Cryptography and Coding 2007. LNCS, vol. 4887, pp. 152–169. Springer, Heidelberg (2007)
9. Courtois, N.T., Klimov, A., Patarin, J., Shamir, A.: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 392–407. Springer, Heidelberg (2000)
10. Ding, J., Hu, L., Nie, X., Li, J., Wagner, J.: High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 233–248. Springer, Heidelberg (2007)
11. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, pp. 197–206. ACM Press (2008) ISBN 978-1-60558-047-0
12. Goldwasser, S., Micali, S.: Probabilistic Encryption. J. Computer and System Sciences 28, 270–299 (1983)
13. Håstad, J.: Solving simultaneous modular equations of low degree. SIAM J. Comput. 17, 336–341 (1988)
14. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A Ring-Based Public Key Cryptosystem. In: Buhler, J.P. (ed.) ANTS 1998. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998)
15. Howgrave-Graham, N.: A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack Against NTRU. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 150–169. Springer, Heidelberg (2007)
16. Howgrave-Graham, N., Silverman, J.H.: A Meet-In-The-Meddle Attack on an NTRU Private Key. Technical report, `http://www.ntru.com/cryptolab/technotes.htm#004`
17. Howgrave-Graham, N., Silverman, J.H.: Implementation Notes for NTRU PKCS Multiple Transmissions. Technical report, `http://www.ntru.com/cryptolab/technotes.htm#006`
18. Lyubashevsky, V., Peikert, C., Regev, O.: On Ideal Lattices and Learning with Errors over Rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010)
19. May, A., Silverman, J.H.: Dimension Reduction Methods for Convolution Modular Lattices. In: Silverman, J.H. (ed.) CaLC 2001. LNCS, vol. 2146, pp. 110–125. Springer, Heidelberg (2001)
20. Nguyên, P.Q., Stern, J.: Cryptanalysis of the Ajtai-Dwork Cryptosystem. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 223–242. Springer, Heidelberg (1998)
21. Odlyzko, A.M.: The rise and fall of knapsack cryptosystems. Cryptology and Computational Number Theory 42, 75–88 (1990)
22. Plantard, T., Susilo, W.: Broadcast Attacks against Lattice-Based Cryptosystems. In: Abdalla, M., Pointcheval, D., Fouque, P.-A., Vergnaud, D. (eds.) ACNS 2009. LNCS, vol. 5536, pp. 456–472. Springer, Heidelberg (2009)

23. Pan, Y., Deng, Y.: A Ciphertext-Only Attack Against the Cai-Cusick Lattice-Based Public-Key Cryptosystem. IEEE Transactions on Information Theory 57, 1780–1785 (2011)
24. Pan, Y., Deng, Y., Jiang, Y., Tu, Z.: A New Lattice-Based Public-Key Cryptosystem Mixed with a Knapsack. In: Lin, D., Tsudik, G., Wang, X. (eds.) CANS 2011. LNCS, vol. 7092, pp. 126–137. Springer, Heidelberg (2011)
25. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: The 37th Annual ACM Symposium on Theory of Computing, pp. 84–93. ACM Press (2004) ISBN 1-58113-960-8
26. Shor, P.: Algorithms for Quantum Computation: Discrete Logrithms and Factoring. In: The 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. IEEE Computer Science Press, Santa Fe (1994)
27. Stehlé, D., Steinfeld, R.: Making NTRU as Secure as Worst-Case Problems over Ideal Lattices. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 27–47. Springer, Heidelberg (2011)