An Improved Security Analysis on an Indeterminate Equation Public Key Cryptosystem by Evaluation Attacks

Akifumi Muroi[1], Shinya Okumura[1], and Atsuko Miyaji[1,2]

[1] Graduate School of Engineering, Osaka University
[2] Japan Advanced Institute of Science and Technology

Abstract. Akiyama, Goto, Okumura, Takagi, Nuida and Hanaoka introduced an indeterminate equation analogue of learning with errors (IE-LWE) problem as a new computationally hard problem and constructed a candidate of post-quantum cryptosystem, called "Giophantus". Giophantus satisfies the indistinguishability under chosen plaintext attack (IND-CPA) if IE-LWE problem is computationally infeasible. Akiyama et al., Shimizu and Ikematsu proposed improved Giophantus to the post-quantum standardization project. Beullens, Castryck and Vercauteren proposed an evaluation at one attack against IND-CPA security of Giophantus. However, Akiyama et al. assert that recommended parameters can resist Vercauteren et al.'s attack. Therefore, the security analysis on Giophantus is still needed.

In this paper, we propose a new kind of evaluation attack against IND-CPA security of Giophantus. Our attack solves IE-LWE problem by combining a part of Vercauteren et al.'s attack with a lattice attack on low rank lattices, e.g., 6-rank lattices for recommended parameters. Moreover, we investigate a way to avoid our attack and some variants of our attack. We give some remarks on modification of the IE-LWE problem. Our experimental analysis shows that our attack can solve IE-LWE problem efficiently, and that Giophantus does not satisfy IND-CPA security unless IE-LWE problem is modified appropriately.

Keywords: IE-LWE problem · evaluation at one attack · closest vector problem.

1 Introduction

Post-quantum cryptography now becomes a central role in cryptography as can be seen from the post-quantum cryptography standardization project (PQC project) by the National Institute of Standards and Technology (NIST) [15]. Some computationally hard problems arising from lattice theory, coding theory and algebraic geometry (solving multivariate polynomial systems) have successfully provided various candidates of post-quantum cryptographic protocols [7, 11, 14, 18]. However, the development of attacks on known computationally hard problems make difficult constructing efficient and practical post-quantum cryptographic protocols. Therefore, finding new computationally hard problems, which are also hard even by using sufficiently large scale quantum computers, is an important task in post-quantum cryptography.

At SAC 2017, Akiyama, Goto, Okumura, Takagi, Nuida and Hanaoka [1] introduced the smallest solution problem and an indeterminate equation analogue of learning with errors (IE-LWE) problem as new computationally hard problems. The smallest solution problem is that given a polynomial $F \in R_p[x, y]$, where $R_p := \mathbb{F}_p[t]/(t^n - 1)$ for a prime p, find a solution $(x, y) = (u_x, u_y) \in R_p^2$ with small coefficients to $F = 0$. IE-LWE problem is roughly described as follows: Given a pair (X, Y) of polynomials in $R_p[x, y]$, distinguish whether (X, Y) is chosen from a 'noisy' set in $R_p[x, y] \times R_p[x, y]$ or not. For more detail, see sections 2.2 and 3.1. The smallest solution problem and the IE-LWE problem are expected to be computationally infeasible even by large scale quantum computers because these problems are reduced to the (approximate) closest vector problem (CVP) on lattices with large rank, which is usually used as a computational hard problem to construct candidates of post-quantum cryptographic protocols.

Akiyama et al. constructed a candidate of post-quantum cryptosystem, which was named "Giophantus$^{\mathrm{TM}}$" later, based on the small solution problem [1]. (We refer to Akiyama et al's cryptosystem as "Giophantus" for short.) Giohantus is not only a candidate of post-quantum cryptosystem but also a multi-bit somewhat homomorphic encryption scheme (cf. [3, Section 11.1]). The smallest solution problem is (almost) equivalent to the recovering secret key problem of Giophantus, and Akiyama et al. proved that Giophantus satisfies the indistinguishability under chosen plaintext attack (IND-CPA) under the assumption that IE-LWE problem is computationally infeasible (cf. [1, Theorem 1]). Akiyama et al. described a key recovery attack and a linear algebra attack, which are based on lattice attacks, and experimentally analyzed their difficulty. Akiyama et al. set recommended parameters according to their experimental analysis and concluded that sizes of public/secret keys of Giophantus are relatively small among well-known candidates of post-quantum cryptosystems, e.g., LWE base [13] and NTRU base [16] cryptosystems (cf. [1, Table 4]). The two properties are important in post-quantum cryptography.

However, at PQCrypto 2018, Xagawa [17] proposed some attacks on Giophantus and firstly suceeded in recovering (partial/full) messages and secret keys of Giophantus for recommended parameters by lattice attacks. Xagawa's attacks decrease ranks of lattices occurring in lattice attacks by applying Gentry's technique for attacking NTRU [10] to recover partial messages and partial secret keys of Giophantus. Xagawa also applied subring technique, which also decreases ranks of lattices by substituting 0 for a variable x (or y) of multivariate polynomials occurring in Giophantus, and succeeded in recovering messages in the case of $\deg(X) = 2$. In order to avoid Xagawa's attacks, a parameter n (degree of modulus polynomial $t^n - 1$) must be increased and should be a prime number, and thus Akiyama et al. modified recommended parameters of Giophantus by executing many experiments and by using "2016 Estimate" [4].

After modifying parameters and security analysis, Akiyama et al., Shimizu and Ikematsu submitted Giophantus [2] to NIST's PQC project. Akiyama et al.'s experiments show that Giophantus with modified parameters is expected to resist Xagawa's attacks. However, Vercauteren, Beullens and Castryck [5] submitted a distinguishing attack for breaking IND-CPA security of Giophantus to official comments of NIST's PQC project. Their attack is based on the fact that a map $\varphi : \mathbb{F}_p[t]/(t^n - 1) \longrightarrow \mathbb{F}_p$ by $f(t) \pmod{t^n - 1} \mapsto f(1) \pmod{p}$ is a ring homomorphism, which is similar to an attack on the Poly-LWE problem [8]. Vercauteren et al.'s attack tries to recover partial messages by substituting 1 for a variable t of ciphertext and by searching small secret elements in small range (see section 3.3 for more detail). We refer to a kind of this attack as an evaluation attack.

Akiyama et al. [3, Section 7.3] analyzed Vercauteren et al.'s attack by many experiments and concluded that recommended parameters of Giophantus can resist Vercauteren et al.'s attack. However, Vercauteren et al.'s attack suggests that there would exist evaluation (at one or at other special values) attacks which can break IND-CPA security of Giophantus. We investigate such evaluation attacks.

1.1 Our Contribution

Our contribution in this paper is sammarized as follows:

1. **Breaking IND-CPA Security of Giophantus**
We propose a new and practical evaluation at one attack on IND-CPA security of Giophantus. Our attack reduces the IE-LWE problem to the closest vector problem (CVP) on low rank lattices, e.g., 6-rank lattices for recommended parameters, by substituting 1 for a variable occurring in the IE-LWE problem, which is similar to the first step of Vercauteren et al.'s attack and an attack on Poly-LWE problem [8]. We note that the dimension of lattices occurring in our attack is also low, e.g., 9-dimensional lattices (with 6-rank) for recommended parameters. We can use exact CVP algorithm which can solve CVP exactly for such lattices. This is an advantage of our attack. Another advantage of our attack is that our attack does not require to search small secret elements, and thus our attack is efficient. We conducted many experiments on our attack by using exact CVP algorithm in computational algebra system Magma [6] and conclude that our attack is efficient (within 4 seconds in average) and can break IND-CPA security with high probability (about 99%). Our implementation of our attack is available at `https://github.com/Shinya-Okumura/S.O..git`.
2. **Modification of Giophantus**
We investigate a way to modify Giophantus to avoid our attack. The IE-LWE problem is characterized by two modulus parameters (a prime number p and a univariate polynomial $t^n - 1$) and by multivariate polynomials. An easy way to avoid our attack is to change the modulus polynomial from $t^n - 1$ to other polynomials $f \in \mathbb{F}_p[t]$ satisfying $f(1) \not\equiv 0 \pmod{p}$. We, however, show that if the modulus polynomial f satisfies $f(\alpha) = 0$ for a small order

$\alpha \in \mathbb{F}_{p^d}$ with any d, i.e., $\alpha^k = 1$ for a small $k \ll n$, then the difficulty of the IE-LWE problem w.r.t. f is decreased as in the Poly-LWE problem [9, 12]. We note that the extension degree d should be small, e.g., $1 \leq d \leq 3$, in the case of attacking the Poly-LWE problem, but the condition on d is not required in the case of attacking the (modified) IE-LWE problem (see section 6). This means that the condition $f(1) \not\equiv 0 \pmod{p}$ is not enough to construct IND-CPA secure Giophantus. As a result, we recommend to use polynomials f with small coefficients, which has roots of large order, e.g., the q-th cyclotomic polynomial with prime power integers q.

1.2 Remark

We remark that Giophantus could not move on to the second round of NIST's PQC project [15], which is mainly due to Vercauteren et al.'s attack. As we mentioned above, the effectiveness of Vercauteren et al.'s attack is still unclear (there is no verification that Akiyama et al.'s analysis is enough). To our best knowledge, our attack is the first attack that determines the correctness of NIST's PQC project members. However, we believe that the study of the IE-LWE problem (and its variants) is still important and interesting for post-quantum cryptography.

1.3 Organization

This paper is organized as follows: Section 2 gives some notation used in this paper. Section 3 describes Giophantus, the IE-LWE problem and some possible attacks on Giophantus. Section 4 describes our evaluation attack. Section 5 gives our experimental results on our attack. Section 6 discusses the modification of the IE-LWE problem and variants of our attack. Section 7 concludes our work.

2 Preliminary

We define some notation used in this paper. Let p be a prime number and $\mathbb{Z}$ the (rational) integer ring. Suppose that any element in $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is represented by integers in $\{0, \ldots, p-1\}$. Set $R_p = \mathbb{F}_p[t]/(t^n - 1)$. For an integer $\ell \ll p$, let R_ℓ be the subset of R_p consisting of all polynomials with coefficients represented by integers in $\{0, \ldots, \ell - 1\}$. For a commutative ring R, we write a two-variable polynomial $A(x, y)$ over R as

$$A(x, y) = \sum_{(i,j) \in \Gamma_A} a_{ij} x^i y^j \ (a_{ij} \in R),$$

where Γ_A is a finite subset of $\mathbb{Z}^2_{\geq 0}$.

2.1 IE-LWE problem

We explain the IE-LWE problem in this section. For finite sets $\mathit{\Gamma}_r$, $\mathit{\Gamma}_{Xr} \subset \mathbb{Z}_{\geq 0}$, we define

$$\begin{aligned}
\mathfrak{F}_{\mathit{\Gamma}_r/R_p} &:= \left\{ \sum_{(i,j)\in \mathit{\Gamma}_r} a_{ij}x^iy^j \middle| a_{ij} \in R_p \right\}, \\
\mathfrak{F}_{\mathit{\Gamma}_{X_r}/R_\ell} &:= \left\{ \sum_{(i,j)\in \mathit{\Gamma}_{Xr}} a_{ij}x^iy^j \middle| a_{ij} \in R_\ell \right\}, \\
\mathfrak{X}(\mathit{\Gamma}_X, \ell)/R_p &:= \{ X \in \mathfrak{F}_{\mathit{\Gamma}_X}/R_p \mid \exists u_x, u_y \in R_\ell,\ X(u_x, u_y) = 0 \}\,.
\end{aligned}$$

We assume

$$(0,0) \in \mathit{\Gamma}_X, (0,0) \in \mathit{\Gamma}_r.$$

For given polynomial sets $\mathfrak{X}(\mathit{\Gamma}_X, \ell)/R_p$, $\mathfrak{F}_{\mathit{\Gamma}_r}/R_p$ and $\mathfrak{F}_{\mathit{\Gamma}_{X_r}}/R_\ell$, we define the IE-LWE problem as follows:

Definition 1 (IE-LWE Problem). *Write U_X and T_X as follows:*

$$\begin{aligned}
&U_X = \mathfrak{X}(\mathit{\Gamma}_X, \ell)/R_p \times \mathfrak{F}_{\mathit{\Gamma}_{X_r}}/R_p, \\
&T_X = \{(X, Xr + e) | X \in \mathfrak{X}(\mathit{\Gamma}_X, \ell)/R_p, r \in \mathfrak{F}_{\mathit{\Gamma}_r}/R_p, \quad e \in \mathfrak{F}_{\mathit{\Gamma}_{X_r}}/R_\ell\}.
\end{aligned}$$

The IE-LWE problem is a problem that for a given pair of polynomials $(X, Y) \in U_X$, determine whether (X, Y) is in T_X or not.

For a set A, the notation $a \overset{U}{\leftarrow}$ means that an element a is sampled from A according to the uniform distribution on A.

Definition 2 (IE-LWE Assumption). *Let p, ℓ, n, $\mathfrak{X}(\mathit{\Gamma}_X, \ell)/R_p$, $\mathfrak{F}_{\mathit{\Gamma}_r}/R_p$ and $\mathfrak{F}_{\mathit{\Gamma}_{X_r}}/R_\ell$ be as above. The IE-LWE assumption is the assumption that for a security parameter k and any probabilistic polynomial-time algorithm $\mathfrak{A}$ for the IE-LWE problem, the advantage of $\mathfrak{A}$ defined as*

$$Adv_{\mathfrak{A}}^{\textit{IE-LWE}}(k) :=$$

$$\left| \begin{array}{l}
Pr\left[\mathfrak{A}(p, \ell, n, \mathit{\Gamma}_r, \mathit{\Gamma}_X, X, Y) \rightarrow 1 \middle| \begin{array}{l} (p, \ell, n, \mathit{\Gamma}_X, \mathit{\Gamma}_r, X) \leftarrow Gen(1^k); \\ r \overset{U}{\leftarrow} \mathfrak{F}_{\mathit{\Gamma}_r}/R_p; e \overset{U}{\leftarrow} \mathfrak{F}_{\mathit{\Gamma}_{Xr}}/R_\ell; \\ Y := Xr + e \end{array} \right] \\
-Pr\left[\mathfrak{A}(p, \ell, n, \mathit{\Gamma}_r, \mathit{\Gamma}_X, X, Y) \rightarrow 1 \middle| \begin{array}{l} (p, \ell, n, \mathit{\Gamma}_X, \mathit{\Gamma}_r, X) \leftarrow Gen(1^k); \\ \\ Y \overset{U}{\leftarrow} \mathfrak{F}_{\mathit{\Gamma}_{Xr}}/R_p \end{array} \right]
\end{array} \right|$$

is negligible, where $\mathrm{Gen}(1^k)$ *is a function that outputs parameters p, ℓ, n, $\mathit{\Gamma}_X$, $\mathit{\Gamma}_r$ and $X \in \mathfrak{X}(\mathit{\Gamma}_X, \ell)/R_p$ for input k.*

2.2 Smallest-Solution Problem

For a given $X \in \mathfrak{X}(\mathit{\Gamma}_X, \ell)/R_p$, let us express a solution $u = (u_x, u_y) \in R_\ell^2$ of an integerminate equation $X = 0$ as

$$u_x = \sum_{i=0}^{n-1} \overline{\alpha}_i t^i,\ u_y = \sum_{i=0}^{n-1} \overline{\beta}_i t^i\ (\overline{\alpha}_i, \overline{\beta} \in R_\ell).$$

Let α_i and β_i be integers representing $\overline{\alpha}_i$ and $\overline{\beta}_i$, respectively, for $0 \le i \le n-1$. Then, we define the norm of the solution $u := (u_x, u_y)$ as follows:

$$\mathrm{Norm}(u) = \max\{\alpha_i, \beta_i \in \{0, ..., \ell - 1\} \mid 0 \le i \le n-1\}.$$

The smallest solution problem is defined as follows:

Definition 3 (Smallest Solution Problem). *Let $X \in R_p[x, y]$ be as above. If $X(x, y) = 0$ is an indeterminate equation over the ring R_p, then a problem of finding a solution $(x, y) = (u_x, u_y)$ to $X = 0$ over R_p with the smallest norm is called a smallest solution problem on X.*

The IE-LWE problem is not more difficult than the smallest solution problem. In fact, let $(X, Y) \in \mathfrak{X}(\mathit{\Gamma}_X, \ell)/R_p \times \mathfrak{F}_{\mathit{\Gamma}_{X_r}}/R_p$ be a sample, which we want to distinguish, and $(u_x, u_y) \in R_\ell$ a solution to the smallest solution problem on X. If (X, Y) is an IE-LWE instance, i.e., $(X, Y) \in T_X$, and the equation (1) below is true, then all coefficients of

$$\ell \cdot Y(u_x, u_y) = \ell \cdot e(u_x, u_y)$$

are less than p and multiples of ℓ (note that we regard all coefficients of $\ell \cdot Y(u_x, u_y)$ as integers, and that any integer $> p$ is reduced by modulo p). If Y is sampled from $\mathfrak{F}_{\mathit{\Gamma}_{X_r}}/R_p$ uniformly at random, then the probability that all coefficients of $\ell \cdot Y(u_x, u_y)$ are less than p and multiples of ℓ (as integers) is about $1 - 1/\ell^n$ which is non-negligible. Therefore, if the smallest solution problem can be solved, then we can solve the IE-LWE problem by checking whether all coefficients of $\ell \cdot Y(u_x, u_y)$ are less than p and multiples of ℓ or not.

3 Description of Giophantus and Known Attacks

In this section, we briefly review Akiyama et al.'s encryption scheme "Giophantus" [1–3] and some possible attacks on Giophantus.

3.1 Giophantus and IE-LWE Problem

Here we describe Giophantus, which is IND-CPA secure under the IE-LWE assumption, proposed by Akiyama et al. at SAC 2017. Let p and ℓ be a prime number and a positive integer, respectively, that satisfy $\ell \ll p$ (as in Section 2). Furthermore, for X, $r \in R_p[x, y]$, w_X and w_r denote the total degrees of X and

r, respectively. In order to decrypt any ciphertext correctly, it is necessary to satisfy the following relation for p and ℓ:

$$p > \#\mathit{\Gamma}_{X_r} \cdot \ell(\ell-1) \cdot (n(\ell-1))^{w_X+w_r}. \tag{1}$$

Next, we describe procedures of key generation, encryption and decryption processes.

- Key Generation
  Choose $u_x,\ u_y \in R_\ell$ uniformly at random with $\deg(u_x) = \deg(u_y) = n-1$ and generate $X(x,y) \in R_p[x,y]$ satsifying $X(u_x,u_y) = 0$ as follows:
  1. Choose a finite set $\mathit{\Gamma}_X \subset (\mathbb{Z}_{\geq 0})^2$ with $(0,0) \in \mathit{\Gamma}_X$.
  2. For each $(i,j) \in \mathit{\Gamma}_X \smallsetminus \{(0,0)\}$, choose $a_{ij} \in R_p$ uniformly at random.
  3. Put $a_{00} = -\sum_{(i,j)\in\mathit{\Gamma}_X\smallsetminus\{(0,0)\}} a_{ij}u_x^i u_y^j$.
  4. Put $X(x,y) = \sum_{(i,j)\in\mathit{\Gamma}_X} a_{ij}x^i y^j$.

  The $X(x,y)$ is a public key, and (u_x,u_y) is a secret key of Giophantus, respectively.
- Encryption
  1. Embed a plaintext M in the coefficients of the plaintext polynomial $m \in R_\ell$.
  2. Choose a polynomial $r(x,y) \in \mathfrak{F}_{\mathit{\Gamma}_r}/R_p$ uniformly at random.
  3. Choose a polynomial $e(x,y) \in \mathfrak{F}_{X_r}/R_\ell$ uniformly at random.
  4. We set a cipher polynomial $c(x,y)$ as follows:

  $$c(x,y) = m + X(x,y)r(x,y) + \ell \cdot e(x,y).$$
- Decryption
  1. Substitute the smallest solution (u_x,u_y) into $c(x,y)$ and obtain

  $$c(u_x,u_y) = m + \ell \cdot e(u_x,u_y).$$

  2. If p and ℓ satisfy the condition of (1), then all coefficiens of $m + \ell \cdot e(u_x,u_y) \in \mathbb{Z}[t]/(t^n-1)$ are in the range $\{0,\ldots,p-1\}$. Compute $m' = c(u_x,u_y)$ (mod. ℓ) (note that we regard the coefficients of $c(u_x,u_y)$ as integers). If p and ℓ satisfy the condition of (1), then all coefficients of $c(u_x,u_y) = m + \ell e(u_x,u_y)$ are smaller than p. Thus we have $m = m'$.
  3. Recover the plaintext M from the coefficients of m.

Akiyama et al. proved that Giophantus is IND-CPA secure if the IE-LWE problem is computationally infeasible. More precisely, the following theorem holds true [3, Theorem 2].

Theorem 1. *We denote by $\mathit{\Sigma}$ the Giophantus encryption scheme. For a security parameter k, let* $\mathrm{Adv}_{\mathfrak{A}}^{\text{IE-LWE}}(k)$ *be as in Definition 2. Similarly, we denote by* $\mathrm{Adv}_{\mathfrak{B},\mathit{\Sigma}}^{\text{IND-CPA}}(k)$ *the advantage of the probabilistic polynomial time algorithm $\mathfrak{B}$ for breaking IND-CPA security of Giophantus. Then we have*

$$\mathrm{Adv}_{\mathfrak{B},\mathit{\Sigma}}^{\text{IND-CPA}}(k) = 2\mathrm{Adv}_{\mathfrak{A}}^{\text{IE-LWE}}(k).$$

Akiyama et al., Xagawa and Vercauteren et al. proposed some possible attacks on Giophantus. In sections 2.2 and 2.3, we briefly review Akiyama et al.'s linear algebra attack and Vercauteren et al.'s evaluation attack because these two attacks are closely related to our new attack.

3.2 Linear Algebra Attack

For a given polynomial pair (X, Y), we can determinate that (X, Y) is sampled from T_X if we find $r \in \mathfrak{F}_{\Gamma_r}/R_p$ and $e \in \mathfrak{F}_{\Gamma_{X_r}}/R_\ell$ such that $Y = Xr + e$. The problem of finding such polynomials r and e can be solved by comparing the coefficients of $x^i y^j$. To make a linear equation, put $X = \sum_{(i,j)\in\Gamma_X} a_{ij}x^i y^j,\ r = \sum_{(i,j)\in\Gamma_r} r_{ij}x^i y^j,\ e = \sum_{(i,j)\in\Gamma_e} e_{ij}x^i y^j$ and $Y = \sum_{(i,j)\in\Gamma_Y} d_{ij}x^i y^j$, where r_{ij} and e_{ij} are variables. We have

$$\sum_{(i,j)\in\Gamma_{X_r}} d_{ij}x^i y^j = \left(\sum_{(i,j)\in\Gamma_X} a_{ij}x^i y^j\right)\left(\sum_{(i,j)\in\Gamma_r} r_{ij}x^i y^j\right) + \left(\sum_{(i,j)\in\Gamma_{Xr}} e_{ij}x^i y^j\right).$$

Consider the case of deg $X =$ deg $r = 1$. Write the polynomials X, r, e and Y as

$$\begin{aligned} X(x,y) &= a_{10}x + a_{01}y + a_{00}, \\ r(x,y) &= r_{10}x + r_{01}y + r_{00}, \\ e(x,y) &= e_{20}x^2 + e_{11}xy + e_{02}y^2 + e_{10}x + e_{01}y + e_{00}, \\ Y(x,y) &= d_{20}x^2 + d_{11}xy + d_{02}y^2 + d_{10}x + d_{01}y + d_{00}. \end{aligned}$$

From the above equation

$$\begin{aligned} X(x,y)r(x,y) = a_{10}r_{10}x^2 &+ (a_{10}r_{01} + a_{01}r_{10})xy + a_{01}r_{01}y^2 + \\ &(a_{10}r_{00} + a_{00}r_{10})x + (a_{01}r_{00} + a_{00}r_{01})y + a_{00}r_{00}, \end{aligned}$$

we get a linear equation

$$\begin{aligned} & a_{10}r_{10} + e_{20} = d_{20}, \\ & a_{10}r_{01} + a_{01}r_{10} + e_{11} = d_{11}, \\ & a_{01}r_{01} + e_{02} = d_{02}, \\ & a_{10}r_{00} + a_{00}r_{10} + e_{10} = d_{10}, \\ & a_{01}r_{00} + a_{00}r_{01} + e_{01} = d_{01}, \\ & a_{00}r_{00} + e_{00} = d_{00}. \end{aligned} \tag{2}$$

If an R_ℓ-valued solution $\{e_{ij}\}_{(i,j)\in\Gamma_{Xr}}$ is found, then (X, Y) is sampled from T_X. In order to avoid a typical brute force attack on polynomial e, the form $\#\Gamma_{Xr}$ is necessary to satisfy

$$((\ell - 1)\ell^{n-1})^{\#\Gamma_{Xr}} > 2^k,$$

where k is a security parameter. Next we use a lattice reduction attack to find a small e_{ij}. Represent a_{10} as follows:

$$a_{10} = a^{(10)}_{n-1}t^{n-1} + \cdots + a^{(10)}_0.$$

When $r_{10}, d_{20} \in R_p$ and $e_{20} \in R_\ell$ are represented in the same way as a_{10}, then $a_{10}r_{10} + e_{20} = d_{20}$ can be represented as follows:

$$\begin{pmatrix} a_{n-1}^{(10)} & a_{n-2}^{(10)} & \cdots & a_1^{(10)} & a_0^{(10)} \\ a_{n-2}^{(10)} & a_{n-3}^{(10)} & \cdots & a_0^{(10)} & a_{n-1}^{(10)} \\ a_{n-3}^{(10)} & a_{n-4}^{(10)} & \cdots & a_{n-1}^{(10)} & a_{n-2}^{(10)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_0^{(10)} & a_{n-1}^{(10)} & \cdots & a_2^{(10)} & a_1^{(10)} \end{pmatrix} \begin{pmatrix} r_0^{(10)} \\ r_1^{(10)} \\ \vdots \\ r_{n-2}^{(10)} \\ r_{n-1}^{(10)} \end{pmatrix} + \begin{pmatrix} e_{n-1}^{(20)} \\ e_{n-2}^{(20)} \\ \vdots \\ e_1^{(20)} \\ e_0^{(20)} \end{pmatrix} = \begin{pmatrix} d_{n-1}^{(20)} \\ d_{n-2}^{(20)} \\ \vdots \\ d_1^{(20)} \\ d_0^{(20)} \end{pmatrix}.$$

Thus the first equation (2) can be written as

$$A_{10}\boldsymbol{r}_{10} + \boldsymbol{e}_{20} = \boldsymbol{d}_{20}, \tag{3}$$

where

$$A_{10} = \begin{pmatrix} a_{n-1}^{(10)} & a_{n-2}^{(10)} & \cdots & a_1^{(10)} & a_0^{(10)} \\ a_{n-2}^{(10)} & a_{n-3}^{(10)} & \cdots & a_0^{(10)} & a_{n-1}^{(10)} \\ a_{n-3}^{(10)} & a_{n-4}^{(10)} & \cdots & a_{n-1}^{(10)} & a_{n-2}^{(10)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_0^{(10)} & a_{n-1}^{(10)} & \cdots & a_2^{(10)} & a_1^{(10)} \end{pmatrix}, \ \boldsymbol{r}_{10} = \begin{pmatrix} r_0^{(10)} \\ r_1^{(10)} \\ \vdots \\ r_{n-2}^{(10)} \\ r_{n-1}^{(10)} \end{pmatrix},$$

$$\boldsymbol{e}_{20} = \begin{pmatrix} e_{n-1}^{(20)} \\ e_{n-2}^{(20)} \\ \vdots \\ e_1^{(20)} \\ e_0^{(20)} \end{pmatrix}, \ \boldsymbol{d}_{20} = \begin{pmatrix} d_{n-1}^{(20)} \\ d_{n-2}^{(20)} \\ \vdots \\ d_1^{(20)} \\ d_0^{(20)} \end{pmatrix}.$$

The equation (3) is an equation over $\mathbb{F}_p$, and we lift the equation (3) to an equation over $\mathbb{Z}$ by adding an integer vector $\boldsymbol{g}_{20}$ to the left-hand side of (3):

$$A_{10}\boldsymbol{r}_{10} + \boldsymbol{e}_{20} + p\boldsymbol{g}_{20} = \boldsymbol{d}_{20}.$$

We consider the integer lattice $\mathcal{L}$ with the basis matrix $(A_{10}\ pI_n)$. If $\boldsymbol{v} \in \mathcal{L}$ is a vector closest to $\boldsymbol{d}_{20}$, then we can expect that a short vector $\pm\boldsymbol{e}_{20}$ is found by calculating $\boldsymbol{d}_{20} - \boldsymbol{v}$. In order to find all $\boldsymbol{e}_{ij}$, one needs to deal with all equations of (2) simultaneously. See [3] for more detail. This means that the IE-LWE problem can be reduced to the closest vector problem (CVP) on the lattice $\mathcal{L}$. This attack is called the linear algebra attack.

3.3 Vercauteren et al.'s Evalution Attack

In this section, we describe Vercauteren et al.'s evaluation attack that tries to break IND-CPA security of Giophantus. This attack uses the fact that a map $R_p = \mathbb{F}_p[t]/(t^n - 1) \longrightarrow \mathbb{F}_p$ by $a(t) \mapsto a(1)$ is a well-defined ring homomorphism.

Let $X(x,y) \in R_p[x,y]$ and $(u_x(t), u_y(t)) \in R_\ell^2$ be the public key and the secret key of Giophantusas, respectively, in section 3.1. The detailed description is as follows:

1. We obtain the equation $X(x,y,1) = 0$ over $\mathbb{F}_p$, where $X(x,y,1)$ means the image of $X(x,y)$ under a map $R_p[x,y] \longrightarrow \mathbb{F}_p[x,y]$ by $\sum f_{ij}(t)x^iy^j \mapsto \sum f_{ij}(1)x^iy^j$.
2. Perform exhaustive search to find a solution (u'_x, u'_y) to $X(x,y,1) = 0$ over $\mathbb{F}_p$ such that u'_x and u'_y are represented by integers in $\{0, \dots, n(\ell-1)\}$. The existence of such a solution is guaranteed by $X(u_x(1), u_x(1), 1) = 0$. In fact, if the secret key is represented as
$$(u_x, u_y) = \left(\sum_{i=0}^{n-1} \overline{\alpha}_i t^i,\ \sum_{i=0}^{n-1} \overline{\beta}_i t^i\right)\ (0 \leq \alpha_i, \beta_i \leq \ell - 1),$$
then we have
$$0 \leq \max\left\{\sum \alpha_i, \sum \beta_i\right\} \leq n(\ell-1),$$
where α_i and β_i are integers representing $\overline{\alpha}_i$ and $\overline{\beta}_i$, respectively. The smallest solution (u'_x, u'_y) can be found in two ways.
   - Choose $\overline{\alpha}_x, \overline{\alpha}_y \in \{\overline{0}, \dots, \overline{n(\ell-1)}\} \subset \mathbb{F}_p$ and check whether $X(\overline{\alpha}_x, \overline{\alpha}_y, 1) = 0$ or not.
   - Choose $\overline{\alpha} \in \{\overline{0}, \dots, \overline{n(\ell-1)}\} \subset \mathbb{F}_p$ and check whether $X(\overline{\alpha}, y, 1)$ has a factor of the form $(y - \overline{\beta})$ with $0 \leq \beta \leq n(\ell-1)$ or not.
3. Let m_0 and m_1 be plaintext polynomials in R_ℓ with $m_0(1) \not\equiv m_1(1)$ (mod. ℓ). Randomly choose $b \in 0, 1$ and put $c(x,y) = m_b + X(x,y)r(x,y) + \ell e(x,y)$. Substitute (u'_x, u'_y) for x and y of $c(x,y)$, respectively, and calculate
$$c(u'_x, u'_y, 1) \equiv m_b(1) + \ell \cdot e(u'_x, u'_y, 1) \pmod{\ell}.$$
4. Calculate $m'_b \equiv c(u'_x, u'_y, 1)$ (mod. ℓ).
5. Under the condition $m_0(1) \not\equiv m_1(1)$ (mod. ℓ), we determine the value of b by comparing $m_0(1)$, $m_1(1)$ and m'_b (mod. ℓ).

To get $m_b(1)$ (mod. ℓ) in Step 4, the modulus p needs to satisfy
$$p > \max\{c(u'_x, u'_y, 1) \mid 0 \leq u'_x, u'_y \leq n(\ell-1)\}.$$

To estimate the value of $c(u'_x, u'_y, 1)$, we consider
$$\begin{aligned} c(u'_x, u'_y, 1) &= m_b(1) + \ell \cdot e(u'_x, u'_y) \\ &= m_b(1) + \ell \cdot \sum_{(i,j) \in \Gamma_e} e_{ij}(1)(u'_x)^i(u'_y)^j. \end{aligned}$$

Since
$$0 \leq m_b(1), e_{ij}(1) \leq n(\ell-1),$$

We have

$$\begin{aligned}
&\max\{c(u'_x, u'_y, 1) \mid 0 \le u'_x, u'_y \le n(\ell-1)\}\\
&\le n(\ell-1) + \ell \cdot \sum_{(i,j)\in\Gamma_e} (n(\ell-1))^{i+j+1}\\
&\le n(\ell-1) + \ell \cdot \sum_{k=0}^{dX+dr} (k+1)(n(\ell-1))^{k+1},
\end{aligned}$$

which is much larger than p if p is the smallest prime number satisfying the inequality (1). Therefore, the above attack does not work well. However, Vercauteren et al. pointed out that the distribution of $c(u'_x, u'_y, 1)$ over the integers would leak information of $m_b(1)$, and thus Akiyama et al. conducted many experiments on the distribution of $c(u'_x, u'_y, 1)$. As a result of their experiments, the distribution of $c(u'_x, u'_y, 1)$ does not leak any information of plaintext polynomials for recommended parameters of Giophantus.

4 Our Evaluation Attack

In this section, we describe our new evaluation attack. An idea of our evaluation attack is similar to Vercauteren et al.'s evaluation attack in section 3.3 and a known attack on Poly-LWE [8]. The main difference between our attack and those attacks is that our attack does not require to search some partial information of secret keys. In our attack, we reduce the IE-LWE problem to CVP on low rank lattices, e.g., 6-rank for recommended parameters. We can solve such CVP efficiently. The detailed description of our attack is as follows: Let (X, Y) be as in section 3.2. By substituting $t = 1$ for the equation (2) and by adding ph_{ij} ($h_{ij} \in \mathbb{Z}$ to each equation of (2), we obtain a new linear equation over $\mathbb{Z}$

$$\begin{aligned}
&a_{10}(1)r_{10}(1) + e_{20}(1) + ph_{20} = d_{20}(1),\\
&a_{10}(1)r_{01}(1) + a_{01}(1)r_{10}(1) + e_{11}(1) + ph_{11} = d_{11}(1),\\
&a_{01}(1)r_{01}(1) + e_{02}(1) + ph_{01} = d_{02}(1),\\
&a_{10}(1)r_{00}(1) + a_{00}(1)r_{10}(1) + e_{10}(1) + ph_{10} = d_{10}(1),\\
&a_{01}(1)r_{00}(1) + a_{00}(1)r_{01}(1) + e_{01}(1) + ph_{01} = d_{01}(1),\\
&a_{00}(1)r_{00}(1) + e_{00}(1) + ph_{00} = d_{00}(1).
\end{aligned}$$

We write $a_{ij}(1)$ as a_{ij} for simplicity. By regarding $r_{ij}(1)$ and $e_{ij}(1)$ as variables, we have the linear equations:

$$\begin{pmatrix} a_{10} & 0 & 0 & p & 0 & 0 & 0 & 0 & 0 \\ a_{01} & a_{10} & 0 & 0 & p & 0 & 0 & 0 & 0 \\ 0 & a_{01} & 0 & 0 & 0 & p & 0 & 0 & 0 \\ a_{00} & 0 & a_{10} & 0 & 0 & 0 & p & 0 & 0 \\ 0 & a_{00} & a_{01} & 0 & 0 & 0 & 0 & p & 0 \\ 0 & 0 & a_{00} & 0 & 0 & 0 & 0 & 0 & p \end{pmatrix} \begin{pmatrix} r_{10} \\ r_{01} \\ r_{00} \\ h_{20} \\ h_{11} \\ h_{02} \\ h_{10} \\ h_{01} \\ h_{00} \end{pmatrix} + \begin{pmatrix} e_{20} \\ e_{11} \\ e_{02} \\ e_{10} \\ e_{01} \\ e_{00} \end{pmatrix} = \begin{pmatrix} d_{20} \\ d_{11} \\ d_{02} \\ d_{10} \\ d_{01} \\ d_{00} \end{pmatrix}.$$

If (X, Y) is an IE-LWE instance, then we have $0 \leq e_{ij} \leq n(\ell - 1)$. We see that $n(\ell - 1)$ is much smaller than p from the inequality (1). Thus if we can find a vector closest to $(d_{20}\ d_{11}\ d_{02}\ d_{10}\ d_{01}\ d_{00})^{\mathrm{T}}$ in the lattice generated by the column vectors of

$$\begin{pmatrix} a_{10} & 0 & 0 & p & 0 & 0 & 0 & 0 & 0 \\ a_{01} & a_{10} & 0 & 0 & p & 0 & 0 & 0 & 0 \\ 0 & a_{01} & 0 & 0 & 0 & p & 0 & 0 & 0 \\ a_{00} & 0 & a_{10} & 0 & 0 & 0 & p & 0 & 0 \\ 0 & a_{00} & a_{01} & 0 & 0 & 0 & 0 & p & 0 \\ 0 & 0 & a_{00} & 0 & 0 & 0 & 0 & 0 & p \end{pmatrix}.$$

We obtain a short vector $(e'_{20}, \ldots, e'_{00})^T$ (not necessarily $(e_{20}, \ldots, e_{00})^T$). As a result of solving CVP, if all e'_{ij} are equal or smaller than $n(\ell - 1)$, then we determine that (X, Y) is an IE-LWE instance. In other words, the IE-LWE problem is reduced to CVP on 6-rank lattices.

5 Experiments on Our attack

In this section, we report experimental results on our new evaluation attack described in the section 4. The procedure of our experiments is as follows:

- Randomly sample IE-LWE instances and determine whether they are IE-LWE instance or not by our attack.
- Randomly sample pairs of polynomials from U_X. Determine whether they are IE-LWE instanses or not by our attack.

In our experiments, we set $\ell = 4$, i.e., the coefficients of the secret keys (u_x, u_y) are in the range $\{0, ..., 3\}$. The number of attack experiments is 100,000 times. The computer environment is shown below.

- CPU: Intel(R)XeonCPU E7-4830 v4@2.00GHz,
- RAM: 3TB,

Table 1. Attack for IE-LWE instances

k	n	p	num. of success	success probability	average time (sec)
143	1201	467424413	100000	1	0.32235
207	1733	973190461	100000	1	0.61882
272	2267	1665292879	100000	1	3.20274

Table 2. Attack for random samples

k	n	p	num. of success	success probability	average time (sec)
143	467424413	130	99870	0.99870	0.22551
207	973190461	151	99849	0.99849	0.43368
272	1665292879	142	99858	0.99858	2.23923

- OS: Ubuntu 10.04.5 LTS,
- Software: Magma [6].

We show our experimental results in Tables 1 and 2. In Tables 1 and 2, ”num. of success” means the number of successes, respectively. From the above results, we see that our attack can efficiently solve the IE-LWE problem within 4 seconds for security parameters $k = 143, 207, 272$. When given a pair of polynomials (X, Y), it is possible to determine whether the pair is an IE-LWE instance or not, and to break the IND-CPA security of Giophantus.

6 Modification of IE-LWE Problem

In this section, we discuss how to modify the IE-LWE problem to avoid our attack and its variant described below. An easy way to avoid our attack is to use other modulus polynomials $f \in \mathbb{F}_p[t]$ satisfying $f(1) \not\equiv 0 \pmod{p}$. However, the following argument implies that the condition is not enough.

If there is a root $\alpha \in \mathbb{F}_{p^d}$ of f, i.e., $f(\alpha) = 0$, then a map $\mathbb{F}_p[t]/(f) \longrightarrow \mathbb{F}_{p^d}$ by $a(t) \mapsto a(\alpha)$ is a well-defined ring homomorphism. We assume that $\alpha^w = 1$ for $w < n - 1$. For simplicity, we also assume $w \mid (n - 1)$, say $n - 1 = ww'$. Put $n_f := \deg(f)$ and $R_p^{(f)} := \mathbb{F}_p[t]/(f)$. Let $R_\ell^{(f)}$ be the subset of $R_p^{(f)}$ defined by the same way as R_ℓ. A variant of the IE-LWE problem is defined by replacing R_p and R_ℓ in Definition 1 by $R_p^{(f)}$ and $R_\ell^{(f)}$, respectively. We call the variant of the IE-LWE problem the IE-LWE$_f$ problem. We try to solve the IE-LWE$_f$ problem by combining the linear algebra attack in section 3.2 and evaluation attack at $t = \alpha$. For a given sample $(X_f, Y_f = X_f r_f + e_f)$ from the IE-LWE$_f$ problem, put $X_f = \sum_{(i,j)\in\Gamma_{X_f}} a_{ij}^{(f)} x^i y^j$, $r_f = \sum_{(i,j)\in\Gamma_{r_f}} r_{ij}^{(f)} x^i y^j$, $e_f = \sum_{(i,j)\in\Gamma_{e_f}} e_{ij}^{(f)} x^i y^j$ and $Y_f = \sum_{(i,j)\in\Gamma_{Y_f}} d_{ij}^{(f)} x^i y^j$, where $r_{ij}^{(f)}$ and $e_{ij}^{(f)}$ are variables. If we find that all $e_{ij}^{(f)}$ are $R_\ell^{(f)}$-values variables, then (X_f, Y_f) is an IE-LWE$_f$ instance.

Put $e_{ij}^{(f)}$ as

$$e_{n-1}^{(ij,f)}t^{n-1} + \cdots + e_0^{(ij,f)}.$$

From the assumption $\alpha^w = 1$, we have

$$\begin{aligned} e_{ij}^{(f)}(\alpha) = {} & (e_{w-1}^{(ij,f)} + \cdots + e_{w'w-1}^{(ij,f)})\alpha^{w-1} \\ & + (e_{w-2}^{(ij,f)} + \cdots + e_{w'w-2}^{(ij,f)})\alpha^{w-2} \\ & + \cdots + (e_0^{(ij,f)} + \cdots + e_{ww'}^{(ij,f)}). \end{aligned}$$

If $e_{ij}^{(f)}$ is in $R_\ell^{(f)}$, then we can regard $e_{ij}^{(f)}(\alpha)$ as a polynomial with small coefficients within $\{0, \ldots, w'(\ell-1)\}$ of degree $w-1 < n-2$. The above argument can be also applied to $a_{ij}^{(f)}$, $r_{ij}^{(f)}$ and $d_{ij}^{(f)}$, i.e., $a_{ij}^{(f)}(\alpha)$, $r_{ij}^{(f)}(\alpha)$ and $d_{ij}^{(f)}(\alpha)$ can be regarded as polynomials of degree $w-1$. We see that $w'(\ell-1) < n(\ell-1)$ is much smaller than p from the inequality (1). Thus, by applying the linear algebra attack, we can expect that the IE-LWE$_f$ problem is solved by solving the (approximate) CVP on lattices with smaller rank. The rank of lattice is reduced by applying Xagawa's method (cf. [3]). We note that $1,\ \alpha, \ldots, \alpha^{w-1}$ would be $\mathbb{F}_p$-linearly dependent elements. Thus, we need to slightly modify the linear algebra attack.

The above attack is similar to attacks on Poly-LWE problem [9,12]. However, in the case of attacking Poly-LWE problem, the extension degree d should be small, e.g., $1 \leq d \leq 3$, because one needs to find secret elements in $\mathbb{F}_{p^d}$ by exhaustive search. On the other hand, the above attack does not require to search secret elements and would work for any d.

From the above argument, we need to use modulus polynomials f whose roots have large order ($> n$) to avoid our attack in section 4 and its variant above. For instance, all roots of the m-th cyclotomic polynomial (mod. p) have order m (see [9]). Moreover, we should use modulus polynomials with small coefficients, e.g., the q-th cyclotomic polynomials with prime power integers q, so that the coefficients of $e(u_x(t), u_y(t))$ does not become so large.

Remark 1. At Symposium on Cryptography and Information Security 2019, which is a big symposium in Japan, Akiyama, Yuntao Wang, Ikematsu and Takagi announced the modified IE-LWE problem and proposed Giophantus$^+$ which is IND-CPA secure if the modified IE-LWE problem is computationally infeasible. Their modification is to use $t^k + 1$ for 2-power integer k, i.e., the $2k$-th cyclotomic polynomial, as a modulus polynomial. Akiyama et al.'s modified IE-LWE problem cannot be solved by our evaluation attack and its variant. However, Akiyama et al.'s analysis is only based on lattice attacks, and the value of k is very limited even though k is closely related to the sizes of public/secret keys and ciphertexts. Therefore, one should also consider other modifications as in our argument above.

7 Conclusion

In this paper, we proposed a new and practical evaluation attack on IND-CPA security of an indeterminate equation public key post-quantum cryptosystem, called "Giophantus". The Giophantus satisfies IND-CPA security under the assumption that an indeterminate equation analogue of learning with errors (IE-LWE) problem is computationally infeasible. However, our attack efficiently succeeded in solving the IE-LWE problem with probability about 99% within 4 seconds in average. Moreover, we investigate how to modify the IE-LWE problem to avoid our attack. We gave the notable argument and a variant of our evaluation attack. As a result, we conclude that one should use polynomials f with small coefficients, which have roots of large order, e.g., the q-th cyclotomic polynomial with prime power integers q.

Although our attack is cleary solve the IE-LWE problem with high probability, we could not give the theoretical estimate of the success probability of our attacks. Moreover, our approach for solving the IE-LWE problem is similar to known attacks on Poly-LWE problem. Therefore, our future work is to estimate the theoretical success probability and to investigate attacks of other approaches.

Acknowledgement

This work is partially supported by JSPS KAKENHI Grant(B) (JP17K18450), Grant (C)(JP15K00183), Microsoft Research Asia, CREST(JPMJCR1404) at Japan Science and Technology Agency, the Japan-Taiwan Collaborative Research Program at Japan Science and Technology Agency, and Project for Establishing a Nationwide Practical Education Network for IT Human Resources Development, Education Network for Practical Information Technologies.

References

1. Akiyama, K., Goto, Y., Okumura, S., Takagi, T., Nuida, K., Hanaoka, G.: A public-key encryption scheme based on non-linear indeterminate equations. In: Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers. pp. 215–234 (2017)
2. Akiyama, K., Goto, Y., Okumura, S., TAkagi, T., NUida, K., Hanaoka, G., Shimizu, H., Ikematsu, Y.: Indeterminate equation publickey cryptosystem (Giophantus^{tm}), in the round-1-submissions of nist pqc standardization, (2017), available at (2017), `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/`
3. Akiyama, K., Goto, Y., Okumura, S., Takagi, T., Nuida, K., Hanaoka, G., Shimizu, H., Ikematsu, Y.: A public-key encryption scheme based on non-linear indeterminate equations (giophantus). IACR Cryptology ePrint Archive **2017**, 1241 (2017), `http://eprint.iacr.org/2017/1241`

4. Albrecht, M.R., Göpfert, F., Virdia, F., Wunderer, T.: Revisiting the expected cost of solving usvp and applications to LWE. In: Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I. pp. 297–322 (2017). https://doi.org/10.1007/978-3-319-70694-8_11, https://doi.org/10.1007/978-3-319-70694-8_11
5. Beullens, W., Castryck, W., Vercauteren, F.: Ind-cpa attack on giophantus, in the official-comments to giophantus for nist round-1-submissions (2018), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/Giophantus-official-comment.pdf
6. Bosma, W., Cannon, J.J., Playoust, C.: The magma algebra system I: the user language. J. Symb. Comput. **24**(3/4), 235–265 (1997). https://doi.org/10.1006/jsco.1996.0125, https://doi.org/10.1006/jsco.1996.0125
7. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings. pp. 164–175 (2005). https://doi.org/10.1007/11496137_12, https://doi.org/10.1007/11496137_12
8. Eisenträger, K., Hallgren, S., Lauter, K.E.: Weak instances of PLWE. In: Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers. pp. 183–194 (2014). https://doi.org/10.1007/978-3-319-13051-4_11, https://doi.org/10.1007/978-3-319-13051-4_11
9. Elias, Y., Lauter, K.E., Ozman, E., Stange, K.E.: Provably weak instances of ring-lwe. In: Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I. pp. 63–92 (2015). https://doi.org/10.1007/978-3-662-47989-6_4, https://doi.org/10.1007/978-3-662-47989-6_4
10. Gentry, C.: Key recovery and message attacks on ntru-composite. In: Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding. pp. 182–194 (2001). https://doi.org/10.1007/3-540-44987-6_12, https://doi.org/10.1007/3-540-44987-6_12
11. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings. pp. 267–288 (1998). https://doi.org/10.1007/BFb0054868, https://doi.org/10.1007/BFb0054868
12. Kudo, M.: Attacks against search poly-lwe. IACR Cryptology ePrint Archive **2016**, 1153 (2016), http://eprint.iacr.org/2016/1153
13. Lindner, R., Peikert, C.: Better key sizes (and attacks) for lwe-based encryption. In: Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings. pp. 319–339 (2011). https://doi.org/10.1007/978-3-642-19074-2_21, https://doi.org/10.1007/978-3-642-19074-2_21
14. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. In: The Deep Space Network Progress Report
15. NIST: Post-quantum cryptography standardization. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

16. Stehlé, D., Steinfeld, R.: Making NTRU as secure as worst-case problems over ideal lattices. In: Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings. pp. 27–47 (2011). https://doi.org/10.1007/978-3-642-20465-4_4, `https://doi.org/10.1007/978-3-642-20465-4\_4`
17. Xagawa, K.: Practical cryptanalysis of a public-key encryption scheme based on non-linear indeterminate equations at SAC 2017. IACR Cryptology ePrint Archive **2017**, 1224 (2017), `http://eprint.iacr.org/2017/1224`
18. Yasuda, T., Sakurai, K.: A multivariate encryption scheme with rainbow. In: Information and Communications Security - 17th International Conference, ICICS 2015, Beijing, China, December 9-11, 2015, Revised Selected Papers. pp. 236–251 (2015). https://doi.org/10.1007/978-3-319-29814-6_19, `https://doi.org/10.1007/978-3-319-29814-6\_19`