J. Math. Cryptol. **8** (2014), 305–329
DOI 10.1515/jmc-2013-0024 © de Gruyter 2014

On the exact decryption range for Gentry–Halevi's implementation of fully homomorphic encryption

Masaya Yasuda, Kazuhiro Yokoyama, Takeshi Shimoyama,
Jun Kogure and Takeshi Koshiba

Communicated by Tran van Trung

Abstract. In this paper, we revisit the fully homomorphic encryption (FHE) scheme implemented by Gentry and Halevi, which is just an instantiation of Gentry's original scheme based on ideal lattices. Their FHE scheme starts from a somewhat homomorphic encryption (SHE) scheme, and its decryption range is deeply related with the FHE construction. Gentry and Halevi gave an experimental evaluation of the decryption range, but theoretical evaluations have not been given so far. Moreover, we give a theoretical upper bound, and reconsider suitable parameters for theoretically obtaining an FHE scheme. In particular, while Gentry and Halevi use the Euclidean norm evaluation in the noise management of ciphertexts, our theoretical bound enables us to use the ∞-norm evaluation, and hence it helps to lower the difficulty of controlling the noise density of ciphertexts.

Keywords. Fully homomorphic encryption, ideal lattices, bootstrapping method, re-encryption process.

2010 Mathematics Subject Classification. Primary 68R01; secondary 15A15.

1 Introduction

Fully homomorphic encryption is public key encryption that allows one to fully interact on encrypted data without decryption. Since this encryption enables one to perform arbitrary computations with protecting the data confidentiality, it has been expected to be applied to cloud computing. After Gentry's breakthrough work [8] in 2009 of constructing a fully homomorphic encryption (FHE) scheme, a number of new schemes, improvements, and implementations have been proposed (see [1, 10–12, 16] for recent papers). At present, there are mainly three variant schemes; one based on ideal lattices [8, 9, 17], another one based on integers [5, 6], and the last one based on the ring learning with errors (ring-LWE) assumption [1–3] (recently, NTRU encryption [13] has turned into an FHE scheme in [16]). Despite of rapid developments in FHE, Gentry's bootstrapping is the only known method so far to construct a "pure" FHE scheme as mentioned in [10] (cf. the leveled FHE scheme in [1]). In the bootstrapping method, it starts from a somewhat homomorphic encryption (SHE) scheme supporting a limited number of additions and multiplications on encrypted data. To make an SHE scheme fully homomorphic, the bootstrapping method transforms a "dirty" ciphertext into a "cleaner" ciphertext by means of re-encryption. To achieve this re-encryption process, it requires that the SHE scheme can evaluate its own decryption function homomorphically.

A typical implementation for a pure FHE scheme is provided by Gentry and Halevi in [9] (see [12] for implementation results of a leveled FHE scheme). Their implementation results suggest that the pure FHE does not reach a level of the practical use. Their scheme is based on ideal lattices, and it is just an instantiation of Gentry's original scheme proposed in [8]. In their SHE scheme, for key parameters (n, t) with $n = 2^m$, we fix a polynomial $v(x) = \sum_{i=0}^{n-1} v_i x^i \in R$ with $|v_i| \leq 2^t$, and consider the principal ideal lattice $L = (v(x)) \subset R$, where $R = \mathbb{Z}[x]/(x^n + 1)$ denotes the ring of integers of the $2n$-th cyclotomic field. The rotation basis and the Hermite normal form basis of L are used as the public and secret keys, respectively. To obtain an FHE scheme, Gentry and Halevi [9] choose suitable key parameters (n, t) so that the re-encryption process can be performed. However, since their key parameters are experimentally chosen, their FHE scheme seems to have a possibility to cause decryption errors for re-encrypted ciphertexts. Our motivation of this paper is to give key parameters (n, t) with a theoretical guarantee for obtaining a pure FHE scheme. Our contributions are summarized as follows:

(a) In the bootstrapping method, it is the most important to evaluate the decryption range of the SHE scheme. While Gentry and Halevi [9] give only an experimental evaluation, we give a theoretical bound on the decryption range and propose a slightly modified key generation so that our theoretical evaluation holds. Let $w(x) = \sum_{i=0}^{n-1} w_i x^i \in R$ be the polynomial satisfying $w(x) \times v(x) \equiv d \pmod{x^n + 1}$, where d denotes the determinant of the lattice L. The decryption range is deeply related with the gap $d/|w_i|$. Our approach is to study values d and $|w_i|$, separately, using fundamental tools in linear algebra, and to give an explicit evaluation of the gap.

(b) Our theoretical evaluation enables us to use the ∞-norm in evaluating the noise size of ciphertexts. The ∞-norm evaluation is independent of the noise density, and hence it helps us to lower the difficulty in the noise management (Gentry and Halevi [9] use the Euclidean norm deeply related with the noise density). Using our theoretical evaluation, we study key parameters (n, t) suitable for the FHE construction. While Gentry and Halevi [9] experimentally estimate that it is enough to take about $t = 400$, our theoretical evaluation shows that it requires about $t = 500$. In taking $t = 500$, we also show that it needs at least $n = 65536$

lattice dimension to have enough security. (Gentry and Halevi [9] only give four parameters for their FHE public challenges with lattice dimensions 512, 2048, 8192, and 32768.)

Notation. The symbols $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ denote the ring of integers, the field of rational numbers, and the field of real numbers, respectively. For two integers z and d, let $[z]_d$ denote the reduction of z modulo d included in the interval $[-d/2, d/2)$ as in [9]; as usual, let $z \pmod d$ denote the reduction z modulo d included in the interval $[0, d)$. For $\vec{a} = (a_1, a_2, \dots, a_n) \in \mathbb{R}^n$, let $\|\vec{a}\|$ denote the Euclidean norm given by

$$\|\vec{a}\| = \sqrt{\textstyle\sum_{i=1}^n a_i^2}.$$

Furthermore, we let $\|\vec{a}\|_1$ and $\|\vec{a}\|_\infty$ denote the 1-norm $\sum_{i=1}^n |a_i|$ and ∞-norm $\max_i |a_i|$, respectively.

2 Gentry–Halevi's somewhat homomorphic encryption

In this section, we briefly review the construction of Gentry and Halevi's SHE scheme (see [9, Part I] for details). For a 2-power integer $n = 2^m$, let $R = \mathbb{Z}[x]/(f_n(x))$ with $f_n(x) = x^n + 1$. Since the canonical map

$$\begin{aligned} R \ni v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1} \\ \mapsto \vec{v} = (v_0, v_1, \dots, v_{n-1}) \in \mathbb{Z}^n \end{aligned} \tag{2.1}$$

gives an isomorphism $R \simeq \mathbb{Z}^n$ as $\mathbb{Z}$-modules, we can regard each element of R as both a polynomial $v(x)$ and an n-dimensional vector $\vec{v} \in \mathbb{Z}^n$.

2.1 Key generation

To generate a public/secret key pair, we need two key parameters (n, t), where n is the lattice dimension of 2-power and t is the bit length of coefficients in the so-called *generating polynomial* $v(x)$. The following construction is based on the key generation described in [9, Part I, Section 3]:

Step 1. We first choose an n-dimensional vector $\vec{v} = (v_0, v_1, \dots, v_{n-1}) \in \mathbb{Z}^n$, where v_i is randomly chosen under the condition

(♠) $|v_i| \le 2^t$ for $0 \le i \le n-1$.

Set $v(x) = \sum_{i=0}^{n-1} v_i x^i \in R$ as the generating polynomial. Consider the rotation matrix

$$V = \mathrm{rot}(\vec{v}) = \begin{pmatrix} v_0 & v_1 & v_2 & \cdots & v_{n-1} \\ -v_{n-1} & v_0 & v_1 & \cdots & v_{n-2} \\ -v_{n-2} & -v_{n-1} & v_0 & \cdots & v_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -v_1 & -v_2 & -v_3 & \cdots & v_0 \end{pmatrix}.$$

Since the i-th row $\vec{v}_i \in \mathbb{Z}^n$ of V corresponds to the polynomial $v(x) \times x^i \in R$ under the isomorphism (2.1) and hence the $\vec{v}_i$'s are linearly independent, the subgroup

$$L = \left\{ \sum_{i=1}^{n} m_i \vec{v}_i \ (m_i \in \mathbb{Z}) \right\} \subset \mathbb{Z}^n$$

gives a (full-rank) lattice of dimension n. Then the matrix V becomes a basis of the lattice L. Furthermore, under the isomorphism (2.1), we have an isomorphism

$$R \supset (v(x)) \simeq L \subset \mathbb{Z}^n$$

as $\mathbb{Z}$-modules, where $(v(x))$ denotes the principal ideal of R generated by $v(x)$. Therefore the lattice L is called an *ideal lattice*.

Step 2. By applying the extended Euclidean-GCD algorithm for polynomials, we obtain the scaled inverse $w(x)$ of $v(x)$ modulo $f_n(x)$ satisfying

$$w(x) \times v(x) \equiv d \pmod{f_n(x)}.$$

Note that d is the resultant of $v(x)$ and $f_n(x)$, which is also equal to the determinant $\det(L) = |\det(V)|$ of the lattice L. If d is even, go back to Step 1 and generate another $\vec{v}$ (we can decrypt a ciphertext without the secret key when d is even). Let $\vec{w} = (w_0, w_1, \ldots, w_{n-1}) \in \mathbb{Z}^n$ denote the vector corresponding to the polynomial $w(x) \in R$. Then the matrix $W = \mathrm{rot}(\vec{w})$ satisfies $W \times V = V \times W = d \cdot E_n$, where E_n is the identity matrix of degree n.

Step 3. We say that $v(x)$ is *good* if the Hermite normal form basis $B = \mathrm{HNF}(L)$ of the lattice L has the form

$$B = \begin{pmatrix} d & 0 & 0 & \cdots & 0 \\ -r & 1 & 0 & \cdots & 0 \\ * & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & 0 & 0 & \cdots & 1 \end{pmatrix}. \tag{2.2}$$

In this step, we check the goodness of $v(x)$. In Gentry–Halevi's construction, they only test if $r = w_1/w_0 \pmod{d}$ satisfies $r^n \equiv -1 \pmod{d}$ (see [9, Lemma 1]); otherwise, go back to Step 1 and generate another $\vec{v} \in \mathbb{Z}^n$.

Step 4. Due to the special form (2.2), we only need to set $\mathsf{sk} = w_i$ as the secret key and $\mathsf{pk} = (d, r)$ as the public key, where w_i is a single coefficient of $\vec{w}$ such that w_i is odd (since d is odd, there always exists an odd coefficient w_i).

2.2 Encryption

The plaintext space is the set $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$. To encrypt a plaintext $b \in \{0, 1\}$ with $\mathsf{pk} = (d, r)$, we first choose a random "noise vector" $\vec{u} = (u_0, u_1, \ldots, u_{n-1})$ with $u_i \in \{0, \pm 1\}$ chosen as 0 with some probability q and as ± 1 with probability $(1-q)/2$ each. Then the "fresh" ciphertext of b is generated by

$$c = \mathsf{Enc}(b, \mathsf{pk}) = \left[b + 2 \cdot \sum_{i=0}^{n-1} u_i r^i \right]_d \in [-d/2, d/2).$$

Set $\vec{a} = 2\vec{u} + b\vec{e}_1 = (2u_0 + b, 2u_1, \ldots, 2u_{n-1}) \in \mathbb{Z}^n$ with $\vec{e}_1 = (1, 0, \ldots, 0)$. Let $a(x) \in R$ denote its corresponding polynomial under the isomorphism (2.1). Then we can simply rewrite $\mathsf{Enc}(b, \mathsf{pk}) = [a(r)]_d$.

Definition 2.1 (Masked plaintext). We call the vector $\vec{a} \in \mathbb{Z}^n$ (or its corresponding polynomial $a(x) \in R$) the *masked plaintext* corresponding to a ciphertext c.

2.3 Homomorphic operations

For two fresh ciphertexts $\mathsf{Enc}(b_1, \mathsf{pk})$ and $\mathsf{Enc}(b_2, \mathsf{pk})$, the homomorphic addition and the homomorphic multiplication are respectively defined by

$$\mathsf{Enc}(b_1, \mathsf{pk}) + \mathsf{Enc}(b_2, \mathsf{pk}) = [\mathsf{Enc}(b_1, \mathsf{pk}) + \mathsf{Enc}(b_2, \mathsf{pk})]_d,$$
$$\mathsf{Enc}(b_1, \mathsf{pk}) \times \mathsf{Enc}(b_2, \mathsf{pk}) = [\mathsf{Enc}(b_1, \mathsf{pk}) \cdot \mathsf{Enc}(b_2, \mathsf{pk})]_d.$$

Let $\vec{a}_1, \vec{a}_2 \in R$ denote the masked plaintexts corresponding to two ciphertexts $\mathsf{Enc}(b_1, \mathsf{pk}), \mathsf{Enc}(b_2, \mathsf{pk})$, respectively. As described in [9, Part I], the above homomorphic operations correspond to the ring structure of R, from which the homomorphic property of the scheme follows. However, homomorphic operations make the size of the noise vector in the corresponding masked plaintext larger. Therefore it is possible to add and multiply ciphertexts until the size of the noise vector grows beyond the decryption range. Hence, the scheme constructed in this section gives just an SHE scheme (not an FHE scheme).

2.4 Decryption

For a fresh or homomorphically operated ciphertext $c \in [-d/2, d/2)$, we can recover the corresponding plaintext with the secret key $\mathsf{sk} = w_i$ by computing

$$[c \cdot \mathsf{sk}]_d \pmod 2. \tag{2.3}$$

Let $\vec{a} \in \mathbb{Z}^n$ denote the masked plaintext corresponding to c. Note that we can recover the correct plaintext if $\|\vec{a} \times W\|_\infty < d/2$ (see [9, Part I, Section 6]).

Remark 2.2. We give a brief review on the construction of the SHE scheme from the mathematical point of view. Since B has the special form (2.2), the principal ideal $(v(x))$ is equal to the ideal $(d, x - r)$ generated by two elements d and $x - r$ (see also [17]). In this case, the element r is a root of $f_n(x) \equiv 0 \pmod d$ and we have an isomorphism

$$R/(v(x)) \simeq \mathbb{Z}/d\mathbb{Z}$$

induced by a map $R \ni a(x) \mapsto a(r) \bmod d \in \mathbb{Z}/d\mathbb{Z}$ (note that the value $v(r)$ is divisible by d). To encrypt a plaintext b with $\mathsf{pk} = (d, r)$, we first generate the masked plaintext $\vec{a} = 2\vec{u} + b\vec{e}_1 \in R = \mathbb{Z}^n$ with a noise vector $\vec{u}$, and then compute a ciphertext $\mathsf{Enc}(b, \mathsf{pk}) = [a(r)]_d$ by using a composition of maps

$$\begin{array}{ccccccc}
\mathbb{Z}/2\mathbb{Z} & \overset{+\text{noise}}{\rightsquigarrow} & R \simeq \mathbb{Z}^n & \to & R/(v(x)) \simeq \mathbb{Z}/d\mathbb{Z} & \simeq & \mathbb{Z}^n/L, \\
b & \mapsto & \vec{a} = 2\vec{u} + b\vec{e}_1 & \mapsto & a(r) \pmod d & \mapsto & (\mathsf{Enc}(b, \mathsf{pk}), 0, \ldots, 0).
\end{array}$$

In principle, the ciphertext space is the set $\mathbb{Z}^n/L$, but a ciphertext is represented as the first entry of a vector in $\mathbb{Z}^n/L$ due to the isomorphism $\mathbb{Z}/d\mathbb{Z} \simeq \mathbb{Z}^n/L$.

3 Theoretical evaluation of the decryption range

As described in Section 2.4, the decryption of a ciphertext c succeeds with sk if $\|\vec{a} \times W\|_\infty < d/2$, where $\vec{a} = (a_0, \ldots, a_{n-1}) \in R = \mathbb{Z}^n$ is the masked plaintext corresponding to c. Since the i-th entry of $\vec{a} \times W$ is represented by

$$\sum_{k=0}^{i-1} a_k w_{i-k-1} - \sum_{k=i}^{n-1} a_k w_{n-k+i-1}, \tag{3.1}$$

the gap $d/|w_i|$ is closely related with the decryption range, and we study the gap under the condition

($\diamondsuit$) $T = |v_{n-1}| = 2^t(1 + \varepsilon_{n-1})$ and $v_i = T\varepsilon_i$ for $0 \le i \le n-2$ with $0 < \varepsilon_{n-1} \ll 1$ and $|\varepsilon_i| \ll 1$ for $0 \le i \le n-2$

for giving a theoretical evaluation. Set $\varepsilon = \max_{0 \le i \le n-1} |\varepsilon_i|$. We give our main theoretical result as follows:

Theorem 3.1. *Assume $\varepsilon < \frac{1}{4c_0 n}$ for a positive number $c_0 \geq 1$. Then $d \approx 2^{nt}$ and there exist two positive numbers c_1 and c_2 determined by c_0 such that*

$$\frac{|w_i|}{d} < \frac{1}{c_1 n 2^t} \text{ for } i \neq 1 \quad \text{and} \quad \frac{|w_1|}{d} < \frac{1}{c_2 2^t}.$$

Moreover, two elements c_1, c_2 can be taken as

$$c_1 = \Big(1 - \frac{1}{2c_0}\Big)\Big(4c_0 - \frac{1}{4c_0 - 1}\Big) \quad \text{and} \quad c_2 = 1 - \frac{2}{4c_0(4c_0 - 1) + 1}.$$

In particular, we have $c_1 = \frac{11}{6}$ and $c_2 = \frac{11}{13}$ when we set $c_0 = 1$.

Before we prove the theorem in Section 4, we give an interpretation of the result to a theoretical upper bound of the decryption range of the SHE scheme.

Corollary 3.2 (Theoretical evaluation). *Assume the condition*

(♣) *$T = |v_{n-1}| = 2^t(1 + \varepsilon_{n-1})$ and $v_i = T\varepsilon_i$ for $0 \leq i \leq n-2$ with $0 < \varepsilon_{n-1} < \frac{1}{4n}$ and $|\varepsilon_i| < \frac{1}{4n}$ for $0 \leq i \leq n-2$.*

Then the decryption of a ciphertext c succeeds if the corresponding masked plaintext $\vec{a}$ satisfies either

$$\|\vec{a}\|_1 < \frac{11 \cdot 2^{t-1}}{13} \quad \text{or} \quad \|\vec{a}\|_\infty < \frac{11n \cdot 2^{t-1}}{19n - 6}. \tag{3.2}$$

Proof. By the expression (3.1), every entry of $\vec{a} \times W$ is less than both $\|\vec{a}\|_1 \cdot \|\vec{w}\|_\infty$ and $\|\vec{a}\|_\infty \cdot \|\vec{w}\|_1$. Furthermore, it follows from Theorem 3.1 that

$$\|\vec{w}\|_1 < \frac{13}{11} \cdot \frac{d}{2^t} + (n-1) \cdot \frac{6}{11} \cdot \frac{d}{n2^t} = \frac{19n - 6}{11n} \cdot \frac{d}{2^t} \quad \text{and} \quad \|\vec{w}\|_\infty < \frac{13}{11} \cdot \frac{d}{2^t}$$

(note that we use the evaluation of the case $c_0 = 1$ in Theorem 3.1). Therefore, if $\vec{a}$ satisfies the condition (3.2), then we have $\|\vec{a} \times W\|_\infty < d/2$. This completes the proof. □

Let c be a ciphertext, and $\vec{a}$ denote its corresponding masked plaintext. Given key parameters (n, t), Gentry and Halevi take $v(x)$ under the condition (♠) as described in Section 2.1, and experimentally estimate in [9, Section 7] that the decryption radius is roughly equal to 2^t and it succeeds to decrypt the ciphertext c if $\|\vec{a}\| \leq 2^t$. Then they always use the Euclidean norm evaluation in the noise management of ciphertexts. In contrast, we slightly modify the key generation by taking $v(x)$ under the condition (♣), and then we can use the theoretical evaluation (3.2) in Corollary 3.2. Note that the condition (♣) can be considered as a restricted version of Gentry–Halevi's condition since $|v_{n-1}| = T \approx 2^t$ and $|v_i| < T/4n \approx 2^t/4n$ for $0 \leq i \leq n-2$ when $\varepsilon_{n-1} > 0$ is sufficiently small. Furthermore, even when we use this restricted condition, the scheme is estimated to have enough security against exhaustive search and birthday attacks on $v(x)$ for large t (for example, $t \geq 100$). The main advantage of the theoretical evaluation (3.2) is to enable us to use the ∞-norm evaluation in the noise management. The reason is that the ∞-norm evaluation is independent of the probability q on noise density defined in Section 2.2, and it helps us to choose key parameters (n, t) with a theoretical guarantee for obtaining an FHE scheme (see Section 5 for details).

Remark 3.3. In [19], we apply the SHE scheme described in Section 2 to efficiently compute the Hamming distance on encrypted data for privacy-preserving biometrics. We use the result of Corollary 3.2 in order to avoid decryption errors (the result of [19, Proposition 1] is the same as Corollary 3.2).

4 Proof of Theorem 3.1

The result of Theorem 3.1 follows from Propositions 4.4 and 4.6–4.9, which we will show below. The way of our proof is to explicitly evaluate values d and $|w_i|$, separately. In this section, we set $v(x) = \sum_{i=0}^{n-1} v_i x^i$ with the condition $(\diamondsuit)$.

4.1 Estimation on *d*

We give an estimation on the determinant d. Let $\mathrm{Syl}(f, g)$ denote the Sylvester matrix of two polynomials $f(x)$ and $g(x)$. Then we have $d = \mathrm{res}(f_n(x), v(x)) = \det(\mathrm{Syl}(f_n, v))$. By its definition, the Sylvester matrix is given by

$$\mathrm{Syl}(f_n, v) = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & 1 & & & \\ & 1 & 0 & \cdots & 0 & 0 & 1 & & \\ & & \ddots & \ddots & & \ddots & \ddots & \ddots & \\ & & & 1 & 0 & \cdots & 0 & 0 & 1 \\ v_{n-1} & v_{n-2} & \cdots & v_1 & v_0 & & & & \\ & v_{n-1} & v_{n-2} & \cdots & v_1 & v_0 & & & \\ & & \ddots & \ddots & & \ddots & \ddots & & \\ & & & & v_{n-1} & v_{n-2} & \cdots & v_1 & v_0 \end{pmatrix},$$

in which the element v_{n-1} appears from the n-th row to the $(2n-1)$-th row. From the n-th row, we eliminate the first $n-1$ entries by subtracting the first row multiplied by v_{n-1} and subtracting the second row multiplied by v_{n-2} and so on. Then the n-th row becomes

$$(0, \ldots, 0, v_0, -v_{n-1}, -v_{n-2}, \ldots, -v_1).$$

In the same manner, for each $(n+k)$-th row, we can eliminate its first $n-1$ entries: Let $s_{n+k,i}$ denote the $(n+k, i)$-entry of $\mathrm{Syl}(f_n, v)$. Then from the $(n+k)$-th row, we subtract each i-th row multiplied by $s_{n+k,i}$ for $1 \leq i \leq n-1$. After these operations, the $(n+k)$-th row becomes

$$(0, \ldots, 0, v_k, \ldots, v_0, -v_{n-1}, \ldots, -v_{k+1}).$$

Finally, the matrix $\mathrm{Syl}(f_n, v)$ is transformed to a block upper triangular matrix

$$\begin{pmatrix} E_{n-1} & * \\ O & D \end{pmatrix}$$

without changing the determinant, where E_{n-1} denotes the identity matrix of degree $n-1$, and D is the $n \times n$-matrix given by

$$D = \begin{pmatrix} v_0 & -v_{n-1} & -v_{n-2} & -v_{n-3} & \cdots & -v_4 & -v_3 & -v_2 & -v_1 \\ v_1 & v_0 & -v_{n-1} & -v_{n-2} & \cdots & -v_5 & -v_4 & -v_3 & -v_2 \\ v_2 & v_1 & v_0 & -v_{n-1} & \cdots & -v_6 & -v_5 & -v_4 & -v_3 \\ \vdots & & \ddots & \ddots & & & & & \vdots \\ \vdots & & & \ddots & \ddots & & & & \vdots \\ v_{n-3} & v_{n-4} & v_{n-5} & v_{n-6} & \cdots & v_1 & v_0 & -v_{n-1} & -v_{n-2} \\ v_{n-2} & v_{n-3} & v_{n-4} & v_{n-5} & \cdots & v_2 & v_1 & v_0 & -v_{n-1} \\ v_{n-1} & v_{n-2} & v_{n-3} & v_{n-4} & \cdots & v_3 & v_2 & v_1 & v_0 \end{pmatrix}.$$

Then we have $d = \det(\mathrm{Syl}(f_n, v)) = \det(E_{n-1}) \times \det(D) = \det(D)$.

Next we replace v_{n-1} with 1 and each v_i with ε_i for $0 \leq i \leq n-2$ in the above matrix D to obtain the matrix

$$M_0 = \begin{pmatrix} \varepsilon_0 & -1 & -\varepsilon_{n-2} & \cdots & -\varepsilon_3 & -\varepsilon_2 & -\varepsilon_1 \\ \varepsilon_1 & \varepsilon_0 & -1 & \cdots & -\varepsilon_4 & -\varepsilon_3 & -\varepsilon_2 \\ \varepsilon_2 & \varepsilon_1 & \varepsilon_0 & \cdots & -\varepsilon_5 & -\varepsilon_4 & -\varepsilon_3 \\ \vdots & & \ddots & & & & \vdots \\ \vdots & & & \ddots & & & \vdots \\ \varepsilon_{n-3} & \varepsilon_{n-4} & \varepsilon_{n-5} & \cdots & \varepsilon_0 & -1 & -\varepsilon_{n-2} \\ \varepsilon_{n-2} & \varepsilon_{n-3} & \varepsilon_{n-4} & \cdots & \varepsilon_1 & \varepsilon_0 & -1 \\ 1 & \varepsilon_{n-2} & \varepsilon_{n-3} & \cdots & \varepsilon_2 & \varepsilon_1 & \varepsilon_0 \end{pmatrix}.$$

Then we have $d = T^n \det(M_0)$. Finally, we transform M_0 to the matrix

$$M = \begin{pmatrix} 1 & \varepsilon_{n-2} & \varepsilon_{n-3} & \cdots & \varepsilon_2 & \varepsilon_1 & \varepsilon_0 \\ -\varepsilon_0 & 1 & \varepsilon_{n-2} & \cdots & \varepsilon_3 & \varepsilon_2 & \varepsilon_1 \\ -\varepsilon_1 & -\varepsilon_0 & 1 & \cdots & \varepsilon_4 & \varepsilon_3 & \varepsilon_2 \\ -\varepsilon_2 & -\varepsilon_1 & -\varepsilon_0 & \cdots & \varepsilon_5 & \varepsilon_4 & \varepsilon_3 \\ \vdots & & \ddots & & & & \vdots \\ \vdots & & & \ddots & & & \vdots \\ -\varepsilon_{n-3} & -\varepsilon_{n-4} & -\varepsilon_{n-5} & \cdots & -\varepsilon_0 & 1 & \varepsilon_{n-2} \\ -\varepsilon_{n-2} & -\varepsilon_{n-3} & -\varepsilon_{n-4} & \cdots & -\varepsilon_1 & -\varepsilon_0 & 1 \end{pmatrix}$$

by multiplying the last $n-1$ rows by -1 and moving the last row to the first one and shifting others. We note that this transformation does not change the determinant and hence we have $\det(M) = \det(M_0)$.

Let $M_{i,j}$ denote the (i, j)-th entry of the matrix M. Then we have

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) M_{1,\sigma(1)} \cdots M_{n,\sigma(n)},$$

where $\mathfrak{S}_n$ denotes the symmetric group of degree n. By counting the number of ones appearing among $M_{1,\sigma(1)}, \ldots, M_{n,\sigma(n)}$, we estimate the value $\det(M)$.

Definition 4.1. For each $1 \le k \le n$, we define s_k as the number of permutations $\sigma \in \mathfrak{S}_n$ such that 1 appears exactly $n-k$ times among $M_{1,\sigma(1)}, \ldots, M_{n,\sigma(n)}$. In this case, the number of ε_j's appearing among $M_{1,\sigma(1)}, \ldots, M_{n,\sigma(n)}$ is equal to k.

The product of all diagonal entries corresponds to the identity permutation, and its value is 1. For the other permutation $\sigma \neq 1$, the number of ones appearing among $M_{1,\sigma(1)}, \ldots, M_{n,\sigma(n)}$ ranges from 0 to $n-2$. Here we call the term corresponding to the identity permutation the *principal term* and the other terms *subsidiary term*. Then the determinant $\det(M)$ can be obtained by estimating the sum of all subsidiary terms. More precisely, it can be shown that the minimal value of $\det(M)$ is not smaller than the value where we set each subsidiary term to have its minimal value $-\varepsilon^k$, and the maximal one is not greater than the value where we set each subsidiary term to have its maximal value ε^k. Here we use $|\varepsilon_i| \le \varepsilon$ for possible minimal and maximal values. Then we have the following two lemmas:

Lemma 4.2. *We have*

$$1 - \sum_{k=2}^{n} s_k \varepsilon^k \le \det(M) \le 1 + \sum_{k=2}^{n} s_k \varepsilon^k.$$

Lemma 4.3. *For $2 \leq k \leq n$, we have*

$$s_k \leq k! \times \binom{n}{k} = n(n-1)\cdots(n-k+1).$$

Proof. We count the number of permutations $\sigma \in \mathfrak{S}_n$ such that 1 appears $n-k$ times among $M_{1,\sigma(1)}, \ldots, M_{n,\sigma(n)}$. For such a permutation σ, the number of indices i with $\sigma(i) = i$ is equal to $n-k$, and it can be determined by choosing $n-k$ indices i with $\sigma(i) = i$ and the action on k other indices. Thus, since the number of choices of $n-k$ indices is equal to $\binom{n}{n-k} = \binom{n}{k}$ and the possible actions on k other indices is bounded by $k!$, the number of such permutations is bounded by the product $k! \times \binom{n}{k}$. This completes the proof of Lemma 4.3. □

Now, we assume $\varepsilon < \frac{1}{4c_0 n}$ for a positive number $c_0 \geq 1$. Then, for each $2 \leq k \leq n$, we have

$$s_k \varepsilon^k < \frac{n(n-1)(n-2)\cdots(n-k+1)}{(4c_0)^k n^k} < \frac{1}{(4c_0)^k}.$$

Since

$$\begin{aligned}\sum_{k=2}^{n} s_k \varepsilon^k &< \sum_{k=2}^{n} \frac{1}{(4c_0)^k} = \frac{1}{16c_0^2} \times \sum_{k=0}^{n-2} \frac{1}{(4c_0)^k} \\ &< \frac{1}{16c_0^2} \times \frac{1}{1-\frac{1}{4c_0}} = \frac{1}{4c_0(4c_0-1)},\end{aligned}$$

we have the following result by Lemma 4.2:

Proposition 4.4. *Assume $\varepsilon < \frac{1}{4c_0 n}$ for a positive number $c_0 \geq 1$. Then the determinant* $\det(M)$ *is estimated as*

$$1 - \frac{1}{4c_0(4c_0-1)} < \det(M) < 1 + \frac{1}{4c_0(4c_0-1)}.$$

Since $d = \det(D) = T^n \det(M)$, the determinant d is estimated as

$$\frac{11}{12}T^n \leq \left(1 - \frac{1}{4c_0(4c_0-1)}\right)T^n < d < \left(1 + \frac{1}{4c_0(4c_0-1)}\right)T^n \leq \frac{13}{12}T^n.$$

As we take $T = 2^t(1+\varepsilon_{n-1}) \approx 2^t$, we have $d \approx 2^{nt}$.

4.2 Estimation on $|w_k|$

We next give an estimation on the value $|w_k|$. Consider the matrix

$$\overline{\mathrm{Syl}}(f_n, v) = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & 1 & & & x^{n-2} f_n(x) \\ & 1 & 0 & \cdots & 0 & 0 & 1 & & x^{n-3} f_n(x) \\ & & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ & & & 1 & 0 & \cdots & 0 & 0 & f_n(x) \\ v_{n-1} & v_{n-2} & \cdots & v_1 & v_0 & & & & x^{n-1} v(x) \\ & v_{n-1} & v_{n-2} & \cdots & v_1 & v_0 & & & x^{n-2} v(x) \\ & & \ddots & \ddots & & \ddots & \ddots & & \vdots \\ & & & & v_{n-1} & v_{n-2} & \cdots & v_1 & v(x) \end{pmatrix}.$$

From the $(2n-1)$-th column, we consider the transformation to subtract the k-th column multiplied by x^{2n-1-k} for $1 \le k \le 2n-2$. Since this transforms $\overline{\mathrm{Syl}}(f_n, v)$ to the matrix $\mathrm{Syl}(f_n, v)$ without changing the determinant, we have

$$\det(\overline{\mathrm{Syl}}(f_n, v)) = \det(\mathrm{Syl}(f_n, v)) = d.$$

For $1 \le k \le 2n-1$, let S_k denote the $(2n-2) \times (2n-2)$-matrix deleting both the $(2n-1)$-th column and the k-th row from $\overline{\mathrm{Syl}}(f_n, v)$. By considering the cofactor expansion of $\overline{\mathrm{Syl}}(f_n, v)$ along the $(2n-1)$-th column, we have the expansion

$$\begin{aligned} d = & \sum_{k=1}^{n-1} (-1)^{2n-1+k} \det(S_k) x^{n-1-k} f_n(x) \\ & + \sum_{k=n}^{2n-1} (-1)^{2n-1+k} \det(S_k) x^{2n-1-k} v(x). \end{aligned}$$

Set

$$\overline{w}(x) = \sum_{k=n}^{2n-1} (-1)^{2n-1+k} \det(S_k) x^{2n-1-k},$$

$$\overline{g}(x) = \sum_{k=1}^{n-1} (-1)^{2n-1+k} \det(S_k) x^{n-1-k}.$$

Then we have $v(x)\overline{w}(x) + f_n(x)\overline{g}(x) = d$ by the above expansion of d. Since $\deg \overline{w}(x) \le n-1$ and $\deg \overline{g}(x) \le n-2$, it follows from the uniqueness of the extended Euclidean-GCD algorithm that we have $\overline{w}(x) = w(x)$ and hence $|w_k| = |\det(S_{2n-1-k})|$ for $0 \le k \le n-1$. In the following, we give an estimation on $|w_k| = |\det(S_{2n-1-k})|$ for each k.

4.2.1 Estimation on $|w_{n-1}|$

We have $|w_{n-1}| = |\det(S_n)|$, where S_n is given by

$$S_n = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & 1 & & \\ & 1 & 0 & \cdots & 0 & 0 & 1 & \\ & & \ddots & \ddots & & \ddots & \ddots & \\ & & & 1 & 0 & \cdots & 0 & 0 \\ 0 & v_{n-1} & v_{n-2} & \cdots & v_1 & v_0 & & \\ & & \ddots & \ddots & & \ddots & \ddots & \\ & & & & v_{n-1} & v_{n-2} & \cdots & v_1 \end{pmatrix}.$$

In much the same way as in Section 4.1, the matrix S_n is transformed to a block upper triangular matrix

$$\begin{pmatrix} E_{n-1} & * \\ O & W_{n-1} \end{pmatrix},$$

where

$$W_{n-1} = \begin{pmatrix} v_1 & v_0 & -v_{n-1} & \cdots & -v_6 & -v_5 & -v_4 & -v_3 \\ v_2 & v_1 & v_0 & \cdots & -v_7 & -v_6 & -v_5 & -v_4 \\ v_3 & v_2 & v_1 & \cdots & -v_8 & -v_7 & -v_6 & -v_5 \\ \vdots & & \ddots & \ddots & & & & \vdots \\ \vdots & & & \ddots & \ddots & & & \vdots \\ v_{n-3} & v_{n-4} & v_{n-5} & \cdots & v_2 & v_1 & v_0 & -v_{n-1} \\ v_{n-2} & v_{n-3} & v_{n-4} & \cdots & v_3 & v_2 & v_1 & v_0 \\ v_{n-1} & v_{n-2} & v_{n-3} & \cdots & v_4 & v_3 & v_2 & v_1 \end{pmatrix}.$$

We replace v_{n-1} with 1 and each v_i with ε_i for $0 \leq i \leq n-2$, and multiple the first $n-3$ rows by -1 to obtain the matrix

$$R = \begin{pmatrix} -\varepsilon_1 & -\varepsilon_0 & 1 & \varepsilon_{n-2} & \cdots & \varepsilon_5 & \varepsilon_4 & \varepsilon_3 \\ -\varepsilon_2 & -\varepsilon_1 & -\varepsilon_0 & 1 & \cdots & \varepsilon_6 & \varepsilon_5 & \varepsilon_4 \\ -\varepsilon_3 & -\varepsilon_2 & -\varepsilon_1 & -\varepsilon_0 & \cdots & \varepsilon_7 & \varepsilon_6 & \varepsilon_5 \\ \vdots & & \ddots & \ddots & & & & \vdots \\ \vdots & & & \ddots & \ddots & & & \vdots \\ -\varepsilon_{n-3} & -\varepsilon_{n-4} & -\varepsilon_{n-5} & -\varepsilon_{n-6} & \cdots & -\varepsilon_1 & -\varepsilon_0 & 1 \\ \varepsilon_{n-2} & \varepsilon_{n-3} & \varepsilon_{n-4} & \varepsilon_{n-5} & \cdots & \varepsilon_2 & \varepsilon_1 & \varepsilon_0 \\ 1 & \varepsilon_{n-2} & \varepsilon_{n-3} & \varepsilon_{n-4} & \cdots & \varepsilon_3 & \varepsilon_2 & \varepsilon_1 \end{pmatrix}.$$

Then we have $|w_{n-1}| = |\det(W_{n-1})| = T^{n-1}|\det(R)|$. Let $R_{i,j}$ be the (i,j)-th entry of R. Then we have

$$\det(R) = \sum_{\sigma \in \mathfrak{S}_{n-1}} \mathrm{sgn}(\sigma) R_{1,\sigma(1)} \cdots R_{n-1,\sigma(n-1)}.$$

We give a definition similar to Definition 4.1.

Definition 4.5. For each $2 \leq k \leq n-1$, we define t_k as the number of permutations $\sigma \in \mathfrak{S}_{n-1}$ such that 1 appears exactly $n-k-1$ times among the elements $R_{1,\sigma(1)}, \ldots, R_{n-1,\sigma(n-1)}$. In this case, the number of ε_j's appearing among $R_{1,\sigma(1)}, \ldots, R_{n-1,\sigma(n-1)}$ is equal to k.

Then we have

$$|\det(R)| \leq \varepsilon + \sum_{k=2}^{n-1} t_k \varepsilon^k$$

by a similar argument as in Section 4.1, and

$$t_k \leq k! \times \binom{n-2}{k-1} = k \times (n-2)(n-3)\cdots(n-k)$$

for $2 \leq k \leq n-1$ by the proof of Lemma 4.3. Assume the same condition as in Proposition 4.4. By using the fact $2^{k-1} \geq k$, we have

$$\begin{aligned} t_k \varepsilon^k &= \varepsilon \times (t_k \varepsilon^{k-1}) \leq \varepsilon \times \frac{k(n-2)(n-3)\cdots(n-k)}{n^{k-1} \times (4c_0)^{k-1}} \\ &= \varepsilon \times \frac{(n-2)(n-3)\cdots(n-k)}{n^{k-1}} \times \frac{k}{2^{k-1}} \times \frac{1}{(2c_0)^{k-1}} \\ &< \varepsilon \times \frac{1}{(2c_0)^{k-1}}. \end{aligned}$$

Hence,

$$\begin{aligned} \sum_{k=2}^{n-1} t_k \varepsilon^k &< \varepsilon \times \sum_{k=2}^{n-1} \frac{1}{(2c_0)^{k-1}} = \varepsilon \times \frac{1}{2c_0} \times \sum_{k=0}^{n-3} \frac{1}{(2c_0)^k} \\ &< \varepsilon \times \frac{1}{2c_0} \times \frac{1}{1 - \frac{1}{2c_0}} = \varepsilon \times \frac{1}{2c_0 - 1}. \end{aligned}$$

By a similar argument as in Section 4.1, we have the following estimation on the gap $d/|w_{n-1}|$:

Proposition 4.6. *We have*

$$|\det(R)| < \varepsilon \times \left(1 + \frac{1}{2c_0 - 1}\right) = \varepsilon \times \frac{2c_0}{2c_0 - 1}.$$

Since $|w_{n-1}| = T^{n-1}|\det(R)|$, *we have* $|w_{n-1}| < \varepsilon \times \frac{2c_0}{2c_0-1} \times T^{n-1}$. *Furthermore, under the assumption of Proposition* 4.4, *we have*

$$\frac{|w_{n-1}|}{d} < \frac{\varepsilon \times \frac{2c_0}{2c_0-1} \times T^{n-1}}{\frac{(4c_0(4c_0-1)-1)\times T^n}{4c_0(4c_0-1)}} = \frac{1}{c_1 n T},$$

where $c_1 = (1 - \frac{1}{2c_0})(4c_0 - \frac{1}{4c_0-1})$. *As* $T = 2^t(1 + \varepsilon_{n-1}) \geq 2^t$, *we have* $\frac{|w_{n-1}|}{d} < \frac{1}{c_1 n 2^t}$.

4.2.2 Estimation on $|w_k|$ with $2 \leq k \leq n-2$

For $2 \leq k \leq n-2$, we have $|w_{n-k}| = |\det(S_{n+k-1})|$. By its definition, the matrix S_{n+k-1} is given by

$$S_{n+k-1} = \left(\begin{array}{ccccccccccc}
1 & 0 & \cdots & \cdots & 0 & 1 & & & & & \\
 & 1 & 0 & \cdots & \cdots & 0 & 1 & & & & \\
 & & \ddots & \ddots & & & & \ddots & \ddots & & \\
 & & & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
v_{n-1} & v_{n-2} & \cdots & \cdots & v_0 & & & & & & \\
 & \ddots & & & & \ddots & & & & & \\
 & & v_{n-1} & v_{n-2} & v_{n-3} & \cdots & v_0 & & & & \\
 & & & & v_{n-1} & v_{n-2} & \cdots & v_1 & v_0 & & \\
 & & & & & \ddots & \ddots & & \ddots & \ddots & \\
 & & & & & & v_{n-1} & v_{n-2} & \cdots & v_1 & v_0 \\
 & & & & & & & v_{n-1} & v_{n-2} & \cdots & v_1
\end{array}\right).$$

By a similar transformation as in Section 4.1, the $(n+i)$-th row becomes

$$\begin{array}{ll}
(0, \ldots, 0, v_i, \ldots, v_0, -v_{n-1}, \ldots, -v_{i+2}) & \text{for } 0 \leq i \leq k-2, \\
(0, \ldots, 0, v_{i+1}, \ldots, v_0, -v_{n-1}, \ldots, -v_{i+3}) & \text{for } k-1 \leq i < n-3, \\
(0, \ldots, 0, v_{n-2}, \ldots, v_0) & \text{for } i = n-3, \\
(0, \ldots, 0, v_{n-1}, \ldots, v_1) & \text{for } i = n-2.
\end{array}$$

Therefore the matrix S_{n+k-1} is transformed to a block upper triangular matrix

$$\begin{pmatrix} E_{n-1} & * \\ O & W_{n-k} \end{pmatrix},$$

where W_{n-k} is the matrix given by

$$\begin{pmatrix}
v_0 & -v_{n-1} & -v_{n-2} & \cdots & \cdots & \cdots & -v_4 & -v_3 & -v_2 \\
v_1 & v_0 & -v_{n-1} & -v_{n-2} & \cdots & & -v_5 & -v_4 & -v_3 \\
\vdots & & \ddots & \ddots & \ddots & & & & \vdots \\
v_{k-2} & v_{k-3} & \cdots & v_0 & -v_{n-1} & -v_{n-2} & \cdots & -v_{k+1} & -v_k \\
v_k & v_{k-1} & \cdots & v_2 & v_1 & v_0 & -v_{n-1} & \cdots & -v_{k+2} \\
v_{k+1} & v_k & \cdots & v_3 & v_2 & v_1 & v_0 & \cdots & -v_{k+3} \\
\vdots & & & & \ddots & \ddots & \ddots & \ddots & \vdots \\
v_{n-3} & v_{n-4} & \cdots & \cdots & \cdots & v_2 & v_1 & v_0 & -v_{n-1} \\
v_{n-2} & v_{n-3} & \cdots & \cdots & \cdots & v_3 & v_2 & v_1 & v_0 \\
v_{n-1} & v_{n-2} & \cdots & \cdots & \cdots & v_4 & v_3 & v_2 & v_1
\end{pmatrix}.$$

We replace v_{n-1} with 1 and each v_i with ε_i for $0 \leq i \leq n-2$, and multiple the first $n-3$ rows by -1 to obtain the matrix

$$R_k = \begin{pmatrix}
-\varepsilon_0 & 1 & \varepsilon_{n-2} & \cdots & \cdots & \cdots & \varepsilon_4 & \varepsilon_3 & \varepsilon_2 \\
-\varepsilon_1 & -\varepsilon_0 & 1 & \varepsilon_{n-2} & \cdots & \cdots & \varepsilon_5 & \varepsilon_4 & \varepsilon_3 \\
\vdots & & \ddots & \ddots & & & & \vdots & \\
-\varepsilon_{k-2} & -\varepsilon_{k-3} & \cdots & -\varepsilon_0 & 1 & \varepsilon_{n-2} & \cdots & \varepsilon_{k+1} & \varepsilon_k \\
-\varepsilon_k & -\varepsilon_{k-1} & \cdots & -\varepsilon_2 & -\varepsilon_1 & -\varepsilon_0 & 1 & \cdots & \varepsilon_{k+2} \\
-\varepsilon_{k+1} & -\varepsilon_k & \cdots & -\varepsilon_3 & -\varepsilon_2 & -\varepsilon_1 & -\varepsilon_0 & \cdots & \varepsilon_{k+3} \\
\vdots & & & & \ddots & \ddots & & \vdots & \\
-\varepsilon_{n-3} & -\varepsilon_{n-4} & \cdots & \cdots & \cdots & -\varepsilon_2 & -\varepsilon_1 & -\varepsilon_0 & 1 \\
\varepsilon_{n-2} & \varepsilon_{n-3} & \cdots & \cdots & \cdots & \varepsilon_3 & \varepsilon_2 & \varepsilon_1 & \varepsilon_0 \\
1 & \varepsilon_{n-2} & \cdots & \cdots & \cdots & \varepsilon_4 & \varepsilon_3 & \varepsilon_2 & \varepsilon_1
\end{pmatrix}.$$

Then we have $|w_{n-k}| = |\det(W_{n-k})| = T^{n-1}|\det(R_k)|$. Let $R_{i,j}^{(k)}$ be the (i, j)-th entry of R_k. Then we have

$$\det(R_k) = \sum_{\sigma \in \mathfrak{S}_{n-1}} \operatorname{sgn}(\sigma) R_{1,\sigma(1)}^{(k)} \cdots R_{n-1,\sigma(n-1)}^{(k)}.$$

Now, we get a result similar to Proposition 4.6.

Proposition 4.7. *Under the assumption of Proposition* 4.4, *for* $2 \leq k \leq n-2$, *we have* $|w_{n-k}| < \varepsilon \times \frac{2c_0}{2c_0-1} \times T^{n-1}$ *and* $\frac{|w_{n-k}|}{d} < \frac{1}{c_1 nT} < \frac{1}{c_1 n 2^t}$ *as* $T \geq 2^t$.

4.2.3 Estimation on $|w_k|$ with $k = 0, 1$

We have $|w_0| = |\det(S_{2n-1})|$ and $|w_1| = |\det(S_{2n-2})|$. By its definition, the matrix S_{2n-1} is given by

$$S_{2n-1} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 1 & & \\ & \ddots & \ddots & & & & & \ddots & \\ & & 1 & 0 & \cdots & \cdots & \cdots & \cdots & 1 \\ & & & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ v_{n-1} & v_{n-2} & \cdots & v_1 & v_0 & & & & \\ & v_{n-1} & \cdots & \cdots & v_1 & v_0 & & & \\ & & \ddots & & & \ddots & \ddots & & \\ & & & v_{n-1} & \cdots & \cdots & v_1 & v_0 & \\ & & & & v_{n-1} & \cdots & \cdots & v_1 & v_0 \end{pmatrix}.$$

As in Section 4.1, the matrix S_{2n-1} is transformed to a block upper triangular matrix

$$\begin{pmatrix} E_{n-1} & * \\ O & W_0 \end{pmatrix},$$

where

$$W_0 = \begin{pmatrix} v_0 & -v_{n-1} & -v_{n-2} & \cdots & \cdots & -v_3 & -v_2 \\ v_1 & v_0 & -v_{n-1} & -v_{n-2} & & -v_4 & -v_3 \\ \vdots & & \ddots & \ddots & & & \vdots \\ \vdots & & & \ddots & \ddots & & \vdots \\ \vdots & & & & \ddots & \ddots & \vdots \\ v_{n-3} & v_{n-4} & \cdots & \cdots & v_2 & v_0 & -v_{n-1} \\ v_{n-2} & v_{n-3} & \cdots & \cdots & \cdots & v_1 & v_0 \end{pmatrix}.$$

Since W_0 has a similar form as W_{n-k} for $1 \leq k \leq n-1$, we have a similar estimation to Proposition 4.6.

Proposition 4.8. *Under the assumption of Proposition* 4.4, *we have* $|w_0| < \varepsilon \times \frac{2c_0}{2c_0-1} \times T^{n-1}$ *and* $\frac{|w_0|}{d} < \frac{1}{c_1 nT} < \frac{1}{c_1 n 2^t}$ *as* $T \geq 2^t$.

Finally, we consider $|w_1| = |\det(S_{2n-2})|$. By its definition, the matrix S_{2n-2} is given by

$$S_{2n-2} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & -1 & & \\ & \ddots & \ddots & & & & & \ddots & \\ & & 1 & 0 & \cdots & \cdots & \cdots & \cdots & -1 \\ & & & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ v_{n-1} & v_{n-2} & \cdots & v_1 & v_0 & & & & \\ & v_{n-1} & \cdots & \cdots & v_1 & v_0 & & & \\ & & \ddots & & & \ddots & \ddots & & \\ & & & v_{n-1} & v_{n-2} & \cdots & v_1 & v_0 & \\ & & & & & v_{n-1} & \cdots & v_2 & v_1 \end{pmatrix}.$$

As in Section 4.1, the matrix S_{2n-2} is transformed to a block upper triangular matrix

$$\begin{pmatrix} E_{n-1} & * \\ O & W_1 \end{pmatrix},$$

where

$$W_1 = \begin{pmatrix} v_0 & -v_{n-1} & -v_{n-2} & \cdots & \cdots & -v_3 & -v_2 \\ v_1 & v_0 & -v_{n-1} & -v_{n-2} & & -v_4 & -v_3 \\ \vdots & & \ddots & \ddots & & & \vdots \\ \vdots & & & \ddots & \ddots & & \vdots \\ \vdots & & & & \ddots & \ddots & \vdots \\ v_{n-3} & v_{n-4} & \cdots & \cdots & v_2 & v_0 & -v_{n-1} \\ v_{n-1} & v_{n-2} & \cdots & \cdots & \cdots & v_2 & v_1 \end{pmatrix}.$$

We replace v_{n-1} with 1 and each v_i with ε_i for $0 \le i \le n-2$, and multiple the first $n-2$ rows by -1 to obtain the matrix

$$R_1 = \begin{pmatrix} -\varepsilon_0 & 1 & \varepsilon_{n-2} & \cdots & \cdots & \varepsilon_3 & \varepsilon_2 \\ -\varepsilon_1 & -\varepsilon_0 & 1 & \varepsilon_{n-2} & & \varepsilon_4 & \varepsilon_3 \\ \vdots & & \ddots & \ddots & & & \vdots \\ \vdots & & & \ddots & \ddots & & \vdots \\ \vdots & & & & \ddots & \ddots & \vdots \\ -\varepsilon_{n-3} & -\varepsilon_{n-4} & \cdots & \cdots & -\varepsilon_2 & -\varepsilon_0 & 1 \\ 1 & \varepsilon_{n-2} & \cdots & \cdots & \cdots & \varepsilon_2 & \varepsilon_1 \end{pmatrix}.$$

Then we have $|w_1| = |\det(W_1)| = T^{n-1}|\det(R_1)|$. Since R_1 has a similar form as the matrix M, we can use a similar argument as in Section 4.1.

Proposition 4.9. *Under the assumption of Proposition* 4.4*, we have*

$$|w_1| < \left(1 + \frac{1}{4c_0(4c_0-1)}\right) \times T^{n-1}$$

and

$$\frac{|w_1|}{d} < \frac{(1+\frac{1}{4c_0(4c_0-1)})T^{n-1}}{(1-\frac{1}{4c_0(4c_0-1)})T^{n}} = \frac{1}{c_2T} < \frac{1}{c_2 2^t},$$

where $c_2 = 1 - \frac{2}{4c_0(4c_0-1)+1}$.

5 FHE parameters revisited

In [9], Gentry and Halevi present a concrete construction of the re-encryption method to obtain an FHE scheme transformed from the SHE scheme described in Section 2. Their construction is just an instantiation of Gentry's bootstrapping approach given in [8], namely, we squash the decryption circuit so that it can be evaluated by the SHE scheme. In this section, we briefly review their re-encryption method (see [18, Section 4.1]) and revisit the SHE key parameters (n, t) for the re-encryption method, by using the theoretical evaluation (3.2) of the decryption range in Corollary 3.2.

5.1 Review of re-encryption method

The idea of Gentry–Halevi's re-encryption method is to rewrite the secret key of the SHE scheme as the solution of a sparse-subset-sum problem (SSSP). To construct such a problem, we need two parameters (s, S) in addition to key pairs $(\mathsf{sk}, \mathsf{pk})$ of the SHE scheme ($\mathsf{pk} = (d, r)$ and $\mathsf{sk} = w_i$ as in Section 2). We first choose s elements $x_i \in [0, d)$ and a random integer $Z \in [1, d)$, and for each $1 \le i \le s$, we take the i-th set $\mathcal{B}_i = \{x_i \cdot Z^j \pmod d \mid j = 0, 1, \ldots, S-1\}$ such that the secret key sk can be written as

$$\mathsf{sk} = \sum_{i=1}^{s}\sum_{j=0}^{S-1} b_{i,j} \cdot x_i \cdot Z^j \pmod d,$$

where only one $b_{i,j}$ satisfies $b_{i,j} = 1$ and the other $b_{i,j}$'s are equal to zero for each i. For each i, let e_i denote the unique index j satisfying $b_{i,j} = 1$. Then we have $\mathsf{sk} = \sum_{i=1}^{s} x_i \cdot Z^{e_i} \pmod d$. For the re-encryption, we need additional ciphertexts $c_{i,j} = \mathsf{Enc}(b_{i,j}, \mathsf{pk})$ for each i, j. The public key of the FHE scheme consists of

$$\mathsf{PK}_{\text{FHE}} = \left(d, r, s, S, Z, \left\{x_i, \{c_{i,j}\}_{j=0}^{S-1}\right\}_{i=1}^{s}\right).$$

On the other hand, we take the set $\{e_i\}_{i=1}^{s}$ as the secret key of the FHE scheme.

For a ciphertext c, set $y_{i,j} = c \cdot x_i \cdot Z^j \pmod d$ for each i, j. It follows from [18, Section 4.1] that the decryption function (2.3) can be rewritten as

$$[c \cdot \mathsf{sk}]_d \pmod 2 = \bigoplus_{i=1}^{s} \bigoplus_{j=0}^{S-1} b_{i,j} \cdot y_{i,j} \pmod 2 \oplus \lceil \mathcal{T} \rfloor \pmod 2, \tag{5.1}$$

where $\mathcal{T} = \sum_{i=1}^{s} \sum_{j=0}^{S-1} b_{i,j} \cdot \frac{y_{i,j}}{d}$. The first double big XOR in the expression (5.1) is just a linear function of the $b_{i,j}$'s, while the function $\lceil \mathcal{T} \rfloor$ is a non-linear term. We need to evaluate its rounding function. By a similar argument as in [18, Section 4.1], if we assume that the masked plaintext $\vec{a}$ corresponding to the ciphertext c satisfies the condition

$$\|\vec{a}\|_\infty < U/(s+1), \tag{5.2}$$

then $\mathcal{T}$ is within distance $1/2(s+1)$ of an integer, where U is the ∞-norm theoretical evaluation in Corollary 3.2. For each i, j, let $z_{i,j}$ denote an approximation of $q_{i,j} = y_{i,j}/d$ up to p bits after the binary point, namely, each $z_{i,j}$ satisfies $|z_{i,j} - y_{i,j}/d| < 2^{-(p+1)}$. Since we have

$$\left| \mathcal{T} - \sum_{i=1}^{s} \sum_{j=0}^{S-1} b_{i,j} \cdot z_{i,j} \right| < \sum_{i=1}^{s} 2^{-(p+1)} = s \cdot 2^{-(p+1)},$$

rounding of $\sum_{i=1}^{s} \sum_{j=0}^{S-1} b_{i,j} \cdot z_{i,j}$ gives us the same result as the function $\lceil \mathcal{T} \rfloor$ under the condition $p \geq \lceil \log_2(s+1) \rceil$, which is needed for avoiding rounding errors. For $a \in \mathbb{Q}$, let $a^{(k)} \in \{0, 1\}$ denote its k-th bit. For each i, j, we only need to take $z_{i,j} = \sum_{k=0}^{p} q_{i,j}^{(-k)}/2^p$ as an approximation of $q_{i,j}$. By the above arguments, we have

$$\lceil \mathcal{T} \rfloor = \left\lceil \sum_{i=1}^{s} \sum_{j=0}^{S-1} b_{i,j} \cdot z_{i,j} \right\rfloor = \left\lceil \sum_{i=1}^{s} \sum_{k=0}^{p} q(i,k)/2^p \right\rfloor, \tag{5.3}$$

where $q(i,k) = \bigoplus_{j=0}^{S-1} b_{i,j} \cdot q_{i,j}^{(-k)} \in \{0, 1\}$. To evaluate the function (5.3), we need to consider the $s \times (p+1)$ matrix A defined by $A = (q(i,k))_{i,k}$, and use the grade-school addition algorithm $\mathsf{grade\_school\_add}$ for the matrix A, which outputs our desired value (5.3) (details of the algorithm are discussed in [9, Section 8.1]). As a summary, the decryption function $[c \cdot \mathsf{sk}]_d \pmod 2$ can be rewritten as

$$\underbrace{\bigoplus_{i=1}^{s}\bigoplus_{j=0}^{S-1} b_{i,j} \cdot y_{i,j}}_{\text{linear term of the } b_{i,j}\text{'s}} \pmod 2 \oplus \underbrace{\mathsf{grade\_school\_add}(A)}_{\text{non-linear term}} \pmod 2. \tag{5.4}$$

Then the re-encryption procedure for a ciphertext c is to compute

$$\mathsf{Recrypt}(c, \mathsf{PK}_{\mathsf{FHE}}) = \bigoplus_{i=1}^{s}\bigoplus_{j=0}^{S-1} c_{i,j} \cdot y_{i,j} \oplus \mathsf{grade\_school\_add}(A_{\text{enc}}), \tag{5.5}$$

where $A_{\text{enc}} = (Q(i,k))_{i,k}$ denotes the $s \times (p+1)$ matrix with

$$Q(i,k) = \bigoplus_{j=0}^{S-1} c_{i,j} \cdot q_{i,j}^{(k)}.$$

The decryption of the re-encrypted ciphertext (5.5) gives us the same result as that of the original ciphertext due to the expression (5.4). The procedure (5.5) is essentially the re-encryption method given by Gentry and Halevi in [9].

Remark 5.1. In [9, Section 9.2], Gentry and Halevi introduce a compression technique in order not to make the public key $\mathsf{PK}_{\mathsf{FHE}}$ huge. This technique enables us to reduce the size of the public key, whereas it increases the depth of the decryption circuit and hence it enforces us to set larger t for the re-encryption procedure. Since our aim is to give the minimum t required for performing the re-encryption procedure, we do not consider to use the technique in this work.

5.2 Suitable key parameters for the re-encryption

Using the theoretical evaluation of the decryption range in Corollary 3.2, we consider suitable key parameters (n, t) of the SHE scheme in order to guarantee the re-encryption method theoretically. As in [9], we first fix $s = 15$ and $p = 4$, which satisfy the condition $p \geq \lceil \log_2(s+1) \rceil$. Furthermore, we set $S = 4096 = 2^{12}$ for the higher security of the FHE scheme (see [15] for his breaking results of the SSSP in Gentry–Halevi's FHE public challenges), and only consider $n \leq 65536 = 2^{16}$ for the performance. Let $\vec{a}_{\text{rec}} \in \mathbb{Z}^n \simeq R$ denote the masked plaintext corresponding to a re-encrypted ciphertext $\mathsf{Recrypt}(c, \mathsf{PK}_{\mathsf{FHE}})$. To evaluate the re-encryption procedure (5.5) homomorphically, we estimate the ∞-norm size of

$\vec{a}_{\text{rec}}$. For each i, j, let $\vec{a}_{i,j} \in \mathbb{Z}^n \simeq R$ denote the masked plaintext corresponding to the ciphertext $c_{i,j}$. Then we have

$$\|\vec{a}_{\text{rec}}\|_\infty \approx \|\mathsf{grade\_school\_add}(A_{\text{mask}})\|_\infty$$

from the equation (5.5) (we ignore the ∞-norm size of the linear term, which is considerably smaller than the size of the non-linear term), where A_{mask} is the $s \times (p+1)$ matrix with the (i,k)-entry $\bigoplus_{j=0}^{S-1} \vec{a}_{i,j} \cdot q_{i,j}^{(k)}$ (cf. the matrix A_{enc}). According to the discussion in [9, Section 4.2], the algorithm grade_school_add is represented as a multivariate polynomial of total degree 15 with about 2^{34} monomials of degree 15. Hence, $\mathsf{grade\_school\_add}(A_{\text{mask}})$ is represented as a multivariate polynomial with about $2^{34} \times S^{15}$ monomials of degree 15 in the $\vec{a}_{i,j}$'s. Then we can estimate

$$\begin{aligned}\|\mathsf{grade\_school\_add}(A_{\text{mask}})\|_\infty &\approx 2^{34} \times S^{15} \times n^{15} \times \left(\max_{i,j} \|\vec{a}_{i,j}\|_\infty\right)^{15} \\ &\le 2^{34} \times 2^{12 \cdot 15} \times 2^{16 \cdot 15} \times 2^{15} = 2^{469},\end{aligned}$$

where $\max_{i,j} \|\vec{a}_{i,j}\|_\infty = 2$ independent of the probability q on noise density. Note that we also use the property that for any two elements $\vec{a}, \vec{b} \in \mathbb{Z}^n \simeq R$, we have

$$\|\vec{a} + \vec{b}\|_\infty \le \|\vec{a}\|_\infty + \|\vec{b}\|_\infty \quad \text{and} \quad \|\vec{a} \times \vec{b}\|_\infty \le n \cdot \|\vec{a}\|_\infty \cdot \|\vec{b}\|_\infty$$

by [14, Lemma 3.2]. Since we need to satisfy the condition

$$\|\vec{a}_{\text{rec}}\|_\infty \approx \|\mathsf{grade\_school\_add}(A_{\text{mask}})\|_\infty \le \frac{U}{s+1} = \frac{11n \cdot 2^{t-5}}{19n - 6}$$

by inequality (5.2) (note that $U = 11n \cdot 2^{t-1}/(19n-6)$ by the ∞-norm evaluation (3.2) in Corollary 3.2), it is enough to set about $t = 500$ to theoretically guarantee the re-encryption method for constructing the FHE scheme.

We then fix $t = 500$. The security of the SHE scheme is based on the hardness of the lattice problem γ-BDDP [9, Section 2.1] with the parameter

$$\gamma = \frac{d^{1/n}}{\min\|\vec{a}\|} \approx 2^t = 2^{500}, \tag{5.6}$$

where $\min\|\vec{a}\|$ denotes the minimal Euclidean norm of the masked plaintexts (note that we have $d \approx 2^{n \cdot t}$ by Proposition 4.4). In the cases $n \le 32768$, we have $\gamma \ge 1.01^n$ by equation (5.6), and hence these cases are estimated to be feasible to solve γ-BDDP by practical lattice reduction algorithms from the analysis of Gama and Nguyen [7]. On the other hand, in the case $n = 65536$, we have $\gamma = 1.0053^n$, which is estimated to have 80-bit security with an enough margin against the state-of-the-art lattice reduction algorithm by the analysis of Chen and Nguyen [4]. As a summary, we need to take

$$(n, t) = (65536, 500)$$

in order to achieve both the re-encryption process and the enough security.

Remark 5.2. For their FHE public challenges, Gentry and Halevi experimentally estimate that it is enough to set about $t = 400$ for the re-encryption method (see [9, Table 3] for parameters). However, their parameters deeply depend on the probability q on noise density, and they select a somewhat aggressive parameter q in order not to increase the Euclidean size of the noise vector (actually, they take q so that the number of the non-zero entries in the noise vector of a fresh ciphertext is between 15 and 20). In contrast, we take $t = 500$ based on the ∞-norm evaluation in Corollary 3.2. This evaluation is independent of the probability q, and hence it enables us to take arbitrary q so that the FHE scheme can be more secure (for example, we can take $q = \frac{1}{3}$ for the highest security).

Bibliography

[1] Z. Brakerski, C. Gentry and V. Vaikuntanathan, (Leveled) fully homomorphic encryption without bootstrapping, in: *Innovations in Theoretical Computer Science* (ITCS 2012), ACM (2012), 309–325.

[2] Z. Brakerski and V. Vaikuntanathan, Efficient fully homomorphic encryption from (standard) LWE, in: *Foundations of Computer Science* (FOCS 2011), IEEE (2011), 97–106.

[3] Z. Brakerski and V. Vaikuntanathan, Fully homomorphic encryption from ring-LWE and security for key dependent message, in: *Advances in Cryptology* (Crypto 2011), Lecture Notes in Comput. Sci. 6841, Springer (2011), 505–524.

[4] Y. Chen and P. Q. Nguyen, BKZ 2.0: Better lattice security estimates, in: *Advances in Cryptology* (Asiacrypt 2011), Lecture Notes in Comput. Sci. 7073, Springer (2011), 1–20.

[5] J.-S. Coron, A. Mandal, D. Naccache and M. Tibouchi, Fully homomorphic encryption over the integers with shorter public-keys, in: *Advances in Cryptology* (Crypto 2011), Lecture Notes in Comput. Sci. 6841, Springer (2011), 487–504.

[6] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, Fully homomorphic encryption over the integers, in: *Advances in Cryptology* (Eurocrypt 2010), Lecture Notes in Comput. Sci. 6110, Springer (2010), 24–43.

[7] N. Gama and P. Q. Nguyen, Predicting lattice reduction, in: *Advances in Cryptology* (Eurocrypt 2008), Lecture Notes in Comput. Sci. 4965, Springer (2008), 31–51.

[8] C. Gentry, Fully homomorphic encryption using ideal lattices, in: *Symposium on Theory of Computing* (STOC 2009), ACM (2009), 169–178.

[9] C. Gentry and S. Halevi, Implementing Gentry's fully-homomorphic encryption scheme, in: *Advances in Cryptology* (Eurocrypt 2011), Lecture Notes in Comput. Sci. 6632, Springer (2011), 129–148.

[10] C. Gentry, S. Halevi and N. P. Smart, Better bootstrapping in fully homomorphic encryption, in: *Public Key Cryptography* (PKC 2012), Lecture Notes in Comput. Sci. 7293, Springer (2012), 1–16.

[11] C. Gentry, S. Halevi and N. P. Smart, Fully homomorphic encryption with polylog overhead, in: *Advances in Cryptology* (Eurocrypt 2012), Lecture Notes in Comput. Sci. 7237, Springer (2012), 465–482.

[12] C. Gentry, S. Halevi and N. P. Smart, Homomorphic evaluation of the AES circuit, in: *Advances in Cryptology* (Crypto 2012), Lecture Notes in Comput. Sci. 7417, Springer (2012), 850–867.

[13] J. Hoffstein, J. Pipher and J. H. Silverman, NTRU: A ring-based public key cryptosystem, in: *Algorithmic Number Theory Third International Symposium* (ANTS-III), Lecture Notes in Comput. Sci. 1423, Springer (1998), 267–288.

[14] K. Lauter, M. Naehrig and V. Vaikuntanathan, Can homomorphic encryption be practical?, in: *Proceedings of the Third ACM Workshop on Cloud Computing Security Workshop*, ACM (2011), 113–124.

[15] M. S. Lee, On the sparse subset sum problem from Gentry–Halevi's implementation of fully homomorphic encryption, preprint (2011), `http://eprint.iacr.org/2011/567.pdf`.

[16] A. López-Alt, E. Tromer and V. Vaikuntanathan, On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption, in: *Symposium on Theory of Computing* (STOC 2012), ACM (2012), 1219–1234.

[17] N. P. Smart and F. Vercauteren, Fully homomorphic encryption with relatively small key and ciphertext sizes, in: *Public Key Cryptography* (PKC 2010), Lecture Notes in Comput. Sci. 6056, Springer (2010), 420–443.

[18] N. P. Smart and F. Vercauteren, Fully homomorphic SIMD operations, *Des. Codes Cryptogr.* **71** (2014), 57–81.

[19] M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama and T. Koshiba, Packed homomorphic encryption based on ideal lattices and its application to biometrics, in: *Security Engineering and Intelligence Informatics*, Lecture Notes in Comput. Sci. 8128, Springer (2013), 55–74.

Received July 4, 2013; revised January 14, 2014; accepted March 4, 2014.

Author information

Masaya Yasuda, Fujitsu Laboratories Ltd., 1-1, Kamikodanaka 4-chome,
Nakahara-ku, Kawasaki, Kanagawa 211-8588, Japan.
E-mail: yasuda.masaya@jp.fujitsu.com

Kazuhiro Yokoyama, Department of Mathematics, Rikkyo University,
3-34-1, Nishi-Ikebukuro, Tokyo 171-8501, Japan.
E-mail: kazuhiro@rikkyo.ac.jp

Takeshi Shimoyama, Fujitsu Laboratories Ltd., 1-1, Kamikodanaka 4-chome,
Nakahara-ku, Kawasaki, Kanagawa 211-8588, Japan.
E-mail: shimo-shimo@jp.fujitsu.com

Jun Kogure, Fujitsu Laboratories Ltd., 1-1, Kamikodanaka 4-chome,
Nakahara-ku, Kawasaki, Kanagawa 211-8588, Japan.
E-mail: kogure@jp.fujitsu.com

Takeshi Koshiba, Division of Mathematics, Electronics and Informatics,
Graduate School of Science and Engineering, Saitama University,
255 Shimo-Okubo, Sakura, Saitama, 338-8570, Japan.
E-mail: koshiba@mail.saitama-u.ac.jp