Security Analysis of Cryptosystems Using Short Generators over Ideal Lattices

Shinya Okumura, Shingo Sugiyama, Masaya Yasuda, and Tsuyoshi Takagi

Institute of Mathematics for Industry, Kyushu University,
744 Motooka Nishi-ku, Fukuoka 819-0395, Japan

Abstract. In this paper, we analyze the security of cryptosystems using short generators over ideal lattices such as candidate multilinear maps by Garg, Gentry and Halevi and fully homomorphic encryption by Smart and Vercauteren. Our approach is based on a recent work by Cramer, Ducas, Peikert and Regev on analysis of recovering a short generator of an ideal of the q-th cyclotomic field from any generator of the ideal for a prime power q. Unfortunately, the main result of Cramer et al. has some flaws since they use an incorrect lower bound of the special values of Dirichlet L-functions at 1.

Our main contribution is to correct Cramer et al.'s main result by estimating explicit lower and upper bounds of the special values of Dirichlet L-functions at 1 for any non-trivial Dirichlet characters modulo a prime power. Moreover, we give various experimental evidence that recovering a short generator is succeeded with high probability. As a consequence, our analysis suggests that the security of the above cryptosystems based on the difficulty of recovering a short generator is reduced to solving the principal ideal problem under the number theoretical conjecture so-called Weber's class number problem.

Key words: Short generators, Cyclotomic fields, Log-unit lattices, Dirichlet L-functions.

1 Introduction

In recent years, lattice-based cryptography has been paid much attention to as a candidate of post-quantum cryptography. Ideal lattices are in a special class of lattices corresponding to ideals in rings of the form $\mathbb{Z}[x]/(f(x))$ for some irreducible polynomial $f(x)$, such as $f(x) = x^n + 1$ for a 2-power integer $n > 1$ (e.g. see [35] for details). In cryptography, ideal lattices have been used as powerful tools to construct a number of efficient and secure cryptosystems, mainly including public key encryption schemes [45, 46], hash functions [33, 37, 41] and digital signatures [32, 34]. Recently, ideal lattices have been applied to construct encryption schemes with high functionality. In 2009, Gentry [21] first proposed a construction of fully homomorphic encryption (FHE) using ideal lattices. After Gentry's breakthrough, a number of variants of Gentry's original FHE scheme have been proposed (in particular, variants of [22, 47] are based on

ideal lattices). In 2013, Garg, Gentry and Halevi [20] first proposed a candidate of multilinear maps from ideal lattices, called the GGH scheme. In 2014, Langlois, Stehlé and Steinfeld [27] improved the GGH scheme for both efficiency and security, and their scheme is called GGHLite (see also [3] for implementation of GGHLite).

For a 2-power integer $n > 1$, let $K = \mathbb{Q}(\zeta_{2n})$ be the $2n$-th cyclotomic field and $O_K = \mathbb{Z}[\zeta_{2n}] \simeq \mathbb{Z}[x]/(x^n + 1)$ its ring of integers, where ζ_m denotes a primitive m-th root of unity for an integer $m > 2$. In the cryptographic constructions of [20, 27, 47], a certain 'short' element $g \in O_K$ is used as a secret key. In contrast, some $\mathbb{Z}$-basis of the principal ideal (g), such as the Hermite normal form $\mathrm{HNF}(g)$, is used as a public key (e.g. see [13, Section 4] for the definition of $\mathrm{HNF}(g)$). Therefore a part of the security of schemes of [20, 27, 47] relies on the computational hardness of the following problem, introduced in [15, Section 1]:

Problem 1 (Short Generator of a Principal Ideal Problem, SG-PIP) Let K be a number field and O_K its ring of integers. Let g be a short element of O_K. Given a $\mathbb{Z}$-basis of the principal ideal (g), the problem is to find g itself or a sufficiently short element $g' \in O_K$ satisfying $(g') = (g)$.

This problem can be divided into the following two problems:

- *Principal Ideal Problem (PIP)*: Given a $\mathbb{Z}$-basis of the principal ideal $I = (g)$, find a generator h of I.
- *Short Generator Problem (SGP)*: Given a generator h of I, recover g itself or a sufficiently short generator g' of I.

1.1 Recent Progress for PIP and SGP

There are several classes of efficient algorithms for PIP over number fields of large degree in both classical and quantum computing models [7–10, 12, 24]. In [24], Hallgren proposed a polynomial-time quantum algorithm for PIP over number fields of small degree. Biasse and Fieker [7] first proposed a subexponential algorithm for an arbitrary class of number fields under the generalized Riemann hypothesis (see also [8]). For security analysis of cryptosystems of [20, 27, 47], we focus on PIP over cyclotomic fields. For 2^k-th cyclotomic fields, Campbell, Groves and Shepherd [12] claimed that there is a polynomial-time quantum algorithm for PIP, although their claim has not been proved yet. Recently, Biasse [9] announced the same claim as Campbell et al.'s one. In a classical computing model, Biasse [10] also presented a heuristic algorithm to solve PIP over 2^k-th cyclotomic fields in time $2^{N^{2/3+\epsilon}}$ for $N = 2^k$ and arbitrarily small $\epsilon > 0$.

As for SGP, Bernstein [6] first pointed out that SGP over (2^k-th) cyclotomic fields is reduced to a closest vector problem (CVP) over the log-unit lattice, which is obtained by the logarithmic embedding. Similar attacks are also sketched by Campbell et al. [12]. Recently, Cramer, Ducas, Peikert and Regev [15] studied the geometry of a sublattice of a log-unit lattice, spanned by the image of the canonical generators of the group of cyclotomic units under the logarithmic

embedding. They claimed in [15, Theorem 3.1] that the basis of the sublattice has good properties. They also proposed an algorithm [15, Theorem 4.1] for SGP over 2^k-th cyclotomic fields, under the assumption that Weber's class number problem holds true (the problem is the conjecture that the class number of $\mathbb{Q}(\zeta_q + \overline{\zeta_q})$ is equal to 1 for any 2-power integer $q > 2$).

Outline of [15] Here let us review Cramer et al.'s analysis for SGP in more detail. Given a prime power $q = p^k$, let $K = \mathbb{Q}(\zeta_q)$ be the q-th cyclotomic field and $O_K = \mathbb{Z}[\zeta_q]$ its ring of integers. Consider the logarithmic embedding $\mathrm{Log} : K^\times \longrightarrow \mathbb{R}^{\varphi(q)/2}$, where $\varphi(q) = \#(\mathbb{Z}/q\mathbb{Z})^\times$ (see Subsection 2.2 below for the definition of the embedding). Let $O_K^\times$ denote the group of units in O_K. Then $\Lambda := \mathrm{Log}(O_K^\times)$ defines a lattice of rank $\varphi(q)/2 - 1$, called the *log-unit lattice*. Set $G = (\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}$. Let Λ' be the sublattice of Λ spanned by the basis

$$\mathbf{B} := \{\mathbf{b}_j := \mathrm{Log}((\zeta_q^j - 1)/(\zeta_q - 1)) \mid j \in G \smallsetminus \{1\}\}.$$

Cramer et al. reduced SGP over K to CVP over Λ', and they gave a condition for succeeding in solving CVP over Λ'. The success of their attack depends on the size of $\|\mathbf{b}_j^\vee\|$ for $j \in G \smallsetminus \{1\}$, where $\mathbf{b}_j^\vee$'s are the dual basis of $\mathbf{B}$ in $\mathbb{R}^{\varphi(q)/2}$. They claimed in [15, Theorem 3.1] that all $\|\mathbf{b}_j^\vee\|$ for $j \in G \smallsetminus \{1\}$ are mutually equal, and gave an upper bound of $\|\mathbf{b}_j^\vee\|$ (their attack is implemented over PARI/GP by Schank [43]).

Flaws in [15] To estimate the size of $\|\mathbf{b}_j^\vee\|$ is important to analyze the success probability of Cramer et al.'s attack for SGP. They gave a relation between the size of $\|\mathbf{b}_j^\vee\|^2$ and $L(1, \chi)$ for any non-trivial even Dirichlet character χ, where $L(s, \chi)$ denotes the Dirichlet L-function associated with χ (see Subsection 2.3 for definitions of Dirichlet characters and Dirichlet L-functions, and see Proposition 1 in Section 5 for the relation). They gave an upper bound of $\|\mathbf{b}_j^\vee\|$ up to constant by using the *incorrect* lower bound

$$|L(1, \chi)| \gg \frac{1}{\log f_\chi}$$

for any non-trivial Dirichlet character χ of conductor f_χ [15, Theorem 2.6] (see Subsection 2.3 for the definition of the conductor of a Dirichlet character). However, this lower bound is valid only for non-quadratic primitive character χ at present. As for quadratic characters, the currently known best lower bound is

$$|L(1, \chi)| \gg_\epsilon \frac{1}{q^\epsilon}, \tag{1}$$

for quadratic characters χ with the implied constant depending only on any $\epsilon > 0$ but ineffective. We refer to Siegel's theorem [44] (see also [16, §21]). The possibility of existence of a Siegel zero causes the ineffectiveness of the implied constant in (1). A Siegel zero is a special zero $\beta \in (1/2, 1)$ of $L(s, \chi)$, which may occur only when χ is quadratic.

1.2 Our Contributions

Our contributions of this paper are as follows:

- **Upper and Lower Bounds of $L(1,\chi)$:** We give explicit upper and lower bounds of $L(1,\chi)$ for each even Dirichlet character χ modulo a prime power $q = p^k$ (Section 6 below). Our analysis is based on the following facts: For each non-trivial Dirichlet character χ modulo q, we have the functional equation $L(s,\chi) = L(s,\chi^*)$, where χ^* is the primitive Dirichlet character inducing χ. By the functional equation, an estimate of $L(s,\chi)$ is deduced to that of $L(s,\chi^*)$. Then we use results on upper and lower bounds of $L(1,\chi)$ by [17, 29, 31, 42]. Another key point is that we give a lower bound of $L(1,\chi)$ for any even *quadratic* Dirichlet character χ modulo q with the aid of the class number formula. Moreover, our bounds are easily computable, namely we can evaluate the size $L(1,\chi)$ for any fixed $k \geq 1$ and χ.
- **Theoretical Estimation of $\|\mathbf{b}_j^\vee\|$:** We give correct upper and lower bounds of the size of $\|\mathbf{b}_j^\vee\|$ by using our bounds of $L(1,\chi)$ (Sections 7 and 8 below). Our strategy is to count the exact number of even Dirichlet characters modulo q having any given conductor f_χ, while Cramer et al. used a rough estimate of the number of such characters. The asymptotic evaluation of our upper bounds of $\|\mathbf{b}_j^\vee\|$ has the same order as Cramer et al.'s one, in other words, we first give a correct proof of their result. In particular, we have $\|\mathbf{b}_j^\vee\| \to 0$ as $k \to \infty$ for any prime number p and $q = p^k$. Different from Cramer et al.'s evaluation, our bounds of $\|\mathbf{b}_j^\vee\|$ are explicit for any fixed k. Specifically, our bounds imply that the success probability of their attack becomes much higher for $q = 2^k$ with $k \geq 11$.
- **Experimental Verification:** By experiments, we verify the effectiveness of Cramer et al.'s attack against cryptosystems of [20, 27, 47] for $q = 2^k$ and $6 \leq k \leq 10$ (Section 9 below). In particular, Cramer et al.'s attack can recover the secret key g with about 50 % (resp. 85 % and 100 %) probability when $k = 6$ (resp. $k = 8$ and $k = 10$). Our experiments also show that the success probability of their attack is independent of the distributions for generating keys in cryptosystems of [20, 27, 47] (e.g. uniformly random and discrete Gaussian distributions).

Recall that the security of cryptosystems of [20, 27, 47] is based on the difficulty of Problem 1 (SG-PIP), which can be divided into two problems PIP and SGP. By combining our theoretical and experimental results, we expect that SGP over 2^k-th cyclotomic fields in cryptosystems of [20, 27, 47] could be solved by Cramer et al.'s attack if $k \geq 10$, under the assumption that Weber's class number problem holds true. Note that $k \geq 10$ is required for high security (e.g. 80-bit security) of these cryptosystems. Thereby, the security of these cryptosystems relies only on the difficulty of PIP.

2 Mathematical Background

In this section, we review mathematical notation for our later discussion. Let $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$ be the set of positive integers, the ring of integers, the field of real

numbers, and the field of complex numbers, respectively. We denote by $\langle \cdot, \cdot \rangle$ and $\| \cdot \|$ the natural inner product and the Euclidean norm on $\mathbb{C}^n$, respectively. We also denote column vectors by lower-case bold letters (e.g. $\mathbf{b}$) and matrices by upper-case bold letters (e.g. $\mathbf{B}$). The symbol $\#S$ stands for the cardinality of a set S. For non-negative functions f and g on a set X, we write $f(x) \ll g(x)$ (or $f(x) = \mathcal{O}(g(x))$) if there exists a constant $C > 0$ such that $f(x) \leq Cg(x)$ for all $x \in X$. For $\epsilon > 0$, we write $f(x) \ll_\epsilon g(x)$ if the implied constant depends on ϵ.

2.1 Lattices and CVP

A *lattice* $\mathcal{L}$ is a discrete additive subgroup of a finite dimensional $\mathbb{R}$-vector space $\mathbb{R}^n$ for some $n \in \mathbb{N}$. The *rank* of $\mathcal{L}$ is defined as $\dim_{\mathbb{R}} \mathcal{L} \otimes_{\mathbb{Z}} \mathbb{R}$. Given any lattice $\mathcal{L} \subset \mathbb{R}^n$ of rank $m \leq n$, there exists a set of $\mathbb{R}$-linearly independent vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ such that $\mathcal{L} = \mathcal{L}(\mathbf{B}) := \sum_{1 \leq i \leq m} \mathbb{Z}\mathbf{b}_i$. We identify $\mathbf{B}$ as an $n \times m$-matrix, and the matrix is called a *basis* of $\mathcal{L}$. For any lattice $\mathcal{L}$ with basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$, there exists a set of $\mathbb{R}$-linearly independent vectors $\mathbf{B}^\vee = \{\mathbf{b}_1^\vee, \ldots, \mathbf{b}_m^\vee\} \subset \mathrm{span}(\mathbf{B}) := \sum_{1 \leq i \leq m} \mathbb{R}\mathbf{b}_i$ such that $\langle \mathbf{b}_i, \mathbf{b}_j^\vee \rangle = \delta_{ij}$, where δ_{ij} is the Kronecker delta given by $\delta_{ij} = 1$ (resp. $\delta_{ij} = 0$) if $i = j$ (resp. otherwise). In other words, $\mathbf{B}^t \cdot \mathbf{B}^\vee = (\mathbf{B}^\vee)^t \cdot \mathbf{B}$ is equal to the identity matrix. Then $\mathcal{L}^\vee := \mathcal{L}(\mathbf{B}^\vee)$ defines a lattice, called the *dual lattice* of $\mathcal{L}$ with the *dual basis* $\mathbf{B}^\vee$ of $\mathbf{B}$.

Given a lattice $\mathcal{L} \subset \mathbb{R}^n$ with basis $\mathbf{B}$ and a target vector $\mathbf{t} \in \mathbb{R}^n \smallsetminus \mathcal{L}$, the closest vector problem (CVP) is to find a lattice vector $\mathbf{v} \in \mathcal{L}$ closest to $\mathbf{t}$. An efficient approach for CVP is the round-off algorithm proposed by Babai [4]. The round-off algorithm for $\mathbf{B}$ and $\mathbf{t}$ outputs $\mathbf{B} \cdot \lfloor (\mathbf{B}^\vee)^t \cdot \mathbf{t} \rceil \in \mathcal{L}$, where the rounding function $\lfloor c \rceil := \lfloor c + \frac{1}{2} \rfloor$ is applied to each entry of $(\mathbf{B}^\vee)^t \cdot \mathbf{t}$ independently. The following lemma suggests a condition for solving CVP by Babai's round-off algorithm.

Lemma 1. ([15, Claim 2.1]) Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice with basis $\mathbf{B}$. Let $\mathbf{t} = \mathbf{v} + \mathbf{e}$ with $\mathbf{v} \in \mathcal{L}$ and $\mathbf{e} \in \mathbb{R}^n$. If $\langle \mathbf{b}_j^\vee, \mathbf{e} \rangle \in \left[-\frac{1}{2}, \frac{1}{2}\right)$ for all $\mathbf{b}_j^\vee \in \mathbf{B}^\vee$, then $\mathbf{v}$ can be recovered by Babai's round-off algorithm for $\mathbf{B}$ and $\mathbf{t}$.

This lemma is a key for solving SGP by Cramer et al.'s attack (see Section 4).

2.2 Log-Unit Lattice and Cyclotomic Units

For an integer $q > 2$, let $\zeta_q \in \mathbb{C}$ be a primitive q-th root of unity. Then the field $K = \mathbb{Q}(\zeta_q)$ is called the q-th *cyclotomic field*. The field K is a Galois extension of $\mathbb{Q}$ of degree $[K : \mathbb{Q}] = \varphi(q)$, where φ denotes the Euler totient function defined by $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ for $n \in \mathbb{N}$. Then $O_K = \mathbb{Z}[\zeta_q]$ is the ring of integers of K. For any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we have $\sigma(\zeta_q) = \zeta_q^j$ for some $j \in \mathbb{Z}$ with $\gcd(j, q) = 1$ since $\sigma(\zeta_q)$ is also a primitive root of unity. In other words, we have

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_j \mid j \in (\mathbb{Z}/q\mathbb{Z})^\times\} \cong (\mathbb{Z}/q\mathbb{Z})^\times$$

with $\sigma_j(\zeta_q) = \zeta_q^j$. Set $G := (\mathbb{Z}/q\mathbb{Z})^\times / \{\pm 1\}$. From now on we fix an enumeration $G \cong \{1, \cdots, \varphi(q)/2\}$ and define the *logarithmic embedding* of $K^\times$ by

$$\mathrm{Log} : K^\times \longrightarrow \mathbb{R}^{\varphi(q)/2},\ a \mapsto (\log |\sigma_j(a)|)_{j \in G}\,.$$

We have $\mathrm{Log}(a \cdot b) = \mathrm{Log}(a) + \mathrm{Log}(b)$ for any $a, b \in K^\times$. Let $O_K^\times$ denotes the group of units in O_K. By the Dirichlet Unit Theorem (e.g. see [40]), $\Lambda := \mathrm{Log}(O_K^\times)$ gives a lattice of rank $\frac{\varphi(q)}{2} - 1$, and the kernel of $\mathrm{Log}|_{O_K^\times}$ is $\mu(K)$, where $\mu(K)$ denotes the group of all roots of unity in K. The lattice Λ is called the *log-unit lattice* of K. It is easy to see that all vectors in Λ are orthogonal to $\mathbf{1} := (1, 1, \ldots, 1) \in \mathbb{R}^{\varphi(q)/2}$ since $N_{K/\mathbb{Q}}(\epsilon) = \prod_{j \in (\mathbb{Z}/q\mathbb{Z})^\times} \sigma_j(\epsilon) = \pm 1$ for any $\epsilon \in O_K^\times$, where $N_{K/\mathbb{Q}}$ denotes the norm map from $K^\times$ to $\mathbb{Q}^\times$.

Let A be the multiplicative subgroup of $K^\times$ generated by $\pm\zeta_q$ and $z_j := \zeta_q^j - 1$ for $j \in G$. We have $\mathrm{Log}(z_j) = \mathrm{Log}(z_{-j})$ since $z_j = -\zeta_q^j z_{-j}$, that is, $z_j \equiv z_{-j} \pmod{\mu(K)}$. The group of *cyclotomic units* C is defined as

$$C := A \cap O_K^\times.$$

In general, it may not be easy to compute generators of C. However, when $q = p^k$ for some prime number p, generators of C are obtained by the following lemma:

Lemma 2. ([49, Lemma 8.1]) Let $q = p^k$ be a prime power and C the group of cyclotomic units of q-th cyclotomic field. Set $G := (\mathbb{Z}/q\mathbb{Z})^\times / \{\pm 1\}$, $z_j := \zeta_q^j - 1$ and $b_j := z_j / z_1$ for $j \in G \setminus \{1\}$. Then the group C is generated by $\pm\zeta_q$ and the b_j's for $j \in G \setminus \{1\}$.

We call the b_j's for $j \in G \setminus \{1\}$ the *canonical generators* of C. Note that $\mathrm{Log}(C)$ is a sublattice of Λ of finite index. More precisely, we have $[\Lambda : \mathrm{Log}(C)] = h^+(q)$ for a prime power q, where $h^+(q)$ is the class number of $K^+ := \mathbb{Q}(\zeta_q + \overline{\zeta_q})$ (see [49, Exercise 8.5] for details).

2.3 Dirichlet Characters and Dirichlet L-functions

Let G be a finite abelian group. The *character group* of G, denoted by $\widehat{G}$, is the set of group homomorphisms from G to $\mathbb{C}^\times$. It is easy to see that $\widehat{G}$ becomes a group with the pointwise product. There is a non-canonical group isomorphism between G and $\widehat{G}$, and hence $\#G = \#\widehat{G}$.

Let us introduce Dirichlet characters and Dirichlet L-functions (e.g. see [16]). For $q \in \mathbb{N}$, we consider the group $(\mathbb{Z}/q\mathbb{Z})^\times$. An element $\chi \in \widehat{(\mathbb{Z}/q\mathbb{Z})^\times}$ is called a *Dirichlet character* (or character) modulo q. The character χ is naturally extended to a multiplicative function $\widetilde{\chi}$ on $\mathbb{N}$ by

$$\widetilde{\chi}(n) = \begin{cases} \chi(n \bmod q) & (\gcd(n, q) = 1), \\ 0 & (\gcd(n, q) > 1). \end{cases}$$

We denote the extended function $\widetilde{\chi}$ by χ for simplicity. The *conductor* f_χ of χ is defined as the minimal positive divisor d of q such that χ factors through some Dirichlet character χ' modulo d, that is, we have

$$\chi : (\mathbb{Z}/q\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/d\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{C}^\times.$$

We denote by χ^* the Dirichlet character modulo f_χ inducing χ. We call χ *primitive* if f_χ is exactly equal to q. Notice that χ^* is primitive. The character χ is called *even* (resp. *odd*) if $\chi(-1) = 1$ (resp. $\chi(-1) = -1$), and χ is called *quadratic* if χ^2 is trivial but χ is non-trivial.

Let $L(s, \chi)$ denote the Dirichlet L-function associated with χ, defined by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \qquad (\mathrm{Re}(s) > 1).$$

The defining series converges absolutely on the region $\mathrm{Re}(s) > 1$. If χ is non-trivial, the series $L(s, \chi)$ converges on the region $\mathrm{Re}(s) > 0$. It is well-known that $L(s, \chi)$ has a meromorphic continuation to the whole plane $\mathbb{C}$, its only possible pole $s = 1$ is simple and occurs only when χ is trivial. We have the relation

$$L(s, \chi) = \{\prod_{\substack{p|q \\ p\nmid f_\chi}} (1 - \chi^*(p)p^{-s})\} L(s, \chi^*) \tag{2}$$

for non-trivial character χ, where p runs over all prime divisors of q such that $p \nmid f_\chi$.

3 Cryptosystems Using Short Generators

As mentioned in Section 1, the security of some cryptosystems [20, 27, 47] relies on the computational hardness of finding a short generator of a principal ideal of a number field from a $\mathbb{Z}$-basis of the ideal. This problem is called the Short Generator of a Principal Ideal Problem (SG-PIP). In this section, we briefly give a relation between these cryptosystems and SG-PIP. These cryptosystems are constructed over the ring $R = \mathbb{Z}[x]/(x^n + 1)$ for give a degree parameter n of 2-power.

3.1 Smart-Vercauteren FHE Scheme

We explain the somewhat homomorphic encryption (SHE) proposed by Smart and Vercautern [47], which is integrated to the fully homomorphic encryption (FHE) using the bootstrapping. The key generation of the SHE scheme over R is as follows:

1. Given a parameter $\eta > 0$, choose a random polynomial $G(x) = \sum_{i=0}^{n-1} g_i x^i \in \mathbb{Z}[x]$, such that $\|G(x)\|_\infty := \max_i |g_i|$ is η-bit, $G(x) \equiv 1 \pmod 2$, and $p = \det(\mathrm{Rot}(G(x)))$ is prime, where $\mathrm{Rot}(G(x))$ denotes the rotation matrix.

2. Compute $D(x) = \gcd(G(x), x^n + 1)$ over $\mathbb{F}_p[x]$, and take the unique root $\alpha \in \mathbb{F}_p$ of $D(x)$.
3. Apply the XGCD-algorithm over $\mathbb{Q}[x]$ to obtain $Z(x) = \sum_{i=0}^{n-1} z_i x^i \in \mathbb{Z}[x]$ satisfying $Z(x) \cdot G(x) \equiv p \pmod{x^n + 1}$. Set $B = z_0 \pmod 2$. Then the public key is $\mathsf{pk} = (p, \alpha)$, and the secret key is $\mathsf{sk} = (p, B)$.

The ideal $\mathfrak{p} = (p, x - \alpha)$ of R is constructed from pk, and its Hermite normal form (HNF) is given by

$$\begin{pmatrix} p & -\alpha & \cdots & -\alpha^{n-1} \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

By the construction, $\mathfrak{p}$ is a principal ideal generated by $G(x) \in R$. As mentioned in [47], sk can be recovered from the inverse of a small generator of $\mathfrak{p}$ (since $\eta \ll p$). Hence, recovering sk from pk is an instance of SG-PIP.

3.2 GGH and GGHLite Schemes

We explain the miltilinear map (GGH scheme) proposed by Garg et al. [20] and its improved version called GGHLite [27]. Let $D_{\mathbb{Z},\sigma}$ denote the discrete Gaussian distribution over $\mathbb{Z}$ with standard deviation $\sigma > 0$. In the GGH scheme, a secret short element $g = \sum_{i=0}^{n-1} g_i x^i \in R$ is randomly chosen with $g_i \leftarrow D_{\mathbb{Z},\sigma}$ for $0 \le i \le n-1$ such that $\|g^{-1}\| \le n^2$ and $I = (g)$ is a prime ideal in R, where $g^{-1} \in R \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}(\zeta_{2n})$ and $\|g^{-1}\|$ is its Euclidean norm. The condition $\|g\| \le \sqrt{n} \cdot \sigma$ is additionally required for the construction of the GGHLite scheme [27]. Moreover, given a modulus parameter $q > 0$, a secret element z is randomly sampled from $R_q = R/qR$. In both the GGH and the GGHLite schemes, the pair (g, z) gives a secret key.

The *zeroizing attack*, which was first introduced in [20] tries to recover a basis $\mathbf{B}$ of the ideal $I = (g)$ from given public parameters such as several encoding of zero and one (See [13, Section 5.1] for details). Therefore, recovering g or a short element g' from the basis $\mathbf{B}$ is an instance of SG-PIP (as mentioned in [13, Section 5.3], recovering $g' \in R$ with $\|g'\| < q^{3/8}/(2n)^4$ is sufficient to attack the GGH scheme).

4 Overview of Cramer et al.'s Attack for SGP

In this section, we briefly review Cramer et al.'s attack for SGP (defined in Section 1) and give some remarks on their attack.

4.1 Attack Algorithm

For a prime power $q = p^k$, we use the same notation such as $G = (\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}$, the log-unit lattice Λ and the group of cyclotomic units C of the q-th cyclotomic field $K = \mathbb{Q}(\zeta_q)$ described in Subsection 2.2. For the canonical generator

$\{\mathbf{b}_j\}_{j\in G\smallsetminus\{1\}}$ of C, set

$$\mathbf{b}_j := \mathrm{Log}(b_j) \in \mathrm{Log}(C) \tag{3}$$

for $j \in G \smallsetminus \{1\}$. Note that $\{\mathbf{b}_j\}_{j\in G\smallsetminus\{1\}}$ is a basis of $\mathrm{Log}(C)$ by Lemma 2. Let $g \in O_K$ be a short element as in Problem 1. Given a generator h of the principal ideal $I = (g)$, SGP is to find g itself or a sufficiently short generator of I. Since both g and h are generators of I, we have $h = ug$ for some $u \in O_K^\times$, and $\mathrm{Log}(h) = \mathrm{Log}(g) + \mathrm{Log}(u)$ with $\mathrm{Log}(u) \in \Lambda = \mathrm{Log}(O_K^\times)$. In order to recover $\mathrm{Log}(u)$ from $\mathrm{Log}(h)$, Cramer et al.'s attack aims to represent

$$\mathrm{Log}(u) = \sum_{j\in G\smallsetminus\{1\}} a_j \mathbf{b}_j \text{ for some } a_j \in \mathbb{Z} \tag{4}$$

by using the basis $\{\mathbf{b}_j\}_{j\in G\smallsetminus\{1\}}$ of $\mathrm{Log}(C)$.

For the representation (4), Cramer et al. first assume that the $\mathrm{Log}(C)$ is exactly equal to the log-unit lattice Λ:

Assumption 1 *We assume* $\mathrm{Log}(C) = \Lambda$.

Moreover, Cramer et al.'s attack algorithm assumes the following (see [15, Theorem 4.1] for details):

Assumption 2 *There is a probabilistic distribution D over K satisfying the following condition: For any unit vectors $\mathbf{v}_1, \ldots, \mathbf{v}_{\varphi(q)/2-1} \in \mathbb{R}^{\varphi(q)/2}$ satisfying $\langle \mathbf{v}_i, \mathbf{1}\rangle = 0$, we have $|\langle \mathrm{Log}(g), \mathbf{v}_i\rangle| < dq^{1/2}(\log q)^{-3/2}$ for all i with probability at least $\alpha > 0$, where g is chosen from D and d is a universal constant.*

Under Assumptions 1 and 2, Cramer et al's attack algorithm for SGP is as follows (see [15, Theorem 4.1] for details):

Algorithm 1

Input : $h = ug$ ($g \leftarrow D$, $u \leftarrow C$)
Output : $g' = ug/u'$ for some $u' \in C$ or "false"

1. Apply Babai's round-off algorithm to $\mathbf{B} := \{\mathbf{b}_j\}_{j\in G\smallsetminus\{1\}}$ and $\mathbf{t} := \mathrm{Log}(h) = \mathrm{Log}(u) + \mathrm{Log}(g)$. Let $\mathbf{v} \in \mathbb{R}^{\varphi(q)/2}$ be its output (i.e. $\mathbf{v} = \mathbf{B} \cdot \lfloor (\mathbf{B}^\vee)^t \cdot \mathbf{t} \rceil$).
2. Compute integers $a_j \in \mathbb{Z}$ for $j \in G \smallsetminus \{1\}$ such that $\mathbf{v} = \sum_{j\in G\smallsetminus\{1\}} a_j \mathbf{b}_j$. If there are no such integers a_j, then return "false".
3. Compute $u' := \prod_{j\in G\smallsetminus\{1\}} b_j^{a_j} \in C$ and output $g' = ug/u'$.

Cramer et al. claimed in [15, Theorem 4.1] that the above algorithm outputs $g' = \pm\zeta_q^j \cdot g$ for some $0 \le j < q$ with probability at least α, under Assumptions 1 and 2.

Note that Assumption 2 comes from the result [15, Theorem 3.1]. More specifically, if the result [15, Theorem 3.1] is correct (we will point out a flaw in Section

5), then there is a constant d' such that $\|\mathbf{b}_j^\vee\| \leq d' q^{-1/2} (\log q)^{3/2}$. Thus, if the universal constant d satisfies $d \leq \frac{1}{2d'}$, then we have

$$\begin{aligned}\alpha &\leq \Pr\left[|\langle \mathrm{Log}(g), \mathbf{b}_i^\vee / \|\mathbf{b}_i^\vee\| \rangle| < d q^{1/2} (\log q)^{-2/3}\right] \\ &= \Pr\left[|\langle \mathrm{Log}(g), \mathbf{b}_i^\vee \rangle| < d q^{1/2} (\log q)^{-2/3} \|\mathbf{b}_i^\vee\| \leq \frac{1}{2}\right].\end{aligned}$$

This implies that the success probability, that is $\Pr\left[|\langle \mathrm{Log}(g), \mathbf{b}_i^\vee \rangle| < \frac{1}{2}, \forall j\right]$, is at least α for the distribution D satisfying Assumption 2.

Remark 1. Since $[\Lambda : \mathrm{Log}(C)] = h^+(q)$, Assumption 1 is related to mathematical problems on $h^+(q)$. In particular, when q is 2-power, Assumption 1 is equivalent to Weber's class number problem (i.e. $h^+(q) = 1$ for all 2-power q). In Appendix A below, we will give several results related to Weber's class number problem.

4.2 Some Remarks

In the first step of Algorithm 1, we are able to compute $\mathbf{v} = \mathrm{Log}(u)$ by Lemma 1 if the condition

$$\left\langle \mathrm{Log}(g), \mathbf{b}_j^\vee \right\rangle \in \left[-\frac{1}{2}, \frac{1}{2}\right) \text{ for all } j \in G \smallsetminus \{1\} \tag{5}$$

is satisfied. In this case, we have $u' \in C$ satisfying $\mathrm{Log}(u') = \mathrm{Log}(u)$ in the second step of Algorithm 1. This implies that u' has the form $\pm\zeta_q^j \cdot u$ for some j since the kernel of $\mathrm{Log}|_{O_K^\times}$ is equal to $\mu(K)$. In other words, under condition (5), Algorithm 1 outputs our desired element $g' = \pm\zeta_q^j \cdot g$ (note that we can recover g from g' by exhaustive search of the elements $\pm\zeta_q^j$'s, whose computational cost is negligible). From Cauchy-Schwarz's inequality $|\langle \mathrm{Log}(g), \mathbf{b}_j^\vee \rangle| \leq \|\mathrm{Log}(g)\| \cdot \|\mathbf{b}_j^\vee\|$, the success of the attack deeply depends on the size of $\|\mathbf{b}_j^\vee\|$, which will be estimated in Section 7 below.

5 Detailed Description of Flaws in [15]

In this section, we describe two flaws in attack on SGP [15] in more detail.

Flaw 1 ([15, Theorem 2.6]) For any Dirichlet character χ modulo q of conductor $f_\chi > 1$, we have

$$\frac{1}{\log f_\chi} \ll |L(1, \chi)| \ll \log f_\chi. \tag{6}$$

Cramer et al. mistakenly cited the upper and lower bounds of $L(1, \chi)$ from [26]. First, the estimate as above is valid only when χ is a non-quadratic primitive character. We state more detail as follows. The upper bound should be replaced with $|L(1, \chi)| \ll \log q$ for any non-trivial Dirichlet character (e.g. [16, (13) in p.96]). As for lower bounds, we need to consider the influence of a possible real zero of $L(s, \chi)$ near to 1.

Theorem 1. ([16, p.93])

(1) There exists a constant $C > 0$ such that for any non-trivial Dirichlet character χ modulo q, $L(s, \chi)$ does not vanish if $s = \sigma + it$ $(\sigma, t \in \mathbb{R})$ is contained in the region

$$\sigma > 1 - \frac{C}{\log\{q(1 + |t|)\}}$$

except for at most one real $\beta = \beta_\chi \in (1 - \frac{C}{\log\{q(1+|t|)\}}, 1)$. We call the region a zero-free region of $L(s, \chi)$.

(2) The exceptional real zero β does not occur when χ is not quadratic. Such a possible β for $L(s, \chi)$ is called a Siegel zero (cf. [39, Chapter 2]).

Siegel zeros are not on the vertical strip $\mathrm{Re}(s) = 1/2$ contrary to the generalized Riemann hypothesis. The Siegel zero of $L(s, \chi)$ are related to lower bounds of $L(1, \chi)$ as follows.

Theorem 2. ([26]) *For any non-trivial Dirichlet character χ modulo q, we have*

$$|L(1, \chi)| \gg \frac{1}{\log q}$$

unless $L(s, \chi)$ has a Siegel zero. Here the implied constant is independent of χ and q. In particular, the inequality as above holds if χ is not quadratic.

Existence of Siegel zeros is a deep problem in number theory as it influences a distribution of zeros of $L(s, \chi)$ and lower bounds of $L(1, \chi)$. We have not reached the non-existence of Siegel zeros for Dirichlet L-functions yet. As for quadratic characters, the best lower bound of $L(1, \chi)$ for quadratic characters χ is currently known as Siegel's theorem [44]. We refer to [16, Chapter 21] and [39, Chapter 2].

Theorem 3. (Siegel's theorem [44]) *For any $\epsilon > 0$, there exists an ineffective constant $C_\epsilon > 0$ such that the inequality*

$$L(1, \chi) \geq \frac{C_\epsilon}{q^\epsilon}$$

holds for any primitive quadratic character χ modulo q. Here recall that $L(1, \chi) > 0$ if χ is quadratic.

The primitivity of χ in Siegel's theorem can be easily dropped out by

$$L(1, \chi) \geq \{\prod_{p|q}(1 - p^{-1})\}L(1, \chi^*) \gg_\epsilon \frac{1}{q^\epsilon}L(1, \chi^*).$$

We remark that the constant C_ϵ is ineffective since it may depend on a possible Siegel zero of $\beta \in (1 - \epsilon, 1)$.

Siegel's theorem can be applied to the following two number theoretical problems. First, the class number h_K of an imaginary quadratic field K goes to infinity as the absolute value d_K of the discriminant of $K/\mathbb{Q}$ tends to infinity. Second,

the asymptotics $h_K \sim \frac{1}{2}\sqrt{d_K}$ holds as $d_K \to \infty$ keeping K imaginary quadratic. It is a spacial case of the Brauer-Siegel theorem (cf. [30]). By this asymptotics, there exist finitely many imaginary quadratic fields K such that $h_K = n$ for any given $n \in \mathbb{N}$.

Later, an effective version of Siegel's theorem was given by Tatuzawa [48] with the implied constant effective for any quadratic character χ except for at most one ineffective quadratic character. Although Tatuzawa's theorem was made explicit by [30] except for one quadratic character, the exceptional one is still ineffective.

Flaw 1 leads the following flaw:

Flaw 2 ([15, Theorem 3.1]) For a prime power $q = p^k$ set $G = (\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}$. Let $\mathbf{b}_j$ for $j \in G$ be the vector as in (3) and let $\{\mathbf{b}_j^\vee\}_{j\in G\smallsetminus\{1\}}$ be the dual basis of $\{\mathbf{b}_j\}_{j\in G\smallsetminus\{1\}}$. Then, we have $||\mathbf{b}_i^\vee|| = ||\mathbf{b}_j^\vee||$ for all i, j and

$$||\mathbf{b}_j^\vee||^2 \leq 2k(\#G)^{-1}(c\log f_\chi)^2 = \mathcal{O}(q^{-1}(\log q)^3), \tag{7}$$

where c is the implied constant in Flaw 1.

This upper bound of $||\mathbf{b}_i^\vee||^2$ is based on the equalities [15, Lemma 3.2 and Corollary 3.4] and the lower bound of $L(1,\chi)$ for $\chi \in \hat{G}$ in Flaw 1.

In Sections 6 and 7, we correct Flaws 1 and 2. As a consequence, this correction guarantees [15, Theorem 4.1].

6 Upper and Lower Bounds of $L(1,\chi)$; correction of Flaw 1

Let $q = p^k$ be a prime power and set $G = (\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}$. Then $\widehat{G}$ is identified with the group of all even Dirichlet characters modulo q. Set

$$E(q) := \frac{1}{\#G}\sum_{\chi\in\widehat{G}\smallsetminus\{1\}} \frac{4}{f_\chi|L(1,\chi)|^2}. \tag{8}$$

Proposition 1. ([15, Lemma 3.2 and Corollary 3.4]) *We have*

$$||\mathbf{b}_j^\vee||^2 = E(q).$$

In particular, $||\mathbf{b}_j^\vee||$ *is independent of* $j \in G \smallsetminus \{1\}$.

In this section, by using explicit estimates of $L(1,\chi)$ (Propositions 2, 3 and 4), we give explicitly computable estimates of $E(q)$, avoiding the use of Siegel's theorem (Theorem 3). Our estimates correct Flaw 1 and are better than the estimate (7) in Flaw 2. From our result, we can easily compute upper and lower bounds of $E(q)$ for the very short time. Experimental results will be shown in Sections 8.1.

6.1 Explicit Lower Bound of $L(1, \chi)$

We give explicit lower bounds of $L(1, \chi)$ for any non-trivial even Dirichlet characters χ modulo $q = p^k$. The evenness of χ is needed for attacks for SGP. First we show propositions for the case $p = 2$ and then two propositions for the case of $p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 4$.

Proposition 2 (Case $p = 2$). *Let $q = 2^k$ with $k \geq 3$. Let χ be a non-trivial character modulo q. If χ is not quadratic, we have*

$$|L(1, \chi)| \geq \frac{1}{10 \log(f_\chi/\pi)}.$$

If χ is even and quadratic, we have

$$L(1, \chi) = \frac{\log(1 + \sqrt{2})}{\sqrt{2}}.$$

Proof. As q is a prime power, we have $L(s, \chi) = L(s, \chi^*)$ by (2). Thus we may assume that χ is primitive. Then, the first assertion is obvious from [31, Corollary 2]. The second assertion is also obvious since χ is the unique even quadratic character with $f_\chi = 8$. □

For any odd prime number p, let χ_p be the primitive quadratic character modulo p. Then, there exists a unique quadratic character modulo p^k. Furthermore such a unique quadratic character is induced by χ_p. Notice that χ_p is even if and only if $p \equiv 1 \pmod 4$.

Proposition 3 (Case $p \equiv 3 \pmod 4$). *Let p be a prime number such that $p \equiv 3 \pmod 4$ and let $q = p^k$ with $k \geq 1$. Then, for any non-trivial even character χ modulo q, we have*

$$|L(1, \chi)| \geq \frac{1}{10 \log(f_\chi/\pi)}.$$

Proof. We note $L(s, \chi) = L(s, \chi^*)$ by (2). Since the unique quadratic character modulo p^k is odd, we obtain the assertion by [31, Corollary 2]. □

Proposition 4 (Case $p \equiv 1 \pmod 4$). *Let p be a prime number such that $p \equiv 1 \pmod 4$ and let $q = p^k$ with $k \geq 1$. Let χ be a non-trivial character modulo q. If χ is not quadratic, we have*

$$|L(1, \chi)| \geq \frac{1}{10 \log(f_\chi/\pi)}.$$

In particular, the esimtate above holds for any quadratic χ if $k_\chi \geq m(p)$ with

$$m(p) = \frac{1}{\log p} \left(\frac{1}{10 L(1, \chi_p)} + \log \pi \right),$$

where k_χ is the number such that $f_\chi = p^{k_\chi}$.

Furthermore, we have

$$L(1,\chi_p) \geq \frac{2}{\sqrt{p}} \log\left(\frac{\sqrt{p-4}+\sqrt{p}}{2}\right).$$

Proof. As we see $L(s,\chi) = L(s,\chi^*)$ by (2), the assertion is obvious from [31, Corollary 2] in the case where χ is not quadratic.

Consider the case $\chi = \chi_p$. Let h_p and ϵ_p be the class number and the fundamental unit of $\mathbb{Q}(\sqrt{p})$, respectively. By $h_p \geq 1$, $\epsilon_p \geq \frac{\sqrt{p-4}+\sqrt{p}}{2}$ and the class number formula for $\mathbb{Q}(\sqrt{p})$, we have the trivial lower bound

$$L(1,\chi_p) = \frac{2^2\, h_p \log \epsilon_p}{2\sqrt{p}} \geq \frac{2}{\sqrt{p}} \log\left(\frac{\sqrt{p-4}+\sqrt{p}}{2}\right).$$

This completes the proof. □

The second assertion of Proposition 4 is not conditional if $m(p) \leq 1$. Here is a table of $L(1,\chi_p)$ and $m(p)$ for $p \leq 100$.

p	$L(1,\chi_p)$	$m(p)$
5	$\frac{2}{\sqrt{5}} \log(\frac{1+\sqrt{5}}{2})$	0.856
13	$\frac{2}{\sqrt{13}} \log(\frac{3+\sqrt{13}}{2})$	0.505
17	$\frac{2}{\sqrt{17}} \log(4+\sqrt{17})$	0.439
29	$\frac{2}{\sqrt{29}} \log(\frac{5+\sqrt{29}}{2})$	0.388
37	$\frac{2}{\sqrt{37}} \log(6+\sqrt{37})$	0.351
41	$\frac{2}{\sqrt{41}} \log(32+5\sqrt{41})$	0.329
53	$\frac{2}{\sqrt{53}} \log(\frac{7+\sqrt{53}}{2})$	0.335
61	$\frac{2}{\sqrt{61}} \log(\frac{39+5\sqrt{61}}{2})$	0.304
73	$\frac{2}{\sqrt{73}} \log(1068+125\sqrt{73})$	0.280
89	$\frac{2}{\sqrt{89}} \log(500+53\sqrt{89})$	0.270
97	$\frac{2}{\sqrt{97}} \log(5604+569\sqrt{97})$	0.262

We can generally calculate the value $L(1,\chi_p)$ with the aid of the expression

$$L(1,\chi_p) = \frac{-1}{\sqrt{p}} \sum_{a=1}^{p-1} \chi_p(a) \log\left(2\sin\frac{\pi a}{p}\right)$$

if we determine all values of χ_p (cf. [16, p.9, (9)]).

6.2 Explicit Upper Bound of $L(1,\chi)$ (Flaw 1)

We have explicit upper bounds of $L(1,\chi)$ for non-trivial even Dirichlet characters χ. On the contrary to the lower bound, we can state the proposition for any prime power as follows.

Proposition 5. *Let χ be a non-trivial even Dirichlet character modulo a prime power $q = p^k$. When $p = 2$ and $k \geq 3$, we have*

$$|L(1,\chi)| \leq \frac{\log f_\chi + 2\log 2}{4}.$$

When $p = 3$, we have

$$|L(1,\chi)| \leq \begin{cases} \dfrac{1}{2}\log f_\chi & (k_\chi = 2), \\ \dfrac{\log f_\chi + 1.104888}{3} & (k_\chi \geq 3), \end{cases}$$

where k_χ is the number such that $f_\chi = p^{k_\chi}$. When $p \geq 5$, we have

$$|L(1,\chi)| \leq \frac{1}{2}\log f_\chi.$$

Proof. As we see $L(s,\chi) = L(s,\chi^*)$ by (2), the assertion for $p = 2$ follows from [42, Corollary 3] or [29, Corollary 1.2]. The assertion for $p = 3$ is given by [42, Corollary 1] and [17, Theorem 1.1]. Remark that $(\log 3^m)/3 + 0.368296 \leq (\log 3^m)/2$ if and only if $m \leq 2$. For $p \geq 5$, use [42, Corollary 1]. □

6.3 Summary of this section

Our contribution of this section is to prove correct upper and lower bounds of $L(1,\chi)$ for any non-trivial even Dirichlet characters χ, as in Propositions 2, 3, 4 and 5. Moreover, we remark that our upper and lower bounds of $L(1,\chi)$ are computable. As for lower bounds, we give the trivial lower bound of $L(1,\chi)$ for quadratic Dirichlet characters χ because of the ineffectiveness of Siegel's theorem. The upper and lower bounds of $L(1,\chi)$ as above will be used in Section 7.

7 Theoretical Estimation of $\|\mathbf{b}_j^\vee\|$; correction of Flaw 2

For any prime number p and $k \in \mathbb{N}$, set $q = p^k$ and $G = (\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}$. In this section we give theoretical upper and lower bounds of $||\mathbf{b}_j^\vee||^2 = E(q)$ (see Proposition 1). In order to divide the sum $E(q)$ in terms of the conductor f_χ, we count the number of even Dirichlet characters of conductor p^j.

In the case $p = 2$, since any element of $(\mathbb{Z}/2^k\mathbb{Z})^\times$ can be expressed uniquely as $5^a(-1)^b$ with $a \in \mathbb{Z}/2^{k-2}\mathbb{Z}$ and $b \in \mathbb{Z}/2\mathbb{Z}$, we have the isomorphism $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong (\mathbb{Z}/2^{k-2}\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$ for $k \geq 3$. In the group $(\mathbb{Z}/2^k\mathbb{Z})^\times$, the elements 5 and -1 are of order 2^{k-2} and 2, respectively.

Lemma 3 (Case $p = 2$). *For any $k \geq 3$, the number of characters of $\mathbb{Z}/2^{k-2}\mathbb{Z}$ of order 2^j is equal to $\varphi(2^j)$ for $1 \leq j \leq k-2$. The conductor of any even Dirichlet character modulo 2^k of order 2^j is equal to 2^{j+2} for $1 \leq j \leq k-2$.*

Proof. Let ψ be a character of $\mathbb{Z}/2^{k-2}\mathbb{Z}$ of order 2^j. Then ψ induces the isomorphism $(\mathbb{Z}/2^{k-2}\mathbb{Z})/\mathrm{Ker}(\psi) \cong \mathrm{Im}(\psi)$. The kernel of ψ depends only on j but not on ψ since a cyclic group is at most one subgroup with index m for a given $m \in \mathbb{N}$. From this, noting that the number of injections of $\mathbb{Z}/2^j\mathbb{Z}$ into $\mathbb{C}^\times$ is $\varphi(2^j)$, the number of characters of $\mathbb{Z}/2^{k-2}\mathbb{Z}$ of order 2^j is also equal to $\varphi(2^j)$.

Let χ be an even Dirichlet character of modulo 2^k of order 2^j. Then, we have the isomorphism $(\mathbb{Z}/2^k\mathbb{Z})^\times/\mathrm{Ker}(\chi) \cong \mathrm{Im}(\chi) \cong \mathbb{Z}/2^j\mathbb{Z}$, and hence χ is induced from a primitive even Dirichlet character of $(\mathbb{Z}/2^{j+2}\mathbb{Z})^\times \cong \mathbb{Z}/2^j\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This completes the proof. □

In the case where p is odd, we have the following.

Lemma 4 (Case $p \neq 2$). *Let p be an odd prime number. Let $k \in \mathbb{N}$ and j be integers such that $0 \leq j \leq k-1$ and let d be a positive divisor of $p-1$. Then, the number of Dirichlet characters modulo p^k of order dp^j is $\varphi(dp^j)$. The conductor of any Dirichlet character modulo p^k of order dp^j is equal to p^{j+1}, unless $(j,d) = (0,1)$.*

In particular, for $j \geq 1$, the number of even Dirichlet characters modulo p^k of conductor p^{j+1} is equal to $\frac{p-1}{2}\varphi(p^j)$. The number of even Dirichlet characters modulo p^k of conductor p is equal to $(p-3)/2$.

Proof. Note $(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{k-1}\mathbb{Z}$ and $G \cong \mathbb{Z}/\frac{p-1}{2}\mathbb{Z} \times \mathbb{Z}/p^{k-1}\mathbb{Z}$. Since $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic, the first assertion is proved in the same way as in Lemma 3. As for the second assertion for $j > 0$, the number of even Dirichlet characters modulo p^k of conductor p^j is equal to $\sum_{d|(p-1)/2} \varphi(d)\varphi(p^j) = \frac{p-1}{2}\varphi(p^j)$. Here we use $\sum_{d|n} \varphi(d) = n$ for any $n \in \mathbb{N}$. As the case $j = 0$ is proved in a similar fashion, we are done. □

Explicit upper bounds of $E(q)$ are given as follows.

Theorem 4. *1. When $p = 2$, we have*

$$E(q) \leq \frac{400}{2^{k+1}}\left[\frac{k(k+1)(2k+1)-84}{6}(\log 2)^2 - (\log 2)(\log \pi)\{k(k+1)-12\} + (\log \pi)^2(k-3)\right] + \frac{1}{2^{k-2}\{\log(1+\sqrt{2})\}^2}.$$

2. When $p \equiv 3 \pmod 4$, we have

$$E(q) \leq \frac{400(p-1)}{p^{k+1}}\left[\frac{k(k+1)(2k+1)-6}{6}(\log p)^2 - \{k(k+1)-2\}(\log p)(\log \pi) + (k-1)(\log \pi)^2\right] + \frac{400(p-3)}{(p-1)p^k}\{\log(p/\pi)\}^2.$$

3. When $p \equiv 1 \pmod 4$, we have

$$E(q) \le \frac{400(p-1)}{p^{k+1}}\Bigg[\frac{k(k+1)(2k+1)-6}{6}(\log p)^2 - \{k(k+1)-2\}(\log p)(\log \pi) + (k-1)(\log \pi)^2\Bigg] + \frac{400(p-5)}{(p-1)p^k}\{\log(p/\pi)\}^2 + \frac{8}{(p-1)p^k L(1,\chi_p)^2}.$$

and the following computable estimate

$$E(q) \le \frac{400(p-1)}{p^{k+1}}\Bigg[\frac{k(k+1)(2k+1)-6}{6}(\log p)^2 - \{k(k+1)-2\}(\log p)(\log \pi) + (k-1)(\log \pi)^2\Bigg] + \frac{400(p-5)}{(p-1)p^k}\{\log(p/\pi)\}^2 + \frac{2p}{(p-1)p^k}\frac{1}{\{\log(\frac{\sqrt{p-4}+\sqrt{p}}{2})\}^2}.$$

Proof. When $p = 2$ and $k \ge 3$, we have

$$E(q) \le \frac{1}{2^{k-2}}\left(\sum_{\chi \in \widehat{G}-\{1\}, \chi^2 \ne 1} \frac{4}{f_\chi |L(1,\chi)|^2} + \frac{4}{8\{\frac{1}{\sqrt{2}}\log(1+\sqrt{2})\}^2}\right).$$

Combining this with Lemma 3, the right-hand side is majorized by

$$\frac{1}{2^{k-2}}\sum_{j=2}^{k-2}\varphi(2^j) \times \frac{4}{2^{j+2}|L(1,\chi)|^2} + \frac{1}{2^{k-2}} \times \frac{4}{8\{\frac{1}{\sqrt{2}}\log(1+\sqrt{2})\}^2},$$

which is evaluated as

$$\frac{400}{2^{k+1}}\sum_{j=2}^{k-2}\{\log(2^{j+2}/\pi)\}^2 + \frac{1}{2^{k-2}\{\log(1+\sqrt{2})\}^2}$$

by Proposition 2. This completes the proof for $p = 2$.

The second, third and the fourth inequalities are proved in the same way as in the case of $p = 2$, using Propositions 3, 4 and Lemma 4 in place of Proposition 2 and Lemma 3; we note that there is no even quadratic Dirichlet character modulo p^k when $p \equiv 3 \pmod 4$. □

Explicit lower bounds of $E(q)$ are given as follows.

Theorem 5. *Let p be a prime number and $q = p^k$ with $k \in \mathbb{N}$. When $p = 2$ with $k \ge 3$, we have*

$$E(q) \ge \frac{8}{2^{k-2}(\log 2)^2}\sum_{j=1}^{k-2}\frac{1}{(j+4)^2}.$$

When $p = 3$, we have

$$E(q) \geq \frac{8}{3^{k-1}} \sum_{j=3}^{k} \frac{1}{(j \log 3 + 1.104888)^2} + \frac{8}{3^{k+1}(\log 3)^2}.$$

When $p \geq 5$, we have

$$E(q) \geq \frac{16}{p^k (\log p)^2} \left(\frac{p-1}{p} \sum_{j=2}^{k} \frac{1}{j^2} + \frac{p-3}{p-1} \right).$$

Proof. Consider the case $p = 2$. By Lemma 3 and Proposition 5, we have

$$E(q) \geq \frac{1}{2^{k-2}} \sum_{j=1}^{k-2} \varphi(2^j) \times \frac{16}{2^{j+2}(\log(2^{j+2}) + 2 \log 2)^2},$$

and hence the assertion for $p = 2$ follows. We obtain the assertions for odd p in a similar fashion by virtue of Proposition 5 and Lemma 4. □

The explicit estimate in Flaw 2 was no longer justified in [15]. However, our explicit estimates in Theorems 4 and 5 justifies the estimate $||\mathbf{b}_j^\vee||^2 = \mathcal{O}(q^{-1}(\log q)^3)$ in Flaw 2 by the following corollary.

Corollary 1. *Let $q = p^k$ be a prime power. Then, we have*

$$\frac{1}{q(\log p)^2} \ll E(q) \ll \frac{k(\log q)^2}{q},$$

where the implied constant is effective and independent of p and k.

Remark 2. Note that the implied constant in the upper bound as above is effective. By Corollary 1, we see that $E(q) \to 0$ as $k \to \infty$ for any prime number p. It suggests that the success condition of Algorithm 1 tends to hold as k is larger.

8 Table and Figure of $\|\mathbf{b}_j^\vee\|$ for $q = 2^k$

Since our estimate of $||\mathbf{b}_j^\vee||$ in Section 7 is effective for all k and prime numbers p, we can show examples of behaviors of $||\mathbf{b}_j^\vee||$. In this section, we consider the case $p = 2$.

8.1 Case of $q = 2^k$

By applying Proposition 1, Theorems 4 and 5 to the case $p = 2$, we have the upper and lower bounds of $\|\mathbf{b}_j^\vee\|$ as follows:

$$E_{\text{lower}}(k) \leq \sqrt{E(2^k)} = ||\mathbf{b}_j^\vee|| \leq E_{\text{upper}}(k).$$

Here, we set

$$E_{\mathrm{upper}}(k) = \left\{ \frac{400}{2^{k+1}} \left[\frac{k(k+1)(2k+1)-84}{6} (\log 2)^2 - (\log 2)(\log \pi)\{k(k+1)-12\} \right.\right.$$
$$\left.\left. + (\log \pi)^2 (k-3) \right] + \frac{1}{2^{k-2}\{\log(1+\sqrt{2})\}^2} \right\}^{1/2}$$

and

$$E_{\mathrm{lower}}(k) = \left\{ \frac{8}{2^{k-2}(\log 2)^2} \sum_{j=1}^{k-2} \frac{1}{(j+4)^2} \right\}^{1/2}.$$

Here are Table 1 and Figure 1 of $E_{\mathrm{lower}}(k)$, $\sqrt{E(2^k)}$ and $E_{\mathrm{upper}}(k)$ for $3 \leq k \leq 25$. To obtain values of $\sqrt{E(2^k)}$, we mainly used a computer with 2.80 GHz CPU (Intel(R) Core(TM) i7-3840QM) and 8GB memory. The OS is Windows 8.1 Pro 64 bit, implementing in Magma V2.19-7. "Time" in Table 1 means the time which it took to obtain the approximate value of $\sqrt{E(2^k)}$ for each $3 \leq k \leq 25$.

We note that, by applying Corollary 1 to the case $p = 2$, we have

$$\sqrt{\frac{1}{2^k}} \ll ||\mathbf{b}_j^\vee|| = \sqrt{E(2^k)} \ll \sqrt{\frac{k^3}{2^k}}.$$

It is easy to compute exact values of $E_{\mathrm{lower}}(k)$ and $E_{\mathrm{upper}}(k)$ contrary to approximate values of $\sqrt{E(2^k)}$. We calculated the approximate values of $\sqrt{E(2^k)}$ up to $k = 15$ because of the limitations of our computer performance. For example, it took ten days to compute the approximate value of $\sqrt{E(2^{15})}$ by our implementation in Magma. We stopped to draw values in Figure 1 for $k \geq 26$ since the difference $E_{\mathrm{upper}}(k) - E_{\mathrm{lower}}(k)$ is getting small for $k \geq 26$.

8.2 Feedback to Hardness of SGP

By Cauchy-Schwalz's inequality

$$|\langle \log(g), \mathbf{b}_j^\vee \rangle| \leq |\mathrm{Log}(g)| \; ||\mathbf{b}_j^\vee||,$$

the success of the attack deeply depends on the size of $\|\mathbf{b}_j^\vee\|$ as in Section 4.2. Now by Figure 1, we get that all $E_{\mathrm{lower}}(k)$, $||\mathbf{b}_j|| = \sqrt{E(2^k)}$ and $E_{\mathrm{upper}}(k)$ decrease monotoneously in $k \in [6, \infty)$. In particular, the upper bound $E_{\mathrm{upper}}(k)$ is rapidly decreasing, so is $\|\mathbf{b}_j^\vee\|$. Therefore, the success probability of Algorithm 1 for SGP is getting higher as $k \geq 6$ increases. We will show our experimental results in Section 9, which suggest that it is sufficient for the success of Algorithm 1 to take $k \geq 10$ for $p = 2$. The attack for the cryptosystems described in Section 3 is succeeded with probability being almost 1 for $k \geq 10$.

Table 1. Upper and lower bounds of $\|\mathbf{b}_j^\vee\|$, and actual value of $\|\mathbf{b}_j^\vee\|$ for $q = 2^k$ with $3 \leq k \leq 25$ (upper and lower bounds are given by $E_{\text{upper}}(k)$ and $E_{\text{lower}}(k)$ respectively, "Time" means that the time which it took to compute the actual value of $\|\mathbf{b}_j^\vee\|$)

k	$E_{\text{lower}}(k)$	$\|\|\mathbf{b}_j^\vee\|\| = \sqrt{E(2^k)}$	$E_{\text{upper}}(k)$	Time
3	0.577	0.802	0.802	0.000 sec.
4	0.531	0.709	5.78	0.000 sec.
5	0.428	0.568	7.10	0.000 sec.
6	0.329	0.445	7.32	0.000 sec.
7	0.246	0.342	6.95	0.015 sec.
8	0.181	0.261	6.27	0.219 sec.
9	0.132	0.197	5.46	1.312 sec.
10	0.0959	0.148	4.63	10.203 sec.
11	0.0692	0.110	3.85	74.918 sec.
12	0.0498	0.0815	3.15	555.170 sec.
13	0.0357	0.0601	2.54	7552.266 sec.
14	0.0256	0.0442	2.03	13.4583 hr.
15	0.0183	0.0324	1.61	310.137 hr.
16	0.0130	N/A	1.26	N/A
17	0.00930	N/A	0.985	N/A
18	0.00662	N/A	0.764	N/A
19	0.00471	N/A	0.589	N/A
20	0.00335	N/A	0.452	N/A
21	0.00238	N/A	0.345	N/A
22	0.00169	N/A	0.263	N/A
23	0.00120	N/A	0.199	N/A
24	0.000854	N/A	0.151	N/A
25	0.000606	N/A	0.114	N/A

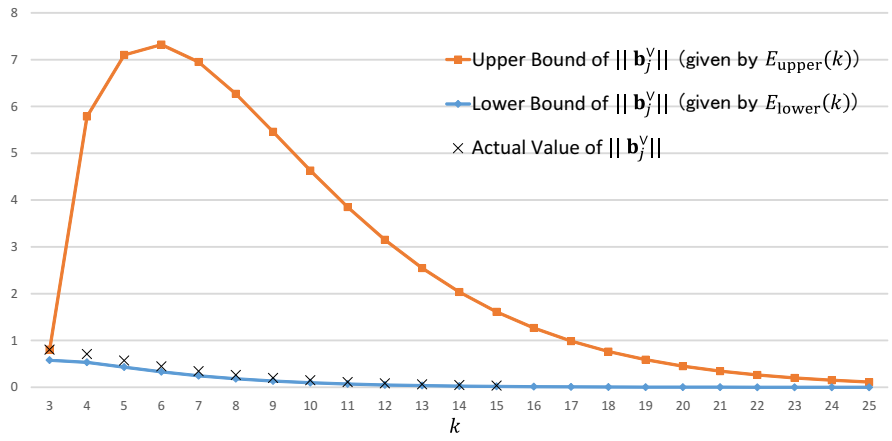

Fig. 1. Upper and lower bounds of $\|\mathbf{b}_j^\vee\|$, and actual value of $\|\mathbf{b}_j^\vee\|$ for $q = 2^k$ with $3 \leq k \leq 25$ (note that the size $\|\mathbf{b}_j^\vee\|$ is independent of $j \in G \setminus \{1\}$ by Proposition 1)

9 Experimental Verification

In this section, we give our experimental results to verify whether or not Algorithm 1 succeeds in recovering short elements g (or sufficiently small g's which can break cryptosystems described in Section 3).

We deal with the case of $q = 2^k$ since our targeted cryptosystems [20, 27, 47] are basically constructed over 2^k-th cyclotomic fields. From the viewpoint of the efficiency of a key generation, encoding and decoding process in cryptosystems of [20, 27, 47], we usually use k with $8 \leq k \leq 25$ in practice. Our theoretical bounds in Subsection 8 allow us to infer that the success probability of Algorithm 1 gets higher as k is greater than 6. Thus, we show our experimental results of the success probability for each k with $6 \leq k \leq 10$. Set $q := 2^k$, $n := 2^{k-1}$, $G := (\mathbb{Z}/q\mathbb{Z})^\times/\{\pm 1\}$ and $R := \mathbb{Z}[x]/(x^n + 1)$.

9.1 Parameter Setting for Our Experiments

In order to analyze the security of our targeted cryptosystems [20, 27, 47], we consider the following setting of the secret key g:

Choice of Distribution of Secret Key g We consider the case where g is randomly chosen from a discrete Gaussian distribution or a uniform distribution. Recall that g is chosen from a discrete Gaussian distribution in GGH and GGHLite schemes, and g is uniformly chosen from a finite subset of $\mathbb{Z}[x]$ in FHE scheme (see Section 3).

Size of Variance In GGH and GGHLite schemes, the spaces of secret keys, that is discrete Gaussian distributions of the mean 0, depend only on its variances and n. (By contrast, in FHE scheme, the space of secret keys depends only on n). Thus, we consider whether the success probability of Algorithm 1 depends on variances of discrete Gaussian distributions by several experiments.

Type of Principal Ideals $I = (g)$ **(Prime or Non-Prime)** In GGH, GGHLite and FHE schemes, a secret key $g \in R$ should be a prime element in R satisfying $R/(g) \simeq \mathbb{F}_p$ for some prime number p. However, as we will note below, this condition can be relaxed in the case of GGH and GGHLite. (In addition, it may be also possible that the primality condition of g can be relaxed for FHE). Thus, we consider whether the success probability of Algorithm 1 depends on the primality of secret keys.

9.2 Effects of Primality and Variance

First, we consider effects of the primality of secret keys and variances of discrete Gaussian distributions. We divide into the case of discrete Gaussian distributions and uniformly distributions.

Case of Discrete Gaussian Distribution

First, we consider the case where a secret key g is chosen from a discrete Gaussian distribution of the mean 0 and a given standard deviation σ, which is the space of secret keys of GGH and GGHLite schemes.

In these cryptosystems, a secret key g is a prime element in R such that $\mathcal{N}(g) := \mathrm{Res}(g'(x), x^n + 1)$ is a prime number, where g' is a polynomial in $\mathbb{Z}[x]$ representing g in R and $\mathrm{Res}(g'(x), x^n+1)$ is the resultant of g' and x^n+1. (This condition is not a necessary condition but a sufficient condition that g is a prime element in R). The primality of g was used in the proof of [20, Lemma 3 and Lemma 4]. In general, it is not efficient to obtain such g for large k, e.g. $k \geq 10$ ([47, Section 7], [3, Section 4]). Fortunately, it is proved in [3] that the primality of g is not necessary to prove these lemmas, and thus the condition on g can be relaxed. Note that in [3], it is suggested that the primality of g is still necessary for some cryptographic applications and it may be possible to attack by using the non-primality of g. Thus, we should experiment whether Algorithm 1 is one of such attacks.

Moreover, from Cramer et al.'s analysis for discrete Gaussian distributions [15, Lemma 5.6], the success probability of Algorithm 1 seems to depend heavily on variances of discrete Gaussian distributions. From this, we should also experiment for several variances.

Before we show our experimental results, we recall from Sections 2 and 4 that the canonical generators of the group of cyclotomic units are $b_j := \frac{\zeta_q^j - 1}{\zeta_q - 1}$ ($j \in G \smallsetminus \{1\}$). and that we set $\mathbf{b}_j := \mathrm{Log}(b_j)$ as in (3). The vectors $\mathbf{1} := (1, 1, \ldots, 1) \in \mathbb{R}^{\varphi(q)/2}$ and $\mathbf{b}_j$'s are $\mathbb{R}$-linearly independent, and thus they constitute an $\mathbb{R}$-basis of $\mathbb{R}^{\varphi(q)/2}$. Thus, for any $g \in R$, we have the following unique representation:

$$\mathrm{Log}(g) = a_1^{(g)}\mathbf{1} + \sum_{j \in G \smallsetminus \{1\}} a_j^{(g)} \mathbf{b}_j.$$

Note that we identify $g \in R$ with the element in $\mathbb{Z}[\zeta_q]$ by using the natural isomorphism $R \simeq \mathbb{Z}[\zeta_q]$ in the above equation. It is easy to see

$$\begin{cases} a_1^{(g)} = \frac{\langle \mathrm{Log}(g), \mathbf{1} \rangle}{\varphi(q)/2}, \\ a_j^{(g)} = \langle \mathrm{Log}(g), \mathbf{b}_j^\vee \rangle \quad (j \in G \smallsetminus \{1\}). \end{cases}$$

It implies that if we have $|a_j| < \frac{1}{2}$ for all $j \in G \smallsetminus \{1\}$, then we can compute g by Algorithm 1.

The procedure for our experiment is as follows:

1. Construct the following three finite subsets of R

   $$\mathrm{SK}_1 := \{g \in R \mid g \leftarrow D_{\mathbb{Z}^n, \sigma} \text{ and } \mathcal{N}(g) \text{ is a prime number}\},$$
   $$\mathrm{SK}_2 := \{g \in R \mid g \leftarrow D_{\mathbb{Z}^n, \sigma} \text{ and the ideal } (g) \text{ is not a prime ideal}\},$$
   $$\mathrm{SK}_3 := \{g \in R \mid g \leftarrow D_{\mathbb{Z}^n, \sigma}\},$$

   such that $\#\,\mathrm{SK}_i = 1000$ for $i = 1, 2, 3$.

Table 2. Values of $a_{\mathrm{ave}}(\mathrm{SK}_i)$ for $6 \leq k \leq 10$ and $i = 1, 2, 3$. The value $a_{\mathrm{ave}}(\mathrm{SK}_1)$ is shown on the left side and the value $a_{\mathrm{ave}}(\mathrm{SK}_2)$ is shown on the right side for $k = 6, 7, 8$. The value $a_{\mathrm{ave}}(\mathrm{SK}_3)$ is shown on the left side for $k = 9, 10$.

k \ $\log_{10}(\sigma)$	1	1.477	1.699	2	3	4
6	0.542 / 0.544	0.539 / 0.546	0.547 / 0.547	0.539 / 0.556	0.546 / 0.549	0.548 / 0.541
7	0.474 / 0.481	0.471 / 0.483	0.479 / 0.485	0.476 / 0.472	0.481 / 0.468	0.472 / 0.477
8	0.406 / 0.403	0.404 / 0.404	0.405 / 0.402	0.403 / 0.404	0.399 / 0.405	0.400 / 0.399
9	0.33 / -	0.328 / -	0.331 / -	0.331/ -	0.33 / -	0.32 / 0.33
10	0.267 / -	0.265 / -	0.268 / -	0.268 / -	0.267 / -	0.268 / -

2. Compute $\mathbf{b}_j$ and $\mathbf{b}_j^{\vee}$ for $j \in G \setminus \{1\}$, where $G := (\mathbb{Z}/q\mathbb{Z})^{\times}/\{\pm 1\}$.
3. Compute $a_j^{(g_i)}$ satisfying $\mathrm{Log}(g_i) = a_1^{(g_i)}\mathbf{1} + \sum_{j \in G \setminus \{1\}} a_j^{(g_i)}\mathbf{b}_j$ for $j \in G \setminus \{1\}$, $g_1 \in \mathrm{SK}_1$, $g_2 \in \mathrm{SK}_2$ and $g_3 \in \mathrm{SK}_3$.

We use the same computer as in Section 8. We use the discrete Gaussian distribution sampler [2], which is implemented in Sage by Martin Albrecht (also see [23]). We implemented in Sage for the first step and implemented in Magma V2.19-7 for the second and the third steps.

We put

$$a_{\max}^{(g_i)} := \max\{|a_j^{(g_i)}| \mid j \in G \setminus \{1\}\} \quad g_i \in \mathrm{SK}_i,$$
$$a_{\mathrm{ave}}(\mathrm{SK}_i) := \frac{1}{\#\,\mathrm{SK}_i} \sum_{g_i \in \mathrm{SK}_i} \left| a_{\max}^{(g_i)} \right|,$$

for $i = 1, 2, 3$. When $i = 1$ and $i = 2$, we computed the value of $a_{\mathrm{ave}}(\mathrm{SK}_i)$ only for $k = 6, 7, 8$, because of the difficulty of choosing many prime elements $g \in R$. In addition, we computed the value of $a_{\mathrm{ave}}(\mathrm{SK}_3)$ only for $k = 9, 10$. In Table 2, we showed our experimental results on the value of $a_{\mathrm{ave}}(\mathrm{SK}_i)$ for $i = 1, 2, 3$.

From Table 2, we can infer that the difficulty of SGP is independent of the primality of secret keys and variances of discrete Gaussian distributions since the difference of $a_{\mathrm{ave}}(\mathrm{SK}_1)$ is almost the same as $a_{\mathrm{ave}}(\mathrm{SK}_2)$ and $a_{\mathrm{ave}}(\mathrm{SK}_3)$ for each k and σ. In other words, the value of $a_{\mathrm{ave}}(\mathrm{SK}_i)$ seems to depend only on k for $i = 1, 2, 3$. Thus, we conclude that the security of cryptosystems constructed over 2^k-th cyclotomic fields by using short generators such as GGH and GGHLite schemes do not depend on the primality of their secret keys and variances of their spaces of secret keys. Our observation above also implies that we can use a non-prime element g as secret keys in those cryptosystems except for some applications.

Case of Uniform Distribution

Next, we consider the case where the secret keys are chosen uniformly from a finite subset of $\mathbb{Z}[x]$ described below, since this is the same as the key generation

Table 3. Values of $a_{\mathrm{ave}}(\mathrm{SK}_i)$ for $6 \leq k \leq 10$ and $i = 1, 2, 3$. The value $a_{\mathrm{ave}}(\mathrm{SK}_1)$ is shown on the left side and the value $a_{\mathrm{ave}}(\mathrm{SK}_2)$ is shown on the right side for $k = 6, 7, 8$.

k	$a_{\mathrm{ave}}(\mathrm{SK}_1)$ / $a_{\mathrm{ave}}(\mathrm{SK}_2)$	$a_{\mathrm{ave}}(\mathrm{SK})$
6	0.229 / 0.224	-
7	0.177 / 0.172	-
8	0.132 / 0.134	-
9	-	0.334
10	-	0.267

process of FHE. Set $N := 2^n$ and $\eta := 2^{\sqrt{N}}$. We recall that in [47], a secret key g is uniformly chosen from the set

$$B(\eta) := \left\{ f = 2\left(\sum_{i=0}^{N-1} a_i x^i\right) + 1 \in \mathbb{Z}[x] \;\middle|\; |a_i| \leq \eta/2 \ (i = 1, 2, \ldots, N-1) \right\}$$

until $\mathcal{N}(g \bmod (x^n + 1))$ becomes a prime number. In our experiment, we use this method of [47].

In this case, we also experiment whether the primality of g affects the success probability of Algorithm 1. Let SK_1 be the set of polynomials chosen by the above method. Let SK_2 be the set of polynomials f uniformly chosen from $B(\eta)$ such that $f \bmod (x^n+1)$ does not generate a prime ideal for $k = 6, 7, 8$. We also choose $g \in B(\eta)$ uniformly without testing the primality of g for $k = 9, 10$. Let SK_3 be the set of such polynomials. We choose g untill $\#\,\mathrm{SK}_1 = \#\,\mathrm{SK}_2 = \#\,\mathrm{SK}_3 = 1000$.

For $i = 1, 2, 3$, set $a_{\mathrm{ave}}(\mathrm{SK}_i)$ as above. In Table 3, we showed our experimental results on the value of $a_{\mathrm{ave}}(\mathrm{SK}_i)$ for $i = 1, 2, 3$.

From Table 3, we conclude that Algorithm 1 is also effective for FHE scheme as in the case of GGH and GGHLite schemes because of the same reason as in the case of discrete Gaussian distributions.

9.3 Success Probability of Algorithm 1

In the last of this section, we show our experimental results on the experimental success probability of Algorithm 1 for $k = 6, 8, 10$ and $\sigma = 10$ in both cases of discrete Gaussian distributions and uniformly distributions, where σ is the standard deviation of a discrete Gaussian distribution. We experimented 1000 times for each parameter. In Figures 2 and 3, we show the value of $\max\{|\langle \mathrm{Log}(g), \mathbf{b}_j^{\vee} \rangle| \mid j \in G \setminus \{1\}\}$ for each g.

From 2 and 3, we infer that Algorithm 1 will succeed in recovering secret keys of FHE, GGH and GGHLite schemes with about 50 % (resp. 85 % and 100 %) probability when $k = 6$ (resp. $k = 8$ and $k = 10$). In other words, the number of successes increases, as k is larger. We believe that it is true for $k > 10$. Thus, our experimental results suggest that the security of FHE, GGH and GGHLite schemes depend heavily on the difficulty of the principal ideal problem.

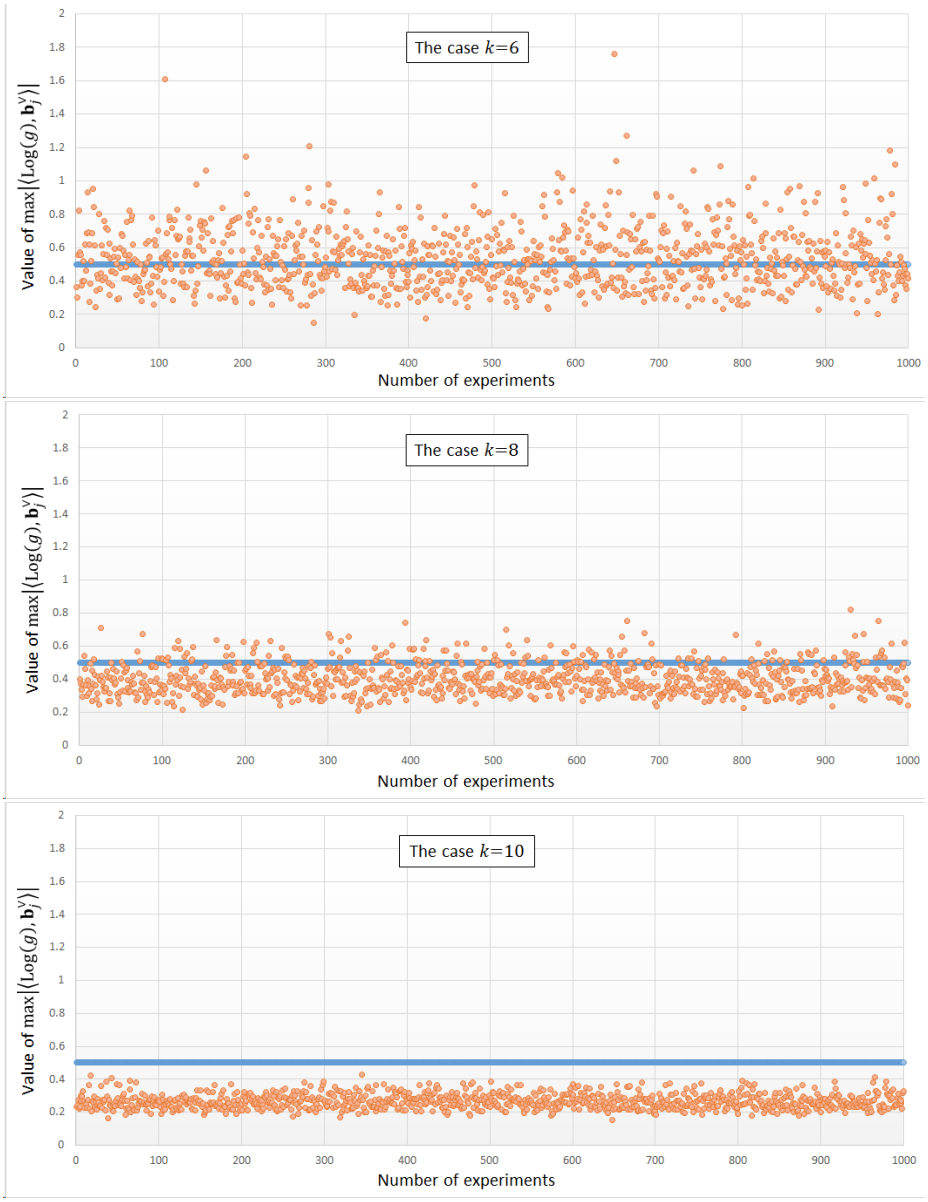

Fig. 2. Values of $\max_{j \in G \setminus \{1\}} |\langle \mathrm{Log}(g), \mathbf{b}_j^\vee \rangle|$ for $q = 2^k$ with $k = 6, 8, 10$. Note that Cramer et al.'s attack for SGP is succeeded (resp. failed) if $\max |\langle \mathrm{Log}(g), \mathbf{b}_j^\vee \rangle| \leq \frac{1}{2}$ (resp. $> \frac{1}{2}$). For each k, the secret key g is randomly generated by a discrete Gaussian distribution at $1,000$ times

Fig. 3. Same as Figure 2, but g is generated by a uniformly random distribution

10 Conclusion

In this paper, we analyzed the security of cryptosystems using short generators over ideal lattices against Cramer et al.'s attack. We corrected the flaws in Cramer et al.'s main result which is important to verify their attack, and thus we first gave theoretical evidence verifying their attack. We also gave various experimental results. Our theoretical and experimental results suggest that breaking those cryptosystems can be reduced to solving the principal ideal problem, which is considered to be solved in quantum polynomial time.

References

1. M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence", *Proceedings of the 29th Annual ACM Symposium on Theory of Computing–STOC 1997*, ACM, pp. 284–293, 1997.
2. M. Albrecht, *Discrete Gaussian Samplers over Lattices*, available at `http://doc.sagemath.org/html/en/reference/stats/sage/stats/distributions/discrete\_gaussian\_lattice.html`.
3. M.R. Albrecht, C. Cocis, F. Laguillaumie and A. Langlois, "Implementing candidate graded encoding schemes from ideal lattices", *IACR Cryptology ePrint Archive*, 2014/928, 2014.
4. L. Babai, On Lovász lattice reduction and the nearest lattice point problem, *Combinatorica*, **6**(1), pp. 1–13, 1986. (Preliminary version in STACS 1985)
5. H. Bauer, Numeriche Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper, *J. Number Theory* **1**, pp. 161–162, 1969.
6. D. Bernstein, "A subfield-logarithm attack against ideal lattices", 2014, available at `http://blog.cr.yp.to/20140213-ideal.html`.
7. J.-F. Biasse and C. Fieker, Subexponential class group and unit group computation in large degree number fields, *LMS J. Comput. Math.* **17**(A), pp. 385–403, 2014.
8. J.-F. Biasse, Subexponential time relations in the class group of large degree number fields, *Adv. Math. Commun.*, **8**(4), pp. 407–425, 2014.
9. J.-F. Biasse, "Finding a generator of a principal ideal", Dagstuhl Seminar, Quantum Cryptanalysis, 2015. (program is available at `http://www.dagstuhl.de/de/programm/kalender/semhp/?semnr=15371`)
10. J.-F. Biasse, "A fast algorithm for finding a short generator of a principal ideal of $\mathbb{Q}(\zeta_{2^n})$", *arXiv preprint arXiv:1503.03107*, 2015, available at `http://arxiv.org/pdf/1503.03107v1.pdf`.
11. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.
12. P. Campbell, M. Groves, and D. Shepherd, "Soliloquy: A cautionary tale", *ETSI 2nd Quantum-Safe Crypto Workshop*, 2014, available at `S07\_Groves\_Annex.pdf`.
13. J.H. Cheon and C. Lee, "Cryptanalysis of the multilinear map on the ideal lattices", *IACR Cryptology ePrint Archive*, 2015/461, 2015.
14. H. Cohn, A numerical study of Weber's real class number calculation I, *Numer. Math.* **2** 347–362, 1960.
15. R. Cramer, L. Ducas, C. Peikert and O. Regev, "Recovering short generators of principal ideals in cyclotomic rings", *IACR Cryptology ePrint Archive*, 2015/313, 2015.

16. H. Davenport, *Multiplicative Number Theory*, Graduate Texts in Mathematics **74**, Springer-Verlag, New York, 2000.
17. S.S. Eddin and D.J. Platt, Explicit upper bounds for $|L(1,\chi)|$ when $\chi(3) = 0$, *Colloq. Math.* **133**(1), pp. 23–34, 2013.
18. T. Fukuda and K. Komatsu, Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, II, *J. Théor. Nombres Bordeaux* **22** (2), pp. 359–368, 2010.
19. T. Fukuda and K. Komatsu, Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, III, *Int. J. Number Theory* 7, no 06, pp. 1627–1635, 2011.
20. S. Garg, C. Gentry and S. Halevi, "Candidate multilinear maps from ideal lattices". *Advances in Cryptology–EUROCRYPT 2013*, Springer LNCS 7881, pp. 1–17, 2013.
21. C. Gentry, "Fully homomorphic encryption using ideal lattices", *Proceedings of the 2009 ACM International Symposium on Theory of Computing–STOC 2009*, ACM, pp. 169–178, 2009.
22. C. Gentry and S. Halevi, "Implementing Gentry's fully homomorphic encryption", *Advances in Cryptology–EUROCRYPT 2011*, Springer LNCS 6632, pp. 129–148, 2011.
23. C. Gentry, C. Peikert and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions", *Proceedings of the 40th Annual ACM Symposium on Theory of Computing–STOC 2008*, ACM, pp. 197–206, 2008.
24. S. Hallgren, "Fast quantum algorithms for computing the unit group and class group of a number field", *Proceedings of the 37th Annual ACM Symposium on Theory of Computing–STOC 2005*, ACM, pp. 468–474, 2005.
25. K. Horie, Certain primary components of the ideal class group pf the $\mathbb{Z}_2$-extension over the rationals, *Tohoku Math. J.* **59**, pp. 259–291, 2007.
26. E. Landau, Über Dirichletsche reihen mit komplexen charakteren, *Journal für die reine und angewandte Mathematik*, no. 157, pp. 26–32, 1927.
27. A. Langlois, D. Stehlé and R. Steinfeld, "GGHLite: More efficient multilinear maps from ideal lattices", *Advances in Cryptology–EUROCRYPT 2014*, Springer LNCS 8441, pp. 239–256, 2014.
28. F. J. van der Linden, Class number computations of real abelian number fields, *Math. Comput.* **39**, pp. 693–707, 1982.
29. S. Louboutin, Majorations explicites de $|L(1,\chi)|$ (quatrième partie), *C. R. Acad. Sci. Paris* **334**, pp. 625–628, 2002.
30. S. Louboutin, Simple proofs of the Siegel-Tatuzawa and Brauer-Siegel theorems, *Colloq. Math.* **108**, pp. 277–283, 2007.
31. S. Louboutin, An explicit lower bound on moduli of Dirichlet L-functions at $s = 1$, *J. Ramanujan Math Soc.* **30**(1), pp. 101–113, 2015.
32. V. Lyubashevsky, "Lattice-based identification schemes secure under active attacks", *Public Key Cryptography–PKC 2008*, Springer LNCS 4939, pp. 162–179, 2008.
33. V. Lyubashevsky and D. Micciancio, "Generalized compact knapsacks are collision resistant", *Automata, Languages and Programming–ICALP 2006*, Springer LNCS 4052, pp. 144–155, 2006.
34. V. Lyubashevsky and D. Micciancio, "Asymptotically efficient lattice-based digital signatures", In *Theory of Cryptography*, Springer LNCS 4948, pp. 37–54, 2008.
35. V. Lyubashevsky, C. Peikert and O. Regev, On ideal lattices and learning with errors over rings, *Journal of the ACM* **60**(3), no. 43, 2013.
36. J.M. Masley, Class numbers of real cyclic number fields with small conductor, *Compos. Math.* **37** pp. 297–319.
37. D. Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient oneway functions, *Computational Complexity* **16**(4), pp. 365–411, 2007.

38. J. C. Miller, *Class numbers of totally real fields and applications to the Weber class number problem*, to appear in Acta Arith.Acta Arith. **164**, no. 4, pp. 381–397, 2014.
39. G. Molteni, L-functions: Siegel-type theorems and structure theorems, Ph.D. thesis, University of Milan, Milan, 1999.
40. J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften **322**, Springer-Verlag Berlin Heidelberg, 1999.
41. C. Peikert and A. Rosen, "Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices", *Theory of Cryptography–TCC 2006*, Springer LNCS 3876, pp. 145–166, 2006.
42. O. Ramaré, Approximate formulae for $L(1, \chi)$, *Acta Arith.* **100**, pp. 245–266, 2001.
43. J. Schank, "LogCVP, Pari implementation of CVP in Log $\mathbb{Z}[\zeta_{2^n}]^*$", 2015, available at `https://github.com/jschanck-si/logcvp`.
44. C.L. Siegel, Über die Classenzahl quadratischer Zahlkörper, *Acta Arith.* **1**, pp. 83–86, 1935.
45. D. Stehlé and R. Steinfeld, "Making NTRU as secure as worst-case problems over ideal lattices", *Advances in Cryptology–EUROCRYPT 2011*, Springer LNCS 6632, pp. 27–47, 2011.
46. D. Stehlé, R. Steinfeld, K. Tanaka and K. Xagawa, "Efficient public key encryption based on ideal lattices", *Advances in Cryptology–ASIACRYPT 2009*, Springer LNCS 5912, pp. 617–635, 2009.
47. N.P. Smart and F. Vercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes", *Public Key Cryptography–PKC 2010*, Springer LNCS 6056, pp. 420–443, 2010.
48. T. Tatuzawa, On a theorem of Siegel, *Japanese J. Math.* **21**, pp. 163–178, 1951.
49. L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83**, Springer New York, 1997.
50. H. Weber, Theorie der Abel'schen Zahlkörper, *Acta Math.* **8**, pp. 193–263, 1886.

A Weber's class number problem

In this appendix, we give some known results on Weber's class number problem. Let $\zeta_q \in \mathbb{C}$ be a q-th primitive root of unity for $q \in \mathbb{N}$. Then $\mathbb{Q}(\zeta_q + \overline{\zeta_q})$ is the unique maximal real subfield of the q-th cyclotomic field $\mathbb{Q}(\zeta_q)$. The class number $h^+(q)$ of $\mathbb{Q}(\zeta_q + \overline{\zeta_q})$ is one of active themes in number theory, inspired by Weber. He proposed the so-called Weber's class number problem that $h^+(2^n)$ equals 1 for all $n \in \mathbb{N}$. This problem is related to Cramer et al.'s attack for SGP as we saw $[\Lambda : \mathrm{Log}(C)] = h^+(2^k)$ in Remark 1. In [50], Weber proved that $h^+(2^3) = h^+(2^4) = h^+(2^5) = 1$ and that $h^+(2^n)$ is odd for all $n \in \mathbb{N}$.

Theorem 6. (Cohn [14]) *Let $\zeta_{2^n} \in \mathbb{C}$ be a 2^n-th primitive root of unity and $K^+ := \mathbb{Q}(\zeta_{2^n} + \overline{\zeta_{2^n}})$. We denote the class number of K^+ by $h^+(2^n)$. We have the following:*

(1) $h^+(2^6) = 1$ *or* $1601 \leq h^+(2^6) \leq 83921$. *In the latter case, $h^+(2^6)$ is a prime number.*
(2) $h^+(2^7) = 1$ *or* $1601 \leq h^+(2^7)$.
(3) $h^+(2^8) = 1$ *or* $1409 \leq h^+(2^8)$.

(4) *For any* $n \geq 9$, $h^+(2^n) = 1$ *or* $257 \leq h^+(2^n)$.

Theorem 7. (Bauer [5]) *Let* p *be a prime number. For any* $n \in \mathbb{N}$ *such that* $p^n < 53$, *we have* $h^+(p^n) = 1$. *We have also* $h^+(2^6) = 1$ *although* 2^6 *is greater than* 53.

Theorem 8. (Masley [36]) *Suppose that* $p^n < 70$. *Then we have* $h^+(p^n) = 1$. *In particular, we have* $h^+(2^6) = 1$.

Theorem 9. (Linden [28]) *Let* K *be a totally real abelian extension of* $\mathbb{Q}$. *Suppose that the conductor* f *of* K *is a prime power. We denote the class number* K *by* h_K. *Let* H_K *be the Hilbert class field of* K, *i.e. the maximal unramified abelian extension of* K. *Then, we have the following:*

(1) *If* $\varphi(f) \leq 66$, *then* $h_K = 1$.
(2) *Assume the generalized Riemman hypothesis (GRH) for the Dedekind zeta function of* H_K. *Then,*

$$h_K = \begin{cases} 4 \text{ if } f = 163, \\ 1 \text{ if } f \neq 163 \text{ and } \varphi(f) \leq 162. \end{cases}$$

In particular, we have $h^+(2^7) = 1$ by Theorem 9 (1) since the conductor of $\mathbb{Q}(\zeta_{2^7} + \overline{\zeta_{2^7}})$ is $\varphi(2^7) = 2^6 < 66$. Moreover, $h^+(2^8) = 1$ holds true by virtue of Theorem 9 (2) under GRH for the Dedekind zeta function of H_K with $K = \mathbb{Q}(\zeta_{2^8} + \overline{\zeta_{2^8}})$.

Theorem 10. (Miller [38]) *We have* $h^+(2^8) = 1$. *Moreover, we have* $h^+(2^9) = 1$ *under GRH for the Dedekind zeta function of* H_K *with* $K = \mathbb{Q}(\zeta_{2^9} + \overline{\zeta_{2^9}})$.

By all theorems described as above, it is well-known that $h^+(2^n) = 1$ holds true only for $n \leq 8$.

The three results below are concerned with the divisibility of $h^+(2^n)$.

Theorem 11. (Horie [25]) *If a prime number* ℓ *satisfies* $\ell \equiv \pm 5$ *(mod* 8*), then* $\ell \nmid h^+(2^n)$.

Theorem 12. (Fukuda, Komatsu [18]) *If a prime number* ℓ *satisfies* $\ell \equiv \pm 9$ *(mod* 16*), then* $\ell \nmid h^+(2^n)$. *Moreover,* $\ell \nmid h^+(2^n)$ *holds for all prime numbers* $\ell < 1.2 \times 10^8$.

Theorem 13. (Fukuda, Komatsu [19]) *If a prime number* ℓ *satisfies* $\ell \equiv \pm 1$ *(mod* 32*), then* $\ell \nmid h^+(2^n)$. *Moreover,* $\ell \nmid h^+(2^n)$ *holds for all prime numbers* $\ell < 10^9$.

All results as above give us that $h^+(2^n)$ is huge for $n \geq 9$ unless $h^+(2^n) = 1$.