Attacks against search Poly-LWE

Momonari Kudo*

December 15, 2016

Abstract

The Ring-LWE (RLWE) problem is expected to be a computationally-hard problem even with quantum algorithms. The Poly-LWE (PLWE) problem is closely related to the RLWE problem, and in practice a security base for various recently-proposed cryptosystems. In 2014, Eisentraeger et al. proposed attacks against the *decision*-variant of the PLWE problem (and in 2015, Elias et al. precisely described and extended their attacks to be applied for that of the RLWE problem). Their attacks against the decision-PLWE problem succeed with sufficiently high probability in polynomial time under certain assumptions, one of which is that the defining polynomial of the PLWE instance *splits completely* over the ground field.

In this paper, we present polynomial-time attacks against the *search*-variant of the PLWE problem. Our attacks are viewed as search-case variants of the previous attacks, but can deal with more general cases where the defining polynomial of the PLWE problem does *not split completely* over the ground field.

Key words— Ring-LWE, Poly-LWE, finite field

1 Introduction

Lattice-based cryptography now plays a central role in quantum-resistant cryptography. In lattice theory, there are many computational problems considered to be hard even with quantum algorithms, and they are bases for the security of recently-proposed encryption schemes. The Ring-LWE (RLWE) problem is well-known to be such a problem, and it is concerned with many hard problems in lattice theory, see e.g., [3], [10], [11] and [12].

The Poly-LWE (PLWE) problem was introduced in [4], and it is known to be the polynomial version of the RLWE problem. Consider a PLWE instance (n, f, q, ℓ, χ), where n and ℓ are positive integers, f a monic irreducible polynomial in $\mathbb{Z}[x]$ of degree n, q a rational prime, and χ an error distribution on $\mathbb{Z}$. Let $P := \mathbb{Z}[x]/f\mathbb{Z}[x]$, $P_q := P/qP$, and $\overline{h} \in P_q$ denote its equivalence class for $h \in P$. For a fixed secret element $\overline{s} \in P_q$ with $s \in P$, the PLWE problem setting involves ℓ PLWE samples $(\overline{a_i}, \overline{a_i s + e_i}) \in P_q \times P_q$ for $1 \leq i \leq \ell$, where $\overline{a_i}$ is uniformly chosen from P_q at random and $\overline{e_i}$ sampled from χ for every i. Here two questions are asked in the PLWE problem; the *decision*-variant of PLWE is to distinguish whether a tuple $(\overline{b_1}, \ldots, \overline{b_\ell})$ is obtained from PLWE samples with $\overline{b_i} = \overline{a_i s + e_i}$ for $1 \leq i \leq \ell$, or uniformly at random from P_q^ℓ. The *search*-variant of PLWE is to recover the secret element $\overline{s}$ from PLWE samples.

*1 Graduate School of Mathematics, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka-shi, Fukuoka, 19-0373, Japan. m-kudo [atmark] math.kyushu-u.ac.jp, *2 Fujitsu Laboratories of America, Inc., 1240 E. Arques Ave., Sunnyvale, CA 94085, USA.

The PLWE problem is viewed as a special case of the RLWE problem, but in practice a security base for various cryptosystems, e.g., [2], [4], and [9]. The hardness of the PLWE problem is reduced to that of the RLWE problem. Specifically the PLWE problem is known to be as hard as the RLWE problem for 2-power cyclotomic number fields, see [5] and [10].

1.1 Existing Attacks against PLWE and Their Analysis

In recent years, Eisentraeger et al. proposed in [6] attacks for the *decision*-variant of the PLWE problem under certain assumptions (cf. in [7], extended versions of their attacks for RLWE are proposed). They also gave a sequence of reductions between the search and decision variants of the RLWE and the PLWE problems. For number fields satisfying their assumptions, their attacks on decision-PLWE efficiently work by determining the value of the secret polynomial evaluated at a root of f modulo q. Their analysis characterized insecure classes of number fields used in the RLWE and the PLWE problems. Specifically, using polynomials splitting completely over the ground field $\mathbb{F}_q$ as f was proved to be vulnerable for large q. For such a polynomial f with some conditions on its roots, they showed that one of their attack is successful with high probability, and terminates in time $\widetilde{O}(\ell q + nq)$. (As we will show in this paper, even using polynomials with at most one root in $\mathbb{F}_q$ is no longer secure for the decision case.)

1.2 Our Contributions

Using search-decision reductions in [6], [7], one can attack to the search-PLWE with their decision-case attacks. In this paper, we consider solving *directly* the *search*-PLWE problem, where the word *directly* means not using any reduction. As pointed out in [7], their method of determining the value of the secret polynomial provides one piece of information about the secret: $g = s(\overline{\alpha})$ for some $\overline{\alpha} \in \mathbb{F}_q$. From this, we first construct a search-case attack as a variant of their decision-case attacks under the same assumption as in [6] and [7]. In our first attack, we combine their method with linear algebra techniques. We also show that the assumption may not be reasonable for the search-case attack; for a given f, the number of q that satisfy the assumption is not many in the sense of *density* of such primes. From this, we give a generalized attack, which can deal with cases where f does *not necessarily split completely*. Our generalization method is based on the theory of finite field, and our extended attack terminates in polynomial time when f has only low degree-irreducible factors in $\mathbb{F}_q[x]$ (e.g., degree 2 or 3).

Our method in the generalized attack is applicable for the decision-variant, which implies that our attack framework is also viewed as a generalization of the previous decision-case attacks in [6] and [7]. With our attack framework, new insecure classes of defining polynomials f and parameters q in the PLWE problem are characterized, which shall be a valuable information to desire more secure cryptosytems.

Organization of This Paper The rest of this paper is organized as follows: In Section 2, we give a brief review on the definition of the PLWE problem and existing attacks against its decision-variant. Section 3 gives search-case variants of the decision-case attacks. In Section 4, we extend the attacks so as to deal with more general cases. In Section 5, we conclude this work.

Notation Given elements $f_1, \ldots, f_t$ in a commutative ring R, we denote by $\langle f_1, \ldots, f_t \rangle_R$ (or simply $\langle f_1, \ldots, f_t \rangle$) the ideal in R generated by $f_1, \ldots, f_t$. Specifically for one element f, the ideal $\langle f \rangle$ is

denoted by fR. Let $\mathbb{Z}$ and $\mathbb{Q}$ denote the ring of rational integers and the field of rational numbers, respectively. For a power of a prime q, let $\mathbb{F}_q$ denote the field of q elements. Throughout this paper, we take a representative of an element in the prime field $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ as an integer in $(-q/2, q/2]$. For an integer α and a prime q, we denote by $[\alpha] \in \mathbb{F}_q$ its equivalence class modulo q.

2 Preliminaries

2.1 Definition(s) of the Poly-LWE problem

Let f be a monic polynomial in $\mathbb{Z}[x]$ of degree $n \geq 1$. Suppose that f is irreducible over $\mathbb{Z}$, and put $P := \mathbb{Z}[x]/\langle f \rangle$. Let q be a rational prime and $P_q := P/qP$. The quotient ring P_q is isomorphic to $\mathbb{F}_q[x]/\langle f^{(q)} \rangle$, where $f^{(q)}$ denotes the polynomial in $\mathbb{F}_q[x]$ given by the reduction modulo q for f. Indeed, we have

$$P_q := P/qP = (\mathbb{Z}[x]/\langle f \rangle)/(\langle q, f \rangle/\langle f \rangle) \cong (\mathbb{Z}[x]/\langle q \rangle)/(\langle q, f \rangle/\langle q \rangle) \cong \mathbb{F}_q[x]/\langle f^{(q)} \rangle.$$

In what follows, we identify P_q with $\mathbb{F}_q[x]/\langle f^{(q)} \rangle$. For $h \in \mathbb{F}_q[x]$, we denote by $\overline{h} = h + \langle f^{(q)} \rangle$ its equivalence class. Each element in P_q is uniquely written of the form

$$c_{n-1}\overline{x}^{n-1} + \cdots + c_1\overline{x} + c_0 \tag{2.1.1}$$

for $c_i \in \mathbb{F}_q$. Note that for $c \in \mathbb{F}_q$, we can identify c with $\overline{c} \in P_q$ via the canonical injection $\mathbb{F}_q \hookrightarrow \mathbb{F}_q[x]/\langle f^{(q)} \rangle$. With this fact, we give an element in P_q as an element in $\mathbb{F}_q[x]/\langle f^{(q)} \rangle$ of the form (2.1.1).

Remark 2.1.1. As mentioned above, P_q is an $\mathbb{F}_q$-vector space of dimension n. Specifically, if $f^{(q)}$ has no double root and splits completely in $\mathbb{F}_q[x]$, say $f^{(q)}(x) = \Pi_{i=1}^{n}(x - [\alpha_i])$ for some distinct elements $[\alpha_i] \in \mathbb{F}_q$ with $\alpha_i \in (-q/2, q/2] \cap \mathbb{Z}$, then we have

$$\mathbb{F}_q[x]/\langle f^{(q)} \rangle \cong \mathbb{F}_q[x]/\langle x - [\alpha_1] \rangle \oplus \cdots \oplus \mathbb{F}_q[x]/\langle x - [\alpha_n] \rangle \cong \underbrace{\mathbb{F}_q \oplus \cdots \oplus \mathbb{F}_q}_{n} \cong \mathbb{F}_q^n.$$

If $f^{(q)}$ is factorized in $\mathbb{F}_q[x]$ as $f^{(q)} = P_1 \cdots P_t$ for co-prime irreducible factors P_i with $\deg(P_i) = d_i$, then we have

$$\mathbb{F}_q[x]/\langle f^{(q)} \rangle \cong \mathbb{F}_q[x]/\langle P_1 \rangle \oplus \cdots \oplus \mathbb{F}_q[x]/\langle P_t \rangle \cong \mathbb{F}_{q^{d_1}} \oplus \cdots \oplus \mathbb{F}_{q^{d_t}}.$$

Each field $\mathbb{F}_{q^{d_i}}$ is a d_i-dimensional $\mathbb{F}_q$-vector space. The dimension of P_q is $d_1 + \cdots + d_t = n$.

With notation as above, we here give formal definitions of the Poly-LWE problems.

Definition 2.1.2 (decision-PLWE)**.** Let $n \in \mathbb{Z}_{>0}$, q a prime, $f \in \mathbb{Z}[x]$ a monic irreducible polynomial of degree n, and χ an error distribution over $(-q/2, q/2] \cap \mathbb{Z}$. Let $\overline{s} \in P_q \cong \mathbb{F}_q[x]/\langle f^{(q)} \rangle$ be a fixed secret element with $s(x) = \sum_{i=0}^{n-1} s_i x^i \in \mathbb{F}_q[x]$ and each coefficient $s_i \in \mathbb{F}_q$ chosen uniformly at random. We define the two samplers $\mathcal{O}_s$ and $\mathcal{O}_u$ as follows: The $\mathcal{O}_s$ outputs samples of the form $(\overline{a}, \overline{as + e}) \in P_q \times P_q$, where each coefficient of $a = \sum_{j=0}^{n-1} a_j x^j \in \mathbb{F}_q[x]$ is uniformly chosen and that of $e = \sum_{j=0}^{n-1} e_j x^j \in \mathbb{F}_q[x]$ is sampled from χ. The $\mathcal{O}_u$ outputs samples uniformly chosen at random from $P_q \times P_q$. Then the *decision Poly-LWE (PLWE) problem*, denoted "decision-PLWE$_{n,f,q,\chi}$", is to distinguish, with non-negligible advantage, between the same number of independent samples in two distributions on $P_q \times P_q$. The first consists of samples from $\mathcal{O}_s$, and the second consists of those from $\mathcal{O}_u$.

Definition 2.1.3 (search-PLWE)**.** Let $n \in \mathbb{Z}_{>0}$, q a prime, $f \in \mathbb{Z}[x]$ a monic irreducible polynomial of degree n, and χ an error distribution over $(-q/2, q/2] \cap \mathbb{Z}$. Let $\overline{s} \in P_q \cong \mathbb{F}_q[x]/\langle f^{(q)} \rangle$ be a fixed secret element with $s(x) = \sum_{i=0}^{n-1} s_i x^i \in \mathbb{F}_q[x]$ and each coefficient $s_i \in \mathbb{F}_q$ chosen uniformly at random. The *search-PLWE problem*, denoted "search-PLWE$_{n,f,q,\chi}$", i is to find $\overline{s}$ given access to arbitrary many independent samples from $\mathcal{O}_s$.

Note that $P \cong \mathbb{Z}^n$ as additive groups since f is a monic polynomial of degree n. With this fact, the error distribution χ is taken in practice as the discrete Gaussian distribution on $\mathbb{Z}$ with standard deviation $\sigma > 0$, denoted by $\mathcal{G}_\sigma$. Throughout the rest of this paper, assume $\chi = \mathcal{G}_\sigma$. As in [7], we also assume that $\chi = \mathcal{G}_\sigma$ is truncated at width 2σ.

2.2 Known attacks for decision-PLWE

This subsection gives a brief review on previously-proposed attacks, given in [6] and [7], against the decision-PLWE problem. First, we state an assumption in [6] and [7]:

Assumption 2.2.1. The polynomial $f^{(q)}(x) \in \mathbb{F}_q[x]$ splits completely in $\mathbb{F}_q[x]$, and has no double root in $\mathbb{F}_q$.

One can check that it is enough for the success of their attacks to assume the following (with some conditions on a root of $f^{(q)}$).

Assumption 2.2.2. The polynomial $f^{(q)}(x) \in \mathbb{F}_q[x]$ has at least one root in $\mathbb{F}_q$.

Throughout the rest of this subsection, we do not suppose Assumption 2.2.1, but suppose Assumption 2.2.2.

Attack based on a small set of error values The concept of this attack is to guess the value of $s(x)$ at a root of $f^{(q)}$ in $\mathbb{F}_q$. Let $[\alpha] \in \mathbb{F}_q$ with $\alpha \in (-q/2, q/2] \cap \mathbb{Z}$ be a solution of (small) order r to $f^{(q)} = 0$. As in [7], we assume for simplicity that n is divisible by r, say $n = n'r$ for $n' \in \mathbb{Z}_{\geq 1}$. Let $(\overline{a}, \overline{b})$ be a PLWE sample. Note that $b([\alpha]) - a([\alpha])s([\alpha]) = e([\alpha])$ since $f([\alpha]) = 0$ in $\mathbb{F}_q$. We determine possible values that $e([\alpha]) \in \mathbb{F}_q$ takes. Writing $e(x) = \sum_{i=0}^{n-1} [e_i] x^i$ for $e_i \in [-2\sigma, 2\sigma] \cap \mathbb{Z}$, we have

$$\begin{aligned}
\sum_{i=0}^{n-1} e_i \alpha^i &= (e_0 + e_1\alpha + \cdots + e_{r-1}\alpha^{r-1}) + (e_r + e_{r+1}\alpha + \cdots + e_{2r-1}\alpha^{r-1}) \\
&\quad + \cdots + (e_{(n'-1)r} + e_{(n'-1)r+1}\alpha + \cdots + e_{n'r-1}\alpha^{r-1}) \\
&= \sum_{j=0}^{r-1} e_j \alpha^j + \sum_{j=0}^{r-1} e_{r+j}\alpha^j + \cdots + \sum_{j=0}^{r-1} e_{(n'-1)r+j}\alpha^j \\
&= \sum_{k=0}^{n'-1} \sum_{j=0}^{r-1} e_{kr+j}\alpha^j = \sum_{j=0}^{r-1} \left(\sum_{k=0}^{n'-1} e_{kr+j} \right) \alpha^j
\end{aligned}$$

in $\mathbb{Z}$ and hence

$$e([\alpha]) = \sum_{j=0}^{r-1} \left[\sum_{k=0}^{n'-1} e_{kr+j} \right] [\alpha]^j$$

in $\mathbb{F}_q$. Since

$$\left|\sum_{k=0}^{n'-1} e_{kr+j}\right| \leq \sum_{k=0}^{n'-1} |e_{kr+j}| \leq 2\sigma n',$$

$e([\alpha])$ is included in the set

$$S_\alpha := \left\{ \sum_{j=0}^{r-1} [\ell_j][\alpha]^j : \ell_j \in [-2\sigma n', 2\sigma n'] \cap \mathbb{Z} \right\},$$

the cardinality of which is bounded by $(4\sigma n/r)^r$. Assume $(4\sigma n/r)^r < q$ for the success of the attack. With notation as above, we conduct the following procedures to guess $s([\alpha]) \in \mathbb{F}_q$:

(0) Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as+e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$.

(1) Compute the set S_α defined above.

(2) Collect $g \in \mathbb{F}_q$ such that $b([\alpha]) - ga([\alpha]) \in S_\alpha$ for all ℓ samples $(\overline{a}, \overline{b})$. Let G be the set of all values g collected as above.

(3) If G consists of just one element g, then we have $s([\alpha]) = g$.

In Algorithm 2.2.1, we give a pseudocode to proceed with the above four steps.

Proposition 2.2.3 ([7], Proposition 1)**.** *Assume $(4\sigma n/r)^r < q$. Algorithm 2.2.1 runs in $\widetilde{O}(\ell q + nq)$. If the algorithm outputs* **NOT PLWE***, then the samples are not chosen from the PLWE distribution. Otherwise the samples are PLWE samples with probability $1 - (\frac{\#S_\alpha}{q})^\ell$.*

Attack based on the size of the error values As in the previous paragraph, let $[\alpha]$ with $\alpha \in (-q/2, q/2] \cap \mathbb{Z}$ be a solution of (small) order r in $\mathbb{F}_q$ to $f^{(q)} = 0$. Let E_i denote the event that the representative of $b_i([\alpha]) - ga_i([\alpha])$ is in the interval $(-q/4, q/4)$ for some sample $(\overline{a_i}, \overline{b_i})$ and guess $g \in \mathbb{F}_q$ for $s([\alpha])$. Let $\mathcal{D}$ denote the distribution from which e_i is sampled. The concept of this attack is to compare the two probabilities $P(E_i \mid \mathcal{D} = \mathcal{U})$ and $P(E_i \mid \mathcal{D} = \mathcal{G}_\sigma)$. If $\mathcal{D} = \mathcal{U}$, then one has $P(E_i \mid \mathcal{D} = \mathcal{U}) = 1/2$. Assuming $\mathcal{D} = \mathcal{G}_\sigma$, we have $b_i([\alpha]) - a_i([\alpha])s([\alpha]) = e_i([\alpha])$ since $f([\alpha]) = 0$ in $\mathbb{F}_q$. We write $e_i(x) = \sum_{j=0}^{n-1} [e_{i,j}] x^j$ for $e_{i,j} \in [-2\sigma, 2\sigma] \cap \mathbb{Z}$. According to Section 3.2 in [7], we give a bound of $e_i^{(\alpha)} := \sum_{j=0}^{n-1} e_{i,j}\alpha^j \in \mathbb{Z}$.

Case of $\alpha = \pm 1$. In this case, the integer $e_i^{(\alpha)}$ is sampled from the discrete Gaussian distribution of mean 0 and variance $\sum_{k=0}^{n-1} \sigma^2 = n\sigma^2$, and hence

$$|e_i^{(\alpha)}| \leq 2\sigma\sqrt{n}. \tag{2.2.1}$$

Assuming $2\sigma\sqrt{n} < q/4$, we have $P(E_i \mid \mathcal{D} = \mathcal{G}_\sigma) = 1$ for $g = s([\alpha])$.

Case of $\alpha \neq \pm 1$. For simplicity, assume n is divisible by r, say $n = n'r$ for $n' \in \mathbb{Z}_{\geq 1}$. As in the previous paragraph, we have the equality

$$e_i^{(\alpha)} = \sum_{j=0}^{r-1} \left(\sum_{k=0}^{n'-1} e_{i,kr+j} \right) \alpha^j.$$

Algorithm 2.2.1 Small set of error values (Algorithm 1 of [7])

Input: a solution $[\alpha]$ with $\alpha \in (-q/2, q/2] \cap \mathbb{Z}$ of order r to $f^{(q)} = 0$, and an integer ℓ
Output: $s([\alpha]) \in \mathbb{F}_q$ or **NOT PLWE** or **INSUFFICIENT SAMPLES**

/* Construct a set S_α of error values */
$S_\alpha \leftarrow \{[\ell_0] + [\ell_1][\alpha] + \cdots + [\ell_{r-1}][\alpha]^{r-1} : \ell_i \in [-2\sigma n/r, 2\sigma n/r] \cap \mathbb{Z} \text{ for } 0 \le i \le r-1\}$
Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as + e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$
$G \leftarrow \emptyset$
for $g = 0$ **to** $q - 1$ **do**
  $appendflag \leftarrow 1$
  for $(\overline{a}, \overline{b})$ in the collection of samples **do**
    Compute $b([\alpha]) - ga([\alpha])$
    if $b([\alpha]) - ga([\alpha]) \notin S_\alpha$ **then**
      $appendflag \leftarrow 0$
      break $(\overline{a}, \overline{b})$
    end if
  end for
  if $appendflag = 1$ **then**
    $G \leftarrow G \cup \{g\}$
  end if
  if $\#G \ge 2$ **then**
    return INSUFFICIENT SAMPLES
  end if
end for
if $G = \emptyset$ **then**
  return NOT PLWE
else if $G = \{g\}$ **then**
  return g
end if

Recall that each $e_{i,j}$ is sampled from $\mathcal{G}_\sigma$. Thus the integer $\sum_{k=0}^{n'-1} e_{i,kr+j}$ is sampled from $\mathcal{G}_{\sigma'}$, where $(\sigma')^2 = \sum_{k=0}^{n'-1} \sigma^2 = n'\sigma^2$. Consequently, $e_i^{(\alpha)}$ is sampled from the discrete Gaussian distribution of mean 0 and variance

$$\sum_{j=0}^{r-1} n'\sigma^2\alpha^{2j} \quad = \quad n'\frac{\alpha^{2r}-1}{\alpha^2-1}\sigma^2.$$

Thus we have

$$\left|e_i^{(\alpha)}\right| \le 2\sigma\sqrt{n'} \cdot \frac{\sqrt{\alpha^{2r}-1}}{\sqrt{\alpha^2-1}}. \tag{2.2.2}$$

Assuming

$$2\sigma\sqrt{n'} \cdot \frac{\sqrt{\alpha^{2r}-1}}{\sqrt{\alpha^2-1}} < \frac{q}{4},$$

we have $P(E_i \mid \mathcal{D} = \mathcal{G}_\sigma) = 1$ for $g = s([\alpha])$.

We set the right hand sides of (2.2.1) and (2.2.2) as $B(\alpha)$. Note that each $B(\alpha)$ does not depend on any sample $(\overline{a_i}, \overline{b_i})$. With notation as above, we conduct the following procedures to guess $s([\alpha]) \in \mathbb{F}_q$:

(0) Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as+e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$.

(1) Collect $g \in \mathbb{F}_q$ such that the absolute value of the representative of $b([\alpha]) - ga([\alpha])$ is bounded by $B(\alpha)$ for all ℓ samples $(\overline{a}, \overline{b})$. Let G be the set of all values g collected as above.

(2) If G consists of just one element g, then we have $s([\alpha]) = g$.

In Algorithm 2.2.2, we give a pseudocode to proceed with the above three steps.

Algorithm 2.2.2 Small error values (Algorithm 2 of [7])

Input: a solution $[\alpha]$ with $\alpha \in (-q/2, q/2] \cap \mathbb{Z}$ of order r to $f^{(q)} = 0$, and an integer ℓ
Output: $s([\alpha]) \in \mathbb{F}_q$ or **NOT PLWE** or **INSUFFICIENT SAMPLES**

if $\alpha = 1$ **or** $\alpha = -1$ **then**
  $B(\alpha) \leftarrow 2\sigma\sqrt{n}$
else
  $B(\alpha) \leftarrow 2\sigma\sqrt{\frac{n}{r}} \cdot \frac{\sqrt{\alpha^{2r}-1}}{\sqrt{\alpha^2-1}}$
end if
Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as+e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$
$G \leftarrow \emptyset$
for $g = 0$ **to** $q-1$ **do**
  $appendflag \leftarrow 1$
  for $(\overline{a}, \overline{b})$ in the collection of samples **do**
    Compute $b([\alpha]) - ga([\alpha])$
    if the representative of $b([\alpha]) - ga([\alpha])$ does not lies in $[-B(\alpha), B(\alpha)]$ **then**
      $appendflag \leftarrow 0$
      break $(\overline{a}, \overline{b})$
    end if
  end for
  if $appendflag = 1$ **then**
    $G \leftarrow G \cup \{g\}$
  end if
  if $\#G \geq 2$ **then**
    return INSUFFICIENT SAMPLES
  end if
end for
if $G = \emptyset$ **then**
  return NOT PLWE
else if $G = \{g\}$ **then**
  return g
end if

Proposition 2.2.4 ([7], Proposition 2)**.** *With notation as above, assume*

(1) $\alpha = \pm 1$ *and* $8\sigma\sqrt{n} < q$*, or*

(2) α *has order* $r \geq 3$ *modulo* q *and*

$$8\sigma\sqrt{\frac{n}{r}} \cdot \frac{\sqrt{\alpha^{2r}-1}}{\sqrt{\alpha^2-1}} < q.$$

Algorithm 2.2.2 runs in $\widetilde{O}(\ell q)$*. If the algorithm outputs* **NOT PLWE***, then the samples are not chosen from the PLWE distribution. Otherwise the samples are PLWE samples with probability* $1 - (\frac{1}{2})^{\ell}$*.*

Example 2.2.5. Consider an example given in Section 5 of [7]. Let n be a positive integer, q a prime, $f(x) = x^n + q - 1$ and $\sigma = 8/\sqrt{2\pi} \approx 3.192$. Note that $f(x)$ is irreducible in $\mathbb{Z}[x]$ and always has a root 1 modulo q. For primes q satisfying $q > (4\sigma n/r)^r = 4\sigma n$, Algorithm 3.1.1 succeeds with probability $1 - (\#S_\alpha/q)^\ell$ for ℓ samples. For $n = 10$, this lower bound becomes $4 \cdot 3.192 \cdot 10 \approx 2^7$.

2.3 Some properties of finite fields and complexity assumptions

In this subsection, we collect some properties of finite fields and our complexity assumptions, which we shall use in the main section (Section 4) of this paper.

Some properties

Lemma 2.3.1. *Let* $P \in \mathbb{F}_q[x]$ *be an irreducible polynomial of degree* d *and* e *an integer with* $e \geq 1$*. Let* K *be a splitting field of* P^e *over* $\mathbb{F}_q$*. Then we have* $K \cong \mathbb{F}_q[x]/\langle P \rangle \cong \mathbb{F}_{q^d}$ *as fields.*

Proof. It suffices to prove that P splits completely in $\mathbb{F}_q[x]/\langle P \rangle \cong \mathbb{F}_{q^d}$. Put $\alpha := x + \langle P \rangle$, a root of P in $\mathbb{F}_q[x]/\langle P \rangle$ such that $\mathbb{F}_q[x]/\langle P \rangle = \mathbb{F}_q(\alpha)$. Since the characteristic is q, one has that for each $0 \leq k \leq d-1$, α^{q^k} is a root of P. We claim that α^{q^k}'s are pairwise distinct. Assume for a contradiction that $\alpha^{q^k} = \alpha^{q^\ell}$ for some $0 \leq k < \ell \leq d-1$, then one has $\alpha^{q^m} = \alpha$ for some integer $1 \leq m \leq d-1$ since $\alpha^{q^d} = \alpha$. One also has $\beta^{q^m} = \beta$ for all $\beta \in \mathbb{F}_q(\alpha) \cong \mathbb{F}_{q^d}$. This contradicts $\#(\mathbb{F}_{q^d}^\times) = q^d - 1$. □

Corollary 2.3.2. *Let* $P \in \mathbb{F}_q[x]$ *be an irreducible polynomial of degree* d *and* e *an integer with* $e \geq 1$*. Let* K *be a splitting field of* P^e *over* $\mathbb{F}_q$*, and* α *one root in* K *of* P*. Then all the roots of* f *are* $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}} \in K$*.*

Lemma 2.3.3. *Let* $P_1, \ldots, P_t \in \mathbb{F}_q[x]$ *be irreducible polynomials, and put* $d_i := \deg(P_i)$ *for* $1 \leq i \leq t$*. Let* $e_1, \ldots, e_t$ *be integers with* $e_i \geq 1$ *for* $1 \leq i \leq t$*. Let* K *be a minimal splitting field of* $P_1^{e_1} \cdots P_t^{e_t}$*, and* d *the least common multiple of* $d_1, \ldots, d_t$*. Then we have* $K \cong \mathbb{F}_{q^d}$ *as fields.*

Proof. A splitting field of each P_i over $\mathbb{F}_q$ is given as $K_{P_i} := \mathbb{F}_q[x]/\langle P_i \rangle \cong \mathbb{F}_{q^{d_i}}$. The field K_{P_i} is embedded into K as the subfield $K(\alpha_1^{(i)}, \ldots, \alpha_{d_i}^{(i)})$, where $\alpha_j^{(i)}$'s are roots in K of P_i. Hence we have

$$[K : \mathbb{F}_q] = [K : K_{P_i}] \cdot [K_{P_i} : \mathbb{F}_q] = [K : K_{P_i}] \cdot d_i,$$

which means that d_i divides $[K : \mathbb{F}_q]$. Thus d divides $[K : \mathbb{F}_q]$, so that $\mathbb{F}_{q^d}$ is embedded into K. Also, it follows from $d_i | d$ that $\mathbb{F}_{q^d} \supset \mathbb{F}_{q^{d_i}} \cong K_{P_i}$. Since P_i completely splits over K_{P_i}, the product $P_1 \cdots P_t$ completely splits over $\mathbb{F}_{q^d}$. From the minimality of K, we have $K \cong \mathbb{F}_{q^d}$. □

Lemma 2.3.4. *Let $P \in \mathbb{F}_q$ be an irreducible polynomial of degree d over $\mathbb{F}_q$. Let m be a positive integer with $d|m$, F any field of q^m elements, and $K = \{a \in F : a^{q^d} = a\}$. (Note that K is a field isomorphic to the field of q^d elements.) For a root $\beta \in K$ of P, the homomorphism*

$$\varphi : \mathbb{F}_q[x]/\langle P\rangle \longrightarrow K \ ; \ \alpha := x + \langle P\rangle \mapsto \beta$$

is bijective, and roots of P in $\mathbb{F}_q[x]/\langle P\rangle$ correspond those in K by $\alpha^{q^k} \leftrightarrow \beta^{q^k}$ via φ. Hence P splits completely over K.

Complexity assumptions Throughout the rest of this paper, assume for our complexity analysis that we do the computation in finite field by school methods, whose complexities are estimated as follows (see e.g., Sections 2.5 and 2.11 in[8]).

Lemma 2.3.5. *For $a, b \in \mathbb{F}_q$,*

(1) Computing $a \pm b$ can be done in $O(\log(q))$ bit operations.

(2) Computing $a \cdot b$ can be done in $O(\log^2(q))$ bit operations.

(3) Computing a^{-1} can be done in $O(\log^2(q))$ bit operations.

Lemma 2.3.6. *With a given polynomial basis of $\mathbb{F}_{q^m}$,*

(1) Addition and subtraction requires $O(m)$ arithmetic operations over $\mathbb{F}_q$.

(2) Computing $a \cdot b$ can be done in $O(m^2)$ arithmetic operations over $\mathbb{F}_q$.

(3) Computing a^{-1} can be done in $O(m^2)$ arithmetic operations over $\mathbb{F}_q$.

3 Attacks against search-PLWE

In this section, we give attacks against the search-variant of the PLWE problem. While [6] and [7] give attacks against the *decision-variant* of the PLWE, we present attacks against the *search-variant* of the PLWE (but the main idea is essentially the same as that of [6], [7]).

3.1 Search-case variants of the previous attacks

With notation as in the previous section, we give an attack against the search-PLWE problem. This attack is based on the idea of the attacks [6] and [7], reviewed in Section 2, against the decision-version of the PLWE problem. Throughout this section, we suppose Assumption 2.2.1, say

$$f^{(q)}(x) = \Pi_{i=1}^{n}(x - [\alpha_i]) \tag{3.1.1}$$

for some distinct $[\alpha_i] \in \mathbb{F}_q$ with $\alpha_i \in (-q/2, q/2] \cap \mathbb{Z}$ of (small) order r_i. Unlike the decision-case, this assumption is needed for the success of the attack against the search-case.

Attack based on a small set of error values (search-case) As we reviewed in the previous section, it is assumed in [6] and [7] for simplicity that the order of a root of $f^{(q)}$ is divisible by n. Here we do not assume it and write down a general-case condition under which their attack works well. Let $[\alpha] \in \mathbb{F}_q$ with $\alpha \in (-q/2, q/2] \cap \mathbb{Z}$ be a solution of order r to $f^{(q)} = 0$, i.e., $\alpha = \alpha_i$ and $r = r_i$ for some $1 \leq i \leq n$. We write $n = n'r + r'$ for $n', r' \in \mathbb{Z}$ with $0 \leq r' \leq r-1$. In a similar way to the previous section, we determine possible values that $e([\alpha])$ takes. Writing $e(x) = \sum_{i=0}^{n-1} [e_i] x^i$ for $e_i \in [-2\sigma, 2\sigma] \cap \mathbb{Z}$, we have

$$\begin{aligned}
\sum_{i=0}^{n-1} e_i \alpha^i &= \sum_{j=0}^{r-1} e_j \alpha^j + \sum_{j=0}^{r-1} e_{r+j} \alpha^j + \cdots + \sum_{j=0}^{r-1} e_{(n'-1)r+j} \alpha^j + \sum_{j=0}^{r'-1} e_{n'r+j} \alpha^j \\
&= \sum_{k=0}^{n'-1} \sum_{j=0}^{r-1} e_{kr+j} \alpha^j + \sum_{j=0}^{r'-1} e_{n'r+j} \alpha^j = \sum_{j=0}^{r-1} \left(\sum_{k=0}^{n'-1} e_{kr+j} \right) \alpha^j + \sum_{j=0}^{r'-1} e_{n'r+j} \alpha^j \\
&= \sum_{j=0}^{r'-1} \left(\sum_{k=0}^{n'} e_{kr+j} \right) \alpha^j + \sum_{j=r'}^{r-1} \left(\sum_{k=0}^{n'-1} e_{kr+j} \right) \alpha^j
\end{aligned}$$

in $\mathbb{Z}$ and hence

$$e([\alpha]) = \sum_{j=0}^{r'-1} \left[\sum_{k=0}^{n'} e_{kr+j} \right] [\alpha]^j + \sum_{j=r'}^{r-1} \left[\sum_{k=0}^{n'-1} e_{kr+j} \right] [\alpha]^j$$

in $\mathbb{F}_q$. It follows from

$$\left| \sum_{k=0}^{n'} e_{kr+j} \right| \leq 2\sigma(n'+1)$$

together with

$$\left| \sum_{k=0}^{n'-1} e_{kr+j} \right| \leq \sum_{k=0}^{n'-1} |e_{kr+j}| \leq 2\sigma n'$$

that $e([\alpha])$ is included in the set S_α of elements of the form

$$[\ell_0] + [\ell_1][\alpha] + \cdots + [\ell_{r'-1}][\alpha]^{r'-1} + [\ell_{r'}][\alpha]^{r'} + \cdots + [\ell_{r-1}][\alpha^{r-1}], \tag{3.1.2}$$

where $\ell_i \in [-2\sigma(n'+1), 2\sigma(n'+1)] \cap \mathbb{Z}$ for $0 \leq i \leq r'-1$ and $\ell_{i'} \in [-2\sigma n', 2\sigma n'] \cap \mathbb{Z}$ for $r' \leq i' \leq r-1$. The cardinality $\#S_\alpha$ is bounded by

$$(4\sigma(n'+1))^{r'} \cdot (4\sigma n')^{r-r'}$$

for $r \leq n$, and by $(4\sigma)^n$ for $r > n$. With notation as above, we conduct the following procedures to find $s([\alpha]) \in \mathbb{F}_q$:

(0) Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as + e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$.

(1) Compute the set S_α of elements of the form (3.1.2).

(2) Collect $g \in \mathbb{F}_q$ such that $b([\alpha]) - g a([\alpha]) \in S_\alpha$ for all ℓ samples $(\overline{a}, \overline{b})$. Let G be the set of all values g collected as above.

Algorithm 3.1.1 Small set of error values (n is not necessarily divisible by r)

Input: a solution $[\alpha] \in \mathbb{F}_q$ with $\alpha \in (-q/2, q/2] \cap \mathbb{Z}$ of order r to $f^{(q)} = 0$, and an integer ℓ
Output: $s([\alpha]) \in \mathbb{F}_q$ or **INSUFFICIENT SAMPLES**

Write $n = n'r + r'$ for $n', r' \in \mathbb{Z}$ with $0 \leq r' \leq r-1$.
Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as+e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$
/* Construct a set S_α of error values */
$S_\alpha \leftarrow$ the set of elements of the form (3.1.2)
$G \leftarrow \emptyset$
for $g = 0$ **to** $q-1$ **do**
  $appendflag \leftarrow 1$
  for $(\overline{a}, \overline{b})$ in the collection of samples **do**
    Compute $b([\alpha]) - ga([\alpha])$
    if $b([\alpha]) - ga([\alpha]) \notin S_\alpha$ **then**
      $appendflag \leftarrow 0$
      break $(\overline{a}, \overline{b})$
    end if
  end for
  if $appendflag = 1$ **then**
    $G \leftarrow G \cup \{g\}$
  end if
  if $\#G \geq 2$ **then**
    return INSUFFICIENT SAMPLES
  end if
end for
return the element g of G

(3) If G consists of just one element g, then we have $s([\alpha]) = g$.

In Algorithm 3.1.1, we give a pseudocode to proceed with the above four steps.

Proposition 3.1.1. *With notation as above, assume $\#S_\alpha < q$. Algorithm 3.1.1 terminates in $O(q\ell n + q\ell \log(q))$ arithmetic operations over the ground field $\mathbb{F}_q$, that is, $O(q\ell n \log^2(q) + q\ell \log^3(q))$ bit operations.*

Proof. It requires $O(r)$ multiplications over $\mathbb{F}_q$ to compute all $[\alpha]^i$ for $0 \leq i \leq r-1$. Each element in S_α is computed by combining $O(r)$ multiplications and $O(r)$ additions, so that it requires $O(r)$ arithmetic operations over $\mathbb{F}_q$. By our assumption, S_α has at most q elements. Hence we compute S_α in $O(r + rq) = O(rq)$ arithmetic operations over $\mathbb{F}_q$.

The main double loop has at most $q\ell$ iterations. For each iteration, we compute $h := b([\alpha]) - ga([\alpha])$ and decide whether $h \in S_\alpha$ or not. With $[\alpha]^i$ computed as above, computing $b([\alpha]) = \sum_{j=0}^{n-1} [b_j][\alpha]^j$ and $a([\alpha]) = \sum_{j=0}^{n-1} [a_j][\alpha]^j$ needs $2n + 2n = O(n)$ arithmetic operations over $\mathbb{F}_q$. Using a binary search to decide whether $h \in S_\alpha$ or not, we do this in $O(\log(q))$ operations. Summing up, each iteration takes $O(n + \log(q))$ arithmetic operations over $\mathbb{F}_q$, and thus $O(q\ell n + q\ell \log(q))$ is required in total.

As a consequence, one conducts all the procedures in $O(rq + q\ell n + q\ell \log(q)) = O(q\ell n + q\ell \log(q))$ arithmetic operations over $\mathbb{F}_q$, i.e., $O(q\ell n (\log(q))^2 + q\ell (\log(q))^3)$ bit operations. □

We can give another version of Algorithm 3.1.1 as follows.

(0) Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as+e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$.

(1) Compute the set S_α of elements of the form (3.1.2), and let $G = \mathbb{F}_q$.

(2) Choose one sample $(\overline{a}, \overline{b})$. For each $h^{(q)} \in S_\alpha$, we compute $g := a([\alpha])^{-1}(b([\alpha]) - h^{(q)}) \in \mathbb{F}_q$. (Note that $b([\alpha]) - a([\alpha])g = h^{(q)}$ in $\mathbb{F}_q$.) Let G' be the set of all values g computed as above.

(3) If $G \cap G'$ consists of just one element g, then we have $s([\alpha]) = g$. Otherwise replace G by $G \cap G'$. Go back to (2), and then choose another sample.

In Algorithm 3.1.2, we give a pseudocode to proceed with the above four steps.

Algorithm 3.1.2 Another version of Small set of error values (n is not necessarily divisible by r)

Input: a solution $[\alpha] \in \mathbb{F}_q$ with $\alpha \in (-q/2, q/2] \cap \mathbb{Z}$ of order r to $f^{(q)} = 0$, and an integer ℓ

Write $n = n'r + r'$ for $n', r' \in \mathbb{Z}$ with $0 \leq r' \leq r-1$.
Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as+e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$
/* Construct a set S_α of error values */
$S_\alpha \leftarrow$ the set of elements of the form (3.1.2)
$G \leftarrow \mathbb{F}_q$
for $(\overline{a}, \overline{b})$ in the collection of samples **do**
    Compute $a([\alpha])$, $a([\alpha])^{-1}$ and $b([\alpha])$ in $\mathbb{F}_q$
    /* Collect possible values for $e([\alpha]) \in \mathbb{F}_q$ */
    $G' \leftarrow \emptyset$
    for $h^{(q)} \in S_\alpha$ **do**
        $g \leftarrow a([\alpha])^{-1}(b([\alpha]) - h^{(q)})$.
        $G' \leftarrow G' \cup \{g\}$
    end for
    $G \leftarrow G \cap G'$
    if $\#G \leq 1$ **then**
        break $(\overline{a}, \overline{b})$
    end if
end for
if $G = \{g\}$ **then**
    return g
else
    return INSUFFICIENT SAMPLES
end if

Proposition 3.1.2. *With notation as above, assume $\#S_\alpha < q$. Algorithm 3.1.2 terminates in $O(rq + \ell n + \ell q)$ arithmetic operations over the ground field $\mathbb{F}_q$, that is, $O((rq + \ell n + \ell q)\log^2(q))$ bit operations.*

Proof. As in the proof of Proposition 3.1.1, it requires $O(rq)$ arithmetic operations over $\mathbb{F}_q$ to compute S_α together with $[\alpha]^i$ for $0 \leq i \leq r-1$.

The main **for**-loop specified at the 6-th line has at most ℓ iterations. For each iteration, we compute $a([\alpha])$, $a([\alpha])^{-1}$ and $b([\alpha])$ by substituting $[\alpha]$ to $a(x)$ and $b(x)$. With $[\alpha]^i$ computed as above, this requires $O(n)$ arithmetic operations over $\mathbb{F}_q$. The **for**-loop specified at the 10-th line has $\#S_\alpha = O(q)$ iterations by our assumption. For each iteration, one computes $g = a([\alpha])^{-1}(b([\alpha]) - h^{(q)})$, where $a([\alpha])^{-1}$ and $b([\alpha])$ have been computed at the 7th line. Thus, $O(q)$ arithmetic operations are required through the **for**-loop on $h^{(q)}$. After the loop on $h^{(q)}$, we compute the set intersection $G \cap G'$. Since the cardinalities of the two sets are bounded by $\#S_\alpha < q$, one computes this intersection in $O(q)$ arithmetic operations, see e.g., [1] for the computation of set intersections. Summing up, it requires in total $\ell(n+q+q) = O(\ell n + \ell q)$ arithmetic operations to conduct the main **for**-loop.

As a consequence, one conducts all the procedures in $O(rq + \ell n + \ell q)$ arithmetic operations over $\mathbb{F}_q$, i.e., $O((rq + \ell n + \ell q)(\log(q))^2)$ bit operations. □

After conducting Algorithm 3.1.1 or 3.1.2 for all roots of $f^{(q)}$, we next try to recover the correct $s(x)$. Writing $s(x) = \sum_{j=0}^{n-1} s_j x^j$ with $s_j \in \mathbb{F}_q$ and regarding $\sum_{j=1}^{n} s_{n-j}[\alpha_i]^{n-j} = s([\alpha_i])$ as an equation on s_j's, we construct the following linear system:

$$\left[\ [\alpha_i]^{n-j}\ \right]_{1\le i,j\le n} \cdot \begin{bmatrix} s_{n-1} \\ \vdots \\ s_0 \end{bmatrix} = \begin{bmatrix} s([\alpha_1]) \\ \vdots \\ s([\alpha_n]) \end{bmatrix}.$$

The coefficient matrix is an $n \times n$ matrix; in other words, the system has n equations with n indeterminates. Since the coefficient matrix has full-rank, i.e., it is invertible over $\mathbb{F}_q$, the secret vector ${}^t[s_{n-1}, \ldots, s_0]$ is uniquely determined.

Remark 3.1.3. Since $f^{(q)}$ has distinct roots, the above matrix $[[\alpha_i]^{n-j}]_{i,j}$ always has full-rank. Indeed, Lagrange's interpolation theorem says that given distinct points $\alpha'_1, \ldots, \alpha'_n \in \mathbb{F}_q$ and arbitrary points $\beta_1, \ldots, \beta_n \in \mathbb{F}_q$, there is a unique polynomial $s'(x) \in \mathbb{F}_q[x]$ of degree $n-1$ such that $s'(\alpha'_i) = \beta_i$ for all $1 \le i \le n$.

In Algorithm 3.1.3, we write down a pseudocode to compute the secret $s(x)$.

Algorithm 3.1.3 Recover the secret polynomial (based on Small set of error values)

Input: a sequence of all solutions $[\alpha_i] \in \mathbb{F}_q$ with $\alpha_i \in (-q/2, q/2] \cap \mathbb{Z}$ of order r_i for $1 \le i \le n$ to $f^{(q)} = 0$, and $(\ell_i)_{i=1}^n$

Output: $s(x) \in \mathbb{F}_q[x]$

1: **for** $i = 1$ **to** n **do**
2: Compute $s([\alpha_i]) \in \mathbb{F}_q$ by Algorithm 3.1.1 or Algorithm 3.1.2 with inputs α_i and ℓ_i.
3: **end for**
4: $A \leftarrow ([\alpha_i]^{n-j})_{i,j}$
5: Compute A^{-1}
6: $\mathbf{s} \leftarrow A^{-1} \cdot {}^t[g_1, \ldots, g_n]$
7: Write ${}^t\mathbf{s} = (s'_{n-1}, \ldots, s'_0)$
8: **return** $s'(x) = \sum_{j=0}^{n-1} s_j x^j$

Proposition 3.1.4. *With notation as above, assume $\#S_\alpha < q$ for all roots $[\alpha] \in \mathbb{F}_q$ with $\alpha \in (-q/2, q/2] \cap \mathbb{Z}$ of $f^{(q)}$. Let $\ell := \max_{1\leq i\leq n} \ell_i$. If one executes Algorithm 3.1.1 in the 4-th line of Algorithm 3.1.3, Algorithm 3.1.3 performs in $O(q\ell n + q\ell\log(q))$ arithmetic operations over $\mathbb{F}_q$, that is, $O(q\ell n\log^2(q) + q\ell\log^3(q))$ bit operations.*

Proof. For each iteration of the first **for**-loop, one conducts Algorithm 3.1.1, which requires $O(q\ell n + q\ell\log(q))$ arithmetic operations by Proposition 3.1.1. Computing $[\alpha]_i^{n-j}$'s is negligible since $[\alpha]_i^k$'s have been computed in Algorithm 3.1.1. Computing A^{-1} and $A^{-1} \cdot {}^t[g_1, \cdots, g_n]$ requires $n^3 + n^2 = O(n^3)$ arithmetic operations.

Consequently, the arithmetic complexity of Algorithm 3.1.3 is bounded by

$$n(q\ell n + q\ell\log(q)) + n^3 = O(q\ell n^2 + nq\ell\log(q) + n^3).$$

Hence its bit complexity is bounded by $O(q\ell n^2(\log(q))^2 + nq\ell(\log(q))^3 + n^3(\log(q))^2)$. □

Attack based on the size of the error values (search-case) The concept of this attack is same as the attack described in the previous paragraph. As in the previous paragraph, we do not assume that the order of a root of $f^{(q)}$ is divisible by n. Let $[\alpha]$ with $\alpha \in (-q/2, q/2] \cap \mathbb{Z}$ be a solution of order r in $\mathbb{F}_q$ to $f^{(q)} = 0$, i.e., $\alpha = \alpha_i$ and $r = r_i$ for some $1 \leq i \leq n$. We write $n = n'r + r'$ for $n', r' \in \mathbb{Z}$ with $0 \leq r' \leq r-1$, and $e_i(x) = \sum_{j=0}^{n-1}[e_{i,j}]x^j$ for $e_{i,j} \in [-2\sigma, 2\sigma] \cap \mathbb{Z}$. In a similar way to the previous section, we give a bound of $e_i^{(\alpha)} := \sum_{j=0}^{n-1} e_{i,j}\alpha^j \in \mathbb{Z}$.

Case of $\alpha = \pm 1$. Similarly to the previous section, we have

$$|e_i^{(\alpha)}| \leq 2\sigma\sqrt{n}. \tag{3.1.3}$$

We set the right hand side of (3.1.3) as $B(\alpha)$.

Case of $\alpha \neq \pm 1$. As in the previous paragraph, we have the equality

$$e_i^{(\alpha)} = \sum_{j=0}^{r'-1}\left(\sum_{k=0}^{n'} e_{kr+j}\right)\alpha^j + \sum_{j=r'}^{r-1}\left(\sum_{k=0}^{n'-1} e_{kr+j}\right)\alpha^j.$$

Recall that each e_i is sampled from $\mathcal{G}_\sigma$. Thus the integers $\sum_{k=0}^{n'} e_{kr+j}$ and $\sum_{k=0}^{n'-1} e_{kr+j}$ are sampled from $\mathcal{G}_{\sigma_1}$ and $\mathcal{G}_{\sigma_2}$, where

$$\sigma_1^2 = \sum_{k=0}^{n'} \sigma^2 = (n'+1)\sigma^2$$

and

$$\sigma_2^2 = \sum_{k=0}^{n'-1} \sigma^2 = n'\sigma^2.$$

Consequently, $e_i^{(\alpha)}$ is sampled from the discrete Gaussian distribution of mean 0 and variance

$$\begin{aligned}\sum_{j=0}^{r'-1}(n'+1)\sigma^2\alpha^{2j} + \sum_{j=r'}^{r-1} n'\sigma^2\alpha^{2j} &= (n'+1)\sigma^2\frac{\alpha^{2r'}-1}{\alpha^2-1} + n'\sigma^2\frac{\alpha^{2(r-r')}-1}{\alpha^2-1}\alpha^{2r'} \\ &= \frac{n'\alpha^{2r} + \alpha^{2r'} - n' - 1}{\alpha^2-1}\sigma^2.\end{aligned}$$

Thus we have

$$\left|e_i^{(\alpha)}\right| \leq 2\sigma \frac{\sqrt{n'\alpha^{2r} + \alpha^{2r'} - n' - 1}}{\sqrt{\alpha^2 - 1}}. \tag{3.1.4}$$

We set the right hand side of (3.1.4) as $B(\alpha)$.

Note that $B(\alpha)$ does not depend on any sample $(\overline{a_i}, \overline{b_i})$. With notation as above, we conduct the following procedures to find $s([\alpha]) \in \mathbb{F}_q$:

(0) Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as + e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$.

(1) Collect $g \in \mathbb{F}_q$ such that the absolute value of the representative of $b(\alpha) - ga(\alpha)$ is bounded by $B(\alpha)$ for all ℓ samples $(\overline{a}, \overline{b})$. Let G be the set of all values g collected as above.

(2) If G consists of just one element g, then we have $s([\alpha]) = g$.

In Algorithm 3.1.4, we give a pseudocode to proceed with the above three steps.

It is straightforward to estimate an upper-bound of the complexity of Algorithm 3.1.4.

Proposition 3.1.5. *With notation as above, assume*

(1) $\alpha = \pm 1$ *and* $4\sigma\sqrt{n} \leq q$, *or*

(2) α *has order* $r \geq 3$ *modulo* q *and*

$$4\sigma \frac{\sqrt{n'\alpha^{2r} + \alpha^{2r'} - n' - 1}}{\sqrt{\alpha^2 - 1}} \leq q.$$

Algorithm 3.1.4 terminates in $O(\ell q n)$ *arithmetic operations over* $\mathbb{F}_q$, *that is,* $O(\ell q n \log^2(q))$ *bit operations.*

We can give another version of Algorithm 3.1.4 as follows.

(0) Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as + e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$.

(1) Compute the bound $B(\alpha)$, ad let $G = \mathbb{F}_q$.

(2) Choose one sample $(\overline{a}, \overline{b})$. For each h in $[-B(\alpha), B(\alpha)] \cap \mathbb{Z}$, we compute $g := a([\alpha])^{-1}(b([\alpha]) - h^{(q)}) \in \mathbb{F}_q$, where $h^{(q)} \in \mathbb{F}_q$ denotes the reduction of h. (Note that $b([\alpha]) - a([\alpha])g = h^{(q)}$ in $\mathbb{F}_q$.) Let G' be the set of all values g computed as above.

(3) If $G \cap G'$ consists of just one element g, then we have $s([\alpha]) = g$. Otherwise replace G by $G \cap G'$. Go back to (2), and then choose another sample.

In Algorithm 3.1.5, we give a pseudocode to proceed with the above four steps.

It is straightforward to estimate an upper-bound of the complexity of Algorithm 3.1.5.

Proposition 3.1.6. *With notation as above, assume*

(1) $\alpha = \pm 1$ *and* $4\sigma\sqrt{n} \leq q$, *or*

Algorithm 3.1.4 Small error values (n is not necessarily divisible by r)

Input: a solution $[\alpha] \in \mathbb{F}_q$ with $\alpha \in (-q/2, q/2] \cap \mathbb{Z}$ of order r to $f^{(q)} = 0$, and an integer ℓ
Output: $s([\alpha]) \in \mathbb{F}_q$ or **INSUFFICIENT SAMPLES**

Write $n = n'r + r'$ for $n', r' \in \mathbb{Z}$ with $0 \leq r' \leq r-1$.
Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as+e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$
if $\alpha = 1$ **or** $\alpha = -1$ **then**
  $B(\alpha) \leftarrow 2\sigma\sqrt{n}$
else
  $B(\alpha) \leftarrow 2\sigma \frac{\sqrt{n'\alpha^{2r} + \alpha^{2r'} - n' - 1}}{\sqrt{\alpha^2 - 1}}$
end if
$G \leftarrow \emptyset$
for $g = 0$ **to** $q-1$ **do**
  $appendflag \leftarrow 1$
  for $(\overline{a}, \overline{b})$ in the collection of samples **do**
    Compute $b([\alpha]) - ga([\alpha])$
    if $b([\alpha]) - ga([\alpha]) \notin [-B(\alpha), B(\alpha)] \cap \mathbb{Z}$ **then**
      $appendflag \leftarrow 0$
      break $(\overline{a}, \overline{b})$
    end if
  end for
  if $appendflag = 1$ **then**
    $G \leftarrow G \cup \{g\}$
  end if
  if $\#G \geq 2$ **then**
    return INSUFFICIENT SAMPLES
  end if
end for
return the element g of G

(2) α has order $r \geq 3$ modulo q and

$$4\sigma \frac{\sqrt{n'\alpha^{2r} + \alpha^{2r'} - n' - 1}}{\sqrt{\alpha^2 - 1}} \leq q.$$

Algorithm 3.1.5 terminates in $O(\ell n + \ell q)$ arithmetic operations over $\mathbb{F}_q$, that is, $O((\ell n + \ell q)\log^2(q))$ bit operations.

Remark 3.1.7. Each constructed set G contains just $2\lfloor B(\alpha) \rfloor + 1$ elements of $\mathbb{F}_q$. Indeed, the *affine map* $\mathbb{F}_q \to \mathbb{F}_q$; $h' \mapsto -a([\alpha])^{-1}h' + a([\alpha])^{-1}b([\alpha])$ is bijective since $a([\alpha]) \neq 0$.

In a similar way to the previous paragraph, we can recover $s(x)$ from $s([\alpha_i])$'s. In Algorithm 3.1.6, we write down a pseudocode to compute the secret $s(x)$.

As in the proof of Proposition 3.1.4, one can prove the following proposition.

Proposition 3.1.8. *With notation as above, assume*

(1) $4\sigma\sqrt{n} \leq q$ if $\alpha_i = \pm 1$, and

Algorithm 3.1.5 Another version of Small error values (n is not necessarily divisible by r)

Input: a solution $[\alpha] \in \mathbb{F}_q$ with $\alpha \in (-q/2, q/2] \cap \mathbb{Z}$ of order r to $f^{(q)} = 0$, and an integer ℓ
Output: $s([\alpha]) \in \mathbb{F}_q$

1: Write $n = n'r + r'$ for $n', r' \in \mathbb{Z}$ with $0 \leq r' \leq r-1$
2: Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as+e}) \in P_q \times P_q$ with $a([\alpha]) \neq 0$
3: **if** $\alpha = 1$ **or** $\alpha = -1$ **then**
4: $\quad B(\alpha) \leftarrow 2\sigma\sqrt{n}$
5: **else**
6: $\quad B(\alpha) \leftarrow 2\sigma \frac{\sqrt{n'\alpha^{2r}+\alpha^{2r'}-n'-1}}{\sqrt{\alpha^2-1}}$
7: **end if**
8: $G \leftarrow \mathbb{F}_q$
9: **for** $(\overline{a}, \overline{b})$ in the collection of samples **do**
10: $\quad$ Compute $a([\alpha])$, $a([\alpha])^{-1}$ and $b([\alpha])$ in $\mathbb{F}_q$
11: $\quad$ /* Collect possible values for $e(\alpha) \in \mathbb{F}_q$ */
12: $\quad G' \leftarrow \emptyset$
13: $\quad$ **for** $h \in [-B(\alpha), B(\alpha)] \cap \mathbb{Z}$ **do**
14: $\quad\quad h^{(q)} \leftarrow$ the reduction in $\mathbb{F}_q$ of h
15: $\quad\quad g \leftarrow a([\alpha])^{-1}(b([\alpha]) - h^{(q)})$.
16: $\quad\quad G' \leftarrow G' \cup \{g\}$
17: $\quad$ **end for**
18: $\quad G \leftarrow G \cap G'$
19: $\quad$ **if** $\#G \leq 1$ **then**
20: $\quad\quad$ **break** $(\overline{a}, \overline{b})$
21: $\quad$ **end if**
22: **end for**
23: **if** $G = \{g\}$ **then**
24: $\quad$ **return** g
25: **else**
26: $\quad$ **return INSUFFICIENT SAMPLES**
27: **end if**

(2)

$$4\sigma \frac{\sqrt{n'\alpha_i^{2r} + \alpha_i^{2r'} - n' - 1}}{\sqrt{\alpha_i^2 - 1}} \leq q$$

if $\alpha_i \neq \pm 1$,

for all $1 \leq i \leq n$. *Let* $\ell := \max_{1 \leq i \leq n} \ell_i$. *If one executes Algorithm 3.1.4 in the* 4*-th line of Algorithm 3.1.6, Algorithm 3.1.6 performs in* $O(q\ell n^2 + n^3)$ *arithmetic operations over* $\mathbb{F}_q$, *that is,* $O(q\ell n^2 \log^2(q) + n^3 \log^2(q))$ *bit operations.*

Remark 3.1.9. While f is assumed to have at least one root in $\mathbb{F}_q$ in the decision-case (Assumption 2.2.2), we need to suppose a stronger assumption (Assumption 2.2.1) for constructing successful attacks in the search-case. As we will see in Section 3.3, for a fixed f of large degree, the number of primes satisfying Assumption 2.2.1 is small in the sense of *density*.

Algorithm 3.1.6 Recover the secret polynomial (based on Small error values)

Input: a sequence of all solutions $[\alpha_i] \in \mathbb{F}_q$ with $\alpha_i \in (-q/2, q/2] \cap \mathbb{Z}$ of order r_i for $1 \leq i \leq n$ to $f^{(q)} = 0$, and $(\ell_i)_{i=1}^n$

Output: $s(x) \in \mathbb{F}_q[x]$

1: **for** $i = 1$ **to** n **do**
2: Compute $s([\alpha_i]) \in \mathbb{F}_q$ by Algorithm 3.1.4 or Algorithm 3.1.5 with inputs α_i and ℓ_i.
3: **end for**
4: $A \leftarrow ([\alpha_i]^{n-j})_{i,j}$
5: Compute A^{-1}
6: $\mathbf{s} \leftarrow A^{-1} \cdot {}^t[g_1, \ldots, g_n]$
7: Write ${}^t\mathbf{s} = (s'_{n-1}, \ldots, s'_0)$
8: **return** $s'(x) = \sum_{j=0}^{n-1} s_j x^j$

3.2 Vulnerable polynomials by the search-case attacks

We use the same notation as in the previous subsection. In this subsection, we characterize defining polynomials for which the search-PLWE problem is solvable by the search-case attacks. Let us focus on Algorithm 3.1.3. Let $n \in \mathbb{Z}_{\geq 1}$, $\sigma \in \mathbb{R}_{>0}$ and q a prime. As showed in the previous subsection, the PLWE instances defined by monic polynomials $f \in \mathbb{Z}[x]$ of degree n satisfying the following conditions can be vulnerable by Algorithm 3.1.3:

V1 $f^{(q)}$ *splits completely* in $\mathbb{F}_q[x]$,

V2 $\#S_\alpha < q$ for *all* roots $\alpha \in \mathbb{F}_q$ of $f^{(q)}$,

where each S_α is determined by n, σ, α and q. Hence for an integer n, $\sigma \in \mathbb{R}_{>0}$, a prime q, and

$$f \in \mathcal{F}_{n,\sigma,q} := \{f \in \mathbb{Z}[x] : f \text{ is monic with } \deg(f) = n \text{ and } f \text{ satisfies } \mathbf{V1} \text{ and } \mathbf{V2}\},$$

the search-PLWE problem is solvable with sufficiently high probability in practical time by Algorithm 3.1.3.

3.3 Density of vulnerable primes

Without Assumption 2.2.1, one may avoid the search-case attacks (Algorithms 3.1.3 and 3.1.6) by choosing an irreducible polynomial $f \in \mathbb{Z}[x]$ such that its Galois group becomes huge; By the Frobenius density theorem (more generally, the Chebotarev density theorem), the density

$$\lim_{x \to \infty} \#\{q \leq x : q \text{ is a prime, and } (f \bmod q) \text{ has } n \text{ roots in } \mathbb{F}_q\}/\#\{q \leq x : q \text{ is a prime}\}$$

is equal to $1/\#G_f$, where G_f denotes the Galois group $\mathrm{Gal}(K_f/\mathbb{Q})$ for the smallest splitting field K_f of f over $\mathbb{Q}$ (note that the smallest splitting filed of a polynomial is unique up to isomorphism). With this fact on the density, we see that when G_f is large enough, the number of primes q such that $f^{(q)}$ has n roots in $\mathbb{F}_q$ is much less than the other cases. In other words, for such an f, the proposed search-case attacks fail for many prime q.

4 General-case attacks

We extend the search-case attacks (Algorithms 3.1.3 and 3.1.6) so as to deal with cases where $f^{(q)}$ does not split completely in $\mathbb{F}_q[x]$, i.e., $f^{(q)}$ has a non-linear irreducible factor in $\mathbb{F}_q[x]$. Our main idea of this extension is to reduce the problem into a problem over the smallest splitting field of each irreducible factor of $f^{(q)}$.

4.1 Our extended attack against PLWE

We use the same notation as in Definition 2.1.3 with $\chi = \mathcal{G}_\sigma$, where $\sigma \in \mathbb{R}_{>0}$. Different from the previous sections, we assume neither Assumptions 2.2.1 nor 2.2.2, but assume the following.

Assumption 4.1.1. The polynomial $f^{(q)}(x) \in \mathbb{F}_q[x]$ is a square-free polynomial over $\overline{\mathbb{F}_q}$, the algebraic closure of $\mathbb{F}_q$.

Then $f^{(q)}$ has the following factorization:

$$f^{(q)}(x) = P_1(x) \cdots P_t(x),$$

where each P_i is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree $d_i \leq n$ with $P_i \neq P_j$ for $i \neq j$, and $\sum_{i=1}^{t} d_i = n$. For the efficiency of our attack, assume that each d_i is small enough, e.g., $d_i = 2$ or 3. Choose P_i, and put $K_{P_i} := \mathbb{F}_q[x]/\langle P_i \rangle \cong \mathbb{F}_{q^{d_i}}$. By Lemma 2.3.1, each K_{P_i} is a smallest splitting field of P_i over $\mathbb{F}_q$. Let α_i be a root of P_i of order r_i in K_{P_i}. It follows from Corollary 2.3.2 that $\alpha_i, \alpha_i^q, \ldots, \alpha_i^{q^{d_i-1}}$ are all the solutions to P_i in K_{P_i}.

Here we try to compute $s(\alpha_i)$ in K_{P_i}. To simplify the notation, we take $i = 1$, $P = P_1$, $d = d_1$, $K_P = K_{P_1}$ and $\alpha = \alpha_1$. We write $n = n'r + r'$ for $n', r' \in \mathbb{Z}$ with $0 \leq r' \leq r - 1$. As in the previous section, we determine possible values that $e(\alpha)$ takes. Writing $e(x) = \sum_{j=0}^{n-1} [e_j] x^j$ with $e_j \in [-2\sigma, 2\sigma] \cap \mathbb{Z}$, one has

$$e(\alpha) = \sum_{j=0}^{r'-1} \left[\sum_{k=0}^{n'} e_{kr+j} \right] \alpha^j + \sum_{j=r'}^{r-1} \left[\sum_{k=0}^{n'-1} e_{kr+j} \right] \alpha^j.$$

Hence $b(\alpha) - a(\alpha)s(\alpha) = e(\alpha)$ is included in the set $S_\alpha \subset K_P$ of elements of the form

$$[\ell_0] + [\ell_1]\alpha + \cdots + [\ell_{r'-1}]\alpha^{r'-1} + [\ell_{r'}]\alpha^{r'} + \cdots + [\ell_{r-1}]\alpha^{r-1}, \tag{4.1.1}$$

where $\ell_i \in [-2\sigma(n'+1), 2\sigma(n'+1)] \cap \mathbb{Z}$ for $0 \leq i \leq r'-1$ and $\ell_{i'} \in [-2\sigma n', 2\sigma n'] \cap \mathbb{Z}$ for $r' \leq i' \leq r-1$. The cardinality $\#S_\alpha$ is bounded by

$$(4\sigma(n'+1))^{r'} \cdot (4\sigma n')^{r-r'}$$

for $r \leq n$, and by $(4\sigma)^n$ for $r > n$. With notation as above, we conduct the following procedures to find $s(\alpha)$.

(0) Access to the PLWE oracle to get ℓ PLWE samples $(\overline{a}, \overline{b} = \overline{as + e}) \in P_q \times P_q$ satisfying $a(\alpha) \neq 0$.

(1) Compute the set S_α of elements of the form (4.1.2). Note that each element of S_α is represented by the basis $\{1, \gamma, \ldots, \gamma^{d-1}\}$ with $\mathbb{F}_q$-coefficients, where $\gamma := x + \langle P \rangle$ (this basis is called a *polynomial basis*). Let $G := \emptyset$.

(2) For each $g \in K_P$, we conduct the following sub-procedures:

(2-1) Choose one sample $(\overline{a}, \overline{b})$. Compute $a(\alpha)$, $b(\alpha)$, and $b(\alpha) - a(\alpha)g$ in $K_P \cong \mathbb{F}_{q^d}$ via the polynomial basis $\{1, \gamma, \ldots, \gamma^{d-1}\}$.

(2-2) If $b(\alpha) - a(\alpha)g \in S_\alpha$, go back to (2-1), and choose another sample.

If $b(\alpha) - a(\alpha)g \in S_\alpha$ for all $(\overline{a}, \overline{b})$, replace G by $G \cup \{g\}$.

(3) If G consists of just one element g, then we have $g = s(\alpha)$.

In Algorithm 4.1.1, we give a pseudocode to conduct the above procedures.

Algorithm 4.1.1 General-case Attack to find $s(\alpha)$

Input: an irreducible polynomial $P \in \mathbb{F}_q[x]$ of degree d, a solution α of order r to P in $K_P := \mathbb{F}_q[x]/\langle P \rangle \cong \mathbb{F}_{q^d}$, and an integer $\ell \geq 2$

Output: $s(\alpha) \in K_P = \mathbb{F}_q[x]/\langle P \rangle \cong \mathbb{F}_{q^d}$

Write $n = n'r + r'$ for $n', r' \in \mathbb{Z}$ with $0 \leq r' \leq r - 1$
$S_\alpha \leftarrow$ the set of elements of the form (4.1.2)
Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as + e}) \in P_q \times P_q$ with $a(\alpha) \neq 0$
$G \leftarrow \emptyset$
for $g \in K_P$ **do**
  $appendflag \leftarrow 1$
  for $(\overline{a}, \overline{b})$ in the collection of samples **do**
    Compute $a(\alpha)$, $b(\alpha)$ and $b(\alpha) - a(\alpha)g$ in K_P
    if $b(\alpha) - a(\alpha)g \notin S_\alpha$ **then**
      $appedflag \leftarrow 0$
      break $(\overline{a}, \overline{b})$
    end if
  end for
  if $appendflag = 1$ **then**
    $G \leftarrow G \cup \{g\}$
  end if
  if $\#G \geq 2$ **then**
    return INSUFFICIENT SAMPLES
  end if
end for
return the element g of G

We can give another version of Algorithm 4.1.1 as follows:

(0) Access to the PLWE oracle to get ℓ PLWE samples $(\overline{a}, \overline{b} = \overline{as + e}) \in P_q \times P_q$ satisfying $a(\alpha) \neq 0$.

(1) Compute the set S_α of elements of the form (4.1.2). Note that each element of S_α is represented by the polynomial basis $\{1, \gamma, \ldots, \gamma^{d-1}\}$ with $\mathbb{F}_q$-coefficients, where $\gamma := x + \langle P \rangle$. Let $G := \emptyset$.

(2) Choose one sample $(\overline{a}, \overline{b})$, we conduct the following sub-procedures:

(2-1) Compute $a(\alpha)$, $b(\alpha)$ and $a(\alpha)^{-1}$ in K_P via the polynomial basis $\{1, \gamma, \ldots, \gamma^{d-1}\}$.

(2-2) For each $h \in S_\alpha$, compute $g := a(\alpha)^{-1}(b(\alpha) - h)$ in $K_P \cong \mathbb{F}_{q^d}$. Let G' be the set of all values g computed as above.

(2-3) If $G \cap G'$ consists of just one element g, then we have $s(\alpha) = g$. Otherwise replace G by $G \cap G'$. Go back to the beginning of (2), and then choose another sample.

In Algorithm 4.1.2, we give a pseudocode to conduct the above procedures.

Algorithm 4.1.2 Another version of General-case Attack to find $s(\alpha)$

Input: an irreducible polynomial $P \in \mathbb{F}_q[x]$ of degree d, a solution α of order r to P in $K_P := \mathbb{F}_q[x]/\langle P \rangle \cong \mathbb{F}_{q^d}$, and an integer $\ell \geq 2$

Output: $s(\alpha) \in K_P = \mathbb{F}_q[x]/\langle P \rangle \cong \mathbb{F}_{q^d}$

Write $n = n'r + r'$ for $n', r' \in \mathbb{Z}$ with $0 \leq r' \leq r - 1$
$S_\alpha \leftarrow$ the set of elements of the form (4.1.2)
Access to the PLWE oracle to obtain ℓ PLWE samples $(\overline{a}, \overline{b} := \overline{as + e}) \in P_q \times P_q$ with $a(\alpha) \neq 0$
$G \leftarrow K_P$
for $(\overline{a}, \overline{b})$ in the collection of samples **do**
  Compute $a(\alpha)$, $a(\alpha)^{-1}$ and $b(\alpha)$ in K_P
  $G' \leftarrow \emptyset$
  for $h \in S_\alpha$ **do**
    $g \leftarrow a(\alpha)^{-1}(b(\alpha) - h)$
    $G' \leftarrow G' \cup \{g\}$
  end for
  $G \leftarrow G \cap G'$
  if $\#G \leq 1$ **then**
    break $(\overline{a}, \overline{b})$
  end if
end for
if $G = \{g\}$ **then**
  return g
else
  return INSUFFICIENT SAMPLES
end if

Once one gets $s(\alpha) \in K_P$, one can also compute $s(\alpha^{q^k})$ for $1 \leq k \leq d_1 - 1$ as follows: Writing $s(x) = \sum_{j=0}^{n-1} s_j x^j$ for $s_j \in \mathbb{F}_q$, we have

$$s(\alpha^{q^k}) = \sum_{j=0}^{n-1} s_j (\alpha^j)^{q^k} = \sum_{j=0}^{n-1} s_j^{q^k} (\alpha^j)^{q^k} = \left(\sum_{j=0}^{n-1} s_j \alpha^j \right)^{q^k} = s(\alpha)^{q^k}$$

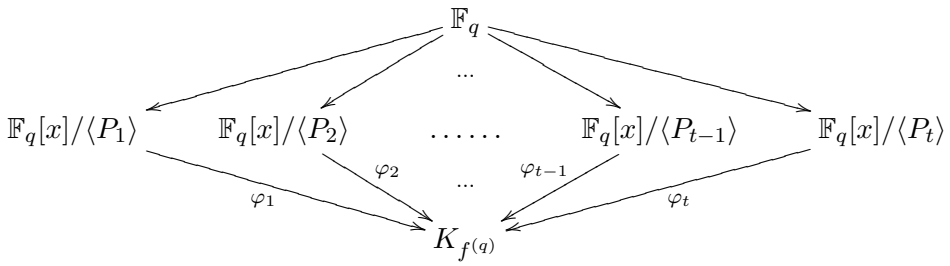
since the characteristic is q.

Next choose P_2, put $K_{P_2} := \mathbb{F}_q[x]/\langle P_2 \rangle \cong \mathbb{F}_{q^{d_2}}$ and let $\alpha_2 \in K_{P_2}$ be a root of P_2. In the same way as $s(\alpha) = s(\alpha_1)$, one can compute $s(\alpha_2^{q^k}) = s(\alpha_2)^{q^k}$ in K_{P_2} for $0 \leq k \leq d_2 - 1$. Similarly we can compute $s(\alpha_i^{q^k}) = s(\alpha_i)^{q^k}$ for $3 \leq i \leq t$ and $0 \leq k \leq d_i - 1$, where $K_{P_i} := \mathbb{F}_q[x]/\langle P_i \rangle \cong \mathbb{F}_{q^{d_i}}$ and $\alpha_i \in K_{P_i}$ is a root of P_i.

With $s(\alpha_i^{q^k}) = s(\alpha_i)^{q^k} \in K_{P_i}$ as above, we recover $s(x) \in \mathbb{F}_q[x]$. Let d' be the least common multiple of $d_1, \ldots, d_t$. Choose an irreducible polynomial $Q \in \mathbb{F}_q[x]$ of degree d', and put $K_{f^{(q)}} := \mathbb{F}_q[x]/\langle Q \rangle \cong \mathbb{F}_{q^{d'}}$, which is a smallest splitting field of $f^{(q)}$ over $\mathbb{F}_q$. For each $1 \le i \le t$, let β_i be a root of P_i in $K_{f^{(q)}}$, $K_i := \{c \in K_{f^{(q)}} : c^{q^{d_i}} = c\} \cong \mathbb{F}_{q^{d_i}}$ and define the field homomorphism

$$\varphi_i : \mathbb{F}_q[x]/\langle P_i \rangle \to K_i \subset K_{f^{(q)}} \ ; \ \gamma_i := x + \langle P_i \rangle \mapsto \beta_i.$$

Note that $\gamma_i^{q^k}$'s are roots of P_i, and thus φ_i sends the set of all roots of P_i in K_{P_i} to that in K_i. In particular, $\varphi_i(\alpha_i) \in K_i$ is a root of P_i. Each $\mathbb{F}_q[x]/\langle P_i \rangle$ is embedded into $K_{f^{(q)}}$ via φ_i.



With this embedding, one can obtain $s(\varphi_i(\alpha_i)^{q^k})$ as follows: Writing

$$s(\alpha_i^{q^k}) = s_{k,d_i-1}^{(i)} \gamma_i^{d_i-1} + \cdots + s_{k,1}^{(i)} \gamma_i + s_{k,0}^{(i)}$$

for $s_{k,j}^{(i)} \in \mathbb{F}_q$, we have

$$\varphi_i(s(\alpha_i^{q^k})) = s_{k,d_i-1}^{(i)} \beta_i^{d_i-1} + \cdots + s_{k,1}^{(i)} \beta_i + s_{k,0}^{(i)}.$$

We also have

$$s(\varphi_i(\alpha_i)^{q^k}) = \sum_{j=0}^{n-1} s_j \varphi_i(\alpha_i^{q^k})^j = \varphi_i \left(\sum_{j=0}^{n-1} s_j (\alpha_i^{q^k})^j \right) = \varphi_i \left(s(\alpha_i^{q^k}) \right).$$

Since $\varphi_i(\alpha_i)^{q^k}$'s are all the roots of P_i in K_i, we get $s(\beta) \in K_{f^{(q)}}$ for all roots β of $f^{(q)}$ in $K_{f^{(q)}}$. As a consequence, one can determine $s(x) \in \mathbb{F}_q[x]$ in a similar way to cases where $f^{(q)}$ splits completely in $\mathbb{F}_q[x]$. With notation as above, we conduct the following procedures to find $s(x)$.

(1) Factorize $f^{(q)}$ into

$$f^{(q)}(x) = P_1(x) \cdots P_t(x),$$

where each P_i is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree $d_i \le n$ with $P_i \ne P_j$ for $i \ne j$, and $\sum_{i=1}^t d_i = n$.

(2) Choose an irreducible polynomial $Q \in \mathbb{F}_q[x]$ of degree $d' := \mathrm{lcm}(d_1, \ldots, d_t)$. Put $K_{f^{(q)}} := \mathbb{F}_q[x]/\langle Q \rangle \cong \mathbb{F}_{q^{d'}}$.

(3) For each $1 \le i \le t$, choose $\ell_i \in \mathbb{Z}_{\ge 1}$ and conduct the following five steps:

(3-1) Let $K_{P_i} := \mathbb{F}_q[x]/\langle P_i \rangle \cong \mathbb{F}_{q^{d_i}}$, and compute a root $\alpha \in K_{P_i}$ of P_i and its order r_i. Note that K_{P_i} is a smallest splitting field of P_i over $\mathbb{F}_q$.

(3-2) By Algorithm 4.1.1 (or Algorithm 4.1.2) with the inputs P_i, α_i and ℓ_i, compute $s(\alpha_i) \in K_{P_i}$.

(3-3) For each $0 \leq k \leq d_i - 1$, compute $s_{k,j}^{(i)}$ with $0 \leq j \leq d_i - 1$ such that

$$s(\alpha_i^{q^k}) = \sum_{j=0}^{d_i-1} s_{k,j}^{(i)} \gamma_i^j,$$

where $\gamma_i := x + \langle P_i \rangle$.

(3-4) Compute a root β_i of P_i in $K_i := \{c \in K_{f^{(q)}} : c^{q^{d_i}} = c\} \subset K_{f^{(q)}}$.

(3-5) For each $0 \leq k \leq d_i - 1$, compute

$$s(\varphi_i(\alpha_i)^{q^k}) = \sum_{j=0}^{d_i-1} s_{k,j}^{(i)} \beta_i^j.$$

(4) With $s(\varphi_i(\alpha_i)^{q^k})$ computed in the previous step, construct a linear system on s_j's, and solve it. Return $\sum_{j=0}^{n-1} s_j x^j$.

Remark 4.1.2. One has $\mathrm{ord}(\gamma_i) \geq d_i$. Indeed, if $\mathrm{ord}(\gamma_i) = r \leq d_i - 1$, then $\{1, \gamma_i, \ldots, \gamma_i^{r-1}\}$ forms an $\mathbb{F}_q$-basis of K_{P_i}, and hence $\dim_{\mathbb{F}_q} K_{P_i} = r < d_i$. This is a contradiction.

Remark 4.1.3. One can construct the decision-variant of our extended attack, not assuming any property on $f^{(q)}$ (cf. for the attack in [7], one assumes that f has at least one root in $\mathbb{F}_q$).

Case of $\alpha_i = \gamma_i$ When $\alpha_i = \gamma_i := x + \langle P_i \rangle$, one can compute $s(\alpha_i)$ not using the order of α_i. To simplify the notation, we take $i = 1$, $P = P_1$, $d = d_1$, $K_P = K_{P_1}$ and $\alpha = \alpha_1$. Since $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is an $\mathbb{F}_q$-basis of $K_P = \mathbb{F}_q[x]/\langle P \rangle$, there exist $[\alpha_{i,j}] \in \mathbb{F}_q$ with $\alpha_{i,j} \in (-q/2, q/2] \cap \mathbb{Z}$ for $d \leq i \leq n-1$ and $0 \leq j \leq d-1$ such that

$$\alpha^i \;=\; [\alpha_{i,d-1}]\alpha^{d-1} + \cdots + [\alpha_{i,1}]\alpha + [\alpha_{i,0}]$$

in $\mathbb{F}_q[x]/\langle P \rangle \cong \mathbb{F}_{q^d}$. Writing $e(x) = \sum_{j=0}^{n-1} [e_j] x^j$ with $e_j \in [-2\sigma, 2\sigma] \cap \mathbb{Z}$, one has

$$e(\alpha) = \sum_{j=0}^{d-1} \left[e_j + \sum_{i=d}^{n-1} \alpha_{i,j} e_i \right] \alpha^j.$$

Write $b(\alpha) - a(\alpha)s(\alpha) = \sum_{j=0}^{n-1} [y_j] x^j$ with $y_j \in (-q/2, q/2] \cap \mathbb{Z}$. It follows from

$$b(\alpha) - a(\alpha)s(\alpha) = e(\alpha) \in \mathbb{F}_q[x]/\langle P \rangle \cong \mathbb{F}_{q^d}$$

that the equalities

$$[y_j] = \left[e_j + \sum_{i=d}^{n-1} \alpha_{i,j} e_i \right] \text{ for } 0 \leq j \leq d-1$$

Algorithm 4.1.3 General Attack

Input: an irreducible polynomial $f \in \mathbb{Z}[x]$ of degree n
Output: $s(x) \in \mathbb{F}_q[x]$

Factorize $f^{(q)}$ to a product of irreducible factors $f^{(q)} = P_1 \cdots P_t$ with $d_i = \deg(P_i)$
$d' \leftarrow \mathrm{lcm}(d_1, \ldots, d_t)$
Choose an irreducible polynomial $Q \in \mathbb{F}_q[x]$ of degree d'
$K_{f^{(q)}} \leftarrow \mathbb{F}_q[x]/\langle Q \rangle$
for $i = 1$ **to** t **do**
  Choose a root $\alpha_i \in K_{P_i} := \mathbb{F}_q[x]/\langle P_i \rangle$ of P_i with order r_i
  Compute $g'_{i,0} := s(\alpha_i) \in K_{P_i}$ by Algorithm 4.1.1 (or Algorithm 4.1.2)
  Compute $g'_{i,k} := s(\alpha_i^{q^k}) = s(\alpha_i)^{q^k}$, and write $g'_{i,k} = \sum_{j=0}^{d_i-1} s_{k,j}^{(i)} \gamma_i^j$ for $1 \le k \le d_i - 1$
  Compute a root β_i of P_i in $K_i := \{c \in K_{f^{(q)}} : c^{q^{d_i}} = c\} \subset K_{f^{(q)}}$
  Compute $g_{i,k} := s(\varphi_i(\alpha_i)^{q^k}) = \sum_{j=0}^{d_i-1} s_{k,j}^{(i)} \beta_i^j$
end for
for $i = 1$ **to** t **do**
  for $k = 0$ **to** $d_i - 1$ **do**
    for $j = 1$ **to** n **do**
      $a_{i+k,j} \leftarrow (\varphi_i(\alpha_i)^{q^k})^{n-j}$
    end for
  end for
end for
$A \leftarrow (a_{i,j})_{i,j}$
$\mathbf{s} \leftarrow A^{-1} \cdot {}^t[g_{1,0}, \ldots, g_{1,d_1-1}, \ldots, g_{t,0}, \ldots, g_{t,d_t-1}]$
$s'(x) \leftarrow 0$
Write ${}^t\mathbf{s} = (s'_{n-1}, \ldots, s'_0)$
return $s'(x) = \sum_{j=0}^{n-1} s_j x^j$

hold over $\mathbb{F}_q$. Recall that each e_i is sampled from $\mathcal{G}_\sigma$. Thus $e_j + \sum_{i=d}^{n-1} \alpha_{i,j} e_i$ is sampled from $\mathcal{G}_{\sigma'}$, where

$$(\sigma')^2 = \sigma^2 + \sum_{i=d}^{n-1} \alpha_{i,j}^2 \sigma^2.$$

Thus one has

$$|y_j| \le B(\alpha)_j := 2\sigma \sqrt{1 + \sum_{i=d}^{n-1} \alpha_{i,j}^2}.$$

Thus, $b(\alpha) - a(\alpha)s(\alpha) = e(\alpha)$ is included in the set S_α of elements of the form

$$[\ell_0] + [\ell_1]\alpha + \cdots + [\ell_{d-1}]\alpha^{d-1}, \tag{4.1.2}$$

where $\ell_j \in [-B(\alpha)_j, B(\alpha)_j] \cap \mathbb{Z}$ for $0 \le j \le d-1$. The cardinality $\#S_\alpha$ is bounded by $\Pi_{j=0}^{d-1} 2B(\alpha)_j$. With notation as above, we take the following procedures to find $s(\alpha) \in K_P$. Let ℓ be the number of samples.

(0) Construct $K_P := \mathbb{F}_q[x]/\langle P \rangle \cong \mathbb{F}_{q^d}$. Note that K_P is a minimal splitting field of P over $\mathbb{F}_q$. Let $\alpha := x + \langle P \rangle$.

(1) Compute $[\alpha_{i,j}] \in \mathbb{F}_q$ with $\alpha_{i,j} \in (-q/2, q/2] \cap \mathbb{Z}$ for $d \leq i \leq n-1$ and $0 \leq j \leq d-1$ such that

$$\alpha^i = \sum_{j=0}^{d-1} [\alpha_{i,j}] \alpha^j$$

in $K_P = \mathbb{F}_q[x]/\langle P \rangle \cong \mathbb{F}_{q^d}$.

(2) Access to the PLWE oracle to get ℓ PLWE samples $(\overline{a}, \overline{b} = \overline{as+e}) \in P_q \times P_q$ satisfying $a(\alpha) \neq 0$. Let $G := \emptyset$.

(3) For each $g \in K_P$, we conduct the following sub-procedures:

(3-1) Choose one sample $(\overline{a}, \overline{b})$. Compute $a(\alpha)$ and $b(\alpha)$ via the polynomial basis $\{1, \alpha, \ldots, \alpha^{d-1}\}$.

(3-2) Compute $y_j \in (-q/2, q/2] \cap \mathbb{Z}$ for $0 \leq j \leq d-1$ such that

$$b(\alpha) - a(\alpha)g = \sum_{j=0}^{d-1} [y_j] \alpha^j$$

in $K_P \cong \mathbb{F}_{q^d}$.

(3-3) If $b(\alpha) - a(\alpha)g \in S_\alpha$, i.e.,

$$|y_j| \leq B(\alpha)_j := 2\sigma \sqrt{1 + \sum_{i=d}^{n-1} \alpha_{i,j}^2}$$

for all $0 \leq j \leq d-1$, go back to (3-1), and choose another sample.

If $b(\alpha) - a(\alpha)g \in S_\alpha$ for all $(\overline{a}, \overline{b})$, replace G by $G \cup \{g\}$.

(4) If G consists of just one element g, then we have $g = s(\alpha)$.

4.2 Complexity Analysis of Our Extended Attacks

In this subsection, we investigate the complexity of our extended attack proposed in the previous subsection (Section 4.1). Assume $d_i \ll n$, and we do not count the computation of the order of an element in a group. We also assume $\#S_{\alpha_i} < q^{d_i}$ for all $\alpha_i \in K_{P_i}$. First, we determine the complexities of Algorithms 4.1.1 and 4.1.2. Note that the computation in K_{P_i} is done with the polynomial basis $\{1, \gamma_i, \ldots, \gamma_i^{d_i-1}\}$.

Complexities of Algorithms 4.1.1 and 4.1.2 Let us first estimate the complexity of Algorithm 4.1.1. It requires $O(r)$ multiplications over $K_P \cong \mathbb{F}_{q^d}$ to compute all α^i for $0 \leq i \leq r-1$. Each element in S_α is computed by combining $O(r)$ multiplications and $O(r)$ additions, so that it requires $O(r)$ arithmetic operations over $K_P \cong \mathbb{F}_{q^d}$. By our assumption, S_α has at most q^d elements. Hence we compute S_α in $O(r + rq^d) = O(rq^d)$ arithmetic operations over $K_P \cong \mathbb{F}_{q^d}$.

The main double loop has at most $q^d \ell$ iterations. For each iteration, we compute $h := b(\alpha) - ga(\alpha)$ and decide whether $h \in S_\alpha$ or not. With α^i computed as above, computing $b(\alpha)$ and $a(\alpha)$ needs $2n+2n = O(n)$ arithmetic operations over $K_P \cong \mathbb{F}_{q^d}$. Using a binary search to decide whether

$h \in S_\alpha$ or not, we do this in $O(\log(q^d)) = O(d\log(q))$ operations. Summing up, each iteration takes $O(n + d\log(q))$ arithmetic operations over $K_P \cong \mathbb{F}_{q^d}$, and thus $O(q^d \ell n + q^d \ell d \log(q))$ is required in total.

As a consequence, Algorithm 4.1.1 performs in $O(rq^d + q^d \ell n + q^d \ell d \log(q)) = O(q^d \ell n + q^d \ell d \log(q))$ arithmetic operations over $K_P \cong \mathbb{F}_{q^d}$, i.e.,

$$O\left(nq^d \ell d^2 \log^2(q) + q^d \ell d^3 \log^3(q)\right)$$

bit operations

Similarly, it follows that Algorithm 4.1.2 terminates in

$$O\left((n-d)d^2(\log(q))^2 + \ell(d(n-d) + q^d d^2)(\log(q))^2\right)$$

bit operations.

Complexity of Algorithm 4.1.3 Let $d = \max_{1 \le i \le t} d_i$. First one factorizes $f^{(q)}$ of degree n over $\mathbb{F}_q$, which requires

$$O(n\log^3(n)\log^3(q))$$

bit operations, see Exercise 2.12.12 of [8].

Second we construct $\mathbb{F}_{q^{d'}}$ with a polynomial basis by generating an irreducible polynomial $Q \in \mathbb{F}_q[x]$ of degree d'. According to Section 2.14.1 of [8], this can be done in

$$O((d')^4 \log^3(q))$$

bit operations, using naive arithmetic.

For each $1 \le i \le t$, we choose one root $\alpha_i \in K_{P_i}$ of P_i. Note that $\gamma_i := x + \langle P_i \rangle$ is a root of P_i in K_{P_i}, and hence the other roots are given by $\gamma_i^{q^k}$ for $1 \le k \le d_i - 1$. Computing $\gamma_i^{q^k}$ for $1 \le k \le d_i - 1$ can be done in $O(d_i q)$ multiplications in K_{P_i}, i.e.,

$$O(d_i^3 q \log^2(q)) = O(d^3 q \log^2(q))$$

bit operations.

For a root $\alpha_i \in K_{P_i}$, we next compute $s(\alpha_i)$. With the complexity estimated in the previous paragraph, one can estimate that this can be done in

$$O\left(nq^d \ell d^2 \log^2(q) + q^d \ell d^3 \log^3(q)\right)$$

bit operations, where $\ell := \max_{1 \le i \le t} \ell_i$.

With $s(\alpha_i)$ computed as above, one computes $s(\alpha_i^{q^k}) = s(\alpha_i)^{q^k}$ for $1 \le k \le d_i - 1$ in

$$O(d_i q d_i^2 \log^2(q)) = O(d^3 q \log^2(q))$$

bit operations.

Finding one root $\beta_i \in K_i \subset K_{f^{(i)}} \cong \mathbb{F}_{q^{d'}}$ of P_i with $\deg(P_i) = d_i$ can be done in

$$O\left(\log(q^{d'})\log(d_i) d_i^2 (d')^2 \log^2(q)\right) = O\left((d')^3 d^2 \log(d) \log^3(q)\right)$$

bit operations, see Exercise 2.12.5 in [8].

Computing β_i^k for $1 \leq k \leq d_i - 1$ can be done in $O(d_i)$ multiplications in $K_{f^{(q)}} \cong \mathbb{F}_{q^{d'}}$, i.e.,

$$O(d_i(d')^2\log^2(q)) = O(d(d')^2\log^2(q))$$

bit operations. We next compute $s(\varphi_i(\alpha)^{q^k})$ for $0 \leq k \leq d_i - 1$. For each $0 \leq k \leq d_i - 1$, it requires $O(d_i)$ multiplications and $O(d_i)$ additions to compute $s(\varphi_i(\alpha)^{q^k})$. Hence computing $s(\varphi_i(\alpha)^{q^k})$ for $0 \leq k \leq d_i - 1$ requires

$$O(d_i^2(d')^2\log^2(q)) = O(d^2(d')^2\log^2(q))$$

bit operations.

Considering t iterations, the **for**-loop indicated at the 5-th line terminates in

$$O\left(tnq^d\ell d^2\log^2(q) + tq^d\ell d^3\log^3(q) + td^2(d')^3\log(d)\log^3(q) + td^2(d')^2\log^2(q)\right)$$

bit operations.

It requires

$$O(n^3(d')^2\log^2(q) + tqd(d')^2\log^2(q))$$

bit operations to compute A^{-1} and $\varphi_i(\alpha_i)^{q^k}$'s.

Putting all the steps together, we can determine the binary complexity of our attack, that is,

$$O\left(n\log^3(n)\log^3(q) + (d')^4\log^3(q) + tnq^d\ell d^2\log^2(q) + tq^d\ell d^3\log^3(q) + td^2(d')^3\log(d)\log^3(q) + tqd^2(d')^2\log^2(q) + n^3(d')^2(\log(q))^2\right).$$

Consequently, if d is small enough, our attack terminates in polynomial time with respect to all the parameters n, q, d', t and ℓ.

4.3 Vulnerable polynomials by our general-case attack

We use the same notation as in the previous subsections (Sections 4.1 and 4.2). In this subsection, we characterize defining polynomials for which the search-PLWE problem is solvable by our general-case attack. Let $n \in \mathbb{Z}_{\geq 1}$, $\sigma \in \mathbb{R}_{>0}$ and q a prime. As showed in the previous subsections, the PLWE instances defined by monic polynomials $f \in \mathbb{Z}[x]$ of degree n satisfying the following conditions can be vulnerable by Algorithm 4.1.3:

V1' $f^{(q)}(x) \in \mathbb{F}_q[x]$ is a square-free polynomial over $\overline{\mathbb{F}_q}$, the algebraic closure of $\mathbb{F}_q$,

V2' For each $1 \leq i \leq t$, there exists $\alpha_i \in K_{P_i}$ such that $\#S_{\alpha_i} < q^d$.

where each S_{α_i} is determined by n, σ, α_i and q. Hence for an integer n, $\sigma \in \mathbb{R}_{>0}$, a prime q, and

$$f \in \mathcal{F}'_{n,\sigma,q} := \{f \in \mathbb{Z}[x] : f \text{ is monic with } \deg(f) = n \text{ and } f \text{ satisfies } \textbf{V1'} \text{ and } \textbf{V2'}\},$$

the search-PLWE problem is solvable with sufficiently high probability by Algorithm 4.1.3.

5 Conclusion and Future works

In this paper, we first gave a search-case variant of Eisentraeger et al.'s attacks against the decision Poly-LWE problem, and showed that the search-case variant of their attacks do not seem to work well for cases where the defining polynomial f of the PLWE instances does not split completely over the ground field $\mathbb{F}_q$. Based on the theory of finite fields, we proposed a new attack, which is viewed as an generalization of the variant to deal with more general cases where f does not necessarily split completely in $\mathbb{F}_q[x]$. We also proved that when f has a square-free factorization of low degree-factors with certain conditions, this attack terminates in polynomial time with respect to the degree of f and q. With our attack, we have new insecure classes of defining polynomials f and parameters q in the PLWE problem, which shall be a useful information to design more secure cryptosystms, furthermore quantum-resistant cryptosystems.

However, our extended attack takes much time if f has high degree-factors, and thus using such an f as the defining polynomial might be still secure in the PLWE problem. Our future work is to investigate the security of PLWE instances adopting such polynomials, which is an important task to develop PLWE-based cryptosystems.

Acknowledgments

The author deeply thanks Hart Montgomery for many helpful comments and discussions on this study. The author also thanks Arnab Roy, Avradip Mandal and his supervisor Masaya Yasuda for helpful comments on this study. This work was supported by Fujitsu Laboratories of America, Inc..

References

[1] V. Boža, *Experimental Comparison of Set Intersection Algorithms for Inverted Indexing*, ITAT 2013 Proceedings, CEUR Workshop Proceeding, Vol. **1003**, pp. 58–64, 2013.

[2] Z. Brakerski, C. Gentry and V. Vaikuntanathan, *Fully homomorphic encryption without bootstrapping*, ACM Trans. Comput. Theory **6** (2014), no. 3, Art. 13, 36 pages.

[3] Z. Brakerski, A. Langlois, C. Peikert, O. Regev and D. Stehlé, *Classical Hardness of Learning with Errors*, In: Proceedings of the 2013 ACM Symposium on Theory of Computing (STOC'13), pp. 575–584, ACM, New York, 2013.

[4] Z. Brakerski and V. Vaikuntanathan, *Fully homomorphic encryption from Ring-LWE and security for key dependent messages*, In: Proceedings of CRYPTO 2011, Lecture Notes in Computer Science, Volume **6841**, pp. 505–524. Springer, 2011.

[5] L. Ducas and A. Durmus, *Ring-LWE in Polynomial Ring*, In: Proceedings of PKC 2012, Lecture Notes in Computer Science, Volume **7293**, pp. 34–51, 2012.

[6] K. Eisentraeger, S. Hallgren and K. Lauter, *Weak Instances of PLWE*, IACR Cryptology ePrint archive 2014/784.

[7] Y. Elias, K. E. Lauter, E. Ozman and K. E. Stange, *Provably weak instances of Ring-LWE*, IACR Cryptology ePrint archive 2015/106.

[8] S. D. Galbraith, *Mathematics of Public Key Cryptography*, Cambridge University Press, 2012.

[9] C. Gentry, S. Halevi and N. P. Smart, *Fully homomorphic encryption with polylog overhead*, In: Advances in Cryptology-EUROCRYPT 2012, Lecture Notes in Computer Science, Volume **7237**, pp. 465–482, Springer, Heidelberg.

[10] V. Lyubashevsky, C. Peikert and O. Regev, *On ideal lattices and learning with errors over rings*, In: Advances in Cryptology-EUROCRYPT 2010, Lecture Notes in Computer Science, Volume **6110**, pp. 1–23, Springer, Berlin, 2010.

[11] D. Micciancio and O. Regev, *Lattice-based cryptography*, In: Proceedings of Post Quantum Cryptography, pp. 147–191, Springer, 2009.

[12] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, J. ACM, **56** (6), pp. 1–40, 2009.