PAPER Special Section on Information and Communication System Security

On the Weakness of Non-Dual Ring-LWE Mod Prime Ideal $\mathfrak{q}$ by Trace Map

Tomoka TAKAHASHI[†a)], **Shinya OKUMURA**[†b)], *Nonmembers*, *and* **Atsuko MIYAJI**[†c)], *Member*

SUMMARY The recent decision by the National Institute of Standards and Technology (NIST) to standardize lattice-based cryptography has further increased the demand for security analysis. The Ring-Learning with Error (Ring-LWE) problem is a mathematical problem that constitutes such lattice cryptosystems. It has many algebraic properties because it is considered in the ring of integers, R, of a number field, K. These algebraic properties make the Ring-LWE based schemes efficient, although some of them are also used for attacks. When the modulus, q, is unramified in K, it is known that the Ring-LWE problem, to determine the secret information $s \in R/qR$, can be solved by determining $s \pmod{\mathfrak{q}} \in \mathbb{F}_{q^f}$ for all prime ideals $\mathfrak{q}$ lying over q. The χ^2-attack determines $s \pmod{\mathfrak{q}} \in \mathbb{F}_{q^f}$ using chi-square tests over $R/\mathfrak{q} \cong \mathbb{F}_{q^f}$. The χ^2-attack is improved in the special case where the residue degree f is two, which is called the two-residue-degree χ^2-attack. In this paper, we extend the two-residue-degree χ^2-attack to the attack that works efficiently for any residue degree. As a result, the attack time against a vulnerable field using our proposed attack with parameter $(q, f) = (67, 3)$ was 129 seconds on a standard PC. We also evaluate the vulnerability of the two-power cyclotomic fields.

key words: *Ring-LWE, prime ideal, trace map, attack*

1. Introduction

Lattice-based cryptography has received a great deal of attention, with the standardization of post-quantum cryptography by the National Institute of Standards and Technology (NIST). On July 5, 2022, four candidate algorithms were selected for standardization [1], among which CRYSTALS-KYBER [2], CRYSTALS-Dilithium [3], and FALCON [4] were lattice-based cryptography. This evidence indicates that lattice-based cryptography has attracted considerable attention. The Learning with Errors (LWE) problem [5] finds a solution to a linear system of equations with errors in the finite field, which is used to construct lattice-based cryptography. The Ring-Learning with Errors (Ring-LWE) problem [6] and the Module-Learning with Errors (M-LWE) problem [7], [8], which are LWE problems with ring structure, are known to be more efficient than the normal LWE problem.

In LWE problems with ring structures, it is common to use the cyclotomic field as the number field, e.g., the NIST candidates based on Ring-LWE problem, NewHope [9] and LAC [10], and M-LWE problem base application CRYSTALS-KYBER [2] and CRYSTALS-Dilithium [3]. On the other hand, it is also known that a more efficient homomorphic encryption scheme can be constructed by using a subfield of a cyclotomic field [11]. Therefore, it is necessary to analyze the difficulty of LWE problems with ring structure over general number fields. In addition, since the reduction from M-LWE to Ring LWE was shown in [12], [13], this research focuses on a security analysis of the Ring-LWE problem.

Let R be the ring of integers of a number field, K. The Ring-LWE problem is a problem defined on the quotient ring, $R_q = R/qR$, of the ring of integers by the modulus q, where determines the $s \in R_q$ from a given Ring-LWE samples, $(a_i, b_i = a_i s + e_i) \in R_q \times R_q$. In this case, $a_i \in R_q$ is sampled uniformly at random, and $e_i \in R$ is sampled from small elements. Applications that use Ring-LWE problem allow Ring-LWE samples to be obtained from the public keys or ciphertexts [6], [10]. These applications have higher security levels by increasing the extension degree $[K : \mathbb{Q}]$.

The main attack strategies against the Ring-LWE problem include attacks of reduction to the LWE problem [14], [15], and attacks using error distribution bias [16]–[18].

The attacks of reduction to LWE problem [14], [15] are performed using a reduction algorithm such as LLL [19] and BKZ [20]. While these attacks are possible with 1 or 2 Ring-LWE samples, the success probability and attack time strongly depend on the extension degree due to the reduction algorithm's property.

If the modulus q is unramified in K, Ring-LWE problem can be converted to Ring-LWE $\pmod{\mathfrak{q}}$ problem that finds $s \pmod{\mathfrak{q}} \in \mathbb{F}_{q^f}$ from $(a_i \pmod{\mathfrak{q}}, b_i \pmod{\mathfrak{q}}) \in \mathbb{F}_{q^f} \times \mathbb{F}_{q^f}$. Here f is called the residue degree and is uniquely determined by the number field K and the modulus q. In [16]–[18], which uses the distribution bias of the error $e_i \pmod{\mathfrak{q}} \in \mathbb{F}_{q^f}$, chi-square tests are used to find $s \pmod{\mathfrak{q}} \in \mathbb{F}_{q^f}$. Since the success probability and attack time depend strongly on the residue degree f and the error distribution, it can be an effective attack even for large extension degrees. On the other hand, the chi-square test requires a large number of samples for the attack. It is easy to obtain sufficient Ring-LWE samples of the same secret in applications, so proper error sampling is necessary to avoid the attack.

The χ^2-attack proposed in [16] assumes the distribution of $e_i \pmod{\mathfrak{q}} \in \mathbb{F}_{q^f}$ is distinguishable from the uniform distribution on $\mathbb{F}_{q^f}$. The χ^2-attack requires $O(q^f)$ samples

Manuscript received November 9, 2022.
Manuscript revised April 2, 2023.
Manuscript publicized July 13, 2023.

[†]The authors are with Graduate School of Engineering, Osaka University, Suita-shi, 565–0871 Japan.
a) E-mail: takahashi.tomoka@megachips.co.jp
b) E-mail: okumura@comm.eng.osaka-u.ac.jp
c) E-mail: miyaji@comm.eng.osaka-u.ac.jp

DOI: 10.1587/transinf.2022ICP0017

since chi-square tests are performed in $\mathbb{F}_{q^f}$. Furthermore, the χ^2-attack is a brute force attack, which is not an efficient attack. However, the χ^2-attack was improved in the case where the residue degree f is two in [17], which is called the two-residue-degree χ^2-attack. Then, the coset $\mathbb{F}_{q^2}/\mathbb{F}_q$ can reduce the number of statistical tests, and performing chi-square tests on $\mathbb{F}_q$ using the Frobenius map can reduce the number of samples from $O(q^2)$ to $O(q)$.

In our preliminary work [18], we extended the two-residue-degree χ^2-attack to the prime-residue-degree and the composite-number-residue-degree χ^2-attack by using the trace map instead of the Frobenius map. Thus, the χ^2-attack can efficiently work in not just those two but also any residue-degree case. Both cases require certain conditions, but the composite fields, $\mathbb{Q}(\zeta_p, \sqrt[4]{d})$, have been shown to be vulnerable to these attacks. The number of operations in $\mathbb{F}_q$ of the trace map from $\mathbb{F}_{q^f}$ to $\mathbb{F}_q$ under the aforementioned conditions can be reduced from $O((n^{1.67} + \log(q)n(\log(n))\log\log(n)) \cdot \log(n))$ to $O(1)$. This allows for efficient attacks. In the χ^2-attack, it took unrealistic time to solve the Ring-LWE (mod $\mathfrak{q}$) problem even with the small parameters used in the experiments. These problems can be resolved using our attacks in a matter of hours on a standard PC.

This paper is the full version of [18]. Compared with our preliminary work [18], the following parts are added and improved:

1. We merged the prime-residue-degree and the composite-number-residue-degree χ^2-attack into one generalized attack. The generalized attack also efficiently works for two-residue-degree which is the target in [17].
2. We evaluate the security of the two-power cyclotomic fields. The results show that our attack over the composite fields works more effectively than that over the two-power cyclotomic fields. The fact that the NIST candidate for standardization chooses the two-power cyclotomic fields rather than the composite fields reflects our results. However, careful error sampling is necessary over any number fields.

Our paper is organized as follows. Section 2 describes the algebraic and lattice problems required in this study, including the Ring-LWE (mod $\mathfrak{q}$) attack methods and their security analysis. Section 3 describes our proposed attack method. Section 4 shows the existence of number fields that are vulnerable to the attack, and presents the experimental comparison between the χ^2-attack and the proposed attack on the vulnerable fields. Section 5.2 shows that the two-power cyclotomic fields are secure to the proposed attack, and Sect. 6 concludes the paper.

2. Preliminary

This section describes the mathematical facts required for this study. We also explain the attack methods on the Ring-LWE (mod $\mathfrak{q}$) problem [6], [16] and their security analysis [21], which are used as a reference for our research.

2.1 Algebra and Statistical Background

In this subsection, we describe the algebraic knowledge and Pearson's chi-square test used in the attack.

Suppose that L is an extension of the field K. Let $\mathrm{Aut}(L/K)$ be the group of all K-isomorphisms from L to L. When an algebraic extension L/K is normal and separable, L/K is called a Galois extension, and $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$ is called the Galois group of L/K. In particular, when $\mathrm{Gal}(L/K)$ is a cyclic group, the corresponding Galois extension L/K is called cyclic extension.

Suppose $q = p^k$ for prime number p and $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a finite cyclic extension of degree n. Then, $\sigma\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}; \alpha \mapsto \alpha^q$ is a generator of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, and there exists an irreducible polynomial $g(x) \in \mathbb{F}_q[x]$ of degree n such that $\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(g(x))$. Arbitrary $\alpha \in \mathbb{F}_{q^n}$ is regarded as a polynomial of degree less than n and can be represented as $\alpha = \sum_{0\le i<n} \alpha_i \xi^i (\alpha_i \in \mathbb{F}_q)$ using the symbol $\xi := x \pmod{g} \in \mathbb{F}_{q^n}$. Suppose d is a divisor of n such that $n = dr$ for some integer r, then $\mathbb{F}_{q^d}$ is a subfield of $\mathbb{F}_{q^n}$, and $\mathbb{F}_q \subset \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$ is a finite separable extension. Arbitrary $\beta \in \mathbb{F}_{q^d}$ can be represented as $\beta = \sum_{0\le i<n,\ r|i} \beta_i \xi^i (\beta_i \in \mathbb{F}_q)$.

In this study, the computational complexity is evaluated in terms of the number of operations in $\mathbb{F}_q$ (sum, subtraction, multiplication, and division). For $\alpha, \beta \in \mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(g(x))$, the sum or subtraction $\alpha \pm \beta \pmod{g(x)}$ takes $O(n)$ operations in $\mathbb{F}_q$, and the multiplication $\alpha \cdot \beta \pmod{g(x)}$ takes $O(M(n))$ operations in $\mathbb{F}_q$. The division $\alpha/\beta \pmod{g(x)}$ takes $O(M(n)\log n)$ operations in $\mathbb{F}_q$, and $\alpha^q \pmod{g(x)}$ takes $O(M(n)\log q)$ operation. Here, the symbol $M(n)$ denotes the upper bound of the operations in $\mathbb{F}_q$ on the multiplication of two polynomials of degree n over $\mathbb{F}_q$, $M(n) = O(n(\log n)\log\log n)$. The symbol $C(n)$ denotes the upper bound of the modular polynomial composition of operations, $C(n) = O(n^{1.67})$ [22].

Our attack used the trace map to perform chi-square tests over $\mathbb{F}_q$.

Definition 1 (Trace map)**.** *Suppose L/K is a separable extension of degree n, and $\bar{K}$ is the algebraic closure of K containing L. Let $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ be the entire K-isomorphisms from L to $\bar{K}$. Then, the trace map from L to K is defined as*

$$\mathrm{Tr}_{L/K}(\alpha) := \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha).$$

The trace map is an additive homomorphism, $\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$ for $\forall \alpha, \beta \in L$. For $\gamma \in K$, we have $\mathrm{Tr}_{L/K}(\gamma \cdot \alpha) = \gamma \cdot \mathrm{Tr}_{L/K}(\alpha)$. If L/M and M/K are a finite separable extension, $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{M/K}(\mathrm{Tr}_{L/M}(\alpha))$. The trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^d}$ is $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(\alpha) = \alpha + \alpha^{q^d} + \alpha^{q^{2d}} + \cdots + \alpha^{q^{(r-1)d}}$ and $\mathrm{Tr}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}(\alpha)) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$.

Kaltofen et al. proposed the trace-like map algorithm to determine $\mathrm{Tr}_{\mathbb{F}_{q^d}/\mathbb{F}_p}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{kd-1}}$ in [22],

where α is a random element in $\mathbb{F}_q[x]/(g(x))$. It requires $O((nC(k) + C(n)M(k) + \log(p)M(n)M(k))\ \log(kd))$ operations in $\mathbb{F}_p$. In the special case where $k = 1, d = n$ and $g(x)$ is a monic irreducible polynomial, the trace-like map is equivalent to the trace map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, which can be computed by $O((C(n) + \log(p)M(n))\log(n))$ operations in $\mathbb{F}_p$.

Pearson's Chi-square Test

Pearson's chi-square test is a statistical hypothesis test in which a hypothesis is proven from the given samples [23], [24]. Suppose that a finite set, S, is divided into subsets $S_1, S_2, \cdots, S_r$. Let p_i be the probability that samples from the assumed distribution are included in S_i. When there are n samples in S, the expected number of samples included in each S_i is $c_i \coloneqq np_i$. If the actual number of samples in subset, S_i, is f_i, then we define the chi-square test statistic, $\chi^2 = \sum_{i=1}^{r} \frac{(f_i - c_i)^2}{c_i}$. For risk ratio α, we set $\delta = F_{r-1}^{-1}(\alpha)$. Here, $F_{r-1}(x)$ is the cumulative distribution function of the χ^2 distribution with $r-1$ degree of freedom. If $\chi^2 < \delta$, the distribution of samples is consistent with the hypothesis, otherwise, we reject the hypothesis.

The chi-square test has the applicability criterion that the expected values $c_i < 5$ should not exceed 20% of the total. The chi-square test requires a sufficient number of samples to satisfy this criterion. Previous works and our proposed attack use chi-square tests under the hypothesis that the given samples in $\mathbb{F}_q$ (or $\mathbb{F}_{q^f}$) are uniformly distributed. Therefore, at least $5 \cdot q$ (or $5 \cdot q^f$) samples are required.

2.2 Discrete Gaussian Distribution

In the security analysis of Ring-LWE problem, more flexible arguments can be done by using the space H. Here, the space H is defined by $H \coloneqq \{(x_1, \cdots x_n)^T \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} : x_{s_1+s_2+j} = \overline{x}_{s_1+j}, 1 \le \forall j \le s_2\} \subseteq \mathbb{C}^n$ for positive integers s_1, s_2 such that $n = s_1 + 2s_2$. For $\boldsymbol{v} = (v_1, \cdots, v_n)^T, \boldsymbol{w} = (w_1, \cdots, w_n)^T \in H$, define the inner product by $\langle \boldsymbol{v}, \boldsymbol{w} \rangle = \sum_{1 \le i \le n} v_i \overline{w_i}$, and the norm by $\|v\| = \langle \boldsymbol{v}, \boldsymbol{v} \rangle$.

Definition 2 (discrete Gaussian distribution)**.** *Let $\rho_r : H \to (0, 1]\ ;\ \boldsymbol{x} \mapsto e^{-\pi\|\boldsymbol{x}\|^2/r^2}$ for $r > 0$. For a lattice $\Lambda \subset H$, the discrete Gaussian distribution over Λ with width r is defined by probability density function*

$$\forall \boldsymbol{x} \in \Lambda,\ D_{\Lambda,r}(\boldsymbol{x}) = \frac{\rho_r(\boldsymbol{x})}{\sum_{\boldsymbol{y} \in \Lambda} \rho_r(\boldsymbol{y})}.$$

The smoothing parameter and the following lemmas are known to describe the properties of the discrete Gaussian distribution. For details, refer to [25].

Lemma 1. *Suppose $\Lambda \subset H$ is a lattice. Let $D_{\Lambda,r}$ denote discrete Gaussian over Λ with a width r. Suppose c is a positive constant such that $c \ge \frac{r}{\sqrt{2\pi}}$. Let $\boldsymbol{v} \in \Lambda$ be a sample from $D_{\Lambda,r}$ and $C_s = s\sqrt{2\pi e} \cdot e^{-\pi s^2}$. Then the following inequality holds:*

$$Prob(\|\boldsymbol{v}\|_2 > c\sqrt{n}) \le C_{c/r}^n.$$

Definition 3. *For an n-dimensional lattice $\Lambda \subset H$, and positive real $\epsilon > 0$, we define its smoothing parameter $\eta_\epsilon(\Lambda)$ to be the smallest r such that $\rho_{1/r}(\Lambda^* \setminus \{0\}) \le \epsilon$.*

Lemma 2. *For any n-dimensional lattice $\Lambda \subset H$ and positive real $\epsilon > 0$, we have*

$$\eta_\epsilon(\Lambda) \le \sqrt{\frac{\ln(2n(1 + 1/\epsilon))}{\pi}} \cdot \lambda_n(\Lambda).$$

In particular, for any superlogarithmic function $\omega(\log n)$, there exists a negligible function $\epsilon(n)$ such that $\eta_\epsilon \le \sqrt{\omega(\log(n))} \cdot \lambda_n(\Lambda)$.

Lemma 3. *For any $r > 0$, and lattice Λ, the statistical distance between $D_{\Lambda,r} \pmod{\Lambda}$ and the uniform distribution over Λ is at most $\frac{1}{2}\rho_{1/r}(\Lambda^* \setminus \{0\})$. In particular, for any $\epsilon > 0$ and any $r \ge \eta_\epsilon(\Lambda)$, the statistical distance is at most $\epsilon/2$.*

In particular, we use Lemma 1 to show that there are number fields that are vulnerable to our proposed attack. The χ^2-attack and our proposed attack assume that the error distribution over the prime ideal is distinguishable from the uniform distribution. In other words, if the error width r is too large, these attacks will fail as Lemma 3 indicates.

2.3 Algebraic Number Theory

Let K be a number field of degree n with the ring of integers R and $\sigma_1, \sigma_2, \cdots, \sigma_n$ be the distinct embeddings of K into the complex number field. Let r_1, r_2 be the number of real embeddings and conjugate pairs of complex embeddings of K respectively, then $n = r_1 + 2r_2$. We assume $\sigma_1, \sigma_2, \cdots, \sigma_{r_1}$ are real embeddings and the complex conjugate $\sigma_{r_1+r_2+j} = \overline{\sigma}_{r_1+j}$ for $1 \le j \le r_2$. The canonical embedding $\sigma : K \to H$ is defined as follows:

$$\sigma : K \to H\ ;\ x \mapsto (\sigma_1(x), \cdots, \sigma_n(x))^T.$$

The norm of $x \in K$ is defined by $\|x\| \coloneqq \|\sigma(x)\|$. The trace map from K to $\mathbb{Q}$ can be defined by the sum of the embeddings:

$$\mathrm{Tr} : K \to \mathbb{Q}\ ;\ a \mapsto \sum_{1 \le i \le n} \sigma_i(a).$$

Notice that for any $a, b \in K$, we have

$$\mathrm{Tr}(a + b) = \mathrm{Tr}(a) + \mathrm{Tr}(b),$$
$$\mathrm{Tr}(a \cdot b) = \sum_{1 \le i \le n} \sigma_i(a)\sigma_i(b) = \langle \sigma(a), \overline{\sigma(b)} \rangle.$$

For a fractional ideal $I \subseteq R$, $\sigma(I) \in H$ is called an ideal lattice. When $b_1, \cdots, b_n$ is an integral basis of I, $(\sigma(b_1), \cdots \sigma(b_n))$ is a basis of $\sigma(I)$. We define the volume of I as $\mathrm{vol}(I) \coloneqq \mathrm{vol}(\sigma(I))$ and the discriminant of K as $\mathrm{disc}(K) \coloneqq \mathrm{vol}(R)^2$. The dual ideal is defined as $I^\vee = \{x \in K : \mathrm{Tr}(xI) \subset \mathbb{Z}\}$. The canonical embedding of

$I^\vee$ is $\sigma(I^\vee) = \overline{\sigma(I)^\vee}$. Also, $I^\vee$ is a fractional ideal of R, and $(I^\vee)^\vee = I$. For an integral basis $B = (b_j)$ of I, its dual basis $B^\vee = (b_j^\vee)$, which is characterized by $\mathrm{Tr}(b_j \cdot b_k^\vee) = \delta_{jk}$, is an integral basis of $I^\vee$. Moreover, $I^\vee = I^{-1} \cdot R^\vee$, where $R^\vee$ is the dual ideal of R. The following lemma is known for the dual basis [26].

Lemma 4. *Let $K = \mathbb{Q}(\alpha)$ and let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α. Write*

$$f(x) = (x - \alpha)(c_{n-1}(\alpha)x^{n-1} + \cdots + c_1(\alpha)x + c_0(\alpha)),$$

where $c_i(\alpha) \in K$. The dual basis to $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is $\left\{\frac{c_0(\alpha)}{f'(\alpha)}, \frac{c_1(\alpha)}{f'(\alpha)}, \cdots, \frac{c_{n-1}(\alpha)}{f'(\alpha)}\right\}$.

2.4 Ring-LWE Problem

In the original Ring-LWE problem, the secret is selected from the dual space of the ring of integers, $R^\vee$ [6]. However, for simplicity, the secret is often selected from R. In [21], [27], it was shown that the two problems of dual Ring-LWE and non-dual Ring-LWE are equivalent. This paper proposes an attack on the non-dual Ring-LWE problem, without considering the dual space.

Definition 4. *Suppose $K/\mathbb{Q}$ is a number field with the ring of integers, R, and quotient ring, $R_q = R/qR$, for a positive integer q. Let $r > 0$ be a positive real number and fix $s \in R_q$. Then, q is called the modulus, and s is called the secret. When a is chosen to be uniformly distributed on R_q and e is chosen according to an error distribution ψ over R, $(a, b = as + e) \in R_q \times R_q$ is called a Ring-LWE sample, and e is called an error.*

When analyzing the non-dual Ring-LWE problem using the discrete Gaussian distribution $\psi = D_{\sigma(R),r}$, one must consider the sparsity of the ideal lattice, $\sigma(R)$, measured by its volume [28]. For width r of the discrete error distribution, we denote the scaled error width r_0 as

$$r_0 = r/\mathrm{vol}(\sigma(R))^{1/n} = r/\mathrm{disc}(K)^{1/2n}.$$

There are two types of Ring-LWE problems: the decision Ring-LWE and search Ring-LWE problems.

Definition 5 (search non-dual Ring-LWE)**.** *Given polynomially many Ring-LWE samples $(a, b) \in R_q \times R_q$, the search Ring-LWE problem determines the secret $s \in R_q$ from these samples.*

Definition 6 (decision non-dual Ring-LWE)**.** *Given polynomially many samples $(a, b) \in R_q \times R_q$, the decision Ring-LWE problem distinguishes whether the samples are Ring-LWE samples or samples selected according to a uniform distribution on $R_q \times R_q$.*

Suppose $\mathfrak{q}$ is a prime ideal in K that lies above a prime number q. Then, $\phi\colon R_q \to R/\mathfrak{q}; \alpha \mapsto \alpha \pmod{\mathfrak{q}}$ is a ring homomorphism, and $R/\mathfrak{q} \cong \mathbb{F}_{q^f}$, where f is the residue degree. With the homomorphism ϕ, we can embed the Ring-LWE sample $(a', b' = a's' + e') \in R_q \times R_q$ into $(a, b = as + e) \in \mathbb{F}_{q^f} \times \mathbb{F}_{q^f}$. That is, we can use ϕ to convert the Ring-LWE problem over R_q into a problem in the finite field $\mathbb{F}_{q^f}$.

Definition 7 (search Ring-LWE $\pmod{\mathfrak{q}}$)**.** *Let $\mathfrak{q}$ be a prime ideal of K that lies above a prime number q. Given polynomially many Ring-LWE samples $(a, b) \in R_q \times R_q$, the search Ring-LWE problem $\pmod{\mathfrak{q}}$ determines $s \pmod{\mathfrak{q}} \in \mathbb{F}_{q^f}$ from these samples.*

The following lemma is known for the Ring-LWE $\pmod{\mathfrak{q}}$ problem [16]. This lemma asserts that if we can determine all $s \pmod{\mathfrak{q}_i}$, then we can solve the Ring-LWE problem on R_q using the Chinese Remainder Theorem.

Lemma 5. *Let $K/\mathbb{Q}$ be a finite Galois extension of degree n with the ring of integers R and let q be a prime unramified in K. Then, there exists a unique divisor r of n and a set of r distinct prime ideals $\mathfrak{q}_1, \cdots \mathfrak{q}_r$ of R such that $qR = \mathfrak{q}_1 \cdots \mathfrak{q}_r$. For all i, $R/\mathfrak{q}_i \cong \mathbb{F}_{q^f}$ where $f = n/r$, and $R_q \cong \mathbb{F}_{q^f} \times \cdots \times \mathbb{F}_{q^f}$.*

2.5 Attacks for Ring-LWE $\pmod{\mathfrak{q}}$

The χ^2-attack

Chen et al. proposed the χ^2-attack to find the secret $s \pmod{\mathfrak{q}} \in \mathbb{F}_{q^f}$ by brute force [16]. The basic concept of this attack is based on the assumption that the distribution $\psi \pmod{\mathfrak{q}}$ is distinguishable from a uniform distribution in the finite field, $\mathbb{F}_{q^f}$.

In this attack, the following conditions were assumed:

- The modulus q is a prime of residue degree, f, in the number field, K.
- Suppose $e' \in R_q$ are sampled from ψ. The distribution of $\phi(e')$ is distinguishable from the uniform distribution on $\mathbb{F}_{q^f}$.

The attack procedure is presented in Algorithm 1. In the χ^2-attack, chi-square tests are performed on $\mathbb{F}_{q^f}$. Therefore, $O(q^f)$ samples are required for this attack. Remark that since every ciphertext is available as a sample, it is not serious to obtain the samples needed for the attack. However, the larger the number of samples, the more computation time is required, making it difficult to execute the attack. Furthermore, the number of guesses was $O(q^f)$ because the test was performed for each guess, g. Thus, the total complexity of the χ^2-attack is $O(q^{2f}M(f))$.

The two-residue-degree χ^2-attack

In the χ^2-attack, both the number of samples and the number of guesses depend on the residue degree f. Therefore, it is difficult to attack when the residue degree is high. Chen et al. showed that when the residue degree is two, the computational complexity of the attack can be reduced using cosets and a Frobenius map [17].

Algorithm 1 The χ^2–Attack

Input: $\mathcal{S}$: collection of Ring-LWE samples, $\mathfrak{q}$: a prime ideal, α: risk ratio
Output: $s \pmod{\mathfrak{q}}$, **NOT-RLWE** or **INSUFFICIENT-SAMPLES**

$\delta \leftarrow F^{-1}_{q^f-1}(\alpha)$, $\mathcal{S}' \leftarrow \emptyset$, $\mathcal{G} \leftarrow \emptyset$
for (a, b) in $\mathcal{S}$ **do**
  $a,\ b \leftarrow a \pmod{\mathfrak{q}},\ b \pmod{\mathfrak{q}}$
  add (a, b) to $\mathcal{S}'$
end for
for g in $\mathbb{F}_{q^f}$ **do**
  $\mathcal{E} \leftarrow \emptyset$
  for (a, b) in $\mathcal{S}'$ **do**
    $e' \leftarrow b - ag$
    add e' to $\mathcal{E}$
  end for
  $\chi^2(\mathcal{E}) \leftarrow$ the chi-square test statistic of $\mathcal{E}$
  if $\chi^2(\mathcal{E}) > \delta$ **then** add g to $\mathcal{G}$
end for
if $\mathcal{G} = \emptyset$ **then** return **NOT-RLWE**, **else if** $\mathcal{G} = \{g\}$ **then** return g, **else** return **INSUFFICIENT-SAMPLES**

Algorithm 2 The two-residue-degree χ^2-attack

Input: $\mathcal{S}$: collection of Ring-LWE samples, $\mathfrak{q}$: a prime ideal, α: risk ratio
Output: $s \pmod{\mathfrak{q}}$, **NOT-RLWE** or **INSUFFICIENT-SAMPLES**

$\delta \leftarrow F^{-1}_{q-1}(\alpha)$, $\mathcal{S}' \leftarrow \emptyset$, $\mathcal{G} \leftarrow \emptyset$
for (a, b) in $\mathcal{S}$ **do**
  $a,\ b \leftarrow a \pmod{\mathfrak{q}},\ b \pmod{\mathfrak{q}}$
  add (a, b) to $\mathcal{S}'$
end for
for $j = 1$ to q **do**
  $\mathcal{E} \leftarrow \emptyset$
  for (a, b) in $\mathcal{S}'$ **do**
    if $a \in \mathbb{F}_q$ **then continue**
    $m_j(a, b) \leftarrow \frac{F(b)-b-F(at_j)}{+} at_j F(a) - a \in \mathbb{F}_q$
    add $m_j(a, b)$ to $\mathcal{E}$
  end for
  $\chi^2(\mathcal{E}) \leftarrow$ the chi-square test statistic of $\mathcal{E}$
  if $\chi^2(\mathcal{E}) > \delta$ **then** let s_0 the most frequent value of $\mathcal{E}$ and add $s_0 + t_j$ to $\mathcal{G}$
end for
if $\mathcal{G} = \emptyset$ **then** return **NOT-RLWE**, **else if** $\mathcal{G} = \{g\}$ **then** return g, **else** return **INSUFFICIENT-SAMPLES**

In this attack, the following conditions were assumed:

- The modulus q is a prime of residue degree two in the number field K.
- Suppose $e' \in R_q$ are sampled from ψ. The probability that $\phi(e') = e_0 + e_1\xi$ lies in the prime subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^2}$ is computationally distinguishable from $1/q$.

The second condition is the distribution of e_1 is not uniform on $\mathbb{F}_q$, and the probability $e_1 = 0 \pmod{q}$ is higher than $1/q$. Suppose $\{t_1, \cdots, t_q\}$ is a fixed complete set of coset representatives of $\mathbb{F}_{q^2}/\mathbb{F}_q$. A unique index, i, and $s_0 \in \mathbb{F}_q$ exist such that $\phi(s') = s = s_0 + t_i$. The number of guesses is reduced by finding s_0 and t_i, respectively. The Frobenius map, denoted by $F(a) := a^q$ ($\forall a \in \mathbb{F}_{q^2}$), allows chi-square tests to be performed in a small sample space, and thus the number of samples required for the attack is reduced.

The attack procedure is presented in Algorithm 2. In the two-residue-degree χ^2-attack, chi-square tests are performed on $\mathbb{F}_q$, and then $O(q)$ samples are required for this attack. Furthermore, because chi-square tests are performed for $t_1, \cdots, t_q$, the number of guesses is $O(q)$. Thus, the total complexity of the two-residue-degree χ^2-attack is $O(q^2 \log qM(f))$.

2.6 Analysis of Error Distribution on a Prime Ideal

If $\psi \pmod{\mathfrak{q}}$ and $U(R/\mathfrak{q})$ are distinglshable, then the χ^2-attack succeeds. Peikert showed that if there exists a small element $w \in \mathfrak{q}^\vee$, $\psi \pmod{\mathfrak{q}}$ and $U(R/\mathfrak{q})$ are distinishable [21].

Since $R/\mathfrak{q}$ and $\mathbb{F}_{q^f}$ are isomorphic, there exists a ring homomorphism $h\colon R/\mathfrak{q} \to \mathbb{F}_{q^f}$. Since $\mathbb{F}_{q^f}$ is a f-dimensional vector space over $\mathbb{F}_q = \mathbb{Z}_q$, an arbitrary $h(r) \in \mathbb{F}_{q^f}$ can be uniquely represented by some fixed $\mathbb{Z}_q$-basis and f-tuple of coefficients. Moreover, the i-th coefficient of $h(r)$, $h_i(r)$, can be represented by an additive homomorphism $h_i\colon R/\mathfrak{q} \to \mathbb{F}_q\ ; x \mapsto q \cdot \mathrm{Tr}(w_i \cdot x)$ using some $w_i \in \mathfrak{q}^\vee$. Since $\mathrm{Tr}(w_i \cdot x) \in \mathbb{Q}$, suppose $\Lambda = \sigma(\mathfrak{q})$ and $\boldsymbol{w} = \overline{\sigma(w_i)} \in \Lambda^\vee$, then $\mathrm{Tr}(w_i \cdot x) = \overline{\mathrm{Tr}(w_i \cdot x)} = \mathrm{Tr}(w_i \cdot x) = \mathrm{Tr}(w_i \cdot x) = \langle\overline{\sigma(w_i)}, \sigma(x)\rangle \in \langle \boldsymbol{w}, \sigma(R) \pmod{\Lambda}\rangle$.

Lemma 6. *Let Λ be any lattice, $\boldsymbol{w} \in \Lambda^\vee \setminus \{0\}$ be any nonzero element of its dual lattice. For any $r > 0$, suppose D_r is the gaussian distribution. Then for $\boldsymbol{x} \leftarrow D_r \pmod{\Lambda}$, the distribution of $\langle \boldsymbol{w}, \boldsymbol{x}\rangle \pmod{\mathbb{Z}}$ is $D_{r\|\boldsymbol{w}\|} \pmod{\mathbb{Z}}$, and*

$$E_{\boldsymbol{x} \leftarrow D_r \pmod{\Lambda}}[\cos(2\pi\langle \boldsymbol{w}, \boldsymbol{x}\rangle)] = \exp(-\pi(r\|\boldsymbol{w}\|^2)).$$

In particular, if $r\|\boldsymbol{w}\| = O(1)$, then the expectation is $\Omega(1)$.

In the case of $\boldsymbol{x} \leftarrow U(H) \pmod{\Lambda}$, $\langle \boldsymbol{w}, \boldsymbol{x}\rangle \pmod{\mathbb{Z}}$ is a random value on $[0, 1)$ independently from $\boldsymbol{w}$, so $E[\cos(2\pi\langle \boldsymbol{w}, \boldsymbol{x}\rangle)] = 0$. On the other hand, if $\boldsymbol{x} \leftarrow D_r \pmod{\Lambda}$ and $r\|\boldsymbol{w}\|$ is sufficiently small, $E[\cos(2\pi\langle \boldsymbol{w}, \boldsymbol{x}\rangle)] = \exp(-\pi(r\|\boldsymbol{w}\|^2)) \cong 1$. That is, when there exists a small element $\boldsymbol{w} \in \Lambda = \sigma(\mathfrak{q})$, $\psi \pmod{\mathfrak{q}}$ and $U(R/\mathfrak{q})$ can be distinguished. Lemma 6 assumes a continuous Gaussian distribution D_r, but it is also valid for a discrete Gaussian distribution $D_{\sigma(R),r}$. Furthermore, in Sect. 4.3 of [21], the usefulness of the analysis using the dual basis of $R^\vee \subset \mathfrak{q}^\vee$ is also shown.

3. Attacks on Ring-LWE $\pmod{\mathfrak{q}}$ by Trace Map

In this section, we describe the details of our proposed attack, which generalizes our preliminary work [18]. Our attack reduces the number of samples by performing chi-square tests on $\mathbb{F}_q$ and also reduces the number of guesses by using cosets $\mathbb{F}_{q^f}/\mathbb{F}_{q^m}$, where m is the divisor of f and $f = mn$. This attack assumes that the error distribution $\psi \pmod{\mathfrak{q}}$ is distinguishable from the uniform distribution in the finite field. It also require certain conditions of ($\mathbb{F}_{q^f} \cong \mathbb{F}_q[x]/(x^f - c) \cong \mathbb{F}_{q^m}[x]/(x^n - c_1)$ and $\mathbb{F}_{q^m} \cong \mathbb{F}_q[x^n]/((x^n)^m - c)$ ($c \in \mathbb{F}_q$, $c_1 = \sqrt[m]{c} \in \mathbb{F}_{q^m}$)).

For any divisor m of f, $\mathbb{F}_{q^m}$ is a subfield of $\mathbb{F}_{q^f}$. Chi-square tests are performed on $\mathbb{F}_q$ by using the trace map from $\mathbb{F}_{q^f}$ to $\mathbb{F}_{q^m}$ and $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ in two steps. In the special case where f is a prime residue degree, we set $m = 1$, and

use one trace map from $\mathbb{F}_{q^f}$ to $\mathbb{F}_q$.

The computational complexity of the trace map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, which is the point of our proposal, is $O((C(n) + \log(q)M(n)) \cdot \log(n))$ [22]. However, by using Theorem 1 shown below, if an irreducible polynomial exists such that $\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(x^n - c)$, it can be derived by $O(1)$ operations in $\mathbb{F}_q$, independent of the extension degree n.

Theorem 1. *Suppose $\alpha = \sum_{0\le l<n} \alpha_l \xi^l$ ($\alpha_k \in \mathbb{F}_q$) is an element of $\mathbb{F}_{q^n}$. If $\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(x^n - c)$ ($c \in \mathbb{F}_q$), the trace map of the finite field $\mathrm{Tr}\colon \mathbb{F}_{q^n} \to \mathbb{F}_q$ is $\mathrm{Tr}(\alpha) = n \cdot \alpha_0$.*

Proof. The roots of $x^n - c$ are $c^{\frac{1}{n}} \cdot \zeta_n^j$ ($j = 0, 1, \cdots, n-1$); thus, we choose $\xi = c^{\frac{1}{n}} \cdot \zeta_n$, and any $\alpha \in \mathbb{F}_{a^n}$ can be denoted as $\alpha = \sum_{0\le i<n} a_i \xi^i = \sum_{0\le i<n} a_i (c^{\frac{1}{n}} \cdot \zeta_n)^i$ ($a_i \in \mathbb{F}_q$). The distinct roots $c^{\frac{1}{n}}\zeta_n^j$ and $c^{\frac{1}{n}}\zeta_n^{j'}$ are conjugate; thus there exists $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$ such that $\sigma(c^{\frac{1}{n}}\zeta_n^j) = c^{\frac{1}{n}}\zeta_n^{j'}$. Moreover $\sigma(c^{\frac{1}{n}}\zeta_n) \neq \sigma'(c^{\frac{1}{n}}\zeta_n)$ for distinct σ, $\sigma' \in \mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$; therefore $\sum_{\sigma\in\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)} \sigma(c^{\frac{1}{n}} \cdot \zeta_n) = \sum_{0\le j<n} c^{\frac{1}{n}} \cdot \zeta_n^j$. Then we have

$$\begin{aligned}
\mathrm{Tr}(\alpha) &= \sum_{\sigma\in\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)} \sigma(\alpha) \\
&= \sum_{\sigma\in\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)} \sigma\left(\sum_{0\le i<n} a_i \cdot \xi^i\right) \\
&= \sum_{\sigma\in\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)} \sum_{0\le i<n} a_i \cdot \sigma(\xi)^i \\
&= \sum_{0\le i<n} a_i \sum_{\sigma\in\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)} \sigma(c^{\frac{1}{n}} \cdot \zeta_n)^i \\
&= \sum_{0\le i<n} a_i \sum_{0\le j<n} (c^{\frac{1}{n}}\zeta_n^j)^i = \sum_{0\le i<n} a_i c^{\frac{i}{n}} \sum_{0\le j<n} \zeta_n^{ij}.
\end{aligned}$$

$\sum_{0\le j<n} \zeta_n^{ij}$ is n and 0 for $i = 0$ and $i \neq 0$, respectively; thus, $\mathrm{Tr}(\alpha) = n \cdot a_0$. □

We propose a basic approach and an improved approach. The basic and improved approaches derive the trace value by $\mathrm{Tr}(\alpha) = \sum_{0\le l<n} \alpha^{q^l}$ and $\mathrm{Tr}(\alpha) = n \cdot \alpha_0$, respectively.

3.1 The Improved χ^2-Attack

Basic approach

In our proposed attack, we assume the following conditions. The condition of the error distribution, the second one, has a significant effect on the success of both attacks.

- The modulus q is a prime of residue degree $f = mn$ in the number field K. Moreover, there exists irreducible polynomials $g(x) = x^f - c \in \mathbb{F}_q[x]$, $g_1(x) = x^n - c_1 \in \mathbb{F}_{q^m}[x]$, $g_2(x^n) = (x^n)^m - c \in \mathbb{F}_q[x^n]$ ($c \in \mathbb{F}_q, c_1 = \sqrt[m]{c} \in \mathbb{F}_{q^m}$) such that $\mathbb{F}_{q^f} \cong \mathbb{F}_q[x]/(g(x)) \cong \mathbb{F}_{q^m}[x]/(g_1(x))$ and $\mathbb{F}_{q^m} \cong \mathbb{F}_q[x^n]/(g_2(x^n))$.
- Suppose $e' \in R_q$ are sampled from ψ and $e = \phi(e') = \sum_{0\le l<f} e_l \xi^l$. The distribution of e_k is distinguishable from the uniform distribution on $\mathbb{F}_q$ for some index k ($0 \le k < f$). Furthermore, the probability that $e_k = 0 \pmod q$ is the highest.

The complete set of coset representatives for $\mathbb{F}_{q^f}/\mathbb{F}_{q^m}$ is $\{t_1, \cdots, t_{q^{f-m}}\} = \{\sum_{0\le l<f,\ n\nmid l} \alpha_l \xi^l \mid \alpha_l \in \mathbb{F}_q\}$ because $\mathbb{F}_{q^m} = \{\sum_{0\le l<f,\ n|l} \alpha_l \xi^l \mid \alpha_l \in \mathbb{F}_q\}$. There is a unique index i and $s_0 = \sum_{0\le l<f,n|l} (s_0)_l \xi^l \in \mathbb{F}_{q^m}$ such that $\phi(s') = s = s_0 + t_i$. We set $\theta = \xi^{f-k}$. For each j ($1 \le j \le q^{f-m}$), $\forall a \in \mathbb{F}_{q^f}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta) \in \mathbb{F}_q \setminus \{0\}$, we define m_j as follows:

$$m_j(a, b) := \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(b\theta) - \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(at_j\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} \in \mathbb{F}_{q^m}.$$

Theorem 2 holds for the distribution of $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j(a, b))$, which is similar to the error coefficient distribution, e_k if and only if $j = i$. We can determine t_i because the distribution of $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j(a, b))$ is not uniform but the related distribution of e_k.

Theorem 2. *Let a be obtained uniformly at random from $\mathbb{F}_{q^f}$ so that $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta) \in \mathbb{F}_q \setminus \{0\}$ and $e = \phi(e')$, where e' is sampled from $D_{\tau(R),r}$. For each $1 \le j \le q^{f-m}$, we have*

1. *If $j \neq i$, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j(a, b))$ is uniformly distributed in $\mathbb{F}_q$.*
2. *If $j = i$, then $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j(a, b)) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0) + \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)}$*

Proof. Since $b = as + e$ and $s = s_0 + t_i$,

$$\begin{aligned}
&m_j(a, b) \\
&= \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(b\theta) - \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(at_j\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} \\
&= \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}((as + e)\theta) - \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(at_j\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} \\
&= \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(as_0\theta + at_i\theta + e\theta) - \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(at_j\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} \\
&= \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a(t_i - t_j)\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} + s_0 + \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)}.
\end{aligned}$$

In the case of $j \neq i$, let $\delta = t_i - t_j \in \{\sum_{1\le l\le f,\ n\nmid l} \alpha_l \xi^l \mid \alpha_l \in \mathbb{F}_q\}$, then $m_j(a, b) = \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta\delta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} + s_0 + \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)}$. From Theorem 1, $a\theta$ is uniformly sampled from the set $\{\alpha_0 + \sum_{1\le l\le f,\ n\nmid l} \alpha_l \xi^l \mid \alpha_0 \in \mathbb{F}_q^*, \alpha_l \in \mathbb{F}_q\}$, then $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)$ and $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta\delta)$ can be assumed to be independent. Therefore, $Pr(\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta) = c,\ \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta\delta) = d) = \frac{1}{q^m(q-1)}$ for $\forall c \in \mathbb{F}_q \setminus \{0\}$ and $\forall d \in \mathbb{F}_{q^m}$. For $\forall z' \in \mathbb{F}_{q^m}$, let $z = z' - s_0$. From the following equality, we can derive that m_j is uniformly distributed when $j \neq i$,

$$Pr(m_j(a, b) = z')$$

$$
\begin{aligned}
&= Pr\left(\frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta\delta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} + \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} = z\right) \\
&= \sum_{x+y=z} Pr\left(\frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta\delta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} = x,\ \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} = y\right) \\
&= \sum_{x+y=z} \sum_{c\in\mathbb{F}_q\setminus\{0\}} Pr(\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta\delta) = cx, \\
&\qquad \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta) = cy,\ \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta) = c) \\
&= \sum_{x+y=z} \sum_{c\in\mathbb{F}_q\setminus\{0\}} Pr(\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta) = cy) \\
&\qquad \cdot Pr(\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta\delta) = cx, \mathrm{Tr}(a\theta) = c) \\
&= \frac{1}{q^m(q-1)} \sum_{y\in\mathbb{F}_{q^m}} \sum_{c\in\mathbb{F}_q\setminus\{0\}} Pr(\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta) = cy) \\
&= \frac{q-1}{q^m(q-1)} \sum_{y\in\mathbb{F}_{q^m}} Pr(\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta) = y) = \frac{1}{q^m}.
\end{aligned}
$$

$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j(a,b))$ is uniformly distributed on $\mathbb{F}_q$ when $i \neq j$ because $m_j(a,b)$ is uniformly distributed on $\mathbb{F}_{q^m}$, and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ is an additive homomorphism and surjective.

On the other hand when $j = i$, $m_i(a,b) = s_0 + \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)}$. We assume $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta) \in \mathbb{F}_q$, then $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)^{-1} \in \mathbb{F}_q$, and so

$$
\begin{aligned}
&\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j(a,b)) \\
&= \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0) + \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(\frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)}\right) \\
&= \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0) + \frac{\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta))}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} \\
&= \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0) + \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)}.
\end{aligned}
$$

□

If $a \in \mathbb{F}_{q^f}$ is chosen uniformly at random, $\frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(e\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)}$ will be uniformly random on $\mathbb{F}_{q^m}$. In this case, it is impossible to distinguish between the distribution of $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j(a,b))$ and the uniform distribution on $\mathbb{F}_q$. Therefore, we restrict the samples a used in the attack to $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta) \in \mathbb{F}_q \setminus \{0\}$.

The distribution of $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j)$ is not uniform if and only if the index $j = i$; therefore, we can determine the value of t_i. We can also obtain $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0) = m \cdot (s_0)_0$ from the most frequent value of $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j)$. If the residue degree is prime and the attack uses the subfield $\mathbb{F}_q$, i.e. $m = 1$, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0) = s_0$, and thus we can determine $s = s_0 + t_i$. In the case of $m \neq 1$, we derive $s_0 = \sum_{0\le l<f,\ n|l} (s_0)_l \xi^l$ by applying the χ^2-attack. We guess the value of s_0 from $(s_0)_0$ by brute-force, and let g be the guess value. For $e' := b - a(g + t_i)$, we determine s_0 by calculating the distribution of

Algorithm 3 The improved χ^2-attack

Input: $\mathcal{S}$: collection of Ring-LWE samples, $\mathfrak{q}$: a prime ideal, α: risk ratio
Output: $s \pmod{\mathfrak{q}}$, **NOT-RLWE** or **INSUFFICIENT-SAMPLES**

$\delta \leftarrow F^{-1}_{q-1}(\alpha)$, $\mathcal{S}' \leftarrow \emptyset$, $\mathcal{G} \leftarrow \emptyset$
for a, b in $\mathcal{S}$ **do**
  $a,\ b \leftarrow a \pmod{\mathfrak{q}},\ b \pmod{\mathfrak{q}}$
  add (a,b) to $\mathcal{S}'$
end for
for $j = 1$ to q^{f-m} **do**
  $\mathcal{E}_j \leftarrow \emptyset$
  for (a,b) in $\mathcal{S}'$ **do**
    if $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta) \notin \mathbb{F}_q \setminus \{0\}$ **then continue**
    $m_j(a,b) \leftarrow \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(b\theta) - \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(at_j\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)}$
    add $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j(a,b))$ to $\mathcal{E}_j$
  end for
  $\chi^2(\mathcal{E}_j) \leftarrow$ the chi-square test statistic of $\mathcal{E}_j$
  if $\chi^2(\mathcal{E}_j) > \delta$ **then**
    $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0) \leftarrow$ the most frequent value of $\mathcal{E}_j$
    if $m = 1$ **then**
      add $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0) + t_j$ to $\mathcal{G}$
    else
      for g in $\{c \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0)\}$ **do**
        $\mathcal{E}_g \leftarrow \emptyset$
        for a, b in S **do**
          $e' \leftarrow b - a(g + t_j)$
          add $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e'\theta)$ to $\mathcal{E}_g$
        end for
        $\chi^2(\mathcal{E}_g) \leftarrow$ the chi-square test statistic of $\mathcal{E}_g$
        if $\chi^2(\mathcal{E}_g) > \delta$ **then** add $g + t_j$ to $\mathcal{G}$
      end for
    end if
  end if
end for
if $\mathcal{G} = \emptyset$ **then** return **NOT-RLWE**, **else if** $\mathcal{G} = \{g\}$ **then** return g, **else** return **INSUFFICIENT-SAMPLES**

$$\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e'\theta) = \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}((b - a(g + t_i))\theta).$$

In the case of $g \neq s_0$, because e' is uniformly random on $\mathbb{F}_{q^f}$ and because $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}$ is a surjective additive homomorphism, $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e'\theta)$ is uniformly random in $\mathbb{F}_q$. In the case of $g = s_0$, from $b = as + e$ and $s = s_0 + t_i$,

$$
\begin{aligned}
\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e'\theta) &= \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(b\theta - a(g + t_i)\theta) \\
&= \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(a(s - (g + t_i))\theta + e\theta) \\
&= \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e\theta) = f \cdot (e_k c).
\end{aligned}
$$

We can obtain s_0 because the distribution of e_k can be distinguished from the uniform distribution on $\mathbb{F}_q$. The calculation of the distribution of $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e'\theta)$ requires the use of a uniform random sample a, unlike the calculation of the distribution of $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(m_j)$. The algorithm is shown in Algorithm 3.

We considered the computational complexity in the case of prime residue degree, i.e. $m = 1$. Because chi-square tests are performed on $\mathbb{F}_q$, we require $O(q)$ samples. Furthermore, the number of guesses is q^{f-1} because the test needs to be performed on all representatives. The computational complexities of $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(b\theta)$ and $\mathrm{Tr}_{q^f/\mathbb{F}_q}(a\theta)$ are $O((C(f) + \log(q)M(f)) \cdot \log(f))$, and $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(at_j\theta)$ re-

quires $O(M(f) + (C(f) + \log(q)M(f)) \cdot \log(f)) = O((C(f) + \log(q)M(f)) \cdot \log(f))$ operations in $\mathbb{F}_q$. The total computational complexity of $m_j(a, b)$ is $O((C(f) + \log(q)M(f)) \cdot \log(f))$ operations in $\mathbb{F}_q$. Therefore, the basic approach requires $O((C(f) + \log(q)M(f)) \cdot q^f \log(f))$ operations in $\mathbb{F}_q$.

Improved approach

For any element $\beta = \sum_{0\le l<f,\ n|l} \gamma'_l \xi^l$ ($\gamma'_l \in \mathbb{F}_q$) in $\mathbb{F}_{q^m}$ and $\alpha = \sum_{0\le l<n} \beta_l \xi^l = \sum_{0\le l<f} \gamma_l \xi^l$ ($\gamma_l \in \mathbb{F}_q$, $\beta_l \in \mathbb{F}_{q^m}$) in $\mathbb{F}_{q^f}$, we have following equality from Theorem 1,

$$\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(\alpha) = n \cdot \beta_0 = n \sum_{0\le l<f,\ n|l} \gamma_l \xi^l, \tag{1}$$

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta) = m \cdot \gamma'_0. \tag{2}$$

As we restrict the samples used in the calculation m_j to $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta) \in \mathbb{F}_q \setminus \{0\}$, we have $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta) = \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(\sum a_l \xi^{l+f-k}) = n \cdot \sum_{0\le l<f,n|l} a_l \xi^{l+f-k} = n \cdot a_k \xi^f$. We denote $at_j = \sum (at_j)_l \xi^l$. Then

$$\begin{aligned} m_j(a, b) &= \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(b\theta) - \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(at_j\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)} \\ &= \frac{n \cdot \sum_{0\le l<f,\ n|l}(b_l - (at_j)_l)\xi^{l+f-k}}{n \cdot a_k \xi^f} \\ &= \frac{\sum_{0\le l<f,\ n|l}(b_l - (at_j)_l)\xi^{l+f-k}}{a_k \xi^f}. \end{aligned}$$

We can write $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j(a, b))$ as

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j(a, b)) &= m \cdot \frac{(b_k - (at_j)_k)\xi^f}{a_k \xi^f} \\ &= m \cdot \frac{b_k - (at_j)_k}{a_k}. \end{aligned}$$

From Theorem 2, when $j = i$, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j(a, b)) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(s_0) + \frac{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e\theta)}{\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_{q^m}}(a\theta)}$. So, we have

$$\begin{aligned} m \cdot \frac{b_k - (at_j)_k}{a_k} &= m \cdot (s_0)_0 + \frac{f \cdot e_k \xi^f}{n \cdot a_k \xi^f}, \\ \frac{b_k - (at_j)_k}{a_k} &= (s_0)_0 + \frac{e_k}{a_k}. \end{aligned}$$

Based on these assumptions, the most frequent value of $\frac{b_k-(at_j)_k}{a_k}$ is $(s_0)_0$ when $j = i$. From $(s_0)_0$, guess the value of s_0 using brute-force and find the secret on the ideals. We denote $g' = a(t_i + g) = \sum_{0\le l<n} g'_l \xi^l$, and have

$$\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e'\theta) = \mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}((b - g')\theta) = f \cdot (b_k - g'_k) \cdot \xi^f.$$

In the improved approach, we calculate the distribution of $(b_k - g'_k)$ instead of $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e'\theta)$.

From (1) and (2), it is possible to replace $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j)$ with $\frac{b_k-(at_j)_k}{a_k}$ and $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e'\theta)$ with $b_k - g'_k$. Then $O(M(f))$ operations in $\mathbb{F}_q$ are required for both $\frac{b_k-(at_j)_k}{a_k}$ and $b_k - g'_k$. Both $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j)$ and $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e'\theta)$ are elements in $\mathbb{F}_q$, witch are calculated $O(q^{f-m+1})$ and $O(q^m)$ times, respectively. Thus, the total complexity in the case of prime-residue-degree and composite-number-residue-degree are $O(M(f)q^f)$ and $O((q^{f-m+1} + q^m)M(f))$, respectively.

3.2 Selection of the Subfield

There is only one subfield $\mathbb{F}_q$ when prime-residue-degree, so the number of guesses is q^{f-1}. However, in the case of composite-number-residue-degree, there are multiple subfields, and the number of guesses varies greatly depending on which subfield $\mathbb{F}_{q^m}$ is used. From Theorem 1, the computational complexities of $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(m_j)$ and $\mathrm{Tr}_{\mathbb{F}_{q^f}/\mathbb{F}_q}(e'\theta)$ are $O(M(f))$. In other words, when the number of guesses $q^{f-m} + q^{m-1}$ is the lowest, the computational complexity of the attack is also the lowest. Let $G(m) = q^{f-m} + q^{m-1} (1 \le m \le f/2)$. Then,

$$\begin{aligned} \frac{dG(m)}{dm} &= -q^{f-m} \log q + q^{m-1} \log q \\ &= (-q^{f-m} + q^{m-1}) \log q. \end{aligned}$$

$G(m)$ has the minimum value when $q^{f-m} = q^{m-1}$, that is, $m = \frac{f+1}{2}$. When the residue degree, f, is a composite number, the attack is the most efficient when using cosets $\mathbb{F}_{q^f}/\mathbb{F}_{q^m}$ with the largest divisor m of f.

4. Vulnerable Field

The proposed attack will succeed when the distribution of the error coefficients, $e_k \in \mathbb{F}_q$, is distinguishable from the uniform distribution on $\mathbb{F}_q$. Since the distribution of errors is different in rings, it is necessary to perform the security analysis against the proposed attacks for each ring.

In [16], [21], it is shown that if the modulus q has residue degree 2 in the composite fields $\mathbb{Q}(\zeta_p, \sqrt{d})$, the error distribution is biased and distinguishable from the uniform distribution. In Sect. 4.1, we generalize the argument to show that error bias also occurs when the composite fields $\mathbb{Q}(\zeta_p, \sqrt[f]{d})$ have any residue degree f, not just $f = 2$. In Sect. 4.2, we report comparisons between the χ^2-attack and the proposed attack, as well as the vulnerability of the composite fields, through experiments.

4.1 Weak Instances to Our Proposed Attacks

For an odd prime p and residue degree f, let d be an integer coprime with p and no f-th root of d in $\mathbb{Z}$. We choose an odd prime q such that $q \equiv 1 \pmod{p}$ and no f-th roots of d in $\mathbb{F}_q$. We assume that the integral basis of the ring of integers of $\mathbb{Q}(\sqrt[f]{d})$ is $\{1, \sqrt[f]{d}, \sqrt[f]{d}^2, \cdots, \sqrt[f]{d}^{f-1}\}$ and $f(x) = x^f - d \in \mathbb{F}_q[x]$ is an irreducible polynomial over $\mathbb{F}_q$.

For $M = \mathbb{Q}(\zeta_p)$, $L = \mathbb{Q}(\sqrt[f]{d})$, let K be the composite field $M \cdot L = \mathbb{Q}(\zeta_p, \sqrt[f]{d})$, R be its ring of integers, and the quotient ring $R_q = R/qR$. We assume that $K/\mathbb{Q}$ is an algebraic

extension with extension degree of $f(p-1)$. This number field, K, is not a Galois extension. However, the modulus q has a residue degree f in K, and $R/\mathfrak{q} \cong \mathbb{F}_{q^f} \cong \mathbb{F}_q[x]/(x^f - d)$ for all prime ideals $\mathfrak{q}$ lying above q because the prime number q splits completely in M and is inert in L.

Theorem 3. *For p, f, d, q, K, R defined above, let $c = d^{\frac{f-1}{f}}$. We set $\beta = min\left\{\left(\frac{c\sqrt{2\pi e}}{r_0} \cdot e^{-\frac{\pi c^2}{r_0^2}}\right)^{f(p-1)}, 1\right\}$ for $r_0 < \sqrt{2\pi} \cdot c$. If $e = \phi(e') = \sum_{0\le l<f} e_l \xi^l$ for e' sampled from the discrete error distribution $D_{\sigma(R),r_0}$, then the probability that $e_{f-1} = 0$ is at least $1-\beta$.*

Proof. We assume that the integral basis of R is

$$\{1, \zeta_p, \cdots, \zeta_p^{p-2}, \sqrt[f]{d}, \sqrt[f]{d}\zeta_p, \cdots, \sqrt[f]{d}\zeta_p^{p-2}, \cdots, \sqrt[f]{d}^{f-1}, \sqrt[f]{d}^{f-1}\zeta_p, \cdots, \sqrt[f]{d}^{f-1}\zeta_p^{p-2}\}.$$

Here, the operation by $\phi\colon R_q \to R/\mathfrak{q} \cong \mathbb{F}_{q^f}$ is expressed as $\zeta_p \mapsto \alpha$ using α, a root of the p-th cyclotomic polynomial (mod q). From the map ϕ, $p-1$ basis from $(p-1)i+1$ to $(p-1)(i+1)$ corresponds to the x^i part of $\mathbb{F}_{q^f}$. Let $\sigma_{i,j} (0 \le i \le f-1, 1 \le j \le p-1)$ be the distinct embeddings from K to $\mathbb{C}$, and σ be the canonical embedding. We can say $\sigma_{i,j}(\sqrt[f]{d}^u \zeta_p^v) = \sqrt[f]{d}^u \zeta_f^{ui} \zeta_p^{vj}$, so for $0 \le u, u' \le f-1$ and $0 \le v, v' \le p-2$,

$$\begin{aligned}
&\langle \sigma(\sqrt[f]{d}^u \zeta_p^v), \sigma(\sqrt[f]{d}^{u'} \zeta_p^{v'}) \rangle \\
&= \sum_{i=0}^{f-1} \sum_{j=0}^{p-2} \sigma_{i,j}(\sqrt[f]{d}^u \zeta_p^v) \overline{\sigma_{i,j}(\sqrt[f]{d}^{u'} \zeta_p^{v'})} \\
&= \sum_{i=0}^{f-1} \sum_{j=0}^{p-2} \sqrt[f]{d}^{u+u'} \zeta_f^{(u-u')i} \zeta_p^{(v-v')j} \\
&= \sqrt[f]{d}^{u+u'} \sum_{j=0}^{p-2} \zeta_p^{(v-v')j} \sum_{i=0}^{f-1} \zeta_f^{(u-u')i}.
\end{aligned}$$

The norm of the integral basis was $\|\sigma(\sqrt[f]{d}^u \zeta_p^v)\| = \sqrt[f]{d}^u \sqrt{f(p-1)}$. When $u \ne u'$, $\langle \sigma(\sqrt[f]{d}^u \zeta_p^v), \sigma(\sqrt[f]{d}^{u'} \zeta_p^{v'}) \rangle = 0$ because $\sum_{i=0}^{f-1} \zeta_f^{(u-u')i} = 0$. The set of $p-1$ bases, $(p-1)i+1$ to $(p-1)(i+1)$, are orthogonal for different $i (1 \le i \le f-1)$. Therefore, $e \in R$ can be expressed as $e = \sum_{i=0}^{f-1} e_i \sqrt[f]{d}^i$ and $\|e\|^2 := \|\sigma(e)\|^2 = \sum_{i=0}^{f-1} \|e_i\|^2 \sqrt[f]{d}^{2i}$. We note that $e_i \in \mathbb{Z}[\zeta_p]$. In particular, if $e_{f-1} \ne 0$, $\|e\| \ge \|e_{f-1}\| \cdot \sqrt[f]{d}^{f-1} = d^{\frac{f-1}{f}} \cdot \sqrt{f(p-1)}$. If $c = d^{\frac{f-1}{f}}$ for Lemma 1, then $\text{Prob}(\|e\| > c\sqrt{f(p-1)}) \le \left(\frac{c\sqrt{2\pi e}}{r} \cdot e^{-\frac{\pi c^2}{r^2}}\right)^{f(p-1)}$. □

4.2 Experimental Comparison with the χ^2-Attack

In this subsection, we attack the Ring-LWE (mod $\mathfrak{q}$) on several parameters of the composite field, as shown in Sect. 4.1. Each parameter is set as listed in Table 1.

Table 1 The parameters of Ring-LWE samples on the composite field K used in the experiments.

	p	d	q	f	degree of K	r_0
R1	11	504	67	3	30	4.1
R2	13	4872	157	3	36	9.1
R3	13	503	53	4	48	5.0
R4	11	507	67	6	60	7.0

Table 2 The experimental results of the χ^2-attack

	#Sample	Success	Time(sec.)
R1	$67^3 \times 10$	-	5.4×10^7(est.)
R2	$157^3 \times 10$	-	9.1×10^{12}(est.)
R3	$53^4 \times 10$	-	3.2×10^{14}(est.)

Table 3 The experimental results of Algorithm 3

			Basic approach		Improved approach	
	#Sample	subfield	Success	Time(sec.)	Success	Time(sec.)
R1	670	$\mathbb{F}_q$	10/10	1471	10/10	129
R2	1570	$\mathbb{F}_q$	12/12	22808	12/12	1667
R3	530	$\mathbb{F}_{q^2}$	12/12	795	12/12	63
R3	530	$\mathbb{F}_q$	-	-	12/12	3553
R4	670	$\mathbb{F}_{q^3}$	10/10	174267	10/10	9330

Note that the parameter f corresponds to the residue degree, and the parameter r_0 corresponds to the error width. The number of samples is $10 \times q^f$ for the χ^2-attack and $10 \times q$ for our attacks, and the risk ratio for the chi-square test is $\alpha = \frac{1}{10 \times q^f}$ for both. The experimental environment is a CPU: Intel(R) Core(TM) i5-7200U CPU @ 2.500GHz, RAM: 8.0GB, OS: Windows10, and SageMath version 9.2 [29]. All relevant codes are available at https://github.com/TakahashiTomoka/RingLWE.git.

The computational complexity of both the χ^2-attack and the proposed attack are determined by the residue degree, f, and modulus parameter q. In the case of the χ^2-attack shown in Table 2, even with the smallest parameter R1 used in this experiment, the χ^2 attack took unrealistic amount of time to solve Ring-LWE (mod $\mathfrak{q}$). On the other hand, our proposed attack shown in Table 3, we succeeded in solving R1 in less than 30 min, even with the basic approach. Comparing the basic approach with the improved approach, the attack time was reduced by more than 90% for all parameters used in this experiment. In the improved approach, only one multiplication in $\mathbb{F}_q$ is required for the trace map, whereas the computational cost depends on the residue degree f and modulus parameter q in the basic approach. In other words, a significant reduction in computation time can be expected when the residue degree and modulus parameters become large.

The parameter R3 was attacked using the subfield $\mathbb{F}_{q^2}$ and $\mathbb{F}_q$ with the improved approach. The attack time is shorter when using the optimal subfield $\mathbb{F}_{q^2}$ shown in Sect. 3.2. This result indicates the importance of using appropriate subfields in the proposed attack.

The attack failed when using larger error widths r_0 than indicated in Table 1. It is also confirmed that $e_{f-1} \ne 0$ has a higher probability than that shown in Theorem 3.

Although the degree of K is small in this experiment,

the attack succeeds with non-negligible probability for large degrees if the error distribution can be distinguishable from the uniform distribution.

5. Security of Two-Power Cyclotomic Field

In this section, we evaluate the vulnerability of the two-power cyclotomic fields against our attack.

Chen et al. theoretically showed that it is difficult to distinguish the error distribution from the uniform distribution for residue degree $f = 1$ in Sect. 5.1 of [17], although it has not been proven for other residue degrees. A theoretical analysis method using the dual space shown in Lemma 6 has been proposed in [21], but no specific analysis for the two-power cyclotomic fields have been performed. In this section, we show that the two-power cyclotomic fields are secure even when the residue degree is not 1, using the dual basis, and verify the result by experiments.

5.1 Vulnerability Analysis by Dual Basis

Let p be a prime number, m be powers of 2, and ζ_m be a primitive m-th root of 1, then $K = \mathbb{Q}(\zeta_m)$ is the m-th cyclotomic field. The extension degree of $K/\mathbb{Q}$ is $n = m/2$, and the ring of integers of K is $R = \mathbb{Z}[\zeta_m]$. The minimal polynomial of ζ_m is $f(x) = x^n + 1 = (x - \zeta_m)(x^{n-1} + \zeta_m x^{n-2} + \cdots + \zeta_m^{n-2}x + \zeta_m^{n-1})$ and $\frac{df(x)}{dx} = n \cdot x^{n-1}$ [6], [30]. From the lemma 4, the dual basis for the integral basis $\{1, \zeta_m, \zeta_m^2, \cdots \zeta_m^{n-1}\}$ of R is $\{\frac{1}{n}, -\frac{\zeta_m^{n-1}}{n}, -\frac{\zeta_m^{n-2}}{n}, \cdots, -\frac{\zeta_m^2}{n}, -\frac{\zeta_m}{n}\}$ and the norm of these dual bases are all $1/\sqrt{n}$. On the other hand, the composite field $K = \mathbb{Q}(\zeta_p, \sqrt[f]{d})$, which was shown the vulnerablirity in Sect. 4.1, assumes to have a large norm in the integral basis $\{\sqrt[f]{d}^{f-1}, \sqrt[f]{d}^{f-1}\zeta_p, \cdots, \sqrt[f]{d}^{f-1}\zeta_p^{p-2}\}$. If we consider a similar discussion to Sect. 4.3 of [21], the norm of these dual basis are very small. Since the two-power cyclotomic fields cannot have a dual basis as small as the composite fields, it can be said that the two-power cyclotomic fields is secure than the composite fields in the analysis using the dual basis.

5.2 Experimental Analysis of Two-Power Cyclotomic Field

The proposed attack will succeed when the distribution of some error coefficient e_l of $e = \sum_{0 \le l < f} e_l \xi_l (e \leftarrow \psi \pmod{\mathfrak{q}})$ is distinguishable from the uniform distribution, $U(\mathbb{F}_q)$. The experimental results confirm that e_l has a similar distribution for any l, so we report the experimental results for e_0.

Figure 1 shows the number of times that the distribution of e_0 was different from the uniform distribution out of 100 times of chi-square tests when the error width r_0 was changed. The parameters, (m, q, f), were chosen to be the modulus q with residue degree $f = 2, 4, 8$ in cyclotomic fields of $m = 64, 128$, and the risk ratio is $\alpha = 0.05$. The experimental results confirmed that the larger error width r_0 and m, the smaller modulus q and residue degree f, the more difficult it is to distinguish from a uniform distribution. Experiments confirmed that the two-power cyclotomic fields

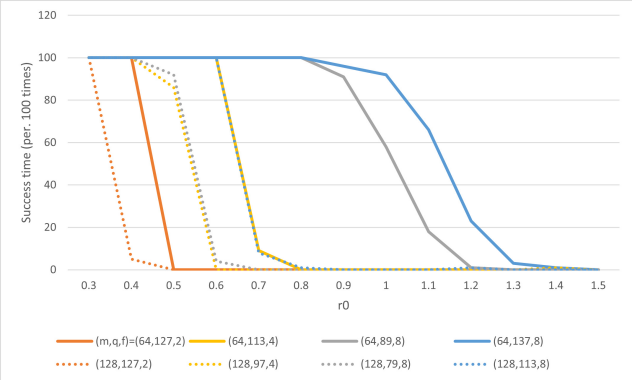

Fig. 1 Experimental result for the two-power cyclotomic fields

are secure against the proposed attack compared to the composite fields $\mathbb{Q}(\zeta_p, \sqrt[f]{d})$, similar to the analysis in dual space. However, our attack can be a threat even for the two-power cyclotomic fields if the error is sufficiently small. Therefore, careful parameter setting is required for applications.

6. Conclusion

In this paper, we improved the χ^2-attack to work efficiently for any residue degree. Our attack showed that the algebraic property of the Ring-LWE problem can be used for attacks as well as for efficiency. The error distributions that determine the success of our attack varies with number fields, confirming that it is useful to analyze from field's duality. In Sect. 5.2, one of the most commonly used number fields, the two-power cyclotomic field, was confirmed to be secure against our proposed attack although the necessity of careful error sampling. However, there are some fields that are vulnerable to our attack, as shown in Sect. 4.1. Attacks using prime ideals as in this study and previous works suggest the importance of proper error sampling in applications. We believe that these attacks are also effective for other LWE problems with ring structures such as M-LWE. While considering the freely configurable attack parameter θ, further research of the error distributions for general number fields is needed for security analysis of lattice-based cryptograpy.

Acknowledgements

This work is partially supported by JSPS KAKENHI Grant Number JP21H03443 and SECOM Science and Technology Foundation.

References

[1] The National Institute of Standards and Technology (NIST), "Post-quantum cryptograph," https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[2] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J.M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS - kyber: A cca-secure module-lattice-based KEM," 2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, pp.353–367, IEEE, 2018.

[3] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS - dilithium: Digital signatures from module lattices," IACR Cryptol. ePrint Arch., 633, 2017.
[4] T. Pornin and T. Prest, "More Efficient Algorithms for the NTRU Key Generation Using the Field Norm," Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, ed. D. Lin and K. Sako, Lecture Notes in Computer Science, vol.11443, pp.504–533, Springer, 2019.
[5] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," Journal of the ACM (JACM), vol.56, no.6, pp.1–40, 2009.
[6] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," Journal of the ACM (JACM), vol.60, no.6, pp.1–35, 2013.
[7] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(leveled) fully homomorphic encryption without bootstrapping," ACM Transactions on Computation Theory (TOCT), vol.6, no.3, pp.1–36, 2014.
[8] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," Designs, Codes and Cryptography, vol.75, no.3, pp.565–599, 2015.
[9] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange - A new hope," 25Th USENIX security symposium (USENIX security 16), pp.327–343, 2016.
[10] X. Lu, Y. Liu, Z. Zhang, D. Jia, H. Xue, J. He, B. Li, and K. Wang, "LAC: Practical Ring-LWE Based Public-Key Encryption with Byte-Level Modulus," IACR Cryptol. ePrint Arch., 1009, 2018.
[11] S. Arita and S. Handa, "Fully Homomorphic Encryption Scheme Based on Decomposition Ring," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol.103-A, no.1, pp.195–211, 2020.
[12] M.R. Albrecht and A. Deo, "Large Modulus Ring-LWE ≥ Module-LWE," Advances in Cryptology - ASIACRYPT 2017, Lecture Notes in Computer Science, vol.10624, pp.267–296, Springer, 2017.
[13] Y. Wang and M. Wang, "Module-LWE versus Ring-LWE, Revisited," IACR Cryptol. ePrint Arch., 930, 2019.
[14] Y. Ikematsu, S. Nakamura, and M. Yasuda, "A Trace Map Attack Against Special Ring-LWE Samples," IWSEC 2021, Proceedings, ed. T. Nakanishi and R. Nojima, Lecture Notes in Computer Science, vol.12835, pp.3–22, Springer, 2021.
[15] G. Bonnoron and C. Fontaine, "A Note on Ring-LWE Security in the Case of Fully Homomorphic Encryption," Progress in Cryptology - INDOCRYPT 2017, Lecture Notes in Computer Science, vol.10698, pp.27–43, Springer, 2017.
[16] H. Chen, K. Lauter, and K.E. Stange, "Attacks on the Search RLWE Problem with Small Errors," SIAM J. Appl. Algebra Geom., vol.1, no.1, pp.665–682, 2017.
[17] H. Chen, K. Lauter, and K.E. Stange, "Security Considerations for Galois Non-dual RLWE Families," Selected Areas in Cryptography - SAC 2016, ed. R. Avanzi and H.M. Heys, Lecture Notes in Computer Science, vol.10532, pp.443–462, Springer, 2016.
[18] T. Takahashi, S. Okumura, and A. Miyaji, "On the weakness of ring-LWE mod prime ideal q by trace map," 29th Selected Areas in Cryptography (SAC), 2022.
[19] A.K. Lenstra, H.W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," Mathematische annalen, vol.261, no.ARTICLE, pp.515–534, 1982.
[20] C.P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," Mathematical programming, vol.66, no.1, pp.181–199, 1994.
[21] C. Peikert, "How (Not) to Instantiate Ring-LWE," Security and Cryptography for Networks - 10th International Conference, SCN 2016, ed. V. Zikas and R.D. Prisco, Lecture Notes in Computer Science, vol.9841, pp.411–430, Springer, 2016.
[22] E. Kaltofen and V. Shoup, "Fast polynomial factorization over high algebraic extensions of finite fields," Proc. 1997 international symposium on Symbolic and algebraic computation, pp.184–188, ACM, 1997.
[23] W.G. Cochran, "Some methods for strengthening the common χ^2 tests," Biometrics, vol.10, no.4, pp.417–451, 1954.
[24] K. Saka, T. Mizuhara, and C. Uno, Reidaichusin Kakuritsu Toukei Nyuumon (Introduction of statistics), Gakujutsu Tosho Shuppansha, 2016 (in Japanese).
[25] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," SIAM Journal on Computing, vol.37, no.1, pp.267–302, 2007.
[26] K. Conrad, "The different ideal," 2009. Available at: https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf.
[27] M. Rosca, D. Stehlé, and A. Wallet, "On the Ring-LWE and Polynomial-LWE Problems," Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, ed. J.B. Nielsen and V. Rijmen, Lecture Notes in Computer Science, vol.10820, pp.146–173, Springer, 2018.
[28] Y. Elias, K.E. Lauter, E. Ozman, and K.E. Stange, "Provably Weak Instances of Ring-LWE," Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, ed. R. Gennaro and M. Robshaw, Lecture Notes in Computer Science, vol.9215, pp.63–92, Springer, 2015.
[29] The Sage Developers, SageMath, Sage Mathematics Software System (Version 9.2), 2020.
[30] Y. Morita, Daisugairon (Introduction of Algebra), Shokabo, 2015 (in Japanese).

Tomoka Takahashi received the B. Sc. in mathematics from Nara Women's University in 2021 and received the M. Sc. in engineering from Osaka University in 2023. She has been with MegaChips Corporation since April 2023.

Shinya Okumura received Dr. Sci. degree in mathematics from Kyushu University in 2015. After working as an academic Researcher, Institute of Math-for-Industry, Kyushu University (April 2015–April 2016), a researcher, Information Security Laboratory, Kyushu Institute of Advanced Science and Technology (May 2016–January 2017), a specially-appointed assistant professor at the Graduate School of Engineering, Osaka University (February 2017–March 2018), Currently, he is an Assistant Professor at Graduate School of Engineering, Osaka University, since April 2018. His main research areas are post quantum cryptography and algorithmic number theory. In 2016, he received the CANDAR 2016, Outstanding Paper Award, and the the IEICE ESS 2016 Information Security Research Encouragement Award. He received the Best Young Speaker Award in 2016 from the Japan Society for Industrial and Applied mathematics.

Atsuko Miyaji received the B. Sc., the M. Sc., and the Dr. Sci. degrees in mathematics from Osaka University,in 1988, 1990, and 1997 respectively. She is an IPSJ fellow. She joined Panasonic Co., LTD from 1990 to 1998 and engaged in research and development for secure communication. She was an associate professor at the Japan Advanced Institute of Science and Technology (JAIST) in 1998. She joined the computer science department of the University of California, Davis from 2002 to 2003. She has been a professor at Japan Advanced Institute of Science and Technology (JAIST) since 2007. She has been a professor at Graduate School of Engineering, Osaka University since 2015. Her research interests include the application of number theory into cryptography and information security. She received Young Paper Award of SCIS '93 in 1993, Notable Invention Award of the Science and Technology Agency in 1997, the IPSJ Sakai Special Researcher Award in 2002, the Standardization Contribution Award in 2003, the AWARD for the contribution to CULTURE of SECURITY in 2007, the Director-General of Industrial Science and Technology Policy and Environment Bureau Award in 2007, DoCoMo Mobile Science Awards in 2008, Advanced Data Mining and Applications (ADMA 2010) Best Paper Award, Prizes for Science and Technology, the Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology, International Conference on Applications and Technologies in Information Security (ATIS 2016) Best Paper Award, the 16th IEEE Trustocm 2017 Best Paper Award, IEICE milestone certification in 2017, the 14th Asia Joint Conference on Information Security (AsiaJCIS 2019) Best Paper Award, Information Security Applications - 20th International Conference (WISA 2020) Best Paper Gold Award, IEICE Distinguished Educational Practitioners Award in 2020, and IEICE Achievement Award in 2023. She is a member of the International Association for Cryptologic Research, the Institute of Electrical and Electronics Engineers, the Institute of Electronics, Information and Communication Engineers, the Information Processing Society of Japan, and the Mathematical Society of Japan.