Attacks on Search-RLWE

No Author Given

No Institute Given

Abstract. We describe a new attack on the Ring learning-with-errors (RLWE) problem based on the chi-square statistical test, and give examples of Galois number fields vulnerable to our attack. We then analyze the security of cyclotomic fields against our attack.

1 Introduction

The Ring Learning-with-Errors (RLWE) problem, proposed in [8], is a variant of the traditional Learning-with-Errors (LWE) problem, and is an active research area in lattice based cryptography. It has been studied extensively in (a lot of papers).

Central to an RLWE problem instance is a choice of a number field K and a prime q called the *modulus*. The authors of [8] considered the case where K is some cyclotomic field, and proved a reduction from certain hard lattice problems to the dual variant of RLWE. The hardness for the non-dual variant was proved in [2]. Also in [8], a search-to-decision reduction was proved for RLWE problems for cyclotomic fields and modulus q which splits completely. This reduction was then generalized to general Galois extensions in [3].

The authors of [4] proposed an attack to decision RLWE problem. The attack makes use of ring homomorphisms $\pi : R \to \mathbb{F}_q$, and works when the image of the RLWE error distribution under the map π only takes value in a stricly smaller subset of $\mathbb{F}_q$, with overwhelming probability. The authors of [4] then gave an infinite family of examples vulnerable to the attack. Unfortunately, the vulnerable number fields in [4] are not Galois extensions of $\mathbb{Q}$. Hence, the search-to-decision reduction theorem does not apply, and the attack can not be directly used to solve the search variant of RLWE for those instances.

In our paper, we generalize the attack of [4] to Galois number fields and moduli of higher degree. Also, we analyze the vulnerability of cyclotomic fields to the [4] attack, and show that they are in general safe, except for the case when the modulus p is equal to the index of the cyclotomic field (i.e., $K = \mathbb{Q}(\zeta_p)$).

1.1 Organization

In section 2, we recall the canonical embedding of number fields and central definitions related to the RLWE problems. In section 3, we review prime factorizations in Galois extensions and prove a search-to-decision reduction for Galois extensions K and unramified moduli. In section 4, we introduce an attack to RLWE problems based on the chi-square statistical test, which directly generalizes the attack in [4]. More precisely, the attack aims at an intermediate problem used in the search-to-decision proof of [8], which we denote by $\mathrm{SRLWE}(\mathcal{R}, \mathfrak{q})$ (see Definition 3.1). The time complexity of our attack is $O(q^{2f})$, where f is the *residual degree* of q in K (see Lemma 3.1). In section 5, we give examples of subfields of cyclotomic fields vulnerable to our new attack, where the modulus q has residual degree two.

In section 6, we show that our attack works on prime cyclotomic fields when the modulus is the unique ramified prime. Finally, in section 8, we use Fourier analysis to give numerical evidence that cyclotomic extensions with unramified moduli are invulnerable to our attack.

All computations in this paper were performed in Sage [11]. All relevant code can be found at `https://github.com/haochenuw/GaloisRLWE`.

2 Background

Let K be a number field of degree n with ring of integers R and let $\sigma_1, \cdots, \sigma_n$ be the embeddings of K into $\mathbb{C}$, the field of complex numbers. The *canonical embedding* of K is

$$\begin{aligned} \iota : K &\to \mathbb{C}^n \\ x &\mapsto (\sigma_1(x), \cdots, \sigma_n(x)). \end{aligned}$$

To work with real vector spaces, we define the *adjusted embedding* of K as follows. Let r_1, r_2 denote the number of real embeddings and conjugate pairs of complex embeddings of K. Without loss of generality, assume $\sigma_1, \cdots, \sigma_{r_1}$ are the real embeddings and $\sigma_{r_1+r_2+j} = \overline{\sigma_{r_1+j}}$ for $1 \le j \le r_2$. We define

$$\begin{aligned} \tilde{\iota} : K &\to \mathbb{R}^n \\ x &\mapsto (\sigma_1(x), \cdots, \sigma_{r_1}(x), \Re(\sigma_{r_1+1})(x), \Im(\sigma_{r_1+1})(x), \cdots, \Re(\sigma_{r_1+r_2})(x), \Im(\sigma_{r_1+r_2})(x)). \end{aligned}$$

Then $\tilde{\iota}(R)$ is a lattice in $\mathbb{R}^n$. Let $w = (w_1, \cdots, w_n)$ be an integral basis for R.

Definition 2.1. *The canonical (resp. adjusted) embedding matrix of w, denoted by A_w (resp. $\widetilde{A_w}$), is the n-by-n matrix whose i-th column is $\iota(w_i)$ (resp. $\tilde{\iota}(w_i)$).*

The two embedding matrices are related in a simple way: let T denote the unitary matrix

$$T = \begin{bmatrix} I_{r_1} & 0 \\ 0 & T_{r_2} \end{bmatrix}, \text{ where } T_s = \frac{1}{\sqrt{2}} \begin{bmatrix} I_{r_2} & I_{r_2} \\ -iI_{r_2} & iI_{r_2} \end{bmatrix},$$

Then we have

$$\widetilde{A_w} = TA_w,$$

and the lattice $\tilde{\iota}(R)$ has a basis consisting of columns of $\widetilde{A_w}$.

For $\sigma > 0$, define the Gaussian function $\rho_\sigma : \mathbb{R}^n \to [0, 1]$ as $\rho_\sigma(x) = e^{-||x||^2/2\sigma^2}$ (our σ is equal to $r/\sqrt{2\pi}$ for the parameter r in [8]).

Definition 2.2. *For a lattice $\Lambda \subset \mathbb{R}^n$ and $\sigma > 0$, the discrete Gaussian distribution on Λ with parameter σ is:*

$$D_{\Lambda,\sigma}(x) = \frac{\rho_\sigma(x)}{\sum_{y \in \Lambda} \rho_\sigma(y)}, \ \forall x \in \Lambda.$$

Equivalently, the probability of sampling any lattice point x is proportional to $\rho_\sigma(x)$.

2.1 Ring LWE problems for general number fields

We follow [4] in setting up the Ring LWE problem for general number fields. In particular, we do not consider the dual of the ring of integers, which is a convenience only in the case of the cyclotomic integers.

Definition 2.3. *An RLWE instance is a tuple $\mathcal{R} = (K, q, \sigma, s)$, where K is a number field with ring of integers R, q is a prime, $\sigma > 0$, and $s \in R/qR$ is the secret.*

Definition 2.4. *Let $\mathcal{R} = (K, q, \sigma, s)$ be an RLWE instance and let R be the ring of integers of K. The error distribution of $\mathcal{R}$, denote by $D_{\mathcal{R}}$, is the discrete Gaussian distribution*

$$D_{\mathcal{R}} = D_{\tilde{\iota}(R),\sigma}.$$

Let n denote the degree of K. As pointed out in [4], when analyzing the error distribution, one needs to take into account the sparsity of the lattice $\tilde{\iota}(R)$, which is measured by its covolume V_R. In light of this, we define a relative version of the standard deviation parameter:

$$\sigma_0 = \frac{\sigma}{V_R^{\frac{1}{n}}}.$$

The notation $x \leftarrow D$ indicates that variable x is distributed according to distribution D.

Definition 2.5 (RLWE distribution). *Let $\mathcal{R} = (K, q, \sigma, s)$ be an RLWE instance with error distribution $D_{\mathcal{R}}$. We let R_q denote R/qR, then a sample from the RLWE distribution of $\mathcal{R}$ is a tuple*

$$(a, b = as + e \pmod{qR}) \in R_q \times R_q,$$

where the first coordinate a is chosen uniformly at random in R_q, and $e \leftarrow D_{\mathcal{R}}$.

We use the shorthand notation $(a, b) \leftarrow \mathcal{R}$ to represent that (a, b) is sampled from the RLWE distribution of $\mathcal{R}$.

The RLWE problem has two major variants: search and decision.

Definition 2.6 (Search RLWE). *Let $\mathcal{R}$ be an RLWE instance. The search Ring-LWE problem, denoted by* $\mathrm{SRLWE}(\mathcal{R})$*, is to discover s given access to arbitrarily many independent samples $(a, b) \leftarrow \mathcal{R}$.*

Definition 2.7 (Decision RLWE). *Let $\mathcal{R}$ be an RLWE instance. The decision Ring-LWE problem, denoted by* $\mathrm{DRLWE}(\mathcal{R})$*, is to distinguish between the same number of independent samples in two distributions on $R_q \times R_q$. The first is the RLWE distribution of $\mathcal{R}$, and the second consists of uniformly random and independent samples from $R_q \times R_q$.*

2.2 Sampling methods

In practice, there are different ways to approximately sample from the RLWE error distribution $D_{\mathcal{R}}$, and we will consider three sampling methods in our paper. While searching for weak Galois RLWE instances as well as attacking ramified primes, we use the sampling algorithm in [5]; when analyzing the security of cyclotomics, we use the PLWE distribution $P_{m,\tau}$ and another distribution $P'_{m,k}$ to assist the analysis. The efficient sampling algorithm in [9] for cyclotomic fields is related to the dual version of RLWE, we will not use it in our paper.

3 search-to-decision reduction

In [3], the search-to-decision reduction of [8] is extended to Ring-LWE for Galois number fields, where q is an unramified prime of degree one. The approach is via an intermediate problem, denoted $\mathfrak{q}_i$-LWE in [8]. In this section, we extend this result to primes $\mathfrak{q}$ of arbitrary residual degree. Our intermediate problem, which we denote by $\mathrm{SRLWE}(\mathcal{R}, \mathfrak{q})$, is to find the secret modulo the prime. The Galois group allows us to bootstrap this piece of information to discover the full secret.

The attack in Section 4 targets $\mathrm{SRLWE}(\mathcal{R}, \mathfrak{q})$ and hence, by the results of this section, will solve Search Ring-LWE. In Section 5, we demonstrate the attack on Search Ring-LWE in practice.

Definition 3.1. *Let $\mathcal{R} = (K, q, \sigma, s)$ be an RLWE instance, and let $\mathfrak{q}$ be a prime of K lying above q. The problem* $\mathrm{SRLWE}(\mathcal{R}, \mathfrak{q})$ *is to determine $s \pmod{\mathfrak{q}}$, given access to arbitrarily many independent samples $(a, b) \leftarrow \mathcal{R}$.*

We recall some facts from algebraic number theory in the following lemma.

Lemma 3.1. *Let $K/\mathbb{Q}$ be a finite Galois extension with ring of integers R, and let q be a prime unramified in K. Then there exists a unique choice of integer $g \mid n$, and set of g distinct prime ideals $\mathfrak{q}_1, \cdots, \mathfrak{q}_g$ of R such that:*

1. *$qR = \prod_{i=1}^{g} \mathfrak{q}_i$,*
2. *the quotient $R/\mathfrak{q}_i$ is a finite field of cardinality q^f for each i, where $f = \frac{n}{g}$,*
3. *there is a canonical isomorphism of rings*

$$R_q \cong R/\mathfrak{q}_1 \times \cdots \times R/\mathfrak{q}_g, \tag{1}$$

4. *the Galois group acts transitively on the ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ and this action descends to an action on R_q which permutes the corresponding factors in (1) in the same way.*

The number f in the above lemma is called the *residual degree* of q in K. Note that the prime q splits completely in K if and only if its residual degree is one.

Theorem 3.1. *Let $\mathcal{R} = (K, q, \sigma, s)$ be an RLWE instance with $K/\mathbb{Q}$ Galois of degree n and q unramified in K with residual degree f. Let $\mathscr{A}$ be an oracle which solves* $\mathrm{SRLWE}(\mathcal{R}, \mathfrak{q})$ *using a list of m samples modulo $\mathfrak{q}$. Let S be a set of m RLWE samples in $R_q \times R_q$. Then the problem* $\mathrm{SRLWE}(\mathcal{R})$ *can be solved using S by n/f calls to the oracle $\mathscr{A}$, $2mn/f$ reductions $R_q \to R/\mathfrak{q}$, and $2mn/f$ evaluations of a Galois automorphism on R_q.*

Proof. The Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ acts on the set $\{\mathfrak{q}_1, \cdots, \mathfrak{q}_g\}$ transitively. Hence for each i, there exists $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$, such that $\sigma_i(\mathfrak{q}) = \mathfrak{q}_i$, Then we call the oracle $\mathscr{A}$ on the input $(\sigma_i^{-1}(S) \pmod{\mathfrak{q}}, \mathfrak{q})$. The algorithm will output $\sigma_i^{-1}(s) \pmod{\mathfrak{q}}$, from which we can recover $s \pmod{\mathfrak{q}_i}$ using σ_i. We do this for all $1 \le i \le g$ and use (1) of Lemma 3.1 to recover s. □

It does? What does polynomial time mean in this context? It is an $O(n)$ reduction, yes?

I did a lot of rewriting here in Lemma 3.2 and Theorem 3.3.

Theorem 3.1 gives a polynomial time reduction from $\mathrm{SRLWE}(\mathcal{R})$ to $\mathrm{SRLWE}(\mathcal{R}, \mathfrak{q})$.

Remark 3.1. For a proper runtime analysis of the reduction, one must examine the implementation, in particular with regards to Galois automorphisms. The runtime for evaluating an automorphism depends rather strongly on the instance and on the way ring elements are represented. For example, for subfields of cyclotomic fields represented with respect to normal integral bases, the Galois autormophisms are simply permutations of the coordinates, so the time needed to apply these automorphisms is trivial.

The search-to-decision reduction will follow from the lemma below.

Lemma 3.2. *There is a probabilistic polynomial time reduction from* $\mathrm{SRLWE}(\mathcal{R}, \mathfrak{q})$ *to* $\mathrm{DRLWE}(\mathcal{R})$.

Proof. This is a rephrasing of [8, Lemma 5.9 and Lemma 5.12]. □

Corollary 3.1. *Suppose $\mathcal{R}$ is an RLWE instance where K is Galois and q is an unramified prime in K. Then there is a probabilistic polynomial-time reduction from* $\mathrm{SRLWE}(\mathcal{R})$ *to* $\mathrm{DRLWE}(\mathcal{R})$.

4 The chi-square attack for uniform distribution

In this section, we extend the $f(1) \equiv 0 \pmod q$ attack of [3] and the root-of-small-order attack of [4]. These attacks can be viewed as examples of a more general attack principle, as follows. Suppose one has a ring homomorphism

$$\phi : R_q \to F$$

where F is a finite field, and where two properties hold:

1. F is small enough that its elements can be examined exhaustively; and
2. the error distribution on R_q, transported by ϕ to F, is detectably non-uniform.

Then the attack on DRLWE on R_q is as follows:

1. Transport the samples (a, b) in $R_q \times R_q$ to $F \times F$ via ϕ.
2. Loop through possible guesses for the image of the secret, $\phi(s)$, in F.
3. For each guess g, compute the distribution of $\phi(b) - \phi(a)g$ on the available samples (this is $\phi(e)$ if the guess is correct).
4. If the samples are RLWE samples with secret s and $g = \phi(s)$, then this distribution will follow the error distribution, which will look non-uniform.
5. If all such distributions look uniform, then the samples were uniform, not RLWE, samples.

The fact that ϕ is a ring homomorphism is essential in guaranteeing that for the correct guess, the distribution in question is the image of the error distribution. The only ring homomorphisms from R_q to a finite field are given by reduction modulo a prime ideal $\mathfrak{q}$ lying above q in R.

4.1 chi-square test for uniform distribution

We briefly review the properties and usage of the chi-square test for uniform distributions over a finite set S. We partition S into r subsets $S = \bigsqcup_{j=1}^{r} S_j$. Suppose there are M samples $y_1, \ldots, y_M \in S$. For each $1 \le j \le r$, we compute the expected number of samples in the j-th subset: $c_j := \frac{|S_j| M}{|S|}$. Then we compute the actual number of samples in S_j, i.e., $t_j := |\{1 \le i \le r : y_i \in S_j\}|$. Finally, the χ^2 value is computed as

$$\chi^2(S, y) = \sum_{j=1}^{r} \frac{(t_j - c_j)^2}{c_j}.$$

Suppose the samples are drawn from the uniform distribution on S. Then the χ^2 value follows the chi-square distribution with $(r-1)$ degrees of freedom, which we denote by χ^2_{r-1}. Let $\mathcal{F}_{r-1}(x)$ denote its cumulative distribution function. For the chi-square test, we choose a confidence level parameter $\alpha \in (0,1)$ and compute $\delta = \mathcal{F}^{-1}_{r-1}(\alpha)$. Then we reject the hypothesis that the samples are drawn from the uniform distribution if $\chi^2(S,y) > \delta$.

If P, Q are two probability distributions on the set S, then their *statistical distance* is defined as

$$d(P,Q) = \frac{1}{2}\sum_{t\in S}|P(t) - Q(t)|.$$

For convenience, we also define the l_2 *distance* between P and Q as $d_2(P,Q) = (\sum_{t\in S}|P(t)-Q(t)|^2)^{\frac{1}{2}}$. We have the inequality $d(P,Q) \le \frac{\sqrt{|S|}}{2} d_2(P,Q)$.

4.2 The chi-square attack on SRLWE($\mathcal{R}, \mathfrak{q}$)

Let $\mathcal{R}$ be an RLWE instance with error distribution $D_{\mathcal{R}}$ and $\mathfrak{q}$ be a prime ideal above q. The basic idea of our attack relies on the assumption that the distribution $D_{\mathcal{R}} \pmod{\mathfrak{q}}$ is distinguishable from the uniform distribution on the finite field $F = R/\mathfrak{q}$. More precisely, the attack loops through all q^f possible values $\bar{s} = s \pmod{\mathfrak{q}}$, and for each guess s', it computes the values $\bar{e}' = \bar{b} - \bar{a}s' \pmod{\mathfrak{q}}$ for every sample $(a,b) \in S$. If the guess is wrong, or if the samples are taken from the uniform distribution in $(R_q)^2$, the values $\bar{e}'$ would be uniformly distributed in F and it is likely to pass the chi-square test. On the other hand, if the guess is correct, then we expect the test on the errors $\bar{e}'$ to reject the null hypothesis. Let $N = q^f$ denote the cardinality of F. We remark that one needs at least $\Omega(N)$ samples for the test to work effectively.

For the attack to be successful, we need the $(N-1)$ tests corresponding to wrong guesses of $s \pmod{\mathfrak{q}}$ to pass, and the one test corresponding to the correct guess to be rejected. For this purpose, we need to choose the confidence level α to be close enough to one (a reasonable choice is $\alpha = 1 - \frac{1}{10N}$). The detailed attack is described in Algorithm 1. Let $\mathcal{F}_{N-1}(x)$ denote the cumulative distribution function of χ^2_{N-1}.

Why is Φ from standard normal distr and not from χ^2 distribution?

Algorithm 1 chi-square attack of $SRLWE(\mathcal{R}, \mathfrak{q})$

Does it matter what bins we use? For example, I think a subfield should be a bin, given the patterns we've observed. Maybe we should put this choice in the Require too.

Input: $\mathcal{R} = (K, q, \sigma, s)$ – an RLWE instance; R – the ring of integers of K; $\mathfrak{q}$ – a prime ideal in K above q; $F = R/\mathfrak{q}$ – the residual field of $\mathfrak{q}$; N – the cardinality of F; $\mathcal{S}$ – a collection of M $(M = \Omega(N))$ RLWE samples from $\mathcal{R}$; $0 < \alpha < 1$ – the confidence level.
Output: a guess of the value $s \pmod{\mathfrak{q}}$, or **NOT-RLWE**, or **INSUFFICIENT-SAMPLES**

```
δ ← F_{N-1}^{-1}(α), G ← ∅.
for s in F do
    E ← ∅.
    for a, b in S do
        ā, b̄ ← a (mod q), b (mod q).
        ē ← b̄ − ā s.
        add ē to E.
    end for
    χ²(E) ← Σ_{j=1}^{N} (|{c ∈ E : c = j}| − M/N)² / (M/N).
    if χ²(E) > δ then
        add s to G.
    end if
end for
if G = ∅ then
    return NOT-RLWE
else if G = {g} then
    return g
else
    return INSUFFICIENT-SAMPLES
end if
```

I think in the algorithm it would be best to use the chi-squared distribution not the normal approximation; in implementations, people can be looser, but no reason not to do it properly in theory.

The time complexity of the attack is $O(N^2)$ since there are N possible values for $s \pmod{\mathfrak{q}}$ and the number of samples needed is $O(N)$. The correctness of the attack is captured in Theorem 4.1 below. We use $D_{\mathcal{R},\mathfrak{q}}$ as a shorthand notation for $D_{\mathcal{R}} \pmod{\mathfrak{q}}$. Let Δ denote the statistical distance between the distribution $D_{\mathcal{R},\mathfrak{q}}$ and the uniform distribution on $R/\mathfrak{q}$. For $\lambda \in \mathbb{R}$ and $d \in \mathbb{Z}$, we use $\mathcal{F}_{d,\lambda}(x)$ to denote the cumulative distribution function of the noncentral chi-square distribution with degree of freedom d and parameter λ.

The explanation of Φ should go in background along with confidence level stuff.

This requirement of the chi-square test should go in background section

Define α in statement.

Theorem 4.1. *Let M be the number of samples used in Algorithm 1, and let $\lambda = 4M\Delta^2$. Let $0 < \alpha < 1$ and let $\delta = \mathcal{F}_{N-1}^{-1}(\alpha)$. If p is the probability of success of the attack in Algorithm 1, then*

$$p \geq \alpha^{N-1}(1 - \mathcal{F}_{N-1;\lambda}(\delta)).$$

Proof. It is a standard fact (see [10], for example) that the chi-square value on samples from $D_{\mathcal{R},\mathfrak{q}}$ follows the noncentral chi-square distribution with $(N-1)$ degrees of freedom and parameter λ_0 given by

$$\lambda_0 = d_2(D_{\mathcal{R},\mathfrak{q}}, U(R/\mathfrak{q}))^2 \cdot MN.$$

Note that we have $\lambda_0 \geq (2d(D_{\mathcal{R},\mathfrak{q}}, U(R/\mathfrak{q}))/\sqrt{N})^2 MN = 4M\Delta^2 = \lambda$. Recall that our attack succeeds if the "error" set $\mathcal{E}$ from each of the $(N-1)$ wrong guesses of $s \pmod{\mathfrak{q}}$ passes the test, and the true reduced errors fails the test. We assume that the results of these tests are independent of each other. Then the first event happens with probability α^{N-1}, whereas the second event has probability $(1 - \mathcal{F}_{N-1;\lambda_0}(\delta))$. Since this is an increasing function in λ_0, we replace λ_0 by λ and the theorem follows. $\square$

I'm worried about the approximation by a normal distribution; at the very least the probability needs to be given as a bound, not an exact probability.

Remark 4.1. One could vary α in Theorem 4.1 to suit the specific instance. The probability of success will change accordingly. When we expect the statistical distance Δ to be large, it is preferable to choose a larger α to increase the probability of success. For example, if we choose $\alpha = 1 - \frac{1}{10N}$, then $\alpha^{N-1} \geq e^{-1/10} = 0.904\cdots$.

Figure 1 shows a plot of p versus Δ for various choices of N, made according to Theorem 4.1, where we fix the number of samples to be $M = 5N$ and fix $\alpha = 1 - \frac{1}{10N}$.

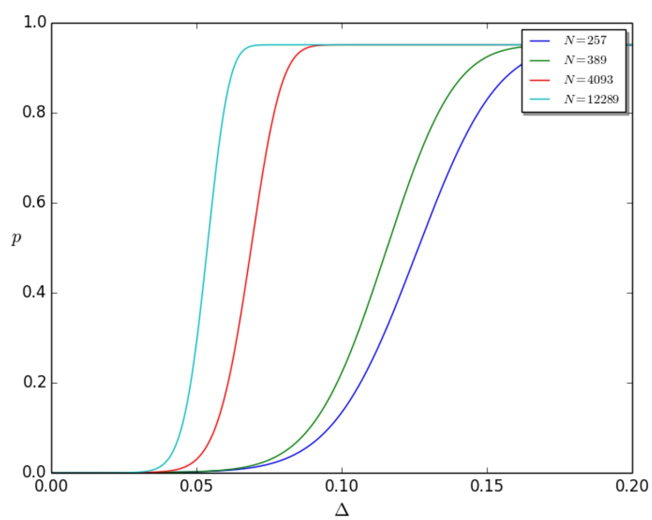

Fig. 1. Success probability versus statistical distance

5 Vulnerable instances among subfields of cyclotomic fields

We searched for instances of RLWE vulnerable to the chi-square attack. For this purpose, we restricted attention to subfields of cyclotomic fields $\mathbb{Q}(\zeta_m)$, where we assume m is *odd and squarefree*. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is canonically isomorphic to $G = (\mathbb{Z}/m\mathbb{Z})^*$. For each subgroup H of G, let $K_{m,H} = \mathbb{Q}(\zeta_m)^H$ be the subfield of elements fixed by H. Then the extension $K_{m,H}/\mathbb{Q}$ is Galois with degree $n = \frac{\varphi(m)}{|H|}$. Also, the residual degree of a prime q in $K_{m,H}$ is equal to the order of $[q]$ in the quotient group G/H. Moreover, $K_{m,H}$ has canonical *normal integral basis*, whose embedding matrix is easy to compute. More precisely, let C denote a set of coset representatives of the coset space G/H. If c is an integer coprime to m, we use $[c]$ to denote its coset in G/H. For each $[c] \in C$, set

$$w_{[c]} = \sum_{h \in H} \zeta_m^{hc}.$$

Then $w := (w_{[c]})_{[c] \in C}$ is a $\mathbb{Z}$-basis of R. (For a proof of this fact, see [6, Proposition 6.1]). Setting $\zeta = \exp(2\pi i/m)$, the canonical embedding embedding matrix of w is

$$(A_w)_{[i],[j]} = \sum_{h \in H} \zeta^{hij}, \text{ for } [i],[j] \in C.$$

Lemma 5.1. *Suppose $\mathcal{R}$ is an RLWE instance such that the underlying field K is a Galois number field and q is unramified in K. Then the reduced error distribution $D_{\mathcal{R},\mathfrak{q}}$ is independent of the choice of prime ideal $\mathfrak{q}$ above q.*

Proof. From Lemma 3.1, we may change from a prime $\mathfrak{q}$ to $\mathfrak{q}'$ via $\mathrm{Gal}(K/\mathbb{Q})$. On the other hand, the Galois group acts on the embedded lattice Λ_R by permuting the coordinates. Hence we have a group homomorphism

$$\phi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(\Lambda).$$

Since permutation matrices are orthogonal, the Galois group action on Λ_R given by ϕ is distance-preserving. In particular, it preserves any spherical discrete Gaussian distribution on Λ_R. □

5.1 Searching

Algorithm 1 allows us to search for vulnerable instances among fields of form $K_{m,H}$ by generating actual RLWE samples and running the attack. Success of the attack will indicate vulnerability of the instance. Note that our field searching requires sampling efficiently from a discrete Gaussian $D_{\Lambda,\sigma}$, for which we use the efficient algorithm of [5].

In Table 1, we list some instances on which the attack has succeeded. The columns of Table 1 are as follows. The first two columns specify m and the generators of H; the column labeled f is the residual degree of q. The last column consists of either the runtime for an actual attack, or an estimation of the runtime. Note that we omitted our choice of prime ideal $\mathfrak{q}$, since due to Lemma 5.1 the choice of $\mathfrak{q}$ is irrelevant to our attack.

Is this really what you did, Hao? It seems like it makes more sense to just chi-square test the distribution of errors, instead of running the full attack (i.e. looping through guesses).

I think there should be some discussion of how σ_0 was chosen

5.2 Discussion

All the vulnerable instances found in Table 1 involve primes of degree 2. We have a heuristic explanation for this phenomenon. Let K be a Galois number field and suppose q is a prime of degree r in K. Suppose we have found a short basis $w_1, \cdots, w_n$ of R with respect to the adjusted embedding. Fix a prime ideal $\mathfrak{q}$ above q. Then the images of the basis under the reduction modulo $\mathfrak{q}$ map are elements of $F = R/\mathfrak{q}$. Now if for some index i, the element w_i lies inside some proper subfield K' of K, and if q has residual degree $r' < r$ in K', then $w_i \pmod{\mathfrak{q}}$ will lie in a proper subfield of F. If this occurs for a large number of the basis elements w_i, then we could expect the reduced error distribution $D_{\mathcal{R},\mathfrak{q}}$ to take values in a proper subfield of F more frequently. This would allow us to distinguish it from the uniform distribution on F.

Did you search $f > 2$ examples? The first sentence seems to imply you searched all f and only found $f = 2$.

[1] The "estimated" runtime means that we did not perform the full attack. Instead, we ran several chi-square tests and estimate the runtime based on the average time for running one test.

Table 1. Attacked sub-cyclotomic RLWE instances

m	generators of H	n	q	f	σ_0	no. samples	runtime (in hours)
2805	[1684, 1618]	40	67	2	1	22445	3.49
15015	[12286, 2003, 11936]	60	43	2	1	11094	1.05
15015	[12286, 2003, 11936]	60	617	2	1.25	8000	228.41 (estimated) [1]
90321	[90320, 18514, 43405]	80	67	2	1	26934	4.81
255255	[97943, 162436, 253826, 248711, 44318]	90	2003	2	1.25	15000	1114.44 (estimated)
285285	[181156, 210926, 87361]	96	521	2	1.1	5000	75.41 (estimated)
1468005Z	[312016, 978671, 956572, 400366]	100	683	2	1.1	5000	276.01 (estimated)
1468005	[198892, 978671, 431521, 1083139]	144	139	2	1	4000	5.72

5.3 A detailed example

In order to illustrate our discussion above together with the search-to-decision reduction, we study a vulnerable Galois RLWE instance in detail, where we generated RLWE samples, performed the attack, and used the search-to-decision reduction to recover the entire secret s.

Let $m = 3003$ and H be the subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$ generated by 2276, 2729 and 1123. Then $K = K_{m,H}$ is a Galois number field of degree $n = 30$. After a LLL lattice reduction on the canonical basis w, we obtained an basis $v_1, \cdots, v_n$ for the ring of integers R, ordered by increasing embedding length. We take the modulus to be $q = 131$, a prime of degree two in K. Finally, we take $\sigma_0 = 1$ and generate the secret s from the discrete Gaussian $D_{\Lambda_R,\sigma}$. It turns out that there are 15 prime ideals in K lying above q, which we denote by $\mathfrak{q}_1, \cdots, \mathfrak{q}_{15}$. We choose a prime $\mathfrak{q}$ above q and denote by $\bar{v}$ the image of v in $R/\mathfrak{q}$. We use $\mathbb{F}_q$ to denote the prime subfield of $R/\mathfrak{q} \cong \mathbb{F}_q^2$. It turns out that $\bar{v}_i \in \mathbb{F}_q$ for $1 \le i \le 15$. We generated 1000 RLWE samples and used Algorithm 1 and Theorem 3.1 to recover $s \pmod{\mathfrak{q}_i}$ for each $1 \le j \le 15$. Then we used Chinese remainder theorem to recover s. The attack succeeded in 32.8 hours.

I'm unclear on how LLL plays into things here. It is not needed for the RLWE attack, right?, so I think if we could segregate the discussion so that is clear, that would be nice.

6 Attacking prime cyclotomic fields when the modulus is the ramified prime

Let p be an odd prime and $K = \mathbb{Q}(\zeta_p)$. Then K has degree $(p-1)$ and discriminant p^{p-2}. In addition, the prime p is totally ramified in K. There is a unique prime ideal $\mathfrak{p} = (1 - \zeta_p)$ above p, and the reduction map $\pi : R/pR \to \mathbb{F}_p$ satisfies

$$\pi(\zeta_p^i) = 1, \quad \forall i \in \mathbb{Z}.$$

Writing an RLWE error as $e = \sum e_i \zeta_m^i$, we have $e \pmod{\mathfrak{p}} = \sum_i e_i$. Since the coefficients e_i tend to be small, it is conceivable that $e \pmod{\mathfrak{p}}$ takes on small values with higher probability, making the instance vulnerable to our chi-square attack. Table 2 contains data of some actual attacks we have done.

Table 2. Attacked instances of DRLWE for $K = \mathbb{Q}(\zeta_p)$ and $q = p$

p	σ_0	runtime(in seconds)
251	0.5	2.62
503	0.575	12.02
809	0.61	34.38

Add a discussion of how σ_0 is chosen here?

7 Can modulus switching be used?

I made this a separate section.

In general, I'm skeptical of the second paragraph. It seems to prove that modulus switching doesn't work for anything, ever. It doesn't depend on our attack being the purpose. I think something is fishy about the claim that a" and b" are uniform and independent.

The modulus switching procedure is a technique to reduce noise in RLWE samples, and has been discussed extensively in [1] and [7]. We recap the basic ideas of modulus switching. Let $\mathcal{R} = (K, q, \sigma, s)$ be an RLWE instance. Choose $p < q$ as the new modulus and consider the instance $\mathcal{R}' = (K, p, \sigma', s)$ for some $\sigma' > \sigma$. The main operation of modulus switching is a map

$$\pi_{q,p} : R_q \to R_p,$$

which ideally takes RLWE samples w.r.t. $\mathcal{R}$ to RLWE samples w.r.t. $\mathcal{R}'$. One example of such map being used in practice is as follows. Take a in R_q, we first scale and get $\frac{p}{q}a \in \frac{1}{q}R$. Then we sample a vector a'' from the shifted discrete Gaussian $D_{\Lambda_R,\tau,\alpha a}$ for some small $\tau > 0$, and output $a' = \alpha a - a''$. Since we expect a'' to be a short vector, the point a' can be viewed as a "rounding" of the point αa to the lattice Λ_R. One also requires that $\pi_{q,p}$ takes uniform distribution on R_q to almost uniform distribution on R_p, which can be by taking τ to be reasonably large. It is a natural question then to ask whether modulus switching can be combined with our attack, to switch from a "strong" modulus to a "weak" modulus. However, a heuristic argument shows that the naive combination of our attack with modulus switching will not work.

My understanding of the issue was that the error distribution is changed by modulus switching, and it becomes something uniform mod q basically because the error grows too much.

To explain, suppose we have a sample $(a, b) \leftarrow \mathcal{R}$ and the switched sample $(a', b') = (\pi_{q,p}(a), \pi_{q,p}(b))$. Consider the error $e' := b' - a's$ and the distribution of $e' \pmod{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ above p. Suppose $b = as + e + \lambda q$ for some $\lambda \in R$. Then

$$\begin{aligned} e' &= b' - a's \\ &= \alpha(b - as) - b'' + a''s. \\ &= \alpha e + \lambda p - b'' + a''s. \end{aligned}$$

Since p and q are coprime, the domain of the reducing modulo $\mathfrak{p}$ map can be extended from R to $\frac{1}{q}R$. Hence $e' \equiv -b'' + a''s \pmod{\mathfrak{p}}$. Also, since $a'' + a' = \alpha a \equiv 0 \pmod{\mathfrak{p}}$, we have $a'' \pmod{\mathfrak{p}} = -a' \pmod{\mathfrak{p}}$. By assumption, the map $\pi_{q,p}$ algorithm maps uniform samples in R_q to uniform samples in R_p. An immediate consequence is that $a' \pmod{\mathfrak{p}}$ is uniformly distributed in $R/\mathfrak{p}$, hence so is $a'' \pmod{\mathfrak{p}}$. The same argument applys to b''. Since the reduced rounding errors $a'' \pmod{\mathfrak{p}}$ and $b'' \pmod{\mathfrak{p}}$ are independent, the new reduced errors $e' \pmod{\mathfrak{p}}$ follows the uniform distribution. So our chi-square attack will fail on these modulus-switched samples, even though p might be a "weak" modulus.

8 Invulnerability of general cyclotomic extensions for unramified primes

In this section we provide some numerical evidence that for cyclotomic fields, the image of the RLWE error distribution modulo an unramified prime ideal $\mathfrak{q}$ is practically indistinguishable from uniform, implying that the cyclotomics are protected against the family of attacks in this paper. We will define two error distributions that approximate the RLWE error distribution (the PLWE error distribution and the modified PLWE error distribution). The advantage of these simpler distributions is the relative accessibility of a formula for a bound on the statistical distance between these distributions and the uniform distribution. This eases computation and allows for heuristic arguments.

So, I gather we have a bound on how far these distributions are from uniform, but NOT a bound on how far they are from the RLWE distribution?

Let $m \geq 1$ be an integer and let $K = \mathbb{Q}(\zeta_m)$ be the m-th cyclotomic field. Let q be a prime such that $q \equiv 1 \pmod{m}$, so q is unramified in K. Finally, let $\mathfrak{q}$ be a prime ideal above q.

First, we introduce the PLWE error distribution on cyclotomic fields, which is commonly used in practice for homomorphic encryption schemes as a substitute for the RLWE error distribution. Let $n = \varphi(m)$ be the degree of K.

Definition 8.1. *Let $\tau > 0$. A sample from the PLWE distribution $P_{m,\tau}$ is*

$$e = \sum_{i=0}^{n-1} e_i \zeta_m^i,$$

where the e_i are sampled independently from the discrete Gaussian $D_{\mathbb{Z},\tau}$.

Next, with the aim of simplifying our analysis, we introduce a class of "shifted binomial distributions" indexed by even integers $k \geq 2$, which approximating discrete Gaussians over $\mathbb{Z}$.

Definition 8.2. *For an even integer $k \geq 2$, let $\mathcal{V}_k$ denote the distribution over $\mathbb{Z}$ such that for every $t \in \mathbb{Z}$,*

$$\mathrm{Prob}(\mathcal{V}_k = t) = \begin{cases} \frac{1}{2^k}\binom{k}{t+\frac{k}{2}} & \text{if } |t| \leq \frac{k}{2} \\ 0 & \text{otherwise} \end{cases}$$

We will abuse notation and also use $\mathcal{V}_k$ to denote the reduced distribution $\mathcal{V}_k \pmod q$ over $\mathbb{F}_q$, and let ν_k denote its probability density function. Figure 2 shows a plot of the function v_8.

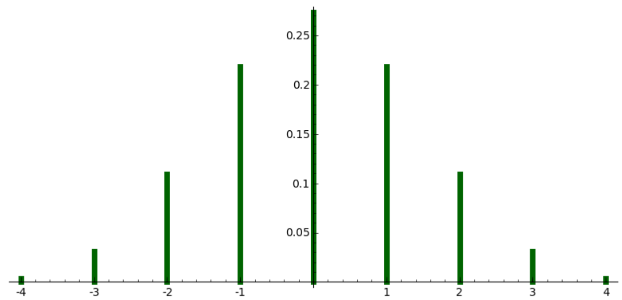

Fig. 2. Probability density function of $\mathcal{V}_8$

Definition 8.3. *Let $k \geq 2$ be an even integer. Then a sample from the modified PLWE error distribution $P'_{m,k}$ is*

$$e' = \sum_{i=0}^{n-1} e'_i \zeta_m^i,$$

where the coefficients e'_i are sampled independently from $\mathcal{V}_k$.

8.1 Bounding the distance from uniform

We recall the definition and key properties of Fourier transform over finite fields. Suppose f is a real-valued function on $\mathbb{F}_q$. The *Fourier transform* of f is defined as

$$\widehat{f}(y) = \sum_{a \in \mathbb{F}_q} f(a)\bar{\chi_y}(a),$$

where $\chi_y(a) := e^{2\pi i a y/q}$.

Let u denote the probability density function of the uniform distribution over $\mathbb{F}_q$, that is $u(a) = \frac{1}{q}$ for all $a \in \mathbb{F}_q$. Let δ denote the characteristic function of the one-point set $\{0\} \subseteq \mathbb{F}_q$. Recall that the convolution of two functions $f, g : \mathbb{F}_q \to \mathbb{R}$ is defined as $(f * g)(a) = \sum_{b \in \mathbb{F}_q} f(a-b)g(b)$. We list without proof some basic properties of the Fourier transform.

1. $\widehat{\delta} = qu$; $\widehat{u} = \delta$.
2. $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$.
3. $f(a) = \frac{1}{q}\sum_{y \in \mathbb{F}_q} \widehat{f}(y)\chi_y(a)$ (the Fourier inversion formula).

The following is a standard result.

Lemma 8.1. *Suppose the random variables F, G are independent random variables with values in $\mathbb{F}_q$, having probability density functions f and g. Then $h = f * g$. In general, suppose $F_1, \cdots, F_n$ are mutually independent random variables in $\mathbb{F}_q$, with probability density functions $f_1, \cdots, f_n$. Let f denote the density function of the sum $F = \sum F_i$, then $f = f_1 * \cdots * f_n$.*

I commented out the proof because I think we need space and this is general stuff, not our stuff.

The Fourier transform of ν_k has a nice closed-form formula, as below.

Lemma 8.2. *For all even integers $k \geq 2$, $\widehat{\nu_k}(y) = \cos\left(\frac{\pi y}{q}\right)^k$.*

Proof. We have

$$\begin{aligned}
2^k \cdot \widehat{\nu_k}(y) &= \sum_{m=-\frac{k}{2}}^{\frac{k}{2}} \binom{k}{m+\frac{k}{2}} e^{2\pi i y m/q} \\
&= e^{-\pi i y k/q} \sum_{m=-\frac{k}{2}}^{\frac{k}{2}} \binom{k}{m+\frac{k}{2}} e^{2\pi i y(m+k/2)/q} \\
&= e^{-\pi i y k/q} \sum_{m'=0}^{k} \binom{k}{m'} e^{2\pi i y m'/q} \\
&= e^{-\pi i y k/q}(1+e^{2\pi i y/q})^k \\
&= (e^{-\pi i y/q} + e^{\pi i y/q})^k \\
&= (2\cos(\pi y/q))^k.
\end{aligned}$$

Dividing both sides by 2^k gives the result. $\square$

Next, we concentrate on the reduced distributions $P_{m,\tau} \pmod{\mathfrak{q}}$ and $P'_{m,k} \pmod{\mathfrak{q}}$. Note that there is a one-to-one correspondence between primitive m-th roots of unity in $\mathbb{F}_q$ and the prime ideals above q in $\mathbb{Q}(\zeta_m)$. Let α be the root corresponding to our choice of $\mathfrak{q}$. Then a sample from $P_{m,\tau} \pmod{\mathfrak{q}}$ (resp. $P'_{m,k} \pmod{\mathfrak{q}}$) is of the form

$$\sum_{i=0}^{n-1} \alpha^i e_i \pmod{q},$$

where e_i are independent variables under the distribution $D_{\mathbb{Z},\tau}$ (resp. $\mathcal{V}_k$). We use e_α and e'_α to denote their probability density functions. Then

Lemma 8.3.

$$\widehat{e'_\alpha}(y) = \prod_{i=1}^{n} \cos\left(\frac{\alpha^i \pi y}{q}\right)^k.$$

Proof. This follows directly from Lemma 8.2 and the basic properties of Fourier transform. $\square$

Now we are able to bound the difference using the Fourier inversion formula.

Proposition 8.1. *Let $f : \mathbb{F}_q \to \mathbb{R}$ be a function such that $\sum_{a\in\mathbb{F}_q} f(a) = 1$. Then for all $a \in \mathbb{F}_q$,*

$$|f(a) - 1/q| \leq \frac{1}{q} \sum_{y\in\mathbb{F}_q, y\neq 0} |\hat{f}(y)|. \tag{2}$$

Proof. For all $a \in \mathbb{F}_q$,

$$\begin{aligned}
f(a) - 1/q &= f - u(a) \\
&= \frac{1}{q}\sum_{y\in\mathbb{F}_q} (\hat{f}(y) - \widehat{u}(y))\chi_y(a) \\
&= \frac{1}{q}\sum_{y\in\mathbb{F}_q} (\hat{f}(y) - \delta(y))\chi_y(a) \\
&= \frac{1}{q}\sum_{y\in\mathbb{F}_q, y\neq 0} \hat{f}(y)\chi_y(a). \qquad (\text{since } \hat{f}(0) = 1)
\end{aligned}$$

Now the result follows from taking absolute values on both sides, and noting that $|\chi_y(a)| \le 1$ for all a and all y. $\square$

Taking $f = e_\alpha$ or $f = e'_\alpha$ in Proposition 8.1, we immediately obtain

Theorem 8.1. *The statistical distance between e_α and u satisfies*

$$d(e_\alpha, u) \le \frac{1}{2} \sum_{y \in \mathbb{F}_q, y \neq 0} |\widehat{e_\alpha}(y)|.$$

Similarly,

$$d(e'_\alpha, u) \le \frac{1}{2} \sum_{y \in \mathbb{F}_q, y \neq 0} |\widehat{e'_\alpha}(y)|. \tag{3}$$

Now let $\epsilon'(m, q, k, \alpha)$ denote the right hand side of (3), i.e.,

$$\epsilon'(m, q, k, \alpha) = \frac{1}{2} \sum_{y \in \mathbb{F}_q, y \neq 0} \prod_{i=0}^{n-1} \cos\left(\frac{\alpha^i \pi y}{q}\right)^k.$$

To take into account all prime ideals above q, we let α run through all primitive m-th roots of unity in $\mathbb{F}_q$ and define

$$\epsilon'(m, q, k) := \max\{\epsilon'(m, q, k, \alpha) : \alpha \text{ has order } m \text{ in } \mathbb{F}_q\}.$$

If $\epsilon'(m, q, k)$ is negligibly small, the distribution $P'_{m,k} \pmod{\mathfrak{q}}$ will be computationally indistinguishable from uniform.

We can run the same analysis for the PLWE distribution, with the only difference being that there is no obvious closed-form formula for the density function d of $D_{\mathbb{Z},\tau} \pmod q$. Nonetheless, we could numerically approximate this probability density function, using the formula

$$d(a) = \frac{\displaystyle\sum_{\substack{z \in \mathbb{Z} \\ z \equiv a \bmod q}} e^{-|z|^2/2\tau}}{\displaystyle\sum_{z \in \mathbb{Z}} e^{-|z|^2/2\tau}}, \quad \forall a \in \mathbb{F}_q.$$

Since the sums in the definition of $d(a)$ converge rapidly, we could obtain good approximations of d by truncating the sums and then evaluating. Then we compute numerically the Fourier transform $\hat{d}$, and obtain

$$\widehat{e_\alpha}(y) = \prod_{i=0}^{n-1} \hat{d}(\alpha^i y)$$

Finally, we compute $\epsilon(m, q, \tau) = \frac{1}{2} \sum_{y \in \mathbb{F}_q, y \neq 0} \prod_{i=0}^{n-1} \widehat{d}(\alpha^i y)$. Then $\epsilon(m, q, \tau)$ is an upper bound of the statistical distance between the distribution e_α and the uniform distribution over $\mathbb{F}_q$. T

8.2 Numerical distance from uniform

I think it would be nice to combine both tables into one.

We have computed $\epsilon'(m, q, k)$ and $\epsilon(m, q, k)$ for various choices of parameters. Smaller values imply that the error distribution looks uniform when transfered to $R/\mathfrak{q}$, rendering the instance of RLWE invulnerable to the attacks suggested in this paper.

The following is a table of data.

Table 3. Values of $\epsilon'(m, q, 2)$

m	n	q	$-[\log_2(\epsilon'(m, q, 2))]$
96	32	4513	35
55	40	10891	44
160	64	20641	61
101	100	1213	177
145	112	19163	176
244	120	1709	230
256	128	3329	194
256	128	14081	208
197	196	3547	337
512	256	10753	431
512	256	19457	414

The data in Table 3 suggests that for $n \geq 100$ and q of polynomial size in n, the statistical distance between $P'_{m,k} \pmod{\mathfrak{q}}$ and the uniform distribution is negligibly small. Also, note that we fixed $k = 2$, and $\epsilon'(m, q, k)$ becomes even smaller when k increases.

Table 4 contains some data for values of $\epsilon(m, q, \tau)$.

Table 4. Values of $\epsilon(m, q, \tau)$

m	n	q	$-[\log_2(\epsilon(m, q, 1))]$
96	32	4513	35
55	40	10891	44
160	64	20641	61
101	100	1213	203
145	112	19163	176
244	120	1709	247
256	128	3329	252
256	128	14081	208
197	196	3547	337
512	256	10753	431
512	256	19457	414

It is possible to generalize our discussion in this section to primes of arbitrary residual degree f, in which case the Fourier analysis will be performed over the field $\mathbb{F}_{q^f}$. The only change in the definitions would be $\chi_y(a) = e^{\frac{2\pi i Tr(ay)}{q}}$. Similarly, we have

$$\widehat{e'_\alpha}(y) = \prod_{i=1}^{n} \cos\left(\frac{\pi Tr(\alpha^i y)}{q}\right)^k .$$

Table 5 contains some data for primes of degree two.

Table 5. Values of $\epsilon'(m, q, 2)$ for primes of degree two

m	q	$-[\log_2(\epsilon'(m, q, 2))]$
53	211	61
55	109	48
63	881	33
64	383	31
512	257	263

8.3 Heuristics

There is a heuristic argument as to why one expects $\epsilon'(m, q, k, \alpha)$ to be small. Each term in the summand is a product of form $\prod_{i=0}^{n-1} \cos\left(\frac{\alpha^i \pi y}{q}\right)^k$. For each $0 \neq y \in \mathbb{F}_q$, if one assumes the elements α^i are distinct and uniformly distributed in $\mathbb{F}_q$, it is very likely that $\alpha^i y$ is close $q/2$ for at least some values of i, making the product of cosines small.

I rephrased this a little, check it please.

References

1. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (leveled) fully homomorphic encryption without bootstrapping. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. pp. 309–325. ACM (2012)
2. Ducas, L., Durmus, A.: Ring-lwe in polynomial rings. In: Public Key Cryptography–PKC 2012, pp. 34–51. Springer (2012)
3. Eisenträger, K., Hallgren, S., Lauter, K.: Weak instances of plwe. In: Selected Areas in Cryptography–SAC 2014, pp. 183–194. Springer (2014)
4. Elias, Y., Lauter, K., Ozman, E., Stange, K.: Provably weak instances of ring-lwe. In: Advances in Cryptology – CRYPTO 2015, Lecture Notes in Comput. Sci., vol. 9215, pp. 63–92. Springer, Heidelberg (2015)
5. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the fortieth annual ACM symposium on Theory of computing. pp. 197–206. ACM (2008)
6. Johnston, H.: Notes on galois modules. Notes accompanying the course Galois Modules given in Cambridge in (2011)
7. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography 75(3), 565–599 (2014)
8. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. Journal of the ACM (JACM) 60(6), 43 (2013)
9. Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for ring-lwe cryptography. In: Advances in Cryptology–EUROCRYPT 2013, pp. 35–54. Springer (2013)
10. Ryabko, B.Y., Stognienko, V., Shokin, Y.I.: A new test for randomness and its application to some cryptographic problems. Journal of statistical planning and inference 123(2), 365–376 (2004)
11. Stein, W., et al.: Sage Mathematics Software (Version 6.4). The Sage Development Team (2014), http://www.sagemath.org