Cryptanalysis of PLWE Based on Zero-Trace Quadratic Roots

Efe İzbudak
ephemer41@liberior.org

January 18, 2025

Ideal lattices

Definition (Ideal lattice)

An ideal lattice is in integer lattice $\mathcal{L}(\mathcal{B}) \subset \mathbb{Z}^n$ isomorphic as a $\mathbb{Z}$-module to some ideal of $\mathcal{R} = \mathbb{Z}[x]/(f)$ where f is irreducible, monic, and of degree n.

Ideal lattices

Definition (Ideal lattice)

An ideal lattice is in integer lattice $\mathcal{L}(\mathcal{B}) \subset \mathbb{Z}^n$ isomorphic as a $\mathbb{Z}$-module to some ideal of $\mathcal{R} = \mathbb{Z}[x]/(f)$ where f is irreducible, monic, and of degree n.

Example

Consider $\mathcal{R} = \mathbb{Z}[x]/(1 + x^2)$ which can be embedded into $\mathbb{C}^2$ via the Minkowski canonical embedding.

$$\begin{aligned} \sigma \colon \mathcal{R} &\to \mathbb{C}^2 \\ 1 &\mapsto (1, 1) \\ x &\mapsto (i, -i) \end{aligned}$$

Then the vectors $(1, 0, 1, 0), (0, 1, 0, -1)$ generate an ideal lattice in $\mathbb{R}^4$.

Discrete Gaussians

Definition (Elliptic Gaussian)

We say that a random variable X has the continuous **elliptic N-dimensional Guassian distribution** of mean zero and covariance matrix Σ if it has probability density function

$$\rho_{\mathbf{r}}(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^N \det(\Sigma)}} \exp\left(-\frac{1}{2}\mathbf{x}^{\mathrm{T}}\Sigma^{-1}\mathbf{x}\right)$$

Discrete Gaussians

Definition (Elliptic Gaussian)

We say that a random variable X has the continuous **elliptic N-dimensional Guassian distribution** of mean zero and covariance matrix Σ if it has probability density function

$$\rho_{\mathbf{r}}(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^N \det(\Sigma)}} \exp\left(-\frac{1}{2}\mathbf{x}^{\mathrm{T}}\Sigma^{-1}\mathbf{x}\right)$$

Definition (Discrete Gaussian)

Let $\mathcal{L}$ be a full-rank lattice in $\mathbb{R}^N$. We say that the discrete random variable X supported on $\mathcal{L}$ is a **discrete elliptic Gaussian random variable** if it has the probability distribution

$$\Pr[X = \mathbf{x}] = \frac{\rho_{\mathbf{r}}(\mathbf{x})}{\rho_{\mathbf{r}}(\mathcal{L})} \text{ for all } \mathbf{x} \in \mathcal{L}.$$

Definition of PLWE

Definition (PLWE Distribution)

Let $f(x)$ be a monic irreducible polynomial in $\mathbb{Z}[x]$. For prime q, denote by $\mathcal{O}_f$ the quotient ring $\mathbb{Z}[x]/(f(x))$ and set $R_q = \mathcal{O}_f/q\mathcal{O}_f$. For $s \in R$ and χ an error distribution over R, the PLWE distribution $\mathcal{B}_{s,\chi}$ is given by

$$a \leftarrow U(R_q), \quad e \leftarrow \chi, \quad b = a \cdot s + e, \quad \text{return } (a, b)$$

Definition of PLWE

Definition (PLWE Distribution)

Let $f(x)$ be a monic irreducible polynomial in $\mathbb{Z}[x]$. For prime q, denote by $\mathcal{O}_f$ the quotient ring $\mathbb{Z}[x]/(f(x))$ and set $R_q = \mathcal{O}_f / q\mathcal{O}_f$. For $s \in R$ and χ an error distribution over R, the PLWE distribution $\mathcal{B}_{s,\chi}$ is given by

$$a \leftarrow U(R_q), \quad e \leftarrow \chi, \quad b = a \cdot s + e, \quad \text{return } (a, b)$$

Definition (Decision PLWE)

Given m independent samples $(a_i, b_i) \in R_q \times R_q$, $i \in \{1, \ldots, m\}$ determine whether these samples are

(i) from $\mathcal{B}_{s,\chi}$ for some fixed s

(ii) from the uniform distribution on $R_q \times R_q$

The original attack

Conditions and overview

Let $\mathcal{R}_q = \mathbb{F}_q[x]/(f(x))$ where f is a monic irreducible polynomial in $\mathbb{Z}[x]$ with a simple root α modulo q. If

1. α is small.
2. Order of α is small.

then for smallness interval Σ with $|\Sigma| < q$ and M samples, the Decision-PLWE problem can be solved in polynomial time with probability $1 - (|\Sigma|/q)^M$.

The original attack

$\alpha = 1$

- Use CRT to attain $\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(x-1) \times \mathbb{F}_q/(g(x))$ for $f(x) = (x-1)g(x)$.

The original attack

$\alpha = 1$

- Use CRT to attain $\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(x-1) \times \mathbb{F}_q/(g(x))$ for $f(x) = (x-1)g(x)$.
- $\psi_\alpha : \mathcal{R}_q \to \mathbb{F}_q[x]/(x-1)$ is the evaluation at α.

The original attack

$\alpha = 1$

- Use CRT to attain $\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(x-1) \times \mathbb{F}_q/(g(x))$ for $f(x) = (x-1)g(x)$.
- $\psi_\alpha : \mathcal{R}_q \to \mathbb{F}_q[x]/(x-1)$ is the evaluation at α.
- Given $(a, b = as + e)$, consider

$$\psi_1(e) = b(1) - a(1)s(1) = \sum_{i=0}^{N-1} e_i$$

which are sampled from a discrete gaussian with standard deviation $\sqrt{N}\sigma = \mathcal{O}(q^{1/4})$

The original attack

$\alpha = 1$

- Use CRT to attain $\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(x-1) \times \mathbb{F}_q/(g(x))$ for $f(x) = (x-1)g(x)$.
- $\psi_\alpha \colon \mathcal{R}_q \to \mathbb{F}_q[x]/(x-1)$ is the evaluation at α.
- Given $(a, b = as + e)$, consider

$$\psi_1(e) = b(1) - a(1)s(1) = \sum_{i=0}^{N-1} e_i$$

  which are sampled from a discrete gaussian with standard deviation $\sqrt{N}\sigma = \mathcal{O}(q^{1/4})$

- For correct guess $s(1)$, $e(1) \in [-\sqrt{N}\sigma, \sqrt{N}\sigma]$ with probability at least 0.65.

The original attack

$\alpha = 1$

- Use CRT to attain $\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(x-1) \times \mathbb{F}_q/(g(x))$ for $f(x) = (x-1)g(x)$.
- $\psi_\alpha : \mathcal{R}_q \to \mathbb{F}_q[x]/(x-1)$ is the evaluation at α.
- Given $(a, b = as + e)$, consider

$$\psi_1(e) = b(1) - a(1)s(1) = \sum_{i=0}^{N-1} e_i$$

  which are sampled from a discrete gaussian with standard deviation $\sqrt{N}\sigma = \mathcal{O}(q^{1/4})$

- For correct guess $s(1)$, $e(1) \in [-\sqrt{N}\sigma, \sqrt{N}\sigma]$ with probability at least 0.65.
- Method: Guess $s(1) \in \mathbb{F}_q$ and check if $e(1) \in [-\sqrt{N}\sigma, \sqrt{N}\sigma]$

The original attack

α has small order

- If $\alpha \neq 1$ is a root of order r, then again construct isomorphism $\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(x-\alpha) \times \mathbb{F}_q/(g(x))$ for $f(x) = (x-\alpha)g(x)$.

The original attack

α has small order

- If $\alpha \neq 1$ is a root of order r, then again construct isomorphism $\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(x-\alpha) \times \mathbb{F}_q/(g(x))$ for $f(x) = (x-\alpha)g(x)$.
- Given $(a, b = as + e)$, consider

$$\psi_\alpha(e) = b(\alpha) - a(\alpha)s(\alpha) = \sum_{j=0}^{r-1} \sum_{i=0}^{\lfloor \frac{N}{r} \rfloor - 1} e_{ir+j}\alpha^j$$

where $\sum_{i=0}^{\lfloor \frac{N}{r} \rfloor - 1} e_{ir+j}$ are sampled from a discrete gaussian with standard deviation $\sqrt{\frac{N}{r}}\sigma$.

The original attack

α has small order

- If $\alpha \neq 1$ is a root of order r, then again construct isomorphism $\mathbb{F}_q[x]/(f(x)) \simeq \mathbb{F}_q[x]/(x-\alpha) \times \mathbb{F}_q/(g(x))$ for $f(x) = (x-\alpha)g(x)$.
- Given $(a, b = as + e)$, consider

$$\psi_\alpha(e) = b(\alpha) - a(\alpha)s(\alpha) = \sum_{j=0}^{r-1} \sum_{i=0}^{\lfloor \frac{N}{r} \rfloor - 1} e_{ir+j}\alpha^j$$

where $\sum_{i=0}^{\lfloor \frac{N}{r} \rfloor - 1} e_{ir+j}$ are sampled from a discrete gaussian with standard deviation $\sqrt{\frac{N}{r}}\sigma$.

- Method: Guess $s(\alpha) \in \mathbb{F}_q$ and check if $e(\alpha) \in \Sigma = \left[-\sqrt{\frac{N}{r}}\sigma, \sqrt{\frac{N}{r}}\sigma\right]$

New attack

Setup: Simplified version

- Assume x^2+1 is irreducible over $\mathbb{F}_q$ and $x^2+1 \mid f(x)$ in $\mathbb{F}_q[x]$. Note that it is reducible over $\mathbb{F}_{q^2}$.

New attack

Setup: Simplified version

- Assume x^2+1 is irreducible over $\mathbb{F}_q$ and $x^2+1 \mid f(x)$ in $\mathbb{F}_q[x]$. Note that it is reducible over $\mathbb{F}_{q^2}$.
- Let $\alpha \in \mathbb{F}_{q^2}$ be a root of x^2+1.

New attack

Setup: Simplified version

- Assume $x^2 + 1$ is irreducible over $\mathbb{F}_q$ and $x^2 + 1 \mid f(x)$ in $\mathbb{F}_q[x]$. Note that it is reducible over $\mathbb{F}_{q^2}$.
- Let $\alpha \in \mathbb{F}_{q^2}$ be a root of $x^2 + 1$.
- Note that $\mathrm{Tr}_{q^2/q}(\alpha) = \alpha + \alpha^q = \alpha + (-\alpha) = 0$.

New attack

Setup: Simplified version

- Assume x^2+1 is irreducible over $\mathbb{F}_q$ and $x^2+1 \mid f(x)$ in $\mathbb{F}_q[x]$. Note that it is reducible over $\mathbb{F}_{q^2}$.
- Let $\alpha \in \mathbb{F}_{q^2}$ be a root of x^2+1.
- Note that $\mathrm{Tr}_{q^2/q}(\alpha) = \alpha + \alpha^q = \alpha + (-\alpha) = 0$.
- For PLWE sample $(a, b = as + e)$ we have

$$\mathrm{Tr}(b(\alpha) - a(\alpha)s(\alpha)) = \mathrm{Tr}(e(\alpha))$$

$$= \sum_{j=0}^{N-1} e_j \mathrm{Tr}(\alpha^i) = 2 \sum_{j=0}^{\lfloor \frac{N-1}{2} \rfloor} e_{2j}(-1)^j$$

New attack

Setup: Simplified version

- Assume x^2+1 is irreducible over $\mathbb{F}_q$ and $x^2+1 \mid f(x)$ in $\mathbb{F}_q[x]$. Note that it is reducible over $\mathbb{F}_{q^2}$.
- Let $\alpha \in \mathbb{F}_{q^2}$ be a root of x^2+1.
- Note that $\mathrm{Tr}_{q^2/q}(\alpha) = \alpha + \alpha^q = \alpha + (-\alpha) = 0$.
- For PLWE sample $(a, b = as + e)$ we have

$$\mathrm{Tr}(b(\alpha) - a(\alpha)s(\alpha)) = \mathrm{Tr}(e(\alpha))$$
$$= \sum_{j=0}^{N-1} e_j \mathrm{Tr}(\alpha^i) = 2\sum_{j=0}^{\lfloor \frac{N-1}{2} \rfloor} e_{2j}(-1)^j$$

- $\Sigma = \left[-2\sqrt{\lfloor \frac{N-1}{2} \rfloor}\sigma, 2\sqrt{\lfloor \frac{N-1}{2} \rfloor}\sigma\right]$ is the smallness region containing at most $4\sqrt{\lfloor \frac{N-1}{2} \rfloor}\sigma + 1$ elements

New attack

Setup: General quadratics

- Assume $x^2 + \rho$ is irreducible, $x^2 + \rho \mid f(x)$ in $\mathbb{F}_q[x]$, and r is the multiplicative order of $\rho \mod n$. Let $\alpha \in \mathbb{F}_{q^2}$ be a root of $x^2 + \rho$.

New attack

Setup: General quadratics

- Assume $x^2 + \rho$ is irreducible, $x^2 + \rho \mid f(x)$ in $\mathbb{F}_q[x]$, and r is the multiplicative order of $\rho \mod n$. Let $\alpha \in \mathbb{F}_{q^2}$ be a root of $x^2 + \rho$.
- For PLWE sample $(a, b = as + e)$ we have for $N^* := \lfloor \frac{N-1}{2} \rfloor$

$$\mathrm{Tr}(b(\alpha) - a(\alpha)s(\alpha)) = \mathrm{Tr}(e(\alpha))$$

$$= 2 \sum_{k=0}^{r-1} (-\rho)^k \sum_{i=0}^{\lfloor \frac{N^*}{r} \rfloor - 1} e_{2(ir+k)}$$

New attack

Setup: General quadratics

- Assume $x^2+\rho$ is irreducible, $x^2+\rho \mid f(x)$ in $\mathbb{F}_q[x]$, and r is the multiplicative order of $\rho \mod n$. Let $\alpha \in \mathbb{F}_{q^2}$ be a root of $x^2+\rho$.
- For PLWE sample $(a, b = as + e)$ we have for $N^* := \lfloor \frac{N-1}{2} \rfloor$

$$\mathrm{Tr}(b(\alpha) - a(\alpha)s(\alpha)) = \mathrm{Tr}(e(\alpha))$$
$$= 2\sum_{k=0}^{r-1}(-\rho)^k \sum_{i=0}^{\lfloor \frac{N^*}{r} \rfloor - 1} e_{2(ir+k)}$$

- For this case, $|\Sigma| \leqslant \left(4\sqrt{\frac{N^*}{r}}\sigma + 1\right)^r$

New attack

$\mathcal{R}_{q,0}$ case

- Define $\mathcal{R}_{q,0} = \{p(x) \in \mathcal{R}_q \mid p(\alpha) \in \mathbb{F}_q\}$ which has $\mathbb{F}_q$-dimension $N - 1$.

New attack

$\mathcal{R}_{q,0}$ case

- Define $\mathcal{R}_{q,0} = \{p(x) \in \mathcal{R}_q \mid p(\alpha) \in \mathbb{F}_q\}$ which has $\mathbb{F}_q$-dimension $N-1$.
- Instead of guessing $s(\alpha) \in \mathbb{F}_{q^2}$ and checking if

$$\frac{1}{2}\mathrm{Tr}(b(\alpha) - a(\alpha)s(\alpha)) = \frac{1}{2}\mathrm{Tr}(b(\alpha)) - \frac{1}{2}a(\alpha)\mathrm{Tr}(s(\alpha)) \in \Sigma$$

it is enough to guess $\mathrm{Tr}(s(\alpha)) \in \mathbb{F}_q$.

New attack

$\mathcal{R}_{q,0}$ case

- Define $\mathcal{R}_{q,0} = \{p(x) \in \mathcal{R}_q \mid p(\alpha) \in \mathbb{F}_q\}$ which has $\mathbb{F}_q$-dimension $N-1$.
- Instead of guessing $s(\alpha) \in \mathbb{F}_{q^2}$ and checking if

$$\frac{1}{2}\mathrm{Tr}(b(\alpha) - a(\alpha)s(\alpha)) = \frac{1}{2}\mathrm{Tr}(b(\alpha)) - \frac{1}{2}a(\alpha)\mathrm{Tr}(s(\alpha)) \in \Sigma$$

  it is enough to guess $\mathrm{Tr}(s(\alpha)) \in \mathbb{F}_q$.
- This attack requires $\mathcal{O}(Mq)$ $\mathbb{F}_q$-multiplications for M samples.

New attack

Setup for probability analysis

Denote $p^*(x) := \sum_{j=0}^{N^*} p_{2j}x^j$ and $\mathcal{R}_q^* := \mathbb{F}_q/(f^*(x))$.

Lemma

Given $(a, b) \in \mathcal{R}_{q,0} \times \mathcal{R}_q$ *and* $g \in \mathbb{F}_q$,

$$(\mathrm{Tr}(b(\alpha) - a(\alpha)g))/2 \in \Sigma \iff b^*(-\rho) - ga^*(-\rho) \in \Sigma$$

and as such the new attack on samples $(a_i, b_i) \in \mathcal{R}_{q,0} \times \mathcal{R}_q$ *gives the same result as the old attack on samples* $(a_i^*, b_i^*) \in \mathcal{R}_q^* \times \mathcal{R}_q^*$.

New attack

Setup for probability analysis

Denote $p^*(x) := \sum_{j=0}^{N^*} p_{2j} x^j$ and $\mathcal{R}_q^* := \mathbb{F}_q/(f^*(x))$.

Lemma

Given $(a, b) \in \mathcal{R}_{q,0} \times \mathcal{R}_q$ *and* $g \in \mathbb{F}_q$,

$$(\mathrm{Tr}(b(\alpha) - a(\alpha)g))/2 \in \Sigma \iff b^*(-\rho) - ga^*(-\rho) \in \Sigma$$

and as such the new attack on samples $(a_i, b_i) \in \mathcal{R}_{q,0} \times \mathcal{R}_q$ *gives the same result as the old attack on samples* $(a_i^*, b_i^*) \in \mathcal{R}_q^* \times \mathcal{R}_q^*$.

Proof.

Follows from $f(\alpha) = f^*(-\rho) = 0$. □

New attack

Setup for probability analysis

Lemma

If $a \xleftarrow{\$} \mathcal{R}_{q,0}$, *then* $a^* \xleftarrow{\$} \mathcal{R}_q^*$ *with probability* $\mathcal{O}(q^{-N^*})$.

New attack

Setup for probability analysis

Lemma

If $a \xleftarrow{\$} \mathcal{R}_{q,0}$, *then* $a^* \xleftarrow{\$} \mathcal{R}_q^*$ *with probability* $\mathcal{O}(q^{-N^*})$.

Sketch of proof.

Write $a = a_0 + a_1$ where

$$a_0(x) = \sum_{j=0}^{N^*} a_{2j}x^{2j}, \quad a_1(x) = \sum_{j=0}^{N^*} (a_{2j+1}x^{2j})x.$$

Fix a_0. Note that any N^*-tuple $(a_1, a_3, \ldots, a_{2N^*+1})$ for $a_1(x)$ with $\sum_{j=0}^{N^*} a_{2j+1}(-\rho)^{2j} = 0$ gives rise to the same polynomial $a^*(x)$. □

New attack

Probability analysis

Proposition

For $|\Sigma| < q$ *and* M *the number of input samples from* $\mathcal{R}_{q,0} \times \mathcal{R}_q$*, the attack we have described succeeds with probability* $1 - \left(\frac{|\Sigma|}{q}\right)^M$.

New attack

Probability analysis

Proposition

For $|\Sigma| < q$ and M the number of input samples from $\mathcal{R}_{q,0} \times \mathcal{R}_q$, the attack we have described succeeds with probability $1 - \left(\frac{|\Sigma|}{q}\right)^M$.

Sketch of proof.

Write

$$(a(x), b(x)) = (a_0(x), b_0(x)) + (a_1(x), b_1(x))$$

for $a_0(x) = a^*(x^2)$, $b_0(x) = b^*(x^2)$ and $a_1(\alpha) = 0$. Show that the attack output for starred and non-starred samples are the same. □

New attack

Setup for general attack

Definition (X_0)

Given a distribution X over $\mathcal{R}_q \times \mathcal{R}_q$, let X_0 denote the random variable which samples X until it obtains (a, b) with $a \in \mathcal{R}_{q,0}$ and returns (a, b) with the number of queries (count) of X.

New attack

Setup for general attack

Definition (X_0)

Given a distribution X over $\mathcal{R}_q \times \mathcal{R}_q$, let X_0 denote the random variable which samples X until it obtains (a, b) with $a \in \mathcal{R}_{q,0}$ and returns (a, b) with the number of queries (count) of X.

Proposition

With the notations above,

1. *If X is uniform over $\mathcal{R}_q \times \mathcal{R}_q$, then X_0 is uniform over $\mathcal{R}_{q,0} \times \mathcal{R}_q$.*
2. *If X is a PLWE distribution then X_0 is a $\mathcal{R}_{q,0} \times \mathcal{R}_q$-valued PLWE distribution.*

New attack

Setup for general attack

Definition (X_0)

Given a distribution X over $\mathcal{R}_q \times \mathcal{R}_q$, let X_0 denote the random variable which samples X until it obtains (a, b) with $a \in \mathcal{R}_{q,0}$ and returns (a, b) with the number of queries (count) of X.

Proposition

With the notations above,

1. *If X is uniform over $\mathcal{R}_q \times \mathcal{R}_q$, then X_0 is uniform over $\mathcal{R}_{q,0} \times \mathcal{R}_q$.*
2. *If X is a PLWE distribution then X_0 is a $\mathcal{R}_{q,0} \times \mathcal{R}_q$-valued PLWE distribution.*

Remark

$\mathrm{count} \sim \mathrm{Geom}(q^{-1})$ *so* $\mathbb{E}[\mathrm{count}] = q = \mathcal{O}(N^2)$.

New attack

Setup for general attack

- Let $\ell = \mathcal{O}(p(N))$ be the maximum number of samples to generate. The probability that for ℓ samples in $\mathcal{R}_q^2$, at least $k \leqslant \ell$ of them belong to $\mathcal{R}_{q,0} \times \mathcal{R}_q$ is (by normal approximation)

$$P[\mathcal{B}(\ell, q^{-1}) \geqslant k] \approx P\left[Z \geqslant \frac{k - \ell q^{-1}}{\sqrt{\ell q^{-1}(1 - q^{-1})}}\right]$$

where $\mathcal{B}$ denotes a random variable with the binomial distribution of parameters ℓ and q^{-1}.

New attack

Setup for general attack

- Let $\ell = \mathcal{O}(p(N))$ be the maximum number of samples to generate. The probability that for ℓ samples in $\mathcal{R}_q^2$, at least $k \leqslant \ell$ of them belong to $\mathcal{R}_{q,0} \times \mathcal{R}_q$ is (by normal approximation)

$$P[\mathcal{B}(\ell, q^{-1}) \geqslant k] \approx P\left[Z \geqslant \frac{k - \ell q^{-1}}{\sqrt{\ell q^{-1}(1 - q^{-1})}}\right]$$

  where $\mathcal{B}$ denotes a random variable with the binomial distribution of parameters ℓ and q^{-1}.

- This probability is $\approx 1/2$ for $k \approx \ell q^{-1} > 5$.

New attack

Setup for general attack

- Let $\ell = \mathcal{O}(p(N))$ be the maximum number of samples to generate. The probability that for ℓ samples in $\mathcal{R}_q^2$, at least $k \leqslant \ell$ of them belong to $\mathcal{R}_{q,0} \times \mathcal{R}_q$ is (by normal approximation)

$$P[\mathcal{B}(\ell, q^{-1}) \geqslant k] \approx P\left[Z \geqslant \frac{k - \ell q^{-1}}{\sqrt{\ell q^{-1}(1 - q^{-1})}}\right]$$

  where $\mathcal{B}$ denotes a random variable with the binomial distribution of parameters ℓ and q^{-1}.
- This probability is $\approx 1/2$ for $k \approx \ell q^{-1} > 5$.
- We choose k so that $1 - \left(\frac{|\Sigma|}{q}\right)^k \geqslant \theta$ where θ is the desired success probability.

New attack

General attack

1. Sample from $\mathcal{R}_q \times \mathcal{R}_q$ until k samples fall in $\mathcal{R}_{q,0} \times \mathcal{R}_q$.
2. Apply the trace attack on the k samples.

Attacks on cyclotomics

1. $\alpha = 1$ is never a root of $\Phi_n(x)$ modulo $q \nmid n$.

Attacks on cyclotomics

1. $\alpha = 1$ is never a root of $\Phi_n(x)$ modulo $q \nmid n$.
2. For $q = 1 \mod n$ (so $\mathbb{F}_q^\times$ contains a cyclic subgroup of order n), the roots of $\Phi_n(x)$ have order n (since they are the primitive nth roots).

Attacks on cyclotomics

1. $\alpha = 1$ is never a root of $\Phi_n(x)$ modulo $q \nmid n$.
2. For $q = 1 \mod n$ (so $\mathbb{F}_q^\times$ contains a cyclic subgroup of order n), the roots of $\Phi_n(x)$ have order n (since they are the primitive nth roots).
3. It is unlikely (heuristic) for $\Phi_n(x)$ to have an irreducible quadratic factor with 0 linear term.

Attacks on cyclotomics

1. $\alpha = 1$ is never a root of $\Phi_n(x)$ modulo $q \nmid n$.
2. For $q = 1 \mod n$ (so $\mathbb{F}_q^\times$ contains a cyclic subgroup of order n), the roots of $\Phi_n(x)$ have order n (since they are the primitive nth roots).
3. It is unlikely (heuristic) for $\Phi_n(x)$ to have an irreducible quadratic factor with 0 linear term.
4. For conductor $n = p^k$ and $q = 1 + p^A u$ for $(u, p) = 1$ and $2 \leqslant A < k$

$$\Phi_{p^k}(x) = \prod_{\rho \in \Omega(p^A)} (x^{p^{k-A}} - \rho)$$

where $\Omega(p^A)$ is the set of primitive p^Ath roots of unity. Attack is efficient for $A = 2$ but the subspace $\mathcal{R}_{q,0}$ has dimension $\approx N/2$ and weak samples are rare.

References

B. Barbero-Lucas, I. Blanco-Chacón, R. Durán-Díaz, and R. Y. N. Nchiwo, "Cryptanalysis of PLWE based on zero-trace quadratic roots," In: *arXiv preprint arXiv:2312.11533*, 2023. [Online]. Available: https://arxiv.org/abs/2312.11533

Y. Elias, K. E. Lauter, E. Ozman, and K. E. Stange, "Provably Weak Instances of Ring-LWE," In: *Advances in Cryptology – CRYPTO 2015*, R. Gennaro and M. Robshaw, Eds., no. 9215 in Lecture Notes in Computer Science, Berlin, Heidelberg, 2015, Springer Berlin Heidelberg, pp. 63–92.