# On the Integer Polynomial Learning with Errors Problem

Julien Devevey[1] Amin Sakzad[2] Damien Stehlé[1,3] Ron Steinfeld[2]

ENS de Lyon, France

Faculty of Information Technology, Monash University, Australia

Institut Universitaire de France

# Main Results

Informal definitions of search PLWE and search I-PLWE:

*Input*: $\{(a_i, a_i s + e_i)\}_{i=1}^{t} \in \mathcal{S}^{2t}$
*Output*: $s \in \mathcal{S}$,

where:

| | $\mathcal{S}$ | $s$ | $a_i$ | $e_i$ |
|---|---|---|---|---|
| sPLWE | $\mathbb{Z}_q[x]/f$ | $\sum_{j=0}^{m-1} s_j x^j$ | $\sum_{j=0}^{m-1} a_{i,j} x^j$ | $\sum_{j=0}^{m-1} e_{i,j} x^j$ |
| sI-PLWE | $\mathbb{Z}_{f(q)}$ | $\sum_{j=0}^{m-1} s_j q^j$ | $\sum_{j=0}^{m-1} a_{i,j} q^j$ | $\sum_{j=0}^{m-1} e_{i,j} q^j$ |

And $|s_j|, |e_{i,j}|$ are small.

# Main Results

**Problem Reduction**

Search PLWE and search I-PLWE are computationally equivalent for a large class of $f$.

**Construction**

There exists an OW-CPA secure PKE, under the search I-PLWE assumption.

# State of the art

- Security of PLWE is well studied (e.g. [SSTX09][1], [LPR10]).
- I-PLWE introduced and studied in the worst-case for $f = x^m + 1$ in [Gu17]
  and a concrete security analysis is given in [BCF20].
- Module extension of I-PLWE used in *ThreeBears* [Ham17], a NIST candidate to the PQC project, with $f = x^m - x^{m/2} - 1$.

[1] Bibliography can be found in the paper

# Motivation

- I-PLWE introduced to take advantage of the security of PLWE and fast large integers arithmetic.
- No average-case reductions between PLWE and I-PLWE was proved, as [Gu17] only gave a worst-case reduction.
- Our work readily extends from Polynomial-LWE to Module-LWE, and as $x^m - x^{m/2} - 1$ belongs to the class of admissible polynomials, it is very close to proving security of *ThreeBears*.

# Table of contents

# PLWE and I-PLWE

# Gaussian distribution

Gaussian distribution extended to polynomials by identification with their coefficient vector:

$$\psi : \begin{pmatrix} P_0 \\ \vdots \\ P_{m-1} \end{pmatrix} \in \mathbb{Z}^m \longmapsto \sum_{i=0}^{m-1} P_i x^i \in \mathbb{Z}^{<m}[x].$$

$D_{\mathbb{Z}^{<m}[x],\sigma,Q}$ denotes the sampling of $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^m,\sigma,\psi^{-1}(Q)}$ and returning $\psi(\mathbf{e})$.

# Polynomial evaluation

$$\begin{aligned} \cdot(q) : (-q/2, q/2][x] &\longrightarrow \mathbb{Z} \\ P = \sum_{i=0}^{n-1} P_i x^i &\longmapsto P(q) = \sum_{i=0}^{n-1} P_i q^i, \end{aligned}$$

naturally extended to $\mathbb{Z}_q[x]$ and $\mathbb{Z}_q[x]/f$.

# PLWE

- $q > 2$ odd,
- $f = x^m + 1$,
- $\sigma > \sigma' > 0$ two Gaussian parameters.

**The** $\mathrm{sPLWE}_{q,\sigma,\sigma',t}$ **problem**

*Input*: $\{(a_i, a_i \cdot s + e_i) \in \mathbb{Z}_q[x]/f \times \mathbb{Z}_q[x]/f\}_{i=1}^{t}$,
*Output*: $s$, where:

- $s \hookleftarrow D_{\mathbb{Z}^{<m}[x],\sigma'} \bmod q$,
- $a_i \hookleftarrow \mathbb{Z}_q[x]/f$,
- $e_i \hookleftarrow D_{\mathbb{Z}^{<m}[x],\sigma} \bmod q$.

⚠ $\sigma \neq \sigma'$ necessary for reduction

- Standard case $\sigma = \sigma'$ reduced to ours by oblivious noise addition

# PLWE

- $q > 2$ odd,
- $f = x^m + 1$,
- $\sigma > \sigma' > 0$ two Gaussian parameters.

**The** $\mathrm{sPLWE}_{q,\sigma,\sigma',t}$ **problem**

*Input*: $\{(a_i, a_i \cdot s + e_i) \in \mathbb{Z}_q[x]/f \times \mathbb{Z}_q[x]/f\}_{i=1}^{t}$,
*Output*: $s$, where:

- $s \hookleftarrow D_{\mathbb{Z}^{<m}[x],\sigma'} \bmod q$,
- $a_i \hookleftarrow \mathbb{Z}_q[x]/f$,
- $e_i \hookleftarrow D_{\mathbb{Z}^{<m}[x],\sigma} \bmod q$.

⚠ $\sigma \neq \sigma'$ necessary for reduction

- Standard case $\sigma = \sigma'$ reduced to ours by oblivious noise addition

# I-PLWE - First attempt

**The** $\mathsf{sI-PLWE}_{q,\sigma,\sigma',t}$ **problem?**

*Input*: $\{(a_i(q), a_i(q) \cdot s(q) + e_i(q)) \in \mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}\}_{i=1}^{t}$,
*Output*: $s(q)$, where:

- $s \hookleftarrow D_{\mathbb{Z}^{<m}[x],\sigma'} \bmod q$,
- $a_i \hookleftarrow \mathbb{Z}_q^{<m}[x]$,
- $e_i \hookleftarrow D_{\mathbb{Z}^{<m}[x],\sigma} \bmod q$.

⚠ $|\mathbb{Z}_{f(q)}| = q^m + 1 > q^m = |\mathbb{Z}_q[x]/f|$.

- $\mathrm{Supp}(a_i(q)) \neq \mathbb{Z}_{q^m+1}$

# I-PLWE - First attempt

**The** $\mathsf{sI-PLWE}_{q,\sigma,\sigma',t}$ **problem?**

*Input*: $\{(a_i(q), a_i(q) \cdot s(q) + e_i(q)) \in \mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}\}_{i=1}^{t}$,
*Output*: $s(q)$, where:

- $s \hookleftarrow D_{\mathbb{Z}^{<m}[x],\sigma'} \bmod q$,
- $a_i \hookleftarrow \mathbb{Z}_q^{<m}[x]$,
- $e_i \hookleftarrow D_{\mathbb{Z}^{<m}[x],\sigma} \bmod q$.

⚠ $|\mathbb{Z}_{f(q)}| = q^m + 1 > q^m = |\mathbb{Z}_q[x]/f|$.

- $\mathrm{Supp}(a_i(q)) \neq \mathbb{Z}_{q^m+1}$

# I-PLWE - Our Definition

**The $\mathsf{sI-PLWE}_{q,\sigma,\sigma',t}$ problem**

*Input*: $\{(a_i, a_i \cdot s(q) + e_i(q)) \in \mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}\}_{i=1}^{t}$,
*Output*: $s(q)$, where:

- $s \hookleftarrow D_{\mathbb{Z}^{<m+1}[x],\sigma'}$ mod $q$ until $s(q) \in \left(-\frac{q^m+1}{2}, \frac{q^m+1}{2}\right]$,
- $a_i \hookleftarrow \mathbb{Z}_{f(q)}$,
- $e_i \hookleftarrow D_{\mathbb{Z}^{<m+1}[x],\sigma}$ mod $q$ until $e_i(q) \in \left(-\frac{q^m+1}{2}, \frac{q^m+1}{2}\right]$.

- To reduce the rejection probability, sample from $D_{\mathbb{Z}^{<m}[x],\sigma('),q}$ and add or subtract $q^m$ with a certain probability.
- Different noise/secret distribution than [Gu17], to get noise over the whole space.

# I-PLWE - Our Definition

**The** $\mathsf{sI-PLWE}_{q,\sigma,\sigma',t}$ **problem**

*Input*: $\{(a_i, a_i \cdot s(q) + e_i(q)) \in \mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}\}_{i=1}^{t}$,
*Output*: $s(q)$, where:

- $s \hookleftarrow D_{\mathbb{Z}^{<m+1}[x],\sigma'}$ mod $q$ until $s(q) \in \left(-\frac{q^m+1}{2}, \frac{q^m+1}{2}\right]$,
- $a_i \hookleftarrow \mathbb{Z}_{f(q)}$,
- $e_i \hookleftarrow D_{\mathbb{Z}^{<m+1}[x],\sigma}$ mod $q$ until $e_i(q) \in \left(-\frac{q^m+1}{2}, \frac{q^m+1}{2}\right]$.

- To reduce the rejection probability, sample from $D_{\mathbb{Z}^{<m}[x],\sigma(')q}$ and add or subtract $q^m$ with a certain probability.
- Different noise/secret distribution than [Gu17], to get noise over the whole space.

# From integers to polynomials

## Centered $q$-ary decomposition of an integer

$$a_i := \frac{a - \sum_{j<i} a_j q^j}{q^i} \bmod q \in (-q/2, q/2], \quad \forall a \in \mathbb{Z}, \forall 0 \leq i \leq \lceil \log_q a \rceil.$$

## Conversion from $\mathbb{Z}$ to $\mathbb{Z}_q[x]$

$$\begin{aligned} \Phi_q : \mathbb{Z} &\longrightarrow \mathbb{Z}_q[x] \\ a &\longmapsto \sum_{i=0}^{\lceil \log_q a \rceil} a_i x^i. \end{aligned}$$

This is a bijection and its inverse is $\cdot(q)$.

# From integers to polynomials

## Centered $q$-ary decomposition of an integer

$$a_i := \frac{a - \sum_{j<i} a_j q^j}{q^i} \bmod q \in (-q/2, q/2], \quad \forall a \in \mathbb{Z}, \forall 0 \leq i \leq \lceil \log_q a \rceil.$$

## Conversion from $\mathbb{Z}$ to $\mathbb{Z}_q[X]$

$$\begin{aligned} \Phi_q : \mathbb{Z} &\longrightarrow \mathbb{Z}_q[X] \\ a &\longmapsto \sum_{i=0}^{\lceil \log_q a \rceil} a_i X^i. \end{aligned}$$

This is a bijection and its inverse is $\cdot(q)$.

# From one quotient ring to another

Let $I_q := (-(q^m+1)/2, (q^m+1)/2]$.

**Conversion from $\mathbb{Z}_{f(q)}$ to $\mathbb{Z}_q[x]/f$**

$$\Phi_q^{(f)} : I_q \longrightarrow \mathbb{Z}_q[x]/f$$

$$\Phi_q^{(f)} : a \longmapsto \sum_{i=0}^{\lceil \log_q a \rceil} a_i x^i \bmod f.$$

In particular, for any $P \in \mathbb{Z}_q[x]/f$,

$$\Phi_q^{(f)}\left(P(q) \bmod f(q)\right) = P,$$

but $\Phi_q^{(f)}$ has collisions...

# From one quotient ring to another

Let $I_q := (-(q^m+1)/2, (q^m+1)/2]$.

**Conversion from $\mathbb{Z}_{f(q)}$ to $\mathbb{Z}_q[x]/f$**

$$\Phi_q^{(f)} : I_q \longrightarrow \mathbb{Z}_q[x]/f$$

$$\Phi_q^{(f)} : a \longmapsto \sum_{i=0}^{\lceil \log_q a \rceil} a_i x^i \bmod f.$$

In particular, for any $P \in \mathbb{Z}_q[x]/f$,

$$\Phi_q^{(f)}\left(P(q) \bmod f(q)\right) = P,$$

but $\Phi_q^{(f)}$ has collisions...

# Carries

# A base remark

**Warning!**

$\Phi_q$ is not a morphism.

**Example**

- $\Phi_3(2) = x - 1$,
- $\Phi_3(3) = x$,

But!

- $\Phi_3(5) = x^2 - x - 1$.

# A base remark

**Warning!**

$\Phi_q$ is not a morphism.

**Example**

- $\Phi_3(2) = x - 1$,
- $\Phi_3(3) = x$,

But!

- $\Phi_3(5) = x^2 - x - 1$.

# A base remark

**Warning!**

$\Phi_q$ is not a morphism.

**Example**

- $\Phi_3(2) = x - 1$,
- $\Phi_3(3) = x$,

But!

- $\Phi_3(5) = x^2 - x - 1$.

There are no carries in polynomial operations!

# Carries

## Computing the carries

- Addition: $c^{(a)}(a,b) = \Phi_q(a+b) - \Phi_q(a) - \Phi_q(b)$,
- Multiplication: $c^{(m)}(a,b) = \Phi_q(ab) - \Phi_q(a)\Phi_q(b)$,

## Size of the carries

$$\|c^{(a)}(a,b)\|_\infty \leq 1$$

and

$$\|c^{(m)}(a,b)\|_\infty \leq \frac{2q + \|a\|_\infty \|b\|_1}{q-1}.$$

# Carries in the quotient rings

**Carries** $\bmod q^m + 1$ **and** $\bmod x^m + 1$

- Addition: $c_f^{(a)}(a, b) = \Phi_q^{(f)}(a + b \bmod f(q)) - \Phi_q^{(f)}(a) - \Phi_q^{(f)}(b)$,
- Multiplication: $c_f^{(m)}(a, b) = \Phi_q^{(f)}(ab \bmod f(q)) - \Phi_q^{(f)}(a)\Phi_q^{(f)}(b)$,

- Computing a $\bmod x^m + 1$ (resp. $\bmod q^m + 1$) corresponds to adding/subtracting $x^m + 1$ (resp. $q^m + 1$) multiple times.
- E.g. computing $\Phi_q(a + b \bmod q^m + 1) \bmod x^m + 1$ yields two addition carries and a few additions/subtractions of $x^m + 1$.

# Size of the carries in the quotient rings

## Size of the carries

$$\|c_f^{(a)}(a,b)\|_\infty \leq 2 + 4\|f\|_\infty = 6$$

and

$$\|c_f^{(m)}(a,b)\|_\infty \leq 2\left(1 + 2\frac{2q + \|a\|_\infty \|b\|_1}{q-1}\right).$$

If $a \hookleftarrow U(\mathbb{Z}_{q^m+1})$, the second bound becomes

$$\|c_f^{(m)}(a,b)\|_\infty \leq 14 + 1.5\|b\|_1,$$

hence the need for a small PLWE secret.

# Reduction

# The right tool for the job

- $P, Q$: discrete probability distributions with finite support.
- $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$.

**Rényi divergence of order 2 and $\infty$**

$$R(P||Q) := \sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^2}{Q(x)} \text{ and } R_\infty(P||Q) := \max_{x \in \mathrm{Supp}(P)} \frac{P(x)}{Q(x)}.$$

**Divergence between off-centered Gaussians [LSS14]**

$$R(D_{\mathbb{Z}^{<m}[x],\sigma,P}||D_{\mathbb{Z}^{<m}[x],\sigma,Q}) = \exp\left(\frac{2\pi\|P-Q\|^2}{\sigma^2}\right).$$

# The right tool for the job

- $P, Q$: discrete probability distributions with finite support.
- $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$.

**Rényi divergence of order 2 and $\infty$**

$$R(P||Q) := \sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^2}{Q(x)} \text{ and } R_\infty(P||Q) := \max_{x \in \mathrm{Supp}(P)} \frac{P(x)}{Q(x)}.$$

**Divergence between off-centered Gaussians [LSS14]**

$$R(D_{\mathbb{Z}^{<m}[x],\sigma,P}||D_{\mathbb{Z}^{<m}[x],\sigma,Q}) = \exp\left(\frac{2\pi\|P-Q\|^2}{\sigma^2}\right).$$

# Rényi divergence: properties [BLRL+18]

## Properties

- **Data Processing Inequality:** $R(f(P)||f(Q)) \leq R(P||Q)$ for any function $f$.
- **Multiplicativity:** $R((P_1, P_2)||(Q_1, Q_2)) \leq R_\infty(P_1||Q_1) \cdot \max_{x_1 \in \mathrm{Supp}(P_1)} R((P_2|x_1)||(Q_2|x_1))$.
- **Probability Preservation:** $\forall E \subseteq \mathrm{Supp}(Q), Q(E) \geq P(E)^2/R(P||Q)$.

# Reductions (Intuition)

- **sPLWE to sI-PLWE:** evaluate in $q$
  Given $\{(a_i, a_i s + e_i)\}_{i=1}^{t} \in (\mathbb{Z}_q[x]/\langle x^m + 1\rangle)^{2t}$,
  give $\{(a_i(q) \bmod f(q), (a_i s + e_i)(q) \bmod f(q))\}_{i=1}^{t}$ to an sI-PLWE solver. Return the same answer.

- **sI-PLWE to sPLWE:** write as a polynomial
  Given $\{(a_i, a_i \cdot s(q) + e_i(q))\}_{i=1}^{t} \in (\mathbb{Z}_{q^m+1})^{2t}$,
  give $\{(\Phi_q^{(f)}(a_i), \Phi_q^{(f)}(a_i \cdot s(q) + e_i(q)))\}_{i=1}^{t}$ to an sPLWE solver. Return the same answer.

# sPLWE to sI-PLWE Reduction Analysis

- $(a_i s + e_i)(q) = a_i(q)s(q) + e'_i \bmod q^m + 1$, where $e'_i = e_i(q) - c_f^{(m)}(a_i, s) - c_f^{(a)}(a_i s, e_i)$.
- $R_\infty(U(\mathbb{Z}_{q^m+1})||U(\mathbb{Z}_q[x]/x^m + 1)(q)) \leq \frac{2(q^m+1)}{q^m}$.
- $R_2(e_i(q)||e'_i) = \exp\left(\frac{2\pi\|c_f^{(m)}(a_i,s)+c_f^{(a)}(a_i s,e_i)\|^2}{\sigma^2}\right)$.
- Conclude using the Multiplicativity and Data Processing inequality

But...

- $R(P||Q)$ is defined if $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$.
- Offset $c_f^{(m)}(a_i, s) + c_f^{(a)}(a_i s, e_i)$ is dependent on $e_i$.

# sPLWE to sI-PLWE Reduction Analysis

- $(a_i s + e_i)(q) = a_i(q)s(q) + e'_i \bmod q^m + 1$, where $e'_i = e_i(q) - c_f^{(m)}(a_i, s) - c_f^{(a)}(a_i s, e_i)$.
- $R_\infty(U(\mathbb{Z}_{q^m+1})||U(\mathbb{Z}_q[x]/x^m + 1)(q)) \leq \frac{2(q^m+1)}{q^m}$.
- $R_2(e_i(q)||e'_i) = \exp\left(\frac{2\pi\|c_f^{(m)}(a_i,s)+c_f^{(a)}(a_i s,e_i)\|^2}{\sigma^2}\right)$.
- Conclude using the Multiplicativity and Data Processing inequality

But...

- $R(P||Q)$ is defined if $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$.
- Offset $c_f^{(m)}(a_i, s) + c_f^{(a)}(a_i s, e_i)$ is dependent on $e_i$.

# Parameters range

**Hardness of sI-PLWE**

If

$$\exp\left(\frac{7m}{\sigma'^2} + 114t\left(1 + \frac{4m^3(1+m^{1/2}\sigma')^2}{\sigma^2}\right)\right) = \mathrm{poly}(m),$$

then $\mathrm{sPLWE}_{q,\sigma,\sigma',t}$ reduces to $\mathrm{sI\text{-}PLWE}_{q,\sigma,\sigma',t}$.

Set the parameters in this order: $t, m, \sigma', \sigma, q$.

# Parameters range

**Hardness of sI-PLWE**

If

$$\exp\left(\frac{7m}{\sigma'^2} + 114t\left(1 + \frac{4m^3(1+m^{1/2}\sigma')^2}{\sigma^2}\right)\right) = \mathrm{poly}(m),$$

then $\mathrm{sPLWE}_{q,\sigma,\sigma',t}$ reduces to $\mathrm{sI\text{-}PLWE}_{q,\sigma,\sigma',t}$.

Set the parameters in this order: $t, m, \sigma', \sigma, q$.

# Equivalence of the problems

**Equivalence of sI-PLWE and sPLWE**

If

$$\exp\left(114t\left(1+456m^3\frac{(1+m^{1/2}\sigma')^2}{\sigma^2}\right)\right)=\mathrm{poly}(m),$$

then $\mathrm{sI\text{-}PLWE}_{q,\sigma,\sigma',t}$ reduces to $\mathrm{sPLWE}_{q,\sigma,\sigma',t}$.

# A public-key encryption based on sI-PLWE

# Construction

- Adapted from [LPS10][2] to I-PLWE, with a tweak to recover encryption randomness.
- KeyGen($1^\lambda$). Sample $(a, b := as + e) \in \mathbb{Z}^2_{f(q)}$, an sI-PLWE$_{q,\sigma,\sigma',1}$ sample and output:

$$\mathsf{pk} := (a, b) \text{ and } \mathsf{sk} := (s, e).$$

- Enc(pk, $(t, e', e'')$). Compute and output:

$$(c_1, c_2) := (a \cdot t + K \cdot e',\ b \cdot t + K \cdot e'') \in \mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}.$$

- Dec(sk, $c_1, c_2$). Let $d := c_2 - c_1 \cdot s =: \sum_i d_i q^i$, compute $d' = \sum_i (d_i \bmod K) \cdot q^i \bmod f(q)$. Return

$$(d'e^{-1}, (c_1 - ad'e^{-1})K^{-1}, (c_2 - bd'e^{-1})K^{-1}) \in \mathbb{Z}^3_{f(q)}.$$

[2] *Lyubashevsky, Palacio, Segev TCC'10*

# Construction

- Adapted from [LPS10][2] to I-PLWE, with a tweak to recover encryption randomness.
- KeyGen($1^\lambda$). Sample $(a, b := as + e) \in \mathbb{Z}^2_{f(q)}$, an sI-PLWE$_{q,\sigma,\sigma',1}$ sample and output:

$$\mathsf{pk} := (a, b) \text{ and } \mathsf{sk} := (s, e).$$

- Enc(pk, $(t, e', e'')$). Compute and output:

$$(c_1, c_2) := (a \cdot t + K \cdot e',\ b \cdot t + K \cdot e'') \in \mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}.$$

- Dec(sk, $c_1, c_2$). Let $d := c_2 - c_1 \cdot s =: \sum_i d_i q^i$, compute $d' = \sum_i (d_i \bmod K) \cdot q^i \bmod f(q)$. Return

$$(d'e^{-1}, (c_1 - ad'e^{-1})K^{-1}, (c_2 - bd'e^{-1})K^{-1}) \in \mathbb{Z}^3_{f(q)}.$$

[2] *Lyubashevsky, Palacio, Segev TCC'10*

# Construction

- Adapted from [LPS10][2] to I-PLWE, with a tweak to recover encryption randomness.
- KeyGen($1^\lambda$). Sample $(a, b := as + e) \in \mathbb{Z}_{f(q)}^2$, an sI-PLWE$_{q,\sigma,\sigma',1}$ sample and output:

$$\mathsf{pk} := (a, b) \text{ and } \mathsf{sk} := (s, e).$$

- Enc(pk, $(t, e', e'')$). Compute and output:

$$(c_1, c_2) := (a \cdot t + K \cdot e',\ b \cdot t + K \cdot e'') \in \mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}.$$

- Dec(sk, $c_1, c_2$). Let $d := c_2 - c_1 \cdot s =: \sum_i d_i q^i$, compute $d' = \sum_i (d_i \bmod K) \cdot q^i \bmod f(q)$. Return

$$(d'e^{-1}, (c_1 - ad'e^{-1})K^{-1}, (c_2 - bd'e^{-1})K^{-1}) \in \mathbb{Z}_{f(q)}^3.$$

[2] *Lyubashevsky, Palacio, Segev TCC'10*

# Construction

- Adapted from [LPS10][2] to I-PLWE, with a tweak to recover encryption randomness.
- KeyGen($1^\lambda$). Sample $(a, b := as + e) \in \mathbb{Z}_{f(q)}^2$, an sI-PLWE$_{q,\sigma,\sigma',1}$ sample and output:

$$\mathsf{pk} := (a, b) \text{ and } \mathsf{sk} := (s, e).$$

- Enc(pk, $(t, e', e'')$). Compute and output:

$$(c_1, c_2) := (a \cdot t + K \cdot e',\ b \cdot t + K \cdot e'') \in \mathbb{Z}_{f(q)} \times \mathbb{Z}_{f(q)}.$$

- Dec(sk, $c_1, c_2$). Let $d := c_2 - c_1 \cdot s =: \sum_i d_i q^i$, compute $d' = \sum_i (d_i \bmod K) \cdot q^i \bmod f(q)$. Return

$$(d'e^{-1}, (c_1 - ad'e^{-1})K^{-1}, (c_2 - bd'e^{-1})K^{-1}) \in \mathbb{Z}_{f(q)}^3.$$

[2] *Lyubashevsky, Palacio, Segev TCC'10*

# Properties

**Correctness**

The scheme is correct for $f(q)$ prime, $K$ small and for message space

$$\mathcal{M} = \{(t, e', e'') \in \mathbb{Z}^3_{f(q)} \mid \|\Phi_q(t)\|_\infty \leq \sigma' \sqrt{m} \\ \wedge \|\Phi_q(e')\|_\infty, \|\Phi_q(e'')\|_\infty \leq \sigma \sqrt{m}\}.$$

# Properties (2)

**Security**

The scheme satisfies OW-CPA security: given a ciphertext for a random plaintext, it is hard to compute the plaintext.

- First step: Replace $(a, b)$ with an (evaluated) PLWE sample.
- Second step: $b$ is indistinguishable from uniform, under decision PLWE (equivalent to search I-PLWE).
- Third step: $((K^{-1}a, K^{-1}c_1), (K^{-1}b, K^{-1}c_2))$ are two samples of the sI-PLWE distribution. Computing $(t, e', e'')$ is thus hard.
- OW-CPA can then be turned into IND-CCA2 in the ROM and QROM with the F-O transform.

# Properties (2)

**Security**

The scheme satisfies OW-CPA security: given a ciphertext for a random plaintext, it is hard to compute the plaintext.

- First step: Replace $(a, b)$ with an (evaluated) PLWE sample.
- Second step: $b$ is indistinguishable from uniform, under decision PLWE (equivalent to search I-PLWE).
- Third step: $((K^{-1}a, K^{-1}c_1), (K^{-1}b, K^{-1}c_2))$ are two samples of the sI-PLWE distribution. Computing $(t, e', e'')$ is thus hard.
- OW-CPA can then be turned into IND-CCA2 in the ROM and QROM with the F-O transform.

# Properties (2)

**Security**

The scheme satisfies OW-CPA security: given a ciphertext for a random plaintext, it is hard to compute the plaintext.

- First step: Replace $(a, b)$ with an (evaluated) PLWE sample.
- Second step: $b$ is indistinguishable from uniform, under decision PLWE (equivalent to search I-PLWE).
- Third step: $((K^{-1}a, K^{-1}c_1), (K^{-1}b, K^{-1}c_2))$ are two samples of the sI-PLWE distribution. Computing $(t, e', e'')$ is thus hard.
- OW-CPA can then be turned into IND-CCA2 in the ROM and QROM with the F-O transform.

# Properties (2)

**Security**

The scheme satisfies OW-CPA security: given a ciphertext for a random plaintext, it is hard to compute the plaintext.

- First step: Replace $(a, b)$ with an (evaluated) PLWE sample.
- Second step: $b$ is indistinguishable from uniform, under decision PLWE (equivalent to search I-PLWE).
- Third step: $((K^{-1}a, K^{-1}c_1), (K^{-1}b, K^{-1}c_2))$ are two samples of the sI-PLWE distribution. Computing $(t, e', e'')$ is thus hard.
- OW-CPA can then be turned into IND-CCA2 in the ROM and QROM with the F-O transform.

# Properties (2)

**Security**

The scheme satisfies OW-CPA security: given a ciphertext for a random plaintext, it is hard to compute the plaintext.

- First step: Replace $(a, b)$ with an (evaluated) PLWE sample.
- Second step: $b$ is indistinguishable from uniform, under decision PLWE (equivalent to search I-PLWE).
- Third step: $((K^{-1}a, K^{-1}c_1), (K^{-1}b, K^{-1}c_2))$ are two samples of the sI-PLWE distribution. Computing $(t, e', e'')$ is thus hard.
- OW-CPA can then be turned into IND-CCA2 in the ROM and QROM with the F-O transform.

# Thank you!