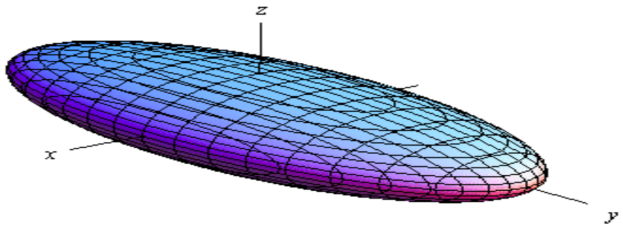
Remarks on the error distributions in ring-based LWE



Wouter Castryck[1,2], Ilia Iliashenko[1], Frederik Vercauteren[1,3]

[1] COSIC, KU Leuven
[2] Ghent University
[3] Open Security Research

PQCRYPTO
ICT-645622

HEAT

0. Abstract

Very brief history:

- 1981: R. Feynman introduces concept of a quantum computer.

0. Abstract

Very brief history:

- 1981: R. Feynman introduces concept of a quantum computer.
- 1994: P. Shor describes polynomial time factoring quantum algorithm.

0. Abstract

Very brief history:

- 1981: R. Feynman introduces concept of a quantum computer.
- 1994: P. Shor describes polynomial time factoring quantum algorithm.
- 2001: Team at IBM factors $15 = 3 \times 5$.

0. Abstract

Very brief history:

- 1981: R. Feynman introduces concept of a quantum computer.
- 1994: P. Shor describes polynomial time factoring quantum algorithm.
- 2001: Team at IBM factors $15 = 3 \times 5$.
- 2012: Team at Bristol factors $21 = 3 \times 7$.

0. Abstract

Very brief history:

- 1981: R. Feynman introduces concept of a quantum computer.
- 1994: P. Shor describes polynomial time factoring quantum algorithm.
- 2001: Team at IBM factors $15 = 3 \times 5$.
- 2012: Team at Bristol factors $21 = 3 \times 7$.

Shor's method also computes discrete logarithms, both in

- the multiplicative group of a finite field $\mathbb{F}_p^\times, \cdot$,
- the group of rational points on an elliptic curve $E(\mathbb{F}_p), +$.

0. Abstract

Very brief history:

- 1981: R. Feynman introduces concept of a quantum computer.
- 1994: P. Shor describes polynomial time factoring quantum algorithm.
- 2001: Team at IBM factors $15 = 3 \times 5$.
- 2012: Team at Bristol factors $21 = 3 \times 7$.

Shor's method also computes discrete logarithms, both in

- the multiplicative group of a finite field $\mathbb{F}_p^\times, \cdot$,
- the group of rational points on an elliptic curve $E(\mathbb{F}_p), +$.

Cryptography should get ready for the post-quantum era...

0. Abstract

Main contenders:

- Solving multivariate quadratic systems mod p:

$$\begin{cases} s_0^2 - 3s_1s_4 + s_0s_5 + 2s_0s_3 - s_6^2 + s_1 + s_4 = 5, \\ s_0s_1 - 3s_1s_6 + 5s_4s_5 + s_5^2 + s_1 + 2s_4 - s_5 - 3s_6 = 2, \\ \vdots \end{cases}$$

0. Abstract

Main contenders:

- Solving multivariate quadratic systems mod p:

$$\begin{cases} s_0^2 - 3s_1s_4 + s_0s_5 + 2s_0s_3 - s_6^2 + s_1 + s_4 = 5, \\ s_0s_1 - 3s_1s_6 + 5s_4s_5 + s_5^2 + s_1 + 2s_4 - s_5 - 3s_6 = 2, \\ \vdots \end{cases}$$

- Solving noisy linear systems mod p:

$$\begin{cases} s_0 - 2s_1 + s_2 + 2s_3 - s_4 - 3s_5 + s_6 \approx 2, \\ 3s_0 + s_1 - s_2 - 7s_3 + 3s_4 - s_5 - s_6 \approx 0, \\ \vdots \end{cases}$$

This is called LWE.

- Many variants: LPN, SIS, Poly-LWE, Ring-LWE, ...

0. Abstract

Main contenders:

- Solving multivariate quadratic systems mod p:

$$\begin{cases} s_0^2 - 3s_1s_4 + s_0s_5 + 2s_0s_3 - s_6^2 + s_1 + s_4 = 5, \\ s_0s_1 - 3s_1s_6 + 5s_4s_5 + s_5^2 + s_1 + 2s_4 - s_5 - 3s_6 = 2, \\ \vdots \end{cases}$$

- Solving noisy linear systems mod p:

$$\begin{cases} s_0 - 2s_1 + s_2 + 2s_3 - s_4 - 3s_5 + s_6 \approx 2, \\ 3s_0 + s_1 - s_2 - 7s_3 + 3s_4 - s_5 - s_6 \approx 0, \\ \vdots \end{cases}$$

This is called LWE.

  - Many variants: LPN, SIS, Poly-LWE, Ring-LWE, ...

- Decoding random linear codes (McEliece).

0. Abstract

Main contenders:

- Solving multivariate quadratic systems mod p:

$$\begin{cases} s_0^2 - 3s_1s_4 + s_0s_5 + 2s_0s_3 - s_6^2 + s_1 + s_4 = 5, \\ s_0s_1 - 3s_1s_6 + 5s_4s_5 + s_5^2 + s_1 + 2s_4 - s_5 - 3s_6 = 2, \\ \vdots \end{cases}$$

- Solving noisy linear systems mod p:

$$\begin{cases} s_0 - 2s_1 + s_2 + 2s_3 - s_4 - 3s_5 + s_6 \approx 2, \\ 3s_0 + s_1 - s_2 - 7s_3 + 3s_4 - s_5 - s_6 \approx 0, \\ \vdots \end{cases}$$

This is called LWE.

  - Many variants: LPN, SIS, Poly-LWE, Ring-LWE, ...

- Decoding random linear codes (McEliece).
- The NTRU problem and its variants.

0. Abstract

Main contenders:

- Solving multivariate quadratic systems mod p:

$$\begin{cases} s_0^2 - 3s_1s_4 + s_0s_5 + 2s_0s_3 - s_6^2 + s_1 + s_4 = 5, \\ s_0s_1 - 3s_1s_6 + 5s_4s_5 + s_5^2 + s_1 + 2s_4 - s_5 - 3s_6 = 2, \\ \vdots \end{cases}$$

- Solving noisy linear systems mod p:

$$\begin{cases} s_0 - 2s_1 + s_2 + 2s_3 - s_4 - 3s_5 + s_6 \approx 2, \\ 3s_0 + s_1 - s_2 - 7s_3 + 3s_4 - s_5 - s_6 \approx 0, \\ \vdots \end{cases}$$

This is called LWE.

  - Many variants: LPN, SIS, Poly-LWE, Ring-LWE, ...

- Decoding random linear codes (McEliece).
- The NTRU problem and its variants.
- Finding elliptic curve isogenies.

0. Abstract

Main contenders:

- Solving multivariate quadratic systems mod p:

$$\begin{cases} s_0^2 - 3s_1s_4 + s_0s_5 + 2s_0s_3 - s_6^2 + s_1 + s_4 = 5, \\ s_0s_1 - 3s_1s_6 + 5s_4s_5 + s_5^2 + s_1 + 2s_4 - s_5 - 3s_6 = 2, \\ \vdots \end{cases}$$

- Solving noisy linear systems mod p:

$$\begin{cases} s_0 - 2s_1 + s_2 + 2s_3 - s_4 - 3s_5 + s_6 \approx 2, \\ 3s_0 + s_1 - s_2 - 7s_3 + 3s_4 - s_5 - s_6 \approx 0, \\ \vdots \end{cases}$$

This is called LWE.

  - Many variants: LPN, SIS, Poly-LWE, Ring-LWE, ...

- Decoding random linear codes (McEliece).
- The NTRU problem and its variants.
- Finding elliptic curve isogenies.

} lattice-based cryptography

0. Abstract

Main contenders:

- Solving multivariate quadratic systems mod p:

$$\begin{cases} s_0^2 - 3s_1s_4 + s_0s_5 + 2s_0s_3 - s_6^2 + s_1 + s_4 = 5, \\ s_0s_1 - 3s_1s_6 + 5s_4s_5 + s_5^2 + s_1 + 2s_4 - s_5 - 3s_6 = 2, \\ \vdots \end{cases}$$

- Solving noisy linear systems mod p:

$$\begin{cases} s_0 - 2s_1 + s_2 + 2s_3 - s_4 - 3s_5 + s_6 \approx 2, \\ 3s_0 + s_1 - s_2 - 7s_3 + 3s_4 - s_5 - s_6 \approx 0, \\ \vdots \end{cases}$$

This is called LWE.

  - Many variants: LPN, SIS, Poly-LWE, Ring-LWE, ...

- Decoding random linear codes (McEliece).
- The NTRU problem and its variants.
- Finding elliptic curve isogenies.

} lattice-based cryptography

0. Abstract

LWE has important features besides being quantum resistant:

- hardness reduction from classical lattice problems,
- versatile building block for cryptography, enabling exciting new applications (FHE)

0. Abstract

LWE has important features besides being quantum resistant:

- hardness reduction from classical lattice problems,
- versatile building block for cryptography, enabling exciting new applications (FHE)

Drawback: key sizes of resulting schemes.

0. Abstract

LWE has important features besides being quantum resistant:

- hardness reduction from classical lattice problems,
- versatile building block for cryptography, enabling exciting new applications (FHE)

Drawback: key sizes of resulting schemes.

O. Regev, V. Lyubashevsky, C. Peikert, ‘10: Ring-LWE.

0. Abstract

LWE has important features besides being quantum resistant:

- hardness reduction from classical lattice problems,
- versatile building block for cryptography, enabling exciting new applications (FHE)

Drawback: key sizes of resulting schemes.

O. Regev, V. Lyubashevsky, C. Peikert, ‘10: Ring-LWE.

Questions:

- Can an attacker exploit the ring structure?
- What is Ring-LWE in fact (lot of confusion)?

0. Abstract

Concretely, in this research we revisited the paper

Provably weak instances of Ring-LWE

by Y. Elias, K. Lauter, E. Ozman, K. Stange, CRYPTO 2015

in which the authors

- investigate if evaluation-at-1-attacks apply to Ring-LWE,

0. Abstract

Concretely, in this research we revisited the paper

Provably weak instances of Ring-LWE

by Y. Elias, K. Lauter, E. Ozman, K. Stange, CRYPTO 2015

in which the authors

- investigate if evaluation-at-1-attacks apply to Ring-LWE,
- claim to have indeed found vulnerable instances.

0. Abstract

Concretely, in this research we revisited the paper

Provably weak instances of Ring-LWE

by Y. Elias, K. Lauter, E. Ozman, K. Stange, CRYPTO 2015

in which the authors

- investigate if evaluation-at-1-attacks apply to Ring-LWE,
- claim to have indeed found vulnerable instances.
- Vulnerable meaning: leak partial information about the secret with non-negligible probability.

0. Abstract

Concretely, in this research we revisited the paper

Provably weak instances of Ring-LWE

by Y. Elias, K. Lauter, E. Ozman, K. Stange, CRYPTO 2015

in which the authors

- investigate if evaluation-at-1-attacks apply to Ring-LWE,
- claim to have indeed found vulnerable instances.
- Vulnerable meaning: leak partial information about the secret with non-negligible probability.

However,

- they did not set up Ring-LWE as described in [LPR].

0. Abstract

Concretely, in this research we revisited the paper

Provably weak instances of Ring-LWE

by Y. Elias, K. Lauter, E. Ozman, K. Stange, CRYPTO 2015

in which the authors

- investigate if evaluation-at-1-attacks apply to Ring-LWE,
- claim to have indeed found vulnerable instances.
- Vulnerable meaning: leak partial information about the secret with non-negligible probability.

However,

- they did not set up Ring-LWE as described in [LPR].
- Their instantiation generates many noise-free equations

0. Abstract

Concretely, in this research we revisited the paper

Provably weak instances of Ring-LWE

by Y. Elias, K. Lauter, E. Ozman, K. Stange, CRYPTO 2015

in which the authors

- investigate if evaluation-at-1-attacks apply to Ring-LWE,
- claim to have indeed found vulnerable instances.
- Vulnerable meaning: leak partial information about the secret with non-negligible probability.

However,

- they did not set up Ring-LWE as described in [LPR].
- Their instantiation generates many noise-free equations
- allowing to recover the entire secret with near certainty.

0. Abstract

Concretely, in this research we revisited the paper

Provably weak instances of Ring-LWE

by Y. Elias, K. Lauter, E. Ozman, K. Stange, CRYPTO 2015

in which the authors

- investigate if evaluation-at-1-attacks apply to Ring-LWE,
- claim to have indeed found vulnerable instances.
- Vulnerable meaning: leak partial information about the secret with non-negligible probability.

However,

- they did not set up Ring-LWE as described in [LPR].
- Their instantiation generates many noise-free equations
- allowing to recover the entire secret with near certainty.

Currently no threat to Ring-LWE.

1. Learning With Errors (LWE)

The LWE problem (O. Regev, '05): solve a linear system

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{pmatrix} \approx \begin{pmatrix} a_{10} & a_{11} & \dots & a_{1,n-1} \\ a_{20} & a_{21} & \dots & a_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m0} & a_{m1} & \dots & a_{m,n-1} \end{pmatrix} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix}$$

over a finite field $\mathbb{F}_p$ for a secret $(s_0, s_1, \dots, s_{n-1}) \in \mathbb{F}_p^n$ where

1. Learning With Errors (LWE)

The LWE problem (O. Regev, '05): solve a linear system

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{pmatrix} \approx \begin{pmatrix} a_{10} & a_{11} & \dots & a_{1,n-1} \\ a_{20} & a_{21} & \dots & a_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m0} & a_{m1} & \dots & a_{m,n-1} \end{pmatrix} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix}$$

over a finite field $\mathbb{F}_p$ for a secret $(s_0, s_1, \dots, s_{n-1}) \in \mathbb{F}_p^n$ where

- each equation is perturbed by a "small" error, i.e.

$$b_i = a_{i0}s_0 + a_{i1}s_1 + \cdots + a_{i,n-1}s_{n-1} + e_i,$$

1. Learning With Errors (LWE)

The LWE problem (O. Regev, '05): solve a linear system

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{pmatrix} \approx \begin{pmatrix} a_{10} & a_{11} & \cdots & a_{1,n-1} \\ a_{20} & a_{21} & \cdots & a_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m0} & a_{m1} & \cdots & a_{m,n-1} \end{pmatrix} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix}$$

over a finite field $\mathbb{F}_p$ for a secret $(s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_p^n$ where

- each equation is perturbed by a "small" error, i.e.

$$b_i = a_{i0}s_0 + a_{i1}s_1 + \cdots + a_{i,n-1}s_{n-1} + e_i,$$

- the $a_{ij} \in \mathbb{F}_p$ are chosen uniformly randomly,

1. Learning With Errors (LWE)

The LWE problem (O. Regev, '05): solve a linear system

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{pmatrix} \approx \begin{pmatrix} a_{10} & a_{11} & \cdots & a_{1,n-1} \\ a_{20} & a_{21} & \cdots & a_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m0} & a_{m1} & \cdots & a_{m,n-1} \end{pmatrix} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix}$$

over a finite field $\mathbb{F}_p$ for a secret $(s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_p^n$ where

- each equation is perturbed by a "small" error, i.e.

$$b_i = a_{i0}s_0 + a_{i1}s_1 + \cdots + a_{i,n-1}s_{n-1} + e_i,$$

- the $a_{ij} \in \mathbb{F}_p$ are chosen uniformly randomly,
- an adversary can ask for new equations ($m > n$).

1. Learning With Errors (LWE)

The LWE problem (O. Regev, '05): solve a linear system

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{pmatrix} = \begin{pmatrix} a_{10} & a_{11} & \dots & a_{1,n-1} \\ a_{20} & a_{21} & \dots & a_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m0} & a_{m1} & \dots & a_{m,n-1} \end{pmatrix} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{m-1} \end{pmatrix}$$

over a finite field $\mathbb{F}_p$ for a secret $(s_0, s_1, \dots, s_{n-1}) \in \mathbb{F}_p^n$ where

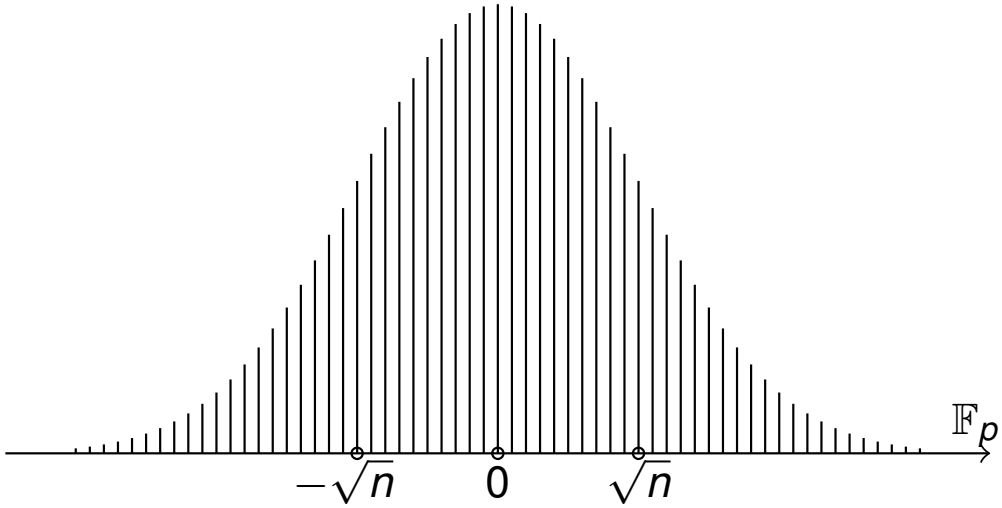
- each equation is perturbed by a "small" error, i.e.

$$b_i = a_{i0}s_0 + a_{i1}s_1 + \cdots + a_{i,n-1}s_{n-1} + e_i,$$

- the $a_{ij} \in \mathbb{F}_p$ are chosen uniformly randomly,
- an adversary can ask for new equations ($m > n$).

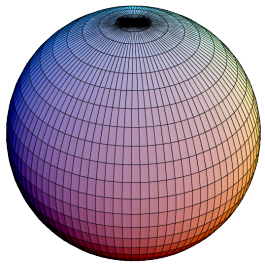
1. Learning With Errors (LWE)

The errors e_i are sampled independently from a Gaussian with standard deviation $\sigma \gtrsim \sqrt{n}$:



When viewed jointly, the error vector

$$\begin{pmatrix} e_0 \\ \vdots \\ e_{m-1} \end{pmatrix}$$



is sampled from a spherical Gaussian.

1. Learning With Errors (LWE)

Known attacks for $q = \text{poly}(n)$:

- Trial and error:
  $2^{O(n \log n)}$ time and $O(n)$ samples.
- A. Blum, A. Kalai, H. Wasserman '03:
  $2^{O(n)}$ time and $2^{O(n)}$ samples.
- S. Arora, R. Ge '11:
  $2^{O(\sigma^2 \log n)}$ time and $2^{O(\sigma^2 \log n)}$ samples.

1. Learning With Errors (LWE)

Known attacks for $q = \text{poly}(n)$:

- Trial and error:
  $2^{O(n \log n)}$ time and $O(n)$ samples.
- A. Blum, A. Kalai, H. Wasserman '03:
  $2^{O(n)}$ time and $2^{O(n)}$ samples.
- S. Arora, R. Ge '11:
  $2^{O(\sigma^2 \log n)}$ time and $2^{O(\sigma^2 \log n)}$ samples.
  Idea: if all errors (almost) certainly lie in $\{-T, \ldots, T\}$, then

$$\prod_{i=-T}^{T} (a_0 s_0 + a_1 s_1 + \cdots + a_{n-1} s_{n-1} - i) = 0.$$

1. Learning With Errors (LWE)

Known attacks for $q = \text{poly}(n)$:

- Trial and error:
  $2^{O(n \log n)}$ time and $O(n)$ samples.
- A. Blum, A. Kalai, H. Wasserman '03:
  $2^{O(n)}$ time and $2^{O(n)}$ samples.
- S. Arora, R. Ge '11:
  $2^{O(\sigma^2 \log n)}$ time and $2^{O(\sigma^2 \log n)}$ samples.
  Idea: if all errors (almost) certainly lie in $\{-T, \ldots, T\}$, then

$$\prod_{i=-T}^{T} (a_0 s_0 + a_1 s_1 + \cdots + a_{n-1} s_{n-1} - i) = 0.$$

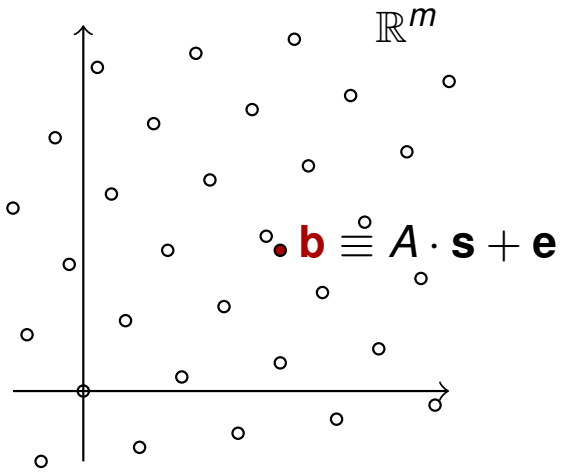
  View as linear system of equations in $\approx n^{2T}$ monomials.

1. Learning With Errors (LWE)

LWE is tightly related to classical lattice problems.

- Can be thought of as an instance of BDD inside the lattice

$$
\begin{array}{c}
(p\mathbb{Z})^m \\
\cap \\
\{\mathbf{w} \in \mathbb{Z}^m \mid \exists \mathbf{s} \in \mathbb{Z}^n : \mathbf{w} \equiv A \cdot \mathbf{s} \bmod p\} \\
\cap \\
\mathbb{Z}^m.
\end{array}
$$

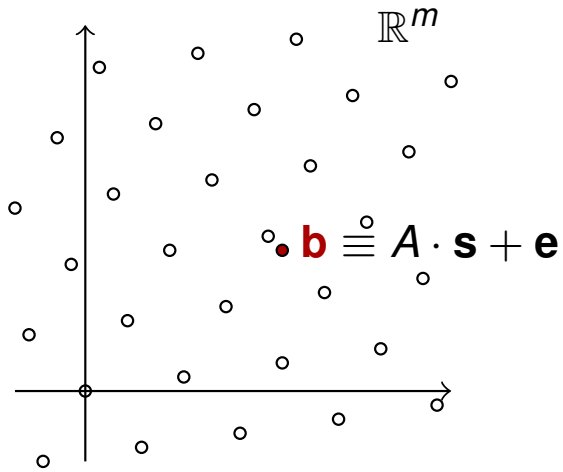


1. Learning With Errors (LWE)

LWE is tightly related to classical lattice problems.

- Can be thought of as an instance of BDD inside the lattice

$$\begin{array}{c} (p\mathbb{Z})^m \\ \cap \\ \{\mathbf{w} \in \mathbb{Z}^m \mid \exists \mathbf{s} \in \mathbb{Z}^n : \mathbf{w} \equiv A\cdot\mathbf{s} \bmod p\} \\ \cap \\ \mathbb{Z}^m. \end{array}$$



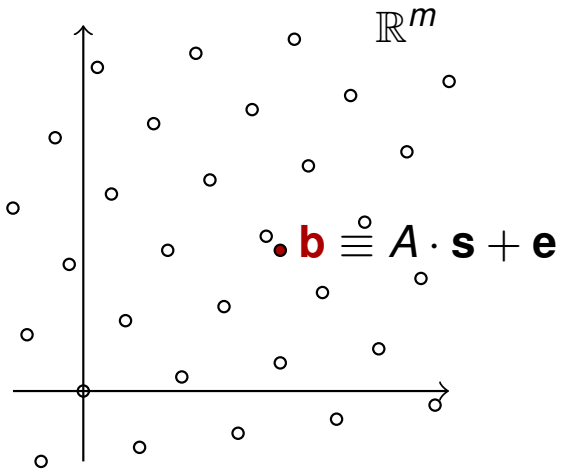
- Proven to be at least as hard as worst-case SVP-type problems, by O. Regev in ‘05 and C. Peikert in ‘09.

1. Learning With Errors (LWE)

LWE is tightly related to classical lattice problems.

- Can be thought of as an instance of BDD inside the lattice

$$\begin{array}{c} (p\mathbb{Z})^m \\ \cap \\ \{\mathbf{w} \in \mathbb{Z}^m \mid \exists \mathbf{s} \in \mathbb{Z}^n : \mathbf{w} \equiv A\cdot\mathbf{s} \bmod p\} \\ \cap \\ \mathbb{Z}^m. \end{array}$$



- Proven to be at least as hard as worst-case SVP-type problems, by O. Regev in ‘05 and C. Peikert in ‘09.
- Not known to be broken by quantum computers.

1. Learning With Errors (LWE)

Application: public-key encryption of a bit (O. Regev, '05).

- Private key: $\mathbf{s} \in \mathbb{F}_p^n$.
- Public key pair: A and $\mathbf{b} = A \cdot \mathbf{s} + \mathbf{e}$.

1. Learning With Errors (LWE)

Application: public-key encryption of a bit (O. Regev, '05).

- Private key: $\mathbf{s} \in \mathbb{F}_p^n$.
- Public key pair: A and $\mathbf{b} = A \cdot \mathbf{s} + \mathbf{e}$.
- Encrypt: pick random row vector $\mathbf{r}^T \in \{0,1\}^m \subset \mathbb{F}_p^m$. Output the pair
  - $\mathbf{a}^T := \mathbf{r}^T \cdot A$ and $b := \mathbf{r}^T \cdot \mathbf{b}$ if the bit is 0,
  - $\mathbf{a}^T := \mathbf{r}^T \cdot A$ and $b := \mathbf{r}^T \cdot \mathbf{b} + \lfloor p/2 \rfloor$ if the bit is 1.

1. Learning With Errors (LWE)

Application: public-key encryption of a bit (O. Regev, '05).

- Private key: $\mathbf{s} \in \mathbb{F}_p^n$.
- Public key pair: A and $\mathbf{b} = A \cdot \mathbf{s} + \mathbf{e}$.
- Encrypt: pick random row vector $\mathbf{r}^T \in \{0,1\}^m \subset \mathbb{F}_p^m$.
  Output the pair
  - $\mathbf{a}^T := \mathbf{r}^T \cdot A$ and $b := \mathbf{r}^T \cdot \mathbf{b}$ if the bit is 0,
  - $\mathbf{a}^T := \mathbf{r}^T \cdot A$ and $b := \mathbf{r}^T \cdot \mathbf{b} + \lfloor p/2 \rfloor$ if the bit is 1.
- Decryption of pair $\mathbf{a}^T, b$: compute

$$b - \mathbf{a}^T \cdot \mathbf{s} = b - \mathbf{r}^T \cdot A \cdot \mathbf{s} \approx b - \mathbf{r}^T \mathbf{b} = \begin{cases} 0 & \text{if bit was 0,} \\ \lfloor p/2 \rfloor & \text{if bit was 1.} \end{cases}$$

1. Learning With Errors (LWE)

Features:

- hardness reduction from classical lattice problems,
- versatile building block for cryptography, enabling exciting applications (FHE, PQ crypto, . . .)

1. Learning With Errors (LWE)

Features:

- hardness reduction from classical lattice problems,
- versatile building block for cryptography, enabling exciting applications (FHE, PQ crypto, . . .)

Drawback: key size.

- To hide the secret one needs an entire linear system:

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{pmatrix} \approx \begin{pmatrix} a_{10} & a_{11} & \cdots & a_{1,n-1} \\ a_{20} & a_{21} & \cdots & a_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m0} & a_{m1} & \cdots & a_{m,n-1} \end{pmatrix} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix}.$$

$m \log p$ $\quad$ $mn \log p$ $\quad$ $n \log p$

2. Ring-based LWE

Solution:

- Identify key space

$$\mathbb{F}_p^n \qquad \text{with} \qquad \frac{\mathbb{Z}[x]}{(p, f(x))}$$

for some monic deg n polynomial $f(x) \in \mathbb{Z}[x]$, by viewing

$$(s_0, s_1, \ldots, s_{n-1}) \quad \text{as} \quad s_0 + s_1 x + s_2 x^2 + \cdots + s_{n-1} x^{n-1}.$$

2. Ring-based LWE

Solution:

- Identify key space

$$\mathbb{F}_p^n \qquad \text{with} \qquad \frac{\mathbb{Z}[x]}{(p, f(x))}$$

for some monic deg n polynomial $f(x) \in \mathbb{Z}[x]$, by viewing

$$(s_0, s_1, \ldots, s_{n-1}) \quad \text{as} \quad s_0 + s_1 x + s_2 x^2 + \cdots + s_{n-1} x^{n-1}.$$

- Use samples of the form

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} \approx A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix}$$

with $A_{\mathbf{a}}$ the matrix of multiplication by some random $\mathbf{a}(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$.

2. Ring-based LWE

Solution:

- Identify key space

$$\mathbb{F}_p^n \qquad \text{with} \qquad \frac{\mathbb{Z}[x]}{(p, f(x))}$$

for some monic deg n polynomial $f(x) \in \mathbb{Z}[x]$, by viewing

$$(s_0, s_1, \ldots, s_{n-1}) \quad \text{as} \quad s_0 + s_1 x + s_2 x^2 + \cdots + s_{n-1} x^{n-1}.$$

- Use samples of the form

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} \approx A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix}$$

with $A_{\mathbf{a}}$ the matrix of multiplication by some random $\mathbf{a}(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$.

- Store $\mathbf{a}(x)$ rather than $A_{\mathbf{a}}$: saves factor n.

2. Ring-based LWE

Example:

- if $f(x) = x^n - 1$, then $A_{\mathbf{a}}$ is the circulant matrix

$$\begin{pmatrix} a_0 & a_{n-1} & \dots & a_2 & a_1 \\ a_1 & a_0 & \dots & a_3 & a_2 \\ a_2 & a_1 & \dots & a_4 & a_3 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \end{pmatrix}$$

of which it suffices to store the first column.

2. Ring-based LWE

Example:

- if $f(x) = x^n - 1$, then $A_{\mathbf{a}}$ is the circulant matrix

$$\begin{pmatrix} a_0 & a_{n-1} & \dots & a_2 & a_1 \\ a_1 & a_0 & \dots & a_3 & a_2 \\ a_2 & a_1 & \dots & a_4 & a_3 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \end{pmatrix}$$

  of which it suffices to store the first column.

- Bad example, because of . . .

3. Evaluation-at-1 attack

Potential threat:

- Suppose $f(1) \equiv 0 \bmod p$, then

$$\frac{\mathbb{Z}[x]}{(p, f(x))} \to \mathbb{F}_p : \mathbf{r}(x) \mapsto \mathbf{r}(1) = r_0 + r_1 + \cdots + r_{n-1},$$

is a well-defined ring homomorphism.

3. Evaluation-at-1 attack

Potential threat:

- Suppose $f(1) \equiv 0 \bmod p$, then

$$\frac{\mathbb{Z}[x]}{(p, f(x))} \to \mathbb{F}_p : \mathbf{r}(x) \mapsto \mathbf{r}(1) = r_0 + r_1 + \cdots + r_{n-1},$$

  is a well-defined ring homomorphism.

- Our ring-based LWE samples

$$\mathbf{b}(x) = \mathbf{a}(x) \cdot \mathbf{s}(x) + \mathbf{e}(x)$$

  evaluate to

$$\mathbf{b}(1) = \mathbf{a}(1) \cdot \mathbf{s}(1) + \mathbf{e}(1).$$

3. Evaluation-at-1 attack

Potential threat:

- Suppose $f(1) \equiv 0 \bmod p$, then

$$\frac{\mathbb{Z}[x]}{(p, f(x))} \to \mathbb{F}_p : \mathbf{r}(x) \mapsto \mathbf{r}(1) = r_0 + r_1 + \cdots + r_{n-1},$$

  is a well-defined ring homomorphism.

- Our ring-based LWE samples

$$\mathbf{b}(x) = \mathbf{a}(x) \cdot \mathbf{s}(x) + \mathbf{e}(x)$$

  evaluate to

$$\mathbf{b}(1) = \mathbf{a}(1) \cdot \mathbf{s}(1) + \mathbf{e}(1).$$

- For each guess for $\mathbf{s}(1) \in \mathbb{F}_p$, analyze distribution of $\mathbf{e}(1)$.

3. Evaluation-at-1 attack

Potential threat:

- Suppose $f(1) \equiv 0 \bmod p$, then

$$\frac{\mathbb{Z}[x]}{(p, f(x))} \to \mathbb{F}_p : \mathbf{r}(x) \mapsto \mathbf{r}(1) = r_0 + r_1 + \cdots + r_{n-1},$$

  is a well-defined ring homomorphism.
- Our ring-based LWE samples

$$\mathbf{b}(x) = \mathbf{a}(x) \cdot \mathbf{s}(x) + \mathbf{e}(x)$$

  evaluate to

$$\mathbf{b}(1) = \mathbf{a}(1) \cdot \mathbf{s}(1) + \mathbf{e}(1).$$

- For each guess for $\mathbf{s}(1) \in \mathbb{F}_p$, analyze distribution of $\mathbf{e}(1)$.
- Non-uniformity might reveal $\mathbf{s}(1)$, and maybe more ...

3. Evaluation-at-1 attack

Potential threat:

- Suppose $f(1) \equiv 0 \bmod p$, then

$$\frac{\mathbb{Z}[x]}{(p, f(x))} \to \mathbb{F}_p : \mathbf{r}(x) \mapsto \mathbf{r}(1) = r_0 + r_1 + \cdots + r_{n-1},$$

  is a well-defined ring homomorphism.

- Our ring-based LWE samples

$$\mathbf{b}(x) = \mathbf{a}(x) \cdot \mathbf{s}(x) + \mathbf{e}(x)$$

  evaluate to

$$\mathbf{b}(1) = \mathbf{a}(1) \cdot \mathbf{s}(1) + \mathbf{e}(1).$$

- For each guess for $\mathbf{s}(1) \in \mathbb{F}_p$, analyze distribution of $\mathbf{e}(1)$.
- Non-uniformity might reveal $\mathbf{s}(1)$, and maybe more ...

Safety measure: restrict to irreducible $f(x) \in \mathbb{Z}[x]$.

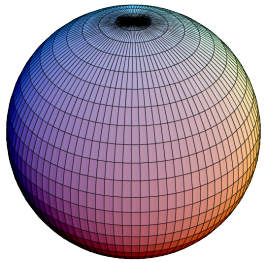
4. Ring-LWE

Direct ring-based analogue of LWE-sample would read

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

with the e_i sampled independently from

$$N(0, \sigma)$$



for some fixed small $\sigma = \sigma(n)$.

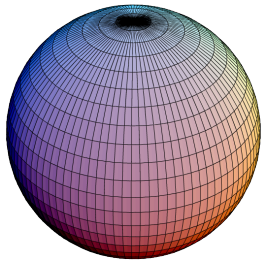
4. Ring-LWE

Direct ring-based analogue of LWE-sample would read

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

with the e_i sampled independently from

$$N(0, \sigma)$$



for some fixed small $\sigma = \sigma(n)$.

This is not Ring-LWE!

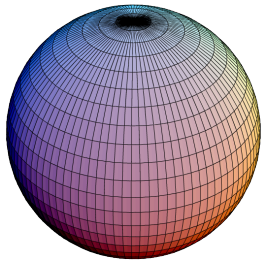
4. Ring-LWE

Direct ring-based analogue of LWE-sample would read

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

with the e_i sampled independently from

$$N(0, \sigma)$$



for some fixed small $\sigma = \sigma(n)$.

This is not Ring-LWE!

- Not backed up by hardness statement.
  - Evaluation-at-1 known to work in special cases [ELS].

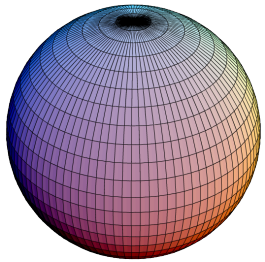
4. Ring-LWE

Direct ring-based analogue of LWE-sample would read

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

with the e_i sampled independently from

$$N(0, \sigma)$$



for some fixed small $\sigma = \sigma(n)$.

This is not Ring-LWE!

- Not backed up by hardness statement.
  - Evaluation-at-1 known to work in special cases [ELS].
- Sometimes called Poly-LWE.

4. Ring-LWE

So what is Ring-LWE according to [LPR]? Samples look like

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

4. Ring-LWE

So what is Ring-LWE according to [LPR]? Samples look like

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

where

- B is the canonical embedding matrix,
- $A_{f'(x)}$ compensates for the fact that one actually picks secrets from the dual.

4. Ring-LWE

So what is Ring-LWE according to [LPR]? Samples look like

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

where

- B is the canonical embedding matrix,
- $A_{f'(x)}$ compensates for the fact that one actually picks secrets from the dual.

Hardness reduction from ideal lattice problems.

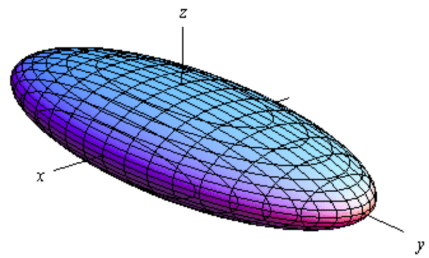
4. Ring-LWE

So what is Ring-LWE according to [LPR]? Samples look like

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

where

- B is the canonical embedding matrix,
- $A_{f'(x)}$ compensates for the fact that one actually picks secrets from the dual.



Hardness reduction from ideal lattice problems.

Note:

- factor $A_{f'(x)} \cdot B^{-1}$ might skew the error distribution,

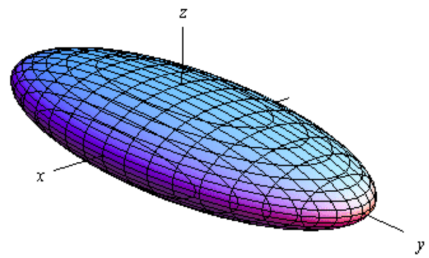
4. Ring-LWE

So what is Ring-LWE according to [LPR]? Samples look like

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

where

- B is the canonical embedding matrix,
- $A_{f'(x)}$ compensates for the fact that one actually picks secrets from the dual.



Hardness reduction from ideal lattice problems.

Note:

- factor $A_{f'(x)} \cdot B^{-1}$ might skew the error distribution,
- but also scales it!

4. Ring-LWE

. . . but also scales it!

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

Indeed, one has

- $\det A_{f'(x)} = \Delta$ with

$$\Delta = |\operatorname{disc} f(x)|, \qquad \leftarrow \text{could be huge}$$

4. Ring-LWE

. . . but also scales it!

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

Indeed, one has

- $\det A_{f'(x)} = \Delta$ with

$$\Delta = |\operatorname{disc} f(x)|, \qquad \leftarrow \text{could be huge}$$

- $\det B^{-1} = 1/\sqrt{\Delta}$.

4. Ring-LWE

. . . but also scales it!

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + A_{f'(x)} \cdot B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}$$

Indeed, one has

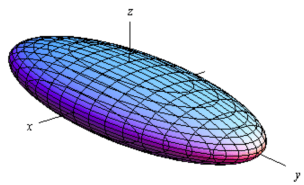
- $\det A_{f'(x)} = \Delta$ with

$$\Delta = |\operatorname{disc} f(x)|, \qquad \leftarrow \text{could be huge}$$

- $\det B^{-1} = 1/\sqrt{\Delta}$.

So "on average", each e_i is scaled up by $\sqrt{\Delta}^{1/n}$ . . .

- . . . but remember: skewness.



5. Provably weak instances of Ring-LWE revisited

[ELOS] constructed families of polynomials $f(x)$ that are vulnerable to an evaluation-at-1 attack.

For convenience they picked non-dual secrets:

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \cancel{A_{f'(x)}}\ B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}.$$

5. Provably weak instances of Ring-LWE revisited

[ELOS] constructed families of polynomials $f(x)$ that are vulnerable to an evaluation-at-1 attack.

For convenience they picked non-dual secrets:

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \cancel{A_{f'(x)}}\ B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}.$$

Recall:

- $\det B^{-1} = 1/\sqrt{\Delta}$, so the errors get squeezed.

5. Provably weak instances of Ring-LWE revisited

[ELOS] constructed families of polynomials $f(x)$ that are vulnerable to an evaluation-at-1 attack.

For convenience they picked non-dual secrets:

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \cancel{A_{f'(x)}}\ B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}.$$

Recall:

- $\det B^{-1} = 1/\sqrt{\Delta}$, so the errors get squeezed.
- To compensate, they scale up the errors by a factor $\sqrt{\Delta}^{1/n}$.

5. Provably weak instances of Ring-LWE revisited

[ELOS] constructed families of polynomials $f(x)$ that are vulnerable to an evaluation-at-1 attack.

For convenience they picked non-dual secrets:

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \sqrt{\Delta}^{1/n} B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}.$$

Recall:

- $\det B^{-1} = 1/\sqrt{\Delta}$, so the errors get squeezed.
- To compensate, they scale up the errors by a factor $\sqrt{\Delta}^{1/n}$.

5. Provably weak instances of Ring-LWE revisited

Issue:

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \sqrt{\Delta}^{1/n} B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}.$$

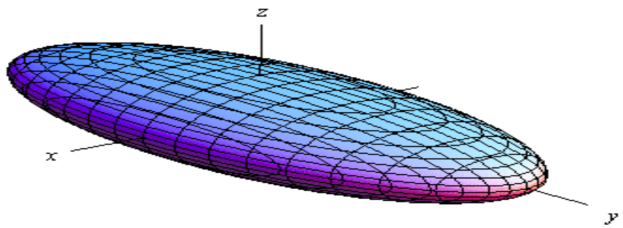
- The factor $\sqrt{\Delta}^{1/n}$ compensates for B^{-1} only “on average”.

5. Provably weak instances of Ring-LWE revisited

Issue:

$$\begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{pmatrix} = A_{\mathbf{a}} \cdot \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{pmatrix} + \sqrt{\Delta}^{1/n} B^{-1} \cdot \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{pmatrix}.$$

- The factor $\sqrt{\Delta}^{1/n}$ compensates for B^{-1} only "on average".
- In some coordinates B^{-1} could scale down much more.



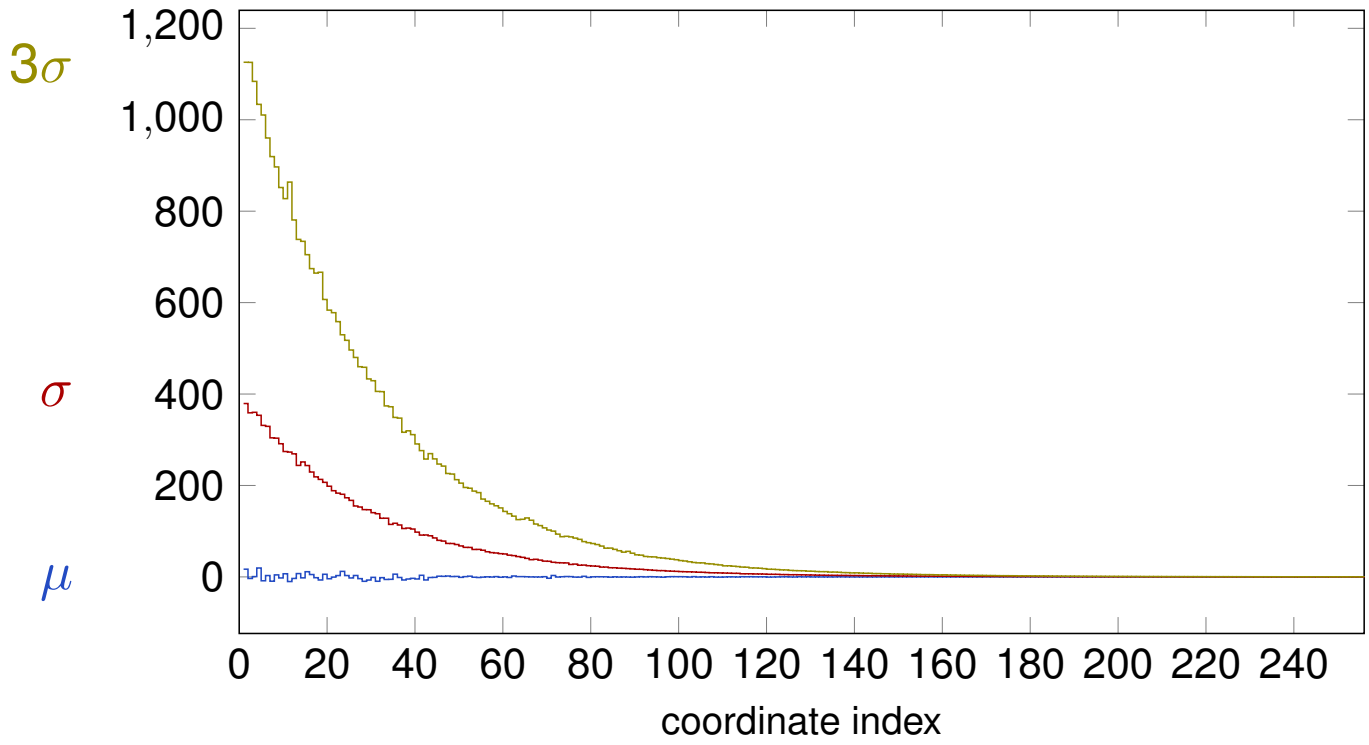
Compensation factor is insufficient

$\rightsquigarrow$ merely rounding yields exact equations in the secret!

5. Provably weak instances of Ring-LWE revisited

All instances from [ELOS] suffer from this skewness.

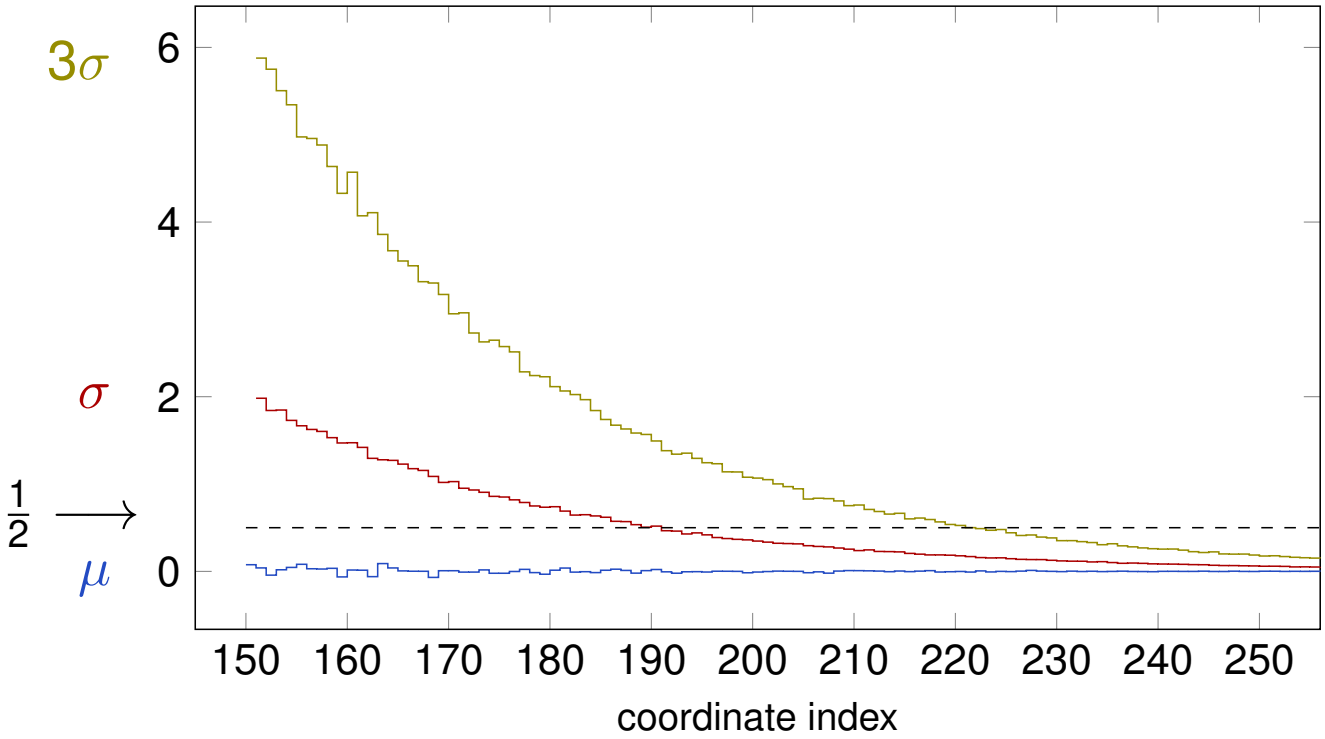
- Example: $f(x) = x^{256} + 8190$, $p = 8191$. ← note: $f(1) \equiv 0 \bmod p$
- Standard deviations even form a geometric series!
  Error distribution in each coordinate (experimental):



5. Provably weak instances of Ring-LWE revisited

All instances from [ELOS] suffer from this skewness.

- Example: $f(x) = x^{256} + 8190$, $p = 8191$. ← note: $f(1) \equiv 0 \bmod p$
- Standard deviations even form a geometric series!
  Error distribution in each coordinate (experimental):



5. Provably weak instances of Ring-LWE revisited

Evaluation-at-1 allowed [ELOS] to recover $\mathbf{s}(1)$,

- using about 20 samples with a success rate of 20%.

5. Provably weak instances of Ring-LWE revisited

Evaluation-at-1 allowed [ELOS] to recover $\mathbf{s}(1)$,

- using about 20 samples with a success rate of 20%.

But after rounding, the last $\approx n/7$ equations become exact,

- so 7 or 8 samples suffice to recover $\mathbf{s}(x)$ exactly.

5. Provably weak instances of Ring-LWE revisited

Evaluation-at-1 allowed [ELOS] to recover $\mathbf{s}(1)$,

- using about 20 samples with a success rate of 20%.

But after rounding, the last $\approx n/7$ equations become exact,

- so 7 or 8 samples suffice to recover $\mathbf{s}(x)$ exactly.

Similar remarks apply to the other instances from [ELOS].

5. Provably weak instances of Ring-LWE revisited

Concluding thoughts/remarks:

5. Provably weak instances of Ring-LWE revisited

Concluding thoughts/remarks:

- Currently, evaluation-at-1 is not a threat to Ring-LWE.

5. Provably weak instances of Ring-LWE revisited

Concluding thoughts/remarks:

- Currently, evaluation-at-1 is not a threat to Ring-LWE.
- Both B^{-1} and $A_{f'(x)} \cdot B^{-1}$ can be very skew, so mostly a matter of insufficient scaling, rather than dual vs. non-dual.

5. Provably weak instances of Ring-LWE revisited

Concluding thoughts/remarks:

- Currently, evaluation-at-1 is not a threat to Ring-LWE.
- Both B^{-1} and $A_{f'(x)} \cdot B^{-1}$ can be very skew, so mostly a matter of insufficient scaling, rather than dual vs. non-dual.
- To compensate for $A_{f'(x)}$ a factor $\Delta^{1/n}$ makes more sense. Does scaling this way lead to a provably hard problem?
  - Possible to construct for each $\varepsilon > 0$ a family of rings in which scaling by $\Delta^{(1-\varepsilon)/n}$ is insufficient.

5. Provably weak instances of Ring-LWE revisited

Concluding thoughts/remarks:

- Currently, evaluation-at-1 is not a threat to Ring-LWE.
- Both B^{-1} and $A_{f'(x)} \cdot B^{-1}$ can be very skew, so mostly a matter of insufficient scaling, rather than dual vs. non-dual.
- To compensate for $A_{f'(x)}$ a factor $\Delta^{1/n}$ makes more sense. Does scaling this way lead to a provably hard problem?
  - Possible to construct for each $\varepsilon > 0$ a family of rings in which scaling by $\Delta^{(1-\varepsilon)/n}$ is insufficient.
- If one does scale the [ELOS] examples sufficiently, then the error coordinates of low index become uniform.

5. Provably weak instances of Ring-LWE revisited

Concluding thoughts/remarks:

- Currently, evaluation-at-1 is not a threat to Ring-LWE.
- Both B^{-1} and $A_{f'(x)} \cdot B^{-1}$ can be very skew, so mostly a matter of insufficient scaling, rather than dual vs. non-dual.
- To compensate for $A_{f'(x)}$ a factor $\Delta^{1/n}$ makes more sense. Does scaling this way lead to a provably hard problem?
  - Possible to construct for each $\varepsilon > 0$ a family of rings in which scaling by $\Delta^{(1-\varepsilon)/n}$ is insufficient.
- If one does scale the [ELOS] examples sufficiently, then the error coordinates of low index become uniform.
- The cyclotomic case seems naturally protected against geometric growth.