# Module-LWE vs. Ring-LWE?

Amit Deo

Royal Holloway, University of London

15 January, 2018

# Main Aim of the Talk

1. Discuss popular variants of the LWE problem
2. Present a collection of reductions between the variants
3. Explicitly state parameter expansions in the reductions

# Outline

1. Definitions
2. Motivation for Ring/Module-LWE
3. Normal Form Secrets
4. “BLPRS13” Style Reductions
5. “Structure-Building” Reduction

# Section 1

## Definitions

# Notation

**Vectors** $\mathbf{x} \in \mathbb{Z}_q^n$:

- Entries integers modulo $q$, i.e. $\mathbb{Z}_q$
- Dimension $n$, i.e. $\mathbf{x} = (x_0, \ldots, x_{n-1})$

**Ring elements** $r \in R_q = \mathbb{Z}_q[X]/(X^n + 1)$:

- Coefficients integers modulo $q$
- Degree at most $n - 1$ i.e.
  $r = r_0 + r_1 \cdot X + \cdots + r_{n-1} \cdot X^{n-1} \in \mathbb{Z}_q[X]/(X^n + 1)$
- Coefficient Embedding $r = (r_0, \ldots, r_{n-1}) \in \mathbb{Z}_q^n$

# Notation

**Module elements $\mathbf{m} \in R_q^d$:**

- A $d$-tuple of ring elements $\mathbf{m} = (m_0, \ldots, m_{d-1})$
- Multiplication: $\mathbf{m} \cdot \mathbf{n} := m_0 n_0 + \cdots + m_{d-1} \cdot n_{d-1}$

**Terminology**:

- $q$ is a "modulus"
- $n$ is a "(ring) dimension"
- $d$ is a "module rank"
- $m$ is the number of samples

# Notation: Distributions

- $U(X)$ - uniform distribution over set X

# Notation: Distributions

- $U(X)$ - uniform distribution over set X
- $\chi_\sigma$ - *discrete* gaussian over the integers, s.d. $\sigma$
- $D_{\Lambda,\sigma}$ - *discrete* gaussian over lattice $\Lambda$, s.d. $\sigma$
- $D_{\Lambda,\mathbf{r}}$ - *discrete ellipsoidal* gaussian with s.d.'s $r_i \in \mathbb{R}$

# Notation: Distributions

- $U(X)$ - uniform distribution over set X
- $\chi_\sigma$ - *discrete* gaussian over the integers, s.d. $\sigma$
- $D_{\Lambda,\sigma}$ - *discrete* gaussian over lattice $\Lambda$, s.d. $\sigma$
- $D_{\Lambda,\mathbf{r}}$ - *discrete ellipsoidal* gaussian with s.d.'s $r_i \in \mathbb{R}$
- $D_\sigma$ - *continuous* gaussian over $\mathbb{R}$
- $D_{\mathbf{r}}$ - *continuous ellipsoidal* gaussian over $\mathbb{R}^n$ with s.d.'s $r_i$

# Generic LWE Problem Framework

Given some uniform random $a$, $b = a \cdot s + e$:

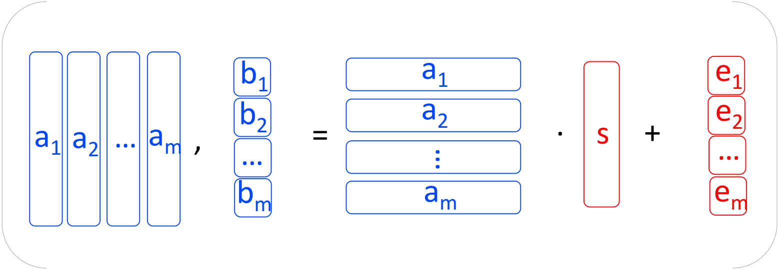
- **(search LWE)** decode the noisy product $b$ i.e. recover $s$ from $b$ for "small" $e$
- **(decision LWE)** distinguish $b$ from uniform random

# Generic LWE Problem Framework

Given some uniform random $a$, $b = a \cdot s + e$:

- **(search LWE)** decode the noisy product $b$ i.e. recover $s$ from $b$ for "small" $e$
- **(decision LWE)** distinguish $b$ from uniform random

Plain LWE sample: $a \leftarrow \mathbb{Z}_q^n$; $s \leftarrow U$ or $\chi_\sigma^n$, $e \leftarrow \chi_\sigma$; $b \in \mathbb{Z}_q$



# Distributions and Parameters

- Uniform $a$
- Error distribution: discrete gaussian $e \leftarrow \chi_\sigma$
- Secret distribution: uniform $s$ or $s \leftarrow \chi_\sigma^n$

Plain LWE sample: $a \leftarrow \mathbb{Z}_q^n$; $s \leftarrow \chi_\sigma^n, e \leftarrow \chi_\sigma; b \in \mathbb{Z}_q$

# Distributions and Parameters

- Uniform $a$
- Error distribution: discrete gaussian $e \leftarrow \chi_\sigma$
- Secret distribution: uniform $s$ or $s \leftarrow \chi_\sigma^n$

Plain LWE sample: $a \leftarrow \mathbb{Z}_q^n$; $s \leftarrow \chi_\sigma^n, e \leftarrow \chi_\sigma$; $b \in \mathbb{Z}_q$

- Absolute error $\sigma$
- Error rate $\alpha := \sigma / q$

# Practical Ring-LWE

Let $R_q = \mathbb{Z}_q[X]/(X^n + 1)$. Given some uniform random $a \in R_q$,

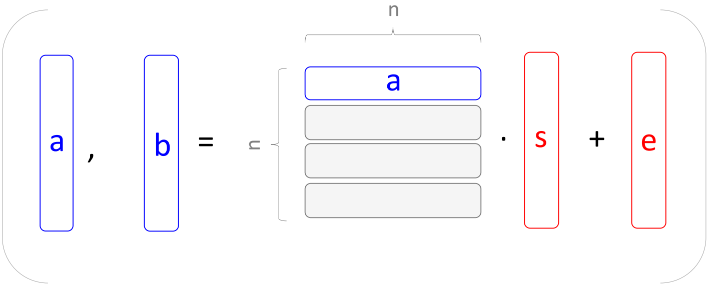
- **(search)** recover $s \in R_q$ from $b = a \cdot s + e$ for "small" $e \in R_q$
- **(decision)** decide whether $b = a \cdot s + e$ or $b$ is random

# Practical Ring-LWE

Let $R_q = \mathbb{Z}_q[X]/(X^n + 1)$. Given some uniform random $a \in R_q$,

- **(search)** recover $s \in R_q$ from $b = a \cdot s + e$ for "small" $e \in R_q$
- **(decision)** decide whether $b = a \cdot s + e$ or $b$ is random

Error distribution: $s, e \leftarrow \chi_\sigma^n$



# Almost Proper Ring-LWE

Given some uniform random $a \in R_q$,

- **(search)** recover $s \in (R_q)^d$ from $b = \frac{1}{q}\mathbf{a} \cdot \mathbf{s} + e \bmod 1$ for "small" $e \in R_q$
- **(decision)** decide whether $b = \frac{1}{q}\mathbf{a} \cdot \mathbf{s} + e \bmod 1$ or $b$ is random

**Notes:**

- The error distribution is now **continuous**
- The discrete Gaussian distribution $\chi_\sigma$ becomes continuous Gaussian $D_\alpha$ where $\alpha := \sigma/q$
- Ignoring canonical embedding and dual ring

# Practical Module-LWE

Given some uniform random $a \in (R_q)^d$,

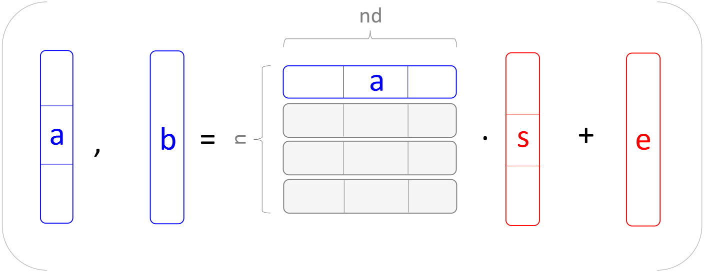
- **(search)** recover $s \in (R_q)^d$ from $b = \mathbf{a} \cdot \mathbf{s} + e$ for "small" $e \in R_q$
- **(decision)** decide whether $b = \mathbf{a} \cdot \mathbf{s} + e$ or $b$ is random

# Practical Module-LWE

Given some uniform random $a \in (R_q)^d$,

- **(search)** recover $s \in (R_q)^d$ from $b = \mathbf{a} \cdot \mathbf{s} + e$ for "small" $e \in R_q$
- **(decision)** decide whether $b = \mathbf{a} \cdot \mathbf{s} + e$ or $b$ is random

Error distribution: $\mathbf{s} \leftarrow \chi_\sigma^{nd}$, $e \leftarrow \chi_\sigma^{n}$



# Almost Proper Module-LWE

Given some uniform random $a \in (R_q)^d$,

- **(search)** recover $s \in (R_q)^d$ from $b = \frac{1}{q}\mathbf{a} \cdot \mathbf{s} + e \bmod 1$ for "small" $e \in R_q$
- **(decision)** decide whether $b = \frac{1}{q}\mathbf{a} \cdot \mathbf{s} + e \bmod 1$ or $b$ is random

**Notes:**

- The error distribution is now **continuous**
- The discrete Gaussian distribution $\chi_\sigma$ becomes continuous Gaussian $D_\alpha$ where $\alpha := \sigma/q$
- Once again, we ignore canonical embedding and dual ring

# Other Variants

- Learning with Rounding (LWR)
- Compact-LWE
- Binary-LWE
- And many more

# Section 2

## Motivation for Ring-LWE/Module-LWE

# Efficiency vs. Security

- Representing $n$ LWE samples:
  - $O(n)$ integers (Ring-LWE)
  - $O(nd)$ integers (Module-LWE)
  - $O(n^2)$ integers (LWE)

# Efficiency vs. Security

- Representing $n$ LWE samples:
  - $O(n)$ integers (Ring-LWE)
  - $O(nd)$ integers (Module-LWE)
  - $O(n^2)$ integers (LWE)
- Lattice hardness:
  - Ideal lattices SIVP (Ring-LWE)
  - Module lattices SIVP (Module-LWE)
  - General lattices SIVP (LWE)

# Flexibility of Module-LWE

- $R = \mathbb{Z}_q[X]/(X^n + 1)$ for power-of-two $n$
- Effective Ring-LWE dimensions: $256, 512, 1024, 2048, \ldots$
- Effective Module-LWE dimensions: $256 \cdot d$, $d = 1, 2, \ldots$

Note:
The cost of multiplying using Module-LWE is larger than the cost of multiplying for Ring-LWE of the same effective dimension.

## Section 3

# Transforming Secret Distributions

# Normal Form LWE

**Lemma**

*Let $q$ be prime. Given $m > n$ uniform secret LWE samples $(A, b) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$, we can produce $m - n$ normal form LWE samples $(A', b') \in \mathbb{Z}_q^{n \times (m-n)} \times \mathbb{Z}_q^{(m-n)}$ (with significant probability $1 - O(1/q)$).*

# Normal Form LWE

### Lemma

*Let $q$ be prime. Given $m > n$ uniform secret LWE samples $(A, b) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$, we can produce $m - n$ normal form LWE samples $(A', b') \in \mathbb{Z}_q^{n\times(m-n)} \times \mathbb{Z}_q^{(m-n)}$ (with significant probability $1 - O(1/q)$).*

### Proof.

1. Write $A = [A_1|A_2]$ where $A_1 \in \mathbb{Z}_q^{n\times n}$ is invertible.
2. $b = [b_1|b_2]^T := [A_1|A_2]^T s + [e_1|e_2]^T$
3. Set $A' := -A_1^{-1}A_2$, $b' := A'^T b_1 + b_2 = A' e_1 + e_2$.

$\square$

# Non-Uniform Secret $\longrightarrow$ Uniform Secret

**Lemma**

*Given a LWE sample $(a, b)$ with non-uniform secret $s$, we can obtain a LWE sample $(a, \tilde{b})$ with a uniform secret $\tilde{s}$.*

**Proof.**

1. Sample $s' \leftarrow U$.
2. Output LWE sample
$$\left(a, \tilde{b} := b + a \cdot s' = a \cdot (s' + s) + e\right) = (a, a \cdot (s' + s) + e).$$

$\square$

Section 4

# BLPRS13 Style Reductions

# Modulus-Dimension Switching LWE Reduction [1]

## Lemma

*There exists a reduction from*
$\mathrm{LWE}_{m,n,q,D_\alpha} \longrightarrow \mathrm{LWE}_{m,n'=n/k,q'=q^k,D_\beta}$ *where* $\beta = \mathcal{O}(\alpha\sqrt{n})$.

"We can reduce the dimension at the cost of increasing the modulus while changing the error rate by a $\sqrt{n}$ factor without decreasing hardness."

[1] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, D. Stéhle. *Classical hardness of learning with errors.* STOC13

# Reduction Intuition

## Goal

Find a reduction (i.e. transformation $\mathcal{F}$) such that the original LWE distribution *almost* maps to the target LWE distribution where the effect that $\mathcal{F}$ has on the secret is reversible.

$$\mathcal{F}(\text{LWE}) \sim_{\text{indist.}} \text{LWE}'$$

$$\mathbf{a} \in \mathbb{Z}_q^n \quad \xrightarrow{\mathcal{F}} \quad \mathbf{a}' \in \mathbb{Z}_{q^k}^{n/k}$$

$$\mathbf{s} \in \mathbb{Z}_q^n \quad \xrightarrow{\mathcal{F}} \quad \mathbf{s}' \in \mathbb{Z}_{q^k}^{n/k}$$

$$b = \left(\frac{1}{q}\mathbf{a} \cdot \mathbf{s} + e\right) \bmod 1 \quad \xrightarrow{\mathcal{F}} \quad b' = \left(\frac{1}{q^k}\mathbf{a}' \cdot \mathbf{s}' + e'\right) \bmod 1$$

# Reduction Intuition $n = 3, n/k = 1$

$$a' = a_0 + qa_1 + q^2 a_2$$
$$s' = s_2 + qs_1 + q^2 s_0$$

# Reduction Intuition $n = 3, n/k = 1$

$$a' = a_0 + qa_1 + q^2 a_2$$
$$s' = s_2 + qs_1 + q^2 s_0$$

$$\implies \frac{1}{q^3} a' \cdot s' \equiv 0 + \frac{1}{q}\mathbf{a} \cdot \mathbf{s} + \frac{1}{q^2}(a_0 \cdot s_1 + a_1 \cdot s_2) + \ldots \bmod 1$$
$$\approx \frac{1}{q}\mathbf{a} \cdot \mathbf{s} \bmod 1$$

# Reduction Intuition $n = 3, n/k = 1$

$$a' = a_0 + qa_1 + q^2 a_2$$
$$s' = s_2 + qs_1 + q^2 s_0$$

$$\implies \frac{1}{q^3} a' \cdot s' \equiv 0 + \frac{1}{q} \mathbf{a} \cdot \mathbf{s} + \frac{1}{q^2}(a_0 \cdot s_1 + a_1 \cdot s_2) + \ldots \bmod 1$$
$$\approx \frac{1}{q} \mathbf{a} \cdot \mathbf{s} \bmod 1$$

Therefore take $b' = b$

# A Closer Look at the Error Distribution

Want to analyse the distribution of:

$$b' - \frac{1}{q^n} a' \cdot s' = e - \sum_{i>j} q^{j-i-1} a_j s_i$$

Problem:

- $q^{j-i-1} a_j s_i$ are *not* continuous gaussians ✗

# INTERLUDE: Fixing a "Bad" Error Distribution - Discrete Version

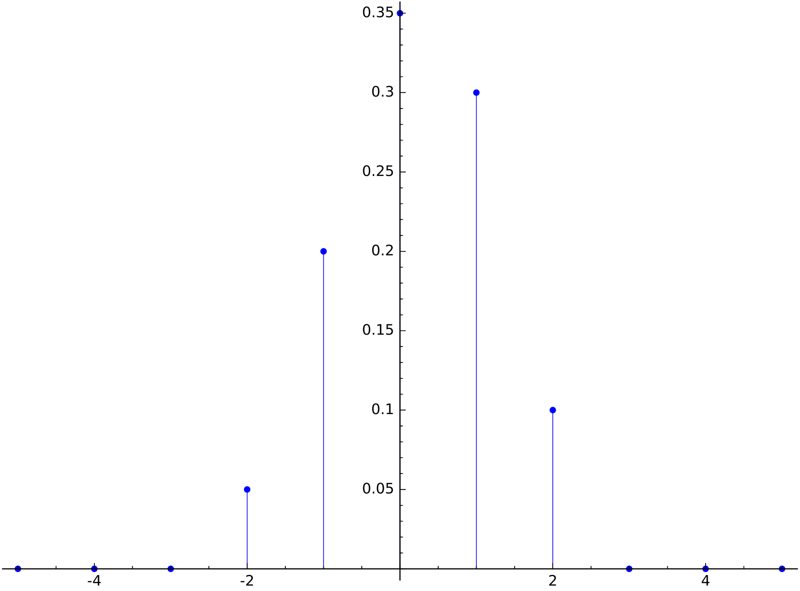
## Aim

Given bad non-Gaussian distribution $\hat{e}$, make it look like a discrete Gaussian.

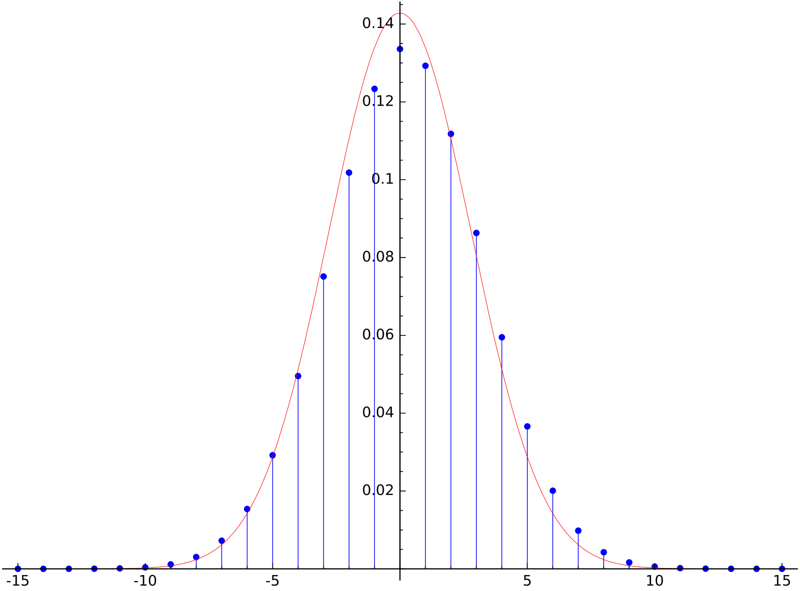
## How?

Drown by adding a wide discrete Gaussian i.e. consider $\hat{e} + \chi_\sigma$

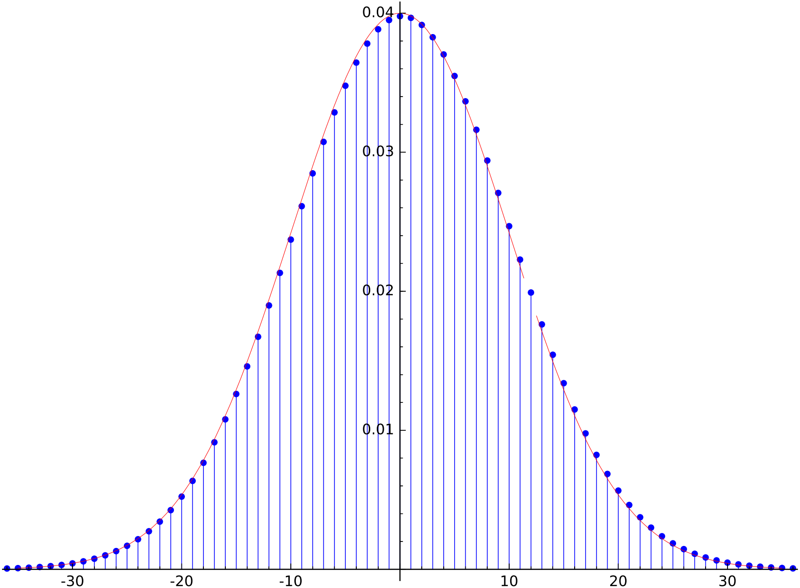
# Fixing a "Bad" Error Distribution - Discrete Version



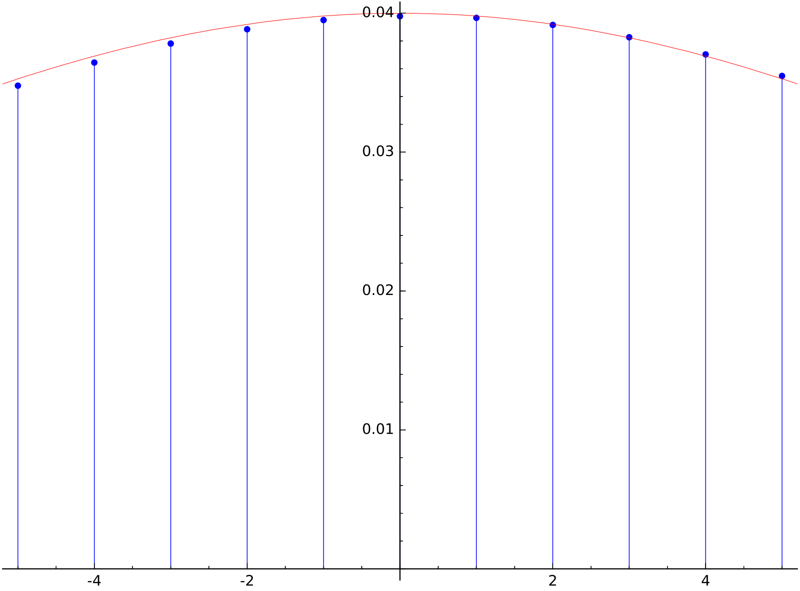
# Drowning ($\sigma = 3$)



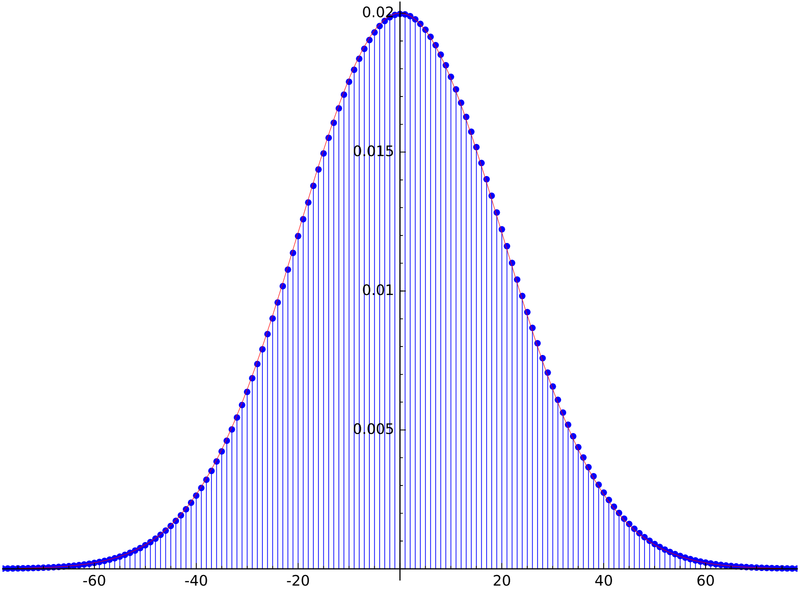
# Drowning ($\sigma = 10$)



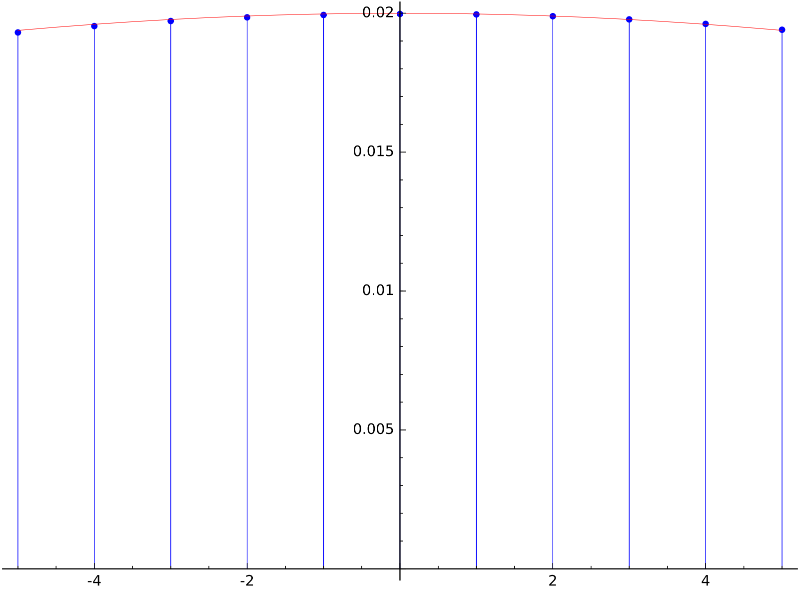
# Drowning ($\sigma = 10$)



# Drowning ($\sigma = 20$)



# Drowning ($\sigma = 20$)



# Drowning Lemma

### Lemma

[2] *Assuming* $(1/r^2 + (||\mathbf{z}||/\alpha)^2)^{-1/2} > \eta_\epsilon(\Lambda)$*, the arising distributions of the following are within statistical distance* $4\epsilon$*:*

1. *Sample* $\mathbf{v} \leftarrow D_{\Lambda+\mathbf{u},r}, e \leftarrow D_\alpha$*, output* $\langle \mathbf{z}, \mathbf{v} \rangle + e$*.*
2. *Let* $\beta = \sqrt{(r||\mathbf{z}||)^2 + \alpha^2}$*, output* $e' \leftarrow D_\beta$*.*

[2] O. Regev. *On lattices, learning with errors, random linear codes, and cryptography*. STOC 2005

# Drowning Lemma

**Lemma**

[2] *Assuming* $(1/r^2 + (||\mathbf{z}||/\alpha)^2)^{-1/2} > \eta_\epsilon(\Lambda)$*, the arising distributions of the following are within statistical distance* $4\epsilon$*:*

1. *Sample* $\mathbf{v} \leftarrow D_{\Lambda+\mathbf{u},r}, e \leftarrow D_\alpha$*, output* $\langle \mathbf{z}, \mathbf{v} \rangle + e$*.*
2. *Let* $\beta = \sqrt{(r||\mathbf{z}||)^2 + \alpha^2}$*, output* $e' \leftarrow D_\beta$*.*

**Notes**:

- Fix $r$, $\mathbf{z}$, $\Lambda \rightarrow$ minimum drowning parameter $\alpha(\epsilon)$.
- $\eta_\epsilon(\Lambda) \leq ||\tilde{\mathbf{B}}|| \cdot \sqrt{\ln(2n(1+1/\epsilon))/\pi}$

[2] O. Regev. *On lattices, learning with errors, random linear codes, and cryptography*. STOC 2005

# "General" Reduction from BLPRS13 ($n' = n/k$)

Define:

- $\mathbf{G} := \mathbf{I}_{n'} \otimes \mathbf{g}$ where $\mathbf{g} := (1, q, \ldots, q^{k-1})^T$ and
- $\Lambda := q^{-k}\mathbf{G}^T\mathbb{Z}^{n'} + \mathbb{Z}^n$
- Let $(\mathbf{a}, b = \frac{1}{q}\mathbf{a} \cdot \mathbf{s} + e) \in \mathbb{Z}_q^n \times \mathbb{T}$ be LWE sample.

[3] efficient sampling possible for $\epsilon \leq 1/4$

# “General” Reduction from BLPRS13 ($n' = n/k$)

Define:

- $\mathbf{G} := \mathbf{I}_{n'} \otimes \mathbf{g}$ where $\mathbf{g} := (1, q, \ldots, q^{k-1})^T$ and
- $\Lambda := q^{-k}\mathbf{G}^T\mathbb{Z}^{n'} + \mathbb{Z}^n$
- Let $(\mathbf{a}, b = \frac{1}{q}\mathbf{a} \cdot \mathbf{s} + e) \in \mathbb{Z}_q^n \times \mathbb{T}$ be LWE sample.

Reduction:

1. Sample $\mathbf{f} \leftarrow D_{\Lambda - \mathbf{a}, r}$ where $r \geq ||\tilde{\mathbf{B}}|| \cdot \sqrt{\ln(2n(1+1/\epsilon))/\pi} \geq \eta_\epsilon(\Lambda)$, [3] and choose $\mathbf{a}'$ as a uniform random solution to $\mathbf{G}^T\mathbf{a}' = \mathbf{a} + \mathbf{f} \mod \mathbb{Z}^n$.
2. Sample $e' \leftarrow D_{rB}$ where $B \geq ||\mathbf{s}||$ and output $b' = b + e'$.
3. Output $(\mathbf{a}', b')$.

[3] efficient sampling possible for $\epsilon \leq 1/4$

# Correctness of the Reduction

Proof.

- $\mathbf{a}'$ is uniform: $\mathbf{a} + \mathbf{f} \in \Lambda/\mathbb{Z}^n$ is uniform random for $r \geq \eta_\epsilon(\Lambda)$ and $\mathbf{G}^T\mathbf{a}' = \mathbf{v} \bmod \mathbb{Z}^n$ has the same number of solutions for every $\mathbf{v}$.
- Error distribution: Let $\mathbf{s}' := \mathbf{G}^T\mathbf{s}$. Then

$$b' - \frac{1}{q^k}\mathbf{a}' \cdot \mathbf{s}' = \langle -\mathbf{f}, \mathbf{s} \rangle + e' + e \bmod 1$$

is statistically close to a Gaussian by the drowning lemma if $r$ is big enough.

$\square$

# Recap of Result (Modulus-Dimension Switching)

**Lemma**

*There exists a reduction from*
$\mathsf{LWE}_{m,n,q,D_\alpha} \longrightarrow \mathsf{LWE}_{m,n'=n/k,q'=q^k,D_\beta}$ *where* $\beta = \mathcal{O}(\alpha\sqrt{n})$.

# Module-LWE $\longrightarrow$ Ring-LWE

### Idea

Treat module elements as vectors of ring elements and apply BLPRS13 ($R^d \leftrightarrow \mathbb{Z}^n, R \leftrightarrow \mathbb{Z}$).

# Reducing (Search) Module-LWE to Ring-LWE

## Goal

Find a reduction (i.e. transformation $\mathcal{F}$) such that the MLWE distribution *almost* maps to a RLWE distribution where the effect that $\mathcal{F}$ has on the secret is reversible.

$$\mathbf{a} \in R_q^d \quad \xrightarrow{\mathcal{F}} \quad a' \in R_{q^d}$$

$$\mathbf{s} \in R_q^d \quad \xrightarrow{\mathcal{F}} \quad s' \in R_{q^d}$$

$$b = \left(\frac{1}{q}\mathbf{a} \cdot \mathbf{s} + e\right) \bmod 1 \quad \xrightarrow{\mathcal{F}} \quad b' = \left(\frac{1}{q^d} a' \cdot s' + e'\right) \bmod 1$$

# Reduction Intuition $d = 3$

$$a' = a_0(X) + qa_1(X) + q^2 a_2(X)$$
$$s' = s_2(X) + qs_1(X) + q^2 s_0(X)$$

# Reduction Intuition $d = 3$

$$a' = a_0(X) + qa_1(X) + q^2 a_2(X)$$
$$s' = s_2(X) + qs_1(X) + q^2 s_0(X)$$

$$\implies \frac{1}{q^3} a' \cdot s' \equiv 0 + \frac{1}{q}\mathbf{a} \cdot \mathbf{s} + \frac{1}{q^2}(a_0 \cdot s_1 + a_1 \cdot s_2) + \ldots \bmod 1$$
$$\approx \frac{1}{q}\mathbf{a} \cdot \mathbf{s} \bmod 1$$

# Reduction Intuition $d = 3$

$$a' = a_0(X) + qa_1(X) + q^2 a_2(X)$$
$$s' = s_2(X) + qs_1(X) + q^2 s_0(X)$$

$$\implies \frac{1}{q^3} a' \cdot s' \equiv 0 + \frac{1}{q}\mathbf{a} \cdot \mathbf{s} + \frac{1}{q^2}(a_0 \cdot s_1 + a_1 \cdot s_2) + \ldots \bmod 1$$
$$\approx \frac{1}{q}\mathbf{a} \cdot \mathbf{s} \bmod 1$$

Therefore take $b' = b$

# A Closer Look at the Error Distribution

Want to analyse the distribution of:

$$b' - \frac{1}{q^d} a' \cdot s' = e - \sum_{i>j} q^{j-i-1} a_j s_i$$

- $e$ is a continuous, narrow Gaussian ✓
- The sum is kind of small ✓

# A Closer Look at the Error Distribution

Want to analyse the distribution of:

$$\tilde{b} - \frac{1}{q^d}\tilde{a} \cdot \tilde{s} = e - \sum_{i>j} q^{j-i-1} a_j s_i$$

Problems:

1. $q^{j-i-1} a_j s_i$ are *not* continuous gaussians ✗
2. Coefficients are *not* independent ✗ (partial solution: canonical embedding)

# INTERLUDE: Rényi Divergence

## Definition

(Rényi Divergence) For any distributions $P$ and $Q$ such that $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$, the Rényi divergence of $P$ and $Q$ of order $a \in [1, \infty]$ is given by

$$R_a\left(P||Q\right) = \begin{cases} \exp\left(\sum_{x \in \mathrm{Supp}(P)} P(x) \log \frac{P(x)}{Q(x)}\right) & \text{for } a = 1, \\ \left(\sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}}\right)^{\frac{1}{a-1}} & \text{for } a \in (1, \infty), \\ \max_{x \in \mathrm{Supp}(P)} \frac{P(x)}{Q(x)} & \text{for } a = \infty. \end{cases}$$

# Properties of Rényi Divergence

Let $P$ and $Q$ be distributions such that $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$. Then we have:

- **Probability Preservation:**

$$\Pr(\mathrm{Success}_Q) \geq \Pr(\mathrm{Success}_P)^{\frac{a}{a-1}} / R_a(P||Q) \ \text{ if } a \in (1, \infty)$$

# Properties of Rényi Divergence

Let $P$ and $Q$ be distributions such that $\mathrm{Supp}(P) \subseteq \mathrm{Supp}(Q)$.
Then we have:

- **Probability Preservation:**

$$\Pr(\mathrm{Success}_Q) \geq \Pr(\mathrm{Success}_P)^{\frac{a}{a-1}} / R_a(P||Q) \ \text{ if } a \in (1, \infty)$$

- **Weak Triangle Inequality:** For intermediate distribution $P_1$,

$$R_a(P||Q) \leq R_\infty(P||P_1)^{\frac{a}{a-1}} \cdot R_a(P_1||Q) \ \text{ if } a \in (1, +\infty).$$

# Drowning Lemma over $n$-dimensions

Lemma (Drowning ellipsoidal discrete Gaussians [4])

*Assume that* $\min_i \frac{r_i \sigma}{\sqrt{r_i^2+\sigma^2}} \geq \eta_\epsilon(\Lambda)$ *for some* $\epsilon \in (0, 1/2)$*. Consider the continuous distributions:*

- $Y$ *obtained by sampling from* $D_{\Lambda+\mathbf{u},\mathbf{r}}$ *and then adding a vector from* $D_\sigma$
- $D_{\mathbf{t}}$ *where* $t_i = \sqrt{r_i^2 + \sigma^2}$

*Then we have* $\Delta(Y, D_{\mathbf{t}}) \leq 4\epsilon$ *and* $R_\infty(D_{\mathbf{t}} || Y) \leq \frac{1+\epsilon}{1-\epsilon}$.

[4] A. Langlois, D. Stéhle. *Worst-case to average-case reductions for module lattices*. DCC15

# Drowning Lemma over $n$-dimensions

Lemma (Drowning ellipsoidal discrete Gaussians [4])

*Assume that* $\min_i \frac{r_i \sigma}{\sqrt{r_i^2+\sigma^2}} \geq \eta_\epsilon(\Lambda)$ *for some* $\epsilon \in (0, 1/2)$. *Consider the continuous distributions:*

- $Y$ *obtained by sampling from* $D_{\Lambda+\mathbf{u},\mathbf{r}}$ *and then adding a vector from* $D_\sigma$
- $D_{\mathbf{t}}$ *where* $t_i = \sqrt{r_i^2 + \sigma^2}$

*Then we have* $\Delta(Y, D_{\mathbf{t}}) \leq 4\epsilon$ *and* $R_\infty(D_{\mathbf{t}} || Y) \leq \frac{1+\epsilon}{1-\epsilon}$.

**Notes**:

- Fix $\mathbf{r}$, $\Lambda \rightarrow$ minimum drowning parameter $\sigma(\epsilon)$.
- $\eta_\epsilon(\Lambda) \leq ||\tilde{\mathbf{B}}|| \cdot \sqrt{\ln(2n(1+1/\epsilon))/\pi}$

[4] A. Langlois, D. Stéhle. *Worst-case to average-case reductions for module lattices*. DCC15

# "General" Reduction $\text{MLWE}_d \to \text{MLWE}_{d'}$ $(d' = d/k)$

Define:

- $\mathbf{G} := \mathbf{I}_{d'} \otimes \mathbf{g} \otimes \mathbf{I}_n$ where $\mathbf{g} := (1, q, \ldots, q^{k-1})^T$ and
- $\Lambda := q^{-k}\mathbf{G}^T\mathbb{Z}^{nd'} + \mathbb{Z}^{nd}$
- Let $(\mathbf{a}, b = \frac{1}{q}\mathbf{a} \cdot \mathbf{s} + e) \in \mathbb{Z}_q^{nd} \times \mathbb{T}^n$ be the MLWE sample.

[5] efficient sampling possible for $\epsilon \leq 1/4$

# "General" Reduction $\mathsf{MLWE}_d \to \mathsf{MLWE}_{d'}$ $(d' = d/k)$

Define:

- $\mathbf{G} := \mathbf{I}_{d'} \otimes \mathbf{g} \otimes \mathbf{I}_n$ where $\mathbf{g} := (1, q, \ldots, q^{k-1})^T$ and
- $\Lambda := q^{-k}\mathbf{G}^T\mathbb{Z}^{nd'} + \mathbb{Z}^{nd}$
- Let $(\mathbf{a}, b = \frac{1}{q}\mathbf{a} \cdot \mathbf{s} + e) \in \mathbb{Z}_q^{nd} \times \mathbb{T}^n$ be the MLWE sample.

Reduction:

1. Sample $\mathbf{f} \leftarrow D_{\Lambda - \mathbf{a}, r}$ where $r \geq ||\tilde{\mathbf{B}}|| \cdot \sqrt{\ln(2n(1+1/\epsilon))/\pi} \geq \eta_\epsilon(\Lambda)$, [5] and choose $\mathbf{a}'$ as a uniform random solution to $\mathbf{G}^T\mathbf{a}' = \mathbf{a} + \mathbf{f} \mod \mathbb{Z}^{nd}$.
2. Sample $\mathbf{e}'_i \leftarrow (D_{rB})^n, i = 1 \ldots d$ where $B \geq ||\mathbf{s}||$ and output $b' = b + \sum \mathbf{e}'_i$.
3. Output $(\mathbf{a}', b')$.

[5] efficient sampling possible for $\epsilon \leq 1/4$

# Correctness of the Reduction (Overview)

- $\mathbf{a}'$ is uniform: $\mathbf{v} = \mathbf{a} + \mathbf{f} \in \Lambda/\mathbb{Z}^{nd}$ is uniform random for $r \geq \eta_\epsilon(\Lambda)$ and $\mathbf{G}^T\mathbf{a}' = \mathbf{v} \bmod \mathbb{Z}^{nd}$ has the same number of solutions for every $\mathbf{v}$

# Correctness of the Reduction (Overview)

Error distribution: Let $\mathbf{s}' := \mathbf{G}^T\mathbf{s}$. Then

$$b' - \frac{1}{q^k}\mathbf{a}' \cdot \mathbf{s}' = \sum_{i=1}^{d} \mathbf{S}_i \cdot (-\mathbf{f}_i) + \mathbf{e}'_i + \mathbf{e} \bmod 1$$

# Correctness of the Reduction (Overview)

Error distribution: Let $\mathbf{s}' := \mathbf{G}^T\mathbf{s}$. Then

$$b' - \frac{1}{q^k}\mathbf{a}' \cdot \mathbf{s}' = \sum_{i=1}^{d} \mathbf{S}_i \cdot (-\mathbf{f}_i) + \mathbf{e}'_i + \mathbf{e} \bmod 1$$

- $\mathbf{S}_i$ is the matrix version of $s_i \in R$
- $\mathbf{f}_i \leftarrow D_{\frac{1}{q}\mathbb{Z}^n + \mathbf{v}_i, r}$
- $\mathbf{S}_i \cdot (\mathbf{f}_i) \leftarrow D_{\frac{1}{q}\mathbf{S}_i\mathbb{Z}^n + \mathbf{S}_i\mathbf{v}_i, r'\mathbf{S}_i^T}$

Apply drowning lemma $d$ times. $\square$

# Recap of Result

**Lemma**

*There exists a reduction from*
$\mathsf{MLWE}_{m,d,q,D_\alpha} \longrightarrow \mathsf{MLWE}_{m,d'=d/k,q'=q^k,D_{\leq\beta}}$ *where*
$\beta = \mathcal{O}(\alpha n^2\sqrt{d})$ *preserving non-negligible success probability.*

# Recap of Result

**Lemma**

*There exists a reduction from*
$\mathsf{MLWE}_{m,d,q,D_\alpha} \longrightarrow \mathsf{MLWE}_{m,d'=d/k,q'=q^k,D_{\leq\beta}}$ *where*
$\beta = \mathcal{O}(\alpha n^2 \sqrt{d})$ *preserving non-negligible success probability.*

**Or for perfectly spherical gaussian errors:**

**Lemma**

*There exists a reduction from*
$\mathsf{MLWE}_{m,d,q,D_\alpha} \longrightarrow \mathsf{LWE}_{m,d'=d/k,q'=q^k,D_\beta}$ *where* $\beta = \mathcal{O}(\alpha n^{9/4} \sqrt{d})$.

# Ring-LWE $(n, q) \rightarrow$ Ring-LWE $(n/2, q^2)$

**Lemma**

*There is a reduction* $RLWE_{m,n,q,\alpha} \longrightarrow RLWE_{m,n/2,q^2,\beta}$ *where* $\beta = \mathcal{O}(n^{9/4} \cdot \alpha)$.

# Ring-LWE $(n, q) \to$ Ring-LWE $(n/2, q^2)$

**Lemma**

*There is a reduction* $RLWE_{m,n,q,\alpha} \longrightarrow RLWE_{m,n/2,q^2,\beta}$ *where* $\beta = \mathcal{O}(n^{9/4} \cdot \alpha)$.

*Remark.*

Can go from $n$ to 2 dimensions by incurring an extra factor of $n$.

# Section 5

## Structure Building Reductions

# Many LWE Samples $\rightarrow$ One Ring-LWE Sample

Aim to show:[6]

$$\mathsf{LWE}_{m=n,d,q,D_\alpha} \quad \longrightarrow \quad \mathsf{RLWE}_{m=1,n,q^d,D_{\alpha\sqrt{d}}} \tag{1}$$

[6] $d$ is the LWE dimension, $n$ is the ring dimension

# Many LWE Samples $\rightarrow$ One Ring-LWE Sample

Aim to show:[6]

$$\mathrm{LWE}_{m=n,d,q,D_\alpha} \quad \longrightarrow \quad \mathrm{RLWE}_{m=1,n,q^d,D_{\alpha\sqrt{d}}} \qquad (1)$$

Main Idea:

- Apply the BLPRS13 reduction (modulus-dimension trade-off) to obtain 1-dimensional LWE samples
- Build Ring-LWE samples from these

[6] $d$ is the LWE dimension, $n$ is the ring dimension

# Step 1: Apply BLPRS13 Reduction

Apply BLPRS13 reduction: $\mathsf{LWE}_{m=n,d,q,D_\alpha} \longrightarrow \mathsf{LWE}_{m=n,1,q^d,D_{\alpha\sqrt{d}}}$

# Step 1: Apply BLPRS13 Reduction

Apply BLPRS13 reduction: $\mathsf{LWE}_{m=n,d,q,D_\alpha} \longrightarrow \mathsf{LWE}_{m=n,1,q^d,D_{\alpha\sqrt{d}}}$

Denote the 1-dimensional samples as

$$\left(a_i, b_i = \frac{1}{q^d} \cdot a_i s_0 + e_i\right) \in \mathbb{Z}_{q^d} \times \mathbb{T} \text{ for } i = 0, \ldots, n-1$$

# Step 2: Build the Ring Structure

(a) Define Ring-LWE secret $s := s_0 \in R_q$

(b) Define uniform ring element $a' := a_0 + \cdots + a_{n-1} \cdot X^{n-1} \in R_q$

(c) Set $b' = \sum_{i=0}^{n-1} b_i \cdot X^i \in R_q$

# Correctness of the Reduction

- Ring-LWE secret $s$ distribution "irrelevant"
- Ring element $a$ is uniformly distributed
- $b' - \frac{1}{q^d} a \cdot s = \sum_{i=0}^{n-1} e_i \cdot X^i$ distributed as $D_{\alpha\sqrt{d}}$

## Lemma

*The ability to solve Ring-LWE in modulus $q^d$ and ring dimension $n$ imples the ability to solve LWE given $n$ sample in dimension $d$ and modulus $q$.*

# Conclusions: Module-LWE vs. Ring-LWE

- There are numerous reductions between the LWE variants
- We can retain:
  1. "LWE hardness" even in dimension 1
  2. "Module-LWE hardness" using Ring-LWE
  3. "Ring-LWE hardness" when decreasing dimension
  4. "LWE hardness" using Ring-LWE
- However, note that we need an modulus that is exponential in the module rank or (ring) dimension as well as an expansion in the error rate

# Thank You!


Martin R. Albrecht and Amit Deo.
Large modulus ring-lwe $>=$ module-lwe.
Cryptology ePrint Archive, Report 2017/612, 2017.
http://eprint.iacr.org/2017/612.

Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé.
Classical hardness of learning with errors.
In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 575–584. ACM, 2013.