Error Correction and Ciphertext Quantization in Lattice-based Cryptography

Daniele Micciancio and Mark Schultz

University of California San Diego

23 August 2023

Contents

Quantum Cryptanalysis

A Short History of BQP Factoring Algorithms

Year	Event
1994	Shor's Algorithm Published

Quantum Cryptanalysis

A Short History of BQP Factoring Algorithms

Year	Event
1994	Shor's Algorithm Published
2002	$15 =$

Quantum Cryptanalysis

A Short History of BQP Factoring Algorithms

Year	Event
1994	Shor's Algorithm Published
2002	$15 = 5 \times 3$ Factored!
2012	$21 =$

Quantum Cryptanalysis

A Short History of BQP Factoring Algorithms

Year	Event
1994	Shor's Algorithm Published
2002	$15 = 5 \times 3$ Factored!
2012	$21 = 7 \times 3$ Factored!

Quantum Cryptanalysis

A Short History of BQP Factoring Algorithms

Year	Event
1994	Shor's Algorithm Published
2002	$15 = 5 \times 3$ Factored!
2012	$21 = 7 \times 3$ Factored!
2019	$35 =$

Quantum Cryptanalysis

A Short History of BQP Factoring Algorithms

Year	Event
1994	Shor's Algorithm Published
2002	$15 = 5 \times 3$ Factored!
2012	$21 = 7 \times 3$ Factored!
2019	$35 = ???$ Failed

Quantum Cryptanalysis

A Short History of BQP Factoring Algorithms

Year	Event
1994	Shor's Algorithm Published
2002	$15 = 5 \times 3$ Factored!
2012	$21 = 7 \times 3$ Factored!
2019	$35 = ???$ Failed

2022: 48-bit numbers Factored

Quantum Cryptanalysis

A Short History of BQP Factoring Algorithms

Year	Event
1994	Shor's Algorithm Published
2002	$15 = 5 \times 3$ Factored!
2012	$21 = 7 \times 3$ Factored!
2019	$35 = ???$ Failed

2022: 48-bit numbers Factored using non-Shor algorithms

Serious Motivation

1. Large Public Funding of Quantum Computing:
   - Europe: $7 billion
   - US: $2 billion
   - China: $15 billion

Serious Motivation

1. Large Public Funding of Quantum Computing:
   - Europe: $7 billion
   - US: $2 billion
   - China: $15 billion
2. Store and Decrypt attack

Serious Motivation

1. Large Public Funding of Quantum Computing:
   - Europe: $7 billion
   - US: $2 billion
   - China: $15 billion
2. Store and Decrypt attack
   - NSA's Utah Data Center: 1+ Exabyte (= 1M terabytes).

Lattices are Big

Parameter Sizes for Practical Crypto (Bytes)

Cipher	pk	Ctx
Kyber512	800	768

Lattices are Big

Parameter Sizes for Practical Crypto (Bytes)

Cipher	pk	Ctx
Kyber512	800	768
ECDH	32	32

Lattices are Big

Parameter Sizes for Practical Crypto (Bytes)

Cipher	pk	Ctx
Kyber512	800	768
ECDH	32	32
RSA-2048	256	256

Lattices are Big

Parameter Sizes for Practical Crypto (Bytes)

Cipher	pk	Ctx
Kyber512	800	768
ECDH	32	32
RSA-2048	256	256

Is this fundamental?

Lattices are Big

Parameter Sizes for Practical Crypto (Bytes)

Cipher	pk	Ctx
Kyber512	800	768
ECDH	32	32
RSA-2048	256	256

Is this fundamental?

- This Work: Mostly*

Contents

LWE

LWE Distribution

Let $\sigma > 0$, $q, n \in \mathbb{N}$. For

- $\vec{s}, \vec{e} \leftarrow \mathcal{N}(0, \sigma^2 I_n)$,
- $A \leftarrow \mathbb{Z}_q^{n \times n}$

$$[A, A\vec{s} + \vec{e}] \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^n$$

- LWE Problem: Distinguish distribution Uniform samples

LWE

LWE Distribution

Let $\sigma > 0$, $q, n \in \mathbb{N}$. For

- $\vec{s}, \vec{e} \leftarrow \mathcal{N}(0, \sigma^2 I_n)$,
- $A \leftarrow \mathbb{Z}_q^{n\times n}$

$$[A, A\vec{s} + \vec{e}] \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^n$$

- LWE Problem: Distinguish distribution Uniform samples
- Parameter Regimes:

LWE

LWE Distribution

Let $\sigma > 0$, $q, n \in \mathbb{N}$. For

- $\vec{s}, \vec{e} \leftarrow \mathcal{N}(0, \sigma^2 I_n)$,
- $A \leftarrow \mathbb{Z}_q^{n\times n}$

$$[A, A\vec{s} + \vec{e}] \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^n$$

- LWE Problem: Distinguish distribution Uniform samples
- Parameter Regimes:
  - Theoretical: $q = \text{poly}(n)$, $\sigma = \Omega(\sqrt{n})$

LWE

LWE Distribution

Let $\sigma > 0$, $q, n \in \mathbb{N}$. For

- $\vec{s}, \vec{e} \leftarrow \mathcal{N}(0, \sigma^2 I_n)$,
- $A \leftarrow \mathbb{Z}_q^{n\times n}$

$$[A, A\vec{s} + \vec{e}] \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^n$$

- LWE Problem: Distinguish distribution Uniform samples
- Parameter Regimes:
  - Theoretical: $q = \text{poly}(n)$, $\sigma = \Omega(\sqrt{n})$
    - Really Theoretical: $q = n^{\omega(1)}$

LWE

LWE Distribution

Let $\sigma > 0$, $q, n \in \mathbb{N}$. For

- $\vec{s}, \vec{e} \leftarrow \mathcal{N}(0, \sigma^2 I_n)$,
- $A \leftarrow \mathbb{Z}_q^{n\times n}$

$$[A, A\vec{s} + \vec{e}] \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^n$$

- LWE Problem: Distinguish distribution Uniform samples
- Parameter Regimes:
  - Theoretical: $q = \text{poly}(n)$, $\sigma = \Omega(\sqrt{n})$
    - Really Theoretical: $q = n^{\omega(1)}$
  - Practical: $\log_2 q \approx 12$, $\sigma = 8$

Encryption from LWE

1. Private-key: Use Uniform sample as One-Time Pad

Encryption from LWE

1. Private-key: Use Uniform sample as One-Time Pad
   - $\vec{m} \mapsto [A, \vec{u} + \vec{m}]$

Encryption from LWE

1. Private-key: Use Uniform sample as One-Time Pad
   - $\vec{m} \mapsto [A, \vec{u} + \vec{m}]$
2. Decrypt $[A, A\vec{s} + \vec{e} + \vec{m}]$?
   - Recover $\vec{m} + \vec{e} \neq \vec{m}$

Encryption from LWE

1. Private-key: Use Uniform sample as One-Time Pad
   - $\vec{m} \mapsto [A, \vec{u} + \vec{m}]$
2. Decrypt $[A, A\vec{s} + \vec{e} + \vec{m}]$?
   - Recover $\vec{m} + \vec{e} \neq \vec{m}$
3. Idea: Encode $\vec{m}$ with error-correction

Lattice Code

A lattice code is the pair of a lattice $L \subseteq \mathbb{R}^n$, along with a rounding algorithm $\mathbb{R}^n \to L$ such that

- $\lfloor 0 \rceil = 0$, and
- $\forall x \in L, \forall y \in \mathbb{R}^n : \lfloor x + y \rceil = x + \lfloor y \rceil$.

Lattice Code

A lattice code is the pair of a lattice $L \subseteq \mathbb{R}^n$, along with a rounding algorithm $\mathbb{R}^n \to L$ such that

- $\lfloor 0 \rceil = 0$, and
- $\forall x \in L, \forall y \in \mathbb{R}^n : \lfloor x + y \rceil = x + \lfloor y \rceil$.

Fundamental Region: $\mathcal{V}_{\lfloor \cdot \rceil} = \{x \in \mathbb{R}^n \mid \lfloor x \rceil = 0\}$

Lattice Code

A lattice code is the pair of a lattice $L \subseteq \mathbb{R}^n$, along with a rounding algorithm $\mathbb{R}^n \to L$ such that

- $\lfloor 0 \rceil = 0$, and
- $\forall x \in L, \forall y \in \mathbb{R}^n : \lfloor x + y \rceil = x + \lfloor y \rceil$.

Fundamental Region: $\mathcal{V}_{\lfloor \cdot \rceil} = \{x \in \mathbb{R}^n \mid \lfloor x \rceil = 0\}$

- Conditions imply $L + \mathcal{V}_{\lfloor \cdot \rceil} = \mathbb{R}^n$

Lattice Code

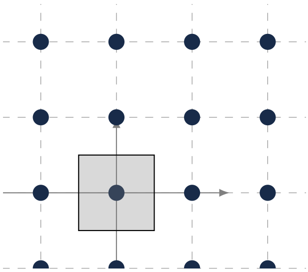
A lattice code is the pair of a lattice $L \subseteq \mathbb{R}^n$, along with a rounding algorithm $\mathbb{R}^n \to L$ such that

- $\lfloor 0 \rceil = 0$, and
- $\forall x \in L, \forall y \in \mathbb{R}^n : \lfloor x + y \rceil = x + \lfloor y \rceil$.

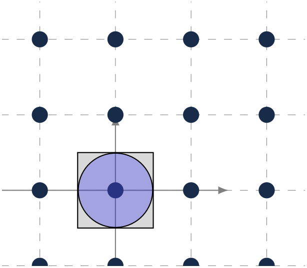
Fundamental Region: $\mathcal{V}_{\lfloor \cdot \rceil} = \{x \in \mathbb{R}^n \mid \lfloor x \rceil = 0\}$

- Conditions imply $L + \mathcal{V}_{\lfloor \cdot \rceil} = \mathbb{R}^n$
- Useful for error correction and quantization

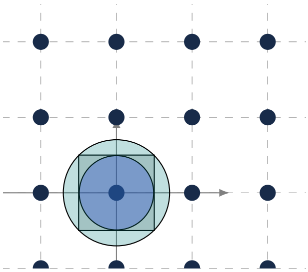
$\mathbb{Z}^n$ as a Lattice Code



$\mathbb{Z}^n$ as a Lattice Code



$\mathbb{Z}^n$ as a Lattice Code



Error Correction and Quantization with $\mathbb{Z}^n$

- Error Correction: $(q/2)\vec{x} + \vec{e} \mapsto \vec{x}$

Error Correction and Quantization with $\mathbb{Z}^n$

- Error Correction: $(q/2)\vec{x} + \vec{e} \mapsto \vec{x}$
  - $\|e\|_\infty < q/4$

Error Correction and Quantization with $\mathbb{Z}^n$

- Error Correction: $(q/2)\vec{x} + \vec{e} \mapsto \vec{x}$
  - $\|e\|_\infty < q/4$
  - $L = (q/2)\mathbb{Z}^n$, $\mathcal{V} = [-q/4, q/4]^n$

Error Correction and Quantization with $\mathbb{Z}^n$

- Error Correction: $(q/2)\vec{x} + \vec{e} \mapsto \vec{x}$
  - $\|e\|_\infty < q/4$
  - $L = (q/2)\mathbb{Z}^n$, $\mathcal{V} = [-q/4, q/4]^n$
- Quantization: $x \in \mathbb{Z}_q^n \mapsto (q/2)\mathbb{Z}_q^n$

Error Correction and Quantization with $\mathbb{Z}^n$

- Error Correction: $(q/2)\vec{x} + \vec{e} \mapsto \vec{x}$
  - $\|e\|_\infty < q/4$
  - $L = (q/2)\mathbb{Z}^n$, $\mathcal{V} = [-q/4, q/4]^n$
- Quantization: $x \in \mathbb{Z}_q^n \mapsto (q/2)\mathbb{Z}_q^n$
  - Modulus Switching

Error Correction and Quantization with $\mathbb{Z}^n$

- Error Correction: $(q/2)\vec{x} + \vec{e} \mapsto \vec{x}$
  - $\|e\|_\infty < q/4$
  - $L = (q/2)\mathbb{Z}^n$, $\mathcal{V} = [-q/4, q/4]^n$
- Quantization: $x \in \mathbb{Z}_q^n \mapsto (q/2)\mathbb{Z}_q^n$
  - Modulus Switching
  - additive error in $\mathcal{V}$
  - Compresses $n \log_2 \frac{q}{\sqrt[n]{\mathrm{vol}(\mathcal{V})}} < n \log_2 q$

Error Correction and Quantization with $\mathbb{Z}^n$

- Error Correction: $(q/2)\vec{x} + \vec{e} \mapsto \vec{x}$
  - $\|e\|_\infty < q/4$
  - $L = (q/2)\mathbb{Z}^n$, $\mathcal{V} = [-q/4, q/4]^n$
- Quantization: $x \in \mathbb{Z}_q^n \mapsto (q/2)\mathbb{Z}_q^n$
  - Modulus Switching
  - additive error in $\mathcal{V}$
  - Compresses $n \log_2 \frac{q}{\sqrt[n]{\mathrm{vol}(\mathcal{V})}} < n \log_2 q$
- $r \cdot \mathcal{B}_2 \subseteq \mathcal{V} \subseteq R \cdot \mathcal{B}_2$

Error Correction and Quantization with $\mathbb{Z}^n$

- Error Correction: $(q/2)\vec{x} + \vec{e} \mapsto \vec{x}$
  - $\|e\|_\infty < q/4$
  - $L = (q/2)\mathbb{Z}^n$, $\mathcal{V} = [-q/4, q/4]^n$
- Quantization: $x \in \mathbb{Z}_q^n \mapsto (q/2)\mathbb{Z}_q^n$
  - Modulus Switching
  - additive error in $\mathcal{V}$
  - Compresses $n \log_2 \frac{q}{\sqrt[n]{\mathrm{vol}(\mathcal{V})}} < n \log_2 q$
- $r \cdot \mathcal{B}_2 \subseteq \mathcal{V} \subseteq R \cdot \mathcal{B}_2$
  - "Spikiness measure": R/r

Error Correction and Quantization with $\mathbb{Z}^n$

- Error Correction: $(q/2)\vec{x} + \vec{e} \mapsto \vec{x}$
  - $\|e\|_\infty < q/4$
  - $L = (q/2)\mathbb{Z}^n$, $\mathcal{V} = [-q/4, q/4]^n$
- Quantization: $x \in \mathbb{Z}_q^n \mapsto (q/2)\mathbb{Z}_q^n$
  - Modulus Switching
  - additive error in $\mathcal{V}$
  - Compresses $n \log_2 \frac{q}{\sqrt[n]{\mathrm{vol}(\mathcal{V})}} < n \log_2 q$
- $r \cdot \mathcal{B}_2 \subseteq \mathcal{V} \subseteq R \cdot \mathcal{B}_2$
  - "Spikiness measure": R/r
  - For $\mathbb{Z}^n$: $\sqrt{n}$

Error Correction and Quantization with $\mathbb{Z}^n$

- Error Correction: $(q/2)\vec{x} + \vec{e} \mapsto \vec{x}$
  - $\|e\|_\infty < q/4$
  - $L = (q/2)\mathbb{Z}^n$, $\mathcal{V} = [-q/4, q/4]^n$
- Quantization: $x \in \mathbb{Z}_q^n \mapsto (q/2)\mathbb{Z}_q^n$
  - Modulus Switching
  - additive error in $\mathcal{V}$
  - Compresses $n \log_2 \frac{q}{\sqrt[n]{\mathrm{vol}(\mathcal{V})}} < n \log_2 q$
- $r \cdot \mathcal{B}_2 \subseteq \mathcal{V} \subseteq R \cdot \mathcal{B}_2$
  - "Spikiness measure": R/r
  - For $\mathbb{Z}^n$: $\sqrt{n}$
  - For $\epsilon\mathbb{Z} \oplus \epsilon^{-1}\mathbb{Z}$: $\Theta(\epsilon^2)$

Error Correction and Quantization with $\mathbb{Z}^n$

- Error Correction: $(q/2)\vec{x} + \vec{e} \mapsto \vec{x}$
  - $\|e\|_\infty < q/4$
  - $L = (q/2)\mathbb{Z}^n$, $\mathcal{V} = [-q/4, q/4]^n$
- Quantization: $x \in \mathbb{Z}_q^n \mapsto (q/2)\mathbb{Z}_q^n$
  - Modulus Switching
  - additive error in $\mathcal{V}$
  - Compresses $n \log_2 \frac{q}{\sqrt[n]{\mathrm{vol}(\mathcal{V})}} < n \log_2 q$
- $r \cdot \mathcal{B}_2 \subseteq \mathcal{V} \subseteq R \cdot \mathcal{B}_2$
  - "Spikiness measure": R/r
  - For $\mathbb{Z}^n$: $\sqrt{n}$
  - For $\epsilon\mathbb{Z} \oplus \epsilon^{-1}\mathbb{Z}$: $\Theta(\epsilon^2)$
  - $\exists L$ with $R/r < 3$.

Crypto from Lattice Codes

LWE[E, Q]

For $\vec{m} \in E$:

- $\mathrm{Enc}_{\vec{s}}(\vec{m}) := [A, \lfloor A\vec{s} + \vec{e} + \vec{m} \rceil_Q]$
- $\mathrm{Dec}_{\vec{s}}(A, \vec{b}) := \lfloor \vec{b} - A\vec{s} \rceil_E$

- Secure

Crypto from Lattice Codes

LWE[E, Q]

For $\vec{m} \in E$:

- $\text{Enc}_{\vec{s}}(\vec{m}) := [A, \lfloor A\vec{s} + \vec{e} + \vec{m} \rceil_Q]$
- $\text{Dec}_{\vec{s}}(A, \vec{b}) := \lfloor \vec{b} - A\vec{s} \rceil_E$

- Secure
- Correct: $\vec{e} + \vec{e}_Q \in \mathcal{V}_E$
  - $\vec{e}_Q \leftarrow \mathcal{V}_Q$ is quantization error

Crypto from Lattice Codes

LWE[E, Q]

For $\vec{m} \in E$:

- $\mathrm{Enc}_{\vec{s}}(\vec{m}) := [A, \lfloor A\vec{s} + \vec{e} + \vec{m} \rceil_Q]$
- $\mathrm{Dec}_{\vec{s}}(A, \vec{b}) := \lfloor \vec{b} - A\vec{s} \rceil_E$

- Secure
- Correct: $\vec{e} + \vec{e}_Q \in \mathcal{V}_E$
  - $\vec{e}_Q \leftarrow \mathcal{V}_Q$ is quantization error
- Public-Key Case:
  - Correct: $\vec{e}' \in \mathcal{V}_E$ for more complicated e'

Crypto from Lattice Codes

LWE[E, Q]

For $\vec{m} \in E$:

- $\text{Enc}_{\vec{s}}(\vec{m}) := [A, \lfloor A\vec{s} + \vec{e} + \vec{m} \rceil_Q]$
- $\text{Dec}_{\vec{s}}(A, \vec{b}) := \lfloor \vec{b} - A\vec{s} \rceil_E$

- Secure
- Correct: $\vec{e} + \vec{e}_Q \in \mathcal{V}_E$
  - $\vec{e}_Q \leftarrow \mathcal{V}_Q$ is quantization error
- Public-Key Case:
  - Correct: $\vec{e}' \in \mathcal{V}_E$ for more complicated e'
    - $\langle \vec{e}, \vec{e}' \rangle$, $\vec{e}, \vec{e}' \sim \mathcal{N}(0, \sigma^2 I_n)$

Crypto from Lattice Codes

LWE[E, Q]

For $\vec{m} \in E$:

- $\mathrm{Enc}_{\vec{s}}(\vec{m}) := [A, \lfloor A\vec{s} + \vec{e} + \vec{m} \rceil_Q]$
- $\mathrm{Dec}_{\vec{s}}(A, \vec{b}) := \lfloor \vec{b} - A\vec{s} \rceil_E$

- Secure
- Correct: $\vec{e} + \vec{e}_Q \in \mathcal{V}_E$
  - $\vec{e}_Q \leftarrow \mathcal{V}_Q$ is quantization error
- Public-Key Case:
  - Correct: $\vec{e}' \in \mathcal{V}_E$ for more complicated e'
    - $\langle \vec{e}, \vec{e}' \rangle$, $\vec{e}, \vec{e}' \sim \mathcal{N}(0, \sigma^2 I_n)$
    - $\langle \vec{e}, \vec{e}_Q \rangle$

Contents

Main Content of Paper

- Bound rate of LWE[E, Q]
  - $0 \leq \frac{\log_2 |\#\text{ptxts}|}{\log_2 |\#\text{ctxts}|} \leq 1$

Main Content of Paper

- Bound rate of LWE$[E, Q]$
  - $0 \leq \frac{\log_2 |\#\text{ptxts}|}{\log_2 |\#\text{ctxts}|} \leq 1$
  - Cost transmitting A as free

Main Content of Paper

- Bound rate of LWE$[E, Q]$
  - $0 \leq \frac{\log_2 |\#\text{ptxts}|}{\log_2 |\#\text{ctxts}|} \leq 1$
  - Cost transmitting A as free
- Two noise models

Main Content of Paper

- Bound rate of LWE$[E, Q]$
  - $0 \leq \frac{\log_2 |\#\text{ptxts}|}{\log_2 |\#\text{ctxts}|} \leq 1$
  - Cost transmitting A as free
- Two noise models
  - Perfect correctness ($\vec{e}$ bounded)
    - Packing arguments

Main Content of Paper

- Bound rate of LWE$[E, Q]$
  - $0 \leq \frac{\log_2 |\#\text{ptxts}|}{\log_2 |\#\text{ctxts}|} \leq 1$
  - Cost transmitting A as free
- Two noise models
  - Perfect correctness ($\vec{e}$ bounded)
    - Packing arguments
  - Correctness whp ($\vec{e}$ concentrated)
    - "Reverse" Chernoff Bounds

Packing Arguments

- $\vec{e} \leftarrow \sigma\sqrt{n} \cdot \mathcal{B}_2$ typical length of a Gaussian

Packing Arguments

- $\vec{e} \leftarrow \sigma\sqrt{n} \cdot \mathcal{B}_2$ typical length of a Gaussian
- Correct if $\sigma\sqrt{n}\mathcal{B}_2 + \mathcal{V}_Q \subseteq \mathcal{V}_E$

Packing Arguments

- $\vec{e} \leftarrow \sigma\sqrt{n} \cdot \mathcal{B}_2$ typical length of a Gaussian
- Correct if $\sigma\sqrt{n}\mathcal{B}_2 + \mathcal{V}_Q \subseteq \mathcal{V}_E$
  - . . . take volumes

Packing Arguments

- $\vec{e} \leftarrow \sigma\sqrt{n} \cdot \mathcal{B}_2$ typical length of a Gaussian
- Correct if $\sigma\sqrt{n}\mathcal{B}_2 + \mathcal{V}_Q \subseteq \mathcal{V}_E$
  - ... take volumes

Bounded Noise Impossibility

For any lattice codes E, Q, $q = \text{poly}(n)$, $\sigma = \Theta(\sqrt{n})$

1. $\text{LWE}[E, \mathbb{Z}^n]$ is not rate $1 - o(1)$,
2. $\sqrt[n]{\text{vol}(\mathcal{V}_Q)} < \sigma^{(1-\epsilon)} \implies \text{LWE}[E, Q]$ is not rate $1 - o(1)$
3. $\sqrt[n]{\text{vol}(\mathcal{V}_Q)} = O(\sigma) \implies \text{LWE}[E, Q]$ is not rate $1 - o(1/(\log q))$.

Concentrated Noise Bounds

- Now want $\vec{e} + \vec{e}_Q \subseteq \mathcal{V}_E$ whp
  - (Reverse) Chernoff Bounds:
    $\exp(-\epsilon^2/(2n\sigma^2)) \geq \Pr[\|\vec{x}\|_2 > \epsilon] \geq 1 - O\left(\frac{\epsilon}{\sqrt{n\sigma^2}}\right)$

Concentrated Noise Bounds

- Now want $\vec{e} + \vec{e}_Q \subseteq \mathcal{V}_E$ whp
  - (Reverse) Chernoff Bounds: $\exp(-\epsilon^2/(2n\sigma^2)) \geq \Pr[\|\vec{x}\|_2 > \epsilon] \geq 1 - O\left(\frac{\epsilon}{\sqrt{n\sigma^2}}\right)$

Log-Concave Impossibility for $Q = \mathbb{Z}^n$

For any E, $q = \text{poly}(n)$, if for some $\epsilon > 0$

- $R_E \leq O(n^{1-\epsilon})$, or
- $R_E/r_E \leq O(n^{1/2-\epsilon})$

Then LWE$[E, \mathbb{Z}^n]$ encryption is not rate $1 - o(1)$.

Concentrated Noise Bounds: Pt 2

Log-Concave Impossibility

For any E, for any Q with $R_Q \leq O(\sqrt{n})$, if $\sqrt[n]{\mathrm{vol}(\mathcal{V}_Q)} \leq O(\sigma)$, LWE$[E, Q]$ cannot have rate

$$1 - o\left(\frac{1}{n \log(q/\sigma)}\right).$$

- $1 - O(1/n)$ achievable

Concentrated Noise Bounds: Pt 3

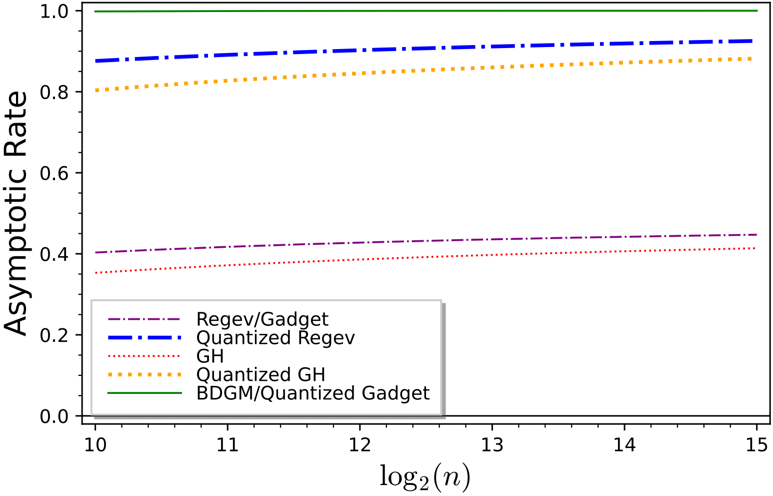
Dimension Reduction for Concentrated Noise

If E, Q are k-dimensional, and $E' = E^{\oplus(n/k)}, Q' = Q^{\oplus(n/k)}$, then under same conditions as before LWE[E, Q] cannot have rate

$$1 - o\left(\frac{1}{k\log(q/\sigma)}\right).$$

- Typically $k = O(\log n)$, exponentially stronger

Some Concrete Rates



Contents

- Info-theoretic bounds on sizes of lattice crypto ciphertexts

- Info-theoretic bounds on sizes of lattice crypto ciphertexts
- Quantization is vital to achieve rate $1 - o(1)$

- Info-theoretic bounds on sizes of lattice crypto ciphertexts
- Quantization is vital to achieve rate $1 - o(1)$
- Open Questions:
  - Optimizing transmission of 128 bits?

- Info-theoretic bounds on sizes of lattice crypto ciphertexts
- Quantization is vital to achieve rate $1 - o(1)$
- Open Questions:
  - Optimizing transmission of 128 bits?
  - FHE operations on compressed ciphertexts?

- Info-theoretic bounds on sizes of lattice crypto ciphertexts
- Quantization is vital to achieve rate $1 - o(1)$
- Open Questions:
  - Optimizing transmission of 128 bits?
  - FHE operations on compressed ciphertexts?
  - Other high-dimensional lattice codes in lattice-based cryptography?

- Info-theoretic bounds on sizes of lattice crypto ciphertexts
- Quantization is vital to achieve rate $1 - o(1)$
- Open Questions:
  - Optimizing transmission of 128 bits?
  - FHE operations on compressed ciphertexts?
  - Other high-dimensional lattice codes in lattice-based cryptography?
  - Algebraic Structure?