A Tool for the Estimation of Lattice Parameters

Bachelor Thesis

Nicolai Krebs

November 26, 2021

Table of Contents

Table of Contents

Background

- Quantum computers can efficiently solve classically hard problems

Background

- Quantum computers can efficiently solve classically hard problems
  - Shor's algorithm (1994)[1]

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

Background

- Quantum computers can efficiently solve classically hard problems
  - Shor's algorithm (1994)[1]
  - Efficiently solves integer factorization problem

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

Background

- Quantum computers can efficiently solve classically hard problems
  - Shor's algorithm (1994)[1]
  - Efficiently solves integer factorization problem
  - E.g., RSA becomes insecure

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

Background

- Quantum computers can efficiently solve classically hard problems
  - Shor's algorithm (1994)[1]
  - Efficiently solves integer factorization problem
  - E.g., RSA becomes insecure
- Different hardness assumptions needed

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

Background

- Quantum computers can efficiently solve classically hard problems
  - Shor's algorithm (1994)[1]
  - Efficiently solves integer factorization problem
  - E.g., RSA becomes insecure
- Different hardness assumptions needed

⇒ Lattice-based cryptography

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

Lattice-based Cryptography

Lattice

A lattice is a discrete Λ additive subgroup of the vector space $\mathbb{R}^m$ and can be defined by a basis $\mathbf{B}$ of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ with $m \geq n$.

Lattice-based Cryptography

Lattice

A lattice is a discrete Λ additive subgroup of the vector space $\mathbb{R}^m$ and can be defined by a basis $\mathbf{B}$ of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ with $m \geq n$.

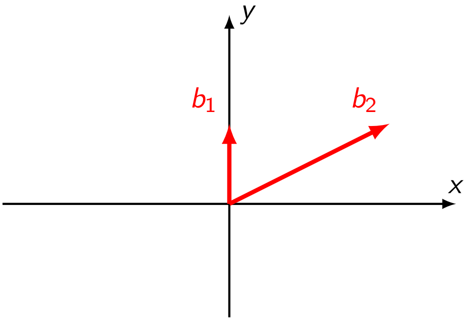


Figure: Lattice with basis $\mathbf{b}_1 = (0, 1)^\intercal,\ \mathbf{b}_2 = (2, 1)^\intercal$

Lattice

A lattice is a discrete Λ additive subgroup of the vector space $\mathbb{R}^m$ and can be defined by a basis $\mathbf{B}$ of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ with $m \geq n$.

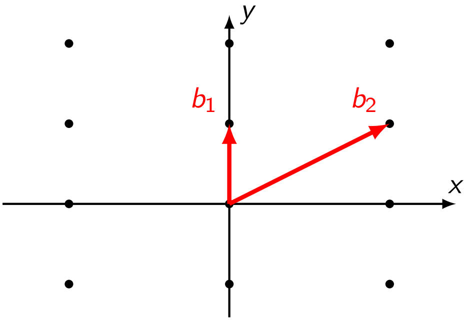


Figure: Lattice with basis $\mathbf{b}_1 = (0, 1)^\intercal$, $\mathbf{b}_2 = (2, 1)^\intercal$

Lattice

A lattice is a discrete Λ additive subgroup of the vector space $\mathbb{R}^m$ and can be defined by a basis $\mathbf{B}$ of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ with $m \geq n$.

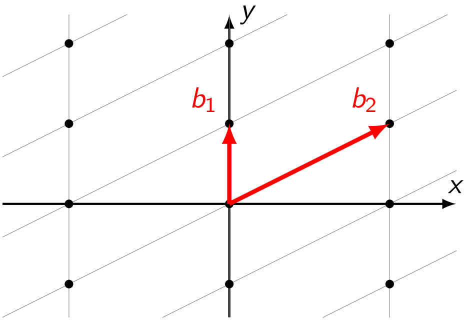


Figure: Lattice with basis $\mathbf{b}_1 = (0, 1)^\intercal$, $\mathbf{b}_2 = (2, 1)^\intercal$

Lattice-based Cryptography

Lattice

A lattice is a discrete Λ additive subgroup of the vector space $\mathbb{R}^m$ and can be defined by a basis $\mathbf{B}$ of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ with $m \geq n$.

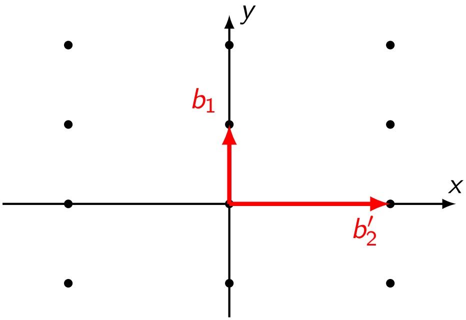


Figure: Lattice with basis $\mathbf{b}_1 = (0,1)^\intercal$, $\mathbf{b}_2' = (2,0)^\intercal$

Lattice

A lattice is a discrete Λ additive subgroup of the vector space $\mathbb{R}^m$ and can be defined by a basis $\mathbf{B}$ of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ with $m \geq n$.

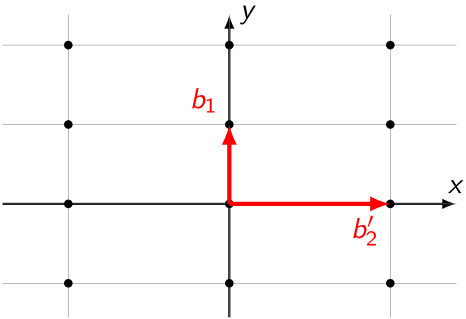


Figure: Lattice with basis $\mathbf{b}_1 = (0,1)^\intercal$, $\mathbf{b}_2' = (2,0)^\intercal$

Lattice-based Cryptography

SVP_γ and $\textsc{GapSVP}_\gamma$

Given a basis $\mathbf{B}$ of a lattice Λ, the (approximate) Shortest Vector Problem (SVP_γ) is the problem of finding a short lattice vector $\mathbf{v} \in \Lambda$ such that $0 < \|\mathbf{v}\| \leq \gamma\lambda_1(\Lambda)$. The corresponding decision version is the $\textsc{GapSVP}_\gamma$ problem, in which we are asked to decide whether $\lambda_1(\Lambda) \leq 1$ or $\lambda_1(\Lambda) \geq \gamma$ given a basis $\mathbf{B}$ of Λ. If neither is the case, any answer is accepted.

Lattice-based Cryptography

SVP_γ and $\textsc{GapSVP}_\gamma$

Given a basis $\mathbf{B}$ of a lattice Λ, the (approximate) Shortest Vector Problem (SVP_γ) is the problem of finding a short lattice vector $\mathbf{v} \in \Lambda$ such that $0 < \|\mathbf{v}\| \leq \gamma\lambda_1(\Lambda)$. The corresponding decision version is the $\textsc{GapSVP}_\gamma$ problem, in which we are asked to decide whether $\lambda_1(\Lambda) \leq 1$ or $\lambda_1(\Lambda) \geq \gamma$ given a basis $\mathbf{B}$ of Λ. If neither is the case, any answer is accepted.

- Worst-case to average-case reduction from SVP_γ to the Short Integer Solution (SIS) problem[2]

[2] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, G. L. Miller, Ed., ACM, 1996, pp. 99–108.

Lattice-based Cryptography

SVP_γ and $\textsc{GapSVP}_\gamma$

Given a basis **B** of a lattice Λ, the (approximate) Shortest Vector Problem (SVP_γ) is the problem of finding a short lattice vector $\mathbf{v} \in \Lambda$ such that $0 < \|\mathbf{v}\| \leq \gamma\lambda_1(\Lambda)$. The corresponding decision version is the $\textsc{GapSVP}_\gamma$ problem, in which we are asked to decide whether $\lambda_1(\Lambda) \leq 1$ or $\lambda_1(\Lambda) \geq \gamma$ given a basis **B** of Λ. If neither is the case, any answer is accepted.

- Worst-case to average-case reduction from SVP_γ to the Short Integer Solution (SIS) problem[2]
- Similar reduction from $\textsc{GapSVP}_\gamma$ to the Learning with Errors (LWE) problem[3]

[2] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, G. L. Miller, Ed., ACM, 1996, pp. 99–108.

[3] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, H. N. Gabow and R. Fagin, Eds., ACM, 2005, pp. 84–93.

The Learning with Errors (LWE) Problem

The $\mathrm{LWE}_{n,q,m,\chi}$ distribution

Given an integer $n \geq 1$, a modulus $q \geq 2$, an error distribution χ on $\mathbb{Z}_q$, and a fixed secret vector $\mathbf{s}$, let $\mathcal{A}_{\mathbf{s},\chi}$ be the probability distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ by choosing a vector $\mathbf{a}_i \in \mathbb{Z}_q^n$ uniformly at random and $e_i \in \mathbb{Z}_q$ according to χ.

The Learning with Errors (LWE) Problem

The $\text{LWE}_{n,q,m,\chi}$ distribution

Given an integer $n \geq 1$, a modulus $q \geq 2$, an error distribution χ on $\mathbb{Z}_q$, and a fixed secret vector $\mathbf{s}$, let $\mathcal{A}_{\mathbf{s},\chi}$ be the probability distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ by choosing a vector $\mathbf{a}_i \in \mathbb{Z}_q^n$ uniformly at random and $e_i \in \mathbb{Z}_q$ according to χ. $\mathcal{A}_{\mathbf{s},\chi}$ outputs m samples

$$(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \mod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q.$$

The Learning with Errors (LWE) Problem

The $\mathrm{LWE}_{n,q,m,\chi}$ distribution

Given an integer $n \geq 1$, a modulus $q \geq 2$, an error distribution χ on $\mathbb{Z}_q$, and a fixed secret vector $\mathbf{s}$, let $\mathcal{A}_{\mathbf{s},\chi}$ be the probability distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ by choosing a vector $\mathbf{a}_i \in \mathbb{Z}_q^n$ uniformly at random and $e_i \in \mathbb{Z}_q$ according to χ. $\mathcal{A}_{\mathbf{s},\chi}$ outputs m samples

$$(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \mod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q.$$

- m samples can be represented by matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and vector $\mathbf{z}$ with

$$\mathbf{z} = \mathbf{A}^\intercal \mathbf{s} + \mathbf{e} \mod q$$

The Learning with Errors (LWE) Problem

The $\text{LWE}_{n,q,m,\chi}$ distribution

Given an integer $n \geq 1$, a modulus $q \geq 2$, an error distribution χ on $\mathbb{Z}_q$, and a fixed secret vector $\mathbf{s}$, let $\mathcal{A}_{\mathbf{s},\chi}$ be the probability distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ by choosing a vector $\mathbf{a}_i \in \mathbb{Z}_q^n$ uniformly at random and $e_i \in \mathbb{Z}_q$ according to χ. $\mathcal{A}_{\mathbf{s},\chi}$ outputs m samples

$$(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \mod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q.$$

- m samples can be represented by matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and vector $\mathbf{z}$ with

$$\mathbf{z} = \mathbf{A}^\intercal \mathbf{s} + \mathbf{e} \mod q$$

- Search-LWE asks to recover $\mathbf{s}$ and Decision-LWE asks to distinguish m samples from uniformly random

The Learning with Errors (LWE) Problem

The $\mathrm{LWE}_{n,q,m,\chi}$ distribution

Given an integer $n \geq 1$, a modulus $q \geq 2$, an error distribution χ on $\mathbb{Z}_q$, and a fixed secret vector $\mathbf{s}$, let $\mathcal{A}_{\mathbf{s},\chi}$ be the probability distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ by choosing a vector $\mathbf{a}_i \in \mathbb{Z}_q^n$ uniformly at random and $e_i \in \mathbb{Z}_q$ according to χ. $\mathcal{A}_{\mathbf{s},\chi}$ outputs m samples

$$(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \mod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q.$$

- m samples can be represented by matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and vector $\mathbf{z}$ with

$$\mathbf{z} = \mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{e} \mod q$$

- Search-LWE asks to recover $\mathbf{s}$ and Decision-LWE asks to distinguish m samples from uniformly random
- (Primal) LWE lattice

$$\Lambda_q(\mathbf{A}^\mathsf{T}) = \{\mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{y} \in \mathbb{Z}^n : \mathbf{v} = \mathbf{A}^\mathsf{T}\mathbf{y} \mod q\}$$

The Short Integer Solution (SIS) Problem

The SIS Problem

Given a uniformly random matrix $\mathbf{A}^{n \times m}$, the $\mathsf{SIS}_{n,q,m,\beta}$ problem asks us to find a vector $\mathbf{s} \in \mathbb{Z}^m$ such that

$$\mathbf{A} \cdot \mathbf{s} = \mathbf{0} \mod q,$$

where $0 < \|\mathbf{s}\| \leq \beta$.

The Short Integer Solution (SIS) Problem

The SIS Problem

Given a uniformly random matrix $\mathbf{A}^{n \times m}$, the $\text{SIS}_{n,q,m,\beta}$ problem asks us to find a vector $\mathbf{s} \in \mathbb{Z}^m$ such that

$$\mathbf{A} \cdot \mathbf{s} = \mathbf{0} \mod q,$$

where $0 < \|\mathbf{s}\| \leq \beta$.

- (Dual) SIS lattice

$$\Lambda_q^{\perp}(\mathbf{A}) = \left\{ \mathbf{v} \in \mathbb{Z}^m \mid \mathbf{A} \cdot \mathbf{v} = \mathbf{0} \mod q \right\}.$$

In Practice

- SIS: OWF, CRHF, IBE, DIGSIG

In Practice

- SIS: OWF, CRHF, IBE, DIGSIG
- LWE: PKE, IBE, SHE, FHE, . . .

In Practice

- SIS: OWF, CRHF, IBE, DIGSIG
- LWE: PKE, IBE, SHE, FHE, . . .
- Security of resulting scheme depends on chosen parameters

In Practice

- SIS: OWF, CRHF, IBE, DIGSIG
- LWE: PKE, IBE, SHE, FHE, ...
- Security of resulting scheme depends on chosen parameters
    - Bit security level $\mathtt{sec}$

In Practice

- SIS: OWF, CRHF, IBE, DIGSIG
- LWE: PKE, IBE, SHE, FHE, ...
- Security of resulting scheme depends on chosen parameters
  - Bit security level $\mathtt{sec}$
  - E.g., $\mathtt{sec} = 128$ means that attacker needs $> 2^{128}$ operations

In Practice

- SIS: OWF, CRHF, IBE, DIGSIG
- LWE: PKE, IBE, SHE, FHE, ...
- Security of resulting scheme depends on chosen parameters
  - Bit security level $\mathtt{sec}$
  - E.g., $\mathtt{sec} = 128$ means that attacker needs $> 2^{128}$ operations
- How to estimate the concrete hardness of a given instance?

In Practice

- SIS: OWF, CRHF, IBE, DIGSIG
- LWE: PKE, IBE, SHE, FHE, ...
- Security of resulting scheme depends on chosen parameters
  - Bit security level $\mathtt{sec}$
  - E.g., $\mathtt{sec} = 128$ means that attacker needs $> 2^{128}$ operations
- How to estimate the concrete hardness of a given instance?
  - Estimate the runtime cost of best attacks

In Practice

- SIS: OWF, CRHF, IBE, DIGSIG
- LWE: PKE, IBE, SHE, FHE, ...
- Security of resulting scheme depends on chosen parameters
  - Bit security level $\mathtt{sec}$
  - E.g., $\mathtt{sec} = 128$ means that attacker needs $> 2^{128}$ operations
- How to estimate the concrete hardness of a given instance?
  - Estimate the runtime cost of best attacks
- LWE Estimator[4] encapsulates attack estimates for LWE

[4] M. R. Albrecht, R. Player, and S. Scott, "On the concrete hardness of learning with errors," *J. Math. Cryptol.*, vol. 9, no. 3, pp. 169–203, 2015.

A Tool for the Estimation of Lattice Parameters

A unified Python library that includes

A Tool for the Estimation of Lattice Parameters

A unified Python library that includes

- Estimates of attack algorithms against LWE and SIS

A Tool for the Estimation of Lattice Parameters

A unified Python library that includes

- Estimates of attack algorithms against LWE and SIS
- Up-to-date cost models

A Tool for the Estimation of Lattice Parameters

A unified Python library that includes

- Estimates of attack algorithms against LWE and SIS
- Up-to-date cost models
- Classes for LWE, SIS and their ring and module variants as well as unconditionally secure variants

A Tool for the Estimation of Lattice Parameters

A unified Python library that includes

- Estimates of attack algorithms against LWE and SIS
- Up-to-date cost models
- Classes for LWE, SIS and their ring and module variants as well as unconditionally secure variants
- Distribution classes and ℓ_p-norm bounds

A Tool for the Estimation of Lattice Parameters

A unified Python library that includes

- Estimates of attack algorithms against LWE and SIS
- Up-to-date cost models
- Classes for LWE, SIS and their ring and module variants as well as unconditionally secure variants
- Distribution classes and ℓ_p-norm bounds
- An efficient generic parameter search

Table of Contents

Lattice Basis Reduction

- Root Hermite factor

Lattice Basis Reduction

- Root Hermite factor
  - Given a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ with $\|\mathbf{b}_1\| \leq \cdots \leq \|\mathbf{b}_n\|$

Lattice Basis Reduction

- Root Hermite factor
  - Given a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ with $\|\mathbf{b}_1\| \leq \cdots \leq \|\mathbf{b}_n\|$
  - Basis $\mathbf{B}$ has root Hermite factor δ iff

$$\|\mathbf{b}_1\| \approx \delta^n \det(\Lambda)^{1/n}$$

- Root Hermite factor
  - Given a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ with $\|\mathbf{b}_1\| \leq \cdots \leq \|\mathbf{b}_n\|$
  - Basis $\mathbf{B}$ has root Hermite factor δ iff

$$\|\mathbf{b}_1\| \approx \delta^n \det(\Lambda)^{1/n}$$

- The Lenstra, Lenstra and Lovász (LLL) algorithm[5]

[5] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, Dec. 1982.

Lattice Basis Reduction

- Root Hermite factor
  - Given a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ with $\|\mathbf{b}_1\| \leq \cdots \leq \|\mathbf{b}_n\|$
  - Basis $\mathbf{B}$ has root Hermite factor δ iff

$$\|\mathbf{b}_1\| \approx \delta^n \det(\Lambda)^{1/n}$$

- The Lenstra, Lenstra and Lovász (LLL) algorithm[5]
  - Finds short vectors of length at most $2^{n/2}\lambda_1(\Lambda)$ in polynomial time

[5] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, Dec. 1982.

Lattice Basis Reduction

- Root Hermite factor
  - Given a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ with $\|\mathbf{b}_1\| \leq \cdots \leq \|\mathbf{b}_n\|$
  - Basis $\mathbf{B}$ has root Hermite factor δ iff

$$\|\mathbf{b}_1\| \approx \delta^n \det(\Lambda)^{1/n}$$

- The Lenstra, Lenstra and Lovász (LLL) algorithm[5]
  - Finds short vectors of length at most $2^{n/2}\lambda_1(\Lambda)$ in polynomial time
  - In practice achieves $\delta \approx 1.021$ on average

[5] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, Dec. 1982.

Lattice Basis Reduction

- The Block Korkin-Zolotarev (BKZ) algorithm[6]

[6] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," in *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

- The Block Korkin-Zolotarev (BKZ) algorithm[6]
  - Simplified runtime estimate: $\rho \cdot n \cdot t_k$

[6] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," in *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

- The Block Korkin-Zolotarev (BKZ) algorithm[6]
  - Simplified runtime estimate: $\rho \cdot n \cdot t_k$
    - ρ: number of rounds

[6] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," in *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

Lattice Basis Reduction

- The Block Korkin-Zolotarev (BKZ) algorithm[6]
  - Simplified runtime estimate: $\rho \cdot n \cdot t_k$
    - ρ: number of rounds
    - t_k: cost of SVP oracle in dimension k

[6] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," in *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

Lattice Basis Reduction

- The Block Korkin-Zolotarev (BKZ) algorithm[6]
  - Simplified runtime estimate: $\rho \cdot n \cdot t_k$
    - ρ: number of rounds
    - t_k: cost of SVP oracle in dimension k
  - Most significant progress in first 8 rounds[7] $\Rightarrow$ LWE-Estimator chooses $\rho = 8$ with estimated output quality

$$\lim_{n \to \infty} \delta \approx \left(\frac{k(\pi k)^{\frac{1}{k}}}{2\pi e} \right)^{\frac{1}{2(k-1)}}$$

[6] C.-P. Schnorr and M. Euchner, “Lattice basis reduction: Improved practical algorithms and solving subset sum problems,” in *Fundamentals of Computation Theory, 8th International Symposium, FCT ’91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

[7] Y. Chen, “Réduction de réseau et sécurité concrete du chiffrement completement homomorphe,” PhD thesis, Paris 7, 2013.

BKZ Cost Models

Realizing an SVP oracle in dimension k:

BKZ Cost Models

Realizing an SVP oracle in dimension k:

- Enumeration algorithms

BKZ Cost Models

Realizing an SVP oracle in dimension k:

- Enumeration algorithms
  - Enumerate all lattice vectors in a bounded region

BKZ Cost Models

Realizing an SVP oracle in dimension k:

- Enumeration algorithms
  - Enumerate all lattice vectors in a bounded region
  - Can be improved by "relaxing" the approximation, pruning the search tree, and preprocessing

BKZ Cost Models

Realizing an SVP oracle in dimension k:

- Enumeration algorithms
  - Enumerate all lattice vectors in a bounded region
  - Can be improved by "relaxing" the approximation, pruning the search tree, and preprocessing
  - In $2^{\mathcal{O}(k \log k)}$ time and polynomial space

BKZ Cost Models

Realizing an SVP oracle in dimension k:

- Enumeration algorithms
  - Enumerate all lattice vectors in a bounded region
  - Can be improved by "relaxing" the approximation, pruning the search tree, and preprocessing
  - In $2^{\mathcal{O}(k \log k)}$ time and polynomial space
- Sieving algorithms

BKZ Cost Models

Realizing an SVP oracle in dimension k:

- Enumeration algorithms
  - Enumerate all lattice vectors in a bounded region
  - Can be improved by "relaxing" the approximation, pruning the search tree, and preprocessing
  - In $2^{\mathcal{O}(k \log k)}$ time and polynomial space
- Sieving algorithms
  - Create a list of lattice points and combine list points such that resulting points have smaller length

BKZ Cost Models

Realizing an SVP oracle in dimension k:

- Enumeration algorithms
  - Enumerate all lattice vectors in a bounded region
  - Can be improved by "relaxing" the approximation, pruning the search tree, and preprocessing
  - In $2^{\mathcal{O}(k \log k)}$ time and polynomial space
- Sieving algorithms
  - Create a list of lattice points and combine list points such that resulting points have smaller length
  - In $2^{\mathcal{O}(k)}$ time and exponential space

BKZ Sieving Cost Models

Name	Cost model
Q-Sieve (paranoid lower bound)[8]	$2^{0.2075k}$
Q-Sieve[9]	$2^{0.265k}$
Sieve [9]	$2^{0.292k}$

[8] E. Alkim, L. Ducas, T. Pöppelmann, *et al.*, "Post-quantum key exchange - A new hope," in *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016*, T. Holz and S. Savage, Eds., USENIX Association, 2016, pp. 327–343.

[9] M. R. Albrecht, V. Gheorghiu, E. W. Postlethwaite, *et al.*, "Estimating quantum speedups for lattice sieves," in *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, S. Moriai and H. Wang, Eds., ser. Lecture Notes in Computer Science, vol. 12492, Springer, 2020, pp. 583–613.

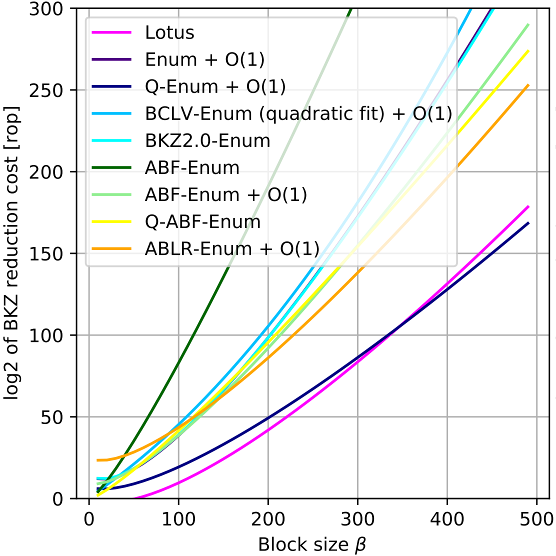
BKZ Enumeration Cost Models

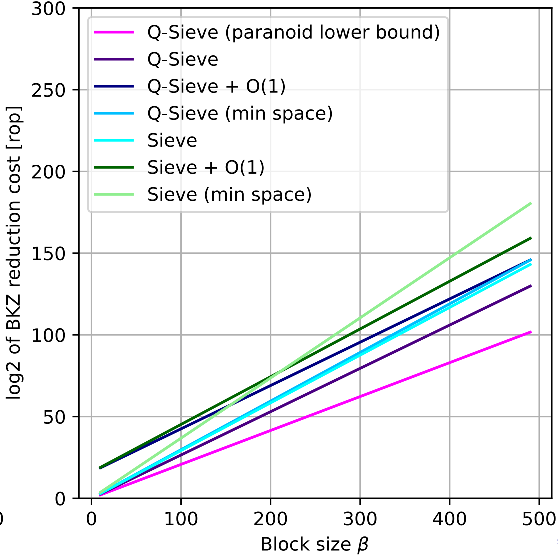
Name	Cost model
Lotus[10]	$2^{0.125k\log k - 0.755k + 2.254}$
Enum + O(1) [10]	$2^{0.187k\log k - 1.019k + 16.1}$
Q-Enum + O(1) [10]	$2^{0.0936k\log k - 0.51k + 8.05}$
BKZ2.0-Enum[11]	$2^{0.184k\log k - 0.995k + 16.25}$
ABF20-Enum [11]	$2^{0.125k\log k}$
Q-ABF20-Enum [11]	$2^{0.0625k\log k}$

[10] M. R. Albrecht, B. R. Curtis, A. Deo, *et al.*, "Estimate all the {lwe, ntru} schemes!" In *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 351–367.

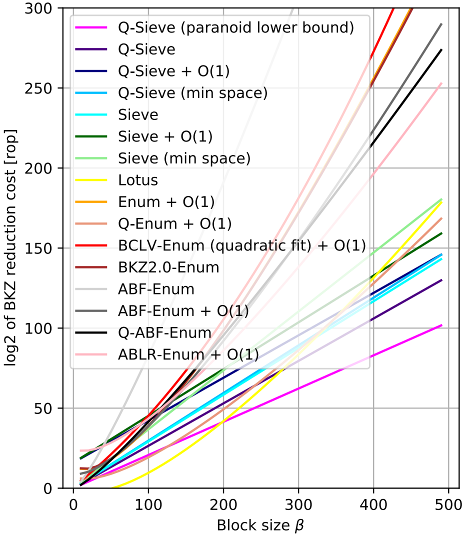
[11] M. R. Albrecht, S. Bai, P.-A. Fouque, *et al.*, "Faster enumeration-based lattice reduction: Root hermite factor $k^{1/(2k)}$ time $k^{k/8+o(k)}$," in *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II*, D. Micciancio and T. Ristenpart, Eds., ser. Lecture Notes in Computer Science, vol. 12171, Springer, 2020, pp. 186–212.

BKZ Enumeration Cost Models

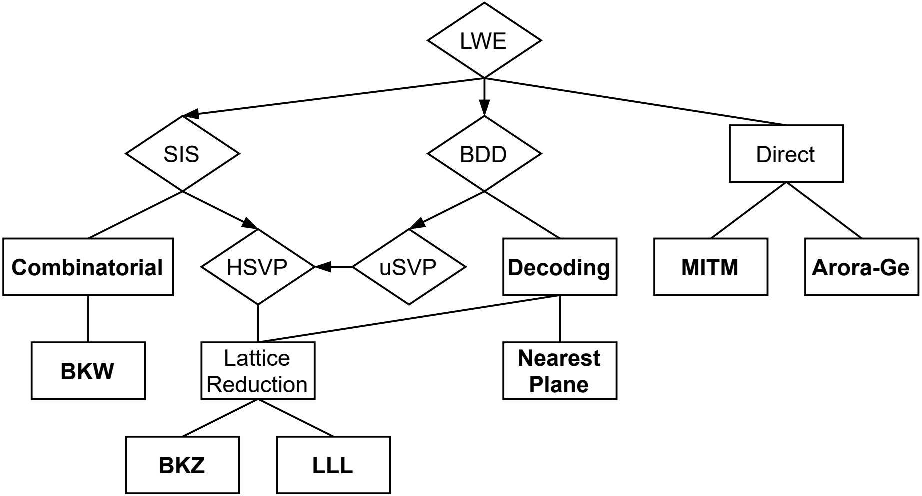




BKZ Enumeration Cost Models



Approaches to Solving LWE



SIS Attack Estimates Comparison

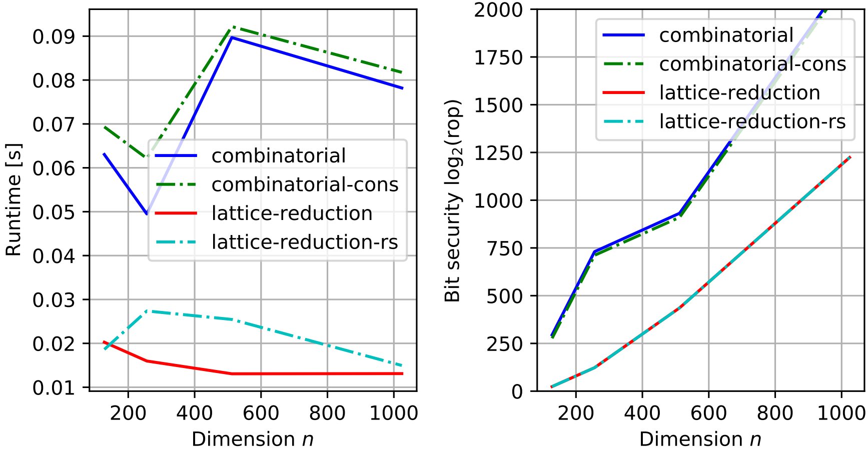


Figure: SIS with $n^2 < q < 2n^2,\ m = 2n\sqrt{n \log q},\ s = 2\sqrt{n \log q}$

SIS Attack Estimates Prioritization

Algorithm	Priority	Justification
Lattice Reduction MR	1	fastest, low cost estimates
Lattice Reduction RS	2	same results as lattice-reduction, not always applicable
Combinatorial Attack	10	fast, often higher cost results
Combinatorial Conservative	9	fast, slighly lower estimates than Combinatorial Attack

LWE Attacks Estimates Comparison

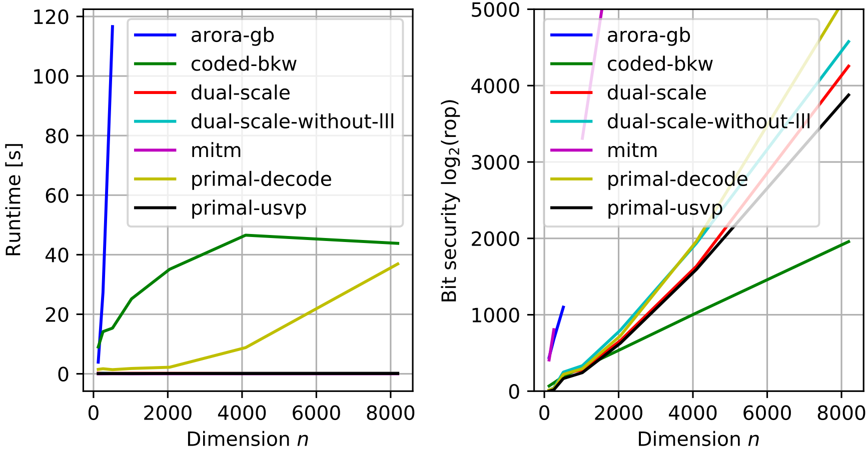


Figure: LWE with $\sigma = 2.828,\ m = \infty,\ n < q < 2n$

LWE Attacks Estimates Comparison

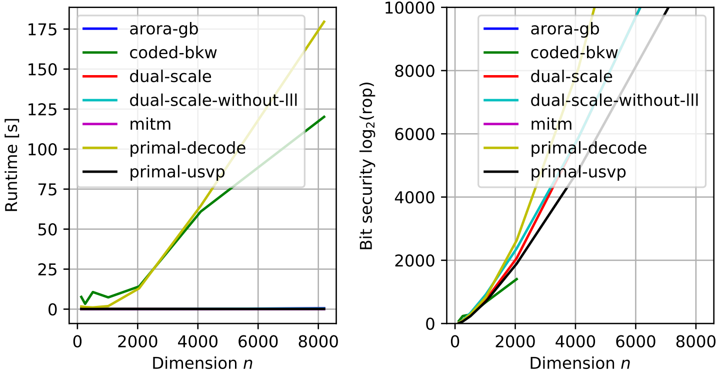


Figure: LWE with parameters chosen as in Regev (ACM 2005)[12]

[12] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, H. N. Gabow and R. Fagin, Eds., ACM, 2005, pp. 84–93.

LWE Attack Estimates Prioritization

Algorithm	Priority	Justification
Meet-in-the-Middle	5	fastest, high cost estimate, as a prefilter
Primal uSVP	10	fast, low cost estimatate estimates
Dual Attack	20	fast, often higher estimates than Primal uSVP
Dual Attack (no LLL)	30	fast, often higher estimates than Dual
Coded-BKW	90	slow, somtimes very low cost estimate (for small stddev), does not always yield results
Decoding Attack	100	slow, often higher estimates than faster algorithms
Arora-Ge	200	extremely slow, often higher estimates, does not always yield results

Table of Contents

Ring and Module Variants

- Interpret $r \in \mathcal{R}$ as an n dimensional vector s.t. $r = \sum_{i=0}^{n-1} r_i x^i$

Ring and Module Variants

- Interpret $r \in \mathcal{R}$ as an n dimensional vector s.t. $r = \sum_{i=0}^{n-1} r_i x^i$
- Each a_i in ring variant corresponds to an $n \times n$ block in the matrix $\mathbf{A}'$ of the standard integer variant obtained by rotation:

$$\mathrm{Rot}(a) = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}$$

Ring and Module Variants

- Interpret $r \in \mathcal{R}$ as an n dimensional vector s.t. $r = \sum_{i=0}^{n-1} r_i x^i$
- Each a_i in ring variant corresponds to an $n \times n$ block in the matrix $\mathbf{A}'$ of the standard integer variant obtained by rotation:

$$\mathrm{Rot}(a) = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}$$

$$\Rightarrow \mathbf{A}' = [\mathrm{Rot}(a_1) \mid \cdots \mid \mathrm{Rot}(a_m)]$$

Ring and Module Variants

- Interpret $r \in \mathcal{R}$ as an n dimensional vector s.t. $r = \sum_{i=0}^{n-1} r_i x^i$
- Each a_i in ring variant corresponds to an $n \times n$ block in the matrix $\mathbf{A}'$ of the standard integer variant obtained by rotation:

$$\mathrm{Rot}(a) = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}$$

$$\Rightarrow \mathbf{A}' = [\mathrm{Rot}(a_1) \mid \cdots \mid \mathrm{Rot}(a_m)]$$

Ring and Module Variants

- Interpret $r \in \mathcal{R}$ as an n dimensional vector s.t. $r = \sum_{i=0}^{n-1} r_i x^i$
- Each a_i in ring variant corresponds to an $n \times n$ block in the matrix $\mathbf{A}'$ of the standard integer variant obtained by rotation:

$$\mathrm{Rot}(a) = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}$$

$$\Rightarrow \mathbf{A}' = [\mathrm{Rot}(a_1) \mid \cdots \mid \mathrm{Rot}(a_m)]$$

- For module variants this becomes

$$n \cdot d \left\{ \overbrace{\begin{bmatrix} \mathrm{Rot}(\boldsymbol{a}_{1,1}) & \mathrm{Rot}(\boldsymbol{a}_{1,2}) & \cdots & \mathrm{Rot}(\boldsymbol{a}_{1,m}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Rot}(\boldsymbol{a}_{d,1}) & \mathrm{Rot}(\boldsymbol{a}_{d,2}) & \cdots & \mathrm{Rot}(\boldsymbol{a}_{d,m}) \end{bmatrix}}^{n \cdot m} \right.$$

Ring and Module Variants

Resulting mapping to standard variant:

- $\mathsf{RSIS}_{n,q,m,\beta} \longrightarrow \mathsf{SIS}_{n,q,m\cdot n,\beta}$

Ring and Module Variants

Resulting mapping to standard variant:

- $\mathsf{RSIS}_{n,q,m,\beta} \longrightarrow \mathsf{SIS}_{n,q,m\cdot n,\beta}$
- $\mathsf{MSIS}_{n,d,q,m,\beta} \longrightarrow \mathsf{SIS}_{n\cdot d,q,m\cdot n,\beta}$

Ring and Module Variants

Resulting mapping to standard variant:

- $\mathsf{RSIS}_{n,q,m,\beta} \longrightarrow \mathsf{SIS}_{n,q,m\cdot n,\beta}$
- $\mathsf{MSIS}_{n,d,q,m,\beta} \longrightarrow \mathsf{SIS}_{n\cdot d,q,m\cdot n,\beta}$
- $\mathsf{RLWE}_{n,q,m,\chi} \longrightarrow \mathsf{LWE}_{n,q,m\cdot n,\chi}$

Ring and Module Variants

Resulting mapping to standard variant:

- $\mathsf{RSIS}_{n,q,m,\beta} \longrightarrow \mathsf{SIS}_{n,q,m \cdot n,\beta}$
- $\mathsf{MSIS}_{n,d,q,m,\beta} \longrightarrow \mathsf{SIS}_{n \cdot d,q,m \cdot n,\beta}$
- $\mathsf{RLWE}_{n,q,m,\chi} \longrightarrow \mathsf{LWE}_{n,q,m \cdot n,\chi}$
- $\mathsf{MLWE}_{n,d,q,m,\chi} \longrightarrow \mathsf{LWE}_{n \cdot d,q,m \cdot n,\chi}$

LWE and SIS Classes Overview

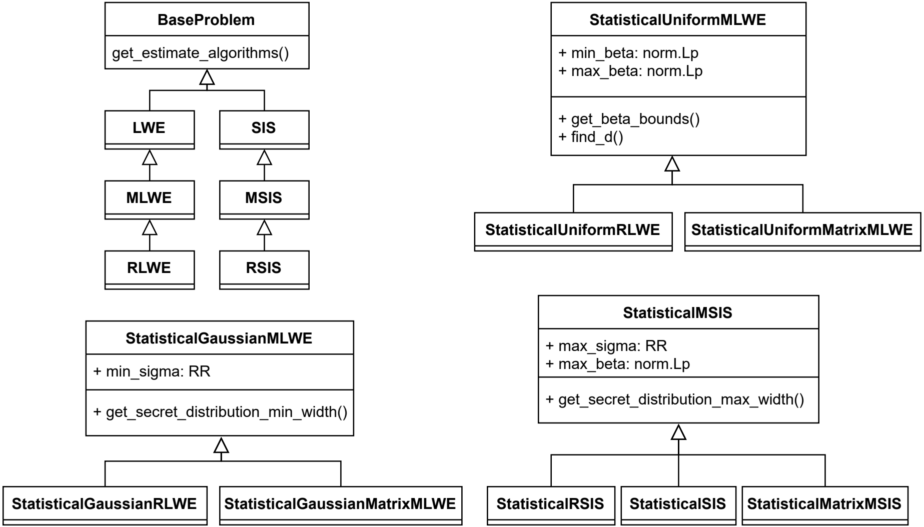


Table of Contents

Norms and Distributions

- Classes `norm.Lp` and `norm.Cp` for ℓ_p-norms and norms on the canonical embedding respectively

Norms and Distributions

- Classes `norm.Lp` and `norm.Cp` for ℓ_p-norms and norms on the canonical embedding respectively
- Norm bounding in class methods `to_Lp()`, addition and multiplication supported

Norms and Distributions

- Classes `norm.Lp` and `norm.Cp` for ℓ_p-norms and norms on the canonical embedding respectively
- Norm bounding in class methods `to_Lp()`, addition and multiplication supported
- Uniform and Gaussian distribution and Gaussian to bound in module `distributions`

Table of Contents

Main functionality

Algorithm 1: Generic Search

Input: sec, initial_params, next_parameters, parameter_cost, problem_instance

Main functionality

Algorithm 1: Generic Search

Input: sec, initial_params, next_parameters, parameter_cost, problem_instance

L = OrderedList(initial_params)

Main functionality

Algorithm 1: Generic Search

Input: sec, initial_params, next_parameters, parameter_cost, problem_instance

```
L = OrderedList(initial_params)
while L ≠ ∅ do
    current_params = L.pop()
    instances = parameter_problem(current_params)
```

Main functionality

Algorithm 1: Generic Search

Input: sec, initial_params, next_parameters, parameter_cost, problem_instance

```
L = OrderedList(initial_params)
while L ≠ ∅ do
    current_params = L.pop()
    instances = parameter_problem(current_params)
    result = estimate(instances, sec)
    if result is secure then
        return (result, current_params)
```

Main functionality

Algorithm 1: Generic Search

Input: sec, initial_params, next_parameters, parameter_cost, problem_instance

```
L = OrderedList(initial_params)
while L ≠ ∅ do
    current_params = L.pop()
    instances = parameter_problem(current_params)
    result = estimate(instances, sec)
    if result is secure then
        return (result, current_params)
    else
        next_param_sets = next_parameters(current_params)
        forall param_set in next_param_sets do
            sort param_set into L according to parameter_cost function
```

Table of Contents

Thank You!

References I

P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, G. L. Miller, Ed., ACM, 1996, pp. 99–108.

O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, H. N. Gabow and R. Fagin, Eds., ACM, 2005, pp. 84–93.

M. R. Albrecht, R. Player, and S. Scott, "On the concrete hardness of learning with errors," *J. Math. Cryptol.*, vol. 9, no. 3, pp. 169–203, 2015.

References II

A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, Dec. 1982.

C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," in *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

Y. Chen, "Réduction de réseau et sécurité concrete du chiffrement completement homomorphe," PhD thesis, Paris 7, 2013.

E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange - A new hope," in *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016*, T. Holz and S. Savage, Eds., USENIX Association, 2016, pp. 327–343.

References III

M. R. Albrecht, V. Gheorghiu, E. W. Postlethwaite, and J. M. Schanck, "Estimating quantum speedups for lattice sieves," in *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, S. Moriai and H. Wang, Eds., ser. Lecture Notes in Computer Science, vol. 12492, Springer, 2020, pp. 583–613.

M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. W. Postlethwaite, F. Virdia, and T. Wunderer, "Estimate all the {lwe, ntru} schemes!" In *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 351–367.

References IV

M. R. Albrecht, S. Bai, P.-A. Fouque, P. Kirchner, D. Stehlé, and W. Wen, "Faster enumeration-based lattice reduction: Root hermite factor $k^{1/(2k)}$ time $k^{k/8+o(k)}$," in *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II*, D. Micciancio and T. Ristenpart, Eds., ser. Lecture Notes in Computer Science, vol. 12171, Springer, 2020, pp. 186–212.

O. Regev, *Lecture notes in lattices in computer science*, Fall 2004.

R. Lindner and C. Peikert, "Better key sizes (and attacks) for lwe-based encryption," in *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, A. Kiayias, Ed., ser. Lecture Notes in Computer Science, vol. 6558, Springer, 2011, pp. 319–339.

References V

M. R. Albrecht, R. Fitzpatrick, and F. Göpfert, "On the efficacy of solving LWE by reduction to unique-svp," in *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*, H.-S. Lee and D.-G. Han, Eds., ser. Lecture Notes in Computer Science, vol. 8565, Springer, 2013, pp. 293–310.

A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, 2003.

D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

References VI

V. Lyubashevsky, C. Peikert, and O. Regev, "A toolkit for ring-lwe cryptography," in *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, T. Johansson and P. Q. Nguyen, Eds., ser. Lecture Notes in Computer Science, vol. 7881, Springer, 2013, pp. 35–54.

C. Baum, I. Damgård, V. Lyubashevsky, S. Oechsner, and C. Peikert, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385.

References VII

I. Damgård, C. Orlandi, A. Takahashi, and M. Tibouchi, "Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices," in *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part I*, J. A. Garay, Ed., ser. Lecture Notes in Computer Science, vol. 12710, Springer, 2021, pp. 99–130.

I. Damgård, V. Pastro, N. P. Smart, and S. Zakarias, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 643–662.

References VIII

V. Lyubashevsky, “Lattice signatures without trapdoors,” in *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, D. Pointcheval and T. Johansson, Eds., ser. Lecture Notes in Computer Science, vol. 7237, Springer, 2012, pp. 738–755.

Gram-Schmidt Orthogonalization

- Given basis $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n]$

Gram-Schmidt Orthogonalization

- Given basis $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n]$
- Define $\tilde{\mathbf{b}}_i$ as follows:

Gram-Schmidt Orthogonalization

- Given basis $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n]$
- Define $\tilde{\mathbf{b}}_i$ as follows:
  - $\tilde{\mathbf{b}}_1 = \mathbf{b}_1$

Gram-Schmidt Orthogonalization

- Given basis $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n]$
- Define $\tilde{\mathbf{b}}_i$ as follows:
  - $\tilde{\mathbf{b}}_1 = \mathbf{b}_1$
  - For $i \in \{2, \ldots, n\}$:

$$\tilde{\mathbf{b}}_i = \mathbf{b}_i - \pi_{\mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})}(\mathbf{b}_i).$$

Gram-Schmidt Orthogonalization

- Given basis $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n]$
- Define $\tilde{\mathbf{b}}_i$ as follows:
  - $\tilde{\mathbf{b}}_1 = \mathbf{b}_1$
  - For $i \in \{2, \ldots, n\}$:

$$\tilde{\mathbf{b}}_i = \mathbf{b}_i - \pi_{\mathsf{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})}(\mathbf{b}_i).$$

- $\tilde{\mathbf{B}} = \left[\tilde{\mathbf{b}}_1 \cdots \tilde{\mathbf{b}}_n\right]$ is the Gram-Schmidt orthogonalization of $\mathbf{B}$

Gram-Schmidt Orthogonalization

- Given basis $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n]$
- Define $\tilde{\mathbf{b}}_i$ as follows:
  - $\tilde{\mathbf{b}}_1 = \mathbf{b}_1$
  - For $i \in \{2, \ldots, n\}$:

$$\tilde{\mathbf{b}}_i = \mathbf{b}_i - \pi_{\mathrm{span}(\mathbf{b}_1,\ldots,\mathbf{b}_{i-1})}(\mathbf{b}_i).$$

- $\tilde{\mathbf{B}} = \left[\tilde{\mathbf{b}}_1 \cdots \tilde{\mathbf{b}}_n\right]$ is the Gram-Schmidt orthogonalization of $\mathbf{B}$
- We define Gram-Schmidt coefficients

$$\mu_{i,j} = \frac{\left\langle \tilde{\mathbf{b}}_j, \mathbf{b}_i \right\rangle}{\left\langle \tilde{\mathbf{b}}_j, \tilde{\mathbf{b}}_j \right\rangle}$$

The LLL Algorithm

- Proposed by Lenstra, Lenstra and Lovász in[13]

[13] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, Dec. 1982.

The LLL Algorithm

- Proposed by Lenstra, Lenstra and Lovász in[13]
- Finds short vectors of length at most $2^{n/2}\lambda_1(\Lambda)$ in polynomial time

[13] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, Dec. 1982.

The LLL Algorithm

- Proposed by Lenstra, Lenstra and Lovász in[13]
- Finds short vectors of length at most $2^{n/2}\lambda_1(\Lambda)$ in polynomial time
- A θ-LLL reduced basis ensures two criteria:

[13] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, Dec. 1982.

The LLL Algorithm

- Proposed by Lenstra, Lenstra and Lovász in[13]
- Finds short vectors of length at most $2^{n/2}\lambda_1(\Lambda)$ in polynomial time
- A θ-LLL reduced basis ensures two criteria:
  - Size-reduced: $|\mu_{i,j}| \leq \frac{1}{2}$ for $1 \leq i \leq n$ and $j < i$

[13] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, Dec. 1982.

The LLL Algorithm

- Proposed by Lenstra, Lenstra and Lovász in[13]
- Finds short vectors of length at most $2^{n/2}\lambda_1(\Lambda)$ in polynomial time
- A θ-LLL reduced basis ensures two criteria:
  - Size-reduced: $|\mu_{i,j}| \leq \frac{1}{2}$ for $1 \leq i \leq n$ and $j < i$
  - Lovász condition: $\theta\|\tilde{\mathbf{b}}_i\|^2 > \|\mu_{i+1,i}\tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}\|^2$ for $1 \leq i < n$

[13] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, Dec. 1982.

The LLL Algorithm

Algorithm 2: The LLL Algorithm[a]

function θ-LLL($\mathbf{B} \in \mathbb{Z}^{m \times n}$)

Compute $\tilde{\mathbf{B}}$

The LLL Algorithm

Algorithm 2: The LLL Algorithm[a]

function θ-LLL($\mathbf{B} \in \mathbb{Z}^{m \times n}$)

Compute $\tilde{\mathbf{B}}$

for $i = 2, \ldots, n$ **do**

for $j = i - 1, \ldots, 1$ **do**

$\mathbf{b}_i = \mathbf{b}_i - \lfloor \mu_{i,j} \rceil \mathbf{b}_j$

The LLL Algorithm

Algorithm 2: The LLL Algorithm[a]

function θ-LLL($\mathbf{B} \in \mathbb{Z}^{m \times n}$)
- Compute $\tilde{\mathbf{B}}$
- **for** $i = 2, \ldots, n$ **do**
  - **for** $j = i - 1, \ldots, 1$ **do**
    - $\mathbf{b}_i = \mathbf{b}_i - \lfloor \mu_{i,j} \rceil \mathbf{b}_j$
- **if** $\exists i$ such that $\theta \|\tilde{\mathbf{b}}_i\|^2 > \|\mu_{i+1,i}\tilde{\mathbf{b}}_i + \tilde{\mathbf{b}}_{i+1}\|^2$ **then**
  - Swap $\mathbf{b}_i$ and $\mathbf{b}_{i+1}$
  - Return θ-LLL($\mathbf{B}$)
- **else**
  - Return $\mathbf{B}$

[a] O. Regev, *Lecture notes in lattices in computer science*, Fall 2004.

The Block Korkin-Zolatarev (BKZ) Algorithm[14]

- LLL reduce input basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$

[14] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," in *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

The Block Korkin-Zolatarev (BKZ) Algorithm[14]

- LLL reduce input basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$
- In jth iteration project block $\mathbf{b}_j, \ldots, \mathbf{b}_{j+k-1}$ to the orthogonal complement of $\operatorname{span}\left(\{\mathbf{b}_i \mid i \in [j-1]\}\right)$

[14] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," in *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

The Block Korkin-Zolatarev (BKZ) Algorithm[14]

- LLL reduce input basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$
- In jth iteration project block $\mathbf{b}_j, \ldots, \mathbf{b}_{j+k-1}$ to the orthogonal complement of $\operatorname{span}(\{\mathbf{b}_i \mid i \in [j-1]\})$
- Run SVP oracle on the projected block to obtain shortest vector $\mathbf{b}'_{\text{new}}$ in the projected lattice

[14] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," in *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

The Block Korkin-Zolatarev (BKZ) Algorithm[14]

- LLL reduce input basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$
- In jth iteration project block $\mathbf{b}_j, \ldots, \mathbf{b}_{j+k-1}$ to the orthogonal complement of $\operatorname{span}(\{\mathbf{b}_i \mid i \in [j-1]\})$
- Run SVP oracle on the projected block to obtain shortest vector $\mathbf{b}'_{\text{new}}$ in the projected lattice
- Recover lattice vector $\mathbf{b}_{\text{new}}$ from $\mathbf{b}'_{\text{new}}$

[14] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," in *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

The Block Korkin-Zolatarev (BKZ) Algorithm[14]

- LLL reduce input basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$
- In jth iteration project block $\mathbf{b}_j, \ldots, \mathbf{b}_{j+k-1}$ to the orthogonal complement of $\mathrm{span}\left(\{\mathbf{b}_i \mid i \in [j-1]\}\right)$
- Run SVP oracle on the projected block to obtain shortest vector $\mathbf{b}'_{\mathrm{new}}$ in the projected lattice
- Recover lattice vector $\mathbf{b}_{\mathrm{new}}$ from $\mathbf{b}'_{\mathrm{new}}$
- If $\mathbf{b}_{\mathrm{new}}$ is new, insert $\mathbf{b}_{\mathrm{new}}$ into list of basis vectors and run LLL on $\{\mathbf{b}_j, \ldots, \mathbf{b}_{j-1}, \mathbf{b}_{\mathrm{new}}, \mathbf{b}_j, \ldots, \mathbf{b}_h\}$ to obtain n linearly independent basis vectors

[14] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," in *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

The Block Korkin-Zolatarev (BKZ) Algorithm[14]

- LLL reduce input basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$
- In jth iteration project block $\mathbf{b}_j, \ldots, \mathbf{b}_{j+k-1}$ to the orthogonal complement of $\operatorname{span}(\{\mathbf{b}_i \mid i \in [j-1]\})$
- Run SVP oracle on the projected block to obtain shortest vector $\mathbf{b}'_{\text{new}}$ in the projected lattice
- Recover lattice vector $\mathbf{b}_{\text{new}}$ from $\mathbf{b}'_{\text{new}}$
- If $\mathbf{b}_{\text{new}}$ is new, insert $\mathbf{b}_{\text{new}}$ into list of basis vectors and run LLL on $\{\mathbf{b}_j, \ldots, \mathbf{b}_{j-1}, \mathbf{b}_{\text{new}}, \mathbf{b}_j, \ldots, \mathbf{b}_h\}$ to obtain n linearly independent basis vectors
- Repeat until no change in n iterations, counter j resets to 1 after $n-k+1$ iterations (one round)

[14] C.-P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," in *Fundamentals of Computation Theory, 8th International Symposium, FCT '91, Gosen, Germany, September 9-13, 1991, Proceedings*, L. Budach, Ed., ser. Lecture Notes in Computer Science, vol. 529, Springer, 1991, pp. 68–85.

BKZ

- Various improvements: early termination, local preprocessing, progressive BKZ

BKZ

- Various improvements: early termination, local preprocessing, progressive BKZ
- Simplified runtime estimate: $\rho \cdot n \cdot t_k$

BKZ

- Various improvements: early termination, local preprocessing, progressive BKZ
- Simplified runtime estimate: $\rho \cdot n \cdot t_k$
  - ρ: number of rounds

BKZ

- Various improvements: early termination, local preprocessing, progressive BKZ
- Simplified runtime estimate: $\rho \cdot n \cdot t_k$
  - ρ: number of rounds
  - t_k: cost of SVP oracle in dimension k

BKZ

- Various improvements: early termination, local preprocessing, progressive BKZ
- Simplified runtime estimate: $\rho \cdot n \cdot t_k$
  - ρ: number of rounds
  - t_k: cost of SVP oracle in dimension k
- Most significant progress in first 8 rounds[15] $\Rightarrow$ LWE-Estimator chooses $\rho = 8$

[15] Y. Chen, "Réduction de réseau et sécurité concrete du chiffrement completement homomorphe," PhD thesis, Paris 7, 2013.

Primal Attack - Reduction of LWE to BDD

BDD_γ

Given a lattice $\Lambda \subset \mathbb{R}^m$ and a target vector $\mathbf{t} \in \mathbb{R}^m$ such that $\mathrm{dist}(\mathbf{t}, \Lambda) < \gamma\lambda_1(\Lambda)$, the (approximate) Bounded Distance Decoding (BDD_γ) is the problem of finding the closest lattice vector $\mathbf{v} \in \Lambda$, i.e., $\mathbf{v} = \arg\min_{\mathbf{v}' \in \Lambda} \|\mathbf{v}' - \mathbf{t}\|$.

Primal Attack - Reduction of LWE to BDD

BDD_γ

Given a lattice $\Lambda \subset \mathbb{R}^m$ and a target vector $\mathbf{t} \in \mathbb{R}^m$ such that $\text{dist}(\mathbf{t}, \Lambda) < \gamma\lambda_1(\Lambda)$, the (approximate) Bounded Distance Decoding (BDD_γ) is the problem of finding the closest lattice vector $\mathbf{v} \in \Lambda$, i.e., $\mathbf{v} = \arg\min_{\mathbf{v}' \in \Lambda} \|\mathbf{v}' - \mathbf{t}\|$.

Consider the LWE lattice $\Lambda_q(\mathbf{A}^\intercal) = \{\mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{y} \in \mathbb{Z}^n : \mathbf{v} = \mathbf{A}^\intercal \mathbf{y} \mod q\}$.

Primal Attack - Reduction of LWE to BDD

BDD$_\gamma$

Given a lattice $\Lambda \subset \mathbb{R}^m$ and a target vector $\mathbf{t} \in \mathbb{R}^m$ such that $\mathrm{dist}(\mathbf{t}, \Lambda) < \gamma\lambda_1(\Lambda)$, the (approximate) Bounded Distance Decoding (BDD$_\gamma$) is the problem of finding the closest lattice vector $\mathbf{v} \in \Lambda$, i.e., $\mathbf{v} = \arg\min_{\mathbf{v}' \in \Lambda} \|\mathbf{v}' - \mathbf{t}\|$.

Consider the LWE lattice $\Lambda_q(\mathbf{A}^\intercal) = \{\mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{y} \in \mathbb{Z}^n : \mathbf{v} = \mathbf{A}^\intercal\mathbf{y} \mod q\}$.

- $\mathbf{z} = \mathbf{A}^\intercal\mathbf{s} + \mathbf{e} \mod q = \mathbf{A}^\intercal\mathbf{s} + \mathbf{e} + q\mathbf{x}$ for some $\mathbf{x} \in \mathbb{Z}^m$

Primal Attack - Reduction of LWE to BDD

BDD_γ

Given a lattice $\Lambda \subset \mathbb{R}^m$ and a target vector $\mathbf{t} \in \mathbb{R}^m$ such that $\text{dist}(\mathbf{t}, \Lambda) < \gamma\lambda_1(\Lambda)$, the (approximate) Bounded Distance Decoding (BDD_γ) is the problem of finding the closest lattice vector $\mathbf{v} \in \Lambda$, i.e., $\mathbf{v} = \arg\min_{\mathbf{v}' \in \Lambda} \|\mathbf{v}' - \mathbf{t}\|$.

Consider the LWE lattice $\Lambda_q(\mathbf{A}^\intercal) = \{\mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{y} \in \mathbb{Z}^n : \mathbf{v} = \mathbf{A}^\intercal \mathbf{y} \mod q\}$.

- $\mathbf{z} = \mathbf{A}^\intercal \mathbf{s} + \mathbf{e} \mod q = \mathbf{A}^\intercal \mathbf{s} + \mathbf{e} + q\mathbf{x}$ for some $\mathbf{x} \in \mathbb{Z}^m$
- $\mathbf{A}^\intercal \mathbf{s} + q\mathbf{x}$

Primal Attack - Reduction of LWE to BDD

BDD_γ

Given a lattice $\Lambda \subset \mathbb{R}^m$ and a target vector $\mathbf{t} \in \mathbb{R}^m$ such that $\mathrm{dist}(\mathbf{t}, \Lambda) < \gamma\lambda_1(\Lambda)$, the (approximate) Bounded Distance Decoding (BDD_γ) is the problem of finding the closest lattice vector $\mathbf{v} \in \Lambda$, i.e., $\mathbf{v} = \arg\min_{\mathbf{v}' \in \Lambda} \|\mathbf{v}' - \mathbf{t}\|$.

Consider the LWE lattice $\Lambda_q(\mathbf{A}^\intercal) = \{\mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{y} \in \mathbb{Z}^n : \mathbf{v} = \mathbf{A}^\intercal \mathbf{y} \mod q\}$.

- $\mathbf{z} = \mathbf{A}^\intercal \mathbf{s} + \mathbf{e} \mod q = \mathbf{A}^\intercal \mathbf{s} + \mathbf{e} + q\mathbf{x}$ for some $\mathbf{x} \in \mathbb{Z}^m$
- $\mathbf{A}^\intercal \mathbf{s} + q\mathbf{x}$
- $\mathrm{dist}(\mathbf{z}, \Lambda_q(\mathbf{A}^\intercal)) = \|\mathbf{e}\|$ and, in general, $\|\mathbf{e}\| < \gamma\lambda_1(\Lambda_q(\mathbf{A}^\intercal))$

Primal Attack - Reduction of LWE to BDD

BDD$_\gamma$

Given a lattice $\Lambda \subset \mathbb{R}^m$ and a target vector $\mathbf{t} \in \mathbb{R}^m$ such that $\mathrm{dist}(\mathbf{t}, \Lambda) < \gamma\lambda_1(\Lambda)$, the (approximate) Bounded Distance Decoding (BDD$_\gamma$) is the problem of finding the closest lattice vector $\mathbf{v} \in \Lambda$, i.e., $\mathbf{v} = \arg\min_{\mathbf{v}' \in \Lambda} \|\mathbf{v}' - \mathbf{t}\|$.

Consider the LWE lattice $\Lambda_q(\mathbf{A}^\intercal) = \{\mathbf{v} \in \mathbb{Z}^m \mid \exists \mathbf{y} \in \mathbb{Z}^n : \mathbf{v} = \mathbf{A}^\intercal \mathbf{y} \mod q\}$.

- $\mathbf{z} = \mathbf{A}^\intercal \mathbf{s} + \mathbf{e} \mod q = \mathbf{A}^\intercal \mathbf{s} + \mathbf{e} + q\mathbf{x}$ for some $\mathbf{x} \in \mathbb{Z}^m$
- $\mathbf{A}^\intercal \mathbf{s} + q\mathbf{x}$
- $\mathrm{dist}(\mathbf{z}, \Lambda_q(\mathbf{A}^\intercal)) = \|\mathbf{e}\|$ and, in general, $\|\mathbf{e}\| < \gamma\lambda_1(\Lambda_q(\mathbf{A}^\intercal))$
- Solving BDD solves LWE

Primal Attack - Variants

- Decoding Attack[16]

[16] R. Lindner and C. Peikert, "Better key sizes (and attacks) for lwe-based encryption," in *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, A. Kiayias, Ed., ser. Lecture Notes in Computer Science, vol. 6558, Springer, 2011, pp. 319–339.

Primal Attack - Variants

- Decoding Attack[16]
  - Reduction step: run BKZ to improve basis quality

[16] R. Lindner and C. Peikert, "Better key sizes (and attacks) for lwe-based encryption," in *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, A. Kiayias, Ed., ser. Lecture Notes in Computer Science, vol. 6558, Springer, 2011, pp. 319–339.

Primal Attack - Variants

- Decoding Attack[16]
  - Reduction step: run BKZ to improve basis quality
  - Decoding step: run a generalized variant of Babai's Nearest Planes (GNP) algorithm to enumerate candidate lattice vectors

[16] R. Lindner and C. Peikert, "Better key sizes (and attacks) for lwe-based encryption," in *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, A. Kiayias, Ed., ser. Lecture Notes in Computer Science, vol. 6558, Springer, 2011, pp. 319–339.

Primal Attack - Variants

- Decoding Attack[16]
  - Reduction step: run BKZ to improve basis quality
  - Decoding step: run a generalized variant of Babai's Nearest Planes (GNP) algorithm to enumerate candidate lattice vectors
  - Choose parameters for BKZ and GNP such that $t_{\text{DEC}} = \rho \cdot (t_{\text{BKZ}} + t_{\text{GNP}})$ is minimized

[16] R. Lindner and C. Peikert, "Better key sizes (and attacks) for lwe-based encryption," in *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, A. Kiayias, Ed., ser. Lecture Notes in Computer Science, vol. 6558, Springer, 2011, pp. 319–339.

Primal Attack - Variants

- Primal uSVP[17]

[17] M. R. Albrecht, R. Fitzpatrick, and F. Göpfert, "On the efficacy of solving LWE by reduction to unique-svp," in *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*, H.-S. Lee and D.-G. Han, Eds., ser. Lecture Notes in Computer Science, vol. 8565, Springer, 2013, pp. 293–310.

Primal Attack - Variants

- Primal uSVP[17]
  - Embed LWE lattice $\Lambda(\mathbf{B})$ in a new lattice $\Lambda(\mathbf{B}')$ with uSVP structure

$$\mathbf{B}' = \begin{pmatrix} \mathbf{B} & \mathbf{z} \\ \mathbf{0}^\intercal & \mu \end{pmatrix}$$

[17] M. R. Albrecht, R. Fitzpatrick, and F. Göpfert, "On the efficacy of solving LWE by reduction to unique-svp," in *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*, H.-S. Lee and D.-G. Han, Eds., ser. Lecture Notes in Computer Science, vol. 8565, Springer, 2013, pp. 293–310.

Primal Attack - Variants

- Primal uSVP[17]
  - Embed LWE lattice $\Lambda(\mathbf{B})$ in a new lattice $\Lambda(\mathbf{B}')$ with uSVP structure

$$\mathbf{B}' = \begin{pmatrix} \mathbf{B} & \mathbf{z} \\ \mathbf{0}^\intercal & \mu \end{pmatrix}$$

  - Unique shortest vector in Λ' is $\mathbf{z}' = [-\mathbf{e}^\intercal, -\mu]^\intercal$ for some μ

[17] M. R. Albrecht, R. Fitzpatrick, and F. Göpfert, "On the efficacy of solving LWE by reduction to unique-svp," in *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*, H.-S. Lee and D.-G. Han, Eds., ser. Lecture Notes in Computer Science, vol. 8565, Springer, 2013, pp. 293–310.

Primal Attack - Variants

- Primal uSVP[17]
  - Embed LWE lattice $\Lambda(\mathbf{B})$ in a new lattice $\Lambda(\mathbf{B}')$ with uSVP structure

$$\mathbf{B}' = \begin{pmatrix} \mathbf{B} & \mathbf{z} \\ \mathbf{0}^\intercal & \mu \end{pmatrix}$$

  - Unique shortest vector in Λ' is $\mathbf{z}' = [-\mathbf{e}^\intercal, -\mu]^\intercal$ for some μ
  - Run BKZ to find $\mathbf{z}'$ and recover $\mathbf{s}$

[17] M. R. Albrecht, R. Fitzpatrick, and F. Göpfert, "On the efficacy of solving LWE by reduction to unique-svp," in *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*, H.-S. Lee and D.-G. Han, Eds., ser. Lecture Notes in Computer Science, vol. 8565, Springer, 2013, pp. 293–310.

Reduction of LWE to SIS[18]

- Consider the dual SIS lattice $\Lambda_q(\mathbf{A}^\top)^\perp = \{\mathbf{y} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{y} = \mathbf{0} \mod q\}$

[18] R. Lindner and C. Peikert, "Better key sizes (and attacks) for lwe-based encryption," in *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, A. Kiayias, Ed., ser. Lecture Notes in Computer Science, vol. 6558, Springer, 2011, pp. 319–339.

Reduction of LWE to SIS[18]

- Consider the dual SIS lattice $\Lambda_q(\mathbf{A}^\intercal)^\perp = \{\mathbf{y} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{y} = \mathbf{0} \mod q\}$
- For a lattice vector $\mathbf{v} \in \Lambda_q(\mathbf{A}^\intercal)^\perp$ it holds that

$$\begin{aligned}\langle \mathbf{v}, \mathbf{z} \rangle &= \langle \mathbf{v}, \mathbf{A}^\intercal \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle = \langle \mathbf{v}\mathbf{A}^\intercal, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle \\ &= \langle \mathbf{v}, \mathbf{e} \rangle \mod q\end{aligned}$$

[18] R. Lindner and C. Peikert, "Better key sizes (and attacks) for lwe-based encryption," in *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, A. Kiayias, Ed., ser. Lecture Notes in Computer Science, vol. 6558, Springer, 2011, pp. 319–339.

Reduction of LWE to SIS[18]

- Consider the dual SIS lattice $\Lambda_q(\mathbf{A}^\intercal)^\perp = \{\mathbf{y} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{y} = \mathbf{0} \mod q\}$
- For a lattice vector $\mathbf{v} \in \Lambda_q(\mathbf{A}^\intercal)^\perp$ it holds that

$$\begin{aligned}\langle \mathbf{v}, \mathbf{z} \rangle &= \langle \mathbf{v}, \mathbf{A}^\intercal \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle = \langle \mathbf{v}\mathbf{A}^\intercal, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle \\ &= \langle \mathbf{v}, \mathbf{e} \rangle \mod q\end{aligned}$$

- Test whether $\langle \mathbf{v}, \mathbf{e} \rangle \mod q$ corresponds to Gaussian of width $\|\mathbf{v}\| \cdot s$

[18] R. Lindner and C. Peikert, “Better key sizes (and attacks) for lwe-based encryption,” in *Topics in Cryptology - CT-RSA 2011 - The Cryptographers’ Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, A. Kiayias, Ed., ser. Lecture Notes in Computer Science, vol. 6558, Springer, 2011, pp. 319–339.

Reduction of LWE to SIS[18]

- Consider the dual SIS lattice $\Lambda_q(\mathbf{A}^\intercal)^\perp = \{\mathbf{y} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{y} = \mathbf{0} \mod q\}$
- For a lattice vector $\mathbf{v} \in \Lambda_q(\mathbf{A}^\intercal)^\perp$ it holds that

$$\begin{aligned} \langle \mathbf{v}, \mathbf{z} \rangle &= \langle \mathbf{v}, \mathbf{A}^\intercal \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle = \langle \mathbf{v}\mathbf{A}^\intercal, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle \\ &= \langle \mathbf{v}, \mathbf{e} \rangle \mod q \end{aligned}$$

- Test whether $\langle \mathbf{v}, \mathbf{e} \rangle \mod q$ corresponds to Gaussian of width $\|\mathbf{v}\| \cdot s$
- Advantage is close to $\exp(-\pi(\|\mathbf{v}\| s/q)^2)$

[18] R. Lindner and C. Peikert, "Better key sizes (and attacks) for lwe-based encryption," in *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, A. Kiayias, Ed., ser. Lecture Notes in Computer Science, vol. 6558, Springer, 2011, pp. 319–339.

Reduction of LWE to SIS[18]

- Consider the dual SIS lattice $\Lambda_q(\mathbf{A}^\intercal)^\perp = \{\mathbf{y} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{y} = \mathbf{0} \mod q\}$
- For a lattice vector $\mathbf{v} \in \Lambda_q(\mathbf{A}^\intercal)^\perp$ it holds that

$$\begin{aligned} \langle \mathbf{v}, \mathbf{z} \rangle &= \langle \mathbf{v}, \mathbf{A}^\intercal \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle = \langle \mathbf{v}\mathbf{A}^\intercal, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle \\ &= \langle \mathbf{v}, \mathbf{e} \rangle \mod q \end{aligned}$$

- Test whether $\langle \mathbf{v}, \mathbf{e} \rangle \mod q$ corresponds to Gaussian of width $\|\mathbf{v}\| \cdot s$
- Advantage is close to $\exp(-\pi(\|\mathbf{v}\| s/q)^2)$
- Finding a short non-zero vector $\mathbf{v}$ in the dual SIS lattice solves Decision-LWE

[18] R. Lindner and C. Peikert, "Better key sizes (and attacks) for lwe-based encryption," in *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, A. Kiayias, Ed., ser. Lecture Notes in Computer Science, vol. 6558, Springer, 2011, pp. 319–339.

The Blum, Kalai and Wassermann (BKW) Algorithm[19]

- Reduce dimension of input matrix $\mathbf{A}$ by finding collisions of its column vectors

[19] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, 2003.

The Blum, Kalai and Wassermann (BKW) Algorithm[19]

- Reduce dimension of input matrix $\mathbf{A}$ by finding collisions of its column vectors
- In each step eliminate b components of the samples

[19] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, 2003.

The Blum, Kalai and Wassermann (BKW) Algorithm[19]

- Reduce dimension of input matrix $\mathbf{A}$ by finding collisions of its column vectors
- In each step eliminate b components of the samples
  - $z_i = \langle \mathbf{a}_i \mathbf{s} \rangle + e_i$ and $z_j = \langle \mathbf{a}_j \mathbf{s} \rangle + e_j$ where $\mathbf{a}_i$ and $\mathbf{a}_j$ match in the last b components

[19] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, 2003.

The Blum, Kalai and Wassermann (BKW) Algorithm[19]

- Reduce dimension of input matrix $\mathbf{A}$ by finding collisions of its column vectors
- In each step eliminate b components of the samples
  - $z_i = \langle \mathbf{a}_i \mathbf{s} \rangle + e_i$ and $z_j = \langle \mathbf{a}_j \mathbf{s} \rangle + e_j$ where $\mathbf{a}_i$ and $\mathbf{a}_j$ match in the last b components
  - $\mathbf{a}_i - \mathbf{a}_j$ has only zero entries in the last b components

[19] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, 2003.

The Blum, Kalai and Wassermann (BKW) Algorithm[19]

- Reduce dimension of input matrix $\mathbf{A}$ by finding collisions of its column vectors
- In each step eliminate b components of the samples
  - $z_i = \langle \mathbf{a}_i \mathbf{s} \rangle + e_i$ and $z_j = \langle \mathbf{a}_j \mathbf{s} \rangle + e_j$ where $\mathbf{a}_i$ and $\mathbf{a}_j$ match in the last b components
  - $\mathbf{a}_i - \mathbf{a}_j$ has only zero entries in the last b components
  - $z_i - z_j = \langle \mathbf{a}_i - \mathbf{a}_j \rangle + e_i - e_j$

[19] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, 2003.

The Blum, Kalai and Wassermann (BKW) Algorithm[19]

- Reduce dimension of input matrix $\mathbf{A}$ by finding collisions of its column vectors
- In each step eliminate b components of the samples
  - $z_i = \langle \mathbf{a}_i \mathbf{s} \rangle + e_i$ and $z_j = \langle \mathbf{a}_j \mathbf{s} \rangle + e_j$ where $\mathbf{a}_i$ and $\mathbf{a}_j$ match in the last b components
  - $\mathbf{a}_i - \mathbf{a}_j$ has only zero entries in the last b components
  - $z_i - z_j = \langle \mathbf{a}_i - \mathbf{a}_j \rangle + e_i - e_j$
- Repeat a times until only small number of components left

[19] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, 2003.

The Blum, Kalai and Wassermann (BKW) Algorithm[19]

- Reduce dimension of input matrix $\mathbf{A}$ by finding collisions of its column vectors
- In each step eliminate b components of the samples
    - $z_i = \langle \mathbf{a}_i \mathbf{s} \rangle + e_i$ and $z_j = \langle \mathbf{a}_j \mathbf{s} \rangle + e_j$ where $\mathbf{a}_i$ and $\mathbf{a}_j$ match in the last b components
    - $\mathbf{a}_i - \mathbf{a}_j$ has only zero entries in the last b components
    - $z_i - z_j = \langle \mathbf{a}_i - \mathbf{a}_j \rangle + e_i - e_j$
- Repeat a times until only small number of components left
- Recover secret vector by means of hypothesis testing and back substitution

[19] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, 2003.

The Blum, Kalai and Wassermann (BKW) Algorithm[19]

- Reduce dimension of input matrix $\mathbf{A}$ by finding collisions of its column vectors
- In each step eliminate b components of the samples
  - $z_i = \langle \mathbf{a}_i \mathbf{s} \rangle + e_i$ and $z_j = \langle \mathbf{a}_j \mathbf{s} \rangle + e_j$ where $\mathbf{a}_i$ and $\mathbf{a}_j$ match in the last b components
  - $\mathbf{a}_i - \mathbf{a}_j$ has only zero entries in the last b components
  - $z_i - z_j = \langle \mathbf{a}_i - \mathbf{a}_j \rangle + e_i - e_j$
- Repeat a times until only small number of components left
- Recover secret vector by means of hypothesis testing and back substitution
- Runtime complexity $\approx (a^2 n) \cdot \frac{q^b}{2}$

[19] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, 2003.

The Blum, Kalai and Wassermann (BKW) Algorithm[19]

- Reduce dimension of input matrix $\mathbf{A}$ by finding collisions of its column vectors
- In each step eliminate b components of the samples
  - $z_i = \langle \mathbf{a}_i \mathbf{s} \rangle + e_i$ and $z_j = \langle \mathbf{a}_j \mathbf{s} \rangle + e_j$ where $\mathbf{a}_i$ and $\mathbf{a}_j$ match in the last b components
  - $\mathbf{a}_i - \mathbf{a}_j$ has only zero entries in the last b components
  - $z_i - z_j = \langle \mathbf{a}_i - \mathbf{a}_j \rangle + e_i - e_j$
- Repeat a times until only small number of components left
- Recover secret vector by means of hypothesis testing and back substitution
- Runtime complexity $\approx (a^2 n) \cdot \frac{q^b}{2}$
- Estimator uses a variant called Coded-BKW

[19] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, 2003.

Other Approaches

- Exhaustive search: Meet-In-The-Middle attack

Other Approaches

- Exhaustive search: Meet-In-The-Middle attack
- Arora-GB: solve system of non-linear equations

Other Approaches

- Exhaustive search: Meet-In-The-Middle attack
- Arora-GB: solve system of non-linear equations
- In practice much slower than other algorithms

Solving SIS - Dual Attack[20]

- Finding short vector $\mathbf{v} \in \Lambda(\mathbf{A}^\intercal)^\perp$ with $\|\mathbf{v}\| \leq \beta$ in the dual SIS lattice solves SIS

[20] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

Solving SIS - Dual Attack[20]

- Finding short vector $\mathbf{v} \in \Lambda(\mathbf{A}^\intercal)^\perp$ with $\|\mathbf{v}\| \leq \beta$ in the dual SIS lattice solves SIS
- Lattice reduction yields $\mathbf{b}_1$ of length length $\|\mathbf{b}_1\| = \delta^m q^{n/m}$ (under the assumption that $\det(\Lambda(\mathbf{A}^\intercal)^\perp) \approx q^n$)

[20] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

Solving SIS - Dual Attack[20]

- Finding short vector $\mathbf{v} \in \Lambda(\mathbf{A}^\intercal)^\perp$ with $\|\mathbf{v}\| \le \beta$ in the dual SIS lattice solves SIS
- Lattice reduction yields $\mathbf{b}_1$ of length length $\|\mathbf{b}_1\| = \delta^m q^{n/m}$ (under the assumption that $\det(\Lambda(\mathbf{A}^\intercal)^\perp) \approx q^n$)
- Optimal subdimension is $m' = \sqrt{\frac{n \log q}{\log \delta}}$

[20] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

Solving SIS - Dual Attack[20]

- Finding short vector $\mathbf{v} \in \Lambda(\mathbf{A}^\intercal)^\perp$ with $\|\mathbf{v}\| \leq \beta$ in the dual SIS lattice solves SIS
- Lattice reduction yields $\mathbf{b}_1$ of length length $\|\mathbf{b}_1\| = \delta^m q^{n/m}$ (under the assumption that $\det(\Lambda(\mathbf{A}^\intercal)^\perp) \approx q^n$)
- Optimal subdimension is $m' = \sqrt{\frac{n \log q}{\log \delta}}$
- Log root Hermite Factor for optimal subdimension is

$$\log \delta = \frac{\log^2 \beta}{4n \log q}$$

[20] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

Solving SIS - Dual Attack[20]

- Finding short vector $\mathbf{v} \in \Lambda(\mathbf{A}^\intercal)^\perp$ with $\|\mathbf{v}\| \leq \beta$ in the dual SIS lattice solves SIS
- Lattice reduction yields $\mathbf{b}_1$ of length length $\|\mathbf{b}_1\| = \delta^m q^{n/m}$ (under the assumption that $\det(\Lambda(\mathbf{A}^\intercal)^\perp) \approx q^n$)
- Optimal subdimension is $m' = \sqrt{\frac{n \log q}{\log \delta}}$
- Log root Hermite Factor for optimal subdimension is

$$\log \delta = \frac{\log^2 \beta}{4n \log q}$$

- Similar result in Rückert and Schneider (2010, IACR Cryptol. ePrint Arch.)

[20] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

Solving SIS - Combinatorial Attack[21]

- Find $\mathbf{v} \in \Lambda(\mathbf{A}^\intercal)^\perp$ with coefficients bounded by β, i.e., $\|\mathbf{v}\|_\infty \leq \beta$

[21] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

Solving SIS - Combinatorial Attack[21]

- Find $\mathbf{v} \in \Lambda(\mathbf{A}^\intercal)^\perp$ with coefficients bounded by β, i.e., $\|\mathbf{v}\|_\infty \leq \beta$
- Divide columns of $\mathbf{A}$ into 2^k sets of $m/2^k$ vectors

[21] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

Solving SIS - Combinatorial Attack[21]

- Find $\mathbf{v} \in \Lambda(\mathbf{A}^\intercal)^\perp$ with coefficients bounded by β, i.e., $\|\mathbf{v}\|_\infty \leq \beta$
- Divide columns of $\mathbf{A}$ into 2^k sets of $m/2^k$ vectors
- Compute a new set of all linear combinations of the vectors for each set with coefficients bounded by β

[21] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

Solving SIS - Combinatorial Attack[21]

- Find $\mathbf{v} \in \Lambda(\mathbf{A}^\intercal)^\perp$ with coefficients bounded by β, i.e., $\|\mathbf{v}\|_\infty \leq \beta$
- Divide columns of $\mathbf{A}$ into 2^k sets of $m/2^k$ vectors
- Compute a new set of all linear combinations of the vectors for each set with coefficients bounded by β

$\Rightarrow$ $L = (2\beta + 1)^{m/2^k}$ vectors per set

[21] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

Solving SIS - Combinatorial Attack[21]

- Find $\mathbf{v} \in \Lambda(\mathbf{A}^\intercal)^\perp$ with coefficients bounded by β, i.e., $\|\mathbf{v}\|_\infty \leq \beta$
- Divide columns of $\mathbf{A}$ into 2^k sets of $m/2^k$ vectors
- Compute a new set of all linear combinations of the vectors for each set with coefficients bounded by β

$\Rightarrow$ $L = (2\beta + 1)^{m/2^k}$ vectors per set

- In each step pairwise combine vectors of two sets such that $\log_q L$ components are eliminated

[21] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

Solving SIS - Combinatorial Attack[21]

- Find $\mathbf{v} \in \Lambda(\mathbf{A}^\intercal)^\perp$ with coefficients bounded by β, i.e., $\|\mathbf{v}\|_\infty \leq \beta$
- Divide columns of $\mathbf{A}$ into 2^k sets of $m/2^k$ vectors
- Compute a new set of all linear combinations of the vectors for each set with coefficients bounded by β

$\Rightarrow$ $L = (2\beta + 1)^{m/2^k}$ vectors per set

- In each step pairwise combine vectors of two sets such that $\log_q L$ components are eliminated
- Overall cost dominated by list size L, total cost $\approx 2^k \cdot L \cdot \log_2(q) \cdot n$

[21] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191, ISBN: 978-3-540-88702-7.

Ring-SIS

RSIS

Let $\mathcal{R}_q$ be the quotient ring $\mathbb{Z}_q[x] / \langle x^n + 1 \rangle$. Given $a_1, \ldots, a_m \in \mathcal{R}_q$ chosen independently from the uniform distribution, the Ring-SIS problem $\mathrm{RSIS}_{n,q,m,\beta}$ asks to find $s_1, \ldots, s_m \in \mathcal{R}$ such that $\sum_{i=1}^{m} \mathbf{a}_i \cdot s_i = 0 \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = [s_1, \ldots, s_m]^\intercal \in \mathcal{R}^m$.

Ring-SIS

RSIS

Let $\mathcal{R}_q$ be the quotient ring $\mathbb{Z}_q[x] / \langle x^n + 1 \rangle$. Given $a_1, \ldots, a_m \in \mathcal{R}_q$ chosen independently from the uniform distribution, the Ring-SIS problem $\text{RSIS}_{n,q,m,\beta}$ asks to find $s_1, \ldots, s_m \in \mathcal{R}$ such that $\sum_{i=1}^{m} \mathbf{a}_i \cdot s_i = 0 \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = [s_1, \ldots, s_m]^\mathsf{T} \in \mathcal{R}^m$.

- Interpret $r \in \mathcal{R}$ as an n dimensional vector s.t. $r = \sum_{i=0}^{n-1} r_i x^i$

Ring-SIS

RSIS

Let $\mathcal{R}_q$ be the quotient ring $\mathbb{Z}_q[x] / \langle x^n + 1 \rangle$. Given $a_1, \ldots, a_m \in \mathcal{R}_q$ chosen independently from the uniform distribution, the Ring-SIS problem $\mathrm{RSIS}_{n,q,m,\beta}$ asks to find $s_1, \ldots, s_m \in \mathcal{R}$ such that $\sum_{i=1}^{m} \mathbf{a}_i \cdot s_i = 0 \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = [s_1, \ldots, s_m]^\mathsf{T} \in \mathcal{R}^m$.

- Interpret $r \in \mathcal{R}$ as an n dimensional vector s.t. $r = \sum_{i=0}^{n-1} r_i x^i$
- Each a_i in RSIS corresponds to an $n \times n$ block in the standard SIS matrix $\mathbf{A}_{\mathrm{SIS}}$ obtained by rotation:

$$\mathrm{Rot}(a) = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}$$

Ring-SIS

RSIS

Let $\mathcal{R}_q$ be the quotient ring $\mathbb{Z}_q[x] / \langle x^n + 1 \rangle$. Given $a_1, \ldots, a_m \in \mathcal{R}_q$ chosen independently from the uniform distribution, the Ring-SIS problem $\mathrm{RSIS}_{n,q,m,\beta}$ asks to find $s_1, \ldots, s_m \in \mathcal{R}$ such that $\sum_{i=1}^{m} \mathbf{a}_i \cdot s_i = 0 \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = [s_1, \ldots, s_m]^{\mathsf{T}} \in \mathcal{R}^m$.

- Interpret $r \in \mathcal{R}$ as an n dimensional vector s.t. $r = \sum_{i=0}^{n-1} r_i x^i$
- Each a_i in RSIS corresponds to an $n \times n$ block in the standard SIS matrix $\mathbf{A}_{\mathrm{SIS}}$ obtained by rotation:

$$\mathrm{Rot}(a) = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}$$

$\Rightarrow \mathbf{A}_{\mathrm{SIS}} = [\mathrm{Rot}(a_1) \mid \cdots \mid \mathrm{Rot}(a_m)]$

Ring-SIS

RSIS

Let $\mathcal{R}_q$ be the quotient ring $\mathbb{Z}_q[x] / \langle x^n + 1 \rangle$. Given $a_1, \ldots, a_m \in \mathcal{R}_q$ chosen independently from the uniform distribution, the Ring-SIS problem $\mathrm{RSIS}_{n,q,m,\beta}$ asks to find $s_1, \ldots, s_m \in \mathcal{R}$ such that $\sum_{i=1}^{m} \mathbf{a}_i \cdot s_i = 0 \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = [s_1, \ldots, s_m]^\mathsf{T} \in \mathcal{R}^m$.

- Interpret $r \in \mathcal{R}$ as an n dimensional vector s.t. $r = \sum_{i=0}^{n-1} r_i x^i$
- Each a_i in RSIS corresponds to an $n \times n$ block in the standard SIS matrix $\mathbf{A}_{\mathrm{SIS}}$ obtained by rotation:

$$\mathrm{Rot}(a) = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}$$

$\Rightarrow$ $\mathbf{A}_{\mathrm{SIS}} = [\mathrm{Rot}(a_1) \mid \cdots \mid \mathrm{Rot}(a_m)]$

- $\mathrm{RSIS}_{n,q,m,\beta} \longrightarrow \mathrm{SIS}_{n,q,m \cdot n,\beta}$

Module-SIS

MSIS

Let $\mathcal{R}^d$ be a module with ring dimension n and module rank d. Given $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathcal{R}_q^d$ chosen independently from the uniform distribution, the Module-SIS problem $\mathrm{MSIS}_{n,d,q,m,\beta}$ asks to find $s_1, \ldots, s_m \in \mathcal{R}$ such that $\sum_{i=1}^m \mathbf{a}_i \cdot s_i = \mathbf{0} \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = [s_1, \ldots, s_m]^\mathsf{T} \in \mathcal{R}^m$.

Module-SIS

MSIS

Let $\mathcal{R}^d$ be a module with ring dimension n and module rank d. Given $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathcal{R}_q^d$ chosen independently from the uniform distribution, the Module-SIS problem $\mathrm{MSIS}_{n,d,q,m,\beta}$ asks to find $s_1, \ldots, s_m \in \mathcal{R}$ such that $\sum_{i=1}^m \mathbf{a}_i \cdot s_i = \mathbf{0} \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = [s_1, \ldots, s_m]^\intercal \in \mathcal{R}^m$.

- Module element $\mathbf{a}_i$ corresponds to $n \cdot d \times n$ block in $\mathbf{A}$ and for $\mathbf{A}$ can be viewed as a $n \cdot d \times n \cdot m$ matrix

Module-SIS

MSIS

Let $\mathcal{R}^d$ be a module with ring dimension n and module rank d. Given $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathcal{R}_q^d$ chosen independently from the uniform distribution, the Module-SIS problem $\mathrm{MSIS}_{n,d,q,m,\beta}$ asks to find $s_1, \ldots, s_m \in \mathcal{R}$ such that $\sum_{i=1}^{m} \mathbf{a}_i \cdot s_i = \mathbf{0} \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = [s_1, \ldots, s_m]^\intercal \in \mathcal{R}^m$.

$$
\begin{array}{cc}
 & \overbrace{\hphantom{\mathrm{Rot}(\boldsymbol{a}_{1,1}) \; \mathrm{Rot}(\boldsymbol{a}_{1,2}) \; \cdots \; \mathrm{Rot}(\boldsymbol{a}_{1,m})}}^{n \cdot m} \\
n \cdot d & \left[\begin{array}{c|c|c|c}
\mathrm{Rot}(\boldsymbol{a}_{1,1}) & \mathrm{Rot}(\boldsymbol{a}_{1,2}) & \cdots & \mathrm{Rot}(\boldsymbol{a}_{1,m}) \\ \hline
\vdots & \vdots & \ddots & \vdots \\ \hline
\mathrm{Rot}(\boldsymbol{a}_{d,1}) & \mathrm{Rot}(\boldsymbol{a}_{d,2}) & \cdots & \mathrm{Rot}(\boldsymbol{a}_{d,m})
\end{array}\right]
\end{array}
$$

Module-SIS

MSIS

Let $\mathcal{R}^d$ be a module with ring dimension n and module rank d. Given $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathcal{R}_q^d$ chosen independently from the uniform distribution, the Module-SIS problem $\mathrm{MSIS}_{n,d,q,m,\beta}$ asks to find $s_1, \ldots, s_m \in \mathcal{R}$ such that $\sum_{i=1}^m \mathbf{a}_i \cdot s_i = \mathbf{0} \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = [s_1, \ldots, s_m]^\intercal \in \mathcal{R}^m$.

- Module element $\mathbf{a}_i$ corresponds to $n \cdot d \times n$ block in $\mathbf{A}$ and for $\mathbf{A}$ can be viewed as a $n \cdot d \times n \cdot m$ matrix
- $\mathrm{MSIS}_{n,d,q,m,\beta} \longrightarrow \mathrm{SIS}_{n\cdot d,q,m\cdot n,\beta}$

Ring-LWE and Module-LWE

RLWE Distribution

Let χ be the error distribution on $\mathbb{T}_{\mathcal{R}^\perp} = K_\mathbb{R}/\mathcal{R}^\perp$ and $s \in \mathcal{R}^\perp$ be the secret. Then, we define $\mathcal{A}^{(\mathcal{R})}_{q,s,\chi}$ as the Ring-LWE (RLWE) distribution on $\mathcal{R}_q \times \mathbb{T}_{\mathcal{R}^\perp}$ obtained by choosing $a \in \mathbb{R}_q$ uniformly at random and an error term $e \in \mathbb{T}_{\mathcal{R}^\perp}$ according to χ, and returning samples $(a, (a \cdot s)/q + e)$.

Ring-LWE and Module-LWE

RLWE Distribution

Let χ be the error distribution on $\mathbb{T}_{\mathcal{R}^\perp} = K_\mathbb{R}/\mathcal{R}^\perp$ and $s \in \mathcal{R}^\perp$ be the secret. Then, we define $\mathcal{A}^{(\mathcal{R})}_{q,s,\chi}$ as the Ring-LWE (RLWE) distribution on $\mathcal{R}_q \times \mathbb{T}_{\mathcal{R}^\perp}$ obtained by choosing $a \in \mathbb{R}_q$ uniformly at random and an error term $e \in \mathbb{T}_{\mathcal{R}^\perp}$ according to χ, and returning samples $(a, (a \cdot s)/q + e)$.

MLWE Distribution

Let χ be the error distribution on $\mathbb{T}_{\mathcal{R}^\perp}$ and $\mathbf{s} \in (\mathcal{R}^\perp)^d$ be the secret vector. Then, we define $\mathcal{A}^{(\mathcal{M})}_{q,\mathbf{s},\chi}$ as the Module-LWE (MLWE) distribution on $(\mathcal{R}_q)^d \times \mathbb{T}_{\mathcal{R}^\perp}$ obtained by choosing $\mathbf{a} \in (\mathbb{R}_q)^d$ uniformly at random and an error term $e \in \mathbb{T}_{\mathcal{R}^\perp}$ according to χ, and returning samples $(\mathbf{a}, \frac{1}{q}\langle \mathbf{a}, \mathbf{s}\rangle + e)$.

- $\mathrm{RLWE}_{n,q,m,\chi} \longrightarrow \mathrm{LWE}_{n,q,m\cdot n,\chi}$

RLWE Distribution

Let χ be the error distribution on $\mathbb{T}_{\mathcal{R}^\perp} = K_\mathbb{R}/\mathcal{R}^\perp$ and $s \in \mathcal{R}^\perp$ be the secret. Then, we define $\mathcal{A}^{(\mathcal{R})}_{q,s,\chi}$ as the Ring-LWE (RLWE) distribution on $\mathcal{R}_q \times \mathbb{T}_{\mathcal{R}^\perp}$ obtained by choosing $a \in \mathbb{R}_q$ uniformly at random and an error term $e \in \mathbb{T}_{\mathcal{R}^\perp}$ according to χ, and returning samples $(a, (a \cdot s)/q + e)$.

MLWE Distribution

Let χ be the error distribution on $\mathbb{T}_{\mathcal{R}^\perp}$ and $\mathbf{s} \in (\mathcal{R}^\perp)^d$ be the secret vector. Then, we define $\mathcal{A}^{(\mathcal{M})}_{q,\mathbf{s},\chi}$ as the Module-LWE (MLWE) distribution on $(\mathcal{R}_q)^d \times \mathbb{T}_{\mathcal{R}^\perp}$ obtained by choosing $\mathbf{a} \in (\mathbb{R}_q)^d$ uniformly at random and an error term $e \in \mathbb{T}_{\mathcal{R}^\perp}$ according to χ, and returning samples $(\mathbf{a}, \frac{1}{q}\langle \mathbf{a}, \mathbf{s}\rangle + e)$.

- $\mathrm{RLWE}_{n,q,m,\chi} \longrightarrow \mathrm{LWE}_{n,q,m\cdot n,\chi}$
- $\mathrm{MLWE}_{n,d,q,m,\chi} \longrightarrow \mathrm{LWE}_{n\cdot d,q,m\cdot n,\chi}$

Statistically Secure MLWE (Gaussian Variant)[22]

- Given mth cyclomatic number field K of degree $n = \phi(m)$ and integer $q \geq 2$ and

[22] V. Lyubashevsky, C. Peikert, and O. Regev, "A toolkit for ring-lwe cryptography," in *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, T. Johansson and P. Q. Nguyen, Eds., ser. Lecture Notes in Computer Science, vol. 7881, Springer, 2013, pp. 35–54.

Statistically Secure MLWE (Gaussian Variant)[22]

- Given mth cyclomatic number field K of degree $n = \phi(m)$ and integer $q \geq 2$ and
- $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ with positive integers $m \leq m + d \leq \text{poly}(n)$ and uniformly random matrix $\bar{\mathbf{A}}$

[22] V. Lyubashevsky, C. Peikert, and O. Regev, "A toolkit for ring-lwe cryptography," in *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, T. Johansson and P. Q. Nguyen, Eds., ser. Lecture Notes in Computer Science, vol. 7881, Springer, 2013, pp. 35–54.

Statistically Secure MLWE (Gaussian Variant)[22]

- Given mth cyclomatic number field K of degree $n = \phi(m)$ and integer $q \geq 2$ and
- $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ with positive integers $m \leq m + d \leq \text{poly}(n)$ and uniformly random matrix $\bar{\mathbf{A}}$
- Let $\mathbf{x} \in (\mathcal{R}_q)^{[m+d]}$ where each component is chosen from a discrete Gaussian distribution of parameter $s > 2n \cdot q^{m/(m+d)+2/(n(m+d))}$ over $\mathcal{R}$

[22] V. Lyubashevsky, C. Peikert, and O. Regev, "A toolkit for ring-lwe cryptography," in *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, T. Johansson and P. Q. Nguyen, Eds., ser. Lecture Notes in Computer Science, vol. 7881, Springer, 2013, pp. 35–54.

Statistically Secure MLWE (Gaussian Variant)[22]

- Given mth cyclomatic number field K of degree $n = \phi(m)$ and integer $q \geq 2$ and
- $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ with positive integers $m \leq m + d \leq \text{poly}(n)$ and uniformly random matrix $\bar{\mathbf{A}}$
- Let $\mathbf{x} \in (\mathcal{R}_q)^{[m+d]}$ where each component is chosen from a discrete Gaussian distribution of parameter $s > 2n \cdot q^{m/(m+d)+2/(n(m+d))}$ over $\mathcal{R}$
- Then $\mathbf{A}\mathbf{x} \in (\mathcal{R}_q)^{[m]}$ is within statistical distance $2^{-\Omega(n)}$ of the uniform distribution over $(\mathcal{R}_q)^{[m]}$)

[22] V. Lyubashevsky, C. Peikert, and O. Regev, "A toolkit for ring-lwe cryptography," in *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, T. Johansson and P. Q. Nguyen, Eds., ser. Lecture Notes in Computer Science, vol. 7881, Springer, 2013, pp. 35–54.

Statistically Secure MLWE (Uniform Variant)[23]

- Given $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ as before, $1 < d_2 < n$, where d_2 is a power of 2 and a prime q congruent to $2d_2 + 1 \pmod{4d_2}$

[23] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385.

Statistically Secure MLWE (Uniform Variant)[23]

- Given $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ as before, $1 < d_2 < n$, where d_2 is a power of 2 and a prime q congruent to $2d_2 + 1 \pmod{4d_2}$
- If $\beta \in \mathbb{R}$ such that $\beta_{min} \leq \beta \leq \beta_{max}$ with

$$\beta_{min} = \frac{q^{m/(m+d)} \cdot 2^{2\mathrm{sec}/((m+d)\cdot n)}}{2}$$

$$\beta_{max} = \frac{1}{2\sqrt{d_2}} \cdot q^{1/d_2} - 1$$

[23] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385.

Statistically Secure MLWE (Uniform Variant)[23]

- Given $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ as before, $1 < d_2 < n$, where d_2 is a power of 2 and a prime q congruent to $2d_2 + 1 \pmod{4d_2}$
- If $\beta \in \mathbb{R}$ such that $\beta_{min} \leq \beta \leq \beta_{max}$ with

$$\beta_{min} = \frac{q^{m/(m+d)} \cdot 2^{2\mathsf{sec}/((m+d)\cdot n)}}{2}$$

$$\beta_{max} = \frac{1}{2\sqrt{d_2}} \cdot q^{1/d_2} - 1$$

[23] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385.

Statistically Secure MLWE (Uniform Variant)[23]

- Given $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ as before, $1 < d_2 < n$, where d_2 is a power of 2 and a prime q congruent to $2d_2 + 1 \pmod{4d_2}$
- If $\beta \in \mathbb{R}$ such that $\beta_{min} \leq \beta \leq \beta_{max}$ with

$$\beta_{min} = \frac{q^{m/(m+d)} \cdot 2^{2\sec/((m+d)\cdot n)}}{2}$$
$$\beta_{max} = \frac{1}{2\sqrt{d_2}} \cdot q^{1/d_2} - 1$$

then any (all-powerful) algorithm $\mathcal{A}$ has advantage at most $2^{-\sec}$ in distinguishing $\mathbf{A}\mathbf{x} \in (\mathcal{R}_q)^{[m]}$ from the uniform distribution, where $\mathbf{x}$ is chosen uniformly random with $\|\mathbf{x}\|_\infty \leq \beta$

[23] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385.

Statistical MSIS[24]

- Given $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ as before

[24] I. Damgård, C. Orlandi, A. Takahashi, *et al.*, "Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices," in *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part I*, J. A. Garay, Ed., ser. Lecture Notes in Computer Science, vol. 12710, Springer, 2021, pp. 99–130.

Statistical MSIS[24]

- Given $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ as before
- It should be hard to find $\mathbf{r}, \mathbf{r}' \in \mathcal{R}_q^{m+d}$ of ℓ_2-norm $\leq B$ such that $\mathbf{A} \cdot (\mathbf{r} - \mathbf{r}') = \mathbf{0} \bmod q$

[24] I. Damgård, C. Orlandi, A. Takahashi, *et al.*, "Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices," in *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part I*, J. A. Garay, Ed., ser. Lecture Notes in Computer Science, vol. 12710, Springer, 2021, pp. 99–130.

Statistical MSIS[24]

- Given $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ as before
- It should be hard to find $\mathbf{r}, \mathbf{r}' \in \mathcal{R}_q^{m+d}$ of ℓ_2-norm $\leq B$ such that $\mathbf{A} \cdot (\mathbf{r} - \mathbf{r}') = \mathbf{0} \bmod q$
- We demand that $\Pr[\mathbf{A} \cdot \mathbf{r} = \mathbf{0}] \leq 2^{-\mathsf{sec}}$ with non zero elements $\mathbf{r}$ in the Euclidean ball $B_m(0, 2B)$

[24] I. Damgård, C. Orlandi, A. Takahashi, *et al.*, "Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices," in *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part I*, J. A. Garay, Ed., ser. Lecture Notes in Computer Science, vol. 12710, Springer, 2021, pp. 99–130.

Statistical MSIS[24]

- Given $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ as before
- It should be hard to find $\mathbf{r}, \mathbf{r}' \in \mathcal{R}_q^{m+d}$ of ℓ_2-norm $\leq B$ such that $\mathbf{A} \cdot (\mathbf{r} - \mathbf{r}') = \mathbf{0} \bmod q$
- We demand that $\Pr[\mathbf{A} \cdot \mathbf{r} = \mathbf{0}] \leq 2^{-\mathsf{sec}}$ with non zero elements $\mathbf{r}$ in the Euclidean ball $B_m(0, 2B)$
- Satisfied if

$$B \leq 2^{\frac{-\mathsf{sec}}{(m+d)\cdot n} - 1} \cdot q^{\frac{m}{m+d}} \cdot \sqrt{\frac{(m+d)\cdot n}{2\pi e}}$$

[24] I. Damgård, C. Orlandi, A. Takahashi, *et al.*, "Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices," in *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part I*, J. A. Garay, Ed., ser. Lecture Notes in Computer Science, vol. 12710, Springer, 2021, pp. 99–130.

Statistical MSIS[24]

- Given $\mathbf{A} = [\mathbf{I}_{[m]} \mid \bar{\mathbf{A}}] \in (\mathcal{R}_q)^{[m]\times[m+d]}$ as before
- It should be hard to find $\mathbf{r}, \mathbf{r}' \in \mathcal{R}_q^{m+d}$ of ℓ_2-norm $\leq B$ such that $\mathbf{A} \cdot (\mathbf{r} - \mathbf{r}') = \mathbf{0} \bmod q$
- We demand that $\Pr[\mathbf{A} \cdot \mathbf{r} = \mathbf{0}] \leq 2^{-\mathsf{sec}}$ with non zero elements $\mathbf{r}$ in the Euclidean ball $B_m(0, 2B)$
- Satisfied if

$$B \leq 2^{\frac{-\mathsf{sec}}{(m+d)\cdot n}-1} \cdot q^{\frac{m}{m+d}} \cdot \sqrt{\frac{(m+d)\cdot n}{2\pi e}}$$

- Also works for RSIS and SIS

[24] I. Damgård, C. Orlandi, A. Takahashi, *et al.*, "Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices," in *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part I*, J. A. Garay, Ed., ser. Lecture Notes in Computer Science, vol. 12710, Springer, 2021, pp. 99–130.

Norm Bounding

Let $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$ and $\sigma : K \to \mathbb{C}$ with number field K the canonical embedding[25] and $p, q \in \mathbb{N}$.

[25] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385; I. Damgård, V. Pastro, N. P. Smart, *et al.*, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 643–662.

Norm Bounding

Let $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$ and $\sigma : K \to \mathbb{C}$ with number field K the canonical embedding[25] and $p, q \in \mathbb{N}$.

- $\|f\|_p \leq \|f\|_q$, for $\infty \geq p \geq q \geq 1$

[25] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385; I. Damgård, V. Pastro, N. P. Smart, *et al.*, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 643–662.

Norm Bounding

Let $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$ and $\sigma : K \to \mathbb{C}$ with number field K the canonical embedding[25] and $p, q \in \mathbb{N}$.

- $\|f\|_p \leq \|f\|_q$, for $\infty \geq p \geq q \geq 1$
- $\lim_{q' \to q} \|f\|_p \leq \lim_{q' \to q} n^{\frac{1}{p} - \frac{1}{q'}} \|f\|_{q'}$ for $1 \leq p \leq q \leq \infty$

[25] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385; I. Damgård, V. Pastro, N. P. Smart, *et al.*, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 643–662.

Norm Bounding

Let $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$ and $\sigma : K \to \mathbb{C}$ with number field K the canonical embedding[25] and $p, q \in \mathbb{N}$.

- $\|f\|_p \leq \|f\|_q$, for $\infty \geq p \geq q \geq 1$
- $\lim_{q' \to q} \|f\|_p \leq \lim_{q' \to q} n^{\frac{1}{p} - \frac{1}{q'}} \|f\|_{q'}$ for $1 \leq p \leq q \leq \infty$
- $\|\sigma(f)\|_\infty \leq \|f\|_1 \leq n^{1-\frac{1}{p}} \|f\|_p$ for $p \geq 1$

[25] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385; I. Damgård, V. Pastro, N. P. Smart, *et al.*, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 643–662.

Norm Bounding

Let $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$ and $\sigma : K \to \mathbb{C}$ with number field K the canonical embedding[25] and $p, q \in \mathbb{N}$.

- $\|f\|_p \leq \|f\|_q$, for $\infty \geq p \geq q \geq 1$
- $\lim_{q' \to q} \|f\|_p \leq \lim_{q' \to q} n^{\frac{1}{p} - \frac{1}{q'}} \|f\|_{q'}$ for $1 \leq p \leq q \leq \infty$
- $\|\sigma(f)\|_\infty \leq \|f\|_1 \leq n^{1-\frac{1}{p}} \|f\|_p$ for $p \geq 1$
- $\|f\|_p \leq n^{\frac{1}{p}} \|f\|_\infty \leq n^{\frac{1}{p}} \|\sigma(f)\|_\infty$ for $p \leq \infty$

[25] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385; I. Damgård, V. Pastro, N. P. Smart, *et al.*, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 643–662.

Norm Bounding

Let $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$ and $\sigma : K \to \mathbb{C}$ with number field K the canonical embedding[26] and $p, q \in \mathbb{N}$.

[26] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385; I. Damgård, V. Pastro, N. P. Smart, *et al.*, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 643–662.

Norm Bounding

Let $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$ and $\sigma : K \to \mathbb{C}$ with number field K the canonical embedding[26] and $p, q \in \mathbb{N}$.

- $\|f \cdot g\|_\infty \leq \|f\|_\infty \cdot \|g\|_1$

[26] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385; I. Damgård, V. Pastro, N. P. Smart, *et al.*, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 643–662.

Norm Bounding

Let $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$ and $\sigma : K \to \mathbb{C}$ with number field K the canonical embedding[26] and $p, q \in \mathbb{N}$.

- $\|f \cdot g\|_\infty \leq \|f\|_\infty \cdot \|g\|_1$
- $\|f \cdot g\|_\infty \leq \|f\|_2 \cdot \|g\|_2$

[26] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385; I. Damgård, V. Pastro, N. P. Smart, *et al.*, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 643–662.

Norm Bounding

Let $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$ and $\sigma : K \to \mathbb{C}$ with number field K the canonical embedding[26] and $p, q \in \mathbb{N}$.

- $\|f \cdot g\|_\infty \leq \|f\|_\infty \cdot \|g\|_1$
- $\|f \cdot g\|_\infty \leq \|f\|_2 \cdot \|g\|_2$
- $\|\sigma(x \cdot y)\|_p \leq \|\sigma(x)\|_\infty \cdot \|\sigma(y)\|_p$

[26] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385; I. Damgård, V. Pastro, N. P. Smart, *et al.*, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 643–662.

Norm Bounding

Let $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$ and $\sigma : K \to \mathbb{C}$ with number field K the canonical embedding[26] and $p, q \in \mathbb{N}$.

- $\|f \cdot g\|_\infty \leq \|f\|_\infty \cdot \|g\|_1$
- $\|f \cdot g\|_\infty \leq \|f\|_2 \cdot \|g\|_2$
- $\|\sigma(x \cdot y)\|_p \leq \|\sigma(x)\|_\infty \cdot \|\sigma(y)\|_p$
- Encapsulated in `to_Lp()` and `to_Cp()` of the norm classes `Lp` and `Cp`

[26] C. Baum, I. Damgård, V. Lyubashevsky, *et al.*, "More efficient commitments from structured lattice assumptions," in *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, D. Catalano and R. D. Prisco, Eds., ser. Lecture Notes in Computer Science, vol. 11035, Springer, 2018, pp. 368–385; I. Damgård, V. Pastro, N. P. Smart, *et al.*, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, R. Safavi-Naini and R. Canetti, Eds., ser. Lecture Notes in Computer Science, vol. 7417, Springer, 2012, pp. 643–662.

Gaussian to Bound

- Classes for uniform and Gaussian distribution in the module `distributions`

[27] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, D. Pointcheval and T. Johansson, Eds., ser. Lecture Notes in Computer Science, vol. 7237, Springer, 2012, pp. 738–755.

Gaussian to Bound

- Classes for uniform and Gaussian distribution in the module `distributions`
- Gaussian

[27] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, D. Pointcheval and T. Johansson, Eds., ser. Lecture Notes in Computer Science, vol. 7237, Springer, 2012, pp. 738–755.

Gaussian to Bound

- Classes for uniform and Gaussian distribution in the module `distributions`
- Gaussian
  - Constructors for standard deviation σ, $s = \sigma\sqrt{2\pi}$, and $\alpha = \frac{s}{q} = \frac{\sqrt{2\pi}\sigma}{q}$

[27] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, D. Pointcheval and T. Johansson, Eds., ser. Lecture Notes in Computer Science, vol. 7237, Springer, 2012, pp. 738–755.

Gaussian to Bound

- Classes for uniform and Gaussian distribution in the module `distributions`
- Gaussian
  - Constructors for standard deviation σ, $s = \sigma\sqrt{2\pi}$, and $\alpha = \frac{s}{q} = \frac{\sqrt{2\pi}\sigma}{q}$
  - Gaussian to bound conversion[27]

[27] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, D. Pointcheval and T. Johansson, Eds., ser. Lecture Notes in Computer Science, vol. 7237, Springer, 2012, pp. 738–755.

Gaussian to Bound

- Classes for uniform and Gaussian distribution in the module `distributions`
- Gaussian
  - Constructors for standard deviation σ, $s = \sigma\sqrt{2\pi}$, and $\alpha = \frac{s}{q} = \frac{\sqrt{2\pi}\sigma}{q}$
  - Gaussian to bound conversion[27]
    - For ℓ_∞-norm:

$$\beta = s\sqrt{\frac{(\sec + 1)\ln(2)}{\pi}}$$

[27] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, D. Pointcheval and T. Johansson, Eds., ser. Lecture Notes in Computer Science, vol. 7237, Springer, 2012, pp. 738–755.

Gaussian to Bound

- Classes for uniform and Gaussian distribution in the module `distributions`
- Gaussian
  - Constructors for standard deviation σ, $s = \sigma\sqrt{2\pi}$, and $\alpha = \frac{s}{q} = \frac{\sqrt{2\pi}\sigma}{q}$
  - Gaussian to bound conversion[27]
    - For ℓ_∞-norm:
$$\beta = s\sqrt{\frac{(\mathsf{sec}+1)\ln(2)}{\pi}}$$
    - For ℓ_2-norm:
$$\Pr\left[\|X\|_2 > \sigma\sqrt{2n}\right] \leq 2^{\frac{n}{2}(1-\log e)}$$

[27] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, D. Pointcheval and T. Johansson, Eds., ser. Lecture Notes in Computer Science, vol. 7237, Springer, 2012, pp. 738–755.

Gaussian to Bound

- Classes for uniform and Gaussian distribution in the module `distributions`
- Gaussian
  - Constructors for standard deviation σ, $s = \sigma\sqrt{2\pi}$, and $\alpha = \frac{s}{q} = \frac{\sqrt{2\pi}\sigma}{q}$
  - Gaussian to bound conversion[27]
    - For ℓ_∞-norm:
$$\beta = s\sqrt{\frac{(\mathsf{sec} + 1)\ln(2)}{\pi}}$$
    - For ℓ_2-norm:
$$\Pr\left[\|X\|_2 > \sigma\sqrt{2n}\right] \leq 2^{\frac{n}{2}(1-\log e)}$$

$\Rightarrow$ Set $\beta = \sigma\sqrt{2n}$, if $2^{\frac{n}{2}(1-\log e)} \leq 2^{-\mathsf{sec}}$

[27] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, D. Pointcheval and T. Johansson, Eds., ser. Lecture Notes in Computer Science, vol. 7237, Springer, 2012, pp. 738–755.

Gaussian to Bound

- Classes for uniform and Gaussian distribution in the module `distributions`
- Gaussian
  - Constructors for standard deviation σ, $s = \sigma\sqrt{2\pi}$, and $\alpha = \frac{s}{q} = \frac{\sqrt{2\pi}\sigma}{q}$
  - Gaussian to bound conversion[27]
    - For ℓ_∞-norm:
$$\beta = s\sqrt{\frac{(\text{sec}+1)\ln(2)}{\pi}}$$
    - For ℓ_2-norm:
$$\Pr\left[\|X\|_2 > \sigma\sqrt{2n}\right] \leq 2^{\frac{n}{2}(1-\log e)}$$

    $\Rightarrow$ Set $\beta = \sigma\sqrt{2n}$, if $2^{\frac{n}{2}(1-\log e)} \leq 2^{-\text{sec}}$
    - In all other cases `to_Lp()` bounds the value via ℓ_2-norm

[27] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, D. Pointcheval and T. Johansson, Eds., ser. Lecture Notes in Computer Science, vol. 7237, Springer, 2012, pp. 738–755.