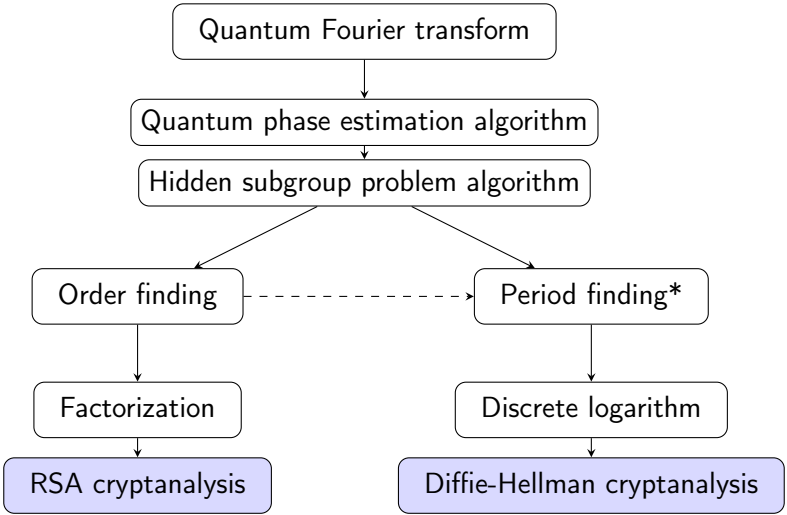
Post-quantum lattice-based cryptography: solutions, trends and open problems

E.S. Malygina[2], A.V. Kutsenko[1], S.A. Novoselov[3], N.S. Kolesnikov[3], A.O. Bakharev[1], I.S. Khilchuk[1], A.S. Shaporenko[1], N.N. Tokareva[1]

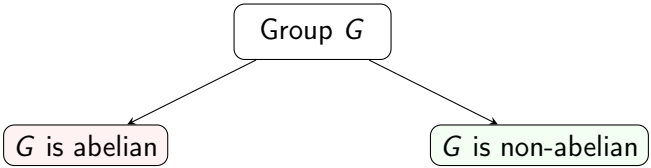
[1] Novosibirsk State University, Novosibirsk, Russia,
[2] QApp, Moscow, Russia,
[3] Immanuel Kant Baltic Federal University, Kaliningrad, Russia

The 13th Workshop on
Current Trends in Cryptology (CTCrypt 2024)
Petrozavodsk, June 3–6, 2024

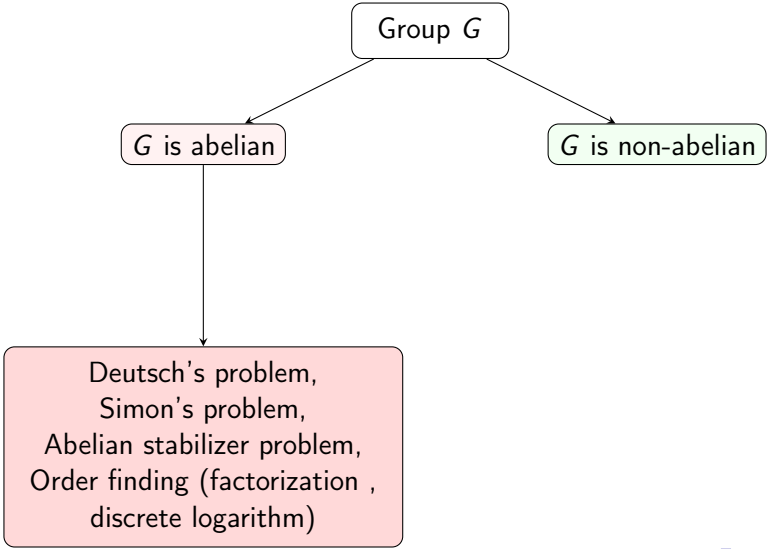
Quantum adversary



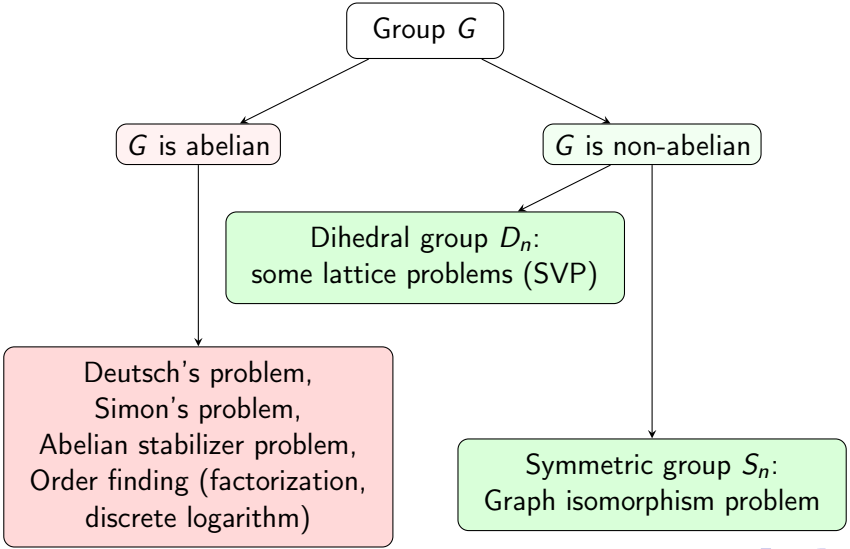
Quantum adversary



Quantum adversary



Quantum adversary



History

80s Powerful *cryptanalysis tool* (Joux, Stern, 1998) due to Lenstra-Lenstra-Lovász (LLL) lattice reduction algorithm;

History

80s Powerful *cryptanalysis tool* (Joux, Stern, 1998) due to Lenstra-Lenstra-Lovász (LLL) lattice reduction algorithm;

1991 Knapsack based cryptosystems (Odlyzko, 1990), which can be seen as an early predecessor of modern lattice schemes, were successfully attacked via lattices (Coster, LaMacchia, Odlyzko, Schnorr, 1991);

History

80s Powerful *cryptanalysis tool* (Joux, Stern, 1998) due to Lenstra-Lenstra-Lovász (LLL) lattice reduction algorithm;

1991 Knapsack based cryptosystems (Odlyzko, 1990), which can be seen as an early predecessor of modern lattice schemes, were successfully attacked via lattices (Coster, LaMacchia, Odlyzko, Schnorr, 1991);

1996 Ajtai's NP hardness proof of the shortest vector problem;

History

80s Powerful *cryptanalysis tool* (Joux, Stern, 1998) due to Lenstra-Lenstra-Lovász (LLL) lattice reduction algorithm;

1991 Knapsack based cryptosystems (Odlyzko, 1990), which can be seen as an early predecessor of modern lattice schemes, were successfully attacked via lattices (Coster, LaMacchia, Odlyzko, Schnorr, 1991);

1996 Ajtai's NP hardness proof of the shortest vector problem;

1997 Ajtai-Dwork cryptosystem with worst- to average-case reduction;

History

80s Powerful *cryptanalysis tool* (Joux, Stern, 1998) due to Lenstra-Lenstra-Lovász (LLL) lattice reduction algorithm;

1991 Knapsack based cryptosystems (Odlyzko, 1990), which can be seen as an early predecessor of modern lattice schemes, were successfully attacked via lattices (Coster, LaMacchia, Odlyzko, Schnorr, 1991);

1996 Ajtai's NP hardness proof of the shortest vector problem;

1997 Ajtai-Dwork cryptosystem with worst- to average-case reduction;

1998 Hoffstein, Pipher and Silverman introduced NTRU cryptosystem: compact lattice bases as public keys;

History

80s Powerful *cryptanalysis tool* (Joux, Stern, 1998) due to Lenstra-Lenstra-Lovász (LLL) lattice reduction algorithm;

1991 Knapsack based cryptosystems (Odlyzko, 1990), which can be seen as an early predecessor of modern lattice schemes, were successfully attacked via lattices (Coster, LaMacchia, Odlyzko, Schnorr, 1991);

1996 Ajtai's NP hardness proof of the shortest vector problem;

1997 Ajtai-Dwork cryptosystem with worst- to average-case reduction;

1998 Hoffstein, Pipher and Silverman introduced NTRU cryptosystem: compact lattice bases as public keys;

2005 Introduction of the Learning with Errors (LWE) problem together with Regev's encryption scheme;

History

80s Powerful *cryptanalysis tool* (Joux, Stern, 1998) due to Lenstra-Lenstra-Lovász (LLL) lattice reduction algorithm;

1991 Knapsack based cryptosystems (Odlyzko, 1990), which can be seen as an early predecessor of modern lattice schemes, were successfully attacked via lattices (Coster, LaMacchia, Odlyzko, Schnorr, 1991);

1996 Ajtai's NP hardness proof of the shortest vector problem;

1997 Ajtai-Dwork cryptosystem with worst- to average-case reduction;

1998 Hoffstein, Pipher and Silverman introduced NTRU cryptosystem: compact lattice bases as public keys;

2005 Introduction of the Learning with Errors (LWE) problem together with Regev's encryption scheme;

- Ring-LWE, Module-LWE...

History

80s Powerful *cryptanalysis tool* (Joux, Stern, 1998) due to Lenstra-Lenstra-Lovász (LLL) lattice reduction algorithm;

1991 Knapsack based cryptosystems (Odlyzko, 1990), which can be seen as an early predecessor of modern lattice schemes, were successfully attacked via lattices (Coster, LaMacchia, Odlyzko, Schnorr, 1991);

1996 Ajtai's NP hardness proof of the shortest vector problem;

1997 Ajtai-Dwork cryptosystem with worst- to average-case reduction;

1998 Hoffstein, Pipher and Silverman introduced NTRU cryptosystem: compact lattice bases as public keys;

2005 Introduction of the Learning with Errors (LWE) problem together with Regev's encryption scheme;

- Ring-LWE, Module-LWE...

2009 Fully homomorphic encryption (Gentry, 2009).

History

2022 NIST standardization of KYBER [BDK+18] as a lattice-based encryption/key encapsulation mechanism, and DILITHIUM [DKL+18] and FALCON [FHK+18] as lattice-based signature schemes;

2023 Call for additional Digital Signature Schemes organised by NIST.

Lattice

Definition

Let $v_1, v_2, \ldots, v_n \in \mathbb{R}^d$ be a set of linearly independent vectors. The **lattice** $\mathcal{L}$ is the set of all integer linear combinations of $v_1, v_2, \ldots, v_n$ that is

$$\mathcal{L} = \{\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n | \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}\}.$$

Definition

The integers d and n are the **dimension** and **rank** of the lattice respectively. If $d = n$, then $\mathcal{L}$ is a **full-rank lattice**.

In most cases, we work with full-rank lattices.

Lattice

Definition

A **basis** of a lattice $\mathcal{L}$ is a set of linearly independent vectors that spans the lattice. Corresponding lattice is denoted by $\mathcal{L}(B)$.

Definition

A matrix $U \in \mathbb{Z}^{n \times n}$ is called **unimodular** if it has a multiplicative inverse in $\mathbb{Z}^{n \times n}$.

The determinant of any unimodular matrix is equal to ± 1.

Lattice

Definition

A **basis** of a lattice $\mathcal{L}$ is a set of linearly independent vectors that spans the lattice. Corresponding lattice is denoted by $\mathcal{L}(B)$.

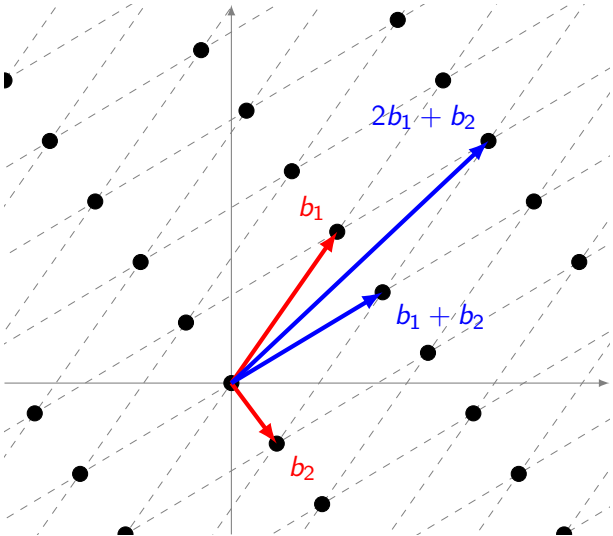
Definition

A matrix $U \in \mathbb{Z}^{n \times n}$ is called **unimodular** if it has a multiplicative inverse in $\mathbb{Z}^{n \times n}$.

The determinant of any unimodular matrix is equal to ± 1.

Proposition

If B and B' are two basis matrices, then $\mathcal{L}(B) = \mathcal{L}(B')$ if and only if $B' = UB$ for some unimodular matrix U.


$2b_1 + b_2$
b_1
$b_1 + b_2$
b_2

Lattice

Definition

Successive minima of linearly independent vectors are defined as follows:

- $\lambda_1(\mathcal{L}) = \min\limits_{x \in \mathcal{L},\ x \neq 0} \|x\| = \min\limits_{x,y \in \mathcal{L},\ x \neq y} \|x - y\|$;
- $\lambda_i(\mathcal{L}) = \min\{r : \mathcal{L} \text{ contains } i \text{ linearly independent vectors of length } \leqslant r\}$.

It holds

$$\lambda_1(\mathcal{L}) \leqslant \lambda_2(\mathcal{L}) \leqslant \ldots \leqslant \lambda_n(\mathcal{L}).$$

Let $\det(\mathcal{L}(B)) = \sqrt{\det(B^T B)}$.

Theorem (Minkowski's second Theorem)

For successive minima of an n-dimensional lattice $\mathcal{L}$ it holds

$$(\lambda_1(\mathcal{L}) \cdot \lambda_2(\mathcal{L}) \cdot \ldots \cdot \lambda_n(\mathcal{L}))^{1/n} \leqslant \sqrt{n} \cdot \det(\mathcal{L})^{1/n}.$$

Gaussian Heuristic

Let $\mathcal{L}$ be an n-dimensional lattice. The **Gaussian heuristic** predicts that $\lambda_1(\mathcal{L})$ equals

$$gh(\mathcal{L}) = \sqrt{\frac{n}{2\pi e}} \det(\mathcal{L})^{1/n}.$$

Shortest Vector Problem (SVP)

Given a lattice basis B, find a shortest non-zero vector in the lattice $\mathcal{L}(B)$, i.e., find a non-zero vector $\boldsymbol{v} \in \mathcal{L}(B)$ such that $\|\boldsymbol{v}\| = \lambda_1(\mathcal{L})$.

The problem is NP-hard (Ajtai, 1998).

Shortest Independent Vectors Problem (SIVP)

Given a lattice basis B of an n-dimensional lattice $\mathcal{L}(B)$, find n linearly independent vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \in \mathcal{L}(B)$ such that

$$\max_{i=1,2,\ldots,n} \|\boldsymbol{v}_i\| = \lambda_n(\mathcal{L}(B)).$$

Definition

An algorithm ALG for a minimization problem is called c-**approximation algorithm** for $c > 1$ if for all instances x, it satisfies

$$\frac{cost(ALG(x))}{cost(OPT(x))} \leqslant c.$$

Definition

For a minimization problem, a c-**gap problem** (where $c > 1$) distinguishes two cases for the optimal solution $OPT(x)$ of an instance x and a given k as follows:

- x is an *YES* instance if $OPT(x) \leqslant k$,
- x is an *NO* instance if $OPT(x) > c \cdot k$.

The γ-Shortest Vector Problem (SVP$_\gamma$)

Given a lattice basis B, find a shortest non-zero vector in the lattice $\mathcal{L}(B)$, i.e., find a non-zero vector $\boldsymbol{v} \in \mathcal{L}(B)$ such that $\|\boldsymbol{v}\| \leqslant \gamma \cdot \lambda_1(\mathcal{L})$.

The γ-GAP Shortest Vector Problem (GapSVP$_\gamma$)

INSTANCE: For a function $\gamma \geqslant 1$, given a real number $D > 0$ and a lattice basis B, the instance (B, k) is

- either a YES instance if $\lambda_1(\mathcal{L}(B)) \leqslant k$;
- or a NO instance if $\lambda_1(\mathcal{L}(B)) \geqslant \gamma \cdot k$.

QUESTION: Is (B, d) a YES or NO instance?

The GapSVP$_\gamma$ problem is NP-hard for any constant γ (Haviv, Regev, 2007; Khot, 2004).

The γ-Closest Vector Problem (CVP_γ)

Given a lattice basis B and a target vector $\boldsymbol{t}$ that is not in the lattice $\mathcal{L}(B)$, find a vector in $\mathcal{L}(B)$ that is closest to $\boldsymbol{t}$ by a factor $\gamma > 1$, i.e., find a vector $\boldsymbol{v} \in \mathcal{L}(B)$ such that for all $\boldsymbol{w} \in \mathcal{L}(B)$ it holds $\|\boldsymbol{v} - \boldsymbol{t}\| \leqslant \|\boldsymbol{w} - \boldsymbol{t}\|$.

- CVP is NP-hard (van Emde Boas, 1981);
- Given oracle access to a subroutine which solves CVP_γ, one may solve in polynomial time SVP_γ (Goldreich, Micciancio, Safra, Seifert, 1999).

The γ-Unique Shortest Vector Problem (uSVP$_\gamma$)

Given a lattice basis B of an n-dimensional lattice $\mathcal{L}(B)$. Provided that $\lambda_2(\mathcal{L}(B)) \geqslant \gamma \cdot \lambda_1(\mathcal{L}(B))$, find a non-zero vector $\boldsymbol{v} \in \mathcal{L}(B)$ such that $\|\boldsymbol{v}\| = \lambda_1(\mathcal{L})$.

The α-Bounded Distance Decoding Problem (BDDα)

Given a lattice basis B of an n-dimensional lattice $\mathcal{L}(B)$ and a target vector $\boldsymbol{t} \in \mathbb{R}^n$ satisfies $\mathrm{dist}(\boldsymbol{t}, \mathcal{L}) \leqslant \alpha \cdot \lambda_1(\mathcal{L})$, find a lattice vector $\boldsymbol{v} \in \mathcal{L}$ that is closest to $\boldsymbol{t}$.

For any polynomially-bounded γ, there is a reduction from uSVP$_\gamma$ to BDD$_{1/\gamma}$ (Lyubashevsky, Micciancio, 2009).

There exists a probabilistic polynomial-time reduction from the BDD$_{1/(\sqrt{2}\cdot\gamma)}$ problem to the uSVP$_\gamma$ for any $\gamma > 1$ that is polynomial in the lattice dimension n (Bai, Stehlé, Wen, 2016).

The γ-Shortest Independent Vectors Problem (SIVP$_\gamma$)

Given a lattice basis B of an n-dimensional lattice $\mathcal{L}(B)$, find n linearly independent vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \in \mathcal{L}(B)$ such that

$$\max_{i=1,2,\ldots,n} \|\boldsymbol{v}_i\| \leqslant \gamma \cdot \lambda_n(\mathcal{L}(B)).$$

SIVP$_\gamma$ is NP-hard for $\gamma = d^{1/\log\log d}$.

The γ-Shortest Basis Problem (SBP$_\gamma$)

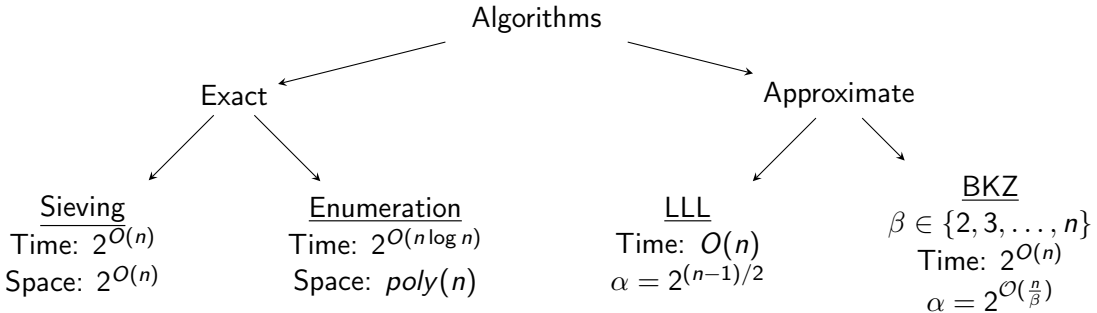
Given a lattice basis B of an n-dimensional lattice $\mathcal{L}(B)$, find a basis $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \in \mathcal{L}(B)$ with

$$\max_{i=1,2,\ldots,n} \|\boldsymbol{v}_i\| \leqslant \gamma \cdot \min \left\{ \max_{i=1,2,\ldots,n} \|\boldsymbol{a}_i\| : \{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n\} \text{ is a basis of } \mathcal{L}(B) \right\}.$$

SVP_γ hardness

Problem	Approximation factor γ	Hardness
SVP	Exact solution	NP-hard (Ajtai, 98)
SVP_γ	$O(1)$	NP-hard (Micciancio, 2001)
	$2^{(\log n)^{1-\epsilon}}$	NP-hard (Haviv, Regev, 2007)
	$\sqrt{n}$	NP$\cap$coNP (Aharonov, Regev, 2005)
	$poly(n)$	—
	$2^{O(n)}$	P (Lenstra, Lenstra, Lovász, 1982)

Solving SVP_γ



Exact solving of SVP_γ

		$\log_2(\text{time})$	$\log_2(\text{space})$
Probabilistic and deterministic	Enumeration	$\frac{n}{2e}\log_2 n$	$\mathcal{O}(\log_2 n)$
	AKS-Sieve	$3.398n$	$1.985n$
	ListSieve	$3.199n$	$1.325n$
	AKS-Sieve-Birthday	$2.571n$	$1.407n$
	ListSieve-Birthday	$2.465n$	$1.233n$
	Voronoi diagram	$2n$	n

Exact solving of SVP_γ

		$\log_2$(time)	$\log_2$(space)
Heuristics	NV-Sieve	$0.415n$	$0.208n$
	GaussSieve	$0.415n$	$0.208n$
	Triple sieve	$0.396n$	$0.189n$
	Overlattice sieve	$0.377n$	$0.293n$
	Triple sieve with NNS	$0.359n$	$0.189n$
	Hyperplane LSH	$0.337n$	$0.337n$
	Spherical LSH	$0.297n$	$0.297n$
	Spherical LSF	$0.292n$	$0.292n$

Learning with errors problem

Originally proposed by Regev in 2005.

Let n, m and q be positive integers, and let χ be a distribution over $\mathbb{Z}$.

Definition

The **LWE sample** is the pair $(\boldsymbol{A}, \boldsymbol{b})$, where $\boldsymbol{A} \in \mathbb{Z}_q^{m \times n}$ is uniformly random, $\boldsymbol{s} \leftarrow \chi^n$, $\boldsymbol{e} \leftarrow \chi^m$ and $\boldsymbol{b} \equiv \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \pmod{q}$.

The **LWE problem** for parameters (n, m, q, χ) is defined as follows:

Search version: given LWE sample $(\boldsymbol{A}, \boldsymbol{b})$, the problem is to find $\boldsymbol{s} \in \mathbb{Z}_q^n$;

Decision version: distinguish between uniformly random samples $(\boldsymbol{A}, \boldsymbol{u}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$ and LWE samples $(\boldsymbol{A}, \boldsymbol{b})$.

Learning with errors problem

Originally proposed by Regev in 2005.

Let n, m and q be positive integers, and let χ be a distribution over $\mathbb{Z}$.

Definition

The **LWE sample** is the pair $(\boldsymbol{A}, \boldsymbol{b})$, where $\boldsymbol{A} \in \mathbb{Z}_q^{m \times n}$ is uniformly random, $\boldsymbol{s} \leftarrow \chi^n$, $\boldsymbol{e} \leftarrow \chi^m$ and $\boldsymbol{b} \equiv \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \pmod{q}$.

The **LWE problem** for parameters (n, m, q, χ) is defined as follows:

Search version: given LWE sample $(\boldsymbol{A}, \boldsymbol{b})$, the problem is to find $\boldsymbol{s} \in \mathbb{Z}_q^n$;

Decision version: distinguish between uniformly random samples $(\boldsymbol{A}, \boldsymbol{u}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$ and LWE samples $(\boldsymbol{A}, \boldsymbol{b})$.

The search and decision problems are in fact equivalent, i.e., if one has access to an efficient distinguisher for Decision-LWE, a polynomial-time algorithm for Search-LWE can be constructed (Regev, 2009).

Example of cryptosystem

Let n, m and q be positive integers, and let χ be a distribution over $\mathbb{Z}$ such that for $\boldsymbol{e} \leftarrow \chi^m$ it holds $\mathrm{P}\left(|\boldsymbol{e} \cdot \boldsymbol{r}| < \left\lfloor \frac{q}{2} \right\rfloor /2\right) > 1 - \mathrm{negl}(n)$ for random $\boldsymbol{r} \in \mathbb{Z}_2^m$.

Private key:

Sample a private key $\boldsymbol{s} = (1, \boldsymbol{t})$, where $\boldsymbol{t} \leftarrow \mathbb{Z}_q^n$.

Public key:

Sample a random matrix $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{m \times n}$ and compute $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{t} + \boldsymbol{e}$ for a random noise vector $\boldsymbol{e} \leftarrow \chi^m$.
Output the public key $\boldsymbol{P} = [\boldsymbol{b}| - \boldsymbol{A}] \in \mathbb{Z}_q^{m \times (n+1)}$.

Example of cryptosystem

Encryption:

Encrypt the bit $M \in \mathbb{Z}_2$ by computing

$$\boldsymbol{c} = \left[\boldsymbol{P}^T \boldsymbol{r} + \left\lfloor \frac{q}{2} \right\rfloor \boldsymbol{M} \right]_q \in \mathbb{Z}_q^{n+1},$$

where $\boldsymbol{M} = (M, 0, \ldots, 0)$ has length $n+1$ and $\boldsymbol{r} \in \mathbb{Z}_2^m$ is random.

Decryption:

Decrypt the ciphertext $\boldsymbol{c}$ using the secret key by computing

$$M = \left[\left\lfloor \frac{2}{q} [\boldsymbol{c} \cdot \boldsymbol{s}]_q \right\rceil \right]_2.$$

Example of cryptosystem

The ciphertext can be rewritten as

$$\boldsymbol{c} = \left[\boldsymbol{b}^T\boldsymbol{r} + \left\lfloor \frac{q}{2} \right\rfloor M| - \boldsymbol{A}^T\boldsymbol{r}\right]_q$$

so we get

$$[\boldsymbol{c}\cdot\boldsymbol{s}]_q = \left[\boldsymbol{e}^T\boldsymbol{r} + \left\lfloor \frac{q}{2} \right\rfloor M\right]_q$$

and by using the property of the distribution we have

$$\frac{2}{q}[\boldsymbol{c}\cdot\boldsymbol{s}]_q \in \begin{cases} (-1/2, 1/2), & M = 0; \\ [-1, -1/2] \cup [1/2, 1], & M = 1. \end{cases}$$

LWE-comlexity

Admits Average-case to worst-case reduction (Regev, 2009).

LWE-comlexity

Admits Average-case to worst-case reduction (Regev, 2009).

Theorem (Regev, 2009)

Let n, q be integers and $\alpha \in (0,1)$ be such that $\alpha q > 2\sqrt{n}$. If there exists an efficient algorithm that solves LWE_{q,χ_α} then there exists an efficient quantum algorithm that approximates the decision version of the shortest vector problem (GapSVP) and the shortest independent vectors problem (SIVP) to within $\widetilde{O}(n/\alpha)$ in the worst case.

LWE-comlexity

Admits Average-case to worst-case reduction (Regev, 2009).

Theorem (Regev, 2009)

Let n, q be integers and $\alpha \in (0,1)$ be such that $\alpha q > 2\sqrt{n}$. If there exists an efficient algorithm that solves LWE_{q,χ_α} then there exists an efficient quantum algorithm that approximates the decision version of the shortest vector problem (GapSVP) and the shortest independent vectors problem (SIVP) to within $\widetilde{O}(n/\alpha)$ in the worst case.

Theorem (BDD to LWE — Regev, 2010)

Let $q \geqslant 2$ be an integer and $\alpha \in (0,1)$ be a real number. Assume there is an LWE oracle for the modulus q and error distribution χ. Then, given as input an n-dimensional lattice $\mathcal{L}$, a sufficient polynomial number of samples from the discrete Gaussian distribution $D_{\mathcal{L}^*,r}$ and a BDD instance $\boldsymbol{x} = \boldsymbol{v} + \boldsymbol{e} \in \mathbb{R}^n$ such that $\|\boldsymbol{e}\| \leqslant \alpha q/\sqrt{2}r$, there is a polynomial time algorithm finds the (unique) closest lattice vector $\boldsymbol{v} \in L$.

Learning With Errors problem

For an LWE instance $(\boldsymbol{A}, \boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e})$, one can consider the corresponding LWE lattice Λ^{LWE} generated by the rows of the following basis matrix

$$\boldsymbol{\Lambda}^{\mathrm{LWE}} = \begin{pmatrix} q\boldsymbol{I}_m & \boldsymbol{A} & \boldsymbol{b} \\ 0 & \boldsymbol{I}_n & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

that is

$$\Lambda^{\mathrm{LWE}} = \{(\boldsymbol{x}, \boldsymbol{y}, t) \in \mathbb{Z}^m \times \mathbb{Z}^n \times \mathbb{Z} | \boldsymbol{x} \equiv \boldsymbol{A}\boldsymbol{y} + t\boldsymbol{b} \pmod{q}\}$$

This is a lattice of rank $d = m + n + 1$ and volume q^m.

Learning With Errors problem

For an LWE instance $(\boldsymbol{A}, \boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e})$, one can consider the corresponding LWE lattice Λ^{LWE} generated by the rows of the following basis matrix

$$\boldsymbol{\Lambda}^{\mathrm{LWE}} = \begin{pmatrix} q\boldsymbol{I}_m & \boldsymbol{A} & \boldsymbol{b} \\ 0 & \boldsymbol{I}_n & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

that is

$$\Lambda^{\mathrm{LWE}} = \{(\boldsymbol{x}, \boldsymbol{y}, t) \in \mathbb{Z}^m \times \mathbb{Z}^n \times \mathbb{Z} | \boldsymbol{x} \equiv \boldsymbol{A}\boldsymbol{y} + t\boldsymbol{b} \pmod{q}\}$$

This is a lattice of rank $d = m + n + 1$ and volume q^m.

Vector $\boldsymbol{t} = (\boldsymbol{e}, \boldsymbol{s}, -1)$ belongs to the lattice and *likely* it is the shortest vector ($\ll$ the Gaussian heuristic).

One standard strategy to solve the LWE problem is to reduce it to a unique SVP (uSVP) problem via Kannan's embedding and then apply a lattice reduction to solve the uSVP problem.

$$\text{LWE/BDD} \xrightarrow{\textit{Kannan}} \text{uSVP}_\Lambda \longrightarrow \text{Lattice reduction}$$

There are two methods for estimating the cost for solving LWE via this strategy:

- the largeness of the gap in the uSVP problem (Gama, Nguyen, 2008)
- the shortness of the projection of the shortest vector to the GramSchmidt vectors (Alkim, Ducas, Pöppelmann, Schwabe, 2016)

One standard strategy to solve the LWE problem is to reduce it to a unique SVP (uSVP) problem via Kannan's embedding and then apply a lattice reduction to solve the uSVP problem.

$$\text{LWE/BDD} \xrightarrow{\textit{Kannan}} \text{uSVP}_\Lambda \longrightarrow \text{Lattice reduction}$$

There are two methods for estimating the cost for solving LWE via this strategy:

- the largeness of the gap in the uSVP problem (Gama, Nguyen, 2008)
- the shortness of the projection of the shortest vector to the GramSchmidt vectors (Alkim, Ducas, Pöppelmann, Schwabe, 2016)

The lattice reduction experiments fit more consistently with the second estimate (Albrecht, Göpfert, Virdia, Wunderer, 2016; Bai, Miller, Wen, 2019).

Small Integer Solutions

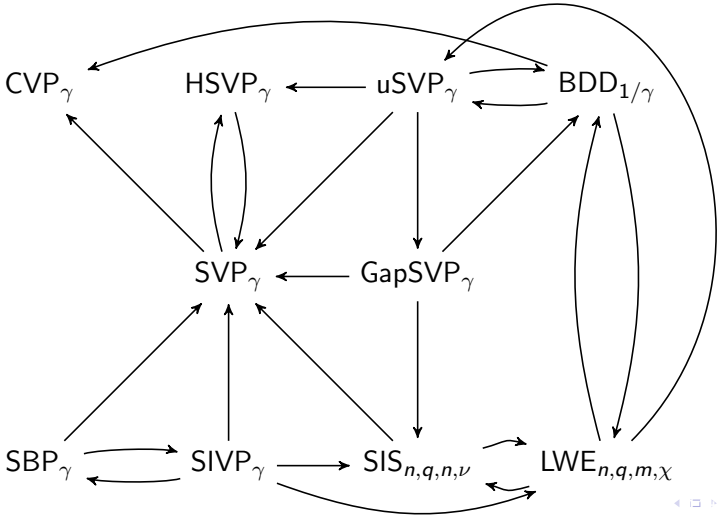
Originally proposed by Micciancio and Regev in 2007.

Inhomogeneous Small Integer Solution (ISIS)

Given positive unteger q, uniformly sampled matrix $A \in \mathbb{Z}_q^{m \times n}$, vector $b \in \mathbb{Z}$ and positive constant β the problem is to find such $x \in \mathbb{Z}_q^n$ that

- $Ax \equiv b \pmod{q}$;
- $\|x\| \leqslant \beta$.

For $\boldsymbol{b} = 0$ it is called homogeneous Small Integer Solution (SIS).


CVP_γ
HSVP_γ
uSVP_γ
$\mathrm{BDD}_{1/\gamma}$
SVP_γ
GapSVP_γ
SBP_γ
SIVP_γ
$\mathrm{SIS}_{n,q,n,\nu}$
$\mathrm{LWE}_{n,q,m,\chi}$

Module-LWE (Brakerski, Gentry, Vaikuntanathan, 2012)

Let n, m, k and q be positive integers. Consider the ring $R = \mathbb{Z}[X]/(X^n + 1)$ and let χ be a distribution of «short» polynomials of R_q. For $k = 1$ Ring-LWE (Lyubashevsky, Peikert, Regev, 2010).

Definition

The **MLWE sample** is the pair $(\boldsymbol{A}, \boldsymbol{b})$, where $\boldsymbol{A} \in R_q^{m \times k}$ is uniformly random, $\boldsymbol{s} \leftarrow \chi^k$, $\boldsymbol{e} \leftarrow \chi^m$ and $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e}$.

The **MLWE problem** for parameters (n, m, k, q, χ) is defined as follows:

Search version: given MLWE sample $(\boldsymbol{A}, \boldsymbol{b})$, the problem is to find $\boldsymbol{s} \in R_q^k$;

Decision version: distinguish between uniformly random samples $(\boldsymbol{A}, \boldsymbol{u}) \in R_q^{m \times k} \times \mathbb{Z}_q^m$ and MLWE samples $(\boldsymbol{A}, \boldsymbol{b})$.

Module-LWE (Brakerski, Gentry, Vaikuntanathan, 2012)

Let n, m, k and q be positive integers. Consider the ring $R = \mathbb{Z}[X]/(X^n + 1)$ and let χ be a distribution of «short» polynomials of R_q. For $k = 1$ Ring-LWE (Lyubashevsky, Peikert, Regev, 2010).

Definition

The **MLWE sample** is the pair $(\boldsymbol{A}, \boldsymbol{b})$, where $\boldsymbol{A} \in R_q^{m \times k}$ is uniformly random, $\boldsymbol{s} \leftarrow \chi^k$, $\boldsymbol{e} \leftarrow \chi^m$ and $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e}$.

The **MLWE problem** for parameters (n, m, k, q, χ) is defined as follows:

Search version: given MLWE sample $(\boldsymbol{A}, \boldsymbol{b})$, the problem is to find $\boldsymbol{s} \in R_q^k$;

Decision version: distinguish between uniformly random samples $(\boldsymbol{A}, \boldsymbol{u}) \in R_q^{m \times k} \times \mathbb{Z}_q^m$ and MLWE samples $(\boldsymbol{A}, \boldsymbol{b})$.

MLWE (as well as MSIS) average-case problem is at least as hard as standard lattice problems restricted to module lattices (Langlois, Stehlé, 2015).

CRYSTALS-Kyber

Let $q = 3329$, $R_q = \mathbb{Z}_q[X]/\left(X^{256}+1\right)$, χ be a distribution on «short» polynomials over R_q, let k be a security parameter, $k \in \{2,3,4\}$ (security categories 1,3,5).

KYBER is constructed first as an IND-CPA-secure PKE scheme, then boosted to an IND-CCA-secure KEM by a Fujisaki–Okomoto type of transform.

Private key:

Sample a private key $\boldsymbol{s} \leftarrow \chi^k$.

Public key:

Sample random matrix $\boldsymbol{A} \in R_q^{k \times k}$ and $\boldsymbol{e} \leftarrow \chi^k$, compute

$$(\boldsymbol{A}, \boldsymbol{b}) = (\boldsymbol{A}, \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e}).$$

CRYSTALS-Kyber

Encryption and decryption instantiate the Lindner–Peikert paradigm (Lindner, Peikert, 2011).

Encryption:

Sample $\boldsymbol{r}, \boldsymbol{e}_1 \leftarrow \chi^k$, $e_2 \leftarrow \chi$. Encrypt the message M (a 256-bit string) by computing

$$c = (\boldsymbol{c}_1, c_2) = \left(\boldsymbol{A}\boldsymbol{r} + \boldsymbol{e}_1, \boldsymbol{r}^T\boldsymbol{b} + e_2 + \left\lfloor \frac{q}{2} \right\rceil \cdot M\right) \in R_q^k \times R_q.$$

Decryption:

Decrypt the ciphertext c using the secret key $\boldsymbol{s}$ by computing

$$\nu = c_2 - \boldsymbol{c}_1^T\boldsymbol{s},$$

then round the value to $\{0, 1\}$.

Encryption and decryption instantiate the Lindner–Peikert paradigm (Lindner, Peikert, 2011).

Encryption:

Sample $\boldsymbol{r}, \boldsymbol{e}_1 \leftarrow \chi^k$, $e_2 \leftarrow \chi$. Encrypt the message M (a 256-bit string) by computing

$$c = (\boldsymbol{c}_1, c_2) = \left(\boldsymbol{A}\boldsymbol{r} + \boldsymbol{e}_1, \boldsymbol{r}^T\boldsymbol{b} + e_2 + \left\lfloor \frac{q}{2} \right\rceil \cdot M\right) \in R_q^k \times R_q.$$

Decryption:

Decrypt the ciphertext c using the secret key $\boldsymbol{s}$ by computing

$$\nu = c_2 - \boldsymbol{c}_1^T\boldsymbol{s},$$

then round the value to $\{0, 1\}$.

$$\nu = c_2 - \boldsymbol{c}_1^T\boldsymbol{s} = \left(\boldsymbol{r}^T\boldsymbol{e} + e_2 - \boldsymbol{e}_1^T\boldsymbol{s}\right) + \left\lfloor \frac{q}{2} \right\rceil \cdot M$$

Module-LWR

Proposed in (Banerjee, Peikert, Rosen, 2011).

Let n, m, k and $q \geqslant p \geqslant 1$ be positive integers. Consider the ring $R = \mathbb{Z}[X]/(X^n + 1)$ and let χ be a distribution of «short» polynomials of R_q.

Definition

The **MLWR sample** is the pair $(\boldsymbol{A}, \boldsymbol{b})$, where $\boldsymbol{A} \in R_q^{m \times k}$ is uniformly random, $\boldsymbol{s} \leftarrow \chi^k$ and $\boldsymbol{b} = \mathrm{Round}\left(\frac{p}{q} \cdot \boldsymbol{A}\boldsymbol{s}\right)$, where $\mathrm{Round} : \mathbb{Z}_q \to \mathbb{Z}_p$ is a rounding to the nearest multiple of $\frac{q}{p}$.

The **MLWR problem** for parameters (n, m, k, q, p, χ) is defined as follows:

Search version: given MLWR sample $(\boldsymbol{A}, \boldsymbol{b})$, the problem is to find $\boldsymbol{s} \in R_q^k$;

Decision version: distinguish between uniformly random samples $(\boldsymbol{A}, \boldsymbol{u}) \in R_q^{m \times k} \times \mathbb{Z}_q^m$ and MLWR samples $(\boldsymbol{A}, \boldsymbol{b})$.

Module-LWR vs Module-LWE

«...all experimental investigations to date have indicated that MLWR (at least the MLWR instances relevant to cryptosystems like Saber) does not differ from MLWE in terms of the cryptanalytic techniques that are applicable or in terms of how successful those techniques are.»[1]

[1]Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

NTRU

Let q be positive integer. Consider the ring $R = \mathbb{Z}[X]/P(x)$, where $P(x)$ is a monic irreducible polynomial and let χ_f, χ_g be distributions on R_q.

Definition

The **NTRU sample** is the element $h = gf^{-1}$, where $f \leftarrow \chi_f$, $\boldsymbol{f}$ is invertible $g \leftarrow \chi_g$.

The **NTRU problem** for parameters $(P(x), q, \gamma, \chi_f, \chi_g)$ is defined as follows:

Search version: given NTRU sample h, the problem is to find a pair $(f, g) \in R_q \times R_q$ with Euclidian norms $\|h\|, \|g\| \leqslant \sqrt{q}/\gamma$;

Decision version: distinguish between uniformly random samples $h \in R_q$ and NTRU samples h.

NTRU in NIST competition

- FALCON selected by the NIST at the 3d round of the post-quantum standardisation;
- NTRU finalist at the 3d round of the post-quantum standardisation;
- NTRU PRIME alternate candidate at the 3d round of the post-quantum standardisation.

Module-NTRU

Let q be positive integer. Consider the ring $R = \mathbb{Z}[X]/P(x)$, where $P(x)$ is a monic irreducible polynomial and let χ_F, χ_g be distributions on R_q.

Definition

The **MNTRU sample** is the element $\boldsymbol{h} = \boldsymbol{F}^{-1}\boldsymbol{g}$, where $\boldsymbol{F} \leftarrow \chi_F^{k \times k}$, $\boldsymbol{F}$ is invertible $\boldsymbol{g} \leftarrow \chi_g^k$.

The **MNTRU problem** for parameters $(P(x), q, \gamma, \chi_F, \chi_g)$ is defined as follows:

Search version: given MNTRU sample $\boldsymbol{h}$, the problem is to find a pair $(\boldsymbol{F}, \boldsymbol{g}) \in R_q^{k \times k} \times R_q^k$ with Euclidian norms $\|\boldsymbol{h}\|, \|\boldsymbol{g}\| \leqslant \sqrt{q}/\gamma$;

Decision version: distinguish between uniformly random samples $\boldsymbol{h} \in R_q^k$ and MNTRU samples $\boldsymbol{h}$.

(M)NTRU overview

NTRU:

- The worst-case approximate SVP_γ over ideal attices can be reduced to an average-case search variant of the NTRU problem (Mary, Stéhle, 2021);
- An average-case search variant of the NTRU problem can be reduced to the decision NTRU problem (Mary, Stéhle, 2021);
- Worst-case module uSVP can be reduced to worst-case NTRU (Felderhof, Mary, Stéhle, 2022).

(M)NTRU overview

NTRU:

- The worst-case approximate SVP_γ over ideal attices can be reduced to an average-case search variant of the NTRU problem (Mary, Stéhle, 2021);
- An average-case search variant of the NTRU problem can be reduced to the decision NTRU problem (Mary, Stéhle, 2021);
- Worst-case module uSVP can be reduced to worst-case NTRU (Felderhof, Mary, Stéhle, 2022).

MNTRU:

- Introduced in (Cheon, Kim, Kim, Son, 2019), and (Chuengsatiansup, Prest, Stehlé), Wallet, Xagawa, 2020);
- MNTRU offers greater flexibility on parameters, such as the underlying ring dimension;
- Encryption scheme on MNTRU with ciphertext sizes 651, 977 and 1257 bytes for NIST Level 1, 3 and 5 security (Bai, Jangir, Lin, Ngo, Wen, Zheng, 2024).

NTWE (NTRU+LWE)

Proposed in 2023 by Gärtner as a new problem for lattice-based cryptography.

Definition

Decision version: distinguish between uniformly random $\left(\boldsymbol{A} \in R_q^{m \times k}, \boldsymbol{b} \in R_q^m\right)$ and $\left(\boldsymbol{A}, \boldsymbol{b} = (\boldsymbol{A}\boldsymbol{s} + \boldsymbol{e})f^{-1}\right)$ with uniformly random $\boldsymbol{A} \in R_q^{m \times k}$, small $\boldsymbol{e} \in R_q^m$, $\boldsymbol{s} \in R_q^k$ and $f \in R_q$.

Search version: recover $\boldsymbol{s}X^i, fX^i$ from the NTWE sample for some i.

NTWE (NTRU+LWE)

Proposed in 2023 by Gärtner as a new problem for lattice-based cryptography.

Definition

Decision version: distinguish between uniformly random $\left(\boldsymbol{A} \in R_q^{m \times k}, \boldsymbol{b} \in R_q^m\right)$ and $\left(\boldsymbol{A}, \boldsymbol{b} = (\boldsymbol{A}\boldsymbol{s} + \boldsymbol{e})f^{-1}\right)$ with uniformly random $\boldsymbol{A} \in R_q^{m \times k}$, small $\boldsymbol{e} \in R_q^m$, $\boldsymbol{s} \in R_q^k$ and $f \in R_q$.

Search version: recover $\boldsymbol{s}X^i, fX^i$ from the NTWE sample for some i.

- A natural combination of NTRU and LWE problems;
- Is not easier than either of NTRU or LWE problem;
- Parameters are less than for MNTRU-like systems (Gärtner, 2023);

Relation to known problems

- Given MLWE instance $(\boldsymbol{A}, \boldsymbol{b})$;
- Sample f from correct distribution and consider $\left(\boldsymbol{A}, \boldsymbol{b} \cdot f^{-1}\right)$ as an NTWE instance;
- Solving NTWE instance gives solution to original MLWE instance.

Relation to known problems

- Given MLWE instance $(\boldsymbol{A}, \boldsymbol{b})$;
- Sample f from correct distribution and consider $\left(\boldsymbol{A}, \boldsymbol{b} \cdot f^{-1}\right)$ as an NTWE instance;
- Solving NTWE instance gives solution to original MLWE instance.

- Given NTRU instance $h_i = g_i f^{-1}$;
- Sample $\boldsymbol{A}$ uniformly at random and produce NTWE instance with

$$\boldsymbol{b} = \left(A \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_k \end{pmatrix} + \begin{pmatrix} h_{k+1} \\ h_{k+2} \\ \vdots \\ h_{k+m} \end{pmatrix} \right) = \left(A \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix} + \begin{pmatrix} g_{k+1} \\ g_{k+2} \\ \vdots \\ g_{k+m} \end{pmatrix} \right) \cdot f^{-1};$$

- Solving NTWE instance implies solution to original NTRU instance.

Lattice Isomorphism Problem (LIP)

Proposed by Ducas, van Woerden (EUROCRYPT 2022), Bennett et al. preprint 2021.

Two lattices $\mathcal{L}, \mathcal{L}'$ are called **isomorphic** if there exists some orthonormal transformation $O \in \mathcal{O}_n(\mathbb{R})$ such that $\mathcal{L}' = O\mathcal{L}$.

Definition

The **LIP problem** for parameters (n, m) is defined as follows:

Search version: Given two bases $B, B' \in \mathbb{R}^{n \times m}$ that generate isomorphic lattices, find $O \in \mathcal{O}_n(\mathbb{R})$ and unimodular $U \in \mathrm{GL}(\mathbb{Z})$ such that $B' = OBU$.

Decision version: Given two bases $B, B' \in \mathbb{R}^{n \times m}$, decide whether there exist an isometry $O \in \mathcal{O}_n(\mathbb{R})$ and an unimodular change-of-basis $U \in \mathrm{GL}(\mathbb{Z})$ such that $B' = OBU$.

Lattice Isomorphism Problem (LIP)

- A worst-case to average-case reduction for search-LIP and distinguish-LIP within an isomorphism class (Ducas, Woerden, 2022);
- **Conjecture**: For any two lattices $\mathcal{L}_0$, $\mathcal{L}_1$ and $1 \leqslant \mathrm{gap}\,(L_i) \leqslant \gamma$, the best attack against an instance of ΔLIP with $\mathcal{L}_0$ and $\mathcal{L}_1$ requires solving SVP_γ for both $\mathcal{L}_0$ and $\mathcal{L}_1$ (Ducas, Woerden, 2023);
- Used in signature scheme HAWK which is one of additional Digital Signature candidates for the PQC standardization process (omSVP, smLIP).

Private key size	184	360
Public key size	1024	2440
Signature size	555	1221

Hints usage

A framework proposed in (Dachman-Soled, Ducas, Gong and Rossi, 2020) when side information in the form of «hints» — about the secret and/or error is available.

Hints usage

A framework proposed in (Dachman-Soled, Ducas, Gong and Rossi, 2020) when side information in the form of «hints» — about the secret and/or error is available.

Earlier: one standard strategy to solve the LWE problem is to reduce it to a unique SVP (uSVP) problem via Kannan's embedding and then apply a lattice reduction to solve the uSVP problem.

$$\text{LWE/BDD} \xrightarrow{\textit{Kannan}} \text{uSVP}_\Lambda \longrightarrow \text{Lattice reduction}$$

Hints usage

A framework proposed in (Dachman-Soled, Ducas, Gong and Rossi, 2020) when side information in the form of «hints» — about the secret and/or error is available.

Earlier: one standard strategy to solve the LWE problem is to reduce it to a unique SVP (uSVP) problem via Kannan's embedding and then apply a lattice reduction to solve the uSVP problem.

$$\text{LWE/BDD} \xrightarrow{\textit{Kannan}} \text{uSVP}_{\Lambda} \longrightarrow \text{Lattice reduction}$$

to

$$\text{LWE/BDD} \longrightarrow \{\text{DBDD}_{\Lambda_i,\mu_i,\Sigma_i}\} \longrightarrow \text{uSVP}_{\Lambda'} \longrightarrow \text{Lattice reduction}$$

Side channel information obtained from the side-channel attack of (Bos, Friedberger, Martinoli, Oswald, Stam, 2018) against Frodo (LWE-based KEM).

- Perfect hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle = l$;
- Modular hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle = l \pmod{k}$;
- Approximate hints: $\langle \boldsymbol{s}, \boldsymbol{v} \rangle = l + \epsilon_\sigma$;

Example: let $\boldsymbol{s}_0$ be a secret coefficient (represented by a signed 16-bits integer), whose a priori distribution is supported by $\{-5, \ldots, 5\}$. Consider the case where we learn the Hamming weight of $\boldsymbol{s}_0$, say 2. Then, we have $\boldsymbol{s}_0 \in \{3, 5\}$. This leads to two hints:

- a modular hint: $\boldsymbol{s}_0 \equiv 1 \pmod{2}$;
- an approximate hint: $\boldsymbol{s}_0 = 4 + \epsilon_1$, where ϵ_1 has variance 1.

Hints usage

The ideas were continued in (May, Nowakowski, 2023), where it was practically determined which number of hints is sufficient to efficiently break LWE-based lattice schemes in practice.

- For modular hints defined over $\mathbb{Z}_q$, wer econstruct Kyber-512 secret keys via only LLL reduction with anamount of 449 hints;
- For LWE dimension n roughly n/2 perfect hints. E.g., we reconstruct via LLL reduction Kyber-512 keys with merely 234 perfecthints.

Thanks for attention!