Lattice-based Cryptography

Basics

Table of Contents

Table of Contents

Classical Cryptography

In classical cryptography, the security of public-key algorithms relies on well-known hard problems:

- Integer factorization problem (RSA, etc.)
- Discrete logarithm problem (Diffie-Hellman, etc.)
- Elliptic curve discrete logarithm problem (Elliptic-curve Diffie-Hellman, etc.)

Quantum Computer

- In the 1980s, Paul A. Benioff proposed a new form of Turing machines using the laws of quantum mechanics
- Improvement in computation: Quantum logic gates, quantum bits (qubit) instead of bits, quantum states instead of "original states"
- There are many models of quantum computers: quantum Turing machine, quantum circuit model, etc.
- Threat from the cryptographic point of view: the Shor Algorithm

Shor's Algorithm

- The most famous quantum algorithm is invented in 1994 by Peter Shor
- Problem: find a non-trivial divisor of a given composite number N
- There are two parts of the algorithm:
  - Classical part: reduction of the problem to the order-finding problem
  - Quantum part: solve the order-finding problem
- Running time is polynomial in $logN$
- Consequence: classical public-key cryptographic primitives are easily breakable

Table of Contents

Possible Solutions: Multivariate Cryptography

- We use multivariate polynomials over certain finite fields
- Security relies on the fact, that solving systems of multivariate polynomial equations is proven to be NP-complete
- Rainbow is one of the most famous multivariate public-key cryptosystems
- It was invented in 2004 by Jintai Ding and Dieter Schmidt
- Importance: It was select as one of the three NIST Post-quantum signature finalists

Now broken!

Possible Solutions: Code-based Cryptography

- The systems rely on error-correcting codes
- The first code-based public-key cryptosystem was invented in 1978 by Robert McEliece
- Security of the original algorithm relies on the fact, that decoding a general linear code is known to be NP-hard
- Importance: a new version of the cryptosystem called Classic McEliece was selected as one of the four NIST Post-quantum public-key encryption and key-establishment finalists

Table of Contents

Lattice-based Cryptography: Introduction

- The idea is to create cryptographic primitives over lattices
- The first lattice-based cryptographic primitive was invented in 1996 by a Hungarian computer scientist Miklós Ajtai
- The security of the primitives relies on the hardness of lattice problems
- Importance: lattice-based cryptography believed to be secure against quantum algorithms
- Famous encryption schemes: GGH, NTRU, LWE, Ring-LWE
- There are many encryption algorithms and digital signature schemes which were selected as finalist of NIST's Post-quantum Security competition

Definitions

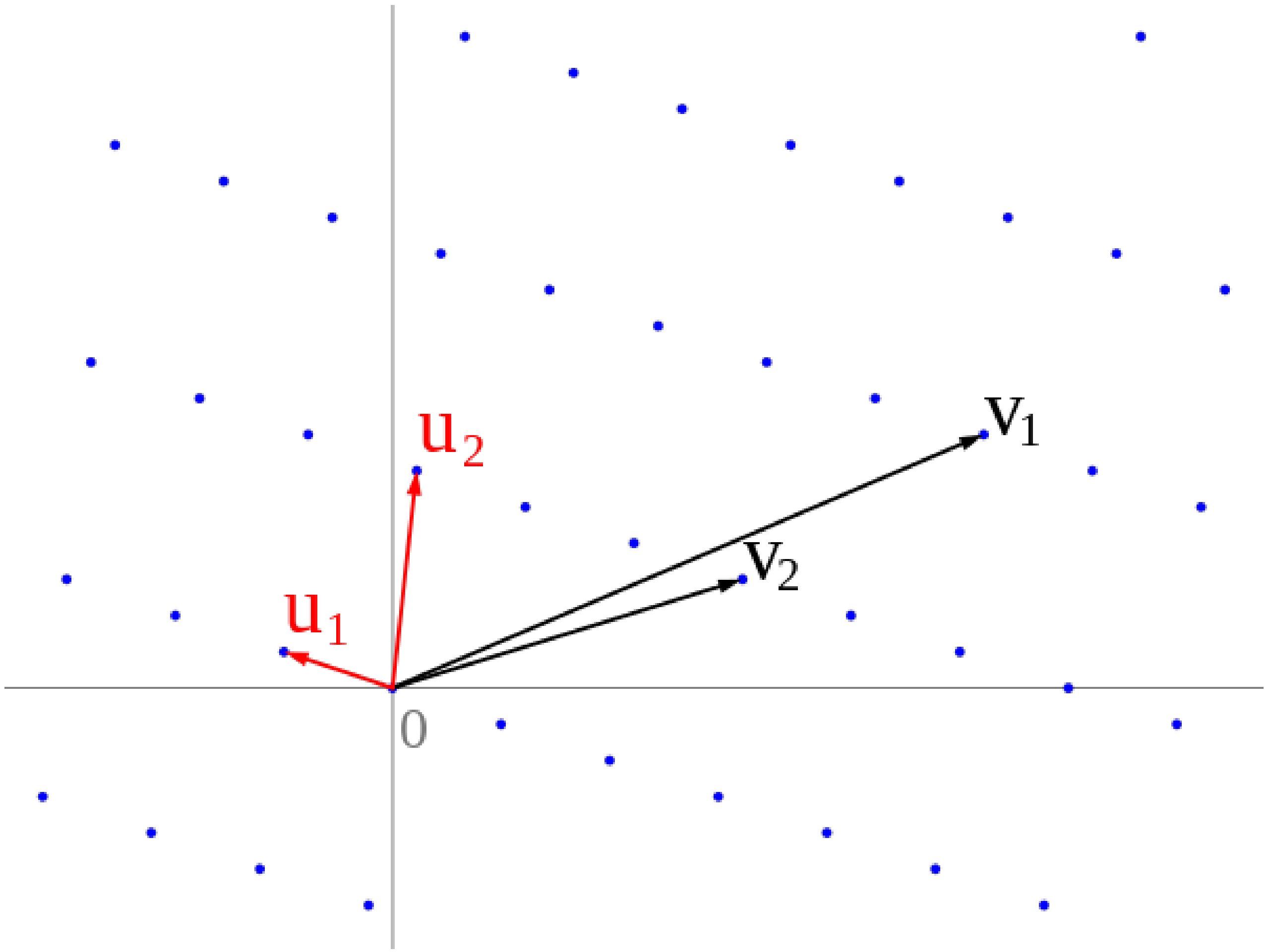
Definition

Given $n \in \mathbb{N}$ linearly independent vectors $b_1, \ldots, b_m \in \mathbb{R}^n$, $m \leq n$. A lattice $\mathcal{L}$, which is generated by all the integer combinations of the vectors $b_1, \ldots, b_m$, is the following set of points:

$$\mathcal{L}(b_1, \ldots, b_m) = \left\{ \sum_{i=1}^{m} z_i b_i | z_i \in \mathbb{Z},\ i \in \{1, \ldots, m\} \right\}.$$

The set of vectors $b_1, \ldots, b_m$ is called the basis of the lattice.

Lattice in 2D whit different bases



Definitions

Definition

The basis can be represented as $B = [b_1 \ldots b_n]$, and the definitions of a lattice will be:

$$\mathcal{L}(B) = \{Bz : z \in \mathbb{Z}^n\}.$$

Remark

Lattices has infinity many different bases.

Remark

If U is a unimodular matrix, then $\mathcal{L}(B) = \mathcal{L}(BU)$.

Definitions

Definition

Let $\mathcal{L}(B)$ be a lattice generated by some basis B. Then:

$$det(\mathcal{L}(B)) = |det(B)|.$$

Definition

The dual of a lattice $\mathcal{L}(B)$, denoted $\mathcal{L}(B)^*$, is the lattice generated by the matrix $(B^{-1})^T$, more formally:

$$\mathcal{L}(B)^* = \mathcal{L}((B^{-1})^T).$$

Special lattices

Definition

A subset $I \subset k[x_1, \ldots x_n]$ is an ideal if:

- $0 \in I$
- $f, g \in I \implies f + g \in I$
- $f \in I \wedge h \in k[x_1, \ldots x_n] \implies hf \in I$.

Definition

Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Then the ideal generated by $f_1, \ldots, f_s$ is the following:

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{t=1}^{s} h_t f_t \ : \ \forall h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}.$$

Special Lattices

Definition

Let $f \in \mathbb{Z}[x]$ be a degree-n monic polynomial and $R = \mathbb{Z}[x]/(f)$. A lattice $\mathcal{L}(B) \in \mathbb{Z}^n$ is an ideal lattice if there exists an ideal $I \subseteq R$ for which $B = \{g \ mod \ f : g \in I\}$. The ideal can be represented as $I = \langle b_1, \ldots, b_k \rangle$, where the vectors $b_1, \ldots, b_k$ are the basis vectors of $\mathcal{L}$.

Lemma

For all $I \in \mathbb{Z}[x]/(f)$ if f is a degree-n monic irreducible integer polynomial, then I is isomorphic to a lattice in $\mathbb{Z}^n$.

Special Lattices

- There are some specific ideal lattices which are interesting from cryptographic point of view. We mention one of them: cyclic lattices.
- There are two ways to define cyclic lattices: using the definition of ideal lattices or defining them with cyclic rotations.

Definition

Let $R = \mathbb{Z}[x]/(f)$ be a quotient ring. An ideal lattice defined over R is a cyclic lattice if $f(x) = x^n - 1$ for some $n \in \mathbb{Z}^+$.

Special lattices

Definition

Let $x = (x_1, \ldots, x_n)^T$ be a vector. Then the cyclic rotation of x is the following:

$$rot(x) = (x_n, x_1, \ldots, x_{n-1}).$$

Definition

The circulant matrix for a given vector $x = (x_1, \ldots, x_n)^T$ is the following:

$$Rot(x) = [x, rot(x), rot^2(x), \ldots, rot^{n-1}(x)].$$

Remark

The rows of $Rot(x)$ are also rotations of x but with reversed order.

Special lattices

Definition

A lattice $\mathcal{L}(B)$ is cyclic if it is closed under cyclic rotation operation. More formally, if $\mathcal{L}(B)$ is cyclic then:

$$x \in \mathcal{L}(B) \implies rot(x) \in \mathcal{L}(B)$$

Remark

The two definitions are the same, that is, if $f(x) = x^n - 1$ and given a vector $v = (v_1, \ldots, v_n)$ then for a corresponding vector $w = (w_1, \ldots, w_n)$: $w \equiv x \cdot v \implies w = (v_n, v_1, \ldots, v_{n-1})$.

Special lattices

Definition

Let $f(x) = x^n + a_n x^{n-1} + \ldots + a_1 \in \mathbb{Z}[x]$ be a cyclotomic polynomial, $q \in \mathbb{Z}$ and $R = \mathbb{Z}_q[x]/(f(x))$ be a ring.

Table of Contents

Table of Contents

SVP

The Shortest Vector Problem (SVP): Given a vector space V with a norm $||.||$ and a basis B of a lattice $\mathcal{L} \subset V$, find a non-zero vector v such that $||v|| = \lambda(L)$, where $\lambda(L)$ denote the length of the shortest non-zero vector in the lattice $\mathcal{L}$, that is:

$$\lambda(L) = \min_{v \in \mathcal{L}/\{0\}} ||v||.$$

In the γ-approximation version SVP_γ, one must find a non-zero lattice vector of length at most $\gamma \cdot \lambda(L)$ for given $\gamma \geq 1$.

CVP

The Closest Vector Problem (CVP): a vector space V and a metric $|.|$ are given for a lattice $\mathcal{L}$ with a corresponding basis B, as well as a vector v in V but not necessarily in $\mathcal{L}$. It is desired to find the vector in $\mathcal{L}$ closest to v (as measured by M). In the γ-approximation version CVP_γ, one must find a lattice vector at distance at most γ

SIVP

Shortest Independent Vectors Problem (SIVP): Given a vector space V with a norm $||.||$ and a basis $B \in \mathbb{Z}^{n \times n}$ of a lattice $\mathcal{L} \subset V$, find n linearly independent lattice vectors $s_1, \ldots, s_n$ for which $max_i ||s_i||$ is minimal.

SIS

Short Integer Solution (SIS): Given m uniformly random vectors b_i of a certain large finite additive group $\mathbb{Z}_q^n$, where the vectors form a matrix $B = [b_1, \ldots, b_m] \in \mathbb{Z}_q^{nxm}$. The task is to find a nonzero vector $z \in \mathbb{Z}^n$, such that: $||z|| < \beta$ and $Bz = \sum b_i z_i = 0$.

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Hermite normal form

Babai's rounding

The protocol

- The private key is a "good" lattice basis $B = [b_1, \ldots, b_n]$. Typically, a good basis is a basis consisting of short, almost orthogonal vectors.
- The public key H is a "bad" basis for the same lattice: $H = HNF(B) = UB$, where U is a unimodular matrix.
- Encryption of v: choose a small error $e \in \mathbb{Z}^n$ and calculate $c = vH + e$
- Decryption: calculate $cB^{-1} = [(v_1, \ldots, v_n)H + (e_q, \ldots, e_n)]B^{-1} = (vH + e)B^{-1} = vUBB^{-1} + eB^{-1} = vU + eB^{-1}$
- Use Babai rounding to eliminate eB^{-1} and calculates $vUU^{-1} = v$

Attacks

Table of Contents

Table of Contents

Table of Contents

Introduction

A very important work of Regev [Reg05] from 2005 introduced the average-case learning with errors (LWE) problem, which is the "encryption-enabling" analogue of the SIS problem. Indeed, the two problems are syntactically very similar, and can meaningfully be seen as duals of each other.

Table of Contents

LWE

The basic idea of LWE is to add some noise to the message. So we embed the message in the lattice, which is constructed by the secret basis matrix B. To find it without knowing the secret key, we have to solve the CVP, which is considered hard. To summarize, we have to solve the following:

$$y = B \cdot z + e \quad (mod \quad q),$$

where $y \in \mathbb{Z}_q^n$ vector is the public key, $B \in \mathbb{Z}^{n \times n}$ is also public, $z \in \mathbb{Z}_q^n$ is the secret and $e \in \mathbb{Z}_q^n$ is the error. From this construction, we have to know the secret key or we have to solve the CVP.

LWE in 2D

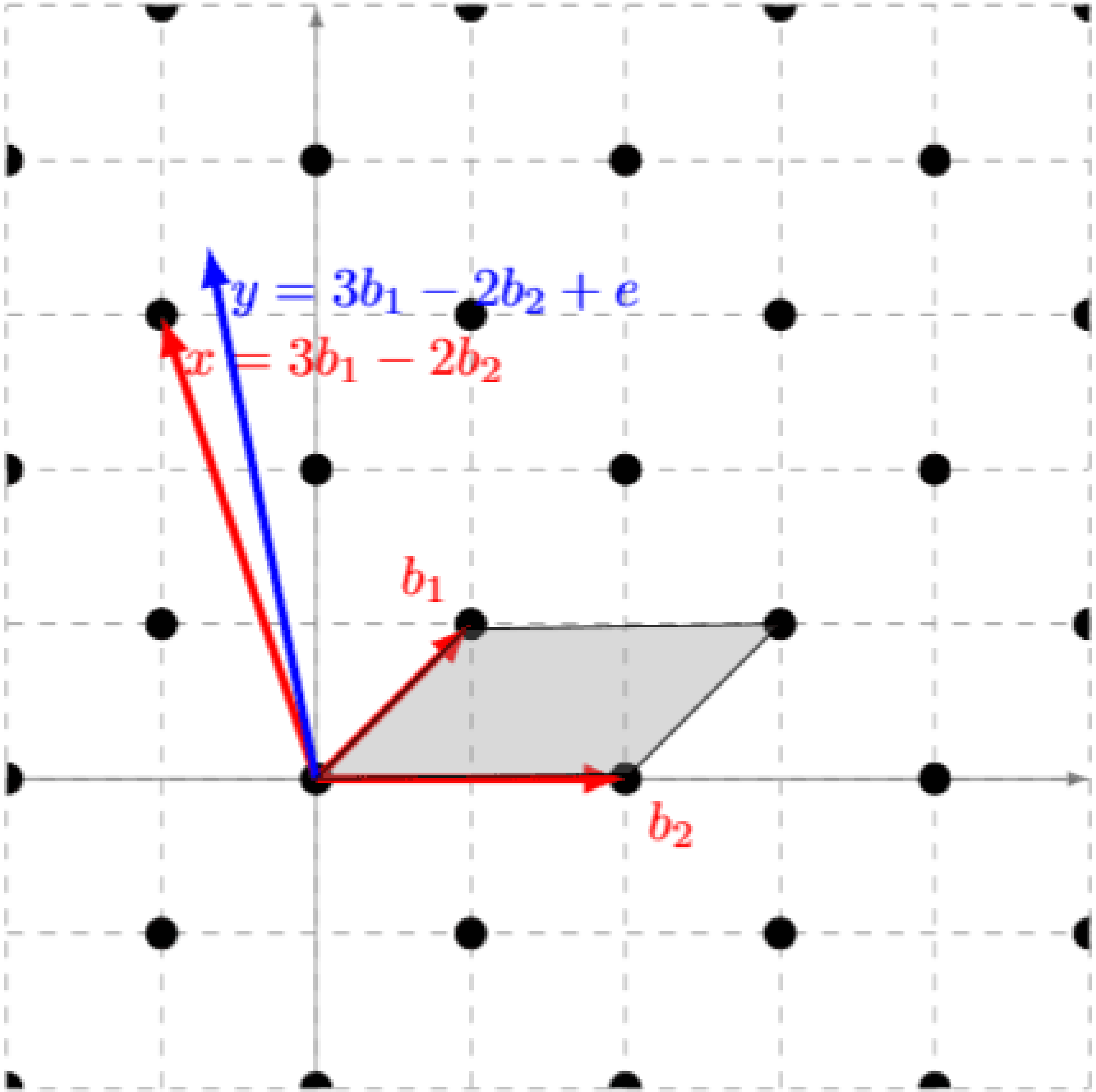


Table of Contents

Table of Contents

The basis

Definition

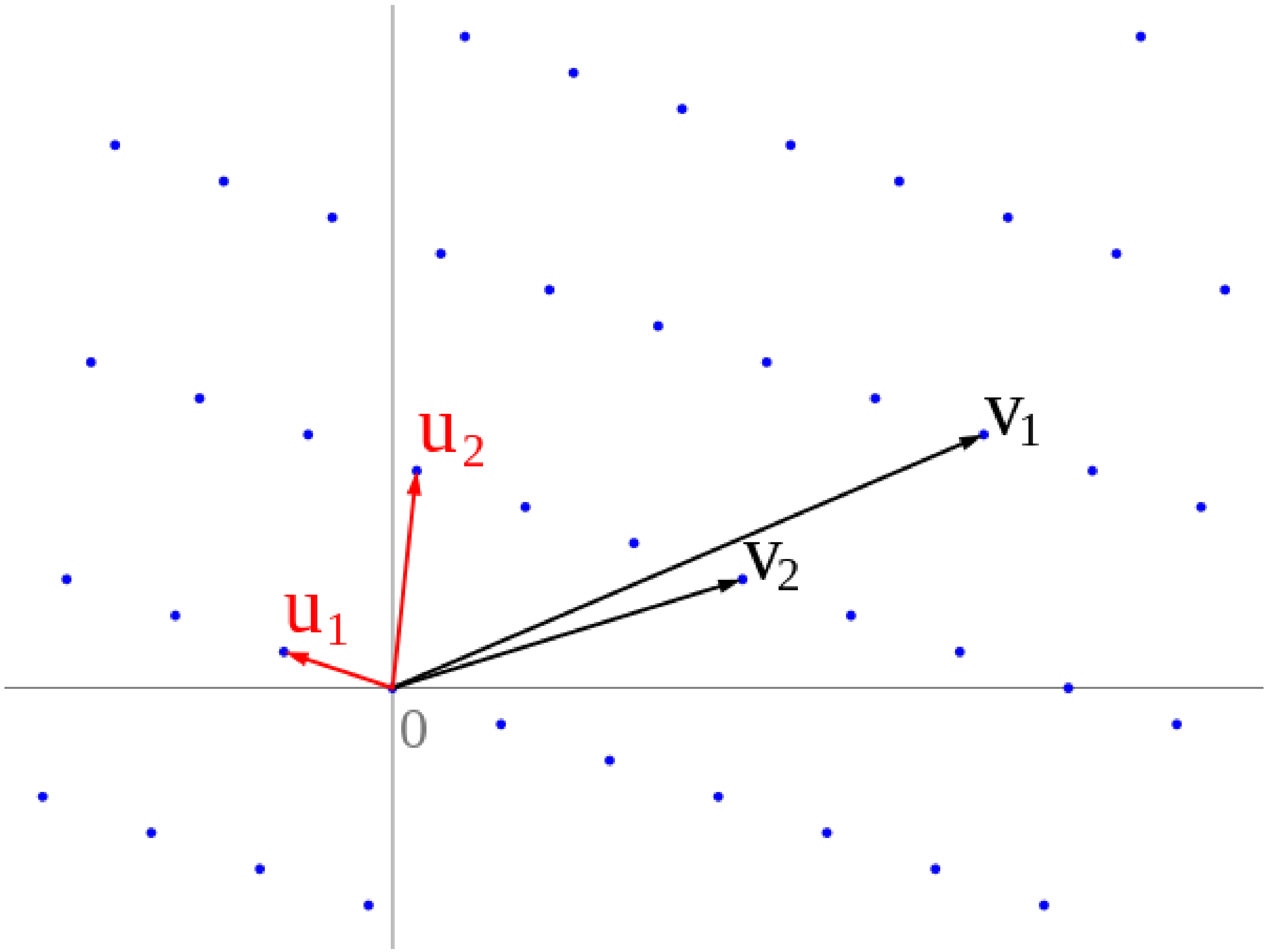
A lattice $\mathcal{L}$ is generated by all the integer combinations of the vectors of some basis B :

$$\mathcal{L}(b_1, \ldots, b_n) = \left\{ \sum_{i=1}^{m} z_i b_i | z_i \in \mathbb{Z}, b_i \in B \right\}.$$

The basis can be represented as $B = [b_1 \ldots b_n]$, and the definitions of a lattice will be:

$$\mathcal{L}(B) = \{Bz : z \in \mathcal{Z}^n\}$$

Lattice in 2D



Motivations

Basis reduction is a process of reducing the basis B of a lattice $\mathcal{L}$ to a shorter basis $B^{'}$ while keeping $\mathcal{L}$ the same. Basis reduction can help solving SVP, because if we cannot reduce a basis anymore, the shortest basis vector should be the shortest vector of the lattice.

Gram-Schmidt orthogonalisation process

LLL reduction

Table of Contents