LWE/(SIS)

and how they are related with lattice

Kurt Pan

ZKPunk.pro

November 12, 2024

Table of Contents

Table of Contents

What is Learning with Errors

Definition (LWE Distribution)

Let ϕ be a probability density function on $\mathbb{T}$, and $\mathbf{s} \in \mathbb{Z}_p^n$ denote the unknown secret vector. The LWE distribution $A_{\mathbf{s},\phi}$ is the distribution over $\mathbb{Z}_p^n \times \mathbb{T}$ obtained by choosing $\mathbf{a} \in \mathbb{Z}_p^n$ uniformly at random and $e \in \mathbb{T}$ according to ϕ, then outputting $\left(\mathbf{a}, \frac{1}{p}\langle \mathbf{a}, \mathbf{s} \rangle + e\right)$.

Definition (Decision-LWE)

Given a polynomial number of samples either from the distribution $A_{\mathbf{s},\phi}$ or independent and uniformly distributed samples from $\mathbb{Z}_p^n \times \mathbb{T}$, output

- YES if the samples are from the LWE distribution $A_{\mathbf{s},\phi}$, or
- NO if the samples are uniformly random over $\mathbb{Z}_p^n \times \mathbb{T}$.

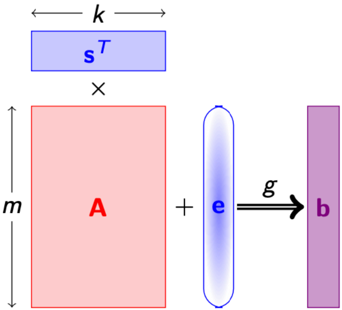


Table of Contents

What is Lattice

Definition (Lattice)

A discrete additive subgroup of $\mathbb{R}^n$

A lattice is the set of all *integer* linear combinations of (linearly independent) *basis* vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^n$:

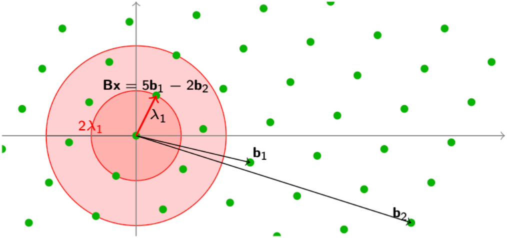
$$\mathcal{L} = \sum_{i=1}^{n} \mathbf{b}_i \cdot \mathbb{Z} = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^n\}$$

The same lattice has many bases

Shortest Vector Problem

Definition (SVP$_\gamma$)

Given a lattice $\mathcal{L}(\mathbf{B})$, find a (nonzero) lattice vector $\mathbf{Bx}$ (with $\mathbf{x} \in \mathbb{Z}^k$) of length (at most) $\|\mathbf{Bx}\| \leq \gamma\lambda_1$



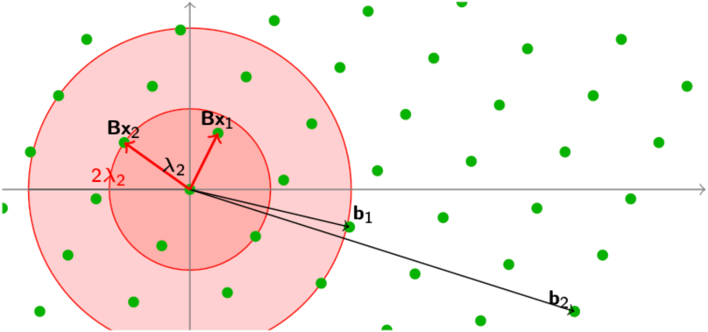
Minimum distance

$$\lambda_1 = \min_{\mathbf{x},\mathbf{y}\in\mathcal{L},\mathbf{x}\neq\mathbf{y}} \|\mathbf{x}-\mathbf{y}\| = \min_{\mathbf{x}\in\mathcal{L},\mathbf{x}\neq\mathbf{0}} \|\mathbf{x}\|$$

Shortest Independent Vectors Problem

Definition (SIVP_γ)

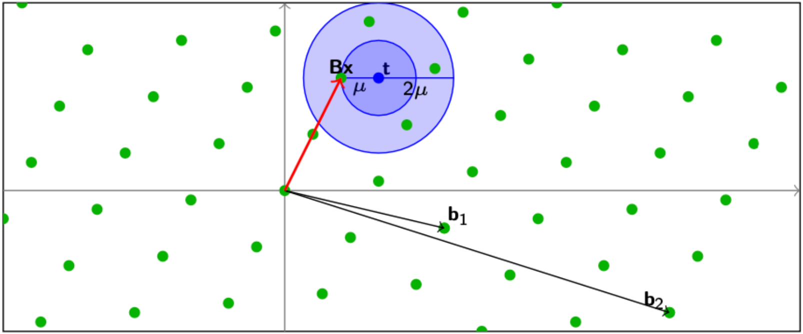
Given a lattice $\mathcal{L}(\mathbf{B})$, find n linearly independent lattice vectors $\mathbf{B}\mathbf{x}_1, \ldots, \mathbf{B}\mathbf{x}_n$ of length (at most) $\max_i \|\mathbf{B}\mathbf{x}_i\| \leq \gamma\lambda_n$



Closest Vector Problem

Definition (CVP$_\gamma$)

Given a lattice $\mathcal{L}(\mathbf{B})$ and a target point $\mathbf{t}$, find a lattice vector $\mathbf{Bx}$ within distance $\|\mathbf{Bx} - \mathbf{t}\| \leq \gamma\mu$ from the target



Special Versions of CVP

Definition

Given $(\mathcal{L}, \mathbf{t}, \boldsymbol{d})$, with $\mu(\mathbf{t}, \mathcal{L}) \leq \boldsymbol{d}$, find a lattice point within distance d from $\boldsymbol{t}$.

- If d is arbitrary, then one can find the closest lattice vector by binary search on d.
- *Bounded Distance Decoding (BDD)*: If $d < \lambda_1(\mathcal{L})/2$, then there is at most one solution. Solution is the closest lattice vector.
- *Absolute Distance Decoding (ADD)*: If $d \geq \mu(\mathcal{L})$, then there is always at least one solution. Solution may not be closest lattice vector.

Relations among lattice problems

- SIVP $\approx$ ADD [MG'01]
- SVP $\leq$ CVP [GMSS'99]
- SIVP $\leq$ CVP [M'08]
- BDD $\lesssim$ SIVP
- CVP $\lesssim$ SVP [L'87]
- GapSVP $\approx$ GapSIVP [LLS'91,B'93]
- GapSVP $\lesssim$ BDD [LM'09]

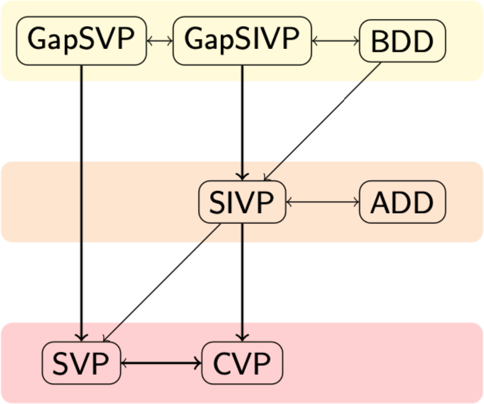


Table of Contents

Random lattices in Cryptography

- Cryptography typically uses (random) lattices $\wedge$ such that $\wedge \subseteq \mathbb{Z}^d$ is an integer lattice and $q\mathbb{Z}^d \subseteq \Lambda$ is periodic modulo a small integer q.
- Cryptographic functions based on q-ary lattices involve only arithmetic modulo q.

Definition (q-ary lattice)

Λ is a q-ary lattice if $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$

Examples (for any $\mathbf{A} \in \mathbb{Z}_q^{n\times d}$)

- $\Lambda_q(\mathbf{A}) = \left\{\mathbf{x} \mid \mathbf{x} \bmod q \in \mathbf{A}^T\mathbb{Z}_q^n\right\} \subseteq \mathbb{Z}^d$
- $\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \mid \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\} \subseteq \mathbb{Z}^d$

$$\mathcal{L}_q^{\perp}\left([\mathbf{A} \mid \mathbf{I}_n]\right) = \mathcal{L}\left(\begin{bmatrix} -\mathbf{I}_m & \mathbf{0} \\ \mathbf{A} & q\mathbf{I}_n \end{bmatrix}\right)$$

$$\mathbf{A} \in \mathbb{Z}_q^{m \times k}, \mathbf{s} \in \mathbb{Z}_q^k, \mathbf{e} \in \mathcal{E}^m.$$

$$g_{\mathbf{A}}(\mathbf{s}; \mathbf{e}) = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$$

Theorem (R'05)

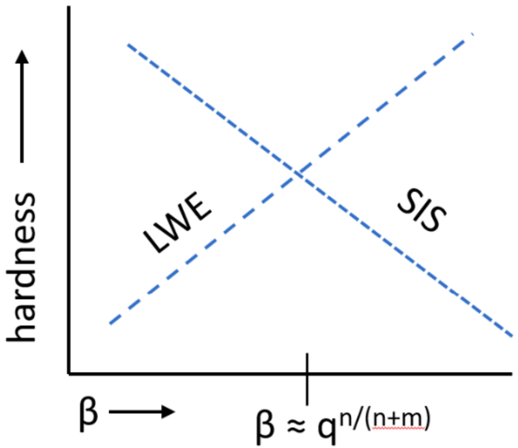
The function $g_{\mathrm{A}}(\mathbf{s}, \mathbf{e})$ is hard to invert on the average, assuming SIVP is hard to approximate in the worst-case.

How are they related?

LWE and q-ary lattices

- If $\mathbf{e} = \mathbf{0}$, then $\mathbf{As} + \mathbf{e} = \mathbf{As} \in \Lambda\left(\mathbf{A}^t\right)$
- Same as CVP in random q-ary lattice $\Lambda\left(\mathbf{A}^t\right)$ with random target $\mathbf{t} = \mathbf{As} + \mathbf{e}$
- Usually $\mathbf{e}$ is shorter than $\frac{1}{2}\lambda_1\left(\Lambda\left(\mathbf{A}^T\right)\right)$, and $\mathbf{e}$ is uniquely determined
- TAKE AWAY:
- LWE $\equiv$ Approximate BDD (Bounded Distance Decoding)

SIS for next time!



Thanks! Kob-khun kub!