Lattice

2021年4月19日 13:31

Recap:

Lattice. Given k independent vectors $b_1, \cdots, b_n \in \mathbb{R}^n$.

$$L(b_1, \cdots, b_n) = \left\{ \sum_{i=1,\cdots,k} x_i b_i \mid x_i \in \mathbb{Z} \right\}$$

Problems.

1. SVP: Given B. find the Shortest Vector $v \neq 0^n$, s.t. $\|v\|_2$ is the shortest in $L(B)$
2. t-Approximate SVP. Find $v \neq 0^n$. $\|v\|_2 \leq t \cdot \|v^*\|_2$.
3. $\lambda_1(L(B)) = v^*$
   $\lambda_2(L(B)) =$ SV length linearly independent with v^*
   ....
   $\lambda_n(L(B))$. ......

LLL Algorithm $\Rightarrow$ $2^{n/2}$ approximation. of SVP.

Ajtai's One-Way function

$2^m > q^n$, so range > image.

"$q = n^2$"

n, q, m, β. $q = poly(n)$, $m = \Omega(n \log q)$. $\beta = O(\sqrt{m})$

Matrix $\underset{n \times m}{A}$: $n\overset{m}{\boxed{A}} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$

$f_A(x) = A \cdot x \mod q$

$(x \in \{0,1\}^m$ s.t. $x \neq 0^m)$.

OWness: $\forall$ p.p.t Adv. $\exists$ negl ε. s.t.

$$\Pr_{A, x}[\,Adv(A, y = Ax \bmod p) \to x',\ Ax' \bmod q = y \text{ and } \|x'\| < \beta \ \&\ x \neq 0\,] < \varepsilon$$

Short-Integer Solution (SIS)

$A \leftarrow \mathbb{Z}_q^{n \times m}$. find x s.t. $Ax = 0 \bmod q$ $x \neq 0^n$ and $\|x\|_2 < \beta$

Theorem. $q = 2^{2n}$, $m = n^2$, $\beta = \sqrt{m}$

Then if $\exists$ algo solves SIS, then $\exists$ algo that solves t-approx-SBP for $t \in poly(n)$

Worst-Case to Average-Case Reduction.

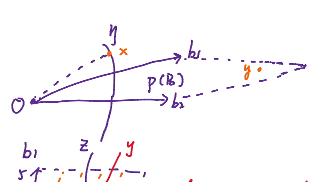
Shortest-basis

$v_1, \cdots, v_n$, $\|v_i\|_2 \leq \lambda_n \cdot t$

Pick η as the radius of a ball

$\eta \in \{2\lambda_n, \cdots, 2^n \lambda_n\}$

$x_i \leftarrow Ball^n(\eta)$

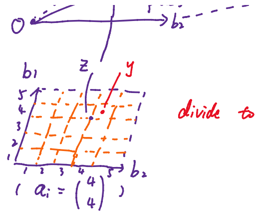


$y \in \{2\lambda_n, \cdots, 2^n \lambda_n\}$

$x_i \leftarrow \mathrm{Ball}^n(y)$

$y_i = x_i \bmod P(B)$

$a_i = \lfloor q B^{-1} y_i \rfloor \quad z_i = \frac{B a_i}{q}$



divide to q slides

Let $A = [a_1, \cdots, a_m]$

Suppose $\mathrm{Algo}(A) \rightarrow w \in \mathbb{Z}^m$, $\|w\|_2 \le \beta$. $Aw = 0 \bmod q$.

$\boxed{\sum_{i=1}^m w_i (x_i - y_i + z_i) \text{ is an approx. SVP.}}$

Prof.
1. a_i distributes evenly over $\mathbb{Z}_q^n$ (big y)
2. $v \in L(B)$.
3. v is short (small y)
4. v is not zero. (big y)

$\Rightarrow 2.\quad v = \sum_{i=1}^m w_i (\underbrace{x_i - y_i}_{\in L(B)} + z_i)$

$\sum_{i=1}^m w_i z_i = \sum_{i=1}^m w_i \frac{B a_i}{q} = B \sum_{i=1}^m \frac{w_i a_i}{q} \in L(B)$ ($\bmod q = 0$)

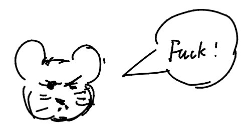
$\Rightarrow 3.\quad v = \sum_{i=1}^m w_i (x_i - y_i + z_i)$

$= \sum_{i=1}^m w_i x_i + \sum_{i=1}^m w_i (z_i - y_i)$ ① $\|w\|_2 < \beta$.

③ $y \sim \log n \cdot \lambda_n$ (compromise to 1. & 4.).

② intuitively bounded by $\frac{1}{q} \cdot$ diameter $(P(B))$. $q \sim 2^{2n}$

Learning with Errors



- Recap. Secret vector $s = [s_1, \cdots, s_n] \in \mathbb{Z}_q^n$

  Oracle $O(s) \Rightarrow \{\sum_{i=1}^n a_i s_i + e \bmod q ; a_i\}$, $a \xleftarrow{\$} \mathbb{Z}_q^n$, $e \xleftarrow{\$} [-B, B]$. $n \le B < q$

  Goal: Find s.

Define. Statistically close

X, Y. $X \approx_s Y$ if

distribution on A

$\sum_{a \in A} |\Pr[X=a] - \Pr[Y=a]| < \text{negl.}$

Given $n \boxed{A}_m$, $y = A^T s + e \bmod q$.

$e_i \leftarrow e^{-\frac{x^2}{\sigma^2}}$, $\sigma = O(\sqrt{n})$.

Decisional LWE

Decide either $(y = A^T s + e \bmod q)$

or $(y = U(\mathbb{Z}_q^m))$

Search LWE = Decision LWE

1) guess $S_1 = k$ Let $y' = y - A_1^T k + (h\, 0) \cdot k$, $A' = \begin{bmatrix} A_1 + h \\ A_{2\sim n} \end{bmatrix}$, $h \xleftarrow{\$} \mathbb{Z}_q^m$

i. if correct, A' & y' be another LWE $\Rightarrow$ not random

ii. if wrong, $A_1^T \cdot (k - S_1) = A_1(k - S_1) + h(k - S_1) = $ random

Public key Enc.

sk: LWE secret $s \leftarrow U(\mathbb{Z}_q^n)$

pk: LWE sample $A \leftarrow U(\mathbb{Z}_q^{n \times m})$ $m = \Omega(n \log q)$, $q = n^2$

$y = A^T s + e \bmod q$, $e \leftarrow X_\sigma$, $\sigma = O(\sqrt{n})$.

$\mathrm{Enc}(b \in \{0,1\}) = \underbrace{Ar \bmod q}_{z}, \underbrace{\langle y, r \rangle + b \lfloor \frac{q}{2} \rfloor \bmod q}_{v}$ $(r \in U_m)$

$\mathrm{Dec}_s(z, v) = \begin{cases} 1 & \text{if } |v - \langle s, z \rangle - \frac{q}{2}| < \frac{q}{4} \\ 0 & \text{if } |v - \langle s, z \rangle - 0| < \frac{q}{4} \end{cases}$

$v = \underbrace{s^T A r}_{\text{easily derived.}} + \underbrace{e^T r} + b \lfloor \frac{q}{2} \rfloor \bmod q.$

$e_i \leftarrow X_\sigma$

$\langle e, r \rangle \leftarrow X_{\sigma'} \cdot \sigma' = \sqrt{n}\, m \ll q$ $\Rightarrow$ Correctness

Security: $\mathrm{Enc}(0) \approx U(\mathbb{Z}_q^n \times \mathbb{Z}_q) \approx \mathrm{Enc}(1)$.

$\langle e, r\rangle \leftarrow \chi_{\sigma'} \cdot \sigma' = \sqrt{n}\, m \ll q$

Security: $Enc_{pk}(0) \approx_c \mathcal{U}(\mathbb{Z}_q^n \times \mathbb{Z}_q) \approx_c Enc_{pk}(1)$.

$A\cdot r,\ \langle y, r\rangle + b\lfloor \frac{q}{2} \rfloor,\ | A, y$

$\approx_c\ A\cdot r,\ \langle r', r\rangle + b\lfloor \frac{q}{2}\rfloor,\ | A, u \leftarrow \mathcal{U}(\mathbb{Z}_q^m)$

$\approx_c\ \mathcal{U}(\mathbb{Z}_q^n \times \mathbb{Z}_q)\ |\ \mathcal{U}(\mathbb{Z}_q^{n\times m}), u$.

Fully Homomorphic Encryption

Def. A (public key) encryption is called a fully homomorphic encryption if:

$\left\{ \begin{array}{l} Gen \rightarrow pk, sk. \\ Enc_{pk}(m, r) \rightarrow c \\ Dec_{sk}(c) \rightarrow m \end{array} \right.$ (Still, $\{pk, Enc_{pk}(m_1)\} \approx_c \{pk, Enc_{pk}(m_2)\}$ for security.

$Eval_{pk}(f, c_1, \cdots, c_k \in D_f) = C_{f, c_1, \cdots, c_k}$ and $Dec_{sk}(C_{f, c_1, \cdots, c_k}) = f(m_1, \cdots, m_k)$

$\forall f \in poly$

Only show $f = NAND$.

[Gentry, Sahai, Waters. 13] Learning with Error $\rightarrow$ levelled homomorphic Encryption

modulus $q = 2^{\ell}$ and $\log n < \ell < n$

Gadget Matrix

$g = \boxed{1\ 2\ 4\ \cdots\ 2^{\ell-1}}$

$G = \begin{pmatrix} g & & & \\ & g & & \\ & & \ddots & \\ & & & g \end{pmatrix} \in \mathbb{Z}^{n\times n\ell}$

Think about $Gx = t \mod q$ as a SIS problem (is trivial)

Define $G^{-1}(t) = \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_n \end{pmatrix}$, $\}\ell \rightarrow$ the bit decomposition of $t_1 \in \{0, \cdots, 2^{\ell}-1\}$

$\Rightarrow G \cdot G^{-1}(t) = t \mod q$

sk: $s \in \mathbb{Z}_q^n$ (LWE secret)

pk: $A \in \mathbb{Z}_q^{n\times m}$, $y = s^T A + e^T \mod q$.

where $e \leftarrow \chi_\sigma^m$. $q = 2^{\ell}$, $\sigma = \sqrt{n}$ $m = \Omega(n \log q)$

$m \in \{0, 1\}$

$Enc_{pk}(\mu)$:

1. $R \leftarrow \{0,1\}^{m \times (n+1)\ell}$
2. $C = \binom{A}{y} \cdot R + \mu G \mod q$ — Gadget $\in \mathbb{Z}^{(n+1)\times(n+1)\ell}$

$Dec_{sk}(C)$:

$$(s^T, -1)\cdot C = (s^T, -1)\binom{A}{y}\cdot R + \mu (s^T, -1) G$$

$$= (s^T A - y) R + \mu (s^T, -1) G$$

$$= \underbrace{-e^T R}_{\text{small}} + \mu (s^T, -1) G$$

If $\mu = 0$ 0.

$\mu = 1$. $(s, -1)\, G$ some entries $\approx \frac{q}{2}$

• $+ \mod q$:

$$C_1 + C_2 = C_+ = \underbrace{\binom{A}{y}(R_1+R_2)}_{\text{Small.}} + (\mu_1+\mu_2)G$$

• AND: C_1, C_2

Eval: $C_1 \cdot G^{-1}(C_2) \longrightarrow \left[\binom{A}{y}R_1 + \mu_1 G\right] G^{-1}(C_2)$

$$= \binom{A}{y}\underset{\{0,1\}}{R_1}\,\underset{\{0,1\}}{G^{-1}(C_2)} + \underbrace{\mu_1 C_2}_{\mu_1 BR_2 + \mu_1\mu_2 G}$$

small

$q >> m$

$$= B\tilde{R} + \mu_1\mu_2 G.$$

(where $\|\tilde{R}\|_\infty < m+1$)

Note that:

$$\underset{1}{\|R\|_\infty} \longrightarrow \underset{m+1}{\|\tilde{R}\|_\infty} \longrightarrow \underset{(m+1)^2}{\|\tilde{\tilde{R}}\|_\infty} \xrightarrow{\dot{\gamma}} (m+1)^{\dot{\gamma}}$$

Need $q > m^{\dot{\gamma}}$

level: (Reduce noise)

C, $Enc_{pk}(sk, r) = C_{sk}$

Eval (Dec-and-ReEnc, C_{sk}, C_m) $\to C_{m\text{fresh}}$