Сложность LWE

Monday 10 May 2021 12:49

I LWE vs. SIS

SIS: для $\underset{m}{\overset{\leftarrow n \rightarrow}{\boxed{A}}} \leftarrow \mathcal{U}(\mathbb{Z}_q^{m\times n})$, найти $x\in\mathbb{Z}^m$: $\overset{x^T}{\longleftrightarrow}\ \boxed{A} = 0 \bmod q$

$\|x\|\le\beta$

LWE: $\boxed{A}$, b $\begin{cases} As+e \ (\text{LWE}),\ e\leftarrow D_{\mathbb{Z}^m, \alpha q} \\ \leftarrow \mathcal{U}(\mathbb{Z}_q^n)\end{cases}$

<u>Утверждение</u> Если $\exists$ эффективный алг-м для SIS, то $\exists$ эффективный алг-м для LWE для $\alpha = \frac{1}{\beta\sqrt{m}}$.

Д. Вход: (A,b) – задача decision-LWE.

1. Запустить алг-м SIS для A. Получим $x\in\mathbb{Z}^m$, т.ч. $x^T\cdot A = 0 \bmod q$ и $\|x\|\le\beta$.
2. Вычислить $x^T b = \begin{cases} x^T\cdot A\cdot s + x^T e = x^T\cdot e, & \text{в случ. LWE} \Rightarrow \|x^T b\| = \|x^T e\| \le \|x\|\cdot\|e\| \le \beta\cdot\alpha q\sqrt{m} \\ x^T b, \text{иначе}, & x^T b\leftarrow \mathcal{U}(\mathbb{Z}_q) \Rightarrow \mathbb{E}[\|x^T b\|] = q/2. \end{cases}$ □

<u>Замечание</u> Эта редукция – частный случай редукции BDD к SIVP: по базису $\mathcal{B}$ решётки L и $t = Bx+e$ ($x\in\mathbb{Z}^m$, $\|e\| \lesssim \lambda_1/\gamma$), найти x. Редукция запускает алг-м SIVP с входным пар-ом B^{-T} – базис $\hat L$. Получает $\hat s_1 \dots \hat s_n$ – лин. независ. короткие вектора в $\hat L$ ($\max_i \|\hat s_i\| \le \gamma'\cdot\lambda_n(\hat L)$). Вычисляет

$$\underbrace{\hat S^T}_{\begin{bmatrix} - \hat s_1 - \\ \vdots \\ - \hat s_n - \end{bmatrix}}\cdot t = \underbrace{\hat S^T\cdot Bx}_{\in\mathbb{Z}^n} + \hat S^T\cdot e \equiv \hat S^T\cdot e \bmod 1$$

$$|\hat S^T e|_\infty \le \max_i |\langle \hat s_i, e\rangle| \le \max\|\hat s_i\|\cdot\|e\| \le \lambda_1(\hat L)\cdot\gamma'\cdot\frac{\lambda_1(L)}{\gamma} \le n\cdot\gamma'/\gamma$$

(т-ма переноса) transference thm

Если $n\cdot\gamma'/\gamma \le 1/4$, то $\hat S^T e \bmod 1 = \hat S^T\cdot e \Rightarrow$ знаем e (лин. алгебра).

Для SIS/LWE имеем решётки:

$L = A\cdot\mathbb{Z}_q^n + q\mathbb{Z}^m$ (LWE решётка; задача search-LWE = BDD в L)

$\hat L = \frac{1}{q}A^\perp = \frac{1}{q}\cdot\{x\in\mathbb{Z}^m : x^T\cdot A = 0 \bmod q\}$ (SIS = SVP в $\hat L$).

II Редукция от SIVP к BDD (Regev'05, SSTX'09)

Положим, имеем BDD оракул.

Задача: для базиса $\mathcal{B}$ решётки L, найти $s_1\dots s_n$ – лин. независ., т.ч. $\max_i\|s_i\| \le \gamma'\cdot\lambda_n(L)$.

<u>Шаг 1.</u> Построить суперпозицию:

$$\underbrace{\alpha \sum_{\substack{x\in\hat L \\ y\in\mathbb{R}^n}} D_s(y)\,|x\rangle|x+y\rangle}\quad (1)$$

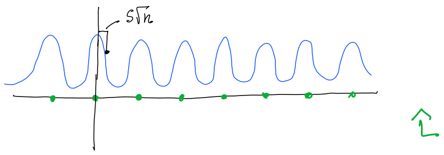
"равномерное" распр-ие на $\hat L$

+

гауссов вектор $y\leftarrow D_{\mathbb{Z}^m, s}$

‖

$x+y$



(!) $\nexists$ равномерного рас-ия на $\hat L$ $\Rightarrow$ задаём на $\hat L / K\hat L$ (K – большое)

(!) $\mathbb{R}^n$ – бесконечно, аппроксимируем $\mathbb{R}^n$ $\hat L\cdot\frac{1}{K'}$

Шаг 2. Классический BDD оракул (по $\overset{\in \hat{L}}{x}+y$, $\|y\| \le \lambda_1(\hat{L})/\gamma$, возвращает x) может быть использован в квантовом алг-ме:

$$|\cancel{***}\rangle |x+y\rangle \xmapsto{BDD^Q} |\cancel{***} + x\rangle |x+y\rangle$$

Применим BDD^Q ко 2-му регистру (1):

$$\sum_{\substack{x \in \hat{L} \\ y \in \mathbb{R}^n}} D_s(y) |-x\rangle |x+y\rangle \xrightarrow{BDD^Q} \sum_{\substack{x \in \hat{L} \\ y \in \mathbb{R}^n}} D_s(y) \underbrace{|0\rangle |x+y\rangle}_{\text{"забыть" 1ый регистр}} =$$

$$= \sum_{\substack{x \in \hat{L} \\ y,\, \|y\| \le \lambda_1(\hat{L})/\gamma}} D_s(y) |0\rangle |x+y\rangle + \sum_{\substack{x \in \hat{L} \\ y,\, \|y\| > \lambda_1(\hat{L})/\gamma}} D_s(y) |0\rangle |x+y\rangle .$$

Если $s \le \dfrac{\lambda_1(\hat{L})}{\gamma\sqrt{n}}$, то $\Pr\limits_{y \leftarrow D_s} \left[\|y\| < \dfrac{\lambda_1(L)}{\gamma} \right] \ge 1 - 2^{-\Omega(n)}$ $\Rightarrow$ $\sum\limits_{\substack{x \in \hat{L} \\ y,\, \|y\| > \lambda_1(\hat{L})/\gamma}} \dots$ имеет экспоненциально малый вес в сумме.

$\Rightarrow$ имеем $\underbrace{\sum\limits_{\substack{x \in L \\ y}} D_s(y) |x+y\rangle}$ (2)

кодирует распределение $1_{\hat{L}} * D_s$ (равномерное на $\hat{L}$ конволюция с D_s)

$$\widehat{1_{\hat{L}} * D_s} = \widehat{1_{\hat{L}}} \cdot \widehat{D_s} = 1_L \cdot D_{1/s} = D_{L, 1/s}.$$

Применяем QFT: (эффективный алг-м) $(2) \xrightarrow{QFT} \sum\limits_{x \in L} D_{1/s}(x) |x\rangle \xrightarrow{\gamma} x \leftarrow D_{L, 1/s}$ (в точности до $\sqrt{2}$ в s)

Для $s = \dfrac{\lambda_1(\hat{L})}{\gamma\sqrt{n}}$, $1/s = \dfrac{(\gamma\sqrt{n})}{\lambda_1(\hat{L})}$ и $\underset{\text{(Гауссов хвост)}}{\|x\| \le \dfrac{\sqrt{n}}{s}} = \dfrac{\gamma n}{\lambda_1(\hat{L})} \underset{\text{(TRANSFERENCE)}}{\le \gamma \cdot n \cdot \lambda_n(L)} \Rightarrow \gamma' = \gamma \cdot n.$

Повторив эту процедуру $poly(n)$ раз, получим $x_1 \dots x_n$ – лин. независ. (P