LWE

Monday 10 May 2021 11:01

Задача обучения с ошибками
Learning with Errors (LWE).

Regev'05 "On lattices, learning with errors, random linear codes, and cryptography".

I Определение задачи LWE

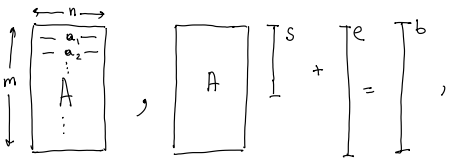
- Распределение LWE $D_{n,q,\alpha}(s)$: для параметров $n \geq 1$, $q \geq 2$, $\alpha \in (0,1)$ и секрета $s \in \mathbb{Z}_q^n$,

  1) Выбрать $a \xleftarrow{\$} \mathbb{Z}_q^n$

  2) выбрать $e \leftarrow D_{\mathbb{Z}, \alpha \cdot q}$ - Гауссово р-ие со средне кв. отклонением αq

  Выход: $(a, b = \langle a, s \rangle + e \mod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$

- Задача поиска $LWE_{n,q,\alpha}$ (search-LWE): $\exists\, s \in \mathbb{Z}_q^n$ - фиксировано. Имея выборку из распределения LWE $D_{n,q,\alpha}(s)$ произвольного р-ра, найти s. Т.е.

  Дано: 

  , Найти s (или e).

- Задача принятия решения $LWE_{n,q,\alpha}$. (decision-LWE): Имея выборку либо из $D_{n,q,\alpha}(s)$ для фикс. s, либо выборку из $U(\mathbb{Z}_q^n \times \mathbb{Z})$ произвольного р-ра, понять, какая выборка дана.

  (формально: построить ppt A т.ч. $\Pr_{S \leftarrow U(\mathbb{Z}_q^n)} \left[\left| \Pr\left[A^{D(s)} \to 1\right] - \Pr\left[A^{U} \to 1\right] \right| \geq 1/\mathrm{poly}(n) \right] \geq 1/\mathrm{poly}(n)$)

Сложность задачи относ. пар-ров:

- $\alpha = 0 \Rightarrow$ LWE тривиально (решение лин. ур-ий)
- $\alpha = 1 \Rightarrow$ LWE сложно ($\langle a, s \rangle + e \sim U(\mathbb{Z}_q)$, ОТР). ; обычно $\alpha = 1/\mathrm{poly}(n)$
- Чем больше n (при фикс. q, α), тем сложнее LWE
- Типичные пар-ры: $n = O(\lambda)$; $\approx 800\text{-}1000$ $q = n^2$; $\alpha = 1/\mathrm{poly}(n)$, $m = \Theta(n)$.

II Задача поиска LWE ≈ Задача принятия решений LWE

(для $\alpha = O\left(\frac{1}{\sqrt{n}}\right)$, $q = \mathrm{poly}(n)$, q - простое)

- Направление "decision-to-search" тривиально (подать на вход алг-му SearchLWE выборку; если он вернёт s' выдать это s' за ответ);

  Как проверить s'? (кандидата на секрет?)

  Для новой выборки $(a_i, b_i)_i$ вычислить $b_i - \langle s', a_i \rangle = \begin{cases} e_i, \text{ если LWE}, & |e_i| \leq \alpha q \sqrt{n} \text{ с в-ю } 1 - 2^{-\Omega(n)} \\ \sim U(\mathbb{Z}_q), \text{ иначе} & \text{т.к. } b_i \sim U(\mathbb{Z}_q^n). \end{cases}$

  Проделать этот тест n раз. Если хотя бы одна проверка вернула $e_i > \alpha q \sqrt{n}$, вернуть "не LWE".

- Направление Search-to-Decision.

  $\exists\, s^*$ - секрет. Найдем $s_1^* \in \mathbb{Z}_q$

  Пусть $s_1' \in \mathbb{Z}_q$ - предположение о значении s_1^*. Проверим его с помощью алгоритма decision-LWE.

  $(a_i, b_i) = (a_i, \langle a_i, s^* \rangle + e_i \mod q) \longrightarrow \left(a_i + \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \langle a_i, s^* \rangle + e_i + s_1'\right)$

  ↗ корректная выборка из $D(s^*)$ для верного s_1'

  ↘ случ. равномерная выборка для неверного s_1' (для простого q).

  s_1^* $\langle (1,0,\dots,0), s^* \rangle$

  $\langle a_i + (1,0,\dots,0), s^* \rangle + e_i$

  Редукция работает за $O(q \cdot n)$ вызовов decision-LWE для восстановления s^*.