Лекция № 16

Задача обучения с ошибками. (Learning with Errors, LWE)

I Определение задачи LWE

O. Regev "On lattices, learning with errors, random linear codes, and cryptography", 2005.

• Распределение LWE $D^{LWE}_{n,q,\alpha}(s)$: для пар-ов $n \geq 1$, $q \geq 2$, $\alpha \in (0,1)$ и секрета $s \in \mathbb{Z}_q^n$:

1. Выбрать $a \xleftarrow{\$} \mathbb{Z}_q^n$
2. Выбрать $e \leftarrow D_{\mathbb{Z}, \alpha q}$ - Гауссово распределение со средним. 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): $\exists s$ - фиксировано. Имея выборку из распр-я LWE $D^{LWE}_{n,q,\alpha}(s)$ произвольного размера, найти s.

Дано:

$$\overset{\leftarrow n \rightarrow}{\begin{matrix} \uparrow \\ m \\ \downarrow \end{matrix}} \begin{bmatrix} - & a_1 & - \\ - & a_2 & - \\ & \vdots & \\ - & a_m & - \end{bmatrix}; \quad \begin{bmatrix} & \\ & A \\ & \end{bmatrix} \begin{bmatrix} | \\ s \\ | \end{bmatrix} + \begin{bmatrix} | \\ e \\ | \end{bmatrix} = \begin{bmatrix} | \\ b \\ | \end{bmatrix} \mod q.$$

Найти: s (или e)

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

Формально: построить эффективного атакующего A (т.е. вероятностного poly-time A), такого что

$$\Pr_{s \leftarrow U(\mathbb{Z}_q^n)} \left[\left| \Pr\left[A^{D^{LWE}(s)} \rightarrow 1\right] - \Pr\left[A^{U} \rightarrow 1\right] \right| \geq \frac{1}{poly(n)} \right] \geq \frac{1}{poly(n)}$$

Сложность задачи LWE относительно пар-ов.

1. $\alpha = 0$, $\alpha \cdot q = 0 \Rightarrow$ LWE тривиально (решение лин. ур-ий)
2. $\alpha = 1 \Rightarrow$ LWE сложно $(\langle a, s \rangle + e \sim U(\mathbb{Z}_q) \Rightarrow$ OTP$)$

   обычно $\alpha = \frac{1}{poly(n)}$
3. Чем больше n (при фикс. α, q), тем сложнее LWE
4. Типичные пар-ры для криптосистемы: $n \sim 800 \div 1000$, $q \sim n^2$, $\alpha = \frac{1}{poly(n)}$, $m = \Theta(n)$

II Задача поиска LWE ≃ Задача принятия решения

(для $\alpha = O(\frac{1}{\sqrt{n}})$, $q = poly(n)$, q – простое)

- Направление "decision-to-search" (от принятия решения к поиску)

  Тривиально: Подать на вход алг-му Search-LWE выборку, полученную от decision-LWE. Если алг-м вернёт s, выдать "LWE" за ответ.

- Направление "search-to-decision"

  $\exists s^*$ – секрет. Найдём $s_1^* \in \mathbb{Z}_q$.

  Пусть $s_1' \in \mathbb{Z}_q$ – предположение о значении s_1^*.

  Проверим его с помощью алгоритма decision-LWE.

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

  – Если $s_1' = s_1^*$, то $\left(a_i + (1,0,\dots,0)^t, \langle a_i, s^* \rangle + e_i + \underbrace{s_1'}_{s_1^*}\right) =$

  $= (a_i + (1,0,\dots,0)^t, \langle a_i + (1,0,\dots,0)^t, s^* \rangle + e_i \bmod q)$ $\langle (1,0,\dots,0), s^* \rangle \rightarrow$

  $\rightarrow$ корректная выборка из $D^{LWE}_{n,q,\alpha}(s^*)$.

  – Если $s_1' \neq s_1^*$, получаем случ. равномерную выборку из $U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$

Запускаем decision-LWE оракул на модифицированной выборке.

Редукция работает за $O(q \cdot n)$ вызовов оракула Decision-LWE для получения s^*.

III HNF-форма LWE

(Hermite Normal Form / эрмитова нормальная форма)

означает, что секрет s выбран не из произвольного распределения над $\mathbb{Z}_q^n$, а из $D_{\mathbb{Z}^n, \alpha q}$, т.е. аналог вектору ошибки.

HNF-форма и "обычная" форма LWE эквивалентны по сложности, т.к. $\exists$ отображение м/д ними. А именно,

$\forall (a_i^*, b_i^*)_{1 \le i \le n}$, т.ч a_i^* - лин. независимы в $\mathbb{Z}_q^n$. Составим матрицу

$$A^* = \begin{bmatrix} - & a_1^* & - \\ & \vdots & \\ - & a_n^* & - \end{bmatrix} \text{ - обратима}, \quad b^* = (b_1^* \dots b_n^*).$$

"$A^* \cdot s + e^*$"

Для каждой последующей пары (a, b) из "обычного" LWE, отобразить

$$(a, b) \to (a', b'), \text{ где } \left(a' = (A^*)^{-T} \cdot a,\ -b + \langle (A^*)^{-T} \cdot a, b^* \rangle\right)$$

- Если $(a, b) \leftarrow U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$, то $(a', b') \sim U(\mathbb{Z}_q^n \times \mathbb{Z}_q)$
- Если $(a, b) \leftarrow D^{LWE}_{n,q,\alpha}$, то $a' = (A^*)^{-T} \cdot a \sim U(\mathbb{Z}_q^n)$, и

$$-b + \langle A^{*-T} \cdot a, b^* \rangle = -\langle a, s \rangle - e + (A^{*-T} \cdot a)^T \cdot (A^* s + e^*)$$

$$= -a^T s - e + a^T \underbrace{(A^{*-T})^T}_{A^{*-1}} \cdot A^* \cdot s + a^T \cdot (A^*)^{-1} e^* = a^T \cdot (A^*)^{-1} \cdot e^* - e$$

$a^T \cdot s$

$$= \underbrace{(A^{*-T} \cdot a)}_{a'} \cdot e^* - e =$$

$$= \langle a', e^* \rangle - e.$$

↑ новый секрет

IV PKE n, m, q, λ – фиксированы

- KeyGen

$$pk = \boxed{A} \leftarrow U(\mathbb{Z}_q^{m \times n}), \quad \begin{bmatrix} \\ \\ b \end{bmatrix} = \boxed{A} \begin{bmatrix} \\ \\ s \end{bmatrix} + \begin{bmatrix} \\ \\ e \end{bmatrix} \bmod q, \text{ где } s \leftarrow D_{\mathbb{Z}_q^n, \sigma_q},\ e \leftarrow D_{\mathbb{Z}_q^m, \sigma_q}$$

$$sk = s$$

- Enc $(pk, \mu \in \{0,1\})$

1. $t \leftarrow D_{\mathbb{Z}_q^m, \sigma_q}$; $f \leftarrow D_{\mathbb{Z}_q^n, \sigma_q}$; $f' \leftarrow D_{\mathbb{Z}, \sigma_q}$

2. $c_1 = \begin{bmatrix} t^T \end{bmatrix} \boxed{A} + \begin{bmatrix} f^T \end{bmatrix} \bmod q \in \mathbb{Z}_q^n$

$$c_2 = \begin{bmatrix} t^T \end{bmatrix} \cdot \begin{bmatrix} \\ \\ b \end{bmatrix} + f' + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor \bmod q \in \mathbb{Z}_q$$

$$c = (c_1, c_2)$$

- Dec $(sk, c = (c_1, c_2))$

$$c_2 - c_1^T \cdot s = t^T \cdot b + f' + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor - t^T \cdot A \cdot s - f^T \cdot s =$$

$$= t^T A s + t^T e + f' + \mu \left\lfloor \frac{q}{2} \right\rfloor - t^T A s - f^T s =$$

$$= t^T e + f' - f^T s + \mu \left\lfloor \frac{q}{2} \right\rfloor$$

$$\leq \sqrt{\sum_{i=1}^{m} (d_q \sqrt{n})^2 \cdot \|e\|^2} + d_q \cdot \sqrt{n} + \sqrt{\sum_{i=1}^{n} (d_q \sqrt{n})^2 \|f\|^2}$$

$$\leq 3 d_q \left(\sqrt{m} + \sqrt{n}\right)^2 \overset{!}{\leq} \frac{q}{4} \Rightarrow \text{схема корректна.}$$

Если $|c_2 - c_1^T \cdot s|$ близко к $\frac{q}{2}$, то $\mu = 1$

Если $|c_2 - c_1^T \cdot s|$ близко к 0, то $\mu = 0$

Безопасность (IND-CPA): злоумышленник, зная pk, не может отличить indistinguishability under chosen plaintext attack)

$Enc(pk, 0)$ от $Enc(pk, 1)$, т.е. $(pk, Enc(pk, 0)) \approx (pk, Enc(pk, 1))$.

Имеем, $(\underbrace{A, As+e}_{pk}, t^T \cdot A + g^T, \underbrace{t^T(As+e) + g' + 0}_{Enc(0)})$

$\approx_{decision\text{-}LWE}$ (вычислительно экв-но под предположением трудности задачи decision-LWE)

$(A, b \in U(\mathbb{Z}_q^m), t^T \cdot A + g^T, t^T \cdot b + g')$

$m \left[\begin{array}{c|c} A & b \end{array}\right]$, $t \left[\begin{array}{c|c} A & b \end{array}\right] + \begin{array}{|c|c|} \hline g^T & g' \\ \hline \end{array}$

новая выборка LWE

$\approx$ вычислительно неотличимо от случайного равномерного под предположением ∂ LWE.

Аналогично для $Enc(pk, 1)$: все публичные эл-ты неотличимы от случайных равномерных величин. $\Rightarrow$

$\Rightarrow Enc(pk, 0) \approx Enc(pk, 1)$.