I. "Потайной ход" (trapdoor) для задачи SIS (Micciancio-Peikert'12)

Задача: выбрать $A \leftarrow U(\mathbb{Z}_q^{m\times n})$ вместе с коротким базисом решётки $A^\perp$.

$$A^\perp = \{x \in \mathbb{Z}^m : \; x\cdot A = 0 \mod q\}.$$

Начнём с A особого вида, называющейся гаджетом.

$$g = \begin{bmatrix} 1 \\ 2 \\ \vdots \\ 2^{k-1} \end{bmatrix} \in \mathbb{Z}^k$$

Лемма Если q – степень 2-ки, положим $k = \log_2 q$ и $S_k = \begin{bmatrix} 2 & -1 & & \\ & 2 & -1 & \\ & & \ddots & -1 \\ & & & 2 \end{bmatrix}$, $\begin{pmatrix} 1 \\ 2 \\ \vdots \\ 2^{k-1}\end{pmatrix}$

Иначе, положим $k = \lceil \log_2 q \rceil$ и ($q = \sum 2^i q_i$), $S_k = \begin{bmatrix} 2 & -1 & & & \\ & 2 & -1 & & \\ & & \ddots & & \\ & & & 2 & -1 \\ q_0 & q_1 & \cdots & & q_{k-1} \end{bmatrix}$.

Тогда S_k – базис $g^\perp$ и $\forall i$: $\|s_i\| \le \sqrt{5}$ (s_i – i-ый столбец)

◁ 1. $S_k \cdot g = 0 \mod q$

2. $\det S_k = q$ (во втором случае $\det[S_k] = (-q_0) + 2\cdot\det\begin{bmatrix} 2 & -1 & \\ & 2 & \\ q_1 & q_2 & \ldots \end{bmatrix} + \ldots$

3. Покажем, что и $\det g^\perp = q$ (отсюда, т.к. $g^\perp \subset \mathbb{Z}^k$ и $S_k \cdot \mathbb{Z}^k \subset \mathbb{Z}^k$, S_k – базис $g^\perp$).

$*$ $\varphi: \mathbb{Z}^k \to \mathbb{Z}_q$, $x \mapsto x^T g \mod q$ – сюрьекция $\Rightarrow \mathbb{Z}_q \cong \mathbb{Z}^k / \mathrm{Ker}\,\varphi = \mathbb{Z}^k / g^\perp$

$\Rightarrow q = \#\mathbb{Z}_q = \#(\mathbb{Z}^k / g^\perp) = \dfrac{\det g^\perp}{\det \mathbb{Z}^k} = \det g^\perp$ ▶

Опр-ие Положим

$$G = \begin{bmatrix} g & & & \\ & g & & \\ & & \ddots & \\ & & & g \end{bmatrix} = g \otimes I_\ell \in \mathbb{Z}_q^{\ell\cdot k \times \ell}, \qquad S = S_k \otimes I_\ell = \begin{bmatrix} S_k & & \\ & S_k & \\ & & S_k \end{bmatrix} \text{ – базис } G^\perp$$

Пусть $A \in \mathbb{Z}_q^{m\times n}$, $G \in \mathbb{Z}_q^{w\times n}$; Тогда $R \in \mathbb{Z}^{w\times(m-w)}$ называется G – "потайным ходом" для A, если (G-trapdoor)

$$\underbrace{\begin{bmatrix} R & I_w \end{bmatrix}}_{m} \cdot \begin{bmatrix} A \end{bmatrix} = \begin{bmatrix} G \end{bmatrix}$$

Нас будет интересовать малое R.

Замечание "Потайной ход" для G + R $\Rightarrow$ "потайной ход" для A.

Лемма] $S \in \mathbb{Z}^{w\times w}$ как опр-но выше, (базис G) R – G-trapdoor для A, и W: $\begin{bmatrix} W \end{bmatrix} \cdot \begin{bmatrix} G \end{bmatrix} = \begin{bmatrix} -I & 0 \end{bmatrix} \cdot \begin{bmatrix} A \end{bmatrix}$.

Тогда $S_A = \begin{bmatrix} I & W \\ 0 & S \end{bmatrix} \cdot \begin{bmatrix} I & 0 \\ R & I \end{bmatrix}$ – "потайной ход" для A.

◁ (на практике)

1. Показать, что $S_A \cdot A = 0 \mod q$: $\begin{bmatrix} I & W \\ 0 & S \end{bmatrix} \cdot \underbrace{\begin{bmatrix} I & 0 \\ R & I \end{bmatrix} \cdot \begin{bmatrix} A \end{bmatrix}}_{\begin{bmatrix} -W\cdot G \\ G \end{bmatrix}} = \begin{bmatrix} I & W \\ 0 & S \end{bmatrix} \cdot \begin{bmatrix} -W\cdot G \\ G \end{bmatrix} = \begin{bmatrix} 0 \\ \underbrace{S\cdot G}_{0} \end{bmatrix} \mod q.$

2. $\det S_A = \det S = \det(S_k \otimes I_n) = q^n$

$\Rightarrow$ достаточно показать, что $\det A^\perp = q^n$.

| опр-м $\mathbb{Z}^w \to \mathbb{Z}_q^n$, $x \mapsto x^T\cdot G$ – сюрьекция

$\Downarrow$

$\varphi: \mathbb{Z}^m \to \mathbb{Z}_q^n$, $x \mapsto x^T\cdot A$ – сюрьекция (для $y \in \mathbb{Z}_q^n$: $y = x^T\cdot G$ для какого-то $\mathbb{Z}$)

$y = x^T \underbrace{[R|I]\cdot A}_{G}$

$\Rightarrow$ биекция $\mathbb{Z}_q^n \cong \mathbb{Z}^m / \mathrm{Ker}\,\varphi = \mathbb{Z}^m / A^\perp \Rightarrow q^n = \det A^\perp$. ▶

Как получить G-потайной ход для A?

$$\underbrace{\begin{bmatrix} R & I \end{bmatrix}}_{\text{мало}} \cdot \begin{bmatrix} A \end{bmatrix} = G \mod q$$

(A — случ. равномерно из $\mathbb{Z}_q^{m\times n}$)

Лемма. (Гауссов остаток / Left-over hash lemma).

Пусть $A \leftarrow U(\mathbb{Z}_q^{m\times n})$, $u \leftarrow U(\mathbb{Z}_q^n)$, $r \leftarrow D_{\mathbb{Z}^m, \sigma, 0}$ для $m \geqslant n \cdot \lg q$, $\sigma \geqslant \sqrt{m}$, q — простое.

Тогда $\Delta\left[(A, r \cdot A), (A, u) \right] \leqslant 2^{-\Omega(n)}$.

$\triangleleft$ (док-во на практике) ① $\varphi_A : \mathbb{Z}^m \to \mathbb{Z}_q^n$ — сюрьекция (при условии, строки A образуют $\mathbb{Z}_q^n$, что верно с в-ю ~ 1).

$x \longmapsto x^t \cdot A \mod q$

$\Rightarrow \mathbb{Z}_q^n \cong \mathbb{Z}^m / A^\perp \Rightarrow$

$D_{\mathbb{Z}^m, \sigma} \cdot A$ — равном. случайно $\Leftrightarrow D^T_{\mathbb{Z}^m, \sigma} \mod A^\perp$ равн. случайно в $\mathbb{Z}^m / A^\perp$.

$$\Pr_{b \leftarrow \mathbb{Z}^m}\left[b \text{ — класс смежности в } A^\perp \right] = \frac{\rho_\sigma(b + A^\perp)}{\rho_\sigma(\mathbb{Z}^m)} \simeq \frac{\rho_\sigma(A^\perp)}{\rho_\sigma(\mathbb{Z}^m)}$$

в точности до множителя $[1 \pm 2^{-\Omega(n)}]$, независ. от b, если $\sigma \geqslant \eta_{2^{-n}}(A^\perp)$.

② $\eta_{2^{-n}}(A^\perp) \leqslant \dfrac{\sqrt{m}}{\lambda_1(\widehat{A^\perp})}$, $\widehat{(A^\perp)} = \dfrac{1}{q} L_q(A) = \dfrac{1}{q}\left(A \cdot \mathbb{Z}_q^n + q\mathbb{Z}^m\right)$

Т-ма Минковского – Хлавки: $\Pr_A\left[\lambda_1^\infty (L_q(A)) \leqslant c \cdot q \right] \leqslant 2^{-\Omega(n)}$

$\Rightarrow \lambda_1(\widehat{A^\perp}) = \dfrac{1}{q} \lambda_1(L_q(A)) \geqslant \dfrac{1}{q} \lambda_1^\infty (L_q(A)) \geqslant \Omega(1)$ с в-тью $\geqslant 1 - 2^{-\Omega(n)}$ (относ. случ. выбора A).

$\Rightarrow \eta_{2^{-n}}(A^\perp) \leqslant \Omega(\sqrt{m})$.

③ В-ть того, что $\mathbb{Z}_q^m \cdot A$ образует $\mathbb{Z}_q^n$ есть $1 - 2^{-\Omega(n)}$

① + ② + ③ $\Rightarrow \Delta\left(D^T_{\mathbb{Z}^m, \sigma} \cdot A,\ U(\mathbb{Z}_q^n) \right) \leqslant 2^{-\Omega(n)}$.

Вывод: Для того, чтобы сгенерировать G-лазейку для A:

$$\overset{\bar m}{\begin{bmatrix} R & I \end{bmatrix}} \cdot \begin{bmatrix} A_{top} \\ A_{bot} \end{bmatrix} = \begin{bmatrix} G \end{bmatrix} \mod q$$

1) Выбираем $A_{top} \leftarrow U(\mathbb{Z}_q^{\bar m \times n})$, $\bar m$ удовл. условиям леммы
2) Выбираем $R \leftarrow D_{\mathbb{Z}_q^{\bar m}, \sigma}$
3) Вычисляем $A_{bot} = G - \underbrace{R \cdot A}_{\text{случ. равном. согласно лемме}}$

(R — мало (||строка R|| $\leqslant \sigma\sqrt{\bar m}$ с в-тью $\geqslant 1 - 2^{-\Omega(n)}$))

II Подпись GPV (Gentry - Peikert - Vaikuntanathan)

Подпись = [KeyGen, Sign, Verify] — эффективные алг-мы:

- $KeyGen(1^n) \to (sk, vk)$
- $Sign(m, sk) \to \sigma$
- $Verify(vk, m, \sigma) \to \{0, 1\}$

Корректность: $\forall m$: $Verify(vk, m, Sign(m, sk)) = 1$ с в-ью $\geqslant 1 - 2^{-\Omega(n)}$ над случ. битами $Sign()$ и $KeyGen()$.

$\boxed{\text{Безопасность}}$ UF-CMA игра

$\mathcal{C}$ (чаллeнджер) $\qquad\qquad \mathcal{A}$ (атакующий)

- (sk, vk)

$\xrightarrow{\quad vk \quad}$

$\xleftarrow{\quad m_i \quad}$

$\xrightarrow{\sigma_i = Sign(sk, m_i)}$

$\xleftarrow{\quad (m^*, \sigma^*) \quad}$

$\mathcal{A}$ побеждает, если $Verify(vk, m^*, \sigma^*) = 1$ и $m^* \notin \{m_i\}_i$.

Подпись UF-CMA — безопасна, если $\nexists$ эффективного $\mathcal{A}$, который побеждает с непренебрежимо малой вер-ью.
(unforgeability under chosen message attack)

$\boxed{\text{Модель случайного оракула (ROM)}}$

Хэш-ф-ия $H()$, используемая в подписи, моделируется как случ. ф-ия и находится под контролем $\mathcal{C}$.
В игре UF-CMA $\mathcal{A}$ может делать хэш-запросы.

GPV – подпись

- **KeyGen:** 1. Построить A, S_A, т.ч. $\underbrace{S_A}_{\text{короткие векторы}} \cdot \underbrace{A}_{m \times n} = 0 \mod q$

  $sk = S_A$, $pk = A$

- **Sign** $(m \in \{0,1\}^*, sk)$
  1. Вычислить $u = Hash(m) \in \mathbb{Z}_q^n$, $H: \{0,1\}^* \to \mathbb{Z}_q^n$ – криптогр. хэш-ф-ция;
  2. Вычислить произвольный $c \in \mathbb{Z}^m$ т.ч. $c^T \cdot A = u^T \mod q$ (таких c много)
  3. Выбрать $x \leftarrow D_{A^\perp, s, -c} + c$, $s = \|S_A\| \cdot \sqrt{m}$

     $\{ x^T \cdot A = (\underset{\in A^\perp}{v} + c) \cdot A = \underset{= 0}{v \cdot A} + cA = u \mod q \}$

     $\sigma = x$

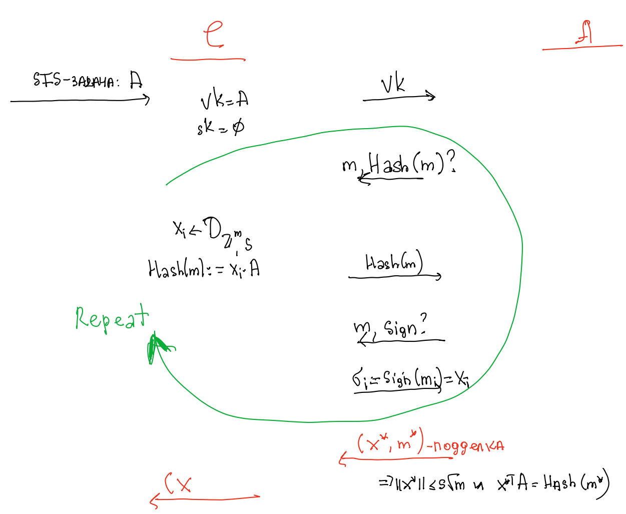
- **Verify** $(m, \underset{= x}{\sigma}, vk)$ Если $(\|x\| \le s\sqrt{m})$ и $x^T \cdot A = H(m)$

  Вернуть 1

  Иначе

  Вернуть 0.

Теорема Если $\exists$ эффект. злоумышленник $\mathcal{A}$, побеждающий uf-cma с непренебрежимо малой вероятностью, то $\exists$ эффект. алгоритм, решающий SIS.



1) Полагаем, что $\mathcal{A}$, прежде чем запросить $Sign(m)$, запрашивает $Hash(m)$ (иначе $\mathcal{C}$ вычисл. $Hash(m)$ самостоятельно).

2) Для $x_i \leftarrow D_{\mathbb{Z}^m, s}$, $x_i^T \cdot A$ – распр-но случайно равномерно (лемма о Гауссовом остатке).

Кроме того, при условии $x_i \cdot A \mod q$, условное распределение x_i есть $D_{A^\perp + c, s}$ для произвольного c: $c^T \cdot A = x_i^T \cdot A \mod q$

$\Rightarrow$ следующие 2 выборки отличаются в стат. разности лишь на $2^{-\Omega(n)}$:

$u \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$	$x \leftarrow D_{A^\perp + c, s}$
$x \leftarrow D_{A^\perp + c, s}$	$u := x^T \cdot A \mod q$
(x, u)	(x, u)

3. $\exists$ (x^*, m^*) – подделка, вычисленная $\mathcal{A}$ и пусть $\mathcal{A}$ запросил $Hash(m^*)$, на что $\mathcal{C}$ вычислил $(x_0, x_0^T \cdot A)$.

x_0 – неизвестно $\mathcal{A}$; $x_0^T \cdot A = Hash(m^*)$ – известно $\mathcal{A}$

Тогда $\mathcal{C}$, зная x^* и x_0, вычисляет

$$(x_0 - x^*)^T \cdot A = \underbrace{x_0^T A}_{Hash(m^*)} - \underbrace{x^{*T} A}_{Hash(m^*)} = 0 \mod q$$

$$\|x_0 - x^*\| \le \|x_0\| + \|x^*\| \le \underbrace{s\sqrt{m}}_{\text{Гауссов хвост}} + \underbrace{s\sqrt{m}}_{\text{валидность подделки}} = 2s\sqrt{m}$$

$x_0 - x^* = 0 \Leftrightarrow x_0 = x^*$, т.е. $\mathcal{A}$ угадал x_0. Вероятность угадывания $\mathcal{A} \le 2^{-\Omega(n)}$, т.к. масса $\forall b \leftarrow D_{A^\perp + c, s} \le \frac{1}{\rho_s(A^\perp)} \le 2^{-\Omega(n)}$ (1 – масса $b = 0$)

благодаря тому, что $s > \eta_{2^{-n}}(A^\perp)$

$\Rightarrow (x_0 - x^*)$ есть решение $SIS_{2s\sqrt{m}}$.