Лекция №15

Схема подписи на решётке

15/05 - Подпись

22/05 } лекции
29/05

05/06 - консультация / сдача доп. работа

12/06 - экзамен

19/06 - -//-

I. Определение цифровой подписи

Подпись = [KeyGen, Sign, Verify] - эфф. алгоритмы:

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

Корректность $\forall m \cdot Verify(vk, m, Sign(sk, m)) = 1$ с вероятностью $> 1 - 2^{-\Omega(n)}$ над случ. битами алг-ма Sign(), KeyGen().

Безопасность

UF-CMA игра

C (челленжер) — A (атакующий)

- (sk, vk)

$vk \to$

$\leftarrow m_i$

$\sigma_i = Sign(sk, m_i)$

$\leftarrow (m^*, \sigma^*)$

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

Подпись UF-CMA (Unforgeability under Chosen-Message Attack) безопасной, если $\nexists$ эффективного A, который побеждает в UF-CMA игре с непренебрежимо малой вероятностью.

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

II GPV-подпись

$H: \{0,1\}^* \to \mathbb{Z}_q^n$ – криптогр. хэш-ф-ия; короткий базис A^{-1}

- **KeyGen:** 1. Построить $A \leftarrow U(\mathbb{Z}_q^{m \times n})$, S_A : $[S_A]\,[A] = 0 \bmod q$

  $sk = S_A$, $vk = A$.

- **Sign** $(sk, m \in \{0,1\}^*)$

  1. Вычислить $u = H(m) \in \mathbb{Z}_q^n$
  2. Вычислить произвольный $c \in \mathbb{Z}^m$, т.ч. $c^T A = u^T \bmod q$ (таких "с" много)
  3. Выбрать $x \leftarrow D_{A^{-1}, \sigma, -c} + c$, $\sigma = \|S_A\| \cdot \sqrt{m}$

     (σ – среднекв. откл.)

  $\sigma = x$ $\quad \{ x^T \cdot A = \underbrace{(v+c)^T}_{\in A^{-1}} \cdot A = \underbrace{v^T \cdot A}_{=0} + \underbrace{c^T A}_{=u} = u^T \bmod q \}$

  $\in D_{A^{-1}, \sigma, -c+c}$

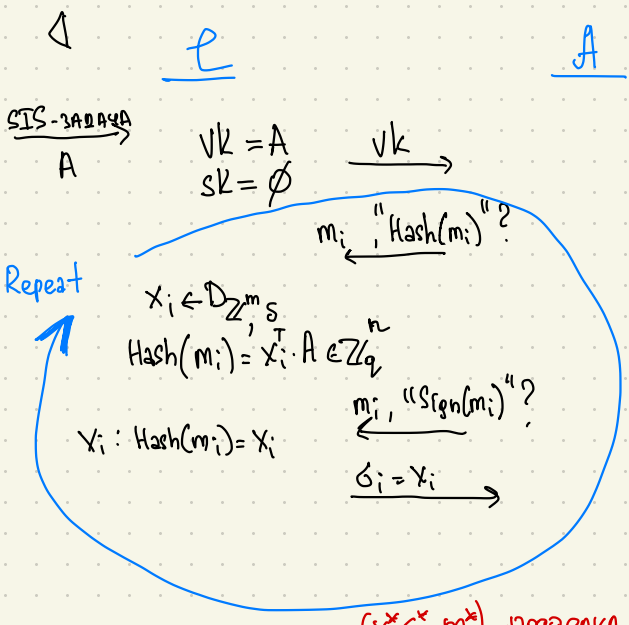
- **Verify** $(m, \underset{x}{\sigma}, vk)$ Если $\|x\| \le \sigma \cdot \sqrt{m}$ и $x^T \cdot A = H(m)$

  Вернуть 1

  Иначе

  Вернуть 0

ТЕОРЕМА Если $\exists$ эффективный атакующий $\mathcal{A}$, побеждающий в UF-CMA игре с непренебрежимо малой вероятностью, то $\exists$ эффективный алг-м, решающий задачу SIS.



Комментарии

1. Полагаем, что А, прежде чем запросить Sign(m_i), запрашивает Hash(m_i)

2. Для $x_i \leftarrow D_{\mathbb{Z}^m, s}$, $x_i^T \cdot A$ стат. "неотлично" от случ. равномерного над $\mathbb{Z}_q^n$ (см. Leftover Hash Lemma, лек 14).

При условии $x_i \cdot A \bmod q$, условное распределение x_i есть $D_{A^\perp + c, s}$, для $c: c^T A = x_i^T A$

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

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

3. $\exists$ (x^*, m^*) - подделка, вычисленная А, и пусть А запросил Hash(m^*) (на что Ч вычислил $(x_0, \underbrace{x_0^T \cdot A}_{\text{Hash}(m^*)})$ — А известно; x_0 — неизвестно А)

Тогда Ч, зная (x_0, x^*), вычислит: $(x_0 - x^*)^T \cdot A = \underbrace{x_0^T A}_{\text{Hash}(m^*)} - \underbrace{x^{*T} \cdot A}_{\text{Hash}(m^*)} = 0 \bmod q$

$\|x_0 - x^*\| \leq \|x_0\| + \|x^*\| \leq \delta \cdot \sqrt{m} + \delta\sqrt{m} = 2\delta\sqrt{m}$

(Гауссов хвост)

$x_0 - x^*$ является решением SIS, т.к. $x_0 \neq x^*$. С большой вероятностью, т.к.

если предположить, что $x_0 = x^*$ $\Rightarrow$ $\mathcal{A}$ угадал x_0. Вероятность угадывания $\mathcal{A} < 2^{-\Omega(n)}$, т.к. масса $\forall b \in D_{A^\perp + c, \delta} \leq \frac{1}{\rho_s(A^\perp)} \leq 2^{-\Omega(n)}$ ← масса $b=0$

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

$\Rightarrow$ $(x_0 - x^*)$ - решение $SIS_{A,\ 2\delta\sqrt{m}}$ ▶.

FALCON - эффективный GPV.

Dilithium - другая конструкция подписи на решётках.