Лекция №14

GPV подпись на решётке

Gentry - Peikert - Vaikuntanathan '07

"Hash-and-Sign" парадигма (RSA).

I Определение цифровой подписи

Подпись = [KeyGen, Sign, Verify] - эффективные алгоритмы (KeyGen, Sign - рандомизированы, Verify - детерминированная):

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

Корректность: $\forall m$: $Verify(vk, m, Sign(sk, m)) = 1$ с вероятностью $1 - 2^{-\omega(\log n)}$ над случайными битами $KeyGen()$, $Sign()$.

Безопасность (UF-CMA игра)
↑ unforgeability under chosen message attack

$\mathcal{C}$ (challenger) $\quad$ $\mathcal{A}$ (атакующий)

- (sk, vk)

vk →

← m_i

$\sigma_i = Sign(sk, m_i)$ ← $\mathcal{C}$

(m^*, σ^*) →

$Verify(vk, m^*, \sigma^*)$

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

Подпись является UF-CMA безопасной, если $\nexists$ эффективного $\mathcal{A}$, который побеждает в UF-CMA игре с непренебрежимо малой вероятностью.

Модель случайного оракула (Random Oracle Model, ROM): хэш-функция $H()$, используемая в протоколе, моделируется как случайная ф-ция и находится под контролем $\mathcal{C}$. В UF-CMA игре $\mathcal{A}$ может делать хэш-запросы к $\mathcal{C}$.

II Конструкция GPV подписи

$H: \{0,1\}^* \to \mathbb{Z}_q^n$ - криптографическая хэш-ф-ция

n, m, q, s - фикс. параметры

$s > \sqrt{m}$

- **KeyGen** 1. Построить $A \leftarrow U(\mathbb{Z}_q^{m \times n})$ и S_A (короткий базис для $A^\perp$): $S_A \cdot A = 0 \bmod q$

  $sk = S_A,\ vk = A$

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

  1. Вычислить $U = H(m) \in \mathbb{Z}_q^n$
  2. Вычислить произвольный $c \in \mathbb{Z}^n$, т.ч. $c^T \cdot A = U^T \bmod q$ (таких c^T много)
  3. Выбрать $x \leftarrow D_{A^\perp, s, -c} + C$, $s = \|S_A\| \cdot \sqrt{m}$ (↑ среднекв. отклонение)

  $$\{ x^T \cdot A = (v + c)^T \cdot A = \underbrace{v^T \cdot A}_{=0} + c^T \cdot A = U^T \bmod q \}$$

  $\sigma = x$ - подпись.

- **Verify** (m, σ, vk) 1. Если $\|x\| \le s\sqrt{m}$ (граница "хвоста" для Гауссовой выборки) и $x^T \cdot A = H(m) \bmod q$:

  Вернуть 1 (подпись принята)

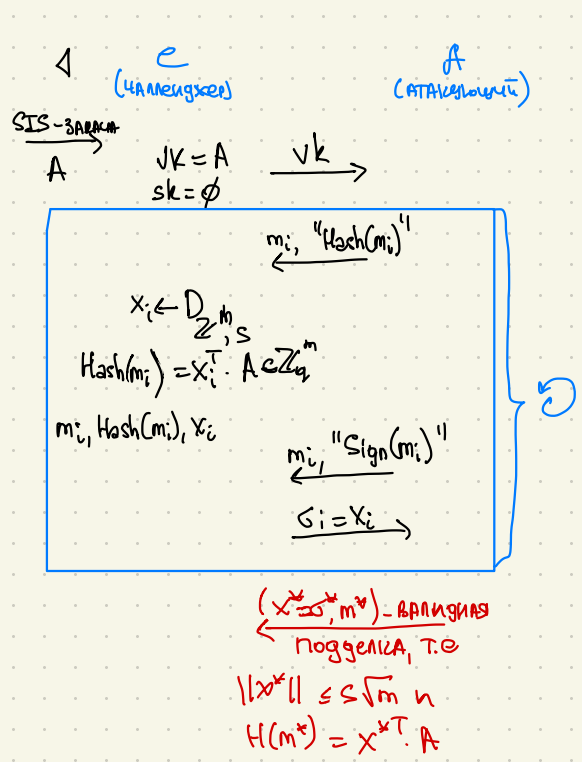
  Иначе

  Вернуть 0.

FALCON - эффективная конструкция подписи GPV.

III Безопасность подписи GPV

Теорема Если $\exists$ эффективный атакующий A, побеждающий в UF-CMA игре с непренебрежимо малой вероятностью, то $\exists$ эффективный алгоритм, решающий задачу SIS.



Комментарии

1. Полагаем, что $\mathcal{A}$, прежде чем запросить "Sign(m_i)", запрашивает "Hash(m_i)".

2. Для $x_i \leftarrow D_{\mathbb{Z}^m, s}$, $x_i^T \cdot A$ статистически неотличимо от случайного равномерного над $\mathbb{Z}_q^n$ (см. Lekhver Hash Lemma, лек. #13)

При условии, что мы знаем $x_i A \bmod q$, условное распределение x_i есть $D_{\Lambda^\perp + c, s}$ для c удовлетворяющего $c^T \cdot A = x_i^T \cdot A$, т.е. следующие 2 выборки отличаются в стат. разности на $\varepsilon^{-\Omega(n)}$:

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

3. J (x^*, m^*) - подделка, полученная от $\mathcal{A}$; при этом пусть $\mathcal{A}$ запросил $Hash(m^*)$, на что $\mathcal{C}$ вычислил $(x_0, \underbrace{x_0^T \cdot A}_{Hash(m^*)})$ ($x_0^T \cdot A$ известно $\mathcal{A}$, неизвестно для $\mathcal{A}$). Тогда $\mathcal{C}$, зная (x_0, x^*) вычисляет:

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

$$\|x_0 - x^*\| \leq \underbrace{\|x_0\|}_{\text{граница хвоста для Гауссового распределения}} + \underbrace{\|x^*\|}_{x^*\text{ - валидная подделка}} \leq s\sqrt{m} + s\sqrt{m} = 2s\sqrt{m}$$

$x_0 - x^*$ является решением SIS, т.к. с большой вероятностью $x_0 \neq x^*$. Это верно, т.к., если предположить, что $x_0 = x^*$, т.е. $\mathcal{A}$ угадал x_0, то вероятность такого угадывания $< 2^{-\Omega(n)}$. Это следует из того, что масса $\forall b \in D_{\Lambda^\perp + c, s}$

$$\leq \underbrace{\frac{1}{\rho_s(\Lambda^\perp)}}_{\text{масса } b=0} \leq 2^{-\Omega(n)}, \text{ т.к. } s > \eta_{\varepsilon}(\Lambda^\perp). \Rightarrow x_0 - x^* \text{ - решение } SIS_{A,\, 2s\sqrt{m}}$$