Сложностная криптография

Эдуард Алексеевич Гирш

http://logic.pdmi.ras.ru/~hirsch

ПОМИ РАН

23 марта 2008 г.

Многоразовая схема из одноразовой

Как сделать?

- Генерируем новый ключ v_0 и подписываем старым $S_s(v_0, r)$.

Многоразовая схема из одноразовой

Как сделать?

- Генерируем новый ключ v_0 и подписываем старым $S_s(v_0, r)$.
- Нельзя использовать старый ключ дважды

  $\Rightarrow$

Многоразовая схема из одноразовой

Как сделать?

- Генерируем новый ключ v_0 и подписываем старым $S_s(v_0, r)$.
- Нельзя использовать старый ключ дважды
  $\Rightarrow$ должно быть два новых ключа v_0, v_1.

Многоразовая схема из одноразовой

Как сделать?

- Генерируем новый ключ v_0 и подписываем старым $S_s(v_0, r)$.
- Нельзя использовать старый ключ дважды
  $\Rightarrow$ должно быть два новых ключа v_0, v_1.
- Нельзя хранить их на будущее
  $\Rightarrow$

Многоразовая схема из одноразовой

Как сделать?

- Генерируем новый ключ v_0 и подписываем старым $S_s(v_0, r)$.
- Нельзя использовать старый ключ дважды
  $\Rightarrow$ должно быть два новых ключа v_0, v_1.
- Нельзя хранить их на будущее
  $\Rightarrow$ надо генерировать путь в бинарном дереве ключей.

Многоразовая схема из одноразовой

Как сделать?

- Генерируем новый ключ v_0 и подписываем старым $S_s(v_0, r)$.
- Нельзя использовать старый ключ дважды
  $\Rightarrow$ должно быть два новых ключа v_0, v_1.
- Нельзя хранить их на будущее
  $\Rightarrow$ надо генерировать путь в бинарном дереве ключей.
- Дерево одно и то же (иначе используем старый ключ дважды)
  $\Rightarrow$

Многоразовая схема из одноразовой

Как сделать?

- Генерируем новый ключ v_0 и подписываем старым $S_s(v_0, r)$.
- Нельзя использовать старый ключ дважды
  $\Rightarrow$ должно быть два новых ключа v_0, v_1.
- Нельзя хранить их на будущее
  $\Rightarrow$ надо генерировать путь в бинарном дереве ключей.
- Дерево одно и то же (иначе используем старый ключ дважды)
  $\Rightarrow$ нельзя использовать случайные числа
  $\Rightarrow$ prff.

Многоразовая схема из одноразовой

Были одноразовая схема (G, S, V) и prff $\{f_\zeta\}_{\zeta \leftarrow Z}$.
Возьмём $(s, v) \leftarrow G(1^n, r_g)$ и $\zeta \leftarrow Z(1^n)$.
Новые ключи: (ζ, s) и v.

Подпись:

- Точка "времени" $\sigma = \sigma_1 \sigma_2 \dots \sigma_n \in \{0,1\}^n$.
- Подпись сообщения, использующая ключи (s_σ, v_σ):

$$S_{s_\sigma}(\mathtt{msg}, \underbrace{f_\zeta(0\sigma)}_{\text{случ.биты для } S}).$$

- Последовательная аутентикация верификационных ключей:

$$\begin{aligned}
&(v_0, && v_1, && S_s(v_0 && \circ v_1 && , f_\zeta(0))),\\
&(v_{\sigma_1 0}, && v_{\sigma_1 1}, && S_{s_{\sigma_1}}(v_{\sigma_1 0} && \circ v_{\sigma_1 1} && , f_\zeta(0\sigma_1))),\\
& && \dots && && && \\
&(v_{\sigma_1 \dots \sigma_{n-1} 0}, && v_{\sigma_1 \dots \sigma_{n-1} 1}, && S_{s_{\sigma_1 \dots \sigma_{n-1}}}(v_{\sigma_1 \dots \sigma_{n-1} 0} && \circ v_{\sigma_1 \dots \sigma_{n-1} 1} && , f_\zeta(0\sigma_1 \dots \sigma_{n-1}))).
\end{aligned}$$

При этом сами ключи $(s_\tau, v_\tau) \leftarrow G(1^n, f_\zeta(1\tau))$.

Наши планы

owf

1-разовая $\ell(n)$-ограниченная

hash — возможны варианты

1-разовая неограниченная

prff (из owf)

многоразовая неограниченная

Хеш-функции без коллизий

Определение (collision-free hashing function family, cfhff)

Семейство $\ell(n)$-хеш-функций без коллизий — это полиномиальные детерминированные алгоритмы Z и H и семейство функций $\{h_\xi\}_\xi$, такие что

- $h_\xi : \{0,1\}^* \to \{0,1\}^{\ell(|\xi|)}$,
- $Z : (1^n, r_Z) \mapsto \xi$,
- $H(\xi, x) = h_\xi(x)$,
- трудно найти коллизию: $\forall$ полин.противника A $\forall k$

$$\Pr\{A(\xi) = (y, y') : h_\xi(y) = h_\xi(y'),\ y \neq y'\} < \frac{1}{n^k}.$$

Упражнение

Показать, что существование cfhff влечёт существование owf.

Одноразовая (неограниченная) схема

Hash-and-sign paradigm

Теорема

Пусть (G, S, V) — надежная одноразовая $\ell(n)$-ограниченная DSS, $\{h_\xi\}_\xi$ — $\ell(n)$-collision-free hashing function family.
Новая DSS:

- Ключи: (ξ, s) и (ξ, v),
  где (s, v) — старые ключи, ξ — индекс в cfhff.
- Подпись: $S'_{(\xi,s)}(\mathtt{msg}) = S_s(h_\xi(\mathtt{msg}))$.

Полученная одноразовая DSS будет по-прежнему надёжной.

Доказательство.

Взлом новой схемы означает, что мы либо найдём коллизию, либо взломаем старую схему подписей. (Детали — упражнение.) □

Universal One-Way Hash Functions Family (uowhff)

Семейство универсальных $\ell(n)$-хеш-функций — это полин. дет. алгоритмы Z и H и семейство функций $\{h_\xi\}_\xi$, такие что

- $h_\xi : \{0,1\}^* \to \{0,1\}^{\ell(|\xi|)}$,
- $Z : (1^n, r_Z) \mapsto \xi$,
- $H(\xi, x) = h_\xi(x)$,
- трудно найти коллизию с **заранее назначенной** строкой:
  $\forall$ полин.противника A $\forall k$
  вероятность успеха следующей игры асимптотически $< \frac{1}{n^k}$:
  1. A выбирает строку y_0;
  2. Z выбирает индекс ξ;
  3. A находит строку $y \neq y_0$, для которой $h_\xi(y) = h_\xi(y_0)$.

Упражнение

Показать, что существование uowhff влечёт существование owf.

Замечание

Верно и обратное! Но непросто это доказать...

Одноразовая (неограниченная) схема на основе uowhff

Hash-and-sign paradigm, revisited

Теорема

Пусть (G, S, V) — надежная одноразовая $(\ell(n)+n)$-ограниченная DSS, $\{h_\xi\}_\xi$ — $\ell(n)$-uowhff.
Новая DSS:

- Ключи — от старой системы: $G' = G$.
- Подпись: $S'_s(\mathtt{msg}) = (\xi,\ S_s(\xi \circ h_\xi(\mathtt{msg})))$, т.е.
  - индекс ξ (генерируем заново!),
  - старая подпись для индекса и для хеша сообщения.

Полученная одноразовая DSS будет по-прежнему надёжной.

Доказательство.

Взлом новой схемы означает, что мы либо найдём коллизию, либо взломаем старую схему подписей. (Детали — упражнение.) □

Псевдослучайные функции

Определение (Семейство псевдослучайных функций, prff)

...это семейство функций $\{f_\zeta\}_\zeta$, для которого

- $f_\zeta : \{0,1\}^n \to \{0,1\}^n$;
- $Z : (1^n, r_Z) \mapsto \zeta$ — полин. генератор индексов;
- $F(\zeta, x) = f_\zeta(x)$ — полин. алгоритм, вычисляющий f_ζ;
- f_ζ неотличима от случайной функции: $\forall M^\bullet \ \forall k \ \exists N \ \forall n > N$

$$\left| \Pr\{M^{f_\zeta}(1^n) = 1\} - \Pr\{M^R(1^n) = 1\} \right| < \frac{1}{n^k},$$

где таблица истинности функции $R : \{0,1\}^n \to \{0,1\}^n$ — случайная, M — полин. вер. противник.

"Маленькая" ζ — экспоненциально большая "книжка" с кодами.

Конструкция псевдослучайных функций

. . . из псевдослучайных генераторов

Пусть $G\colon \{0,1\}^n \to \{0,1\}^{2n}$ — $2n$-PRG,
разрежем его выход на две части $G_0, G_1\colon \{0,1\}^n \to \{0,1\}^n$.

Пусть индексы $\zeta \in \{0,1\}^n$ генерируются равномерно,

$$f_\zeta(b_1 b_2 \dots b_n) = G_{b_n}(G_{b_{n-1}}(\dots(G_{b_1}(G_{b_0}(\zeta)))\dots)).$$

Тогда $\{f_\zeta\}_\zeta$ — prff.

Это непростая теорема. . .

Конструкция псевдослучайных функций

. . . из псевдослучайных генераторов

Пусть $G\colon \{0,1\}^n \to \{0,1\}^{2n}$ — $2n$-PRG,
разрежем его выход на две части $G_0, G_1\colon \{0,1\}^n \to \{0,1\}^n$.

Пусть индексы $\zeta \in \{0,1\}^n$ генерируются равномерно,

$$f_\zeta(b_1 b_2 \dots b_n) = G_{b_n}(G_{b_{n-1}}(\dots(G_{b_1}(G_{b_0}(\zeta))\dots)).$$

Тогда $\{f_\zeta\}_\zeta$ — prff.

Это непростая теорема. . .
. . . которую мы сейчас докажем.

PRG: “одноразовые” vs “многоразовые”

Будем сводить prff к PRG. Но prff давалась противнику как (многоразовый) оракул, а PRG — как одна случайная переменная.

Определение

$G : \{0,1\}^\ell \to \{0,1\}^{f(\ell)}$, где $f(\ell) > \ell$, называется $f(\ell)$-генератором псевдослучайных чисел ($f(\ell)$-PRG), если для $\forall$ полин.противника A $\forall k$

$$\left|\Pr\{A(G(x)) = 1\} - \Pr\{A(y) = 1\}\right| < \frac{1}{\ell^k},$$

где вероятность берется по случайным числам A и по равномерно распределенным $x \in \{0,1\}^\ell$ и $y \in \{0,1\}^{f(\ell)}$.

Определение

. . . называется многоразовым $f(\ell)$-PRG, если для $\forall A$ $\forall k$ $\forall m$

$$\left|\Pr\{A(G(x_1), \ldots, G(x_{\ell^m})) = 1\} - \Pr\{A(y_1, \ldots, y_{\ell^m}) = 1\}\right| < \frac{1}{\ell^k},$$

где вероятность берется по случайным числам A и по равномерно распределенным $x_i \in \{0,1\}^\ell$ и $y_i \in \{0,1\}^{f(\ell)}$.

Доказательство того, что получилось prff

Whiteboard

(Здесь должно было быть нарисовано несколько деревьев, символизирующих переход от псевдослучайной функции к случайной. . .)