Сложностная криптография

Эдуард Алексеевич Гирш

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

ПОМИ РАН

16 марта 2008 г.

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 криптосистемы с общим ключом

. . . на основе псевдослучайных функций

1. Сначала научимся кодировать сообщения длины ровно n (но много!).

Генератор ключа = генератор индекса ζ для prff,

$$E(\mathtt{msg}, \zeta, r_E) = (f_\zeta(r_E) \oplus \mathtt{msg}, r_E).$$

2. Перейдём к сообщениям произвольной длины — порежем на куски:

$$E'(\mathtt{msg}, \zeta, \underbrace{r_1 r_2 \ldots}_{r_E}) = (|\mathtt{msg}|, E(\mathtt{msg}[1..n], \zeta, r_1), E(\mathtt{msg}[n{+}1..2n], \zeta, r_2), \ldots)$$

Поскольку E надёжно относительно **последовательности** сообщений, можно спокойно использовать ключ ζ многократно.

Конструкция криптосистемы с общим ключом

. . . на основе псевдослучайных функций

1. Сначала научимся кодировать сообщения длины ровно n (но много!).

Генератор ключа = генератор индекса ζ для prff,

$$E(\mathtt{msg}, \zeta, r_E) = (f_\zeta(r_E) \oplus \mathtt{msg}, r_E).$$

2. Перейдём к сообщениям произвольной длины — порежем на куски:

$$E'(\mathtt{msg}, \zeta, \underbrace{r_1 r_2 \ldots}_{r_E}) = (|\mathtt{msg}|, E(\mathtt{msg}[1\,..\,n], \zeta, r_1), E(\mathtt{msg}[n{+}1\,..\,2n], \zeta, r_2), \ldots)$$

Поскольку E надёжно относительно **последовательности** сообщений, можно спокойно использовать ключ ζ многократно.

Надёжность prff $\Rightarrow$ надёжность криптосистемы

Различили

$$\{(f_\zeta(r_i) \oplus \mathtt{msg}^{(i)}, r_i)\}_i \text{ и } \{(f_\zeta(r_i') \oplus \underset{\text{random}}{\rho^{(i)}}, r_i')\}_i$$

$\Rightarrow$ различили одно из двух:

$$\{(R(r_i) \oplus \mathtt{msg}^{(i)}, r_i)\}_i \text{ и } \{(R(r_i') \oplus \underset{\text{random}}{\rho^{(i)}}, r_i')\}_i \qquad (1)$$

или

$$f_\zeta \text{ и } R.$$

Но (1) неразличимы, т.к. с вер. $1 - t^2 \cdot 2^{-n}$ все r_i различны, так что $R(r_i) \oplus \ldots$ независимы и равномерно распределены.

□

Цифровые подписи

Определение (схема цифровых подписей, digital signatures scheme, DSS)

...это полиномиальные алгоритмы G, S, V:

- $G : (1^n, r_g) \mapsto (s, v)$ (ключ для подписи и $\overbrace{\text{ключ для проверки}}^{\text{публичный}}$),
- $S : (s, \texttt{msg}) \mapsto \texttt{sign}$ (подписывающий алгоритм),
- $V : (v, \texttt{msg}, \texttt{sign}) \mapsto 0$ или 1,

Будем писать S_s вместо $S(s, \ldots)$ и V_v вместо $V(v, \ldots)$.
Условие корректности:

- $\forall \texttt{msg} \ \Pr\limits_{r_g}\{V_v(\texttt{msg}, S_s(\texttt{msg})) = 0\} = 0.$

Упражнение

Покажите, что всё равно, детерминированные S и V или вероятностные.

Надёжность цифровых подписей

Определение (надежная цифровая подпись)

Схема называется надежной, если $\forall$ полин.противника $A^\bullet$ $\forall k$

$$\Pr\{A^{S_s}(v) = (\texttt{msg}, \texttt{sign}) : V_v(\texttt{msg}, \texttt{sign}) = 1\} < \frac{1}{n^k}.$$

Здесь $A^\bullet$ запрещено выдавать $\texttt{msg}$, о которых он запрашивал оракула.

Определение (одноразовая надежная цифровая подпись)

. . . если обращение к оракулу лишь одно.

Определение ($\ell(n)$-ограниченная цифровая подпись, $\ell(n)$-DSS)

. . . если подписываются только сообщения длины $\ell(n)$.
Если для таких сообщений соблюдается условие надёжности, то это $\ell(n)$-ограниченная надёжная DSS.

Наши планы

↓ owf

1-разовая $\ell(n)$-ограниченная

↓ hash — возможны варианты

1-разовая неограниченная

↓ prff (из owf)

многоразовая неограниченная

Вообще говоря, достаточно owf.

Наши планы

owf

1-разовая $\ell(n)$-ограниченная

hash — возможны варианты

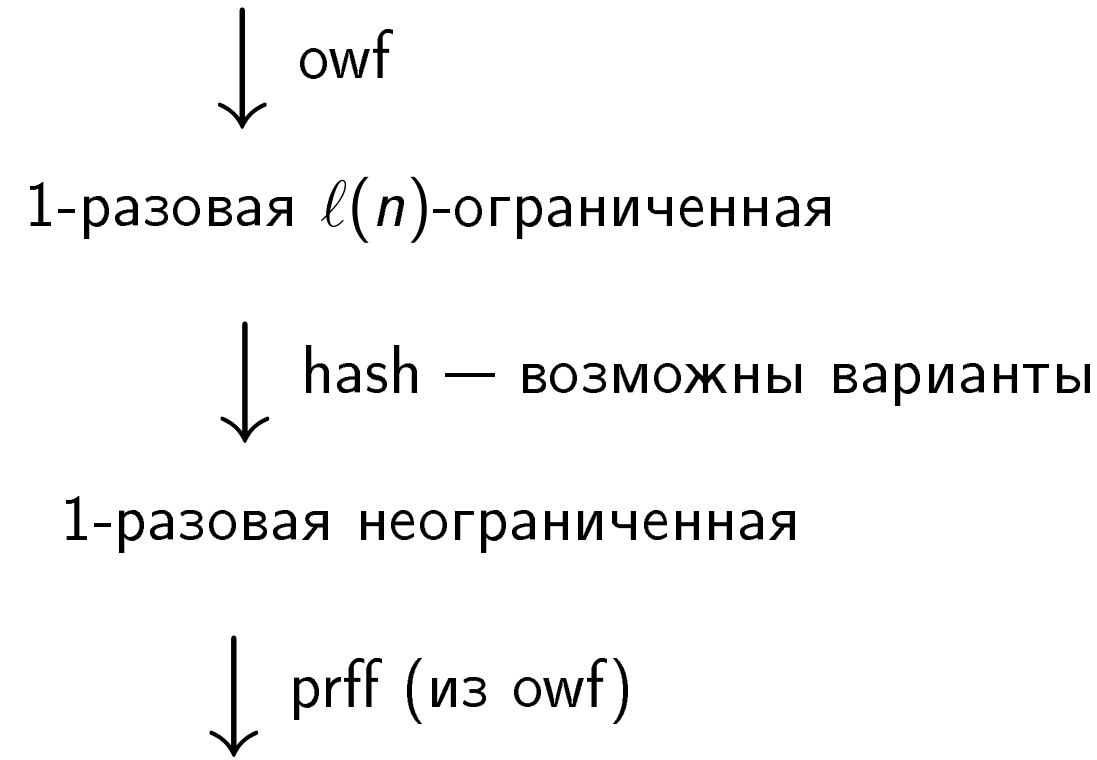
1-разовая неограниченная

prff (из owf)

многоразовая неограниченная

Вообще говоря, достаточно owf.

Наши планы



Вообще говоря, достаточно owf.

Конструкция одноразовой ограниченной схемы

$$s_k^i \xrightarrow{f} v_k^i$$

Теорема

Пусть f — owf, $m = \ell(n)$ — полином. Положим

$$G(1^n) = ((s_1^0, s_1^1, \ldots, s_m^0, s_m^1), (v_1^0, v_1^1, \ldots, v_m^0, v_m^1)),$$

где $s_k^i \in \{0,1\}^n$ выбраны случайным образом, $v_k^i = f(s_k^i)$. Подпись

$$S_s(\mu_1 \ldots \mu_m) = (s_1^{\mu_1}, \ldots, s_m^{\mu_m}).$$

V достаточно проверить, что $f(s_i^{\mu_i}) = v_i^{\mu_i}$ для всех i.
Полученная конструкция является надёжной одноразовой $\ell(n)$-DSS.

Доказательство.

Взламываем f при помощи взломщика для нашей DSS.

Нам дали y.
Генерируем ключ, заменяем в нем v_k^i на y (k и i случайны).
Запускаем старого противника.

Если при обращении к оракулу противник не спросит нас $f^{-1}(v_k^i)$ (вероятность этого $= \frac{1}{2}$), то с вероятностью[1] $\frac{1}{m}$ он попытается вычислить нам $f^{-1}(y)$.

Итого мы обратим f с вероятностью лишь в $2m$ раз меньшей. □

Упражнение

Формально записать все эти вероятностные рассуждения, учитывая потенциальную возможность зависимости между событиями.

[1] Это — вероятность, что мы угадали то место, в котором будут отличаться запрос к оракулу и подписываемое сообщение.

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" $\sigma = \sigma_1\sigma_2 \ldots \sigma_n \in \{0,1\}^n$.
- 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:

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

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