Сложностная криптография

Эдуард Алексеевич Гирш

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

ПОМИ РАН

9 марта 2008 г.

Напоминание: PRG

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 $y \in \{0,1\}^{f(\ell)}$.

Теорема

$\exists$ PRG $\Leftrightarrow$ $\exists$ owf.

Докажем частично.

PRG $\Rightarrow$ owf

Теорема

G — 2ℓ-PRG $\Rightarrow$ он owf.

Доказательство.

Пусть, напротив, есть взломщик, который обращает G на доле $\geq \frac{1}{\ell^k}$.
Различающий алгоритм:

- $z = G^{-1}(y)$;
- Выдать 1, если $G(z) = y$; иначе 0.

Если $y \in \operatorname{Im} G$, то вероятность выдать 1 — хотя бы $\frac{1}{\ell^k}$.

Если y равномерно распределён на $\{0,1\}^{2\ell}$, то вероятность просто попасть y в $\operatorname{Im} G$ равна $\frac{|\operatorname{Im} G|}{2^{2\ell}} \leq 2^{-\ell}$. А тем более — выдать 1. $\square$

owf $\Rightarrow$ PRG

Теорема

Пусть f — owp, сохраняющая длину, B — её трудный бит, p — полином. Тогда

$$G(x) = f^{p(\ell)-\ell}(x) \circ B(x) \circ B(f(x)) \circ \ldots \circ B(f^{p(\ell)-\ell-1}(x))$$

является $p(\ell)$-PRG.

Доказательство для $(\ell+1)$-PRG.

Итак, $G(x) = f(x) \circ B(x)$.
Пусть он не PRG, т.е. существует взломщик A, такой, что

$$|\underbrace{\Pr\{A(G(x)) = 1\}}_{\gamma} - \underbrace{\Pr\{A(y) = 1\}}_{\nu}| \geq \frac{1}{\ell^k}.$$

$\alpha := \Pr\{A(f(x) \circ b) = 1 | b = B(x)\} = \Pr\{A(f(x) \circ B(x)) = 1\} = \gamma,$
$\beta := \Pr\{A(f(x) \circ b) = 1 | b = \overline{B(x)}\} = \Pr\{A(f(x) \circ \overline{B(x)}) = 1\}.$

$$\begin{aligned}\nu &= \Pr\{A(f(x) \circ b) = 1\} = \\ &= \Pr\{b = B(x)\} \cdot \alpha + \Pr\{b = \overline{B(x)}\} \cdot \beta \\ &= \tfrac{\alpha+\beta}{2}.\end{aligned}$$

НУО, $\frac{1}{\ell^k} \leq \gamma - \nu = \alpha - \frac{\alpha+\beta}{2} = \frac{\alpha-\beta}{2}$.

Мы отличаем трудный бит от его отрицания!
Остаётся этим формально воспользоваться.

Доказательство для $(\ell+1)$-PRG (окончание).

Новый взломщик A', находящий $B(x)$ по $f(x)$:

- выбрать $b \in \{0,1\}$ случайным образом;
- если $A(f(x) \circ b) = 1$, то выдать b, иначе выдать $\overline{b}$.

Тогда

$$\Pr\{A'(f(x)) = B(x)\} =$$
$$\Pr\{b = B(x)\} \cdot \Pr\{A(f(x) \circ B(x)) = 1\} +$$
$$\Pr\{b = \overline{B(x)}\} \cdot \Pr\{A(f(x) \circ \overline{B(x)}) \neq 1\} =$$
$$\frac{1}{2}\alpha + \frac{1}{2}(1-\beta) = \frac{1}{2} + \frac{\alpha-\beta}{2} \geq \frac{1}{2} + \frac{1}{\ell^k},$$

что противоречит тому, что $B(x)$ — трудный бит. □

$\ell + 1 \rightsquigarrow p(\ell)$

Покажем, что

$$f^{p(\ell)-\ell}(x) \circ B(x) \circ \cdots \circ B(f^{p(\ell)-\ell-1}(x)) \qquad (\nabla)$$

неотличимо от равномерного распределения, то есть

$$f^{p(\ell)-\ell}(x) \circ b_1 \circ \cdots \circ b_{p(\ell)-\ell}. \qquad (\Delta)$$

Превращаем (∇) в (Δ):

$$\begin{array}{lcl}
D_0(x) & = & f^{p(\ell)-\ell}(x) \circ B(x) \circ \ldots \circ B(f^{p(\ell)-\ell-1}(x)) \\
\ldots & & \\
D_i(x) & = & f^{p(\ell)-\ell-i}(x) \circ b_1 \circ \ldots \circ b_i \circ B(x) \circ B(f(x)) \circ \ldots \circ B(f^{p(\ell)-\ell-i-1}(x)) \\
D_{i+1}(x) & = & f^{p(\ell)-\ell-i-1}(x) \circ b_1 \circ \ldots \circ b_i \circ b_{i+1} \circ B(x) \circ \ldots \circ B(f^{p(\ell)-\ell-i-2}(x)) \\
\ldots & & \\
D_{p(\ell)-\ell}(x) & = & x \circ b_1 \circ \ldots \circ b_{p(\ell)-\ell}
\end{array}$$

Взломщик должен различать и какие-то D_i, D_{i+1}.

Тогда взломаем и наш старый $(\ell+1)$-PRG:
Нам дали y и b, строим строку, как будто $y = f(x)$, $b = B(x)$:

$$f^{p(\ell)-\ell-i}(x) \circ b_1 \circ \cdots \circ b_i \circ B(x) \circ B(f(x)) \circ \cdots \circ B(f^{p(\ell)-\ell-i-1}(x))$$

и даём взломщику, отличающему D_i от D_{i+1}.

Криптосистемы с общим ключом

(секретным, закрытым, private)

- Определение — как с публичным, просто E использует $e = d$.
- Надёжность — как с публичным, просто не даём ключа противнику:

Определение (перестаём писать r_e и 1^n...)

Криптосистема называется неразличимой, если
$\forall k$ $\forall$ пары сообщений (m_0, m_1) полин.длины $\forall$ вер.полин.схем C

$$\left|\Pr\{C(E(m_0, d), m_0, m_1) = 1\} - \Pr\{C(E(m_1, d), m_0, m_1) = 1\}\right| < \frac{1}{n^k} \quad \ldots$$

Криптосистема называется семантически надежной, если
$\forall h$ $\forall f$ $\forall C$ $\forall k$ $\exists \widetilde{C}$ $\forall M$

$$\Pr\{C(E(m, d), f(m)) = h(m)\} \leq \Pr\{\widetilde{C}(f(m)) = h(m)\} + \frac{1}{n^k},$$

где $f, h, C, \widetilde{C}, M$ — вер.полин.схемы, ...

Но это не вся правда о надёжности!

Криптосистемы с общим ключом

(секретным, закрытым, private)

- Определение — как с публичным, просто E использует $e = d$.
- Надёжность — как с публичным, просто не даём ключа противнику:

Определение (перестаём писать r_e и 1^n...)

Криптосистема называется неразличимой, если
$\forall k$ $\forall$ пары сообщений (m_0, m_1) полин.длины $\forall$ вер.полин.схем C

$$\left|\Pr\{C(E(m_0, d), m_0, m_1) = 1\} - \Pr\{C(E(m_1, d), m_0, m_1) = 1\}\right| < \frac{1}{n^k} \quad \ldots$$

Криптосистема называется семантически надежной, если
$\forall h$ $\forall f$ $\forall C$ $\forall k$ $\exists \widetilde{C}$ $\forall M$

$$\Pr\{C(E(m, d), f(m)) = h(m)\} \leq \Pr\{\widetilde{C}(f(m)) = h(m)\} + \frac{1}{n^k},$$

где $f, h, C, \widetilde{C}, M$ — вер.полин.схемы, ...

Но это не вся правда о надёжности!

Криптосистемы с общим ключом

(секретным, закрытым, private)

- Определение — как с публичным, просто E использует $e = d$.
- Надёжность — как с публичным, просто не даём ключа противнику:

Определение (перестаём писать r_e и $1^n \dots$)

Криптосистема называется неразличимой, если
$\forall k$ $\forall$ пары сообщений (m_0, m_1) полин.длины $\forall$ вер.полин.схем C

$$\left|\Pr\{C(E(m_0, d), m_0, m_1) = 1\} - \Pr\{C(E(m_1, d), m_0, m_1) = 1\}\right| < \frac{1}{n^k} \quad \dots$$

Криптосистема называется семантически надежной, если
$\forall h$ $\forall f$ $\forall C$ $\forall k$ $\exists \widetilde{C}$ $\forall M$

$$\Pr\{C(E(m, d), f(m)) = h(m)\} \leq \Pr\{\widetilde{C}(f(m)) = h(m)\} + \frac{1}{n^k},$$

где $f, h, C, \widetilde{C}, M$ — вер.полин.схемы, ...

Но это не вся правда о надёжности!

Криптосистемы с общим ключом

(секретным, закрытым, private)

- Определение — как с публичным, просто E использует $e = d$.
- Надёжность — как с публичным, просто не даём ключа противнику:

Определение (перестаём писать r_e и $1^n \dots$)

Криптосистема называется неразличимой, если
$\forall k$ $\forall$ пары сообщений (m_0, m_1) полин.длины $\forall$ вер.полин.схем C

$$\left|\Pr\{C(E(m_0, d), m_0, m_1) = 1\} - \Pr\{C(E(m_1, d), m_0, m_1) = 1\}\right| < \frac{1}{n^k} \quad \dots$$

Криптосистема называется семантически надежной, если
$\forall h$ $\forall f$ $\forall C$ $\forall k$ $\exists \widetilde{C}$ $\forall M$

$$\Pr\{C(E(m, d), f(m)) = h(m)\} \leq \Pr\{\widetilde{C}(f(m)) = h(m)\} + \frac{1}{n^k},$$

где $f, h, C, \widetilde{C}, M$ — вер.полин.схемы, ...

Но это не вся правда о надёжности!

Криптосистема с общим ключом на основе owp

Неправильная

Мы научились из owp делать PRG любой полиномиальной длины.
Ключ k — seed для PRG, любая строка из $\{0,1\}^n$;

$$E(m,k) = m \oplus G(k) = (m_1 \oplus G_1(k)) \circ (m_2 \oplus G_2(k)) \circ \ldots \circ (m_p \oplus G_p(k)),$$

где $G_i(k)$ — i-й бит $G(k)$.

Доказательство.

Отличаем m от $m' \Rightarrow$ взламываем G:
закодируем сами и отличим от "кода случайного сообщения". □

- Длина полиномиальна?
  Но надёжность — для сообщений полиномиальной длины.
- Есть другая проблема...

Криптосистема с общим ключом на основе owp

Неправильная

Мы научились из owp делать PRG любой полиномиальной длины.
Ключ k — seed для PRG, любая строка из $\{0,1\}^n$;

$$E(m,k) = m \oplus G(k) = (m_1 \oplus G_1(k)) \circ (m_2 \oplus G_2(k)) \circ \ldots \circ (m_p \oplus G_p(k)),$$

где $G_i(k)$ — i-й бит $G(k)$.

Доказательство.

Отличаем m от $m' \Rightarrow$ взламываем G:
закодируем сами и отличим от "кода случайного сообщения". □

- Длина полиномиальна?
  Но надёжность — для сообщений полиномиальной длины.
- Есть другая проблема...

Криптосистема с общим ключом на основе owp

Неправильная

Мы научились из owp делать PRG любой полиномиальной длины.
Ключ k — seed для PRG, любая строка из $\{0,1\}^n$;

$$E(m,k) = m \oplus G(k) = (m_1 \oplus G_1(k)) \circ (m_2 \oplus G_2(k)) \circ \ldots \circ (m_p \oplus G_p(k)),$$

где $G_i(k)$ — i-й бит $G(k)$.

Доказательство.

Отличаем m от $m' \Rightarrow$ взламываем G:
закодируем сами и отличим от "кода случайного сообщения". □

- Длина полиномиальна?
  Но надёжность — для сообщений полиномиальной длины.
- Есть другая проблема...

Криптосистема с общим ключом на основе owp

Неправильная

Мы научились из owp делать PRG любой полиномиальной длины.
Ключ k — seed для PRG, любая строка из $\{0,1\}^n$;

$$E(m,k) = m \oplus G(k) = (m_1 \oplus G_1(k)) \circ (m_2 \oplus G_2(k)) \circ \ldots \circ (m_p \oplus G_p(k)),$$

где $G_i(k)$ — i-й бит $G(k)$.

Доказательство.

Отличаем m от $m' \Rightarrow$ взламываем G:
закодируем сами и отличим от "кода случайного сообщения". □

- Длина полиномиальна?
  Но надёжность — для сообщений полиномиальной длины.
- Есть другая проблема...

Криптосистема с общим ключом на основе owp

Взлом неправильной конструкции

Нам дали $E(0, k)$ и $E(m, k)$.

Криптосистема с общим ключом на основе owp

Взлом неправильной конструкции

Нам дали $E(0, k)$ и $E(m, k)$.

Найдём $m = E(0, k) \oplus E(m, k)$.

Аналогично можно выяснить, одинаковы ли i-е биты в двух неизвестных сообщениях.

Криптосистема с общим ключом на основе owp

Взлом неправильной конструкции

Нам дали $E(0, k)$ и $E(m, k)$.

Найдём $m = E(0, k) \oplus E(m, k)$.

Упражнение: Почему не нарушается “обычная” надёжность?
Что, найти m мы можем, а отличить m от 0 — нет?

Private key:

Определение

Криптосистема называется неразличимой, если
$\forall k$ $\forall$ пары **последовательностей** (x, y) полин.длины
сообщений $x^{(1)}, \dots x^{(t)}$ (соответственно, $y^{(1)}, \dots, y^{(t)}$) полин.длины
$\forall$ вер.полин.схем C

$$\left| \Pr\{C(E(x^{(1)}, d, r_E^{(1)}), \dots E(x^{(t)}, d, r_E^{(t)}), \quad 1^n, x, y) = 1\} - \right.$$
$$\left. \Pr\{C(E(y^{(1)}, d, r_E^{(1)}), \dots E(y^{(t)}, d, r_E^{(t)}), \quad 1^n, x, y) = 1\} \right| < \frac{1}{n^k} \dots$$

Public key:

Определение

Криптосистема называется неразличимой, если
$\forall k$ $\forall$ пары **последовательностей** (x, y) полин.длины
сообщений $x^{(1)}, \dots x^{(t)}$ (соответственно, $y^{(1)}, \dots, y^{(t)}$) полин.длины
$\forall$ вер.полин.схем C

$$\left| \Pr\{C(E(x^{(1)}, e, r_E^{(1)}), \dots E(x^{(t)}, e, r_E^{(t)}), e, 1^n, x, y) = 1\} - \right.$$
$$\left. \Pr\{C(E(y^{(1)}, e, r_E^{(1)}), \dots E(y^{(t)}, e, r_E^{(t)}), e, 1^n, x, y) = 1\} \right| < \frac{1}{n^k} \dots$$

Private key:

Определение

Криптосистема называется семантически надежной, если
$\forall h\ \forall f\ \forall C\ \forall k\ \exists \widetilde{C}\ \forall M$

$$\Pr\{C(E(m^{(1)}, d, r_E^{(1)}), \ldots, E(m^{(t)}, d, r_E^{(t)}), \quad f(m^{(1)}, \ldots, m^{(t)})) = h(m^{(1)}, \ldots, m^{(t)}$$
$$\leq \Pr\{\widetilde{C}(\quad f(m^{(1)}, \ldots, m^{(t)})) = h(m^{(1)}, \ldots, m^{(t)})\} + \frac{1}{n^k},$$

где $f, h, C, \widetilde{C}, M$ — вер.полин.схемы,
причём $M(1^n)$ генерирует **последовательность** из t сообщений.

Public key:

Определение

Криптосистема называется семантически надежной, если
$\forall h\ \forall f\ \forall C\ \forall k\ \exists \widetilde{C}\ \forall M$

$$\Pr\{C(E(m^{(1)}, e, r_E^{(1)}), \ldots, E(m^{(t)}, e, r_E^{(t)}), e, f(m^{(1)}, \ldots, m^{(t)})) = h(m^{(1)}, \ldots, m^{(t)}$$
$$\leq \Pr\{\widetilde{C}(e, f(m^{(1)}, \ldots, m^{(t)})) = h(m^{(1)}, \ldots, m^{(t)})\} + \frac{1}{n^k},$$

где $f, h, C, \widetilde{C}, M$ — вер.полин.схемы,
причём $M(1^n)$ генерирует **последовательность** из t сообщений.

Single vs Miltiple Messages Setting

Private key: неэквивалентны.

Public key: эквивалентны.

Доказательство.

Умеем различать коды $x_1, \ldots, x_t$ и $y_1, \ldots, y_t \Rightarrow$

умеем различать коды $x_1, \ldots, x_{i-1}, x_i, y_{i+1}, \ldots, y_t$ и

$$x_1, \ldots, x_{i-1}, y_i, y_{i+1}, \ldots, y_t \Rightarrow$$

сгенерируем все коды $E(x_1), \ldots, E(x_{i-1}), \cancel{E(?)}, E(y_{i+1}), \ldots, E(y_t)$,
вместо i-го подставим данный нам код неизвестного слова (x_i или y_i),
запустим старого противника.

Важно: можем сами генерировать коды. □

Промежуточные итоги

Итак,

- криптосистемы с открытым ключом строятся на основе tdpf; неважно, сколько сообщений;
- криптосистемы с общим ключом должны быть устойчивы относительно многих сообщений — простая конструкция на основе owp не годится;
- но на самом деле существования owf достаточно — поговорим о другой конструкции на следующей лекции...

Промежуточные итоги

Итак,

- криптосистемы с открытым ключом строятся на основе tdpf; неважно, сколько сообщений;
- криптосистемы с общим ключом должны быть устойчивы относительно многих сообщений —
  простая конструкция на основе owp не годится;
- но на самом деле существования owf достаточно
  — поговорим о другой конструкции на следующей лекции...

Промежуточные итоги

Итак,

- криптосистемы с открытым ключом строятся на основе tdpf; неважно, сколько сообщений;
- криптосистемы с общим ключом должны быть устойчивы относительно многих сообщений —
  простая конструкция на основе owp не годится;
- но на самом деле существования owf достаточно
  — поговорим о другой конструкции на следующей лекции...