Сложностная криптография

Эдуард Алексеевич Гирш

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

ПОМИ РАН

2 марта 2008 г.

Криптосистемы с открытым ключом

. . . кодирующие строки произвольной длины

Определение

. . . добавим (полиномиальные) алгоритмы

$$E: \quad \{0,1\}^* \times \{0,1\}^{\varepsilon(n)} \times \{0,1\}^{r(n)} \to \{0,1\}^*$$
$$D: \quad \{0,1\}^* \times \{0,1\}^{\delta(n)} \to \{0,1\}^*$$

- $\forall \mathtt{msg}\ D(E(\mathtt{msg}, \ldots), \ldots) = \mathtt{msg}$ с вероятностью δ, близкой к 1.
- Уже несущественно, что e, d — схемы. Просто ключи.
- Упражнение: можно D дать r_d, но это ничего не изменит.

Замечание

Можно иначе: пусть G получает на вход длину сообщения и выдаёт схемы для этой длины. Красиво (никаких E и D), но неудобно.

Криптосистемы с открытым ключом

. . . кодирующие строки произвольной длины

Определение

. . . добавим (полиномиальные) алгоритмы

$$E: \quad (\mathtt{msg}, e, r_e) \mapsto \mathtt{code}$$
$$D: \quad (\mathtt{code}, d) \mapsto \mathtt{msg}$$

- $\forall \mathtt{msg}\ D(E(\mathtt{msg}, \ldots), \ldots) = \mathtt{msg}$ с вероятностью δ, близкой к 1.
- Уже несущественно, что e, d — схемы. Просто ключи.
- Упражнение: можно D дать r_d, но это ничего не изменит.

Замечание

Можно иначе: пусть G получает на вход длину сообщения и выдаёт схемы для этой длины. Красиво (никаких E и D), но неудобно.

Криптосистемы с открытым ключом

. . . кодирующие строки произвольной длины

Определение

. . . добавим (полиномиальные) алгоритмы

$$E: \quad (\mathtt{msg}, e, r_e) \mapsto \mathtt{code}$$
$$D: \quad (\mathtt{code}, d) \mapsto \mathtt{msg}$$

- $\forall \mathtt{msg}\ D(E(\mathtt{msg}, \ldots), \ldots) = \mathtt{msg}$ с вероятностью δ, близкой к 1.
- Уже несущественно, что e, d — схемы. Просто ключи.
- Упражнение: можно D дать r_d, но это ничего не изменит.

Замечание

Можно иначе: пусть G получает на вход длину сообщения и выдаёт схемы для этой длины. Красиво (никаких E и D), но неудобно.

Криптосистемы с открытым ключом

. . . кодирующие строки произвольной длины

Определение

. . . добавим (полиномиальные) алгоритмы

$$E: \quad (\mathtt{msg}, e, r_e) \mapsto \mathtt{code}$$
$$D: \quad (\mathtt{code}, d) \mapsto \mathtt{msg}$$

- $\forall \mathtt{msg}\ D(E(\mathtt{msg}, \ldots), \ldots) = \mathtt{msg}$ с вероятностью δ, близкой к 1.
- Уже несущественно, что e, d — схемы. Просто ключи.
- Упражнение: можно D дать r_d, но это ничего не изменит.

Замечание

Можно иначе: пусть G получает на вход длину сообщения и выдаёт схемы для этой длины. Красиво (никаких E и D), но неудобно.

Вычислительная неразличимость

Как отличить...

- счётчик Гейгера от компьютера,
- одно вероятностное распределение от другого.

Кто отличает?

- математик?
- компьютер?
- полиномиально ограниченный компьютер!

Определение

P и Q неразличимы, если $\forall k$ $\forall$ противника A

$$\left| \Pr_{x \leftarrow \mathbf{P}} \{A(x) = 1\} - \Pr_{x \leftarrow \mathbf{Q}} \{A(x) = 1\} \right| < \frac{1}{n^k}$$

для достаточно больших n.

Вычислительная неразличимость

Как отличить...

- счётчик Гейгера от компьютера,
- одно вероятностное распределение от другого.

Кто отличает?

- математик?
- компьютер?
- полиномиально ограниченный компьютер!

Определение

P и **Q** неразличимы, если $\forall k$ $\forall$ противника A

$$\left| \Pr_{x \leftarrow \mathbf{P}} \{A(x) = 1\} - \Pr_{x \leftarrow \mathbf{Q}} \{A(x) = 1\} \right| < \frac{1}{n^k}$$

для достаточно больших n.

Вычислительная неразличимость

Как отличить...

- счётчик Гейгера от компьютера,
- одно вероятностное распределение от другого.

Кто отличает?

- математик?
- компьютер?
- полиномиально ограниченный компьютер!

Определение

P и Q неразличимы, если $\forall k$ $\forall$ противника A

$$\left| \Pr_{x \leftarrow \mathbf{P}} \{A(x) = 1\} - \Pr_{x \leftarrow \mathbf{Q}} \{A(x) = 1\} \right| < \frac{1}{n^k}$$

для достаточно больших n.

Вычислительная неразличимость

Как отличить...

- счётчик Гейгера от компьютера,
- одно вероятностное распределение от другого.

Кто отличает?

- математик?
- компьютер?
- полиномиально ограниченный компьютер!

Определение

P и Q неразличимы, если $\forall k$ $\forall$ противника A

$$\left| \Pr_{x \leftarrow \mathbf{P}} \{A(x) = 1\} - \Pr_{x \leftarrow \mathbf{Q}} \{A(x) = 1\} \right| < \frac{1}{n^k}$$

для достаточно больших n.

Вычислительная неразличимость

Как отличить...

- счётчик Гейгера от компьютера,
- одно вероятностное распределение от другого.

Кто отличает?

- математик?
- компьютер?
- полиномиально ограниченный компьютер!

Определение

P и **Q** неразличимы, если $\forall k$ $\forall$ противника A

$$\left| \Pr_{x \leftarrow \mathbf{P}} \{A(x) = 1\} - \Pr_{x \leftarrow \mathbf{Q}} \{A(x) = 1\} \right| < \frac{1}{n^k}$$

для достаточно больших n.

Определение надёжности: неразличимость

Определение

Криптосистема называется неразличимой, если
$\forall k$ $\forall$ пары сообщений (m_0, m_1) полин.длины[1] $\forall$ вер.полин.схем[2] C

$$\Big| \Pr\{C(E(m_0, e, r_e), e, 1^n, m_0, m_1) = 1\} - \Pr\{C(E(m_1, e, r_e), e, 1^n, m_0, m_1) = 1\} \Big| < \frac{1}{n^k}$$

для достаточно больших n;
вероятность берется по r_g, r_e и случайным битам C.

Замечание

Потом будет более сильное определение, добьёмся пока этого.

[1] Вообще-то их тоже соперник генерирует по 1^n.
[2] Вообще-то они эквивалентны детерминированным схемам.

Надежность PKCS для 1 бита, revisited

Определение (1 бит, надёжность против схем)

δ-PKCS *надёжна*, если $\forall$ вер.полин.схем A $\forall k \in \mathbb{N}$ $\exists N$ $\forall n > N$

$$\Pr\{A(e(\mathtt{msg}, r_e), 1^n, e) = \mathtt{msg}\} < \frac{1}{2} + \frac{1}{n^k},$$

где $G(1^n, r_g) = (e, d)$, а вероятность берётся по случайным числам, используемым A, и по (равномерно распределённым) r_g, r_e и $\mathtt{msg}$.

Определение (1 бит, неразличимость схемами)

δ-PKCS *надёжна*, если $\forall$ вер.полин.схем A $\forall k \in \mathbb{N}$ $\exists N$ $\forall n > N$

$$\left|\Pr\{A(e(1, r_e), 1^n, e) = 1\} - \Pr\{A(e(0, r_e), 1^n, e) = 1\}\right| < \frac{1}{n^k},$$

где $G(1^n, r_g) = (e, d)$, а вероятность берётся по случайным числам, используемым A, и по (равномерно распределённым) r_g, r_e ~~и $\mathtt{msg}$~~.

Надежность PKCS для 1 бита, revisited

Определение (1 бит, надёжность против схем)

δ-PKCS *надёжна*, если $\forall$ вер.полин.схем A $\forall k \in \mathbb{N}$ $\exists N$ $\forall n > N$

$$\Pr\{A(e(\mathtt{msg}, r_e), 1^n, e) = \mathtt{msg}\} < \frac{\mathbf{1}}{\mathbf{2}} + \frac{1}{n^k},$$

где $G(1^n, r_g) = (e, d)$, а вероятность берётся по случайным числам, используемым A, и по (равномерно распределённым) r_g, r_e и $\mathtt{msg}$.

Определение (1 бит, неразличимость схемами)

δ-PKCS *надёжна*, если $\forall$ вер.полин.схем A $\forall k \in \mathbb{N}$ $\exists N$ $\forall n > N$

$$\left|\Pr\{A(e(\mathbf{1}, r_e), 1^n, e) = 1\} - \Pr\{A(e(\mathbf{0}, r_e), 1^n, e) = 1\}\right| < \frac{1}{n^k},$$

где $G(1^n, r_g) = (e, d)$, а вероятность берётся по случайным числам, используемым A, и по (равномерно распределённым) r_g, r_e ~~и $\mathtt{msg}$~~.

Криптосистемы с открытым ключом

От одного бита к произвольным строкам

Взломаем криптосистему для одного бита e при помощи взломщика для $E(b_1 b_2 \ldots) = (e(b_1), e(b_2) \ldots)$ (ключи одинаковые!).

Сделаем $m_1 = t_1 \ldots t_p$ из $m_0 = s_1 \ldots s_p$, меняя по одному биту.

$$
\begin{aligned}
&|\Pr\{C(E(s_1 s_2 \ldots s_{p-1} s_p, \ldots\} - \Pr\{C(E(s_1 s_2 \ldots s_{p-1} t_p, \ldots\}| + \\
&|\Pr\{C(E(s_1 s_2 \ldots s_{p-1} t_p, \ldots\} - \Pr\{C(E(s_1 s_2 \ldots t_{p-1} t_p, \ldots\}| + \\
&\qquad\qquad\qquad\qquad \ldots \\
&|\Pr\{C(E(s_1 s_2 \ldots t_{p-1} t_p, \ldots\} - \Pr\{C(E(s_1 t_2 \ldots t_{p-1} t_p, \ldots\}| + \\
&|\Pr\{C(E(s_1 t_2 \ldots t_{p-1} t_p, \ldots\} - \Pr\{C(E(t_1 t_2 \ldots t_{p-1} t_p, \ldots\}| > \frac{1}{n^k}.
\end{aligned}
$$

Какая-то из этих разностей $|\ldots s_i \ldots - \ldots t_i \ldots| > \frac{1}{n^{k'}}$.

Чтобы различить коды двух битов, будем подставлять их вместо s_i и t_i, а остальное генерировать, как в этой разности.

Другое определение: семантическая надёжность

Определение

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

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

где f (посторонняя подсказка) и h (наш интерес) —
— полиномиально вычислимые функции,
M — противник, дающий сообщения,
C — противник, выясняющий по их кодам функцию h,
$\widetilde{C}$ — делающий это *вообще без кода*!

Все работают полиномиальное время, получают на вход также 1^n и $1^{|m|}$.
Вероятность берется по r_g, r_e и $m \leftarrow M(1^n)$.

Равносильность определений

Теорема

Семантическая надежность $\Leftrightarrow$ неразличимость.

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

Лемма

Если g — односторонняя перестановка, сохраняющая длину, B — ее трудный бит, то

$$G(x) = \left(g^{f(\ell)-\ell}(x), B(x), B(g(x)), ..., B(g^{f(\ell)-\ell-1}(x)) \right)$$

является $f(\ell)$-PRG.

PKCS для сообщений произвольной длины

Более эффективная

Пусть g — кодирующая функция tdpf, B — ее трудный бит. Пусть

$$E(b_1 \dots b_m, g, r) = (g^m(r), B(r) \oplus b_1, B(g(r)) \oplus b_2, \dots),$$

где $b_1 \dots b_m$ — сообщение, r — случайные биты.

- Подумайте, почему это эффективнее.
- Подумайте, как раскодировать.

PKCS для сообщений произвольной длины

Более эффективная

Пусть g — кодирующая функция tdpf, B — ее трудный бит. Пусть

$$E(b_1 \dots b_m, g, r) = (g^m(r), B(r) \oplus b_1, B(g(r)) \oplus b_2, \dots),$$

где $b_1 \dots b_m$ — сообщение, r — случайные биты.

- Подумайте, почему это эффективнее.
- Подумайте, как раскодировать.

PKCS для сообщений произвольной длины

Более эффективная

Пусть g — кодирующая функция tdpf, B — ее трудный бит. Пусть

$$E(b_1 \dots b_m, g, r) = (g^m(r), B(r) \oplus b_1, B(g(r)) \oplus b_2, \dots),$$

где $b_1 \dots b_m$ — сообщение, r — случайные биты.

Доказательство неразличимости.

Неразличимость $\Rightarrow$
неотличимость от случайного сообщения $\Rightarrow$
взломщик для PKCS ломает PRG. $\square$