Сложностная криптография

Эдуард Алексеевич Гирш

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

ПОМИ РАН

24 февраля 2008 г.

Криптосистемы с открытым ключом

. . . кодирующие 1 бит

Определение

δ-корректная криптосистема с открытым ключом (δ-PKCS) — это полиномиальный по времени алгоритм $G: (1^n, r_g) \mapsto (e, d)$, (порождающий булевы схемы "надёжности n"), т.ч.

- $e: \{0,1\}^{1+r(n)} \to \{0,1\}^{c(n)}$,
- $d: \{0,1\}^{c(n)} \to \{0,1\}$,
- $\forall \mathtt{msg} \in \{0,1\} \qquad \Pr_{r_e, r_g}\{d(e(\mathtt{msg}, r_e)) = \mathtt{msg}\} \geq \delta$.

Определение

δ-PKCS *надёжна*, если $\forall$ ВПМТ 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 $\mathtt{msg}$.

Криптосистемы с открытым ключом

. . . кодирующие 1 бит

Определение

δ-корректная криптосистема с открытым ключом (δ-PKCS) — это полиномиальный по времени алгоритм $G: (1^n, r_g) \mapsto (e, d)$, (порождающий булевы схемы "надёжности n"), т.ч.

- $e: (\mathtt{msg}, r_e) \mapsto \mathtt{code}$,
- $d: \mathtt{code} \mapsto \mathtt{msg}$.
- $\forall \mathtt{msg} \in \{0,1\}^* \qquad \Pr_{r_e, r_g}\{d(e(\mathtt{msg}, r_e)) = \mathtt{msg}\} \geq \delta$.

Определение

δ-PKCS *надёжна*, если $\forall$ ВПМТ 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 $\mathtt{msg}$.

Трудный бит

- Трудно обратить = трудно узнать все биты.
- Что, если просто узнать первый бит? Все нечётные биты?

Определение

$B\colon \{0,1\}^n \to \{0,1\}$ — трудный бит (hardcore predicate) для f, если

$$\forall k\ \forall A\ \exists N\ \forall n > N \quad \Pr\{A(f(x)) = B(x)\} < \frac{1}{2} + \frac{1}{n^k},$$

где A — вероятностный полиномиальный по времени противник; вероятность берется по случайным битам A и по $x \in \{0,1\}^n$.

Теорема (Голдрейха-Левина)

Если f является owp (tdpf)[1], то $\tilde{f}(x,r) = (f(x), r)$ тоже является owp (tdpf) и имеет трудный бит $B(x,r) = \langle x, r\rangle = x_1 r_1 \oplus x_2 r_2 \oplus \dots$.

[1] "p": permutation = инъективная функция

PKCS from trapdoor with hardcore predicate

$$e'(m, r) = (e(s(r)), B(s(r)) \oplus m),$$

Теорема

Если $G : \ldots \mapsto (e, d, s)$ — tdpf, а B — ее трудный бит, то $G' : \ldots \mapsto (e', d')$ — надежная криптосистема.

Доказательство.

Пусть A' ломает G'. Угадаем $B(s(r))$ по $e(s(r))$!
Берем случайную строку b, и пару $(e(s(r)), b)$ даем A'
(это код какого-то сообщения!).
Если его ответ m верен, то $m \oplus b$ — искомый трудный бит.
Остаётся убедиться, что вероятность — как надо. □

Следствие

$\exists$ tdpf $\Rightarrow \exists$ надежная криптосистема (1-PKCS).

Доказательство теоремы Голдрейха-Левина

Первая попытка

$\tilde{B}$ угадывает трудный бит $\Rightarrow$ взломаем f:

$$\begin{aligned} x_i &= \langle x, r \rangle \oplus \langle x, r \oplus e_i \rangle \\ &= B(x, r) \oplus B(x, r \oplus e_i) \\ &\stackrel{?}{=} \tilde{B}(f(x), r) \oplus \tilde{B}(f(x), r \oplus \bar{e}_i) \end{aligned}$$

($r \oplus \bar{e}_i$ означает, что мы поменяли i-й бит в r).

Доказательство теоремы Голдрейха-Левина

Первая попытка

$\tilde{B}$ угадывает трудный бит $\Rightarrow$ взломаем f:

$$\begin{aligned} x_i &= \langle x, r\rangle \oplus \langle x, r \oplus e_i\rangle \\ &= B(x,r) \oplus B(x, r \oplus e_i) \\ &\stackrel{?}{=} \tilde{B}(f(x), r) \oplus \tilde{B}(f(x), r \oplus \bar{e}_i) \end{aligned}$$

- $\tilde{B}(\ldots) \overset{\text{не всегда}}{=\!=} B(\ldots)$;
  успех в вычислении $B(x,r)$ и $B(x, r \oplus \bar{e}_i)$ – зависимые события!
- Поэтому $\tilde{B}(f(x), r)$ не взламываем —
  — перебираем 2 значения (для всех i ответ одинаков).
- Уменьшаем ошибку (n ошибок!) $\sim$
  $\sim$ повторяем для разных r, слишком много перебирать!
- Сконструируем много разных r с известными ответами.

Доказательство теоремы Голдрейха-Левина

Первая попытка

$\tilde{B}$ угадывает трудный бит $\Rightarrow$ взломаем f:

$$\begin{aligned} x_i &= \langle x, r\rangle \oplus \langle x, r \oplus e_i\rangle \\ &= B(x, r) \oplus B(x, r \oplus e_i) \\ &\stackrel{?}{=} \tilde{B}(f(x), r) \oplus \tilde{B}(f(x), r \oplus \bar{e}_i) \end{aligned}$$

- $\tilde{B}(\ldots) \overline{\overline{\text{не всегда}}} B(\ldots)$;
  успех в вычислении $B(x, r)$ и $B(x, r \oplus \bar{e}_i)$ – зависимые события!
- Поэтому $\tilde{B}(f(x), r)$ не взламываем —
  — перебираем 2 значения (для всех i ответ одинаков).
- Уменьшаем ошибку (n ошибок!) $\sim$
  $\sim$ повторяем для разных r, слишком много перебирать!
- Сконструируем много разных r с известными ответами.

Доказательство теоремы Голдрейха-Левина

Small sample space

Будем проделывать не совсем независимые эксперименты:

- логарифмическое число независимых случайных строк r^j;
- логарифмическое число ответов $\beta_j = B(x, r^j)$ можно перебрать;
- из них построим много не вполне независимых $r^{\mathbf{J}}$ с уже известными ответами.

Для каждого непустого $\mathbf{J} \subseteq \{1, \ldots, l\}$

$$r^{\mathbf{J}} = \bigoplus_{j \in \mathbf{J}} r^j,$$

$$\beta^{\mathbf{J}} = \bigoplus_{j \in \mathbf{J}} \beta^j.$$

Положим $l = (2k+2)\lceil \log_2 n \rceil$ (если $\frac{1}{2} + \frac{1}{n^k}$ — вероятность успеха $\tilde{B}$).
Итого,

$$x_i^{\mathbf{J}} = \beta^{\mathbf{J}} \oplus \tilde{B}(f(x), r^{\mathbf{J}} \oplus \bar{e}_i),$$

$$\tilde{x}_i = \operatorname*{maj}_{\mathbf{J}} x_i^{\mathbf{J}}.$$

Доказательство теоремы Голдрейха-Левина

Подсчёт вероятности

Лемма

Пусть $\tilde{B}$ ломает трудный бит с вероятностью $\frac{1}{2} + \epsilon$. Пусть

$$S_n = \{x \mid \Pr\{\tilde{B}(f(x), r) = B(x, r)\} \geq \frac{1}{2} + \frac{\epsilon}{2}\}.$$

Тогда $|S_n| \geq \frac{\epsilon}{2} \cdot 2^n$.

Лемма

$r^{\mathbf{J}}$ равномерно распределены и попарно независимы.

Рассмотрим $\zeta_i^{\mathbf{J}} = \{x_i = x_i^{\mathbf{J}}\} (\in \{0, 1\})$ — успех (да/нет) для одного $\mathbf{J}$.
Всего их $m = 2^l - 1$.

Лемма

Для достаточно больших n $\Pr\left\{\sum_{\mathbf{J}} \zeta_i^{\mathbf{J}} \leq \frac{m}{2}\right\} < \frac{1}{2n}$.

Лемма

Пусть $\tilde{B}$ ломает трудный бит с вероятностью $\frac{1}{2} + \epsilon$. Пусть

$$S_n = \{x \mid \underbrace{\Pr\{\tilde{B}(f(x), r) = B(x, r)\}}_{S(x)} \geq \tfrac{1}{2} + \tfrac{\epsilon}{2}\}.$$

Тогда $|S_n| \geq \frac{\epsilon}{2} \cdot 2^n$.

Доказательство леммы.

$|\overline{S_n}| = 2^n \Pr_x \left\{S(x) < \frac{1}{2} + \frac{\epsilon}{2}\right\} = 2^n \Pr_x \left\{1 - S(x) \geq \frac{1}{2} - \frac{\epsilon}{2}\right\};$

$\mathbf{E}(1 - S(x)) = 1 - \left(\frac{1}{2} + \epsilon\right) = \frac{1}{2} - \epsilon.$

Неравенство Маркова: $\Pr\{\alpha > \alpha'\} \leq \frac{\mathbf{E}\alpha}{\alpha'}$, где $\alpha \geq 0$.

У нас $\mathbf{E}\alpha = \frac{1}{2} - \epsilon, \quad \alpha' = \frac{1}{2} - \frac{\epsilon}{2}$.

Итак, $2^n \dfrac{\frac{1}{2} - \epsilon}{\frac{1}{2} - \frac{\epsilon}{2}} = 2^n \dfrac{1 - 2\epsilon}{1 - \epsilon} \leq 2^n \left(1 - \dfrac{\epsilon}{2}\right).$ □

Лемма

$r^{\mathbf{J}}$ равномерно распределены и попарно независимы.

Доказательство.

То, что они равномерно распределены, очевидно. Если $K \subseteq \mathbf{J}$, то

$$\mathbf{P}\{r^{\mathbf{J}} = t,\ r^{K} = t'\} = \mathbf{P}\{r^{\mathbf{J}\setminus K} = t \oplus t',\ r^{K} = t'\} \overset{(\mathbf{J}\setminus K)\cap K = \emptyset}{=}$$

$$\mathbf{P}\{r^{\mathbf{J}\setminus K} = t \oplus t'\} \cdot \mathbf{P}\{r^{K} = t'\} \overset{\text{равномерно распределены!}}{=} \mathbf{P}\{r^{\mathbf{J}} = t\} \cdot \mathbf{P}\{r^{K} = t'\}.$$

Значит, можно считать, что $\mathbf{J} \setminus K \neq \emptyset$ и $K \setminus \mathbf{J} \neq \emptyset$. Тогда

$$\mathbf{P}\{r^{\mathbf{J}} = t,\ r^{K} = t'\} = \sum_{t''} \mathbf{P}\{r^{\mathbf{J}} = t,\ r^{K} = t',\ r^{\mathbf{J}\cap K} = t''\} =$$

$$\sum_{t''} \mathbf{P}\{r^{\mathbf{J}\setminus K} = t,\ r^{K\setminus \mathbf{J}} = t',\ r^{\mathbf{J}\cap K} = t''\} =$$

$$\mathbf{P}\{r^{\mathbf{J}\setminus K} = t\} \cdot \mathbf{P}\{r^{K\setminus \mathbf{J}} = t'\} \cdot \underbrace{\sum_{t''} \mathbf{P}\{r^{\mathbf{J}\cap K} = t''\}}_{1} \overset{\text{равн. распр.!}}{=} \mathbf{P}\{r^{\mathbf{J}} = t\} \cdot \mathbf{P}\{r^{K} = t'\}. \quad \square$$

Лемма

Для достаточно больших n $\Pr\left\{\sum_{\mathsf{J}} \zeta_i^{\mathsf{J}} \le \frac{m}{2}\right\} < \frac{1}{2n}$, где $\zeta_i^{\mathsf{J}} = \{x_i = x_i^{\mathsf{J}}\}$ $(\in \{0,1\})$.

Доказательство.

Вероятность успеха в одном испытании равна $\frac{1}{2} + \frac{\epsilon}{2}$, если $x \in S_n$ (на $\Pr\{x \in S_n\}$ потом домножим — она полиномиальна).
Испытания попарно независимы, поэтому

$$\mathbf{E}\sum \zeta_i^{\mathsf{J}} = m\left(\frac{1}{2} + \frac{\epsilon}{2}\right) \Rightarrow \frac{m}{2} = \mathbf{E}\ldots - \frac{m\epsilon}{2}$$

Применим неравенство Чебышёва ($\Pr\{\alpha < \mathbf{E}\alpha - \delta\} < \frac{\mathbf{D}\alpha}{\delta^2}$):

$$\Pr\left\{\sum_{\mathsf{J}} \zeta_i^{\mathsf{J}} < \mathbf{E}\ldots - \frac{m\epsilon}{2}\right\} < \frac{4\mathbf{D}\sum \zeta_i^{\mathsf{J}}}{m^2\epsilon^2} < \frac{4}{m\epsilon^2} \le \frac{4}{n^2}$$

для достаточно больших n (здесь использовано, что благодаря попарной независимости $\mathbf{D}\sum \zeta_i^{\mathsf{J}} = m\mathbf{D}\zeta_i^{\mathsf{J}} < m$). □

Упражнения

Упражнение

Использует ли доказательство тот факт, что $|f(x)| = |f(x')|$, *если* $|x| = |x'|$*?*

Упражнение

Конструкция использует известную ей вероятность успеха противника; как от этого избавиться?

Упражнение

Убедиться, что утверждение теоремы выполнено и для неинъективной owf.

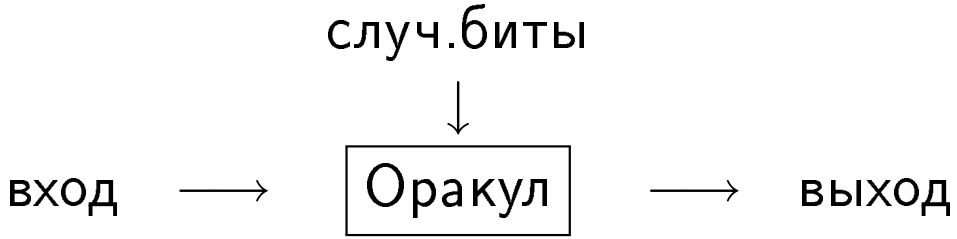
Вычисления с оракулом

Оракул — “чёрный ящик”:

Машина $T^\bullet$ с оракулом — $T^\bullet$ может обращаться к оракулу и получать ответ за 1 шаг. Можно подставлять в $T^\bullet$ разные оракулы, получая вычислительные устройства T^A, T^B, ...

Вычисления с оракулом

Оракул — “чёрный ящик”:



Машина $T^\bullet$ с оракулом — $T^\bullet$ может обращаться к оракулу и получать ответ за 1 шаг. Можно подставлять в $T^\bullet$ разные оракулы, получая вычислительные устройства T^A, T^B, ...

Взломщики

Определение

Функция $f : \{0,1\}^* \to \{0,1\}^*$ — **слабо односторонняя функция**, если

- f вычислима за полиномиальное время на ДПМТ
- и $\exists k \in \mathbb{N} \;\; \forall$ВПМТ A $\;\; \exists N \;\; \forall n > N$

$$\Pr\{A(f(x), 1^n) \in f^{-1}(f(x))\} < 1 - \frac{1}{n^k},$$

где вероятность берётся по случайным числам, используемым A, и равномерному распределению по входным строкам $x \in \{0,1\}^n$.

Определение

Оракул A **взламывает** функцию f с вероятностью $q(n)$, если для бесконечной последовательности длин n_i

$$\Pr_{|x|=n_i}\{A(f(x), 1^n) \in f^{-1}(f(x))\} \geq q(n_i).$$

Сведéния

Определение

$f \rightsquigarrow g$, если $\exists T^{\bullet}$ $\forall k_f$ $\exists k_g$ $\forall$ оракула A

$$A \text{ взламывает } g \text{ с вероятностью } 1 - \frac{1}{n^{k_g}} \Rightarrow$$

$$T^A \text{ взламывает } f \text{ с вероятностью } 1 - \frac{1}{n^{k_f}}.$$

Здесь T — полиномиальный вероятностный алгоритм, A используется как вероятностный оракул (его случайные биты учитываются при запуске T^A).

Определение

u — универсальная [односторонняя] функция, если $\forall f$ (полиномиально вычислимая, честная) $f \rightsquigarrow u$.

u — "самая трудная": $\exists$owf $\Longrightarrow$ u — owf

Универсальная [односторонняя] функция

Конструкция

Теорема

Пусть $u(M, x) = (M, M(x))$, где M — описание машины, x — вход для этой машины, $M(x)$ — выход машины на входе x, причем моделируем мы в течение времени $|x|^2$, а если не успеваем завершить работу, выдаем x. Тогда u — универсальная.

Упражнение

А какое утверждение верно для сильной owf?

Лемма

$\forall$ слабой owf f $\exists \tilde{f}$, вычислимая за время $|x|^2$, т.ч. $f \rightsquigarrow \tilde{f}$.

Доказательство.

$$\tilde{f}(x_1 x_2) = f(x_1)x_2, \text{ где } |x_1| = n,\ |x_2| = m = m(n).$$

Мы можем добиться времени работы $t_f(n) \leq (m+n)^2 - m$ выбором подходящего полинома $m(n)$, т.к. $t_f(n)$ также полином.

Взлом f:

- нам дали $f(x_1)$;
- дописываем к нему случайную строку x_2;
- ломаем оракулом для $\tilde{f}$;
- отбрасываем суффикс.

f ломаем с той же вероятностью, что и оракул для $\tilde{f}$.

Выбором $\tilde{k}$ добиваемся $\dfrac{1}{(m+n)^{\tilde{k}}} < \dfrac{1}{n^k}$. $\square$

Доказательство теоремы.

Сведём взлом f^*, вычисляемой машиной M^* за время n^2, к взлому u.

Для достаточно длинных входов u вычисляет результат именно M^* на доле входов $\mu = \frac{1}{2^{|M^* \cdot \mathrm{const}|}} = \mathrm{const}$.

Если мы не взламываем лишь долю $\frac{1}{n^k}$ от всех входов u, то должны взламывать значительную долю входов из сектора, соответствующего машине M^*; именно, мы взламываем долю $\mu - \frac{1}{n^k}$, что составляет

$$1 - \frac{1}{\mu n^k} \tag{1}$$

по отношению ко всем входам машины M^* длины $n - |M^*|$. Ясно, что для любой требуемой вероятности взлома M^* мы можем подобрать достаточно большие k и n, для которых (1) будет больше искомой. □

Упражнения

Упражнение

Что произойдет в случае семейств односторонних функций (сильных либо слабых)?

Упражнение

Что произойдет, если соперник — детерминированный? Если он задан схемами?