Сложностная криптография

Эдуард Алексеевич Гирш

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

ПОМИ РАН

17 февраля 2008 г.

Основания криптографии

Постановка задачи:

- **Честные участники** *(Алиса, Боб)*.
- **Нечестные участники** *(Чарли)*.
- **Решаемая задача** *(например, передать сообщение от Алисы к Бобу, если есть общий ключ)*.
- **Надёжность** *(например, Чарли, не знающий ключа, не может расшифровать сообщения)*.

Средства:

- **примитивы — «кирпичики», из которых всё строится** *(например, односторонние функции)*,
- **сведéния.**

Односторонние функции

$$\text{просто} \quad \begin{array}{c} \longrightarrow \\ \longleftarrow \end{array} \quad \text{трудно}$$

«Первое приближение»:

- «легко»: $\in \widetilde{\mathbf{P}}$ (можно детерминированно за полиномиальное время),
- «трудно»: $\notin \widetilde{\mathbf{P}}$ (нельзя ...).

Теорема

Пусть $\mathbf{P} \neq \mathbf{NP}$. Тогда существует такая $f \in \widetilde{\mathbf{P}}$, что $f^{-1} \notin \widetilde{\mathbf{P}}$.

Односторонняя в наихудшем случае: доказательство

Доказательство.

Действительно, пусть Φ — формула в КНФ, а A — набор значений переменных. Определим одностороннюю функцию:

$$f(\Phi, A) = \begin{cases} (\Phi, 1^{|A|}), & \text{if } \Phi[A] = \texttt{True}, \\ (\Phi, 0^{|A|}), & \text{otherwise.} \end{cases}$$

Если бы могли обратить эту функцию, мы могли бы найти выполняющий набор для любой выполнимой формулы, вычислив

$$f^{-1}(\Phi, 1^{\text{кол-во переменных}}).$$

Но мы знаем, что эта задача **NP**-трудна. □

Обратная теорема

Определение

Функция f называется честной, если у любой точки z её образа имеется прообраз, длина которого полиномиально (от длины z) ограничена.

В дальнейшем все рассматриваемые односторонние функции и прочие конструкции, основанные на них, — по существу, честные (даже если определения допускают иное).

Упражнение

Доказать обратную теорему

$$\exists f\ (f \in \widetilde{\mathbf{P}} \wedge f^{-1} \notin \widetilde{\mathbf{P}}) \Rightarrow \mathbf{P} \neq \mathbf{NP}$$

в предположении, что f — честная.

Односторонние функции

$$\text{просто} \quad \begin{array}{c} \longrightarrow \\ \longleftarrow \end{array} \quad \text{трудно}$$

«Первое приближение»:

- «легко»: $\in \widetilde{\mathbf{P}}$ (можно детерминированно за полиномиальное время),
- «трудно»: $\notin \widetilde{\mathbf{P}}$ (нельзя . . .).

Чарли может пользоваться случайными числами!
Чарли может обратить во всех точках, кроме одной!
Чарли может обратить для почти всех длин ключей!

Односторонние функции

просто

$\Longrightarrow$

$\Longleftarrow$

трудно

Определение

Функция $f : \{0,1\}^* \to \{0,1\}^*$ называется [сильно] односторонней (one-way function, owf), если

- f вычислима за полиномиальное время на ДПМТ[1],
- $\forall$ ВПМТ A $\quad \forall k \in \mathbb{N} \quad \exists N \quad \forall n > N$

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

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

[1] ДПМТ/ВПМТ = детерминированная/вероятностная полиномиальная по времени машина Тьюринга

Односторонние функции

$$\text{просто} \quad \underset{\longleftarrow}{\longrightarrow} \quad \text{трудно}$$

Определение

Функция $f : \{0,1\}^* \to \{0,1\}^*$ называется [сильно] односторонней (one-way function, owf), если

- f вычислима за полиномиальное время на ДПМТ[1],
- $\forall$ ВПМТ A $\quad \forall k \in \mathbb{N} \quad \exists N \quad \forall n > N$

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

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

[1] ДПМТ/ВПМТ = детерминированная/вероятностная полиномиальная по времени машина Тьюринга

Примеры кандидатов в owf

Пример

$f(a, b) = a \cdot b$.

Пример

$f(p, q) = p \cdot q$, где $p, q \in \mathbb{P}$, $\log p \approx \log q$.

Пример

$f(x_1, x_2, \ldots, x_n, I) = (x_1, x_2, \ldots, x_n, \sum_{i \in I} x_i)$, где $I \subseteq \{1, \ldots, n\}$
(это NP-трудная задача SUBSET SUM, похожая на задачу о рюкзаке).

Что такое здесь запятые?

Примеры кандидатов в owf

Пример

$f(a, b) = a \cdot b$.

Пример

$f(p, q) = p \cdot q$, где $p, q \in \mathbb{P}$, $\log p \approx \log q$.

Пример

$f(x_1, x_2, \ldots, x_n, I) = (x_1, x_2, \ldots, x_n, \sum_{i \in I} x_i)$, где $I \subseteq \{1, \ldots, n\}$
(это NP-трудная задача SUBSET SUM, похожая на задачу о рюкзаке).

Что такое здесь запятые?

Примеры кандидатов в owf

Пример

$f(a, b) = a \cdot b$.

Пример

$f(p, q) = p \cdot q$, где $p, q \in \mathbb{P}$, $\log p \approx \log q$.

Пример

$f(x_1, x_2, \ldots, x_n, I) = (x_1, x_2, \ldots, x_n, \sum_{i \in I} x_i)$, где $I \subseteq \{1, \ldots, n\}$
(это NP-трудная задача SUBSET SUM, похожая на задачу о рюкзаке).

Что такое здесь запятые?

Примеры кандидатов в owf

Пример

$f(a, b) = a \cdot b$.

Пример

$f(p, q) = p \cdot q$, где $p, q \in \mathbb{P}$, $\log p \approx \log q$.

Пример

$f(x_1, x_2, \ldots, x_n, I) = (x_1, x_2, \ldots, x_n, \sum_{i \in I} x_i)$, где $I \subseteq \{1, \ldots, n\}$
(это NP-трудная задача SUBSET SUM, похожая на задачу о рюкзаке).

Что такое здесь запятые?

Упражнения

Упражнение

Пусть f вычислима на ВПМТ: изменится ли понятие, будет ли существование старых owf эквивалентно существованию новых owf?

Упражнение

Наоборот, пусть A — ДПМТ: ...

Упражнение

A если f или A — последовательности булевых схем, детерминированных или вероятностных?..

Упражнение (СЕЙЧАС)

Что будет, если x будет распределено на $\{0,1\}^n$ не равномерно, а иначе (но вычислимо за полиномиальное время)?

Упражнения

Упражнение

Пусть f вычислима на ВПМТ: изменится ли понятие, будет ли существование старых owf эквивалентно существованию новых owf?

Упражнение

Наоборот, пусть A — ДПМТ: ...

Упражнение

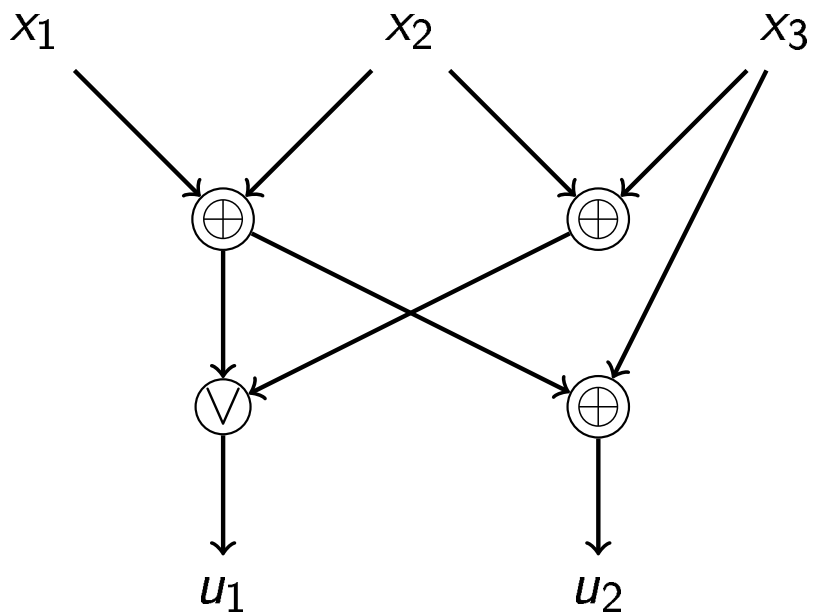
A если f или A — последовательности булевых схем, детерминированных или вероятностных?..

Упражнение (СЕЙЧАС)

Что будет, если x будет распределено на $\{0,1\}^n$ не равномерно, а иначе (но вычислимо за полиномиальное время)?

Булевы схемы: напоминание

- Ориентированный граф без циклов.
- Бинарные (и унарные) операции над битами: $\wedge$, $\vee$, $\oplus$, ...
- Пример (4 гейта):



- «Время» = количество гейтов.

Упражнения

Упражнение

Пусть f вычислима на BMT: изменится ли понятие, будет ли существование старых owf эквивалентно существованию новых owf?

Упражнение

Наоборот, пусть A — $ДMT$: ...

Упражнение

A если f или A — последовательности булевых схем, детерминированных или вероятностных?..

Упражнение (СЕЙЧАС)

Что будет, если x будет распределено на $\{0,1\}^n$ не равномерно, а иначе (но вычислимо за полиномиальное время)?

Упражнения

Упражнение

Пусть f вычислима на BMT: изменится ли понятие, будет ли существование старых owf эквивалентно существованию новых owf?

Упражнение

Наоборот, пусть A — $ДMT$: ...

Упражнение

A если f или A — последовательности булевых схем, детерминированных или вероятностных?..

Упражнение (СЕЙЧАС)

Что будет, если x будет распределено на $\{0,1\}^n$ не равномерно, а иначе (но вычислимо за полиномиальное время)?

Семейства односторонних функций

Много кому надо шифровать — значит, каждому нужна своя собственная односторонняя функция!

Определение

Семейство односторонних функций (one-way function family, owff) — это детерминированный полиномиальный по времени алгоритм $G\colon (1^n, r_g) \mapsto (e, s)$ (булевы схемы), где

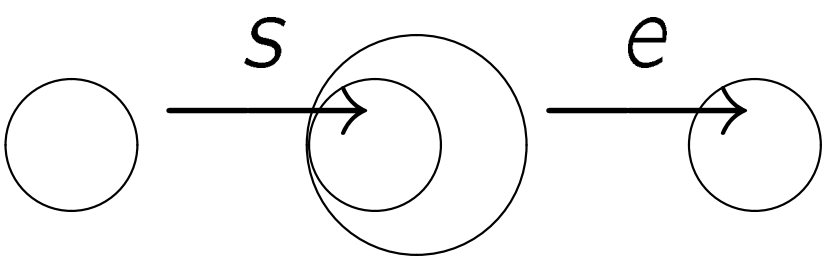
- $e\colon \{0,1\}^n \to \{0,1\}^{\epsilon(n)}$ (encryptor)
- $s\colon \{0,1\}^{\sigma(n)} \to \{0,1\}^n$ (sampler),

причём $\forall$ ВПМТ $A \quad \forall k \in \mathbb{N} \quad \exists N \quad \forall n > N$

$$\Pr\{A(e(s(r_s)), 1^n, e, s) \in e^{-1}(e(s(r_s)))\} < \frac{1}{n^k},$$

где $G(1^n, r_g) = (e, s)$, а вероятность берётся по случайным числам, используемым A, и по (равномерно распределённым) r_g и r_s.

Семейства односторонних функций



Упражнения

Упражнение

А нужно ли передавать взломщику s?

Упражнение

Что произойдёт, если ограничиться $e\colon \{0,1\}^n \to \{0,1\}^n$ или, наоборот, разрешить[2] *$e\colon \{0,1\}^{p(n)} \to \{0,1\}^{p(n)}$?*

Упражнение

Сравнить определение односторонней функции с определением из какой-нибудь книги[3] *и понять, эквивалентны ли они.*

---

[2] **NB:** в книге Голдрейха именно так.

[3] К примеру, Oded Goldreich, Foundations of Cryptography.

owf vs owff

Теорема

$\exists f$ — односторонняя функция $\Leftrightarrow$
$\exists G$ — семейство односторонних функций.

Доказательство.

"$\Rightarrow$":

$G(1^n, \cdot)$:

- e — моделирует[4] работу алгоритма, вычисляющего f на длине n,
- s — тривиальная схема $s(x) = x$.

"$\Leftarrow$":

- $f(r_g, r_s) = (e(s(r_s)), e, s)$, где $G(1^n, r_g) = (e, s)$.

□

[4] Как моделируется цикл? Почему этого достаточно?

Слабо односторонние функции

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 $x \in \{0,1\}^n$.

Теорема

$\exists f_w$ — слабо односторонняя функция $\Leftrightarrow$
$\exists f_s$ — сильно односторонняя функция.

Слабая $\mapsto$ сильная owf

Конструкция:

$$f_s(x_1, x_2, \ldots, x_m) = (f_w(x_1), f_w(x_2), \ldots, f_w(x_m)),$$

где $m = m(n)$ — полином.

Сведéние:

A_s обращает f_s с вероятностью $1/n^{k_s}$

$\Downarrow$

Построим A'_w, обращающий f_w.

$A'_w(y)$:

- `for each` $j = 1..m$,
  - $x_1, \ldots, x_m \leftarrow$ random;
  - $x = A_s(f_w(x_1), \ldots, f_w(x_{j-1}), y, f_w(x_{j+1}), \ldots, f_w(x_m))_j$.
  - `if` $f_w(x) = y$, `then return` x.

Упражнения

Упражнение

Можно ли перенести эту теорему на случай owff?

Упражнение

f_s получилась определённой на довольно редком множестве. Как быть со входами длины, отличной от mn?

Функции с секретом

Определение

Семейство функций с секретом (trapdoor function family, tdff) — это детерминированный полиномиальный по времени алгоритм $G\colon (1^n, r_g) \mapsto (e, d, s)$ (булевы схемы), где

- $e\colon \{0,1\}^n \to \{0,1\}^{\epsilon(n)}$ (encryptor)
- $d\colon \{0,1\}^{\epsilon(n)} \to \{0,1\}^n$ (decryptor)
- $s\colon \{0,1\}^{\sigma(n)} \to \{0,1\}^n$ (sampler),

причём $\forall x \in \mathrm{Im}(s)\ d(e(x)) = x$ и

$\forall$ ВПМТ A $\quad \forall k \in \mathbb{N}\ \ \exists N\ \ \forall n > N$

$$\Pr\{A(e(s(r_s)), 1^n, e, s) \in e^{-1}(e(s(r_s)))\} < \frac{1}{n^k},$$

где $G(1^n, r_g) = (e, d, s)$, а вероятность берётся по случайным числам, используемым A, и по (равномерно распределённым) r_g и r_s.

Функции с секретом

Определение

Семейство функций с секретом (trapdoor function family, tdff) — это детерминированный полиномиальный по времени алгоритм $G\colon (1^n, r_g) \mapsto (e, d, s)$ (булевы схемы), где

- $e\colon \{0,1\}^n \to \{0,1\}^{\epsilon(n)}$ (encryptor)
- $d\colon \{0,1\}^{\epsilon(n)} \to \{0,1\}^n$ (decryptor)
- $s\colon \{0,1\}^{\sigma(n)} \to \{0,1\}^n$ (sampler),

причём $\forall x \in \mathrm{Im}(s)\ d(e(x)) = x$ и
$\forall$ ВПМТ $A \quad \forall k \in \mathbb{N} \quad \exists N \quad \forall n > N$

$$\Pr\{A(e(s(r_s)), 1^n, e, s) \in e^{-1}(e(s(r_s)))\} < \frac{1}{n^k},$$

где $G(1^n, r_g) = (e, d, s)$, а вероятность берётся по случайным числам, используемым A, и по (равномерно распределённым) r_g и r_s.

tdff — пример

Пример

$$
\begin{aligned}
s(x) &= x, \\
e(x) &= x^{\varepsilon} \mod N, \\
d(x) &= x^{\delta} \mod N,
\end{aligned}
$$

где

$$
\begin{aligned}
&\varepsilon \cdot \delta \equiv 1 \pmod{(p-1)(q-1)}, \\
&N = p \cdot q, \\
&p, q \in \mathbb{P}
\end{aligned}
$$