Курс лекций по теоретической криптографии

Тема 8. **Псевдослучайные семейства функций и перестановок**

Шокуров А.В.

Определение псевдослучайного семейства функций

Будем рассматривать семейства функций вида

$$F = \bigcup_{n\in\mathbb{N}} F_n = \{f_{n,i} : \mathbb{B}^{l(n)} \to \mathbb{B}^{m(n)}\}_{\substack{n\in\mathbb{N}\\ i\in\mathbb{B}^n}}, \qquad F_n \subseteq \mathrm{Fun}(\mathbb{B}^{l(n)}, \mathbb{B}^{m(n)}),$$

где $l(\cdot)$, $m(\cdot)$ — некоторые полиномы, а $\mathrm{Fun}(X, Y)$ — множество всех функций, определённых на X и принимающих значения в Y.

Определение

F называется *псевдослучайным семейством функций*, если

1. F полиномиально вычислимо[a];
2. для любой п. в. м. Т. A

$$\left|\Pr_i\left[A^{f_{n,i}}(1^n) = 1\right] - \Pr_\varphi\left[A^{\varphi}(1^n) = 1\right]\right| = \mathrm{negl}(n),$$

где $i \in_U \mathbb{B}^n$, $\varphi \in_U \mathrm{Fun}(\mathbb{B}^{l(n)}, \mathbb{B}^{m(n)})$.

[a] То есть полиномиально вычислима функция $(1^n, i, x) \mapsto f_{n,i}(x)$.

Функции $f_{n,i}$ и φ машине A неизвестны, но она имеет доступ к оракулам, возвращающим значения соответствующих функций на заданном машиной A аргументе.

Генераторы псевдослучайных функций

NB В более общем варианте определения i выбирается согласно произвольному полиномиально конструируемому распределению. Но это не принципиально, так как в таком случае можно рассматривать равномерное распределение на заполнении «случайной» ленты машины, реализующей это распределение.

То же самое понятие можно рассматривать как особый генератор семейства функций.

Генератор для семейства функций F — это пара алгоритмов (I, C),

- I — полиномиальная вероятностная машина Тьюринга:
  $I(1^n) = i$ — индекс (описание) функции в F_n, $\quad i \leftrightarrow f_{n,i} \in F_n$;
- C — полиномиальная (детерминированная) машина Тьюринга:
  для всех n, i и $x \in \mathbb{B}^{l(n)}$ $\quad C(1^n, i, x) = f_{n,i}(x)$.

Генератором псевдослучайных функций будем называть генератор (I, C) для псевдослучайного семейства функций F относительно некоторого семейства вероятностных распределений $\{\mathcal{I}_n\}$.

Семейство $\{f'_{n,r} = f_{n,I(r;1^n)}\}$ (с несколько изменённой индексацией функций) будет удовлетворять определению псевдослучайного семейства функций (относительно семейства *равномерных* распределений на множествах индексов).

Необходимое условие существования псевдослучайных семейств

Утверждение

Если существует псевдослучайное семейство функций,
то существует псевдослучайный генератор.

Доказательство.
Пусть семейство $F = \{f_{n,i} : \mathbb{B}^{l(n)} \to \mathbb{B}^{m(n)}\}_{\substack{n\in\mathbb{N} \\ i\in\mathbb{B}^n}}$ псевдослучайно.

Обозначим: $s(n) = \left\lfloor \frac{n}{m(n)} \right\rfloor + 1$.

Будем считать[1], что $n < 2^{l(n)} m(n)$ для всех n, поэтому $s(n) \leqslant 2^{l(n)}$.

Найдутся такие *различные* строки $w_{n,1}, \ldots, w_{n,s(n)} \in \mathbb{B}^{l(n)}$, что функция $1^n \mapsto (w_{n,1}, \ldots, w_{n,s(n)})$ полиномиально вычислима
(например, $w_{n,t}$ — двоичная запись числа $t-1$).

Определим функцию g на аргументах $x \in \mathbb{B}^n$ по всем n:

$$g(x) = f_{n,x}(w_{n,1}) \ldots f_{n,x}(w_{n,s(n)}).$$

[1] По-хорошему, надо это условие включить в формулировку утверждения, но мы для простоты отбрасываем «крайний» случай, когда $l(n)$ и $m(n)$ почти не растут.

Необходимое условие существования псевдослучайных семейств

Покажем, что g — псевдослучайный генератор.

- g полиномиально вычислима.
- $g(\mathbb{B}^n) \subset \mathbb{B}^{m(n)s(n)}$,
  $m(n)s(n) > n \quad \Rightarrow \quad |g(x)| > |x|$ для всех x.
- Рассмотрим произвольную п. в. м. Т. D и возьмём п. в. м. Т. A:

$$A^h(1^n) = D\big(1^n, h(w_{n,1}) \ \ldots h(w_{n,s(n)})\big)$$

для любой функции $h \in \mathrm{Fun}(\mathbb{B}^{l(n)}, \mathbb{B}^{m(n)})$.

Если $\varphi \in_{\mathcal{U}} \mathrm{Fun}(\mathbb{B}^{l(n)}, \mathbb{B}^{m(n)})$, то $\varphi(y)$ для разных $y \in \mathbb{B}^{l(n)}$ — независимые равномерно распределённые случайные величины.
Следовательно, случайная величина $\varphi(w_{n,1}) \ \ldots \varphi(w_{n,s(n)})$ имеет равномерное распределение на $\mathbb{B}^{m(n)s(n)}$.

$$\big|\Pr\big[D(1^n, g(\upsilon_n)) = 1\big] - \Pr\big[D(1^n, \upsilon_{m(n)s(n)}) = 1\big]\big| =$$

$$= \big|\Pr\big[A^{f_{n,\upsilon_n}}(1^n) = 1\big] - \Pr\big[A^{\varphi}(1^n) = 1\big]\big| = \mathrm{negl}(n) \text{ по условию.} \qquad \square$$

Теорема Гольдрайха—Гольдвассер—Микали

Теорема (Goldreich, Goldwasser, Micali)

Если существует псевдослучайный генератор, то для любых полиномов $l(\cdot)$ и $m(\cdot)$ существует псевдослучайное семейство функций $F = \{f_{n,i} : \mathbb{B}^{l(n)} \to \mathbb{B}^{m(n)}\}_{\substack{n\in\mathbb{N}\\ i\in\mathbb{B}^n}}$.

Схема доказательства.

Возьмём псевдослучайный генератор g, $g(\mathbb{B}^n) \subset \mathbb{B}^{2n}$ для всех n, и функции

$$g_0(y) = g(y)^{[1\,\ldots n]}, \qquad g_1(y) = g(y)^{[n+1\,\ldots 2n]}, \qquad y \in \mathbb{B}^n, \quad n \in \mathbb{N}.$$

Определим функции семейства для $x \in \mathbb{B}^{l(n)}$ по всем n:

$$f'_{n,i}(x) = g_{x^{[l(n)]}}\left(\ \ldots g_{x^{[2]}}\left(g_{x^{[1]}}(i)\right)\ \ldots\right) \in \mathbb{B}^n.$$

Псевдослучайность семейства $F' = \{f'_{n,i}\}$ доказывается от противного:
если п. в. м. Т. A отличает функции семейства от случайных, построим п. в. м. Т. B, которая запускает A, выдаёт ей (вместо оракула) значения хитро строящейся функции h и возвращает в конце выход машины A,
тогда B будет нарушать определение псевдослучайного генератора g.

Далее «растянем» (до длины $m(n)$) значения функций семейства F' с помощью их композиции с подходящим псевдослучайным генератором. Полученное семейство F будет таким же псевдослучайным, как и F'.

Псевдослучайные семейства функций для построения шифров

Следствие

Псевдослучайные семейства функций существуют тогда и только тогда, когда существуют односторонние функции.

Псевдослучайные семейства функций можно использовать для построения стойких[2] криптосистем с секретным ключом.

Пусть $\{f_{n,i}\}$ — псевдослучайное семейство функций.

n — параметр стойкости

m — открытый текст, при необходимости дополненный до длины $m(n)$

- $G \equiv I$: $G(1^n) = i$ — секретный ключ
- E: $r \in_{\mathcal{U}} \mathbb{B}^{l(n)}$, $\quad E(r; 1^n, i, m) = m \oplus f_{n,i}(r) = c$ — криптограмма

  Получателю передаётся пара (r, c).
- D: $D(1^n, i, r, c) = c \oplus f_{n,i}(r) = m$

Это система *вероятностного* шифрования для сообщений фиксированной (для заданного n) длины. Более длинные сообщения разбиваются на блоки длины $m(n)$ и шифруются поблоково. Подобные криптосистемы называются *блоковыми*.

[2] В том же смысле, что и для примера потокового шифра на прошлой лекции.

Полиномиально инвертируемые псевдослучайные семейства перестановок

Будем рассматривать семейства *перестановок* $F = \{f_{n,i} : \mathbb{B}^{l(n)} \to \mathbb{B}^{l(n)}\}_{\substack{n \in \mathbb{N} \\ i \in \mathbb{B}^n}}$, где $f_{n,i}$ — биекции.

Определение

F — *псевдослучайное семейство перестановок*, если

1. F полиномиально вычислимо;
2. для любой п. в. м. Т. A

$$\left|\Pr_i\left[A^{f_{n,i}}(1^n) = 1\right] - \Pr_\pi\left[A^{\pi}(1^n) = 1\right]\right| = \mathrm{negl}(n),$$

где $i \in_{\mathcal{U}} \mathbb{B}^n$, $\pi \in_{\mathcal{U}} \mathrm{Per}(\mathbb{B}^{l(n)})$.

Дополнительное условие:

Определение

F называется *полиномиально инвертируемым семейством перестановок*, если полиномиально вычислима функция $(1^n, i, y) \mapsto f_{n,i}^{-1}(y)$, где $n \in \mathbb{N}$, $i \in \mathbb{B}^n$, $y \in \mathbb{B}^{l(n)}$.

Теорема Луби—Ракоффа

Теорема (Luby, Rackoff)

Если существует псевдослучайное семейство функций, сохраняющих длину, то существует полиномиально инвертируемое псевдослучайное семейство перестановок.

Схема доказательства. Рассмотрим *преобразование Файстеля* Φ, которое превращает произвольную функцию, сохраняющую длину, в перестановку.

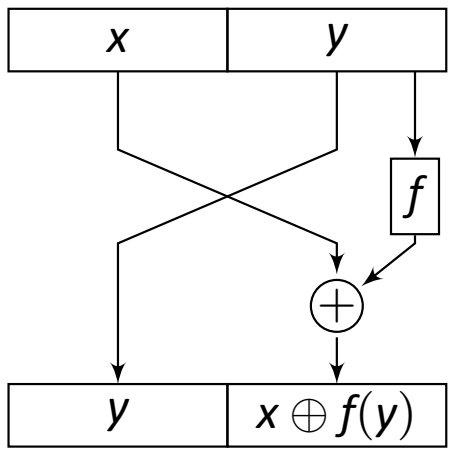
$$f : \mathbb{B}^n \to \mathbb{B}^n \quad \mapsto \quad \Phi_f : \mathbb{B}^{2n} \to \mathbb{B}^{2n}$$

для всех $n \in \mathbb{N}$

$$\Phi_f(xy) = y(x \oplus f(y))$$

$x, y, u, v \in \mathbb{B}^n$

$$\Phi_f^{-1}(uv) = (v \oplus f(u))u$$



Пусть $\{f_{n,i} : \mathbb{B}^n \to \mathbb{B}^n\}$ — псевдослучайное семейство функций.

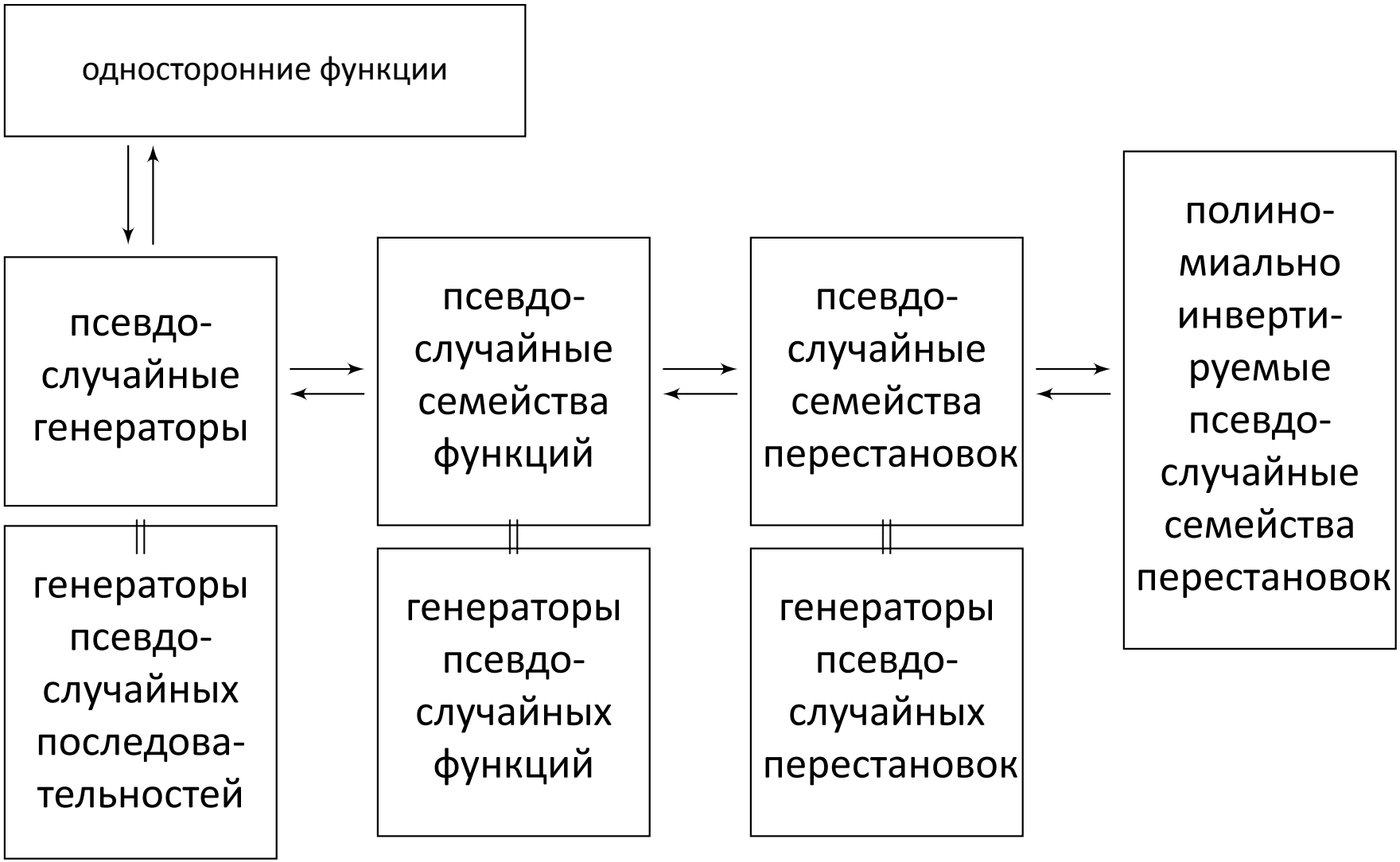
Для всех n и $i_1, i_2, i_3 \in \mathbb{B}^n$ определим перестановки $g_{n,i_1 i_2 i_3} \in \mathrm{Per}(\mathbb{B}^{2n})$ так:

$$g_{n,i_1 i_2 i_3}(x) = \Phi_{f_{n,i_3}}\left(\Phi_{f_{n,i_2}}\left(\Phi_{f_{n,i_1}}(x)\right)\right), \quad x \in \mathbb{B}^{2n}$$

Семейство $\{g_{n,i_1 i_2 i_3}\}_{\substack{n \in \mathbb{N} \\ i_1, i_2, i_3 \in \mathbb{B}^n}}$ — очевидно, полиномиально инвертируемое.

Далее доказывается, что оно псевдослучайно.

Критерии существования криптографических примитивов



Построение криптосистемы из полиномиально инвертируемого псевдослучайного семейства перестановок

Пусть $F = \{f_{n,i} : \mathbb{B}^{l(n)} \to \mathbb{B}^{l(n)}\}$ — полиномиально инвертируемое псевдослучайное семейство перестановок.

n — параметр стойкости

m — открытый текст, при необходимости дополненный до длины $l(n)$

$M_n = \mathbb{B}^{l(n)}$

- G: $G(1^n) = i \in_{\mathcal{U}} \mathbb{B}^n$ — секретный ключ
- E: $E(1^n, i, m) = f_{n,i}(m) = c \in \mathbb{B}^{l(n)}$ — криптограмма
- D: $D(1^n, i, c) = f_{n,i}^{-1}(c) = m$

D — полиномиальная м. Т., так как семейство F полиномиально инвертируемо

Такая (блоковая) криптосистема с секретным ключом — IND-CPA-стойкая.

NB Но если позволить шифровать более длинные сообщения, разбивая их на блоки длины $l(n)$ и применяя к ним перестановку по отдельности, то такая система уже не будет IND-стойкой.

? Придумайте метод осуществления угрозы различения двух шифртекстов, если соответствующий оракул на запрос $m = m_1 m_2 \ldots m_k \in \mathbb{B}^{k \cdot l(n)}$, где $m_j \in \mathbb{B}^{l(n)}$, возвращает

$$E(1^n, i, m) = f_{n,i}(m_1) f_{n,i}(m_2) \ldots f_{n,i}(m_k).$$