

# „Теоретико-сложностные основы криптографии“.

## Заметки к курсу в СПбАУ

А.В. Смаль

12 апреля 2018 г.

### Аннотация

Курс посвящён изучению теоретических оснований, на которых строится надёжность криптографических протоколов.

### Содержание

<b>1. Совершенная надёжность</b>	<b>2</b>
<b>2. Односторонние функции</b>	<b>2</b>
2.1. Односторонние функции с худшем случае . . . . .	3
2.2. Односторонние функции для алгоритмов . . . . .	3
2.3. Односторонние функции для неравномерного противника . . . . .	3
2.4. Примеры односторонних функций . . . . .	4
2.5. Построение сильно односторонних функций из слабо односторонних . . . . .	5
2.6. Частичные односторонние функции . . . . .	7
<b>3. Генераторы псевдослучайных чисел</b>	<b>9</b>
3.1. Вычислительно неотличимые случайные величины . . . . .	9
3.2. Генераторы псевдослучайных чисел . . . . .	10
3.3. Трудный бит . . . . .	11
<b>4. Протоколы с секретным ключом</b>	<b>16</b>
4.1. Эффективная схема шифрования с закрытым ключом . . . . .	20
<b>5. Протоколы с открытым ключом</b>	<b>20</b>
<b>6. Протокол привязки (схема обязательства, commitment protocol)</b>	<b>22</b>
6.1. Неинтерактивный протокол привязки к строке . . . . .	22
<b>7. Интерактивные протоколы</b>	<b>23</b>
7.1. Интерактивные протоколы привязки к строке . . . . .	23
7.2. Протокол подбрасывания монетки . . . . .	24

## Введение

Мы будем предполагать, что алгоритмы шифрования/дешифрования всем известны (т.е. по security by obscurity).

### 1. Совершенная надёжность

**Определение 1.1.** Система шифрования с закрытым ключом — это пара алгоритмов  $E(k, m)$  и  $D(k, c)$ , такая, что для любых  $k$  и  $m$  выполняется  $D(k, E(k, m)) = m$ . Система называется *совершенно надёжной*, если для любых двух сообщений  $m_1$  и  $m_2$  случайные величины  $E(k, m_1)$  и  $E(k, m_2)$  при  $k \leftarrow \mathcal{U}(\mathcal{K})$  распределены одинаково ( $\mathcal{K}$  — пространство ключей).

*Замечание 1.1.* Система шифрования с одноразовым шифроблокнотом является совершенно надёжной.

*Замечание 1.2.* Для совершенной надёжности необходимо, чтобы длина ключа была не менее длины сообщения.

**Теорема 1.1.** Пусть  $P = NP$ . Тогда для любой системы шифрования с закрытым ключом  $(E, D)$  с полиномиальным алгоритмом  $E$ , в которой  $|m| > |k|$ , существуют сообщения  $m_0$  и  $m_1$  и полиномиальный алгоритм  $A$ , для которого

$$\left| \Pr_k[A(E(k, m_0)) = 1] - \Pr_k[A(E(k, m_1)) = 1] \right| \geq \frac{1}{2}.$$

*Доказательство.* Не уменьшая общности предположим, что  $\mathcal{K} = \{0, 1\}^{n-1}$ . Возьмём в качестве  $m_0 = 0^n$ . Пусть  $S = \{E(k, 0^n) \mid k \in \mathcal{K}\}$ . Легко видеть, что  $S \in NP$  и  $|S| \leq 2^{n-1}$ . Возьмём в качестве алгоритма  $A$  полиномиальный разрешающий алгоритм для  $S$ , т.е.  $A(y) := [y \in S]$  (он существует по предположению  $P = NP$ ).

Для каждого сообщения  $m$  рассмотрим  $t_m = |\{k \mid E(k, m) \in S\}|$ . Если существует сообщение  $m^*$ , для которого  $t_{m^*} \leq 2^{n-1}$ , то  $m_1 = m^*$  удовлетворяет требованиям.

Предположим теперь, что  $t_m > 2^{n-2}$  для любого  $m$ . Это значит, что существуют более  $2^{n-2} \cdot 2^n = 2^{2n-2}$  пар ключ-сообщение  $(k, m)$ , для которых  $E(k, m) \in S$ . Следовательно, для некоторого  $y \in S$  существует более  $2^{2n-2}/|S| \geq 2^{n-1}$  пар  $(k, m) : E(k, m) = y$ , т.е. существуют ключ  $k$  и два различных сообщения  $m'$  и  $m'' : E(k, m') = E(k, m'')$ . Это противоречит корректности системы шифрования.  $\square$

### 2. Односторонние функции

Доказывать надёжность криптографических протоколов без каких-либо предположений, к сожалению, не получается — из такого доказательства следовало бы  $P \neq NP$ . Было бы здорово показать, что криптография возможна, если  $P \neq NP$ , но это тоже не получается сделать. Поэтому в дальнейшем мы будем отталкиваться от более сильного предположения — предположения о существовании *односторонней функции*.

В дальнейшем мы будем рассматривать семейства функций  $f_n : \{0, 1\}^{k(n)} \rightarrow \{0, 1\}^{l(n)}$ , где  $k(n)$  и  $l(n)$  будут некоторыми полиномами. Кроме того, нас почти всегда будут интересовать функции, которые можно вычислить за полиномиальное время.

**Определение 2.1.** Семейство функций  $f_n : \{0, 1\}^{k(n)} \rightarrow \{0, 1\}^{l(n)}$  называется *полиномиально вычислимым*, если имеется алгоритм, который получая на вход число  $n$  и  $x$  длины  $k(n)$  вычисляет  $f_n(x)$  за полиномиальное от  $n$  время.

## 2.1. Односторонние функции с худшем случае

**Определение 2.2.** Полиномиально вычислимое семейство функций  $f_n : \{0, 1\}^{k(n)} \rightarrow \{0, 1\}^{l(n)}$  называется *односторонним в худшем случае*, если не существует полиномиально вычислимой функции  $g_n$ , что для любого  $x \in \{0, 1\}^{k(n)}$  верно  $f_n(g_n(f_n(x))) = f_n(x)$ .

**Теорема 2.1.** *Односторонние функции с худшем случае существуют  $\iff P \neq NP$ .*

*Доказательство.*

$\Rightarrow$  Пусть  $P = NP$ . Определим язык  $L = \{(1^n, y, z) \mid \exists x, |x| = k(n), z \sqsubset x, f_n(x) = y\}$ ,  $L \in NP$ . По предположению для  $L$  существует полиномиальный разрешающий алгоритм. Для нахождения прообраза  $y$  запустим этот алгоритм сначала на слове  $(1^n, y, \lambda)$ , где  $\lambda$  — пустая строка. Если это слово не принадлежит  $L$ , то  $y$  не имеет прообраза. В противном случае восстановим прообраз  $y$  по битам: сначала запустим алгоритм для слова  $(1^n, y, 0)$  и проверим, есть ли у  $y$  прообраз начинающийся с нуля. Далее аналогично восстановим второй и все последующие биты. Нам потребуется  $k(n) + 1$  запуск полиномиального алгоритма, т.е. прообраз можно найти алгоритмически за полиномиальное время.

$\Leftarrow$  Если  $P \neq NP$ , то можно построить одностороннюю в худшем на основе любой  $NP$ -трудной задачи. Пусть  $R(x, y)$  — это отношение, задающее  $NP$ -трудную задачу  $S$  (например, для  $S = SAT$ :  $R(\phi, a) = 1 \iff \phi(a) = 1$ ). Пусть  $f_n(x, y) = (x, R(x, y))$ . Если  $f_n^{-1}$  вычисляется за полиномиальное время, то и задачу  $S$  можно решить за полиномиальное время, вычислив  $f^{-1}(x, 1)$ .

□

## 2.2. Односторонние функции для алгоритмов

Мы будем определять *односторонние функции* (one-way function, owf) для противника, который является вероятностным полиномиальным алгоритмом, т.е. для *равномерного противника*.

**Определение 2.3.** Полиномиально вычислимое семейство  $f_n$  называется *слабо односторонним для равномерного противника*, если **существует** такой полином  $p$ , что для любого полиномиального вероятностного алгоритма  $R$  при всех достаточно больших  $n$

$$\Pr_{x,R}[f_n(R(1^n, f_n(x))) = f_n(x)] < 1 - \frac{1}{p(n)}.$$

**Определение 2.4.** Полиномиально вычислимое семейство  $f_n$  называется *сильно односторонним для равномерного противника*, если **для любого** полинома  $q$ , что для любого полиномиального вероятностного алгоритма  $R$  при всех достаточно больших  $n$

$$\Pr_{x,R}[f_n(R(1^n, f_n(x))) = f_n(x)] < \frac{1}{q(n)}.$$

## 2.3. Односторонние функции для неравномерного противника

Аналогичным образом можно определить односторонние функции для противника, являющегося последовательностью схем, т.е. для *неравномерного противника*.

**Определение 2.5.** Полиномиально вычислимое семейство  $f_n$  называется *слабо односторонним для неравномерного противника*, если **существует** такой полином  $p$ , что для любой последовательности схем  $C_n$  полиномиального размера при всех достаточно больших  $n$

$$\Pr_x[f_n(x) = f_n(C_n(f_n(x)))] < 1 - \frac{1}{p(n)}.$$

**Определение 2.6.** Полиномиально вычислимое семейство  $f_n$  называется *сильно односторонним для неравномерного противника*, если **для любого** полинома  $q$ , что для любой последовательности схем  $C_n$  полиномиального размера при всех достаточно больших  $n$

$$\Pr_x[f_n(x) = f_n(C_n(f_n(x)))] < \frac{1}{q(n)}.$$

*Замечание 2.1.* Односторонние функции для неравномерного противника можно было бы определять для *вероятностных* схем, т.е. для схем, которым на вход подаются не только  $f_n(x)$ , но и некоторую строку со случайными битами  $r$ . Однако, легко показать, что от случайных битов в таких определениях можно избавиться: для этого нужно для каждого  $n$  выбрать одну “самую лучшую” строку  $r_n$ , на которой достигается максимальная вероятность обращения  $f_n$  и “зашить” её в схему. Нетрудно увидеть, что вероятность обращения при  $r = r_n$  будет не меньше, чем по всем  $r$  в среднем.

В дальнейшем мы часто будем говорить про односторонние *функции*, подразумевая под этим *семейства* односторонних функций. Когда говорят про *одностороннюю функцию*, то имеется в виду сильно односторонняя функция.

**Определение 2.7.** Если в определении односторонней функции убрать требование полиномиальной вычислимости, то получится определение *необратимой* функции.

## 2.4. Примеры односторонних функций

Неизвестно, существуют ли односторонние или хотя бы слабо односторонние функции (даже для равномерного противника). Доказательство их существования повлечёт за собой  $P \neq NP$ .

**Теорема 2.2.** Если  $P = NP$ , то любое полиномиально вычислимое семейство функций  $f_n$  не является слабо необратимым даже для равномерного противника. Более того, существует детерминированный алгоритм, который для всех  $x$  по  $n$  и  $f_n(x)$  за полиномиальное от  $n$  время находит некоторый прообраз  $f_n(x)$  длины  $k(n)$ .

*Доказательство.* См. пункт “ $\Rightarrow$ ” доказательства теоремы 2.1. □

*Пример 2.1* (произведение натуральных чисел). Семейство  $f_n$  устроено следующим образом:  $k(n) = l(n) = 2n$ , вход  $x$  делится пополам, каждая половинка представляет собой  $n$ -битовое число, результат  $f_n$  — произведение этих чисел (получится не более чем  $2n$ -битовое число).

*Пример 2.2* (SUBSET-SUM). Семейство  $f_n$  для SUBSET-SUM устроено следующим образом:  $k(n) = n^2 + n$ ,  $l(n) = n^2 + 2n + \lceil \log n \rceil$ , вход  $x$  разбивается на  $n + 1$  блок длины  $n$ , первые  $n$  блоков интерпретируются как  $n$ -битовые числа  $x_1, \dots, x_n$ , а последний блок интерпретируется как подмножество  $[n]$ . Тогда  $f_n(x) = \langle x_1, x_2, \dots, x_n, \sum_{i \in I} x_i \rangle$ .

## 2.5. Построение сильно односторонних функций из слабо односторонних

**Теорема 2.3.** *Если существуют слабо односторонние функции, то существуют и сильно односторонние функции (это верно для любых противников).*

*Доказательство.* Будем доказывать для равномерного противника — для неравномерного доказательство будет аналогичным. Пусть  $f$  — слабо односторонняя функция, т.е. существует такой полином  $p$ , что для любого полиномиального вероятностного алгоритма  $R$  при всех достаточно больших  $n$

$$\Pr_{x,r}[f_n(x) = f_n(R(1^n, f_n(x), r))] < 1 - \frac{1}{p(n)}.$$

Определим функцию  $F$ , которая определяется следующим соотношением:

$$F_n(x_1, x_2, \dots, x_N) = \langle f_n(x_1), f_n(x_2), \dots, f_n(x_N) \rangle,$$

т.е.  $F_n : \{0, 1\}^{N \cdot k(n)} \rightarrow \{0, 1\}^{N \cdot l(n)}$ . Для того, чтобы обратить  $F_n$  нам нужно  $N$  раз обратить функцию  $f_n$ . В каждом случае вероятность ошибки не меньше  $1/p(n)$ , поэтому общая вероятность успеха не более  $(1 - 1/p(n))^N$ . Для  $N = n \cdot p(n)$  эта вероятность близка к  $e^{-n}$ , что убывает быстрее любого обратного полинома. Таким образом функция  $F$  — сильно односторонняя.

В предыдущем рассуждении кроется ошибка. Дело в том, что мы предполагаем, что обращающий алгоритм будет обязательно устроен следующим образом: он будет пытаться  $N$  раз обратить  $f_n$ , т.е. найти прообразы для  $f_n(x_1), f_n(x_2), \dots, f_n(x_N)$ . Это не обязательно так — мы не можем предполагать, что этот алгоритм будет устроен каким-то конкретным образом. Поэтому предыдущее доказательство ошибочное, хотя получившаяся функция  $F$  действительно сильно односторонняя.

Корректное доказательство этого факта будет устроено другим образом. Мы предположим, что функция  $F$  не является сильно односторонней и из этого покажем, что в свою очередь функция  $f$  не является слабо односторонней. Для этого мы воспользуемся алгоритмом, который обращает  $F$ , для построения алгоритма обращения  $f$ . Предположим, что алгоритм  $R_F$  умеет обращать  $F$  с вероятностью успеха более  $1/q(n)$  для некоторого полинома  $q$ . Тогда мы покажем, что существует алгоритм  $R_f$ , который обращает  $f$  с вероятностью успеха более  $1 - 1/p(n)$ .

Алгоритм  $R_f$  мог бы быть устроен так: для обращения  $y$  мы выберем случайные  $x_2, x_3, \dots, x_N$  и запустим алгоритм  $R_F$  на входе  $\langle y, f_n(x_2), f_n(x_3), \dots, f_n(x_N) \rangle$ . Действительно, если  $R_F$  найдёт прообраз для этого входа, то он в т.ч. найдёт и прообраз для  $y$ . Вероятность успеха  $R_F$  на таком входе для случайного  $y$  не менее вероятности успеха  $R_F$  для случайных  $x_1, \dots, x_N$ . Однако нам этого недостаточно — мы хотели бы получить вероятность успеха близкую к единице.

Для этого будем использовать два дополнительных приёма:

- будем пытаться подставить  $y$  не только на место  $f_n(x_1)$ , а для каждого  $i$  будем запускать алгоритм  $R_F$  на входе  $\langle f_n(x_1), \dots, f_n(x_{i-1}), y, f_n(x_{i+1}), \dots, f_n(x_N) \rangle$  для случайных  $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_N$ ;<sup>1</sup>
- будем повторять каждую итерацию  $M$  раз для различных случайных независимых наборов  $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_N$ .

<sup>1</sup>Этот приём необходим, т.к. в противном случае у нас не получится увеличивать вероятность успеха. Действительно, если представить, что алгоритм  $R_F$  не работает на строках, у которых первый бит нулевой, то вероятность успеха такого алгоритма вполне может быть  $1/2$ . Но тогда и вероятность успеха  $R_f$  не может быть выше  $1/2$ .

Давайте выделим один раунд алгоритма  $R_f$ : для каждого  $i$  выбирается независимый случайный набор входов  $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_N$  и вызывается алгоритм  $R_f$  на входе  $\langle f_n(x_1), \dots, f_n(x_{i-1}), y, f_n(x_{i+1}), \dots, f_n(x_N) \rangle$ . Этот этап будет повторён  $M$  раз. Значение  $M$  мы выберем позже, это будут некоторый полином от  $n$ .

Через  $s_i(x)$  мы будем обозначать вероятность того, что алгоритм  $R_f$  найдёт прообраз  $\langle f_n(x_1), \dots, f_n(x_{i-1}), f_n(x), f_n(x_{i+1}), \dots, f_n(x_N) \rangle$  для случайных  $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_N$ . Через  $\hat{s}(x)$  обозначим вероятность успеха одного раунда алгоритма  $R_f$ . Эта вероятность заведомо не меньше максимальной вероятности среди всех  $s_i(x)$ , т.е.  $\hat{s}(x) \geq \max_i s_i(x)$ .

Рассмотрим отдельно входы  $x$ , которые наш алгоритм  $R_f$  обращает с маленькой вероятностью, т.е. это “трудные” для обращения входы. Будем говорить, что  $x$  — трудный, если  $\hat{s}(x) < \epsilon$  для некоторого обратного полинома  $\epsilon$ , который мы выберем дальше. Долю трудных “трудных” слов среди всех слов длины  $n$  мы обозначим через  $\delta$ , т.е.  $\delta = \Pr_{x \leftarrow U_n}[\hat{s}(x) < \epsilon]$ .

Дальнейшее доказательство будет построено так: мы предположим, что получившийся алгоритм  $R_f$  не обращает функцию  $f$  с нужной вероятностью, т.е. вероятность его ошибки больше  $1/p(n)$ . Из этого будет следовать, что доля трудных слов  $\delta$  довольно большая (больше некоторого обратного полинома). А раз трудных слов много, то и вероятность успеха  $R_f$  не может быть больше  $1/q(n)$ . Таким образом мы придём к противоречию. Для реализации этого плана потребуются следующие две леммы.

**Лемма 2.1.** *Вероятность ошибки  $R_f$  при обращении слова  $f_n(x)$  для случайного  $x$  не больше  $\delta + (1 - \epsilon)^M$ .*

*Доказательство.* По формуле полной вероятности вероятность ошибки  $R_f$  при обращении слова  $f_n(x)$  для случайного  $x$  можно расписать как вероятность ошибки на “трудных” входах и на простых входах.

$$\begin{aligned} \Pr_{x,r}[\text{ошибка } R_f] &= \Pr_r[\text{ошибка } R_f \mid \hat{s}(x) < \epsilon] \cdot \Pr_x[\hat{s}(x) < \epsilon] \\ &\quad + \Pr_r[\text{ошибка } R_f \mid \hat{s}(x) \geq \epsilon] \cdot \Pr_x[\hat{s}(x) \geq \epsilon] \\ &\leq 1 \cdot \delta + (1 - \epsilon)^M \cdot 1. \end{aligned}$$

□

**Лемма 2.2.** *Вероятность успеха алгоритма  $R_F$  при обращении слова  $F(\bar{x})$  для случайного  $\bar{x} = x_1, \dots, x_N$  не больше  $N\delta\epsilon + (1 - \delta)^N$ .*

*Доказательство.* Оценим вероятность успеха сверху по формуле полной вероятности:

$$\begin{aligned} \Pr_{\bar{x},r}[\text{успех } R_F] &= \Pr_r[\text{успех } R_F \mid \exists i, \hat{s}(x_i) < \epsilon] \cdot \Pr_{\bar{x}}[\exists i, \hat{s}(x_i) < \epsilon] \\ &\quad + \Pr_r[\text{успех } R_F \mid \forall i, \hat{s}(x_i) \geq \epsilon] \cdot \Pr_{\bar{x}}[\forall i, \hat{s}(x_i) \geq \epsilon] \\ &\leq \epsilon \cdot N\delta + 1 \cdot (1 - \delta)^N. \end{aligned}$$

□

Предположим теперь, что у получившегося алгоритма  $R_f$  вероятность ошибки больше, чем  $1/p(n)$ , т.е.  $R_f$  обращает  $f$  с вероятностью успеха меньше  $1 - \frac{1}{p(n)}$ . Положим  $M = n/\epsilon$ . Тогда второе слагаемое в лемме 2.1 будет порядка  $e^{-n}$ , что при достаточно больших  $n$  меньше, чем  $\frac{1}{2p(n)}$ . Таким образом  $\delta > \frac{1}{2p(n)}$ .

Теперь мы хотим определить  $N$  и  $\epsilon$  так, чтобы вероятность успеха  $R_F$  оказалась меньше, чем  $1/q(n)$ . Выберем  $N = n \cdot p(n)$ , тогда при  $\delta > \frac{1}{2p(n)}$  мы получаем, что второе слагаемое в лемме 2.2 будет порядка  $e^{-n/2}$ :

$$(1 - \delta)^N < \left(1 - \frac{1}{2p(n)}\right)^{n \cdot p(n)} = \left[\left(1 - \frac{1}{2p(n)}\right)^{2p(n)}\right]^{n/2} \approx e^{-n/2}.$$

При достаточно больших  $n$  это меньше, чем  $\frac{1}{2q(n)}$ . Осталось определить  $\epsilon$  так, чтобы и первое слагаемое лемме 2.2 было меньше  $\frac{1}{2q(n)}$ . Например, это достигается при

$$\epsilon = \frac{1}{2N \cdot q(n)} = \frac{1}{2n \cdot p(n) \cdot q(n)}.$$

При таких  $M$ ,  $N$  и  $\epsilon$  получается, что алгоритм  $R_f$  вызовет полиномиальный алгоритм  $R_F$  не более  $M \cdot N = 2n^3 \cdot p^2(n) \cdot q(n)$  раз, т.е.  $R_f$  сам по себе будет полиномиальным.  $\square$

## 2.6. Частичные односторонние функции

Односторонние функции, которые мы определили выше, определены для всех слов длины  $k(n)$ . Можно обобщить это определение на случай частичных функций, которые определены на некотором  $D_n \subset \{0, 1\}^{k(n)}$ . Для того, чтобы такие функции можно было применять для построения криптографических протоколов, мы дополнительно потребуем возможности генерировать *почти* равномерное распределение на  $D_n$ .

**Определение 2.8.** Последовательность распределений вероятностей  $\mu_n$  на множестве двоичных слов называется *полиномиально моделируемой*, если существует полиномиальный вероятностный алгоритм  $K$ , такой, что для всех  $x \in \{0, 1\}^*$

$$\Pr_r[K(1^n, r) = x] = \mu_n(x).$$

**Определение 2.9.** *Статистическим расстоянием* между распределениями вероятностей  $\mu$  и  $\nu$  называется

$$\delta(\mu, \nu) = \max_{A \subset \{0, 1\}^*} |\mu(A) - \nu(A)|.$$

Не сложно показать, что максимум достигается при  $A$  равном  $\{x \mid \mu(x) > \nu(x)\}$  и его дополнению. Таким образом

$$\delta(\mu, \nu) = \frac{1}{2} \sum_x |\mu(x) - \nu(x)|.$$

**Определение 2.10.** Последовательности распределений  $\mu_n$  и  $\nu_n$  называются *статистически неотличимыми*, если статистическое расстояние между ними стремится к нулю быстрее любого обратного полинома от  $n$  при  $n \rightarrow \infty$ .

**Определение 2.11.** Случайные величины  $\alpha_n$  и  $\beta_n$  называются *статистически неотличимыми*, если их распределения  $\mu_n(x) = \Pr[\alpha_n = x]$  и  $\nu_n(x) = \Pr[\beta_n = x]$  статистически неотличимы.

**Определение 2.12.** Распределение  $\mu_n$  называется *доступным*, если оно статистически неотлично от некоторого полиномиально моделируемого распределения  $\nu_n$ .

**Определение 2.13.** Семейство частичных функций  $f_n$  с областями определения  $D_n$  называется *сильно односторонним*, если  $f_n$  полиномиально вычислимо, равномерное распределение на  $D_n$  доступно, и для любого полинома  $q$  и для любого полиномиального вероятностного алгоритма  $R$ ,

$$\Pr_{x \leftarrow D_n, r} [f_n(x) = f_n(R(1^n, f_n(x), r))] < \frac{1}{q(n)}$$

при всех достаточно больших  $n$ . Сильно одностороннее семейство частичных функций  $f_n$  называется *сильно односторонней перестановкой* (one-way permutation, owp), если для всех  $n$  оно является перестановкой своей области определения  $D_n$ .

Аналогичным образом определяются *слабо односторонние функции* и *односторонние функции* для неравномерного противника.

*Пример 2.3* (Предположительно сильно односторонние частичные функции).

1. *Функция Рабина.* Функция  $f_n$  определена на словах вида  $xy$  длины  $4n$ , где  $|x| = |y| = 2n$ . При этом  $x$  и  $y$  интерпретируются как  $2n$ -битовые числа, удовлетворяющих следующим требованиям:

- (a)  $y = p \cdot q$ , где  $p$  и  $q$  простые  $n$ -битовые числа вида  $4k + 3$ ;
- (b)  $x = z^2 \pmod{y}$  для некоторого  $z$ , взаимно простого с  $y$ .

Значение функции на  $xy$  равно конкатенации слов  $x^2 \pmod{y}$  и  $y$ .

2. *Функция RSA.* Функция RSA является обобщением функции Рабина. Она определена на словах вида  $xuz$ , где  $x$ ,  $u$  и  $z$  имеют длину  $2n$  и интерпретируются как двоичные записи чисел, удовлетворяющие следующим требованиям:

- (a)  $y = p \cdot q$ , где  $p$  и  $q$  простые  $n$ -битовые числа;
- (b)  $x \in [1, pq - 1]$  и взаимно просто с  $y$ ;
- (c)  $z$  взаимно просто  $\phi(pq) = (p - 1) \cdot (q - 1)$ .

Значение функции на  $xuz$  равно конкатенации слов  $(x^z \pmod{y})$ ,  $u$  и  $z$ .

3. *Дискретная экспонента.* Функция определена на словах вида  $xuz$ , где  $x$ ,  $u$  и  $z$  имеют длину  $n$  и соответствующие числа удовлетворяют следующим требованиям:

- (a)  $y$  —  $n$ -битовое простое число,
- (b)  $x \in [2, y - 1]$ , порождает всю мультипликативную группу вычетов по модулю  $y$  (т.е. любой ненулевой вычет является степенью  $x$ ),
- (c)  $z \in [1, y - 1]$ .

Значение функции на  $xuz$  равно конкатенации слов  $x$ ,  $u$  и  $(x^z \pmod{y})$ . Обращение этой функции — является дискретным логарифмированием.

Более подробно об этих примерах см. [1].

**Определение 2.14.** Частичная функция  $f_n : \{0, 1\}^{k(n)} \rightarrow \{0, 1\}^{l(n)}$  называется *проверяемой*, если по  $n$ , любому слову  $x$  длины  $k(n)$  и любому слову  $y$  из множества значений  $f_n$  можно за полиномиальное время проверить, верно ли, что  $f_n$  определена на  $x$  и её значение на  $x$  равно  $y$ .

*Замечание 2.2.* Неизвестно, является ли функция Рабина проверяемой, т.к. неясно, как за полиномиальное время проверить, является ли данное число квадратичным вычетом по составному модулю.



### 3. Генераторы псевдослучайных чисел

#### 3.1. Вычислительно неотличимые случайные величины

**Определение 3.1** (Для неравномерного противника). Случайные величины  $\alpha_n$  и  $\beta_n$ , зависящие от натурального параметра  $n$ , со значениями в множестве слов некоторой длины  $l(n)$  называются *вычислительно неотличимыми*, если для любой последовательности схем  $C_0, C_1, \dots, C_n, \dots$  размера  $\text{poly}(n)$  (с  $l(n)$  входами и одним выходом) вероятность событий  $C_n(\alpha_n) = 1$  и  $C_n(\beta_n) = 1$  отличаются на пренебрежимо малую величину, т.е.

$$|\Pr[C_n(\alpha_n) = 1] - \Pr[C_n(\beta_n) = 1]| < \epsilon_n,$$

где  $\epsilon_n$  убывает быстрее любого обратного полинома. Схема  $C_n$  в этом контексте называется *тестом* и мы говорим, что случайная величина  $\alpha_n$  проходит тест  $C_n$ , если  $C_n(\alpha_n) = 1$ . Таким образом, мы требуем, чтобы  $\alpha_n$  и  $\beta_n$  проходили любые тесты полиномиального размера с приблизительно равной вероятностью.

**Определение 3.2** (Для равномерного противника). Случайные величины  $\alpha_n$  и  $\beta_n$ , зависящие от натурального параметра  $n$ , со значениями в множестве слов некоторой длины  $l(n)$  называются *вычислительно неотличимыми*, если для любого вероятностного полиномиального алгоритма  $T$  вероятность событий  $T(1^n, \alpha_n) = 1$  и  $T(1^n, \beta_n) = 1$  отличаются на пренебрежимо малую величину, соответственно

$$|\Pr[T(1^n, \alpha_n) = 1] - \Pr[T(1^n, \beta_n) = 1]| < \epsilon_n,$$

где  $\epsilon_n$  убывает быстрее любого обратного полинома. Алгоритм  $T$  в этом контексте называется *тестом* и мы говорим, что случайная величина  $\alpha_n$  проходит тест  $T$ , если  $T(1^n, \alpha_n) = 1$ .

*Замечание 3.1.* Если  $\alpha_n$  и  $\beta_n$  статистически неотличимы, то они и вычислительно неотличимы (например, для неравномерного противника), поскольку разность вероятностей  $\alpha_n$  и  $\beta_n$  в множество  $\{x \mid C_n(x)\}$ , задаваемое тестом  $C_n$ , не превосходит статистического расстояния между  $\alpha_n$  и  $\beta_n$ .

**Лемма 3.1** (Свойства вычислительной неотличимости).

1. Отношение вычислительной неотличимости рефлексивно, симметрично и транзитивно.
2. Для неравномерного противника: вычислительно неотличимые последовательности случайных величин  $\alpha_n$  и  $\beta_n$  вычислительно неотличимы и вероятностными тестами полиномиального размера. Это означает, что для любой последовательности  $T_n$  вероятностных схем полиномиального от  $n$  размера с  $l(n)$  входами, вероятности событий  $T_n(\alpha_n) = 1$  и  $T_n(\beta_n) = 1$  приблизительно равны.
3. Если  $\alpha_n$  и  $\beta_n$  вычислительно неотличимы, а  $C_n$  — последовательность вероятностных схем полиномиального размера с  $l(n)$  входами, то и случайные величины  $C_n(\alpha_n)$  и  $C_n(\beta_n)$  вычислительно неотличимы. Аналогично для равномерного противника.
4. Пусть случайные величины  $\alpha_n$ ,  $\beta_n$  и  $\gamma_n$  имеют совместное распределение. И пусть для любой последовательности значений  $c_n$  случайной величины  $\gamma_n$  случайные величины  $(\alpha_n \mid \gamma_n = c_n)$  и  $(\beta_n \mid \gamma_n = c_n)$  вычислительно неотличимы. Тогда и  $\alpha_n \gamma_n$  и  $\beta_n \gamma_n$  вычислительно неотличимы.

Для равномерного противника это свойство справедливо только для независимых случайных величин  $\alpha_n$ ,  $\gamma_n$ , причём случайная величина  $\gamma_n$  должна быть полиномиально моделируемой.

*Доказательство.*

1-2. Очевидно.

3. Пусть дана последовательность тестов  $T_n$  позволяет отличать  $C_n(\alpha_n)$  и  $C_n(\beta_n)$ . Тогда последовательность схем  $D_n(x) = T_n(C_n(x))$  будет вероятностным тестом полиномиального размера для случайных величин  $\alpha_n$  и  $\beta_n$ .
4. Допустим, что существует последовательность схем-тестов  $T_n$  полиномиального размера такая, что вероятность  $T_n(\alpha_n \gamma_n) = 1$   $T_n(\beta_n \gamma_n) = 1$  отличается  $\epsilon = 1/\text{poly}(n)$  для бесконечно многих  $n$ . Разность вероятностей событий  $T_n(\alpha_n \gamma_n) = 1$  и  $T_n(\beta_n \gamma_n) = 1$  равна среднему значению разности вероятностей

$$\Pr[T_n(\alpha_n c) \mid \gamma_n = c] - \Pr[T_n(\beta_n c) \mid \gamma_n = c]$$

по случайно выбранному  $c$  (в соответствии с распределением случайной величины  $\gamma_n$ ). Поэтому для бесконечно многих  $n$  найдётся  $c = c_n$  в множестве значений  $\gamma_n$ , для которой разность вероятности не меньше  $\epsilon$ . Если “защитить”  $c_n$  в схему  $T_n$ , то получится полиномиальный тест, различающий  $(\alpha_n \mid \gamma_n = c_n)$  и  $(\beta_n \mid \gamma_n = c_n)$ .

□

### 3.2. Генераторы псевдослучайных чисел

**Определение 3.3.** Пусть даны многочлены  $k(n)$  и  $l(n)$  такие, что  $l(n) > k(n)$  для всех  $n$ . Генератором псевдослучайных чисел типа  $k(n) \rightarrow l(n)$  будем называть семейство функций  $G_n : \{0, 1\}^{k(n)} \rightarrow \{0, 1\}^{l(n)}$ , удовлетворяющее следующим условиям.

1. Семейство  $G_n$  вычислимо за полиномиальное от  $n$  время.
2. (Надежность генератора ПСЧ.) Случайная величина  $G_n(s)$  для равномерного случайного  $s$  вычислительно неотличима от случайной величины равномерно распределенной на всех словах длины  $l(n)$ .

**Определение 3.4.** Генератор псевдослучайных чисел типа  $k(n) \rightarrow \infty$  будем называть семейство отображений  $G_n : \{0, 1\}^{k(n)} \rightarrow \{0, 1\}^*$ , удовлетворяющее следующим требованиям.

1. Существует алгоритм, который по слову  $s$  и натуральному числу  $l$  вычисляет элемент последовательности  $G_n(s)$  с номером  $l$  за время, полиномиальное от  $|s| + l$ .
2. Случайная величина  $G_n(s)$  вычислительно неотличима от равномерно распределённой бесконечной последовательности нулей и единиц. (Это означает, что для любого полинома  $p(n)$  первые  $p(n)$  битов  $G_n(s)$  вычислительно неотличимы от случайной величины равномерно распределённой на всех словах длины  $p(n)$ .)

*Замечание 3.2.* По генератору ПСЧ типа  $k(n) \rightarrow \infty$  можно построить генератор ПСЧ типа  $k(n) \rightarrow l(n)$  для любого полинома  $l(n)$  (нужно взять первый  $l(n)$  битов).

**Теорема 3.1.** Если существует генератор ПСЧ  $G_n$  типа  $k(n) \rightarrow l(n)$ , то существуют и односторонние функции.

*Доказательство.* Действительно, можно рассмотреть сам генератор  $G_n$  как слабо одностороннюю функцию. Давайте покажем, что никакая последовательность схем полиномиального размера  $C_n$  не обращает  $G_n$  с вероятностью успеха более  $3/4$  для бесконечно многих  $n$ . Предположим, что такая последовательность существует. Тогда можно рассмотреть следующий полиномиальный тест для последовательностей длины  $l(n)$ : для входа  $y$  проверяем, что  $G_n(C_n(y)) = y$ . Если это верно (т.е. обращение произошло удачно), то выдаём 1, а иначе 0. Вероятность того, что  $G_n$  пройдёт такой тест не менее  $3/4$ . При этом равномерно распределённая на  $l(n)$  случайная величина пройдёт этот тест с вероятностью не более  $1/2$  (т.к. размер образа  $G_n$  не более  $1/2$ ).  $\square$

Обратное утверждение тоже верно.

**Теорема 3.2** ([4]). *Если существует односторонняя функция, то существует и генератор псевдослучайных чисел типа  $n \rightarrow \infty$ .*

Мы же докажем более простое утверждение.

**Теорема 3.3.** *Если существует односторонняя перестановка, то существует и генератор псевдослучайных чисел типа  $n \rightarrow \infty$ .*

В дальнейшем мы будем говорить про *полиномиального противника* подразумевая под этим две возможных формулировки: полиномиальный вероятностный алгоритм и семейство схем полиномиального размера.

### 3.3. Трудный бит

**Определение 3.5.** Для пары совместно распределённых случайных величин  $(\beta_n, \gamma_n)$ , где  $\beta_n$  распределена на  $\{0, 1\}$  будем говорить, что  $\beta_n$  является *вычислительно трудной* относительно  $\gamma_n$ , если для любого полиномиального противника  $B$

$$|\Pr[B(\gamma_n) = \beta_n] - \frac{1}{2}| < \frac{1}{p(n)}$$

для любого полинома  $p$  для достаточно больших  $n$ .

**Теорема 3.4.** *Случайная величина  $\beta_n$  вычислительно трудна относительно  $\gamma_n$  тогда и только тогда, когда случайная величина  $\beta_n \gamma_n$  вычислительно неотличима от  $r_n \gamma_n$ , где  $r_n$  — это равномерно распределённая на  $\{0, 1\}$  случайная величина.*

*Доказательство.*

$\Leftarrow$  Пусть существует противник  $B$ , который для бесконечного числа  $n$  предсказывает  $\beta_n$  по  $\gamma_n$  с хорошей вероятностью, т.е.

$$\Pr[B(\gamma_n) = \beta_n] \geq \frac{1}{2} + \epsilon_n,$$

где  $\epsilon_n$  — обратный полином. Используя противника  $B$  построим противника  $A$ , который различает  $\beta_n \gamma_n$  и  $r_n \gamma_n$ .

$$A(x, y) = \begin{cases} 1, & B(y) = x, \\ 0, & B(y) \neq x. \end{cases}$$

Тогда  $\Pr[A(\beta_n \gamma_n) = 1] \geq \frac{1}{2} + \epsilon_n$ , а  $\Pr[A(r_n \gamma_n) = 1] = \frac{1}{2}$ .

⇒ Пусть существует противник  $A$ , который для бесконечного числа  $n$  различает  $\beta_n \gamma_n$  и  $r_n \gamma_n$  с хорошей вероятностью, т.е.

$$\Pr[A(\beta_n \gamma_n) = 1] - \Pr[A(r_n \gamma_n) = 1] \geq \epsilon_n,$$

где  $\epsilon_n$  — обратный полином. Построим противника  $B$ , который предсказывает  $\beta_n$  по  $\gamma_n$ .

$$B(x) = \begin{cases} r, & A(0x) = 0, A(1x) = 0, \\ 1, & A(0x) = 0, A(1x) = 1, \\ 0, & A(0x) = 1, A(1x) = 0, \\ r, & A(0x) = 1, A(1x) = 1, \end{cases}$$

где  $r$  означает случайный бит.

Покажем, что

$$\Pr[B(\gamma_n) = \beta_n] = \frac{1}{2} + \Pr[A(\beta_n \gamma_n) = 1] - \Pr[A(r_n \gamma_n) = 1] \geq \frac{1}{2} + \epsilon_n.$$

Давайте докажем это равенство для фиксированного  $\gamma_n = x$ :

$$\Pr[B(\gamma_n) = \beta_n \mid \gamma_n = x] = \frac{1}{2} + \Pr[A(\beta_n \gamma_n) = 1 \mid \gamma_n = x] - \Pr[A(r_n \gamma_n) = 1 \mid \gamma_n = x].$$

Отсюда по формуле полной вероятности получается требуемое равенство. Для того, чтобы убедиться, что это равенство верно, нужно подставить все четыре возможных варианта из определения  $B$  и проверить, что равенство выполняется. Например, в первом случае вероятность слева будет равна  $1/2$ , т.к.  $B$  возвращает случайный бит, а справа обе вероятности равны нулю. Для второго случая вероятность слева будет равна первой вероятности справа, а последняя  $= 1/2$ .

*Замечание 3.3.* В случае неравномерного противника данная конструкция даёт вероятностную схему, которую, как описано выше можно переделать в детерминированную. В случае равномерного противника нам потребовалось бы также фиксировать внутренние биты вероятностного алгоритма.

□

**Определение 3.6.** Для односторонней перестановки  $f_n : D_n \rightarrow D_n$ , где  $D_n \subset \{0, 1\}^{k(n)}$ , будем называть *трудным битом* такую полиномиально вычислимую функцию  $h_n : D_n \rightarrow \{0, 1\}$ , для которой случайная величина  $h_n(U(D_n))$  трудна для  $f_n(U(D_n))$ .

**Утверждение 3.1.** Пусть  $f_n : D_n \rightarrow D_n$  — односторонняя перестановка с трудным битом  $h_n : D_n \rightarrow \{0, 1\}$ . Тогда случайная величина  $h_n(x)f_n(x)$  вычислительно неотличима от  $rx$ , где  $x \leftarrow U(D_n)$ , а  $r \leftarrow U_1$ .

*Доказательство.* Заметим, что  $f_n(x)$  распределено так же, как  $x$  (важно, что  $f_n$  — перестановка). Поэтому  $rf_n(x)$  распределено так же, как  $rx$ . Осталось применить теорему 3.4 для  $rf_n(x)$  и  $h_n(x)f_n(x)$ . □

Эту конструкцию можно итерировать. Например,  $h_n(x)h_n(f_n(x))f_n(f_n(x))$  позволяет получить два бита. Заметим, что если случайная величина  $h_n(x)h_n(f_n(x))f_n(f_n(x))$  отличима от  $rh_n(f_n(x))f_n(f_n(x))$ , то отличимы  $h_n(x)f_n(x)$  и  $rf_n(x)$  (первые можно получить из вторых). Продолжая рассуждение получаем, что  $h_n(x)h_n(f_n(x))f_n(f_n(x))$  неотличима от  $rr'x$ , где  $r, r' \leftarrow U_1$ .

**Теорема 3.5.** Пусть  $f_n : D_n \rightarrow D_n$  — односторонняя перестановка с трудным битом  $h_n : D_n \rightarrow \{0, 1\}$ . Тогда случайная величина

$$h_n(x)h_n(f_n(x)) \dots h_n(f_n^{(p(n))})f_n^{(p(n)+1)}(x)$$

вычислительно неотличима от случайной величины

$$r_1 r_2 \dots r_{p(n)} x,$$

где  $r_1, \dots, r_{p(n)} \leftarrow U_1$ ,  $x \leftarrow U(D_n)$ .

**Следствие 3.1.**  $G_n(x) = h_n(x)h_n(f_n(x)) \dots h_n(f_n^{(p(n))})f_n^{(p(n)+1)}(x)$  является надёжным генератором псевдослучайных чисел.

*Доказательство.* Доказательство „гибридным“ методом.

$$\begin{array}{rcccccc} T_0 = & h_n(x) & h_n(f_n(x)) & \dots & h_n(f_n^{(p(n)-1)}) & f_n^{(p(n))}(x) \\ T_1 = & r_1 & h_n(x) & \dots & h_n(f_n^{(p(n)-2)}) & f_n^{(p(n)-1)}(x) \\ T_2 = & r_1 & r_2 & \dots & h_n(f_n^{(p(n)-3)}) & f_n^{(p(n)-2)}(x) \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ T_{p(n)} = & r_1 & r_2 & \dots & r_{p(n)} & x \end{array}$$

Пусть взломщик  $B$  отличает  $T_0$  от  $T_{p(n)}$ , т.е.  $\Pr[B(T_0) = 1] - \Pr[B(T_{p(n)}) = 1] \geq \epsilon_n$  для бесконечного числа  $n$  и обратного полинома  $\epsilon_n$ . Тогда существует такое  $i$ , что

$$\Pr[B(T_i) = 1] - \Pr[B(T_{i+1}) = 1] \geq \epsilon_n/p(n).$$

Т.е. мы научились отличать

$$\begin{array}{cccccc} r_1 & \dots & r_i & h_n(x) & h_n(f_n(x)) & \dots & h_n(f_n^{(p(n)-i-1)}) & f_n^{(p(n)-i)}(x) \\ r_1 & \dots & r_i & r_{i+1} & h_n(x) & \dots & h_n(f_n^{(p(n)-i-2)}) & f_n^{(p(n)-i-1)}(x) \end{array}$$

Используя противника, который отличает эти две случайные величины мы можем отличать  $h_n(f)h_n(x)$  от  $rx$  — по этим случайным величинам можно детерминированным алгоритмом построить соответствующие значения  $T_i$  и  $T_{i+1}$ , что противоречит утверждению 3.1.

*Замечание 3.4.* В этом доказательстве мы воспользовались тем, что наш у нас неравномерный противник, т.е. для схема, т.к. мы в эту схему зашили число  $i$ . В случае с алгоритмами можно взять случайное  $i$  и доказать, что с хорошей вероятностью оно подойдёт. □

**Теорема 3.6** (Голдрейх, Левин). Пусть  $f_n : D_n \rightarrow D_n$  — односторонняя перестановка,  $D_n \subseteq \{0, 1\}^{k(n)}$ . Рассмотрим две функции:  $g_n : D_n \times \{0, 1\}^{k(n)} \rightarrow D_n \times \{0, 1\}^{k(n)}$  и  $h_n : D_n \times \{0, 1\}^{k(n)} \rightarrow \{0, 1\}$ , такие что

$$g_n(xy) = f_n(x)y, \quad h_n(x, y) = x \odot y = \bigoplus_{i=1}^{k(n)} x_i y_i = \sum_{i=1}^{k(n)} x_i y_i \pmod{2}.$$

Тогда  $g_n$  — односторонняя перестановка с трудным битом  $h_n$ .

**Определение 3.7.** Код Уолша-Адамара — это код исправляющий ошибки  $WH : \{0, 1\}^k \rightarrow \{0, 1\}^{2^k}$ , определяющий следующим соотношением  $WH(x) = (x \odot y)_{y \in \{0, 1\}^k}$ .

Код Уолша-Адамара не очень удобен в практических применениях, т.к. он удлиняет строки в экспоненту раз. Однако он обладает одним очень хорошим свойством.

**Утверждение 3.2.** *Код Уолша-Адамара имеет расстояние  $2^{k-1}$ .*

*Доказательство.* Пусть  $x_i \neq y_i$ . Рассмотрим  $r$  и  $r^{\oplus i}$ , где  $r, r^{\oplus i} \in \{0, 1\}^k$  и отличаются только в бите  $i$ . Тогда либо  $x \odot r$  отличается от  $x \odot r^{\oplus i}$ , либо  $y \odot r$  отличается от  $y \odot r^{\oplus i}$ . Т.е. все  $\{0, 1\}^k$  можно разбить на пары, различающиеся в одном бите, то все пары строк имеют коды, отличающиеся ровно в половине всех битов.  $\square$

**Лемма 3.2.** *Пусть  $s \in \{0, 1\}^{2^m}$  и  $\Pr_i[s_i \neq WH(x)] \leq 1/2 - \epsilon$  (в терминах расстояния Хемминга  $\Delta(WH(x), s) \leq (1/2 - \epsilon)2^m$ ). Существует вероятностный алгоритм  $A^s$  со временем работы  $\text{poly}(m, \frac{1}{\epsilon})$ , который выдаёт список  $L$  слов длины  $m$  такой, что  $x \in L$  с вероятностью не менее  $1/2$  (алгоритм получает оракульный доступ к строке  $s$ ).*

*Доказательство теоремы Голдрейха-Левина.* Функция  $g_n$  является перестановкой. Легко показать, что если противник взламывает  $g_n$ , то он взламывает и  $f_n$ , т.е.  $g_n$  является односторонней перестановкой.

Теперь нужно показать, что  $h_n$  является трудным битом  $g_n$ . Пусть существует неравномерный противник  $B$  (в дальнейшем будем предполагать, что противник — это всегда семейство схем), который предсказывает  $h_n$ , т.е.

$$\Pr_{x \leftarrow U(D_n), y \leftarrow U_{k(n)}} [B(f(x)y) = x \odot y] \geq 1/2 + \epsilon_n$$

для бесконечного числа  $n$  и обратного полинома  $\epsilon_n$ . Построим противника  $C$ , который обращает  $f_n$ , т.е.

$$\Pr_{x \leftarrow U(D_n)} [C(f_n(x)) = x] \geq \epsilon_n/4.$$

Противник  $C$  будет использовать алгоритм декодирования списком кода Уолша-Адамара из леммы 3.2 и при обращении к биту  $y$  выдаём значение  $B(f(x)y)$ . В списке  $L$ , который возвращает алгоритм  $A$  ищем  $z$  такое, что  $f_n(z) = f_n(x)$ . Если такое  $z$  нашлось, то выдаём его, иначе выдаём любую строку.

Пусть  $M \subseteq D_n$  и  $x \in M \iff \Pr_{y \leftarrow U_{k(n)}} [B(f_n(x)y) = x \odot y] \geq 1/2 + \epsilon_n/2$ . Давайте покажем, что  $\Pr_{x \leftarrow U(D_n)} [x \in M] \geq \epsilon_n/2$ . Пусть это не так, тогда

$$\begin{aligned} \Pr_{x,y} [B(f_n(x)y) = x \odot y] &= \Pr_{x,y} [B(f_n(x)y) = x \odot y \mid x \in M] \cdot \Pr_x [x \in M] \\ &\quad + \Pr_{x,y} [B(f_n(x)y) = x \odot y \mid x \notin M] \cdot \Pr_x [x \notin M] \\ &< 1 \cdot \epsilon_n/2 + (1/2 + \epsilon_n/2) \cdot 1 < 1/2 + \epsilon_n. \end{aligned}$$

Заметим, что  $\Pr_x [C(f_n(x)) = x \mid x \in M] \geq 1/2$ , т.к. с вероятностью не менее  $1/2$  в списке будет искомый элемент. Поэтому получаем

$$\Pr_x [C(f_n(x)) = x] \geq \Pr_x [C(f_n(x)) = x \mid x \in M] \cdot \Pr_x [x \in M] \geq \frac{1}{2} \cdot \frac{\epsilon_n}{2} = \frac{\epsilon_n}{4}.$$

$\square$

*Доказательство леммы 3.2.* Будем рассматривать код Уолша-Адамара как таблицу истинности некоторой функции  $f : \{0, 1\}^m \rightarrow \{0, 1\}$ . Пусть  $WH(x)$  соответствует  $f$ , а кодовое

слово  $s$  — некоторой функции  $\tilde{f}$ . Таким образом для восстановления  $x$  нам нужно вычислить  $f$  на входах  $100 \dots 0, 010 \dots 0, 001 \dots 0, \dots$ . Действительно,

$$\begin{aligned} x_1 &= f(100 \dots 0) \\ x_2 &= f(010 \dots 0) \\ &\vdots \\ x_n &= f(000 \dots 1) \end{aligned}$$

Используя линейность  $f$  мы можем вычислять  $f(z)$  следующим образом: выберем случайный  $r$  и вычислим  $f(z) = f(r) \oplus f(z \oplus r)$ . Проблема в том, что доступа к  $f$  у нас нет, а есть доступ к  $\tilde{f}$ , про которую известно  $\Pr_y[f(y) \neq \tilde{f}(y)] \leq 1/2 - \epsilon$ . Используя идею с линейностью мы можем попробовать вычислять  $f(z) = \tilde{f}(r) \oplus \tilde{f}(z \oplus r)$  (добавление  $r$  позволяет вычислять  $\tilde{f}$  в случайной точке, в то время как значение  $\tilde{f}$  на строках вида  $00 \dots 010 \dots 00$  может быть неправильным). Если бы ошибка в  $\tilde{f}$  случалась с вероятностью менее  $1/4 - \epsilon$ , то суммарная ошибка при таком вычислении  $f(z)$  была бы не более  $1/2 - 2\epsilon$ . Тогда мы могли бы её амплифицировать и получить  $f(z)$  с хорошей вероятностью. Однако, ошибка в  $f$  случается с большей вероятностью.

**Идея.** Если бы у нас был доступ к истинному значению, то тогда бы тоже всё сработало  $f(z) = f(r) \oplus \tilde{f}(z \oplus r)$ . Предположим, что мы всё же умеем вычислять  $f(r)$  вместо  $\tilde{f}(r)$ . Тогда мы можем вычислить  $f(z)$  следующим образом: выберем случайные  $r_1, r_2, \dots, r_N$  и вычислим  $\text{maj}_i\{f(r_i) \oplus \tilde{f}(z \oplus r_i)\}$ . С хорошей вероятностью полученное значение будет совпадать с  $f(z)$ . Чтобы оценить это давайте вспомним следующий факт из теории вероятностей.

*Замечание 3.5.* Неравенство Чебышёва (закон больших чисел для 2-независимых случайных величин). Пусть  $X_1, X_2, \dots, X_N$  — одинаково распределённые попарно-независимые Бернулиевские случайные величины,  $\forall i, \Pr[X_i = 1] = p$ , тогда

$$\Pr \left[ \left| \frac{\sum_i X_i}{N} - p \right| \geq \delta \right] \leq \frac{1}{\delta^2 N}.$$

Для применения этого неравенства нам нужны попарно независимые случайные величины. Пусть  $N = 2^k - 1$ , конкретное значение для  $N$  мы определим позже. Выберем  $t_1, t_2, \dots, t_k \leftarrow U_m$  — независимые случайные строки. Из этих случайных строк можно сгенерировать  $N$  попарно независимых следующим образом:

$$\forall J \subseteq \{1, \dots, k\}, J \neq \emptyset, r_J = \bigoplus_{i \in J} t_i.$$

**Утверждение 3.3.** Если  $J_1 \neq J_2$ , то  $r_{J_1}$  и  $r_{J_2}$  будут независимыми.

**Следствие 3.2.**  $\{r_J\}_J$  — 2-независимые случайные величины.

Теперь опишем алгоритм декодирования кода Уолша-Адамара используя нашу идею с вычислением  $f(r)$ . Сгенерируем независимые  $t_1, t_2, \dots, t_k \leftarrow U_m$  и по ним определим  $r_J = \bigoplus_{i \in J} t_i, J \subseteq [n], J \neq \emptyset$ . Так как доступа к  $f$  у нас нет, то вычислить  $f(r)$  мы не можем. Вместо этого мы переберём все значения для  $f(r)$ . Если бы все  $r$  были независимы, то нам пришлось бы перебрать  $2^N$  различных значений. Однако, наши  $r$  получаются из  $k$  строк  $t_i$ . Поэтому достаточно перебрать значения  $f$  на  $t_i$ . Пусть  $\forall i, a_i = f(t_i)$ , тогда

$$f(r^J) = f\left(\bigoplus_{j \in J} t_j\right) = \bigoplus_{j \in J} f(t_j) = \bigoplus_{j \in J} a_j.$$

Таким образом, алгоритм декодирования для всех возможных  $a_1, \dots, a_k \in \{0, 1\}$  добавит в список  $L$  строку  $x_1, \dots, x_m$ , полученную по следующей процедуре:

$$x_i = \text{maj}_J \left\{ \bigoplus_{j \in J} a_j \oplus \tilde{f} \left( (0 \dots \underset{i}{1} \dots 0) \oplus r^J \right) \right\},$$

Для успеха  $x_i$  должен быть верен с вероятностью не менее  $1 - \frac{1}{10m}$  (тогда весь  $x$  мы угадаем с вероятностью  $\geq 9/10$ ). Определим случайные величины  $\{X_i^J\}$  такие, что

$$X_i^J = 1 \iff \tilde{f} \left( (0 \dots \underset{i}{1} \dots 0) \oplus r^J \right) = f \left( (0 \dots \underset{i}{1} \dots 0) \oplus r^J \right).$$

Пусть  $p = \Pr[X_i^J = 1] \geq 1/2 + \epsilon$ . По закону больших чисел вероятность того, что при вычислении  $\text{maj}$  мы получим более половины неправильных значений  $\tilde{f}$  не более  $\frac{1}{\epsilon^2 N}$ .

$$\begin{aligned} \Pr[x_i \text{ ошибочный}] &= \Pr \left[ \sum_J \frac{X_i^J}{N} \leq \frac{1}{2} \right] \\ &= \Pr \left[ \sum_J \frac{X_i^J}{N} - \left( \frac{1}{2} + \epsilon \right) \leq -\epsilon \right] \\ &\leq \Pr \left[ \left| \sum_J \frac{X_i^J}{N} - \left( \frac{1}{2} + \epsilon \right) \right| \geq \epsilon \right] \\ &\leq \Pr \left[ \left| \sum_J \frac{X_i^J}{N} - p \right| \geq \epsilon \right] \leq \frac{1}{\epsilon^2 N}. \end{aligned}$$

Таким образом, мы требуем, чтобы  $\frac{1}{\epsilon^2 N} \leq \frac{1}{10m}$ , следовательно  $N \geq \frac{10m}{\epsilon^2}$ .  $\square$

## 4. Протоколы с секретным ключом

**Определение 4.1.** Пусть дана доступная случайная величина  $d_n$ . *Одноразовый протокол с секретным ключом* задаётся двумя вероятностными полиномиальными алгоритмами  $E(d, x)$  и  $D(d, m)$ , такими, что  $D(d, E(d, x)) = x$ . Будем говорить, что этот протокол *надёжный*, если для некоторого полинома  $l$  и любых последовательный строк  $x_n$  и  $y_n$  длины  $l(n)$  случайные величины  $E(d_n, x_n)$  и  $E(d_n, y_n)$  вычислительно неотличимы.

Такой протокол мы уже можем построить. Возьмём генератор псевдослучайных чисел  $G : \{0, 1\}^n \rightarrow \{0, 1\}^{l(n)}$ . Возьмём  $d_n = U_n$  и для  $x \in \{0, 1\}^{l(n)}$  определим

$$\begin{aligned} E(d, x) &= G(d) \oplus x, \\ D(d, m) &= G(d) \oplus m. \end{aligned}$$

Если бы противник научился отличать случайные величины  $E(d_n, x_n)$  и  $E(d_n, y_n)$ , то он также научился бы отличать одну из этих случайных величин от равномерного распределения  $U_{l(n)}$ . Пусть он умеет отличать  $E(d_n, x_n)$  от  $U_{l(n)}$ . Тогда мы можем зашифровать  $x_n$  в схему и таким образом научиться отличать образ  $G(d_n)$  от  $U_{l(n)}$ .

**Определение 4.2.** Пусть  $S_n \subseteq \{0, 1\}^{l(n)}$  и для любого  $s \in S_n$  определена функция  $f_n^s : \{0, 1\}^n \rightarrow \{0, 1\}^n$ . Множество функций  $\{f_n^s\}_{s \in S_n}$  называется *семейством псевдослучайных функций*, если выполняются следующие свойства.

1. Существует полиномиальный алгоритм, который по  $(s, x)$  вычисляет  $f_n^s(x)$ .



2. Распределение  $U(S_n)$  доступно.

3. (*слабая надёжность*) Для любого полинома  $p$  и для любого набора различных строк  $t_1, \dots, t_{p(n)} \in \{0, 1\}^n$  случайная величина  $f_n^s(t_1)f_n^s(t_2) \cdots f_n^s(t_{p(n)})$  вычислительно неотличима от  $U_{np(n)}$ , где  $s \leftarrow U(S_n)$ .

3'. (*сильная надёжность*) Для любого полинома  $p$ , любого семейства схем полиномиального размера  $\{C_i\}_{i=1}^{p(n)-1}$  и любого  $t_1 \in \{0, 1\}^n$  определим случайные величины  $\{y_i\}_{i=1}^{p(n)}$  следующим образом:

$$\begin{aligned} s &\leftarrow U(S_n), \\ y_1 &= f_n^s(t_1), \\ t_2 &= C_1(t_1, y_1), \\ y_2 &= f_n^s(t_2), \\ t_3 &= C_2(t_1, y_1, y_2), \\ y_3 &= f_n^s(t_3), \\ &\vdots \end{aligned}$$

Тогда случайная величина  $y_1 y_2 \cdots y_{p(n)}$  вычислительно неотличима от  $U_{np(n)}$  (при условии, что все  $t_i$  различны).

**Теорема 4.1.** *Если существует генератор псевдослучайных чисел, то существует и семейство псевдослучайных функций.*

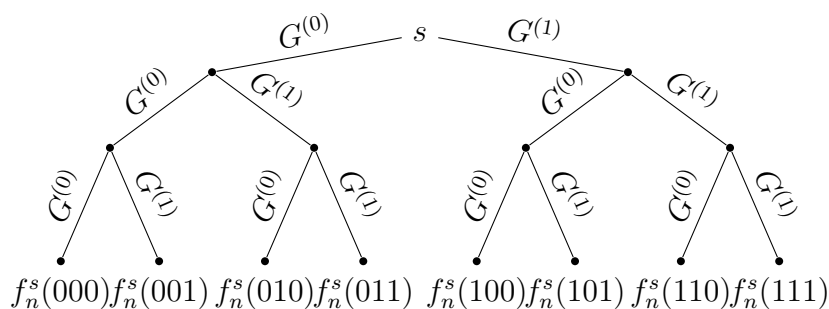
*Доказательство.* Пусть  $G_n : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$ . Мы построим семейство псевдослучайных функций  $\{f_n^s\}_{s \in S_n}$ , где  $S_n = \{0, 1\}^n$ ,  $f_n^s : \{0, 1\}^n \rightarrow \{0, 1\}^n$ . Для этого определим функции  $G_n^{(0)}, G_n^{(1)} : \{0, 1\}^n \rightarrow \{0, 1\}^n$  исходя из следующего соотношения:

$$G_n(r) = G_n^{(0)}(r) G_n^{(1)}(r).$$

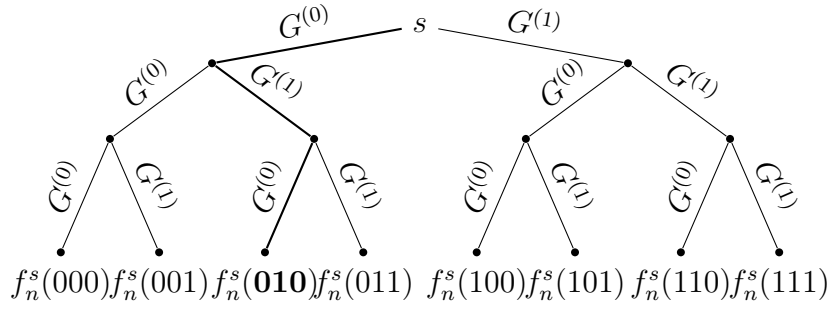
Тогда

$$f_n^s(x) = G_n^{(x_n)}(\cdots G_n^{(x_2)}(G_n^{(x_1)}(s)) \cdots).$$

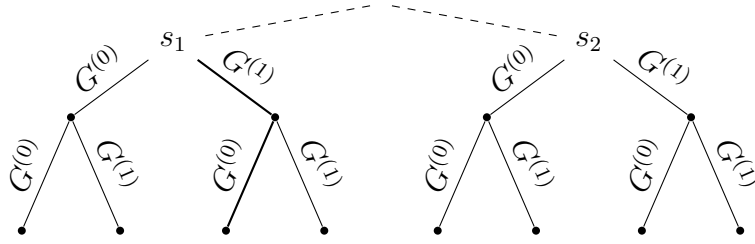
Можно представить вычисление  $f_n^s$  на всевозможных  $x$  в виде бинарного дерева: в корне записано число  $s$ ; если в вершине записано число  $z$ , то в его наследниках будут записаны  $G_n^{(0)}(z)$  и  $G_n^{(1)}(z)$ ; в листьях дерева будут все возможные  $f_n^s(x)$ .



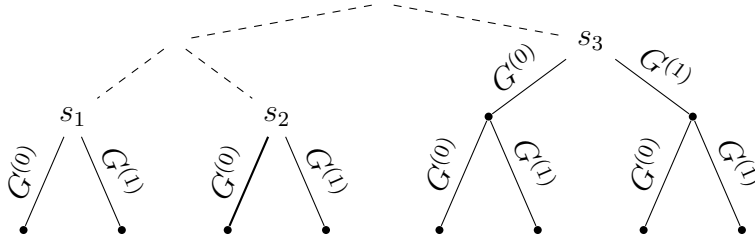
Будем доказывать гибридным методом. Для этого нам нужно построить последовательность распределений, которые постепенно сходятся к равномерному. Изначальное распределение задаёт дерево  $T_0$ , в корне которого выбирается  $s$ , а дальше вычисление происходит детерминировано. Каждое  $t_i$  задаёт некоторый путь от корня к листьям. Мы будем модифицировать исходное дерево следующим образом: для каждой вершины на пути соответствующему  $t_1$  мы будем удалять эту вершину из дерева и заменять её сыновей на случайные строки из  $U(S_n)$ .



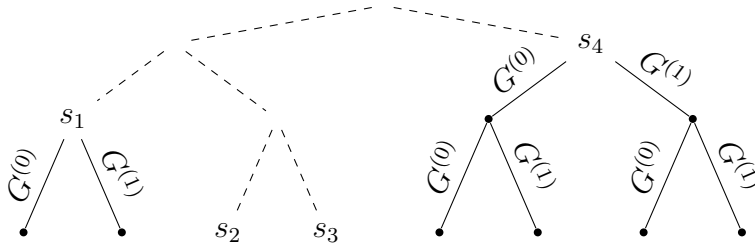
Для примера  $t_1 = 010$ .



Удаляем корневую вершину и заменяем её сыновей на  $s_1, s_2 \leftarrow U(S_n)$



Удаляем следующую вершину и заменяем сыновей на случайные элементы из  $U(S_n)$ .



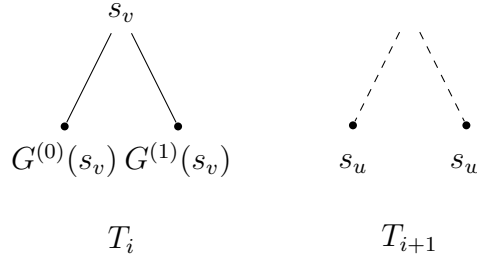
Удаляем последнюю вершину и заменяем сыновей на случайные элементы из  $U(S_n)$ .

В конце этого процесса в вершине, которая раньше соответствовала  $t_1$ , будет некоторый  $s_j \leftarrow U(S_n)$ . Мы повторим этот процесс для всех  $t_i$ . Таким образом получится последовательность из  $n \cdot p(n) + 1$  дерева, которые задают распределения  $\{T_i\}_{i=0}^{np(n)}$ . В последнем распределении  $T_{np(n)}$  значение для каждого  $f_n^s(t_i)$  выбирается из  $U(S_n)$ , т.е. это соответствует равномерному распределению.

Если существует противник, который отличает первое распределение от последнего, то существуют и два последовательных распределения, которые этот противник различает с хорошей вероятностью:

$$\Pr_{z \leftarrow T_0} [B(z) = 1] - \Pr_{z \leftarrow T_{np(n)}} [B(z) = 1] \geq \epsilon_n \implies \exists i : \Pr_{z \leftarrow T_i} [B(z) = 1] - \Pr_{z \leftarrow T_{i+1}} [B(z) = 1] \geq \frac{\epsilon_n}{np(n)}.$$

Дерево распределения  $T_{i+1}$  отличается от  $T_i$  в трёх вершинах:



Таким образом противник может отличить образ генератора  $G(s_v) = G^{(0)}(s_v)G^{(1)}(s_v)$  от полностью случайной строки  $s_us_w$  с вероятностью больше  $\epsilon_n/(n \cdot p(n))$ .  $\square$

*Замечание 4.1.* Это было доказательство надёжности в смысле п.3. То же самое доказательство работает и для п.3'.

**Определение 4.3.** Пусть  $d_n$  — доступная случайная величина  $d_n \in \{0, 1\}^{k(n)}$ . *Многоразовый протокол с секретным ключом* — это пара полиномиальных вероятностных алгоритмов  $E(d, x)$  и  $D(d, m)$  таких, что  $D(d, E(d, x)) = x$ , и выполняются следующее условие надёжности.

- а) (*слабая надёжность*) Для любых полиномов  $p$  и  $q$  и для любого набора сообщений  $x_1, \dots, x_{p(n)} \in \{0, 1\}^{q(n)}$  при  $d \leftarrow d_n$  случайные величины  $E(d, x_1) \cdots E(d, x_{p(n)})$  и  $E(d, 0^{q(n)}) \cdots E(d, 0^{q(n)})$  вычислительно неотличимы.
- б) (*сильная надёжность*) Для любых полиномов  $p$  и  $q$ , любого  $x_1 \in \{0, 1\}^{q(n)}$  и семейства полиномиальных схем  $\{C_i\}_{i=1}^{p(n)-1}$  определим  $\{x_i\}_{i=2}^{p(n)}$  следующим образом:

$$\begin{aligned}
d &\leftarrow d_n, \\
c_1 &= E(d, x_1), \\
x_2 &= C_1(x_1, c_1), \\
c_2 &= E(d, x_1), \\
x_3 &= C_2(x_1, c_1, c_2), \\
c_3 &= E(d, x_2), \\
x_4 &= C_3(x_1, c_1, c_2, c_3), \\
&\vdots \\
x_{p(n)} &= C_{p(n)-1}(x_1, c_1, \dots, c_{p(n)-1}), \\
c_{p(n)} &= E(d, x_{p(n)}).
\end{aligned}$$

Тогда получившаяся случайная величина  $c_1, \dots, c_{p(n)}$  вычислительно неотличима от случайной величины  $E(d, 0^{q(n)}) \cdots E(d, 0^{q(n)})$ .

**Теорема 4.2.** *Если существует семейство псевдослучайных функций, то существует и многоразовый протокол с секретным ключом.*

*Доказательство.* Докажем для сообщения из одного бита. Из этого будет следовать, что есть протокол для сообщения любой длины. Пусть  $f_s : \{0, 1\}^n \rightarrow \{0, 1\}$  — семейство псевдослучайных функций,  $s \in \{0, 1\}^n$ . Тогда  $d_n = U_n$ . Алгоритм шифрования  $E(d, m)$  для ключа  $d \leftarrow d_n$  и бита  $m \in \{0, 1\}$  выбирает  $z \leftarrow U_n$  и выдаёт  $(m \oplus f_d(z), z)$ . Алгоритм дешифровки  $D(d, y)$ , где  $y \in \{0, 1\}^{n+1}$ ,  $y = bz$ , выдаёт  $b \oplus f_d(z)$ . Корректность протокола очевидна. Нужно доказать многоразовую надёжность.

Пусть коды сообщений  $m_1, \dots, m_{p(n)}$  соответственно

$$(f_d(z_1) \oplus m_1, z_1), (f_d(z_2) \oplus m_2, z_2), \dots, (f_d(z_{p(n)}) \oplus m_{p(n)}, z_{p(n)}).$$

Нужно показать, что такая случайная величина вычислительно неотличима от строки из  $U_{(n+1) \cdot p(n)}$ . Если это не так, то мы могли бы отличить псевдослучайные функции от равномерного распределения (см. соответствующее определение надёжности псевдослучайных функций).  $\square$

*Замечание 4.2.* У этой схемы есть существенный недостаток: длина шифра в  $n + 1$  раз длиннее самого сообщения.

#### 4.1. Эффективная схема шифрования с закрытым ключом

Для шифрования сообщений  $m \in \{0, 1\}^{k(n)}$  возьмём семейство псевдослучайных функций  $f^s : \{0, 1\}^n \rightarrow \{0, 1\}^n$ , где  $s \in S_n = \{0, 1\}^n$ , и генератор псевдослучайных чисел  $G : \{0, 1\}^n \rightarrow \{0, 1\}^{k(n)}$ . Тогда алгоритм шифрования может быть устроен так: выберем случайное  $z \leftarrow U_n$  и определим  $E(d, m) = (G(f^d(z)) \oplus m, z)$ ,  $D(d, (c, z)) = G(f^d(z)) \oplus c$ .

**Утверждение 4.1.** *Описанная схема шифрования надёжна.*

*Схема доказательства.* Доказываем гибридным методом в два этапа. Сначала заменяем функции  $f^s$  на случайные строки длины  $n$  (за один шаг), а потом заменяем применения генераторов на случайные строки длины  $k(n)$  (за  $p(n)$  шагов).  $\square$

### 5. Протоколы с открытым ключом

**Определение 5.1.** Пусть  $(e_n, d_n)$  — доступные случайные величины. Пара вероятностных полиномиальных алгоритмов  $(E, D)$  называется *системой шифрования с открытым ключом*, если алгоритмы шифрования и дешифрования,  $E(e, m)$  и  $D(e, d, c)$ , связаны следующим соотношением (корректность):  $D(e, d, E(e, m)) = m$ . *Надёжность* протокола определяется следующим образом: для любого полинома  $p$  и любых сообщений  $x, y \in \{0, 1\}^{p(n)}$  случайные величины  $\langle e, E(e, x) \rangle$  и  $\langle e, E(e, y) \rangle$  вычислительно неотличимы для  $e \leftarrow e_n$ .

*Замечание 5.1.* В такой системе шифрования значение  $e$  сообщается всем (*публичный ключ*), а  $d$  — никому (*секретный ключ*).

*Замечание 5.2.* Шифрование с закрытым ключом называют *симметричным* (для шифрования и дешифрования используется один и тот же ключ), а шифрование с открытым ключом — *асимметричным* (ключи разные).

*Замечание 5.3.* Для протоколов с открытым ключом из одноразовой надёжности следует многократная надёжность.

**Определение 5.2** (trapdoor permutation family). Пусть задан полиномиальный вероятностный алгоритм  $K$ , который получив на вход  $1^n$  генерирует пару слов  $\langle e, d \rangle$  или выдаёт  $\perp$  (символ неудачи), причём последнее происходит с пренебрежимо малой вероятностью. Слова  $e$  и  $d$  называются соответственно *открытым и закрытым ключами*. Будем через  $A_n$  обозначать первые компоненты всех возможных пар  $\langle e, d \rangle$ , генерируемых алгоритмом  $K$  на входе  $1^n$ . Пусть для каждого  $e \in A_n$  задана перестановка  $f_n^e$  некоторого множества слов  $D_n^e$  длины  $l(n)$ . Последовательность пар  $\{(\langle e_n, d_n \rangle, f_n^e)\}$  будем называть *семейством односторонних перестановок с секретом*, если выполнены следующие условия.

1. (Доступность равномерного распределения на области определения). Существует вероятностный полиномиальный алгоритм  $B$ , который по  $1^n$  и любому  $e \in A_n$  генерирует случайную величину, статистически неотличимую от равномерно распределённой на  $D_n^e$  случайной величины при известном  $e_n$ . (Т.е. пара, состоящая из  $e$  и выхода

алгоритма  $B$  статистически неотличима от пары, состоящей из  $e$  и случайной строки  $D_n^e$ .)

Из этого условия следует доступность случайной величины  $\langle e, U(D_n^e) \rangle$ .

2. (Полиномиальная вычислимость.) Функция  $\langle 1^n, e, x \rangle \rightarrow f_n^e(x)$  вычислима за полиномиальное от  $n$  время.
3. (Необратимость.) Для любой последовательности схем  $C_n$  полиномиального размера вероятность того, что  $C_n$  по  $\langle e, f_n^e(x) \rangle$  найдёт  $x$ , стремится к нулю быстрее любого обратного полинома от  $n$  ( $e$  выбирается случайно из  $A_n$ ,  $x$  выбирается случайно из  $D_n^e$ ).
4. (Возможность обращения при известном закрытом ключе.) Существует полиномиальный вероятностный алгоритм, который по тройке  $\langle 1^n, d, f_n^e(x) \rangle$  с вероятностью близкой к 1 вычисляет  $x$ . Здесь пара  $\langle e, d \rangle$  выбирается генератором случайной величины  $\langle e_n, d_n \rangle$ , а  $x$  выбирается равномерно в  $D_n^e$ .

*Замечание 5.4.* Предположение о существовании односторонних перестановок с секретом сильнее, чем существование односторонних функций. Если функция Рабина или RSA является односторонней, то существуют односторонние перестановки с секретом.

- В случае RSA открытым ключом будет  $\langle p \cdot q, z \rangle$ , а закрытым  $z^{-1} \bmod \phi(p \cdot q)$ .
- В функции Рабина открытым ключом будет  $p \cdot q$ , а секретным ключом будет  $\langle p, q \rangle$ .

**Определение 5.3.** Для односторонней перестановки с секретом  $f_n^e : D_n \rightarrow D_n$ , где  $D_n \subset \{0, 1\}^{k(n)}$ , будем называть *трудным битом* такую полиномиально вычислимую функцию  $h_n : D_n \rightarrow \{0, 1\}$ , для которой случайная величина  $h_n(U(D_n))$  трудна для  $\langle e, f_n^e(U(D_n)) \rangle$ .

**Теорема 5.1.** Если существует семейство перестановок с секретом, то существует протокол с открытым ключом.

*Доказательство.* Заметим, что если есть многократная надёжность, то достаточно научиться шифровать сообщения из одного бита (будем пересылать сообщение зашифрованное побитово). Воспользуемся теоремой Голдрейха-Левина и по перестановке с секретом  $f_n^e$  построим перестановку с секретом  $g_n^e$  с трудным битом  $h_n^e$ :

$$g_n^e(x, r) = f_n^e(x)r, \quad h_n^e(x, r) = x \odot r.$$

**Утверждение 5.1.** Величина  $h_n^e(x, r)$  является трудной для  $\langle e, g_n^e(x, r) \rangle$ .

*Доказательство.* Аналогично доказательству теоремы Голдрейха-Левина. □

Теперь построим протокол для кодирования одного бита. Для ключей  $\langle e, d \rangle \leftarrow K$ :

- алгоритм  $E(e, m)$ , где  $m \in \{0, 1\}$ , выбирает случайный элемент  $x \leftarrow U(D_n)$ , случайные биты  $r \leftarrow U_{l(n)}$  и выдаёт  $\langle m \oplus h_n^e(x, r), g_n^e(x, r) \rangle$ ;
- алгоритм  $D(e, d, \sigma r)$  вычисляет  $x = (g_n^e)^{-1}(y)$  и возвращает  $\sigma \oplus h_n^e(x, r)$ .

Давайте докажем, что при известном  $e$  для любых последовательностей битов  $y_n, z_n$  случайные величины  $\langle y_n \oplus h_n^e(x, r), g_n^e(x, r), e \rangle$  и  $\langle z_n \oplus h_n^e(x, r), g_n^e(x, r), e \rangle$  будут вычислительно неотличимы. Обе эти случайные величины неотличимы от  $\langle U_1, U(D_n), e \rangle$  по соответствующей теореме о трудном бите. □

*Замечание 5.5.* Можно научиться посылать несколько длинные сообщения, если воспользоваться конструкцией, которую мы использовали для псевдослучайного генератора (т.е. получится последовательность случайных битов).

## 6. Протокол привязки (схема обязательства, commitment protocol)

Один участник хочет послать другому участнику некоторый зашифрованный секрет таким образом, что

- без знания ключа секрет невозможно расшифровать,
- не существует другого ключа, который расшифровывал код, в другой секрет.

### 6.1. Неинтерактивный протокол привязки к строке

**Определение 6.1.** *Неинтерактивный протокол привязки к строке* — это пара полиномиальных алгоритмов  $S$  и  $R$ :

- вероятностный алгоритм  $S(x, 1^n) = (c, k)$  шифрует секрет, где  $x$  — это секрет (строка),  $c(x)$  — шифр секрета, а  $k(x)$  — ключ,
- детерминированный алгоритм  $R(c, k) \in \{x, \perp\}$  по зашифрованному секрету и ключу либо восстанавливает *исходный* секрет, либо сообщает, что ключ не подходит.

При этом выполняются следующие условия.

1. (Полнота) Если  $S(x, 1^n) = (c, k)$ , то  $R(c, k) = x$  с вероятностью близкой к 1.
2. (Неразглашение) Для любого полинома  $p$  и любых последовательностей строк  $x_n, y_n$ ,  $|x_n| = |y_n| = p(n)$ , если  $c_n$  — привязка  $x_n$ ,  $d_n$  — привязка  $y_n$ , то случайные величины  $c_n$  и  $d_n$  вычислительно неотличимы.
3. (Недвусмысленность) Ни для какого  $n$  не существует таких  $c, k_1, k_2$ , что одновременно  $R(c, k_1) \neq \perp$ ,  $R(c, k_2) \neq \perp$  и  $R(c, k_1) \neq R(c, k_2)$ .

*Замечание 6.1.* Достаточно научиться привязывать к биту (т.е. достаточно построить конструкцию для  $p(n) = 1$ ).

**Определение 6.2.** Будем называть одностороннюю перестановку  $f_n : D_n \rightarrow D_n$  *правильной*, если доступно равномерное распределение на  $D_n \cup \{\perp\}$  (т.е., если не получилось сгенерировать элемент из  $D_n$ , то выдаётся особый символ  $\perp \notin D_n$ ).

**Теорема 6.1.** *Если существует правильная односторонняя перестановка, то существует и неинтерактивный протокол привязки к биту.*

*Доказательство.* Пусть  $f_n : D_n \rightarrow D_n$  — односторонняя перестановка с трудным битом  $h_n$ . Будем привязывать бит  $\sigma \in \{0, 1\}$ . Выберем строку  $x$  из распределения на  $D_n$ , которое вычислительно неотлично от равномерного (есть по свойству доступности). Тогда  $S(\sigma, 1^n) = (\underbrace{\langle h_n(x) \oplus \sigma, f_n(x) \rangle}_c, \underbrace{r_n}_k)$ , где  $r_n$  — это случайные биты, которые использовались

для генерации  $x$ .<sup>2</sup> Соответственно,  $R(c, k)$  генерирует  $x$  используя в качестве случайных битов  $k$  и проверяет, что  $f_n(x)$  совпадает с соответствующими битами  $c$ . Если это так, то бит  $\sigma$  восстанавливается по первому биту  $c$ . Несложно увидеть, что свойство 1 выполняется по построению, свойство 2 следует из определения трудного бита, а свойство 3 из того, что  $K$  возвращает только элементы из  $D_n$ .  $\square$

<sup>2</sup>Нельзя в качестве ключа выбрать  $x$ , т.к. тогда нужно было бы уметь проверять, что  $x \in D_n$ .

## 7. Интерактивные протоколы

**Определение 7.1.** *Интерактивный протокол* — это пара вероятностных алгоритмов  $A(1^n, x, h)$  и  $B(1^n, y, h)$ , которые „общаются между собой”, передавая сообщения друг другу. Интерактивный протокол состоящий из  $t$  раундов устроен так:

$$\begin{aligned} s_1 &\leftarrow A(1^n, x, \lambda), \\ s_2 &\leftarrow B(1^n, x, s_1), \\ s_3 &\leftarrow A(1^n, x, \langle s_1, s_2 \rangle), \\ s_4 &\leftarrow B(1^n, x, \langle s_1, s_2, s_3 \rangle), \\ &\vdots \\ s_{t-1} &\leftarrow A(1^n, x, \langle s_1, s_2, \dots, s_{t-2} \rangle), \\ s_t &\leftarrow B(1^n, x, \langle s_1, s_2, \dots, s_{t-1} \rangle). \end{aligned}$$

В последнем сообщении  $s_t$  содержится некоторый признак (например, специальный символ), который сигнализирует об окончании общения. Алгоритмы такого вида будем называть *интерактивными алгоритмами*. Через  $\pi_{A(x), B(y)}$  будем обозначать историю взаимодействия алгоритмов  $A$  и  $B$  на входах  $x$  и  $y$  соответственно. Для  $t$ -раундового протокола  $\pi_{A(x), B(y)} = \langle s_1, s_2, \dots, s_t \rangle$ . После завершения общения алгоритмы  $A$  и  $B$  ещё раз запускаются на полученной истории и печатают результат, т.е. на стороне алгоритма  $A$  результатом будет  $A(1^n, x, \pi_{A(x), B(y)})$ , а на стороне алгоритма  $B$  —  $B(1^n, y, \pi_{A(x), B(y)})$ . Аналогичное определение можно дать и для схем, нужно только позаботиться о том, чтобы аккуратно закодировать неполную историю (можно, например, использовать алфавит с дополнительными символами).

### 7.1. Интерактивные протоколы привязки к строке

Для неинтерактивного протокола привязки нам потребовалось предположить существование правильных односторонних перестановок. Оказывается, что если добавить интерактивность, то можно построить протокол привязки при более слабом предположении.

**Определение 7.2.** *Интерактивный протокол привязки к строке* — полиномиальный (по суммарному времени, а следовательно и по количеству раундов) интерактивный протокол, заданный полиномиальными вероятностными алгоритмами  $S(1^n, \sigma, h)$  и  $T(1^n, h)$ , и детерминированный полиномиальный алгоритм  $R(1^n, c, k)$ , где  $S$  — алгоритм стороны, которая осуществляет привязку,  $T$  — алгоритм стороны, которая получает привязку, а  $R$  — алгоритм проверяющий, что привязка действительно соответствует исходной строке. Привязкой строки  $\sigma$  в этом интерактивном алгоритме будет  $c(\sigma) = \pi_{S(\sigma), T}$ . После окончания взаимодействия алгоритм  $S$  выдаёт ключ  $k(\sigma)$ , соответствующий этой привязке. Алгоритм  $R(c, k)$  выдаёт либо строку  $\sigma$ , по которой была построена привязка, либо один из специальных символов  $\perp_S$  и  $\perp_T$ , которые „обвиняют” соответственно, протокол  $S$  и  $T$  в жульничестве. Кроме того, должны выполняться следующие свойства.

1. (Корректность)  $R(\pi_{S(\sigma), T}, k_{n, \sigma}) = \sigma$  с вероятностью 1.
2. (Полнота) Для любого (схемного) противника  $T^*$

$$R(\pi_{S(\sigma), T^*}, k_{n, \sigma}) \in \{\sigma, \perp_T\}$$

с вероятностью пренебрежимо отличающейся от 1.

3. (Неразглашение) Для любого противника  $T^*$ , полинома  $p(n)$  и любых последовательностей строк  $x_n, y_n, |x_n| = |y_n| = p(n)$ , случайные величины  $\pi_{S(x_n), T^*}$  и  $\pi_{S(y_n), T^*}$  вычислительно неотличимы.
4. (Недвусмысленность привязки) Для любого противника  $S^*$  вероятность

$$\Pr[\exists k_1, k_2 \mid R(\pi_{S^*, T}, k_1) \neq \perp_S, R(\pi_{S^*, T}, k_2) \neq \perp_S, R(\pi_{S^*, T}, k_1) \neq R(\pi_{S^*, T}, k_2)]$$

пренебрежимо мала.

5. Вероятность  $\Pr[\exists k \mid R(\pi_{S^*, T}, k) = \perp_T]$  пренебрежимо мала.

**Теорема 7.1.** *Если существует генератор псевдослучайных чисел, то существует интерактивный протокол привязки к биту.*

*Доказательство.* Определим протокол привязки для бита  $\sigma \in \{0, 1\}$ . Возьмём генератор псевдослучайных чисел  $G_n : \{0, 1\}^n \rightarrow \{0, 1\}^{3n}$ . Алгоритм  $T(1^n)$  генерирует случайную строку  $r \leftarrow U_{3n}$  и посылает её  $S$ . Алгоритм  $S(1^n, \sigma)$  ожидает получения строки  $r \in \{0, 1\}^{3n}$ , генерирует строку  $s \leftarrow U_n$  и посылает сообщение

$$t = \begin{cases} G(s) \oplus r, & \sigma = 1, \\ G(s), & \sigma = 0. \end{cases}$$

Ключом для этой привязки будет  $k = \sigma s$ .

Алгоритм  $R(1^n, (r, t), k)$  проверяет, что все длины строк в привязке соответствуют ожидаемым:  $|r| = |t| = 3n, |k| = n + 1$ . Если длины неправильные, то  $R$  обвиняет соответствующую сторону. После этого алгоритм  $R$  по  $k = \sigma s$  вычисляет  $t \oplus G(s)$ :

- если получилось  $0^{3n}$ , то проверяет, что  $\sigma = 0$ , и выдаётся 0;
- если получилось  $r$ , то проверяет, что  $\sigma = 1$ , и выдаётся 1;
- если получилось что-то ещё, то выдаёт  $\perp_S$ .

Свойства 1, 2 и 5 выполняются по построению. Свойство 3 означает, что следующие случайные величины  $\langle r, G_n(s) \rangle$  и  $\langle r, G_n(s) \oplus r \rangle$  должны быть вычислительно неотличимы. Если мы умеем их различать, то умеем одну из них отличать от  $\langle r, U_{3n} \rangle$ , а это позволяет взломать генератор  $G_n$ . Осталось проверить свойство 4. Давайте оценим

$$\Pr[\exists s_0, s_1 \mid G_n(s_0) \oplus t = 0^{3n}, G_n(s_1) \oplus t = r] = \Pr[\exists s_0, s_1 \mid G_n(s_0) \oplus G_n(s_1) = r] \leq \frac{2^{2n}}{2^{3n}} = 2^{-n}.$$

□

## 7.2. Протокол подбрасывания монетки

**Определение 7.3.** *Интерактивный протокол подбрасывания монетки* — это полиномиальный (по суммарному времени и по количеству раундов) интерактивный протокол, заданный полиномиальными вероятностными алгоритмами  $A(1^n, h)$  и  $B(1^n, h)$ , и детерминированный полиномиальный алгоритм  $D(1^n, h)$ , где  $A$  и  $B$  — это алгоритмы сторон, а  $D$  — алгоритм, позволяющий по истории общения получить результат подбрасывания монетки. Стороны запускают  $D$  после завершения протокола и определяют результат. Для стороны  $A$  и любого противника  $B^*$  должны выполняться следующие свойства (интересы стороны  $A$ ):



1. вероятность  $\Pr[D(\pi_{A,B^*}) = \perp_A]$  пренебрежимо мала,
2. для любого  $\sigma \in \{0, 1\}$   $\Pr[R(\pi_{A,B^*}) = \sigma] \leq \frac{1}{2} + \alpha_n$ , где  $\alpha_n$  — пренебрежимо мала.

Такие же свойства должны выполняться и для стороны  $B$  и любого противника  $A^*$ .

**Теорема 7.2.** *Если существует интерактивный протокол привязки к биту, то существует и интерактивный протокол подбрасывания монетки.*

*Доказательство.* Пусть  $(S, T, R)$  — интерактивный протокол привязки. Сторона  $A$  генерирует бит  $\sigma$  и запускает алгоритм привязки  $S(\sigma)$ , сторона  $B$  запускает алгоритм  $T$ ; в конце протокола обе стороны знают привязку  $c(\sigma)$ , а сторона  $A$  ещё дополнительно знает ключ  $k(\sigma)$ . Потом сторона  $B$  генерирует бит  $\tau$  и посылает его алгоритму  $A$ , а сторона  $A$  в ответ посылает ключ  $k(\sigma)$ .

Алгоритм  $C(c(\sigma), \tau, k(\sigma))$  запускает алгоритм  $R(c(\sigma), k(\sigma))$  для проверки для привязки. Если алгоритм проверки привязки обвиняет какую-то сторону, то  $C$  обвиняет соответствующую сторону. В противном случае  $C$  выдаёт  $\sigma \oplus \tau$ .

Давайте проверим, что интересы стороны  $A$  соблюдаются. Свойство 1 следует из протокола привязки (т.к. обвинение стороны возможно только в протоколе привязки). Предположим, что второе свойство нарушается. Тогда  $B^*$  может подбирать бит  $\tau$  так, чтобы угадывать  $\sigma$  с нетривиальной вероятностью, а значит  $B^*$  можно использовать для взлома протокола привязки.

Интересы стороны  $B$  соблюдаются из-за недвусмысленности протокола привязки, поэтому вероятность того, что  $A$  сможет подменить ключ пренебрежимо мала.  $\square$

## Список литературы

- [1] Н.К. Верещагин. Курс лекций “Теоретико-сложностные проблемы криптографии”, МГУ, <http://lpcs.math.msu.su/~ver/teaching/cryptography/index.html>.
- [2] Д.М. Ицкисон. Курс “Теоретико-сложностные основы криптографии”, CS центр, <https://compsclub.ru/courses/cryptography-foundations/2016-spring/>.
- [3] O. Goldreich. *Foundations of cryptography*.
- [4] J. Håstad, R. Impagliazzo, L.A. Levin, M. Luby. *A Pseudorandom Generator from any One-way Function*. SIAM J. Comput. 28, 4 (March 1999), 1364-1396.  
DOI: <https://doi.org/10.1137/S0097539793244708>
- [5] J. Katz, Y. Lindell. *Introduction to Modern Cryptography*.

## Todo list