Лекция 5

Эквивалентность существования owf и PRG

(Конспект: К. Шмаков)

Напомним, что $q(k)$-PRG означает псевдослучайный генератор $\{0,1\}^k \to \{0,1\}^{q(k)}$, а $\circ$ — конкатенацию строк.

Теорема 5.1. *$\exists$ $2k$-PRG $\Rightarrow \exists$ owf.*

Теорема 5.2. *$\exists$ owp, сохраняющая длину $\Rightarrow \forall d \ \exists \ k^d$-PRG, а именно,*

$$G(x) = f^{k^d-k}(x) \circ B(x) \circ B(f(x)) \circ \ldots \circ B(f^{k^d-k-1}(x)),$$

где B — трудный бит для owp f, сохраняющей длину.

Замечание 5.1. Можно было бы воспользоваться и owf, но это сложно.

Доказательство теоремы 5.1. Пусть G — $2k$-PRG. Возьмём $f(x \circ y) = G(x)$, где x и y — длины k. Покажем, что f — односторонняя.

Пусть нет, и есть взломщик, который её взламывает на доле $\geq \frac{1}{p(k)}$ для некоторого полинома p. Это означает, что существует противник, который находит элемент из $G^{-1}(G(x))$ с вероятностью $\geq \frac{1}{p(k)}$.

Тогда различающий выходы генератора алгоритм будет следующий: он берёт свой вход y, вычисляет $z = G^{-1}(y)$ и выдаёт единицу, если $G(z) = y$. Если y порождён G, то вероятность этого события $\geq \frac{1}{p(k)}$. Если же y взят в соответствии с равномерным распределением на $\{0,1\}^{2k}$, то вероятность, что он попал в $\operatorname{Im} G$, составляет $\frac{|\operatorname{Im} G|}{2^{2k}} \leq 2^{-k}$, т.е. вероятность выдать единицу на случайных входах экспоненциально мала и её разность с полиномиальной вероятностью на выходах генератора — тоже хотя бы полиномиальна. Противоречие с тем, что G — PRG. $\square$

Доказательство теоремы 5.2. Сначала докажем существование $(k+1)$-PRG, а потом — k^d-PRG.

Пусть $f\colon \{0,1\}^k \to \{0,1\}^k$ — (сильно) односторонняя перестановка, сохраняющая длину, а B — её трудный бит. Покажем, что $G(x) = f(x) \circ B(x)$ — это $(k+1)$-PRG.

Пусть нет, и G — не PRG, т.е. существует A, такой, что

$$|\Pr\{A(G(x)) = 1\} - \Pr\{A(y) = 1\}| \geq \frac{1}{q(k)}$$

для некоторого многочлена q. (Будем в дальнейшем эти вероятности называть *"первая"* и *"вторая"*.)

Введём обозначения:

$$\begin{aligned}\alpha &= \Pr\{A(f(x) \circ b) = 1 | b = B(x)\} = \Pr\{A(f(x) \circ B(x)) = 1\},\\ \beta &= \Pr\{A(f(x) \circ b) = 1 | b = \overline{B(x)}\} = \Pr\{A(f(x) \circ \overline{B(x)}) = 1\}.\end{aligned}$$

Поскольку f — перестановка, сохраняющая длину, *вторую* вероятность можно переписать следующим образом:

$$\begin{aligned}&\Pr\{A(f(x) \circ b) = 1\} = \\ &\Pr\{b = B(x)\} \cdot \Pr\{A(f(x) \circ B(x)) = 1\} + \Pr\{b = \overline{B(x)}\} \cdot \Pr\{A(f(x) \circ \overline{B(x)}) = 1\} \\ &= \frac{\alpha + \beta}{2}.\end{aligned}$$

Первая вероятность — это как раз α. Не умаляя общности, будем считать, что на гарантированной нам бесконечной последовательности длин входов, где A взламывает G, выполняется $\alpha \geq \beta$ (в противном случае будем рассматривать другую машину: $\widetilde{A}(f(x) \circ b) = A(f(x) \circ \overline{b})$). Тогда

$$\frac{1}{q(k)} \leq \Pr\{A(G(x)) = 1\} - \Pr\{A(y) = 1\} = \alpha - \frac{\alpha + \beta}{2} = \frac{\alpha - \beta}{2},$$

и мы получаем алгоритм A', который по $f(x)$ будет находить $B(x)$:

- выбрать $b \in \{0,1\}$ случайным образом;
- если $A(f(x) \circ b) = 1$, то выдать b, иначе выдать $\overline{b}$.

Тогда

$$\begin{aligned}
&\Pr\{A'(f(x)) = B(x)\} = \\
&\qquad \Pr\{b = B(x)\} \cdot \Pr\{A(f(x) \circ B(x)) = 1\} + \\
&\qquad \Pr\{b = \overline{B(x)}\} \cdot \Pr\{A(f(x) \circ \overline{B(x)}) \neq 1\} = \\
&\qquad\qquad \frac{1}{2}\alpha + \frac{1}{2}(1-\beta) = \frac{1}{2} + \frac{\alpha-\beta}{2} \geq \frac{1}{2} + \frac{1}{q(k)},
\end{aligned}$$

что противоречит тому, что $B(x)$ — трудный бит.

————————

Теперь, когда мы умеем строить $(k+1)$-PRG, докажем, что

$$f^{k^d}(x) \circ B(x) \circ \dots \circ B(f^{k^d-1}(x)) \qquad (\bigtriangledown)$$

является k^d-PRG.

Если вдруг случилось, что его умеют неплохо отличать от случайных битов, это означает, что есть противник A, который хорошо (с разностью вероятностей хотя бы $\varepsilon = \frac{1}{q(k)}$) отличает выходы генератора от случайных строк, каковые можно представить в виде

$$f^{k^d}(x) \circ b_1 \circ \dots \circ b_{k^d} \qquad (\bigtriangleup)$$

(b_i — случайные биты) в силу того, что f — перестановка, сохраняющая длину.

Рассмотрим следующую цепочку распределений, в которой $(\bigtriangledown)$ постепенно превращается в $(\bigtriangleup)$:

$$\begin{array}{lllllllll}
D_0(x) & = f^{k^d}(x) & \circ\, B(x)\, \circ & & \dots & & & & \circ\, B(f^{k^d-1}(x)) \\
\vdots & & & & & & & & \\
D_i(x) & = f^{k^d-i}(x) & \circ\, b_1 & \circ \dots \circ\, b_i & \circ\, B(x) & \circ\, B(f(x)) & \circ \dots & & \circ\, B(f^{k^d-i-1}(x)) \\
D_{i+1}(x) & = f^{k^d-i-1}(x) & \circ\, b_1 & \circ \dots \circ\, b_i & \circ\, b_{i+1} & \circ\, B(x) & \circ \dots & & \circ\, B(f^{k^d-i-2}(x)) \\
\vdots & & & & & & & & \\
D_{k^d}(x) & = x & \circ\, b_1 & \circ & \dots & & & & \circ\, b_{k^d}
\end{array}$$

Пусть $p_i = \Pr\{A(D_i(x)) = 1\}$. Тогда

$$\varepsilon \leq |p_{k^d} - p_0| \leq \sum_{i=0}^{k^d-1} |p_{i+1} - p_i|.$$

Поэтому существует такое i_*, что

$$|p_{i_*+1} - p_{i_*}| \geq \frac{\varepsilon}{q(k)} = \varepsilon'.$$

Отсюда получаем алгоритм, который который будет отличать построенный нами $(k+1)$-PRG от случайных чисел с разностью вероятностей $\varepsilon'' = \frac{\varepsilon'}{q(k)}$. С вероятностью $\frac{1}{q(k)}$ угадываем $i = i_*$. Далее по входным $f(x)$ и b строим строчку:

$$f^{k^d-i}(x) \circ b_1 \circ \dots \circ b_i \circ b \circ B(f(x)) \circ \dots \circ B(f^{k^d-i-1}(x)).$$

Пусть $z = f(x)$; то, что A отличает D_{i+1} от D_i, означает, что он отличает с вероятностями, разнящимися на ε', строку

$$f^{k^d-i}(x) \circ b_1 \circ \dots \circ b_i \circ B(x) \circ B(f(x)) \circ \dots \circ B(f^{k^d-i-1}(x)),$$

которую мы построили в случае, если нам дали $b = B(x)$, от от строчки вида

$$f^{k^d-i-1}(z) \circ b_1 \circ \dots \circ b_i \circ b_{i+1} \circ B(z) \circ \dots \circ B(f^{k^d-i-2}(z)),$$

которая получается при том же построении, если нам дали случайный бит b.

Таким образом, мы построили алгоритм, который взламывает построенный нами в первой части доказательства $(k+1)$-PRG с вероятностью ε''. Противоречие. $\square$