Криптография, Лекция № 4

29 сентября 2014 г.

Продолжение доказательства теоремы о существовании генератора псевдо-случайных чисел, если существует односторонняя перестановка.

Сперва построим генератор псевдо-случайных числе, отображающий n битов в $p(n)$, имея генератор псевдо-случайных чисел ($n \mapsto n+1$).

По генератору $G(x) = g(x)h(x)$ построим $G'(x) = h(x)h(g(x))h(g(g(x)))\dots$

Claim 1.
Если $G(x)$ - генератор псевдо-случайных чисел, то $G'(x)$ - генератор псевдо-случайных чисел.

Доказательство.
Метод гибридного аргумента:

$$G_{k+1}(x) = h(x)h(g(x))h(g(g(x)))\dots h(g^k(x))g^{k+1}(x)$$

$$G_k(x, r_1) = r_1 h(x)h(g(x))h(g(g(x)))\dots h(g^{k-1}(x))g^k(x)$$

$$G_k(x, r_1, r_2) = r_1 r_2 h(x)h(g(x))h(g(g(x)))\dots h(g^{k-2}(x))g^{k-1}(x)$$

$$G_1(x, r) = r_1 r_2 \dots r_{k+1} x$$

$$G_0(x, r) = r_1 r_2 \dots r_k h(x) g(x)$$

G_0 - истинно случайные биты. G_k - претендент на генератор.

Если $G_{k+1} = G'$ - не генератор, то

$$\exists D\ \exists q(\cdot)\ \forall N\ \exists n > N\ |Pr_{x,r}\{D(G_0(x,r)) = 1\} - Pr_{x,r}\{D(G_k(x,r)) = 1\}| \geq \frac{1}{q(n)}$$

$$\Rightarrow \exists q'\ \forall N\ \exists n > N\ \exists i | Pr_{x,r}\{D(G_i(x,r)) = 1\} - Pr_{x,r}\{D(G_{i+1}(x,r)) = 1\}| \geq \frac{1}{q'(n)}$$

Тогда G - не генератор:
отличили

$$r_1 r_2 \dots r_{k-i+1} h(x)h(g(x))\dots h(g^{i-1}(x))g^i(x)$$

от

$$r_1 r_2 \dots r_{k-i} h(x)h(g(x))\dots h(g^i(x))g^{i+1}(x)$$

Переобозначим: $y = g^i(x)$, $s = r_1 \dots r_{k-i}$, $T(x) = h(x) \dots h(g^{i-1}(x))g^i(x)$.

В этих обозначения мы отличили $sr_{k-i+1}T(x)$ от $sh(x)T(g(x))$.

Фиксируя s, отличили $rT(x)$ от $h(x)T(g(x))$.

$$D'(x, r) = D(srT(x))$$

D' будет оличать xr от $g(x)h(x)$. Что привододит к противоречию с тем, что $g(x)h(x)$ - генератор псевдо-случайных чисел. □

Осталось по односторонней перестановке построить одностороннюю перестановку с трудным битом. Но сперва поговорим немного о кодах Адамара.

Definition 1. Код Адамара $H\colon \{0,1\}^n \to \{0,1\}^{2^n}$.

$$H(x_1, \dots, x_n) = (x_1y_1 + \dots + x_ny_n)|_{(y_1,\dots,y_n)\in\{0,1\}^n}$$

Коды Адамара могут быть декодированы списком:
Если расстояние Хэминга $\rho_H(z, \bar{z}) \le \frac{1}{2} - \varepsilon$, то за время $poly(\frac{n}{\varepsilon})$ можно выдать полиномиальный список, содержащий прообраз z. $z, \bar{z} \in \{0,1\}^{2^n}$; $z \in ImH$ (z - кодовое слово H).

Доказательство. (Существования декодирования)

Definition 2.
Расстояние Хэмминга $\rho_H(t, t') = \frac{\#\{i\colon t_i \neq t'_i\}}{2^n}$

К $\bar{z}$ произвольный доступ: по j за константное время можно найти $\bar{z}_j$

Без искажений достаточно запросить n битов с номерами $(1, 0, \dots, 0), \dots, (0, \dots, 0, 1)$

Обозначим $z(y)$ - соответствующий бит z.

Claim 2.
$z(y + r) = z(y) + z(r)$

Из утверждения $z(y) = z(y + r) + z(r) =$ большинство из $\bar{z}(y + r) + z(r)$

Idea 1.
Выберем специальным образом попарно независимые $r_1, \dots, r_s$; выберем z_y как большинство из $\bar{z}(y + r_i) + z(r_i)$

Выбор $r_1, \dots, r_s$:

A - матрица размера $(2^m - 1) \times m$, строки - ненулевые элементы $\{0,1\}^m$.
Пусть $s = 2^m - 1$.

Claim 3.
u - случайный вектор $m \times 1 \Rightarrow$ величины Au попарно независимы.

Возьмем $u_1, \ldots, u_n$ - случайные векторы размера $m \times 1$. U - случайная матрица размера $m \times n$.

$R = (r_1, \ldots, r_s)^T = AU$, матрица рамера $(2^m - 1) \times n$.

$$r_i = A_i U = (A_{i_1} e_1 + \ldots + A_{i_m} e_m)U = A_{i_1} e_1 U + \ldots + A_{i_m} e_m U = A_{i_1} \bar{U}_1 + \ldots + A_{i_m} \bar{U}_m$$

$$z(r_i) = A_{i_1} z(\bar{U}_1) + \ldots + A_{i_m} z(\bar{U}_m)$$

То есть достаточно задать $z(\bar{U}_1), \ldots, z(\bar{U}_m)$ чтобы вычислить $z(r_i)$. Но все эти 2^m вариантов можно перебрать. Для каждого варианта вычисляем $z(r_i)$ и имея $\bar{z}$ с произвольным доступом, вычисляем значения по большинству.

Еще раз конструкция: для фиксированного набора $z(\bar{u}_1), \ldots, z(\bar{u}_m)$ при $j = 1, \ldots, n$. $z(e_j)$ выбирается как большинство из $\bar{z}(e_j + r_i) + z(r_i)$
ξ_i - случайная величина равная 1, если и только если $z(y) \neq \bar{z}(y + r_i) + z(r_i)$

$$Pr\{\xi_i = 1\} \leq \frac{1}{2} - \varepsilon$$

Нужно посчитать вероятность $Pr\{\frac{1}{s}(\xi_1 + \ldots + \xi_s) \leq \frac{1}{2}\}$ для попарно независимых $\xi_1, \ldots, \xi_s$ $\square$