Криптография, Лекция № 3

29 сентября 2014 г.

1 Генераторы псевдо-случайных чисел

Definition 1.
α_n, β_n вычислительно не отличимые семейства случайных величин, если

$$\forall p(\cdot)\ \forall \{D_n\}\ \exists N\ \forall n > N\ |Pr\{D_n(\alpha_n) = 1\} - Pr\{D_n(\beta_n) = 1\}| < \frac{1}{p(n)}$$

где $p(\cdot)$ - полином, D_n - схема полиномиального размера.

Lemma 1.

1. *Вычислительная неотличимость - отношение эквивалентности. (Сумма двух функций, которые стремятся к нулю быстрее любого полинома обладет тем же свойством).*

2. $\alpha_n \sim \beta_n \Rightarrow \alpha_n\gamma_m \sim \beta_n\gamma_n$, *$\gamma_n$ не зависит от α_n и β_n*

   Пусть не выполнено условие в правой части, тогда:

$$\begin{aligned} & |Pr_{\alpha,\gamma}\{D_n(\alpha_n\gamma_n) = 1\} - Pr_{\beta,\gamma}\{D_n(\beta_n\gamma_n) = 1\}| = \\ = \quad & |E_\gamma(Pr_\alpha\{D_n(\alpha_n\gamma_n) = 1\} - Pr_\beta\{D_n(\beta_n\gamma_n) = 1\})| > \frac{1}{q(n)} \end{aligned}$$

3. $\alpha_n \sim \beta_n \Rightarrow C_n(\alpha_n) \sim C_n(\beta_n)$, *$C_n$ - схема полиномиального размера.*

   Пусть не выполнено условие в правой части, тогда: Если D_n отличает $C_n(\alpha)$ от $C_n(\beta)$, то $D_n \circ C_n$ отличает α_n от β_n.

Definition 2.
$G_n \colon \{0,1\}^{k(n)} \to \{0,1\}^{l(n)}$ - **генератор псевдо-случайных чисел**, если случайные величины $G_n(U_{k(n)})$ и $U_{l(n)}$ вычислительно неотличимы то есть:

$$\forall p(\cdot)\ \forall \{D_n\}\ \exists N\ \forall n > N\ |Pr\{D_n(\alpha_n) = 1\} - Pr\{D_n(\beta_n) = 1\}| < \frac{1}{p(n)}$$

Remark 1.

- *Важна именно вычислительная неотличимость. Заменить ее на статистическую неотличимость не получится.*

- G_n *- сильно одностороння функция.*
  Пусть $\ldots Pr\{G_n(R_n(G_n(x))) = G_n(x)\} > \varepsilon$.

$$D_n(y) = \begin{cases} 1 & G_n(_n(y)) = y \\ 0 & \textit{иначе} \end{cases}$$

Definition 3.
$\beta(x)$ - **Трудный бит** для f, если

$$\forall p\ \forall\{C_n\}\ \exists N\ \forall n > N\ |Pr\{C_n(f(x)) = \beta(x)\} - \frac{1}{2}| < \frac{1}{p(n)}$$

Example 1. *(Предположительный)*
Функция Рабина: $(x,\ y) \mapsto (x^2\ mod\ y,\ y)$. *Трудный бит - четность* x.

План доказательста существования генератора случайных битов, если известно, что существует одностороння функция:

- Односторонняя перестановка $\mapsto$ одностороння перестановка с трудным битом.
  $g(x,y) = (f(x), y)$
  $\beta(x,y) = x \odot y = \oplus_{i=1}^{n} x_i y_i$

- Односторонняя перестановка с трудным битом $\mapsto$ генератор

- Генератор$(n \to n+1) \mapsto$ Генератор$(n \to p(n))$

Lemma 2.
$\beta(x)$ *- трудный бит для* $f(x) \Leftrightarrow x \mapsto f(x)\beta(x)$ *- генератор.*

Доказательство.
$\Leftarrow$
β можно угадать $\Rightarrow f(x)\beta(x)$ можно отличить от y.
$D_n(y) = (C_n(y\ |_{1\ldots n}) \leftrightarrow y_{n+1})$
y случайное $\Rightarrow D_n$ угадывает с вероятностью $\frac{1}{2}$.
$y = f(x)\beta(x) \Rightarrow D_n$ угадает с вероятностью $\frac{1}{2} + \frac{1}{p(n)}$
$\Rightarrow$
$f(x)\beta(x)$ умеем отличать от $y \Rightarrow$ можно предсказать $\beta(x)$ по $f(x)$.
y можно представить в виде $f(x)r$.

		$D(f(x)1)$	
		0	1
$D(f(x)0)$	0	random	1
	1	0	random

Введем $p_0, p_1, q_0, q_1, r_0, r_1, s_0, s_1$ - вероятности в соответствующих условиях того, что $\beta(x) = 0$ и $\beta(x) = 1$
Например: $r_1 = Pr\{\beta(x) = 1,\ D(f(x)0) = 1,\ D(f(x)1) = 0\}$.

$$Pr\{C_n(f(x)) = \beta(x)\} = \tfrac{1}{2}(p_0 + p_1) + q_1 + r_0 + \tfrac{1}{2}(s_0 + s_1) \ominus$$

$Pr\{D(f(x)r) = 1\} = (s_0 + s_1) + \frac{1}{2}(r_0 + r_1) + \frac{1}{2}(q_0 + q_1)$

$Pr\{D(f(x)\beta(x)) = 1\} = (s_0 + s_1) + r_0 + q_1$

$\frac{1}{2}(r_0 - r_1) + \frac{1}{2}(q_1 - q_0) > \varepsilon$

$$\begin{aligned} \ominus \quad & \frac{1}{2}(p_0 + p_1) + \frac{1}{2}(q_1 + q_0) + \frac{1}{2}(r_0 + r_1) + \frac{1}{2}(r_0 - r_1) + \frac{1}{2}(s_0 + s_1) = \\ = \quad & \frac{1}{2} + \frac{1}{2}(q_1 - q_0) + \frac{1}{2}(r_0 - r_1) > \frac{1}{2} + \varepsilon \end{aligned}$$

□

Idea 1. *Последнего шага*
$x \mapsto g(x)h(x) \mapsto g(g(x))h(g(x))h(x) \mapsto g(g(g(x)))h(g(g(x)))h(g(x))h(x) \mapsto \ldots$