Криптография, Лекция № 2

15 сентября 2014 г.

Вспомним определения сильно односторонних функций:

$$\forall\{R_n\}\ \exists p(\cdot)\ \exists N\ \forall n > N\ Pr\{f(R_n(f(x))) = f(x)\} < 1 - \frac{1}{p(n)}$$

$$\exists p(\cdot)\ \forall\{R_n\}\ \exists N\ \forall n > N\ Pr\{f(R_n(f(x))) = f(x)\} < 1 - \frac{1}{p(n)}$$

Из второго всегда следует первое.
Отрицание второго:

$$\forall p(\cdot)\ \exists\{R_n\}\ \forall N\ \exists n > N\ Pr\{f(R_n(f(x))) = f(x)\} \geq 1 - \frac{1}{p(n)}$$

Можно найти такую последовательность из отрицания выше:

$$\forall k\ \exists\{R_n^{(k)}\}\ \forall N\ \exists n > N\ Pr\{f(R_n(f(x))) = f(x)\} \geq 1 - \frac{1}{n^k}$$

$$R_{n_1^{(1)}} : Pr\{\cdots\} \geq 1 - \frac{1}{n_1}$$

$$R_{n_2^{(2)}} : n_2 > n_1, Pr\{\cdots\} \geq 1 - \frac{1}{n_2^2}$$

И так далее.
Из этого ряда вытекает следующее:

$$\exists\{R_n\}\ \forall k\ \forall N\ \exists n = max\{n_k, n_k > N\} > NPr\{\cdots\} \geq 1 - \frac{1}{n^k}$$

$$\exists p(\cdot)\ \forall\{R_n\}\ \exists N\ \forall n > N\ Pr\{f(R_n(f(x))) = f(x)\} < 1 - \frac{1}{p(n)}$$

$$F(x_1, \ldots, x_N) = f(x_1) \ldots f(x_N)$$

Theorem 1.
Если $N = n \cdot p(n)$, то F - сильно односторонняя, то есть

$$\forall q(\cdot)\ \forall\{T_n\}\ \exists N\ \forall n > N\ Pr\{F(T_n(F(x))) = F(x)\} < \frac{1}{q(n)}$$

Доказательство.
Пусть

$$\exists q(\cdot)\ \exists\{T_n\}\ \forall N\ \exists n > N\ Pr\{F(T_n(F(x))) = F(x)\} \geq \frac{1}{q(n)}$$

Построим R_n: M раз повторить процедуру:

- При всех i от 1 до N выбрать случайные $x_1, \ldots, x_N$
- Посчитать $T_n(f(x_1) \ldots f(x_{i-1}) y f(x_{i+1}) \ldots f(x_N))$
- Проверить успешность обращения y.

$S_i(x)$ - вероятность успешного обращения $f(x)$ на шаге i внутреннего цикла. $S(x) = max\{S_1(x), \ldots, S_N(x)\}$ - нижняя оценка вероятности обращения на 1 шаге внешнего цикла. Все x разделим на две части по предикату $S(x) \geq \delta = \frac{1}{poly(n)}$.

Для первых, удовлетворяющих предикату, повторение $M = n \cdot \frac{1}{\delta}$ раз приведет к вероятности обращения $f(x) \sim 1 - e^{-n}$
Вероятность того, что обращение не сработает ни на одном шаге: $(1-\delta)^M = (1-\delta)^{n \cdot \frac{1}{\delta}} \sim e^{-n}$

Для вторых, трудных, докажем, что таких x мало (например, $< \frac{1}{2p(n)}$)
Вход T_n: $x_1 \ldots x_N$ все x_i легкие с вероятностью $(1-\varepsilon)^N$, где ε - доля трудных x.

x_i трудный, остальные случайные. В этом случае условная вероятность обращения $< \delta$.

Общая вероятность обращения $\leq N\delta\varepsilon + (1+\varepsilon)^N$ - что-то типа формулы включений-исключений. Получим противоречие, если покажем, например, что $N\delta\varepsilon + (1+\varepsilon)^N < \frac{1}{q(n)}$

Если $\varepsilon < \frac{1}{2p(n)}$, получим противоречие со слабой одностороностью F.

Если же $\varepsilon \geq \frac{1}{2p(n)}$, возьмем $\delta = \frac{1}{2np(n)q(n)}$. Получим противоречие с предположением, что F не является сильно односторонней.

□

Часто в проложениях бывает так, что нельзя сделать так, чтобы функция была везде определена. (Например, функция, определенная только на произведении двух больших чисел.) Часто бывает нужно выбрать случайный элемент из области определения.

Definition 1.
Пусть μ_n - случайная величина со значениями в $\{0,1\}^{k(n)}$. Будем говорить, что μ_n - полиномиально вычислимая, если существует полиномиальный вероятностный алгоритм с пустым входом S такой, что $\forall x \in \{0,1\}^{k(n)}\ Pr\{S(\varepsilon) = x\} = Pr\{\mu_n = x\}$

Definition 2.
Статистическое расстояние: $dist(\mu_n, \nu_n) = max_{T \subset \{0,1\}^{k(n)}} |Pr\{\mu_n \; in T\} - Pr\{\nu_n \in T\}| = \sum_{x \; in \{0,1\}^{k(n)}} \frac{1}{2} |Pr\{\mu_n = x\} - Pr\{\nu_n = x\}|$

Definition 3.
μ_n доступна, если

$$\exists \nu_n \; \forall p(\cdot) \; \exists N \; \forall n > N dist(\mu_n, \nu_n) < \frac{1}{p(n)}$$

ν_n - полиномиально вычислима.

Definition 4.
$f \colon D \to \{0,1\}^n$ - частичная односторонняя функция есил:

- Равномерная случайная величина на D доступна
- f вычислима за полиномиальное время
- $\forall R_n \; \forall p(\cdot) \; \exists N \; \forall n > N \; Pr_{x \in D}\{R_n(f(x)) \in D, f(R_n(f(x))) = f(x)\} < \frac{1}{p(n)}$

Предположительные частично односторонние функции:

- Функция Рабина: $(x, y) \to (x^2 \; mod \; y, y)$
  $y = p \cdot q$
  p_n, q - простые вида $4k + 3$
  x - квадратичный вычет.
- Функция RSA: $(x, y, z) \to (x^z \; mod \; y, y, z)$ - извлечение корня степени z
  $y = p \cdot q$
  x - вычет, взаимно простый с y
  z - взаимно просто с $\phi(p \cdot q) = (p - 1)(q - 1)$
- Дискретная экспонента $(x, y, z) \to (x, y, x^z)$ - логарифм по основанию x.