Криптография, Лекция № 1

8 сентября 2014 г.

Definition 1.
Функция $f\colon \{0,1\}^{k(n)} \to \{0,1\}^{l(n)}$ называется сильно односторонней, если f вычисляется за время $poly(n)$ и

$$\forall p \forall \{Rn\}_{n=1}^{\infty} \exists N \forall n > N Pr_{x \in \{0,1\}^{k(n)}} \{f(Rn(f(x))) = f(x)\} < \frac{1}{p(n)}$$

Rn - семейства схем полиномиального размера

Definition 2.
Функция $f\colon \{0,1\}^{k(n)} \to \{0,1\}^{l(n)}$ называется слабо односторонней, если f вычисляется за время $poly(n)$ и

$$\exists q \forall \{Rn\}_{n=1}^{\infty} \exists N \forall n > N Pr_{x \in \{0,1\}^{k(n)}} \{f(Rn(f(x))) = f(x)\} < 1 - \frac{1}{q(n)}$$

Rn - семейства схем полиномиального размера

Remark 1.
Сильно односторонняя функция является слабо односторонней. Достаточно взять $p = 2$

Claim 1.
Если существует слабо одностороняя функция, то $P \neq NP$

Доказательство.
$L = \{y \in \{0,1\}^{l(n)} \colon \exists x \in \{0,1\}^{k(n)} f(x) = y\} \in NP$
Если $P = NP$, то соответсвующая задача поиска решается за полиномиальное время. А эта задача обращает $f(x)$. □

Claim 2.
Если f *- одностороння функция, то* $h(x) = f(x)0\ldots0$ *(*$l(n)$ *нулей) - односторонняя функция.*

Доказательство.
Дан y, хотим найти $x\colon f(x) = y$. Запишем y дополненный $l(n)$ нулями, обратим h, получим x. □

Claim 3.
Если f *- одностороння функция, то* $h(x) = f(x)f(x)$ *(конкатенация) - односторонняя функция.*

Доказательство.
Дан y, хотим найти $x\colon f(x) = y$. Запишем y два раза подряд, обратим g, получим x. $\square$

Definition 3.
Функция $f\colon \{0,1\}^{k(n)} \to \{0,1\}^{l(n)}$ называется сильно односторонней в вероятностной схеме, если f вычисляется за время $poly(n)$ и

$$\forall p \forall \{Rn\}_{n=1}^{\infty} \exists N \forall n > N Pr_{x \in \{0,1\}^{k(n)}, r}\{f(Rn(f(x), r)) = f(x)\} < \frac{1}{p(n)}$$

Rn - семейства схем полиномиального размера

Remark 2.
Сильно односторонняя функция является сильно односторонней в вероятностной схеме и наоборот

Примеры предположительно односторонних функций:

1. Умножение (слабо односторонняя функция)
   $f(x) = x \cdot y$
   $|x| = |y| = n$
2. SUBSET-SUM
   $(n_1, \ldots, n_k, s) \to (n_1, \ldots, n_k, N)$, $|s| = k$
   $N = \sum_{i\colon s_i = 1} n_i$

Claim 4.
Если существует сильно односторонняя функция, то существует слабо одностороняя функция, не являющаяся сильно односторонней.

Доказательство.
$g(x0) = f(x)0$
$g(x1) = x1$
Такая g - слабо односторонняя, ибо если ее можно обратить с вероятностью $\frac{2}{3}$, то ее можно обратить в первом случае с вероятностью $\frac{1}{3}$. Тогда и f можно обратить с такой вероятностью, а значит, f - не сильно односторонняя. $\square$

Theorem 1.
Если существует слабо одностороняя функция, то существвет сильно одностороняя функция.

Idea 1.
$F(x_1, \ldots, x_N) = f(x_1) \ldots f(x_N)$
Пусть обратитель F пытается обратить все компоненты по отдельности. Тогда вероятность успеха $\leq \left(1 - \frac{1}{q(n)}\right)^N = l^{-n}$

Доказательство.
Нужно по рбратиелю F построить обратитель f.
$S(y)\colon$ запуск $R(y, f(x_2), \ldots, f(x_N))$, проверка успешности
запуск $R(y, f(x_2), \ldots, f(x_N))$, проверка успешности
запуск $R(y, f(x_2), \ldots, f(x_N))$, проверка успешности

Достаточно доказать утверждение:

Claim 5.
Если R успешен с вероятностью $\geq \frac{1}{p(n)}$, то

$$\forall q \exists m S \text{успешен с вероятностью} \geq 1 - \frac{1}{q(n)}$$

$$S_1(x) = Pr_{x_2,\ldots,x_n}\{f(R_1(f(x), f(x_2), \ldots, f(x_N))) = f(x)\}$$

$$S_i(x) = Pr_{x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_N}\{f(R_1(f(x_1), \ldots, f(x_{i-1}), f(x), f(x_{i+1}), \ldots, f(x_N))) = f(x)\}$$

Вероятность успеша 1 шага $S \geq max\{S_1(x), \ldots, S_N(x)\}$

Idea 2.
Если $maxS_i(x) > \frac{1}{poly(n)}$, тогда за счет выбора m можно повысить вероятность успеха до $1 - \frac{1}{q(n)}$ таких x, что $maxS_i(x) < \frac{1}{poly(n)}$, мало.

□