Draft on WOWF ⇒ SOWF.

Monday, 12 October 2020 7:27 AM

Defn:

$$\Pr\left(x \leftarrow \{0,1\}^n;\ y \leftarrow f(x);\ x' \leftarrow A(1^n, y) : f(x') = f(x) \right)$$

is $neg(n)$.

Defn: Let p be a polynomial. f is p-weak oneway function if.

1) There exist an efficient c that on input x, returns $f(x)$.
2) For any Rand. Poly. A, for all suff. large n,

$$\Pr\left(x \leftarrow \{0,1\}^n, y = f(x), x' = A(1^n, y) ;\ f(x') \neq f(x) \right) \geqslant \frac{1}{p(n)}.$$

Strong: A succeeds with neg probability.
weak: A fails with decent probability. (noticeable).

---

weak ⇒ A succeeds with prob $\leq 1 - \frac{1}{p(n)}$.

strong ⇒ . . . $\leq \frac{1}{n^c}$ for any c.

Let $F = \{ f_n : n \in N \}$ be a collection of p-weak one-way fns;

Let $m = 2n^2 p(n)$.

$G = \{ g_m \}$ $\quad g_m : \{0,1\}^m \rightarrow \{0,1\}^m$

$$g(x_1, x_2, \ldots, x_{n2p(n)}) = (f_n(x_1) \cdot f_n(x_2) \cdots f_n(x_{n2p(n)}))$$

Assume, for the sake of contradiction, g is not one-way:

$\therefore \exists$ efficient adversary : A & a poly q.

$\ni$ $\Pr\left(x \leftarrow \{0,1\}^m, y \leftarrow g_m(x), x' = A(1^n, y) : g_m(x') = g_m(x) \right) \geqslant \frac{1}{q(m)}$.

Our goal is to construct A' (using A) that can invert f_n with probability $\geqslant 1 - \frac{1}{p(n)}$.

(This is a contradiction)

A': $y \in \{0,1\}^n$, $y = f_n(x)$ for a random x.

Repeat $4n^2 p(n) q(m)$ times.

For $i = 1$ to $2n\,p(n)$

Randomly choose $x_j \in \{0,1\}^n$

$j = 1, 2, \ldots i-1, i+1, \ldots 2n\,p(n)$

$y_j = f_n(x_j)$.

if A successfully inverts $(y_1, \ldots y_{i-1}, y, y_{i+1}, \ldots y_{2np(n)})$

then Let $(x_1, x_2, \ldots x_{i-1}, x_i, x_{i+1}, \ldots x_{2np(n)})$

Return x_i & halt.

$x \in \{0,1\}^n$ is bad if.

$\Pr($ single iteration of A' returns $f_n^{-1}(f_n(x))\ ) < \frac{1}{4n\,p(n)\,q(m)}$

Let $e(A', x)$ be the event that A' does not invert $f_n(x) = y$. (A' is run on y)

$$\Pr(e(A', x)) = \Pr(e(A', x) \mid x \in BAD) \cdot \Pr(x \in BAD) + \Pr(e(A', x) \mid x \notin BAD) \cdot \Pr(x \notin BAD)$$

$$\leq 1 \cdot \Pr(x \in BAD) + \left(1 - \frac{1}{4n\,p(n)\,q(m)}\right)^{4n^2 p(m) \cdot (q(m) \cdot)}$$

$$\leq \Pr(x \in BAD) + e^{-n}.$$

$$\left(1 - \frac{1}{t}\right)^t < e^{-1}$$

---

if we show $\Pr(x \in BAD) \leq \frac{1}{2p(n)}$

Then

$$\Pr(e(A', x)) \leq \frac{1}{2(p(n))} + e^{-n} \leq \frac{1}{2p(n)} + \frac{1}{2p(n)} = \frac{1}{p(n)}.$$

A' is poly and it fails to invert — with prob $< \frac{1}{p(n)}$ —

Contradiction to p-weakness of f_n.

Goal - $\Pr(x \in BAD) \leq \frac{1}{2p(n)}$.

Assume if possible

$$\Pr(x \in BAD) > \frac{1}{2(p(n))}.$$

$$\Pr(x \notin BAD) \leq 1 - \frac{1}{2p(n)}$$

$$\Pr(x_i \notin BAD)\ \forall i = 1, 2, \ldots 2n\,p(n) \leq \left(1 - \frac{1}{2p(n)}\right)^{2n\,p(n)} \leq e^{-n}$$

Hard core predicate: