Next bit predictor:

$f : \{0,1\}^n \to \{0,1\}^n$

$E(h_f) = \sum_{x' \in \{0,1\}^n} \left(h_f(x') \right)^2$

$\Pr\left(\text{dist}(x', x) = 1 \right)$.

$\Pr(\text{dist}(x', x) = 1)$ is the prob. with which x' is chosen.

If $h_f \to$ bit gen by f

$E(h_f) \to$ uniform bits.

$\left| E(h_f) - E(h_r) \right| \geq \frac{1}{2}$.

$f : \{0,1\}^n \to \{0,1\}^n$

random mod

$h_f(x_1, x_2)$

$\{x_1, \ldots, x_n\}$

Indexing a distribution on $\{x_i\}$, $1 \leq i \leq k$.

$h_f(x_1)^{x_2}$ $\quad z_2 = (x_1)^{x_2}$

z_1 the prob. distribution transformed by f on 2^n bits.

NBP : $\{z_1^{[i-1]}\} \to z_2$.

$(x_1, \ldots x_{i-1}) \to 1$

Given that $(x_1, \ldots x_{i-1})$ is generated by f,

$\left(\text{NBP}(x_1, \ldots x_{i-1}) = z_i \right) \Big| (x_1, \ldots x_{i-1})$

$\Pr(x_1, \ldots x_{i-1}) \cdot \Pr\left(\text{NBP}(\ldots) = z_i \right)$

for a specific input $(x_1, \ldots x_{i-1})$

Success prob of NBP.

Success prob of NBP.

$\sum_{(x_1, \ldots x_{i-1}) \in \{0,1\}^{i-1}} \Pr(x_1, \ldots x_{i-1}) \cdot \Pr\left(\text{NBP}(\ldots) = z_i \right)$

$\geq \frac{1}{2} + \frac{\epsilon}{2}$

The NBP is said to have ϵ - advantage.

$f : \{0,1\}^n \to \{0,1\}^n$.

Output from f is NBP with ϵ adv.

Then

h_f can be distinguished from h_r

NBP : $\{z_1^{[i-1]}\} \to z_2$.

2^{n^2} bit water.

?

Is this a good i^{th} bit pred. for h_f?

① $(x_1, \ldots x_{i-1})$ gen by f.

② z_i is the next bit gen by f.

③ if $\text{NBP}(x_1, \ldots x_{i-1}) = z_i$.

Then NBP is successful.

$\left(\frac{1}{2^{i-1}} \right)$

$h_f(1, 1, \ldots 1)$ $\quad z_i \left(1, 1, \ldots 1 \right)$

$\text{NBP}(1, 1, \ldots 1) \to z_i$.

$\text{NBP}(1, 1, \ldots 1)$

$\text{NBP}\left(z_1^{[i-1]} \right) = z_i$.

$g(x_1) = f(x)$.

$h(x) \to$

$\Pr(z_1 = 1) \left(x_1, x_2 \right)$

$z_1 \frac{2^n}{2^n} \left| \frac{2^n}{2^n} \right|$

$\Pr(z_1 = 1) \left(x_1, x_2 \right)$

$2^n \left\{ \begin{array}{l} \\ \\ \\ \end{array} \right.$

$\left(\begin{array}{l} x_1 \\ x_2 \\ \ldots \end{array} \right)