Pseudo random function

Wednesday, 22 February 2023 8:33 PM

We are given a PRNG G and we follow the construction

$$F_k(x_1 \cdots x_n) = G_{x_n}(G_{x_{n-1}} \cdots (G_{x_2}(G_{x_1}(k))))$$

Let $H_n = \{ F_k : k \in \{0,1\}^n \}$

H_0 has $F_k(x) = G_{x_n}(G_{x_{n-1}} \cdots G_{x_1}(s) \cdots)$

H_n has $F_k(x) = U_n$

H_1 has $F_k(x) = G_{x_n}(G_{x_{n-1}} \cdots G_{x_2}(U_n) \cdots)$

$\therefore$ H_i has $F_k(x) = G_{x_n}(G_{x_{n-1}} \cdots G_{x_{i+1}}(U_n)) \cdots)$

Let D be determiner that is give 1^n as input

H_n corresponds to uniform distribution

$$\therefore \left| \Pr_{k \leftarrow \{0,1\}^n}[D^{F_k(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1] \right|$$

$$= \left| \Pr_{f \leftarrow H_0^n}[D^{f(\cdot)}(1^n) = 1] - \Pr_{f \leftarrow H_n^n}[D^{f(\cdot)}(1^n) = 1] \right|$$

Now we show that for a algorithm A whose output is $D(\text{pref})$ for some prefix $x_1 \cdots x_{j+1}$ i.e A's output is a uniform $2^n \cdot (t(n))$ bit string.

$\therefore$

$$\Pr[A(r_1 \| \cdots r_{t(n)}) = 1] - \Pr[A(G(s_1) \| \cdots G(s_n)) = 1]$$

$$= \frac{1}{n} \cdot \left| \Pr_{f \leftarrow H_n^0}[D^{f(\cdot)}(1^n) = 1] - \Pr[D^{f(\cdot)}(1^n) = 1] \right|$$

LHS is negl $\therefore$ RHS is also negl

hence proved.