Assignment 1

2020111013

PRF

② PRF

Construction of PRF (F_k)

Let the PRG that F_k uses be G, defined as (for key k)

$$G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$$

$$F_k : \{0,1\}^n \rightarrow \{0,1\}^n$$

Let the input be ~~$x = x_n x_{n-1} x_{n-2}$~~ x, $x = x_1 x_2 x_3 \cdots x_{n-1} x_n$

Here G_0 & G_1 are defined as $G_i : \{0,1\}^n \rightarrow \{0,1\}^n \; \forall i \in \{0,1\}$

$$F_k(x) = G_{x_n}(G_{x_{n-1}}(G_{x_{n-2}}(\cdots(G_{x_2}(G_{x_1}(k)))\cdots)))$$

$G_0(x) \rightarrow$ left $(G(x))$ (take n bits to the left as output & discard rest)

$G_1(x) \rightarrow$ right $(G(x))$ (" " " " right " " " " ")

Proof of Security

Given that the input x, the random seed, is random, the algorithm will perform $G_0(x)$ or $G_1(x)$ randomly as well.

We also know that the G used is a provably secure pseudorandom generator.

$\therefore$ For an n-bit PRG output

$$\Pr[D(G_{x_n}(G_{x_{n-1}} \cdots (G_{x_2}(G_{x_1}(k))\cdots)] \leq \frac{1}{2^n} + negl(n)$$

↳ probability of guessing a random n-bit string

$\therefore$ Pr[Determining PRF] − Pr[Determining random string] $\leq negl(n)$

$\therefore$ The Given construction is a valid & secure PRF