Pseudo Random FUnction(PRF)

Sarthak Mahajan, 2018111005

March 7, 2022

1 Definition of PRF:

Let $F : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be an efficient, length-preserving, keyed function. We say that F is a pseudorandom function if for all probabilistic polynomial-time distinguishers D, there exists a negligible function neg such that:

$$\left|\Pr\left[D^{F_k(\cdot)}\left(1^n\right)=1\right]-\Pr\left[D^{f(\cdot)}\left(1^n\right)=1\right]\right| \leq n\,\mathrm{eg}(n),$$

where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random and f is chosen uniformly at random from the set of functions mapping n-bit strings to n-bit strings.

2 PRF from PRG

2.1 Building PRF using PRG:

Let G be a pseudorandom generator with expansion factor $\ell(n) = 2n$. Denote by $G_0(k)$ the first half of G 's output, and by $G_1(k)$ the second half of $G's$ output. For every $k \in \{0,1\}^n$, define the function $F_k : \{0,1\}^n \rightarrow \{0,1\}^n$ as:

$$F_k\left(x_1 x_2 \cdots x_n\right)=G_{x_n}\left(\cdots\left(G_{x_2}\left(G_{x_1}(k)\right)\right)\cdots\right).$$

2.2 THEOREM:

If G is a pseudorandom generator with expansion factor $(n) = 2n$, then the above construction is a pseudorandom function.

3 Provable security using PRF:

4 Idea:

We apply the pseudorandom function on some random number, rather than the message, in this way even if the adversary has access to the encryption server(CPA attack), he won't be able to decrypt as he doesn't have the random number that the pseudorandom function is being applied on. Since the PRF applied on this random number is XOR'ed with the message, and the adversary can't access this random number and the encryption of the message varies depending on this number(non-deterministic), the adversary won't be able to decrypt.

4.1 Provable CPA security using PRF:

Let F be a pseudorandom function. Define a private-key encryption scheme for messages of length n as follows:

- **Gen:** on input 1^n, choose $k \leftarrow \{0,1\}^n$ uniformly at random and output it as the key.
- **Enc:** on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, choose $r \leftarrow \{0,1\}^n$ uniformly at random and output the ciphertext

  $$c := \langle r, F_k(r) \oplus' m \rangle .$$

- **Dec:** on input a key $k \in \{0,1\}^n$ and a ciphertext $c = \langle r, s \rangle$, output the plaintext message

  $$m := F_k(r) \oplus s$$