

# Security of Symmetric Ciphers

Notes for CS555: Fall 2004

## 1 PRF and PRP

Readings: Sections 3.1–3.5 of Bellare&Rogaway

### 1.1 Function Families

- A *function family* is a map  $F : \mathcal{K} \times D \rightarrow R$ .  $\mathcal{K}$  is the *keyspace*,  $D$  the *domain*, and  $R$  the range of  $F$ .
- The function  $F_K : D \rightarrow R$  is defined by  $F_K(X) = F(K, X)$ . We call  $F_K$  an *instance* of  $F$ .
- Usually,  $\mathcal{K} = \{0, 1\}^k$ ,  $D = \{0, 1\}^\ell$ , and  $R = \{0, 1\}^L$ , where  $k$  is the *key length*,  $\ell$  the *input length*, and  $L$  the *output length*.
- $K \xleftarrow{\$} \mathcal{K}$  means that  $K$  is uniformly randomly chosen from  $\mathcal{K}$ . That  $f \xleftarrow{\$} F$  means that  $f$  is uniformly randomly chosen from  $F$ .
- A *permutation* is a bijection (i.e., a one-to-one onto map) whose domain and range are the same set.
- A block cipher is a family of permutations, e.g., DES:  $\{0, 1\}^{56} \times \{0, 1\}^{64} \rightarrow \{0, 1\}^{64}$ .

### 1.2 Random functions and permutations

- $\text{Func}(D, R)$  is the family of all functions mapping  $D$  to  $R$ .  $\text{Perm}(D)$  is the family of all permutations on  $D$ .

- $\text{Func}(\ell, L)$  is the family of all functions mapping  $\{0, 1\}^\ell$  to  $\{0, 1\}^L$ ;  $\text{Func}(\ell)$  is the family of all functions mapping  $\{0, 1\}^\ell$  to  $\{0, 1\}^\ell$ ; and  $\text{Perm}(\ell)$  is the family of all permutations on  $\{0, 1\}^\ell$ .
- The keyspace for  $\text{Func}(\ell, L)$  is:

$$\text{Keys}(\text{Func}(\ell, L)) = \{(Y_1, \dots, Y_{2^\ell}) : Y_1, \dots, Y_{2^\ell} \in \{0, 1\}^L\}$$

The size of this keyspace is  $2^{L2^\ell}$ , and the key length is  $L2^\ell$ .

- A random function  $g$  mapping  $\{0, 1\}^\ell$  to  $\{0, 1\}^L$  is a random instance of  $\text{Func}(\ell, L)$ , i.e.,  $g \xleftarrow{\$} \text{Func}(\ell, L)$ . How to implement such a function?  
A random function means that the function is chosen randomly. The function itself is deterministic.
- Look at Example 3.3.
- The keyspace for  $\text{Perm}(\ell)$ ,  $\text{Keys}(\text{Perm}(\ell))$ , is:

$$\{(Y_1, \dots, Y_{2^\ell}) : Y_1, \dots, Y_{2^\ell} \in \{0, 1\}^\ell \text{ and } Y_1, \dots, Y_{2^\ell} \text{ are distinct}\}$$

The keyspace has size  $2^\ell!$ .

- How to implement a random permutation on  $\{0, 1\}^\ell$ , i.e., a random instance of  $\text{Perm}(\ell)$ .
- Look at example 3.5.

### 1.3 Pseudorandom functions

- A *pseudorandom* function is a family  $F$  of functions with the property that the input-output behavior of a random instance of the family is “computationally indistinguishable” from that of a random function.
- Consider the following scenario of distinguishing the following two worlds: one with a random function (i.e.,  $g \xleftarrow{\$} \text{Func}(D, R)$ ), the other with a function drawn at random from  $F$ , a function family mapping  $D$  to  $R$ .
- Consider an adversary  $A$  with oracle access to a function  $g$ . An adversary is a probabilistic algorithm (Turing Machine).

- The *prf-advantage* of an adversary  $A$ .

$$\mathbf{Adv}_F^{\text{prf}}(A) = \Pr[\mathbf{Exp}_F^{\text{prf}-1}(A) = 1] - \Pr[\mathbf{Exp}_F^{\text{prf}-0}(A) = 1]$$

- An alternative way of defining the advantage: a game between a Challenger and an adversary:

1. The Challenger chooses  $b \xleftarrow{\$} \{0, 1\}$ , and let  $g \xleftarrow{\$} \text{Func}(D, R)$  if  $b = 0$ , and let  $g \xleftarrow{\$} F$  if  $b = 1$ .
2. The Challenger then interacts with the adversary  $A$ , it evaluates  $g$  for the adversary at each point the adversary queries.
3. The adversary  $A$  outputs  $b' \in \{0, 1\}$  and wins if  $b' = b$ .

The advantage is defined to be  $|\Pr[A \text{ wins}] - 0.5|$ .

- We say that a function family  $F$  is a “secure” PRF if, under certain resource restrictions, no adversary has a “significant” advantage.

## 1.4 Pseudorandom permutations

- PRP under CPA: Given a family  $F$  of permutations on  $D$ , consider an adversary that is given oracle access to a function  $g$ , which is either a random permutation on  $D$  or a random instance of  $F$ , the adversary is asked to tell whether  $g$  is taken from  $F$ .

Models chosen-plaintext attack against a cipher; however, the objective of the attack is to tell whether it is random.

- PFP under CCA: Similar to the CPA case, but the adversary has access to two oracles:  $g$  and  $g^{-1}$ .

Models chosen-ciphertext (and chosen-plaintext) attack against a cipher.

- PRP-CCA implies PRP-CPA

## 1.5 Modeling block ciphers

- Security against key recovery attack is insufficient.
- Conjecture DES and AES are PRP with some parameters.