CS655: Cryptography **Feb 13, 2007**

More on PRF and PRP

1 PRF Revisited

Applications PRF can be used to build symmetric encryption schemes as well as MAC. A construction for encryption is $E_k[M] = [F_k(R) \oplus M, R]$. If F is a PRF, then E is semantically secure.

GGM Construction of PRF from PRNG Let $G : \{0,1\}^s \to \{0,1\}^{2s}$ be a PRNG. Let $G_0(x)$ denote the first half of $G(x)$ and $G_1(x)$ the second half. Define

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

Theorem 1 *If G is a (t,ϵ)-PRNG, then F is a $(t - cn, eqn, q)$-PRF for some constant c.*

MAC and PRF

- PRF's are MAC's.
- MAC's do not need to be PRF's.

Unpredictable functions

Definition 1 *A function $F : \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^T$ is a (t,ϵ,q) unpredictable function (UF) if*

1. *Given $k \in \{0,1\}^s$, $F_k(x)$ can be efficiently evaluated.*
2. *For all t-time algorithms that make at most q queries to F,*

$$\mathsf{Pr}\left[F_k(M) = \mathit{Tag} \mid k \xleftarrow{\$} \{0,1\}^s; (M, \mathit{Tag}) \leftarrow A^{F_k}\right] < \epsilon$$

Deterministic MAC's are UF's. PRF's are UF's. PRF can be constructed from UF.

2 PRP Revisited

We use Strong PRP (SPRP) to denote PRP under chosen ciphertext attacks, and PRP to denote PRP under chosen plaintext attacks.

Definition 2 (Feistel Permutation) *Let $L, R \in \{0,1\}^n$ and $f : \{0,1\}^n \to \{0,1\}^n$. Define*

$$D_f(L,R) = (R, L \oplus f(R))$$

Then $D_f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is a permutation.

Theorem 2 (Luby-Rackoff (88)) . *If* $f : \{0,1\}^n \times \{0,1\}^s \rightarrow \{0,1\}^n$ *is a* (t, ϵ, q)*-PRF, then*

$$E_{k_1,k_2,k_3} = D_{f_{k_1}} \cdot D_{f_{k_2}} \cdot D_{f_{k_3}}$$

is a $(t, \epsilon + (q^2/2^n), q)$*-PRP. And*

$$E_{k_1,k_2,k_3,k_4} = D_{f_{k_1}} \cdot D_{f_{k_2}} \cdot D_{f_{k_3}} \cdot D_{f_{k_4}}$$

is a $(t, \epsilon + (q^2/2^n), q)$*-SPRP.*

Constructing PRFs from PRPs PRPs can be used as PRFs, but suffers from the birthday attack.