Notes from CS 6260 (Applied Cryptography) Georgia Tech, Fall 2012

Christopher Martin chris.martin@gatech.edu

1 Symmetric cryptography scheme

 $\begin{array}{c|c} \text{Key space} & \mathcal{G} \\ \text{Message space} & \mathcal{M} \\ \text{Cypher space} & \mathcal{C} \\ \text{Key generator} & \text{Gen}: \phi \to \mathcal{G} \\ \text{Encryption function} & \text{Enc}: \{\mathcal{G} \times \mathcal{M}\} \to \mathcal{C} \\ \text{Decryption function} & \text{Dec}: \{\mathcal{G} \times \mathcal{C}\} \to \mathcal{M} \\ \end{array}$

2 Information theoretic security

Information theoretic security repels even resource-unbounded attackers. Shannon secrecy and perfect secrecy are equivalent definitions of information theoretic security for symmetric cryptography schemes.

Shannon secrecy A scheme is Shannon-secret with respect to the distribution D over \mathcal{M} iff the ciphertext reveals no additional information about the message.

$$\forall\,M\in\mathcal{M},\,C\in\mathcal{C}:\,\Pr_{\substack{k\in\mathsf{Gen}\\m\in D}}\left[\,m=M\,|\,\mathsf{Enc}_k(m)=C\,\right]=\Pr_{m\in D}\left[\,m=M\,\right]$$

Perfect secrecy A scheme is perfectly secret iff the distributions of ciphertexts for any two messages are identical.

$$\forall\, M_1,M_2\in\mathcal{M},\,C\in\mathcal{C}:\,\Pr_{K_1\in\operatorname{Gen}}\left[\,\operatorname{Enc}_{K_1}(M_1)=C\,\right]=\Pr_{K_2\in\operatorname{Gen}}\left[\,\operatorname{Enc}_{K_2}(M_2)=C\,\right]$$

This model considers only a single message and ciphertext, so although a one-time pad it perfectly secret, a "two-time pad" is not.

Perfect secrecy $\Rightarrow |\mathcal{K}| \geq |\mathcal{M}|$. Proof idea: If not, \exists 2 messages with different probabilities of encrypting to the same cypertext.

3 Pseudo-random functions

Uniformly random function U is a random variable chosen uniformly from the set of all functions $\{0,1\}^m \to \{0,1\}^n$.

Pseudo-random function A PRF belongs to a family of functions $F: \{0,1\}^{\ell} \times \{0,1\}^{m} \to \{0,1\}^{n}$. Write $F_{k}(\cdot)$ to denote $F(k,\cdot)$.

DES
$$\ell=56$$
 $m=64$ $n=64$ Dimensions of some well-known AES₁₂₈ $\ell=128$ $m=128$ $n=128$ PRFs AES₁₉₂ $\ell=192$ $m=128$ $n=128$

Distinguishing advantage Consider an adversary A who knows F, having oracle access to F_k where k was chosen uniformly at random, trying to distinguish the oracle's responses from a random function. The distinguishing advantange of A against F is

$$\mathrm{Adv}_F^{\mathrm{prf}}(A) = \Pr_{k \in \{0,1\}^\ell} \left[\, A^{F_k(\cdot)} \, \operatorname{accepts} \, \right] - \Pr_U \left[\, A^{U(\cdot)} \, \operatorname{accepts} \, \right]$$

 (t, q, ε) -secure PRF A PRF F is (t, q, ε) -secure iff any adversary A, bounded by time t and number of queries q, has advantage $\leq \varepsilon$.

$$\begin{array}{c|c} t & 2^{128} & \text{Examples of reasonable constants} \\ q & 2^{64} \text{ or } 2^{32} \\ \varepsilon & 2^{-128} \end{array}$$