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

Christopher Martin
chris.martin@gatech.edu

1 Symmetric cryptography scheme

Key space	$\mathcal{G}$
Message space	$\mathcal{M}$
Cypher space	$\mathcal{C}$
Key generator	$\mathsf{Gen} : \phi \to \mathcal{G}$
Encryption function	$\mathsf{Enc} : \{\mathcal{G} \times \mathcal{M}\} \to \mathcal{C}$
Decryption function	$\mathsf{Dec} : \{\mathcal{G} \times \mathcal{C}\} \to \mathcal{M}$

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.

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

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

Theorem 1. Perfect secrecy $\Rightarrow |\mathcal{K}| \geq |\mathcal{M}|$.

Proof. If not, $\exists$ 2 messages with different probabilities of encrypting to the same cypertext. $\square$

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
AES_{128}	$\ell = 128$	$m = 128$	$n = 128$	PRFs
AES_{192}	$\ell = 192$	$m = 128$	$n = 128$	

Distinguishing advantage Consider an adversary $\mathcal{A}$ 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 $\mathcal{A}$ against F is

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

In time $O(t)$, we can brute-force t keys to get advantage $t/2^\ell$.

(t, q)-bounded adversary

t	Running time
q	Number of queries

(t, q, ε)-secure PRF F is (t, q, ε)-secure iff $\forall$ (t, q)-bounded $\mathcal{A}$,

$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \varepsilon .$$

t	2^{128}	Examples of reasonable constants
q	2^{64} or 2^{32}	
ε	2^{-128}	

The existence of secure PRFs has not been proven, but there are some functions that have never been broken and are widely assumed to be PRFs.

4 Reduction

Karp (many-to-one) reduction Reduction from A to B transforms an instance of A to an instance of B.

Cook (Turing) reduction Reduction from A to B solves A using a subroutine that solves B.

Key recovery security F is (t, q, ε)-kr-secure iff $\forall$ (t, q)-bounded $\mathcal{A}$,

$$\mathrm{Adv}_F^{\mathrm{kr}} \equiv \Pr_{k \in \{0,1\}^\ell} \left[\mathcal{A}^{F_k(\cdot)} \text{ outputs } k \right] \leq \varepsilon \ .$$

Theorem 2. If F is a (t, q, ε)-secure PRF for $q < 2^m$, then F is (t', q', ε')-kr-secure for $t' \approx t$, $q' = q - 1$, $\varepsilon' = \epsilon + 2^{-n}$.

Proof. Cook reduction. For any kr-adversary $\mathcal{A}'$ running in time t' and making $q' < 2^m$ queries, let $\mathcal{A}$ be the PRF adversary:

$k' \leftarrow \mathcal{A}'(\mathcal{O})$
$x \leftarrow$ a value that $\mathcal{A}'$ did not query with
$y \leftarrow \mathcal{O}(x)$
Accept iff $y = F_{k'}(x)$

$\mathcal{A}$ runs in time $t \approx t'$ and makes $q = q' + 1$ queries.

$$\mathrm{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \geq \mathrm{Adv}_F^{\mathrm{kr}}(\mathcal{A}') - 2^{-n} \ . \qquad \square$$