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

Christopher Martin
chris.martin@gatech.edu

1 Symmetric cryptography scheme

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

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.

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

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

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

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 $F(k, \cdot)$.

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

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

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 $\mathcal{A}$,

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

Examples of reasonable constants

t	2^{128}
q	2^{64} or 2^{32}
ε	2^{-128}

Existence 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.

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

Example PRF construction For PRF $F : \{0,1\}^\ell \times \{0,1\}^n \to \{0,1\}^n$, $F'_k(x) \equiv F_k(F_k(x)) \| F_k(\overline{F_k(\overline{x})})$

Theorem 3. F' is $(t, \frac{q}{3}, \varepsilon + \frac{q^2}{2^n})$-secure.

Proof. Let $\mathcal{A}'$ be an attacker on F'. Define $\mathcal{A}$ as:

$\mathcal{O}' \equiv \mathcal{O}(\mathcal{O}(x)) \| \mathcal{O}(\overline{\mathcal{O}(\overline{x})})$ (done with 3 queries to $\mathcal{O}$)
Accept iff $\mathcal{A}'^{\mathcal{O}'}$ accepts

$\mathcal{O}'(x)$ simulates F' perfectly, so $\Pr_k \left[\mathcal{A}^{F_k} \right] = \Pr_k \left[\mathcal{A}'^{F'_k} \right]$.

$\mathcal{O}'$ does not simulate U perfectly, but it is close. We have independence as long as all of the $\mathcal{O}(x)$, $\overline{\mathcal{O}(\overline{x})}$ are distinct. Using union bound, this probability $\leq \frac{q^2}{2^n}$ $\square$

5 Pseudo-random permutations

In a permutation family $F : \{0,1\}^\ell \times \{0,1\}^n \to \{0,1\}^n$, every F_k is bijective.

A secure PRP is computationally indistinguishable from a uniformly random permutation.

Some well-known PRPs

DES	$\ell = 56$	$n = 64$
AES_{128}	$\ell = 128$	$n = 128$
AES_{192}	$\ell = 192$	$n = 128$

Strong PRP / block cipher Attackers with oracle access to both F and F^{-1} have small advantage.

$$\mathrm{Adv}_F^{\mathrm{sprp}} \equiv \Pr_k\left[\mathcal{A}^{F_k, F_k^{-1}} \text{ accepts}\right] - \Pr_P\left[\mathcal{A}^{P,P^{-1}} \text{ accepts}\right] \le \varepsilon$$

PRF/PRP switching lemma If G is a (t, q, ε)-secure PRP (not necessarily strong), then F is a $(t, q, \varepsilon + \frac{q^2}{2^{n+1}})$-secure PRF.

6 Secure symmetric encryption

Perfect secrecy is impossible where $m > \ell$, but computational security is possible with pseudorandom objects.

Electronic code block (ECB) Suppose F is a secure PRP $\{\mathtt{0},\mathtt{1}\}^\ell \times \{\mathtt{0},\mathtt{1}\}^n \to \{\mathtt{0},\mathtt{1}\}^n$ with F and F^{-1} efficiently computable.

Gen	$k \leftarrow \{\mathtt{0},\mathtt{1}\}^\ell$
Enc	$M' \leftarrow$ Pad message M with $\mathtt{1}$ and some $\mathtt{0}$s to a multiple of n. Break M' into n-bit blocks $m_0, m_1, \ldots$ Apply F_k to each of the $\{m\}$
Dec	Apply F_k' to each of the $\{m\}$

Repeated blocks give repeated ciphertext. Never use ECB.

Security model Adversary, seeing all cipthertexts and having oracle access to Enc_k, learns nothing about plaintexts (except message length, which is unavoidable).

$SE = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is (t, σ, ε)-IND-CPA secure ("indistinguishable under chosen-plaintext attack") iff $\forall$ (t, σ)-bounded $\mathcal{A}$,

$$\mathrm{Adv}_{SE}^{\mathrm{indcpa}}(\mathcal{A}) \equiv \Pr_{k \leftarrow \mathsf{Gen}}\left[\mathcal{A}^{L_k} \text{ accepts}\right] - \Pr_{k \leftarrow \mathsf{Gen}}\left[\mathcal{A}^{R_k} \text{ accepts}\right] ,$$

$$L_k(m, m') \equiv \mathsf{Enc}_k(m) \text{ if } |m| = |m'| \text{ else } \perp ,$$

$$R_k(m, m') \equiv \mathsf{Enc}_k(m') \text{ if } |m| = |m'| \text{ else } \perp ,$$

t is the running time, and σ total length of all message queries.

Equivalent definition: Enc_k is computationally indistinguishable from a zero-encrypting oracle $Z_k \equiv \mathsf{Enc}_k(\mathsf{0}^m)$.

Stateful counter mode (CTRS) Let F be a PRF with $m = n$.

Gen	$k \leftarrow \{\mathsf{0}, \mathsf{1}\}^\ell$, *counter* $\leftarrow 0$

Enc	echo *counter*
	for each message block m:
	    echo $F_k(\mathit{counter}) \oplus m_i$
	    increment *counter*

If F is a (t, q, ε)-secure PRF, then CTRS(F) is $(t' \approx t, qn, 2\varepsilon)$-IND-CPA secure.