

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	$\text{Gen} : \phi \rightarrow \mathcal{K}$
Encryption function	$\text{Enc} : \{\mathcal{K} \times \mathcal{M}\} \rightarrow \mathcal{C}$
Decryption function	$\text{Dec} : \{\mathcal{K} \times \mathcal{C}\} \rightarrow \mathcal{M}$

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.

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

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

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

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 ciphertext. \square

3 Pseudo-random functions

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

Pseudo-random function A PRF belongs to a family of functions $F : \{0, 1\}^\ell \times \{0, 1\}^m \rightarrow \{0, 1\}^n$. 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 advantage of \mathcal{A} against F is

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

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

(t, q) -bounded adversary $\begin{array}{l|l} t & \text{Running time} \\ q & \text{Number of queries} \end{array}$

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

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

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

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} ,

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

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

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.

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

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

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:

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

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

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

5 Pseudo-random permutations

In a permutation family $F : \{0, 1\}^\ell \times \{0, 1\}^n \rightarrow \{0, 1\}^n$, 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.

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

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 $\{0, 1\}^\ell \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ with F and F^{-1} efficiently computable.

Gen	$k \leftarrow \{0, 1\}^\ell$
Enc	$M' \leftarrow \text{Pad message } M \text{ with 1 and some 0s to a multiple of } n.$ Break M' into n -bit blocks m_0, m_1, \dots 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 ciphertexts and having oracle access to Enc_k , learns nothing about plaintexts (except message length, which is unavoidable).

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

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

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

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

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 $Z_k \equiv \text{Enc}_k(0^m)$.

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

Gen	$k \leftarrow \{0, 1\}^\ell, \text{ counter} \leftarrow 0$
Enc	echo <i>counter</i> for each message block m : echo $F_k(\text{counter}) \oplus m_i$ increment <i>counter</i>

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