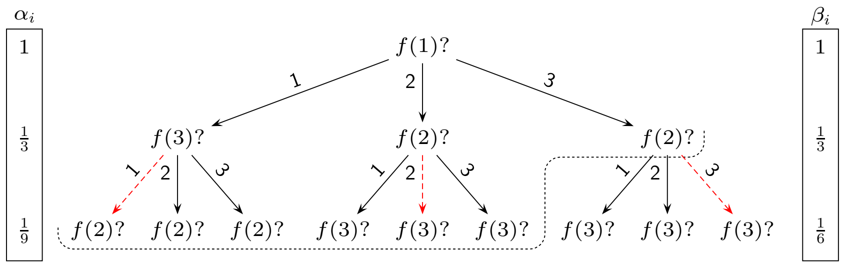
MTAT.07.003 Cryptology II
Spring 2008 / Homework 3

PRP/PRF switching lemma



1. Let $\mathcal{A}$ be the adversary that tries to distinguish a random permutation $f : \{1, 2, 3\} \to \{1, 2, 3\}$ from a random function $f : \{1, 2, 3\} \to \{1, 2, 3\}$ according to the adaptive querying strategy depicted above. The dashed line corresponds to the decision border, where $\mathcal{A}$ stops querying and outputs his or her guess.

   (a) Compute the following probabilities

   $$\Pr[f \leftarrow \mathcal{F}_{\text{all}} : \mathcal{A} \text{ reaches vertex } u] \enspace ,$$
   $$\Pr[f \leftarrow \mathcal{F}_{\text{all}} : \mathcal{A} \text{ reaches vertex } u \wedge \neg\mathsf{Collision}] \enspace ,$$
   $$\Pr[f \leftarrow \mathcal{F}_{\text{all}} : \neg\mathsf{Collision}] \enspace ,$$
   $$\Pr[f \leftarrow \mathcal{F}_{\text{all}} : \mathcal{A} \text{ reaches vertex } u|\neg\mathsf{Collision}] \enspace ,$$
   $$\Pr[f \leftarrow \mathcal{F}_{\text{prm}} : \mathcal{A} \text{ reaches vertex } u]$$

   for all nodes u in the decision border.

   (b) Compute these probabilities for an arbitrary message space $\mathcal{M}$ under the assumption that $\mathcal{A}$ makes exactly q queries and conclude

   $$\Pr[\mathcal{A} = 0|\mathcal{F}_{\text{all}} \wedge \neg\mathsf{Collision}] = \Pr[\mathcal{A} = 0|\mathcal{F}_{\text{prm}}] \enspace .$$

2. For the proof of the PRP/PRF switching lemma, consider the following games. In the game $\mathcal{G}_0$, the challenger first draws $f \leftarrow \mathcal{F}_{\text{all}}$ and then answers up to q distinct queries. In the game $\mathcal{G}_1$, the challenger draws $f \leftarrow \mathcal{F}_{\text{prm}}$ and then answers up to q distinct queries. In both games, the output is determined by the adversary $\mathcal{A}$ who submits its final verdict.

   (a) Formalise both games as short programs, where $\mathcal{G}$ can make oracle calls to $\mathcal{A}$. For example, something like

$$
\begin{array}{l}
\mathcal{G}_0^{\mathcal{A}} \\
\left[\begin{array}{l}
f \xleftarrow[u]{} \mathcal{F}_{\mathrm{all}} \\
y_0 \leftarrow \bot \\
\quad \text{For } i \in \{1, \dots, q\} \text{ do} \\
\quad \left[\begin{array}{l}
x_i \leftarrow \mathcal{A}(y_{i-1}) \\
\text{If } x_i = \bot \text{ then break the cycle} \\
y_i \leftarrow f(x_i)
\end{array}\right. \\
\mathsf{return}\ \mathcal{A}
\end{array}\right.
\end{array}
$$

(b) Rewrite both games so that there are no references to the function f but the behaviour does not change. Denote these games by $\mathcal{G}_2, \mathcal{G}_3$.

(c) Analyse what is the probability that execution in the games $\mathcal{G}_2$ and $\mathcal{G}_3$ starts to diverge. Conclude $\mathsf{sd}_\star(\mathcal{G}_2, \mathcal{G}_3) = \Pr[\mathsf{Collision}]$

Hint: Note that following code fragment samples uniformly permutations

$$
\begin{array}{l}
\text{Sample } f(x_i) \\
\left[\begin{array}{l}
y_i \xleftarrow[u]{} \mathcal{M} \\
\quad \text{If } y_i \in \{y_1, \dots, y_{i-1}\} \text{ then} \\
\quad \left[\, y_i \xleftarrow[u]{} \mathcal{M} \setminus \{y_1, \dots, y_i\} \right.
\end{array}\right.
\end{array}
$$

What is the probability we ever reach the if branch?

3. Let $y_1, \dots, y_q$ be chosen uniformly and independently from the set $\mathcal{M}$. Let $\mathsf{Distinct}(k)$ denote the event that $y_1, \dots, y_k$ are distinct. Estimate the value of $\Pr[\mathsf{Distinct}(k) | \mathsf{Distinct}(k-1)]$ and this result to prove

$$\Pr[\mathsf{Distinct}(k)] \leq e^{-q(q-1)/(2|\mathcal{M}|)}$$

How one can use this result to prove the birthday bound

$$\Pr[\mathsf{Collision} | q \text{ queries}] \geq 0.316 \cdot \frac{q(q-1)}{|\mathcal{M}|} \quad .$$

Hint: Note that $1 - x \leq e^{-x}$.
Hint: Note that $1 - e^{-x} \geq (1 - e^{-1})x$ if $x \in [0, 1]$.

Computational indistinguishability

4. The IND-CPA security notion is also applicable for symmetric cryptosystems. Namely, a symmetric cryptosystem $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is (t, ε)-IND-CPA secure, if for any t-time adversary $\mathcal{A}$:

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}(\mathcal{A}) = |\Pr[\mathcal{Q}_0^{\mathcal{A}} = 1] - \Pr[\mathcal{Q}_1^{\mathcal{A}} = 1]| \leq \varepsilon$$

where

$$\begin{array}{ll}
\mathcal{Q}_0^{\mathcal{A}} & \mathcal{Q}_0^{\mathcal{A}} \\
\left[\begin{array}{l} \mathsf{sk} \leftarrow \mathsf{Gen} \\ (m_0, m_1) \leftarrow \mathcal{A}^{\mathcal{O}_1(\cdot)} \\ \mathsf{return}\ \mathcal{A}^{\mathcal{O}_1(\cdot)}(\mathsf{Enc}_{\mathsf{sk}}(m_0)) \end{array}\right. & \left[\begin{array}{l} \mathsf{sk} \leftarrow \mathsf{Gen} \\ (m_0, m_1) \leftarrow \mathcal{A}^{\mathcal{O}_1(\cdot)} \\ \mathsf{return}\ \mathcal{A}^{\mathcal{O}_1(\cdot)}(\mathsf{Enc}_{\mathsf{sk}}(m_1)) \end{array}\right.
\end{array}$$

and the oracle $\mathcal{O}_1$ serves encryption calls.

Estimate computational distance between following games

(a) Left-or-right games

$$\begin{array}{ll}
\mathcal{G}_0^{\mathcal{A}} & \mathcal{G}_1^{\mathcal{A}} \\
\left[\begin{array}{l} \mathsf{sk} \leftarrow \mathsf{Gen} \\ \quad \text{For } i = 1, \ldots, q \text{ do} \\ \quad \left[\begin{array}{l} (m_0^i, m_1^i) \leftarrow \mathcal{A} \\ \text{Give } \mathsf{Enc}_{\mathsf{sk}}(m_0^i) \text{ to } \mathcal{A} \end{array}\right. \\ \mathsf{return} \text{ the output of } \mathcal{A} \end{array}\right. & \left[\begin{array}{l} \mathsf{sk} \leftarrow \mathsf{Gen} \\ \quad \text{For } i = 1, \ldots, q \text{ do} \\ \quad \left[\begin{array}{l} (m_0^i, m_1^i) \leftarrow \mathcal{A} \\ \text{Give } \mathsf{Enc}_{\mathsf{sk}}(m_1^i) \text{ to } \mathcal{A} \end{array}\right. \\ \mathsf{return} \text{ the output of } \mathcal{A} \end{array}\right.
\end{array}$$

(b) Real-or-random games

$$\begin{array}{ll}
\mathcal{G}_0^{\mathcal{A}} & \mathcal{G}_1^{\mathcal{A}} \\
\left[\begin{array}{l} \mathsf{sk} \leftarrow \mathsf{Gen} \\ \quad \text{For } i = 1, \ldots, q \text{ do} \\ \quad \left[\begin{array}{l} m^i \leftarrow \mathcal{A} \\ \text{Give } \mathsf{Enc}_{\mathsf{sk}}(m^i) \text{ to } \mathcal{A} \end{array}\right. \\ \mathsf{return} \text{ the output of } \mathcal{A} \end{array}\right. & \left[\begin{array}{l} \mathsf{sk} \leftarrow \mathsf{Gen} \\ \quad \text{For } i = 1, \ldots, q \text{ do} \\ \quad \left[\begin{array}{l} m_0^i \leftarrow \mathcal{A}, m_1^i \xleftarrow{u} \mathcal{M} \\ \text{Give } \mathsf{Enc}_{\mathsf{sk}}(m_1^i) \text{ to } \mathcal{A} \end{array}\right. \\ \mathsf{return} \text{ the output of } \mathcal{A} \end{array}\right.
\end{array}$$

5. Show that the Goldwasser-Micali cryptosystem is IND-CPA secure if the Quadratic Residuosity Problem is hard. All necessary concepts are defined below. The proof is similar to the analysis of the ElGamal cryptosystem.

Number theory. A prime p is a Blum prime if $p \equiv 3 \mod 4$. Let $N = pq$ where p, q are Blum primes. Then for each element $a \in \mathbb{Z}_N$, we can efficiently compute the Jacobi symbol $(\frac{a}{n})$. One can show that Jacobi symbols satisfies following equations

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\cdot\left(\frac{b}{n}\right) \qquad \text{and} \qquad \left(\frac{a^2}{n}\right) = 1\ .$$

In the following, we also need a set

$$J_N(1) = \left\{x \in \mathbb{Z}_N : \left(\frac{x}{n}\right) = 1\right\}\ .$$

Finally, recall that an element b is a quadratic residue if there exists a such that $b = a^2 \mod N$. The set of quadratic residues is denoted by QR_N.

Quadratic residuosity problem. Let $\mathbb{P}_n$ denote uniform distribution over n-bit Blum primes. We say that the set of n-bit Blum primes is (t, ε)-secure with respect to quadratic residuosity problem if for all t-time adversaries $\mathcal{A}$:

$$\mathsf{Adv}^{\mathsf{qrp}}_{\mathbb{P}_n}(\mathcal{A}) = |\Pr[\mathcal{Q}_0^{\mathcal{A}} = 1] - \Pr[\mathcal{Q}_0^{\mathcal{A}} = 1]| \le \varepsilon$$

where

$$\begin{array}{ll}
\mathcal{Q}_0^{\mathcal{A}} & \mathcal{Q}_1^{\mathcal{A}} \\
\left[\begin{array}{l} p, q \xleftarrow[u]{} \mathbb{P}(n) \\ N \leftarrow pq \\ x \xleftarrow[u]{} QR_N \\ \mathsf{return}\ \mathcal{A}(x) \end{array}\right. & \left[\begin{array}{l} p, q \xleftarrow[u]{} \mathbb{P}(n) \\ N \leftarrow pq \\ x \xleftarrow[u]{} J_N \setminus QR_N \\ \mathsf{return}\ \mathcal{A}(x) \end{array}\right.
\end{array}$$

Goldwasser-Micali cryptosystem.

- **Key generation.** Sample primes $p, q \in \mathbb{P}(n)$ and choose quadratic non-residue $y \in J_N(1)$ modulo $N = pq$. Set $\mathsf{pk} = (N, y)$, $\mathsf{sk} = (p, q)$.
- **Encryption.** First choose a random $x \leftarrow \mathbb{Z}_N^*$ and then compute

$$\mathsf{Enc}_{\mathsf{pk}}(0) = x^2 \mod N \quad \text{and} \quad \mathsf{Enc}_{\mathsf{pk}}(1) = yx^2 \mod N.$$

- **Decryption.** Output 0 if the ciphertext c is quadratic residue and 1 otherwise. The latter is easy if the factorisation of N is known.

6. Recall that a block cipher is modelled as a (t, q, ε)-pseudo-random permutation family $\mathcal{F}$. As such it is perfect for encrypting a single message block. To encrypt longer messages, we have to use encryption modes that can handle multiple blocks. Three most common encryption modes are following:

ECB: The electronic codebook mode uses the same permutation $f \leftarrow \mathcal{F}$ for all message blocks:

$$\text{ECB}_f(m_1\|\ldots\|m_n) = f(m_1)\|\ldots\|f(m_n)\ .$$

- The counter encryption mode uses the permutation $f \leftarrow \mathcal{F}$ as a pseudo-random generator

$$\textsc{Ctr}_f(m_1\| \ldots \|m_n) = f(1) \oplus m_1\| \ldots \|f(n) \oplus m_n \enspace .$$

- The cipher-block chaining mode uses the permutation $f \leftarrow \mathcal{F}$ to link plaintext and ciphertexts

$$\textsc{Cbc}_f(m_1\| \ldots \|m_n) = c_1\| \ldots \|c_n \qquad \text{where} \qquad c_i = f(m_i \oplus c_{i-1})$$

  and c_0 is know as initialisation vector (nonce).

Let us now analyse the security of these working modes.

(a) Show that the Ecb working mode is insecure, i.e., construct a distinguisher that can distinguish $\textsc{Ecb}_f : \mathcal{M}^n \to \mathcal{M}^n$ from random permutation over $\mathcal{M}^n$. Is this weakness relevant in practise or not?

(b) Show that the Ctr working mode is secure. More precisely, show that the sequence $f(1)\| \ldots \|f(n)$ is indistinguishable from the uniform distribution over $\mathcal{M}^n$. Conclude that Ctr working mode is secure for a single encryption query. How to make it secure for many encryption queries? What are the corresponding security guarantees?

($\star$) Show that the Cbc working mode is secure. Again, show that the output is indistinguishable from the uniform distribution over $\mathcal{M}^n$. How to make it secure for many encryption queries? What are the corresponding security guarantees?

($\star$) We say that a cryptosystem is (t, ε)-IND-FPA (indistinguishable in fixed plaintext attacks) if for all t-time adversaries

$$\mathsf{Adv}^{\mathsf{ind\text{-}fpa}}(\mathcal{A}) = |\Pr[\mathcal{G}_0^{\mathcal{A}} = 1] - \Pr[\mathcal{G}_1^{\mathcal{A}} = 1]| \leq \varepsilon$$

where

$$\begin{array}{ll} \mathcal{G}_0^{\mathcal{A}} & \qquad \mathcal{G}_1^{\mathcal{A}} \\ \left[\begin{array}{l} (m_0, m_1) \leftarrow \mathcal{A} \\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ \mathsf{return}\ \mathcal{A}(\mathsf{Enc}_{\mathsf{pk}}(m_0)) \end{array}\right. & \qquad \left[\begin{array}{l} (m_0, m_1) \leftarrow \mathcal{A} \\ (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} \\ \mathsf{return}\ \mathcal{A}(\mathsf{Enc}_{\mathsf{pk}}(m_1)) \end{array}\right. \end{array}$$

Show that IND-FPA security implies that distributions $(\mathsf{pk}, \mathsf{Enc}_{\mathsf{pk}}(m_0))$ and $(\mathsf{pk}, \mathsf{Enc}_{\mathsf{pk}}(m_1))$ are computationally indistinguishable for all $m_0, m_1 \in \mathcal{M}$. Secondly, show that if there exists an efficient IND-CPA secure cryptosystem, there also exists an efficient IND-FPA secure cryptosystem that is not IND-CPA secure.