4. PRPs, PRFs, Semantic Security

This chapter is dedicated to central concepts of cryptography. We will introduce a new definition of security, so-called *semantic security* in different variants, which is the standard definition in modern cryptography.

4.1 Definitions and Basic Properties

Before investigating semantic security we will introduce the concepts of pseudo-random permutations (PRPs) and functions (PRFs). These are two important concepts and will enable us to prove security of certain modes of operations according to the definition of semantic security.

A (deterministic) function will be named pseudo-random, if no efficient adversary can distinguish it from what we call a *random function*. We will explain shortly the nature of such a random function. Consider the set of all functions from $\mathcal{X}$ to $\mathcal{Y}$ written $\mathsf{Func}(\mathcal{X},\mathcal{Y})$. For finite sets $\mathcal{X}$ and $\mathcal{Y}$, this set has $|\mathcal{Y}|^{|\mathcal{X}|}$ elements, thus the uniform distribution on this set is given by $P_{\mathcal{U}}[f] = \frac{1}{|\mathcal{Y}|^{|\mathcal{X}|}}$ for all $f \in \mathsf{Func}(\mathcal{X},\mathcal{Y})$. A random function is an element from $\mathsf{Func}(\mathcal{X},\mathcal{Y})$ that is drawn according to this uniform distribution. It has the following properties: (i) it is a deterministic function (!), (ii) for each $x \in \mathcal{X}$, $f(x)$ is distributed uniformly random in $\mathcal{Y}$, independently of any other $f(y)$, if $x \neq y$.

Random permutations are similarly defined, except that they are drawn from $\mathsf{Perm}(\mathcal{X})$, the set of all permutation of $\mathcal{X}$, which has $|\mathcal{X}|!$ elements.

4.1.1 Pseudo-random Permutations (PRPs)

Intuitively, a pseudo-random permutation is a keyed function, i.e., a deterministic function $\mathsf{E} : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{X}$ such that for a fixed but secret key K no machine can distinguish the resulting permutation from a random permutation. This is expressed, as most definitions in cryptography, in terms of a game, that an adversary plays against a *challenger*.

Definition 4.1 (PRP Challenger) *Let $\mathsf{E} : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{X}$ be a PRP candidate function. Then the PRP challenger for E is defined in three stages as follows:*

- *First, it randomly chooses a bit b.*
- *Secondly, depending on the value of b, it proceeds as follows:*
  - *If $b = 0$ let $K \leftarrow_{\mathcal{R}} \mathcal{K}$, $F := \mathsf{E}(K,\cdot)$.*
  - *If $b = 1$ let $F \leftarrow_{\mathcal{R}} \mathsf{Perm}(\mathcal{X})$.*
- *Finally, it receives a message $x \in \mathcal{X}$ and outputs $F(x)$. This stage is repeated arbitrarily often.*

$\diamond$

An adversary wins the game against the PRP-challenger if it is able to deduce the bit b significantly better than by pure guessing. The adversary can guess correctly with probability $\frac{1}{2}$ by simply outputting a random value b^*. As formalized by the following definition, its advantage captures

how much better an adversary can do than to purely guess the bit. In the following, $Exp_{\mathsf{A}}^{\mathsf{PRP}}(b)$ denotes the experiment where the adversary A interacts with the PRP challenger whose bit is chosen as b. Furthermore $Exp_{\mathsf{A}}^{\mathsf{PRP}}(b) = 0$ and $Exp_{\mathsf{A}}^{\mathsf{PRP}}(b) = 1$ denote the event that the adversary outputs 0 and 1 in the respective experiment.

Definition 4.2 (PRP advantage) *Let $\mathsf{E} : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ be a* PRP *candidate function. The advantage of the adversary A against the* PRP *challenger for E is defined as follows:*

$$Adv^{\mathsf{PRP}}[\mathsf{A}, \mathsf{E}] := \left| \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{PRP}}(0) = 1\right] - \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{PRP}}(1) = 1\right] \right|.$$

$\diamond$

The definition of security will be asymptotic, so we need a sequence of ciphers. Let $\mathsf{E} = (\mathsf{E}_n)_{n\in\mathbb{N}}$ be a sequence of functions where $\mathsf{E}_n : \mathcal{K}_n \times \mathcal{X}_n \to \mathcal{X}_n$. We say E is polynomial-time computable iff $\mathsf{E}_n(K, m)$ can be computed in time polynomial in n for all m, K. This parameter n is also called the *security parameter*. For a sequence of permutations $\mathsf{E} = (\mathsf{E}_n)_{n\in\mathbb{N}}$ and a sequence of adversaries $\mathsf{A} = (\mathsf{A}_n)_{n\in\mathbb{N}}$, we define

$$Adv^{\mathsf{PRP}}[\mathsf{A}, \mathsf{E}](n) := Adv^{\mathsf{PRP}}[\mathsf{A}_n, \mathsf{E}_n].$$

Definition 4.3 (Pseudo-random Permutation) *A* pseudorandom permutation *is a sequence $\mathsf{E} = (\mathsf{E}_n)_{n\in\mathbb{N}}$ of functions $\mathsf{E}_n : \mathcal{K}_n \times \mathcal{X}_n \to \mathcal{X}_n$, where for each $n \in \mathbb{N}$ and for each $K \in \mathcal{K}_n$:*

(1) *E_n is efficiently computable,*
(2) *$\mathsf{E}_n(K, \cdot)$ is bijective,*
(3) *$\mathsf{E}_n^{-1}(K, \cdot)$ is efficiently computable and*
(4) *$Adv^{\mathsf{PRP}}[\mathsf{A}, \mathsf{E}]$ is negligible in n, for all (sequences of) adversaries A.*

$\diamond$

4.1.2 Pseudo-random Functions (PRFs)

Pseudo-random functions are defined in a very similar manner, mainly by dropping the requirements (2) and (3) in Definition 4.3.

Definition 4.4 (PRF Challenger) *Let $\mathsf{E} : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ be a* PRF *candidate function. The* PRF challenger *for E is defined in three stages as follows:*

- *First, it randomly chooses a bit b.*
- *Secondly, depending on the value of b, it proceeds as follows:*
  - *If $b = 0$ let $K \leftarrow_{\mathcal{R}} \mathcal{K}$, $F := \mathsf{E}(K, \cdot)$.*
  - *If $b = 1$ let $F \leftarrow_{\mathcal{R}} \mathsf{Func}(\mathcal{X}, \mathcal{Y})$.*
- *Finally, it receives a message $x \in \mathcal{X}$ and outputs $F(x)$. This stage is repeated arbitrarily often.*

$\diamond$

Definition 4.5 (PRF Advantage) *Let $\mathsf{E} : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ be a* PRF *candidate function. The advantage of the adversary A against the* PRF *challenger for E is defined as follows:*

$$Adv^{\mathsf{PRF}}[\mathsf{A}, \mathsf{E}] := \left| \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{PRF}}(0) = 1\right] - \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{PRF}}(1) = 1\right] \right|.$$

$\diamond$

For a sequence of functions $\mathsf{E} = (\mathsf{E}_n)_{n\in\mathbb{N}}$ and a sequence of adversaries $\mathsf{A} = (\mathsf{A}_n)_{n\in\mathbb{N}}$ one defines

$$Adv^{\mathsf{PRF}}[\mathsf{A},\mathsf{E}](n) := Adv^{\mathsf{PRF}}[\mathsf{A}_n,\mathsf{E}_n].$$

Definition 4.6 (Pseudo-random Functions) *A* pseudo-random function *is a sequence* $\mathsf{E} = (\mathsf{E}_n)_{n\in\mathbb{N}}$ *of functions* $\mathsf{E}_n : \mathcal{K}_n \times \mathcal{X}_n \to \mathcal{Y}_n$*, where for each* $n \in \mathbb{N}$ *and for each* $K \in \mathcal{K}_n$*:*
(1) E_n *is efficiently computable and*
(4) $Adv^{\mathsf{PRF}}[\mathsf{A},\mathsf{E}](n)$ *is negligible in* n*.*

◇

We will drop the subscripts n if they are clear from the context, and we often simply speak of functions/adversaries instead of sequences of functions/adversaries in the following.

4.1.3 Switching Lemma

We have already seen examples of pseudo-random permutations, namely blockciphers such as DES and AES are considered to be pseudo-random permutations. The switching lemma states that every pseudo-random permutation is also a pseudo-random function.

Lemma 4.1 (Switching Lemma) *Each PRP* E *on* $(\mathcal{K},\mathcal{X})$ *is also a PRF on* $(\mathcal{K},\mathcal{X},\mathcal{X})$*. More precisely, if* A *is an adversary making at most* q *queries, then we have*

$$\left|Adv^{\mathsf{PRP}}[\mathsf{A},\mathsf{E}] - Adv^{\mathsf{PRF}}[\mathsf{A},\mathsf{E}]\right| \leq q^2/(2|\mathcal{X}|).$$

□

Proof. First we bound the left side in one direction:

$$\begin{aligned}
& Adv^{\mathsf{PRP}}[\mathsf{A},\mathsf{E}] \\
= \;& \left|\mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(0)=1\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(1)=1\right]\right| \\
= \;& \left|\mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(0)=1\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(1)=1\right]\right| \\
= \;& \left|\mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(0)=1\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1)=1\right] + \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1)=1\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(1)=1\right]\right| \\
\overset{(1)}{\leq} \;& Adv^{\mathsf{PRF}}[\mathsf{A},\mathsf{E}] + \left|\mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1)=1\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(1)=1\right]\right| \qquad (4.1)
\end{aligned}$$

The other direction is derived similarly:

$$\begin{aligned}
& Adv^{\mathsf{PRF}}[\mathsf{A},\mathsf{E}] \\
= \;& \left|\mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(0)=1\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1)=1\right]\right| \\
= \;& \left|\mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(0)=1\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1)=1\right]\right| \\
= \;& \left|\mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(0)=1\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(1)=1\right] + \mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(1)=1\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1)=1\right]\right| \\
\overset{(1)}{\leq} \;& Adv^{\mathsf{PRP}}[\mathsf{A},\mathsf{E}] + \left|\mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1)=1\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(1)=1\right]\right| \qquad (4.2)
\end{aligned}$$

In both calculations (1) follows from the triangular inequality. Now let *Coll* denote the event that, for the adversary A making queries $x_1, \ldots, x_q$ in experiment $Exp^{\mathsf{PRF}}_{\mathsf{A}}(1)$, a collision occurs, i.e., for $x_i \neq x_j$ we have $F(x_i) = F(x_j)$, where F is a random function from $\mathcal{X}$ to $\mathcal{X}$. Thus we have

$$
\begin{aligned}
& \left| \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1) = 1\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRP}}(1) = 1\right] \right| \\
= \; & \Big| \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1) = 1 \mid \mathit{Coll}\right] \cdot \mathsf{Pr}\left[\mathit{Coll}\right] + \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1) = 1 \mid \neg \mathit{Coll}\right] \cdot \mathsf{Pr}\left[\neg \mathit{Coll}\right] \\
& \quad - \mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(1) = 1\right] \Big| \\
= \; & \Big| \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1) = 1 \mid \mathit{Coll}\right] \cdot \mathsf{Pr}\left[\mathit{Coll}\right] + \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1) = 1 \mid \neg \mathit{Coll}\right] \cdot (1 - \mathsf{Pr}\left[\mathit{Coll}\right]) \\
& \quad - \mathsf{Pr}\left[Exp^{\mathsf{PRP}}_{\mathsf{A}}(1) = 1\right] \Big| \\
\overset{(2)}{=} \; & \left| \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1) = 1 \mid \mathit{Coll}\right] \cdot \mathsf{Pr}\left[\mathit{Coll}\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1) = 1 \mid \neg \mathit{Coll}\right] \cdot \mathsf{Pr}\left[\mathit{Coll}\right] \right| \\
= \; & \left| \mathsf{Pr}\left[\mathit{Coll}\right] \cdot \left(\mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1) = 1 \mid \mathit{Coll}\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1) = 1 \mid \neg \mathit{Coll}\right] \right) \right| \\
= \; & \left| \mathsf{Pr}\left[\mathit{Coll}\right] \right| \cdot \left| \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1) = 1 \mid \mathit{Coll}\right] - \mathsf{Pr}\left[Exp^{\mathsf{PRF}}_{\mathsf{A}}(1) = 1 \mid \neg \mathit{Coll}\right] \right| \\
\overset{(3)}{\leq} \; & \left| \mathsf{Pr}\left[\mathit{Coll}\right] \right|
\end{aligned}
$$

Here (2) follows from the fact that the experiment $Exp^{\mathsf{PRP}}_{\mathsf{A}}(1)$ is identical to the experiment $Exp^{\mathsf{PRF}}_{\mathsf{A}}(1)$ if no collision occurred, and (3) follows from the fact that the right term is between 0 and 1. In the last step of the proof we have to bound the expression $|\mathsf{Pr}\left[\mathit{Coll}\right]|$.

$$
\begin{aligned}
\left| \mathsf{Pr}\left[\mathit{Coll}\right] \right| &= \left| \frac{1}{|\mathcal{X}|} + \frac{2}{|\mathcal{X}|} + \ldots + \frac{q-1}{|\mathcal{X}|} \right| \\
&= \frac{q(q-1)}{2|\mathcal{X}|} \leq \frac{q^2}{2|\mathcal{X}|}
\end{aligned}
$$

■

4.1.4 Luby-Rackoff

The next theorem makes a statement about the opposite direction: A three-round Feistel network, where the round functions are PRFs, turns out to be a PRP. This can be seen as a justification for DES.

Theorem 4.1 (Luby-Rackoff) *A 3-round Feistel network whose three round functions are PRFs is itself a PRP.* □

4.2 On Definitions of Security

We have already seen that there are two parameters for defining security: The *capabilities* the adversary has, and the *goal* he pursues. Here we focus on the goal of *semantic security*, which intuitively captures that the adversary does not learn any partial information about the plaintexts. We distinguish the following adversary capabilities:

- Ciphertext-only attack (CT-only): Here the adversary sees one ciphertext only. Beforehand, he may choose two plaintexts, one of which is encrypted. If he cannot distinguish which of these (self-chosen) plaintexts is inside the given ciphertext, he learns no partial information. We already heave sees ciphers fulfilling this notion, e.g., the One-time Pad and stream ciphers.
- Chosen-plaintext Attack (CPA): Here the adversary sees (polynomially) many ciphertexts of self-chosen plaintexts, i.e., in addition to CT-only attacks, he may select arbitrary plaintexts that he sees the encryption of, before proceeding as above. Examples of ciphers fulfilling this stronger notion are randomized CBC based on PRPs as well as randomized counter mode based on PRFs.
- Chosen-ciphertext Attack (CCA): Additionally to the above, the adversary may choose ciphertexts that get decrypted for him. In order to avoid trivial distinguishability, these ciphertexts must of course be different from the ciphertext received as a response to the two challenge plaintext. We will treat CCA later in this lecture.

4.3 Semantic Security for Ciphertext-only Attack

Semantic security is one of the central definitions in cryptography. The intuition is that even if an adversary chooses two plaintexts and sees the encryption of one of them, he cannot tell which plaintext was encrypted. First we give the definition for encryption schemes where only one plaintext is encrypted and the resulting ciphertext is observed by the adversary.

Definition 4.7 (CT-only Challenger) *Let* (E, D) *be an encryption scheme on* $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. *The* CT-only challenger *for* E *is defined in two stages as follows:*

- *First, it randomly chooses a bit* b *and a key* $K \leftarrow_{\mathcal{R}} \mathcal{K}$.
- *Secondly, it receives two plaintexts* $m_0, m_1 \in \mathcal{M}$, *with* $|m_0| = |m_1|$, *computes* $c \leftarrow \mathsf{E}(K, m_b)$ *and outputs* c.

$\diamond$

An adversary wins the game against the CT-only challenger if, intuitively, it is able to deduce the bit b better than by pure guessing after seeing c. In the following, $Exp_{\mathsf{A}}^{\mathsf{CT-only}}(b)$ denotes the experiment where the adversary A interacts with the CT-only challenger whose bit is chosen as b. Furthermore $Exp_{\mathsf{A}}^{\mathsf{CT-only}}(b) = 0$ and $Exp_{\mathsf{A}}^{\mathsf{CT-only}}(b) = 1$ denote the event that the adversary outputs 0 and 1 in the respective experiment. The advantage of an adversary is formalized by the following definition.

Definition 4.8 (CT-only Advantage) *Let* (E, D) *be an encryption scheme on* $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. *The* advantage *of an adversary* A *against the* CT-only challenger *for* E *is defined as follows:*

$$Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{E}] := \left| \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CT-only}}(0) = 1 \right] - \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CT-only}}(1) = 1 \right] \right|.$$

$\diamond$

Again, the definition of semantic security is asymptotic, which means we are formally given a sequence of ciphers $(\mathsf{E}, \mathsf{D}) = (\mathsf{E}_n, \mathsf{D}_n)_{n \in \mathbb{N}}$ on $(\mathcal{K}_n, \mathcal{M}_n, \mathcal{C}_n)_{n \in \mathbb{N}}$ and a sequence of adversaries $\mathsf{A} = (\mathsf{A}_n)_{n \in \mathbb{N}}$, and we write

$$Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{E}](n) := Adv^{\mathsf{CT-only}}[\mathsf{A}_n, \mathsf{E}_n].$$

Again, we simply drop the subscript n in the following and simply speak of ciphers and adversaries, instead of sequences thereof.

Definition 4.9 (Semantic Security under Ciphertext-only Attack (CT-only)) *We say that a cipher* (E, D) *is* semantically secure under ciphertext-only attack (CT-only) *if for all efficient adversaries* A*, the advantage* $Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{E}]$ *is negligible in* n*.* ◇

4.3.1 Consequences of Semantic Security

Semantic security implies secrecy of every single bit of a plaintext. This is easy to see, so we do not give a formal proof. For contradiction suppose there exists an adversary A that can guess the i-th bit of a message with probability $\frac{1}{2} + p$ for some $0 < p \leq \frac{1}{2}$, after seeing its ciphertext. Then we construct an adversary B for the CT-only challenger as follows:

- Choose two messages, with $|m_0| = |m_1|$, such that the i-th bit in m_b is b,
- send these messages to the CT-only challenger and receive an encryption c,
- run A on input c, from which B obtains a bit b',
- and output b'.

The probability of success is given as follows:

$$\begin{aligned} Adv^{\mathsf{CT-only}}[\mathsf{B}, \mathsf{E}] &= \left| \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CT-only}}(0) = 1 \right] - \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CT-only}}(1) = 1 \right] \right| \\ &= |(1/2 - p) - (1/2 + p)| \\ &= 2p \end{aligned}$$

4.3.2 Semantic Security of the One-time Pad

The *one-time Pad* is semantically secure under ciphertext-only attack. This follows easily from perfect secrecy.

Lemma 4.2 *For* all *adversaries* A *(even for computationally unbounded ones) we have*

$$Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{E}^{\mathsf{OTP}}] = 0.$$

where $\mathsf{E}^{\mathsf{OTP}}$ *denotes the one-time pad encryption function.* □

4.3.3 Semantic Security of Deterministic Counter Mode (detCTR

Deterministic counter mode, i.e., counter mode with fixed initial value $IV = 0$, is semantically secure under ciphertext-only attack.

Theorem 4.2 (Semantic Security of detCTR mode) *For any* $L > 0$*: If* E *is a* PRF *over* $(\mathcal{K}, \mathcal{X})$ *then* $\mathsf{E}^{\mathsf{detCTR}}$ *over* $(\mathcal{K}, \mathcal{X}^L, \mathcal{X}^L)$ *is semantically secure. In particular, for any attacker* A *against* $\mathsf{E}^{\mathsf{detCTR}}$ *there exists an adversary* B *against* E *such that*

$$Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{E}^{\mathsf{detCTR}}] = 2 \cdot Adv^{\mathsf{PRF}}[\mathsf{B}, \mathsf{E}].$$

□

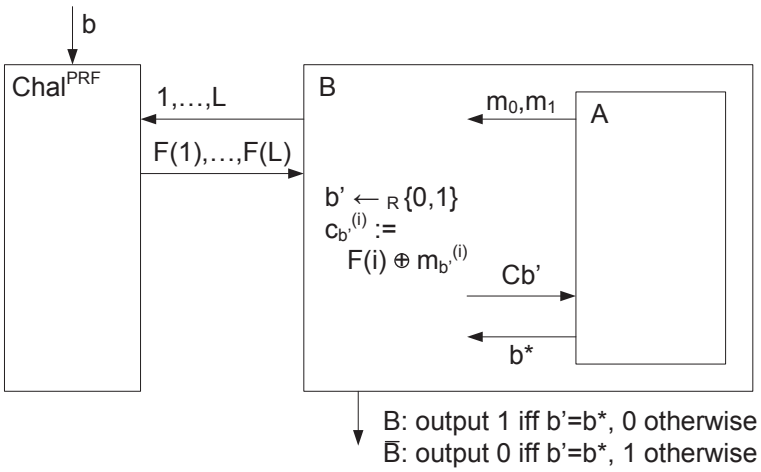

Figure 4.1: Construction of adversary B from A.

Proof. Given an adversary A against the CT-only challenger we construct an adversary B against the PRF challenger as in Figure 4.1. We need to estimate the following value

$$Adv^{\mathsf{PRF}}[\mathsf{B},\mathsf{E}] = \left|\mathsf{Pr}\left[Exp_{\mathsf{B}}^{\mathsf{PRF}}(0)=1\right] - \mathsf{Pr}\left[Exp_{\mathsf{B}}^{\mathsf{PRF}}(1)=1\right]\right| \tag{4.3}$$

First observe that for the second expression, we have

$$\mathsf{Pr}\left[Exp_{\mathsf{B}}^{\mathsf{PRF}}(1)=1\right] = \frac{1}{2}, \tag{4.4}$$

as the values $F(i)$ in this experiment are chosen independently at random. Thus the encryption $c_{b'}$ computed by B is as good as the one-time pad, so the adversary A gains absolutely no information on B's random bit b'.

Now let us calculate the first expression of the absolute value in Equation 4.3:

$$\begin{aligned}
& \mathsf{Pr}\left[Exp_{\mathsf{B}}^{\mathsf{PRF}}(0)=1\right] \\
= \;& \mathsf{Pr}\left[b'=b^* \mid b=0\right] \qquad (4.5)\\
= \;& \mathsf{Pr}\left[b'=b^*=0 \mid b=0\right] + \mathsf{Pr}\left[b'=b^*=1 \mid b=0\right] \\
= \;& \frac{1}{2}\cdot \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CT-only}}(0)=0\right] + \frac{1}{2}\cdot \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CT-only}}(1)=1\right] \\
= \;& \frac{1}{2}\cdot \left(1-\mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CT-only}}(0)=1\right]\right) + \frac{1}{2}\cdot \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CT-only}}(1)=1\right] \\
= \;& \frac{1}{2} + \frac{1}{2}\cdot \left(\mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CT-only}}(1)=1\right] - \mathsf{Pr}\left[Exp_{\mathsf{A}}^{\mathsf{CT-only}}(0)=1\right]\right) \qquad (4.6)
\end{aligned}$$

If the right expression is positive, then Equation 4.6 equals $\frac{1}{2} + Adv^{\mathsf{CT-only}}[\mathsf{A},\mathsf{E}]$, which completes the proof.

Otherwise, if the right expression is negative, then we define the attacker $\bar{\mathsf{B}}$ to output 0 if B outputs 1 and vice versa. Then the same calculation as above yields

$$\mathsf{Pr}\left[Exp_{\bar{\mathsf{B}}}^{\mathsf{PRF}}(0)=1\right] = \frac{1}{2} + \frac{1}{2}\cdot Adv^{\mathsf{CT-only}}[\mathsf{A},\mathsf{E}] \tag{4.7}$$

Thus there exists some adversary B (either B itself or $\bar{\mathsf{B}}$ such that the following holds:

$$\begin{aligned} & Adv^{\mathsf{PRF}}[\mathsf{B},\mathsf{E}] = \left(\frac{1}{2} + \frac{1}{2} \cdot Adv^{\mathsf{CT-only}}[\mathsf{A},\mathsf{E}^{\mathsf{detCTR}}]\right) - \frac{1}{2} \\ \Leftrightarrow \quad & 2 \cdot Adv^{\mathsf{PRF}}[\mathsf{B},\mathsf{E}] = Adv^{\mathsf{CT-only}}[\mathsf{A},\mathsf{E}^{\mathsf{detCTR}}], \end{aligned}$$

which concludes the proof. ∎

4.4 Semantic Security under Chosen-plaintext Attack

The above definition of semantic security covered the case where the attacker sees a single encryption only. This is not sufficient for most uses of encryption schemes, but the notion can be extended to the more general case as well.

Definition 4.10 (CPA Challenger) *Let* (E,D) *be an encryption scheme on* $(\mathcal{K},\mathcal{M},\mathcal{C})$*. The* CPA challenger *for* E *is defined in three stages as follows:*

- *First, it chooses a bit* b *and a random key* $K \leftarrow_{\mathcal{R}} \mathcal{K}$*.*
- *Secondly, it receives a plaintext* x*. If* $x \notin \mathcal{M}$*, then it does nothing. Otherwise, it computes* $c \leftarrow \mathsf{E}(K,x)$ *and outputs* c*. It repeats this stage until the input satisfies the conditions of the third stage.*
- *It receives two plaintexts* $m_0, m_1 \in \mathcal{M}$ *with* $|m_0| = |m_1|$*, computes the encryption* $c \leftarrow \mathsf{E}(K,m_b)$ *and outputs* c*.*

◇

An adversary wins the game against the CPA challenger if, intuitively, it is able to deduce the bit b better than by pure guessing. In the following, $Exp^{\mathsf{CPA}}_{\mathsf{A}}(b)$ denotes the experiment where the adversary A interacts with the *CPA challenger* whose bit is chosen as b. Furthermore $Exp^{\mathsf{CPA}}_{\mathsf{A}}(b) = 0$ and $Exp^{\mathsf{CPA}}_{\mathsf{A}}(b) = 1$ denote the event that the adversary outputs 0 and 1 in the respective experiment.

Definition 4.11 (CPA Advantage) *Let* (E,D) *be an encryption scheme on* $(\mathcal{K},\mathcal{M},\mathcal{C})$*. The* advantage *of an adversary* A *against the* CPA challenger *for* E *is defined as follows:*

$$Adv^{\mathsf{CPA}}[\mathsf{A},\mathsf{E}] := \left|\mathsf{Pr}\left[Exp^{\mathsf{CPA}}_{\mathsf{A}}(b) = 0\right] - \mathsf{Pr}\left[Exp^{\mathsf{CPA}}_{\mathsf{A}}(b) = 1\right]\right|.$$

◇

Given a sequence of ciphers $(\mathsf{E},\mathsf{D}) = (\mathsf{E}_n,\mathsf{D}_n)_{n\in\mathbb{N}}$ on $(\mathcal{K}_n,\mathcal{M}_n,\mathcal{C}_n)_{n\in\mathbb{N}}$ and a sequence of adversaries $\mathsf{A} = (\mathsf{A}_n)_{n\in\mathbb{N}}$, and we write

$$Adv^{\mathsf{CPA}}[\mathsf{A},\mathsf{E}](n) := Adv^{\mathsf{CPA}}[\mathsf{A}_n,\mathsf{E}_n].$$

Definition 4.12 (Semantic Security under Chosen-plaintext Attack (CPA)) *A cipher* (E,D) *is* semantically secure under chosen-plaintext attack (CPA) *if for all efficient adversaries* A*, the advantage* $Adv^{\mathsf{CPA}}[\mathsf{A},\mathsf{E}]$ *is negligible in* n*.* ◇

4.4.1 Semantic Security of Modes of Operation

Theorem 4.3 (Semantic Security of CBC) *For any $L > 0$: If E is a PRP over $(\mathcal{K}, \mathcal{X})$ then $\mathsf{E}^{\mathsf{CBC}}$ over $(\mathcal{K}, \mathcal{X}^L, \mathcal{X}^L)$ is semantically secure. In particular, for any attacker A against $\mathsf{E}^{\mathsf{CBC}}$ making at most q queries there exists an adversary B against E such that*

$$Adv^{\mathsf{CPA}}[\mathsf{A}, \mathsf{E}^{\mathsf{CBC}}] = 2 \cdot Adv^{\mathsf{PRF}}[\mathsf{B}, \mathsf{E}] + \frac{2q^2L^2}{|\mathcal{X}|}.$$

□

This means that CBC is secure as long as $q \ll \frac{\sqrt{|\mathcal{X}|}}{L}$.

Theorem 4.4 (Semantic Security of Random Counter Mode (rndCTR)) *For any $L > 0$: If E is a PRP over $(\mathcal{K}, \mathcal{X})$ then $\mathsf{E}^{\mathsf{rndCTR}}$ over $(\mathcal{K}, \mathcal{X}^L, \mathcal{X}^{L+1})$ is semantically secure. In particular, for any attacker A against $\mathsf{E}^{\mathsf{rndCTR}}$ making at most q queries there exists an adversary B against E such that*

$$Adv^{\mathsf{CPA}}[\mathsf{A}, \mathsf{E}^{\mathsf{rndCTR}}] = 2 \cdot Adv^{\mathsf{PRF}}[\mathsf{B}, \mathsf{E}] + \frac{2q^2L}{|\mathcal{X}|}.$$

□

This means that random counter mode is secure as long as $q \ll \sqrt{\frac{|\mathcal{X}|}{L}}$.