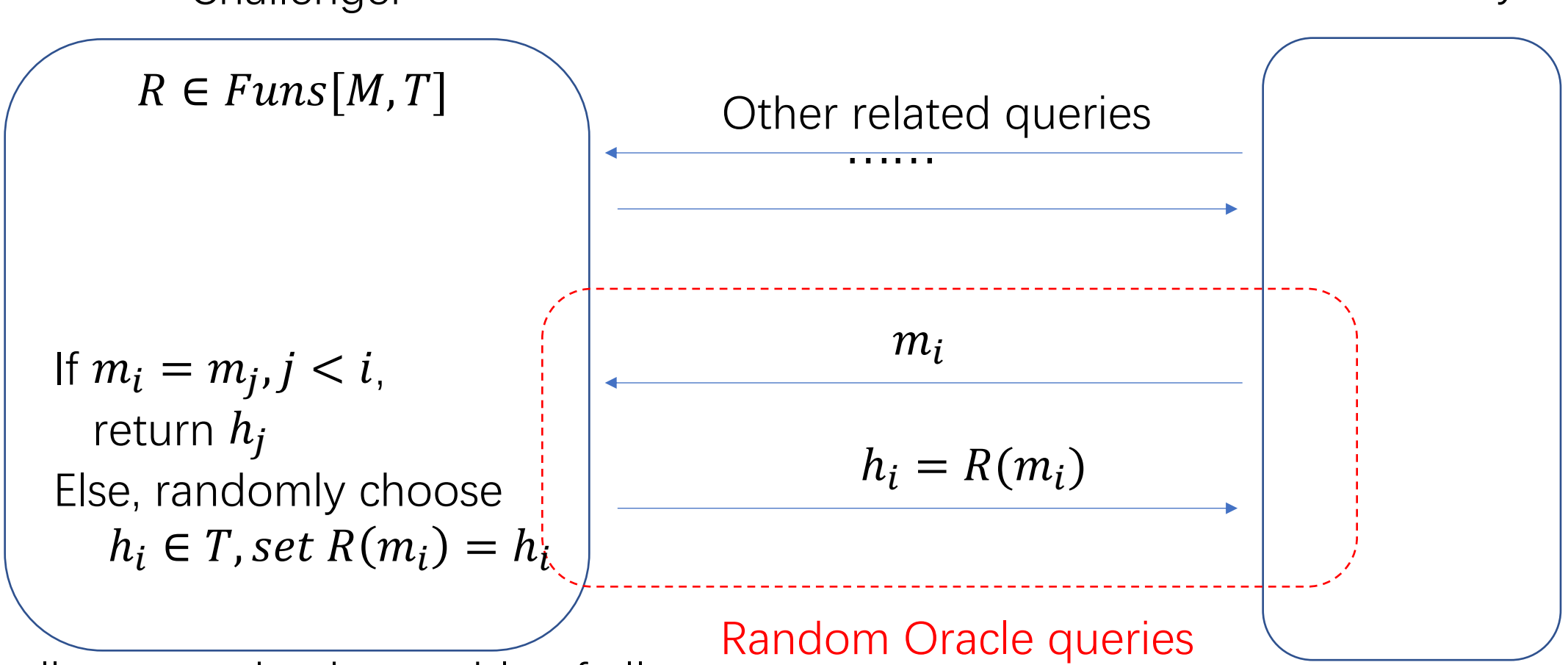
Encryption based on a trapdoor function scheme

2023.10.26

Random Oracle Model

Scheme S involves computing a hash function H. If scheme S evaluates H at arbitrary points of its choice, but does not look at the internal implementation of H, we say S use H as an oracle



Challenger maintains a table of all queried mi and the corresponding hi

CPA secure public key encryption

Our encryption scheme is called ε_{TDF}, and is built out of several components:

- a trapdoor function scheme $T = (G, F, F^{-1})$, defined over $(\mathcal{X}, \mathcal{Y})$,
- a symmetric cipher $\varepsilon_s = (E_s, D_s)$, defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$,
- a hash function $H : X \to K$.

The key generation, encryption, and decryption algorithms for ϵ_{TDF}.

- The key generation algorithm for ε_{TDF} is the key generation algorithm for T .
- For a given public key pk, and a given message $m \in \mathcal{M}$,

$$E(pk; m) := x \xleftarrow{R} X, y \longleftarrow E(pk, x), k \longleftarrow H(x); c \longleftarrow E_s(k, m)$$

output (y, c).

- For a given secret key sk, and a given ciphertext $(y, c) \in \mathcal{Y} \times \mathcal{C}$

$$D(sk, (y, c)) := x \longleftarrow F^{-1}(sk, y), k \longleftarrow H(x), m \longleftarrow D_s(k, c)$$

output m.

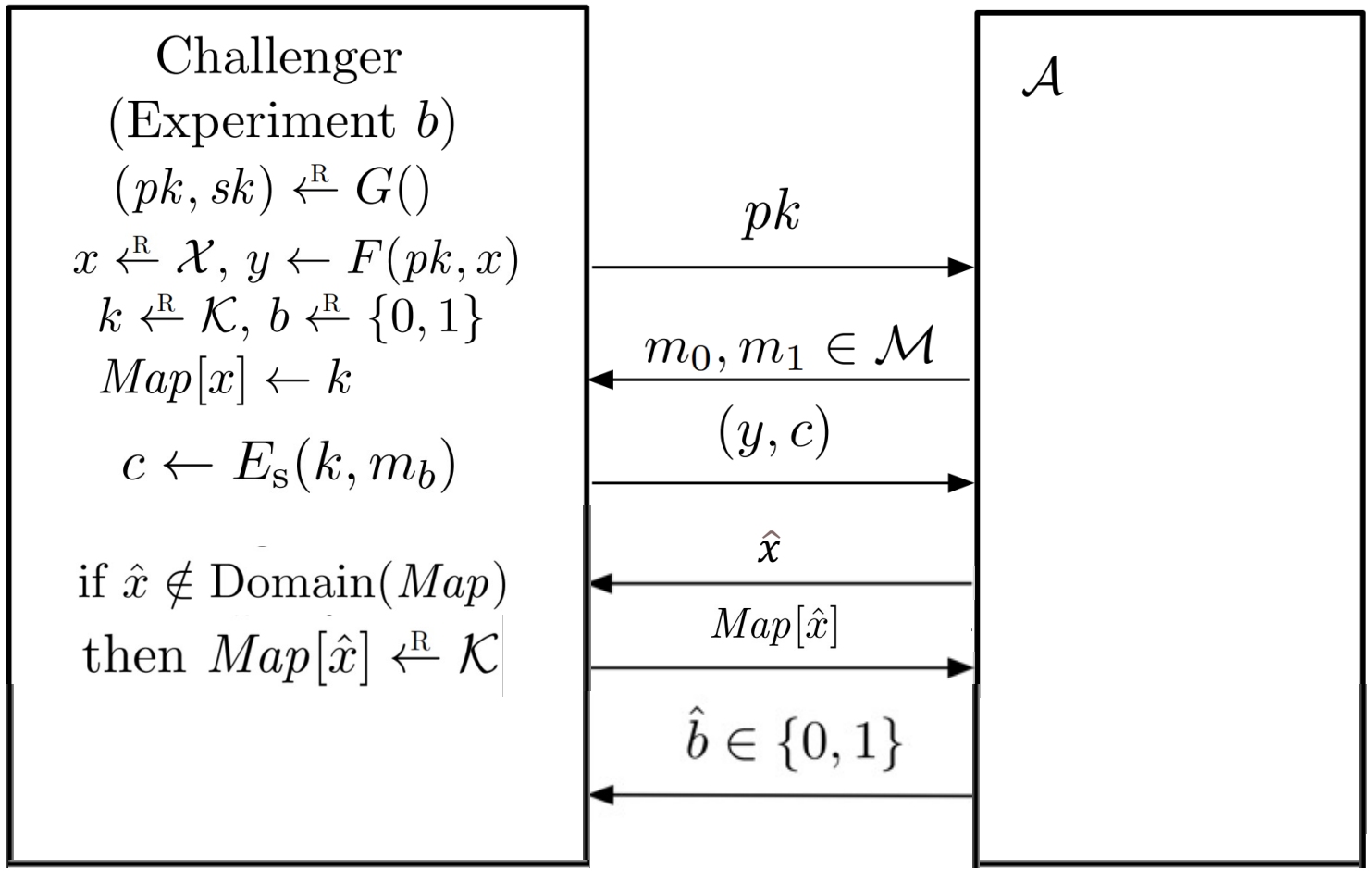
$\varepsilon_{TDF} = (G, E, D)$, and is defined over $(\mathcal{M}; \mathcal{Y} \times \mathcal{C})$.

Theorem Assume $H : X \to K$ is modeled as a random oracle. If T is one-way and ε_s is semantically secure, then ε_{TDF} is semantically secure.

$$SS^{ro}adv^*[\mathcal{A}, \varepsilon_{TDF}] \leq OWadv[\mathcal{B}_{ow}; T] + SSadv^*[\mathcal{B}_s; \varepsilon_s].$$

Game 0

$(pk, sk) \xleftarrow{R} G(), x \xleftarrow{R} \mathcal{X}, y \leftarrow F(pk, x)$
initialize an empty associative array $Map : \mathcal{X} \rightarrow \mathcal{K}$

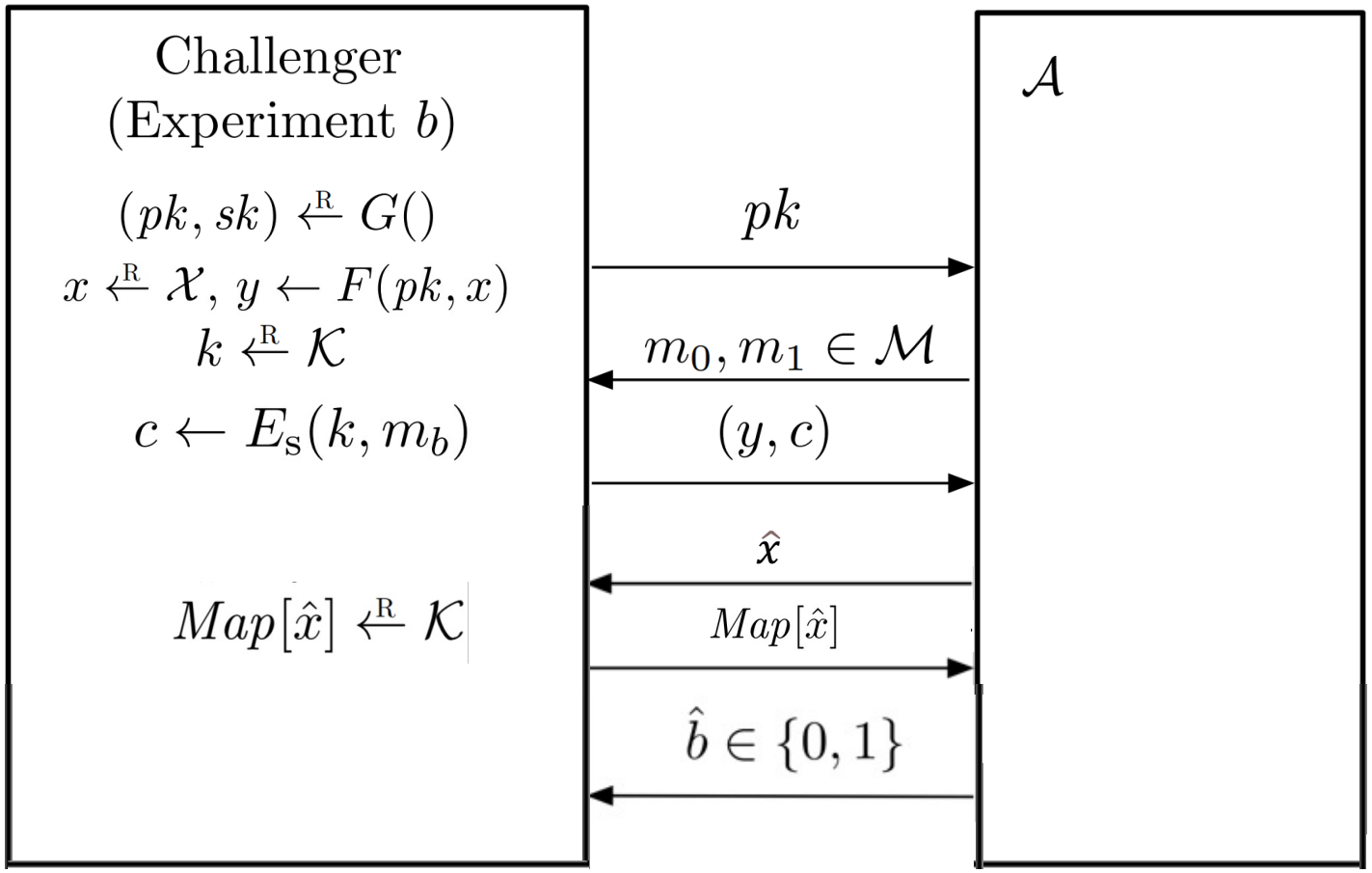


Define W_j to be the event that $\hat{b} = b$ in Game j.

$$\mathrm{SS^{ro}adv^*}[\mathcal{A}, \mathcal{E}_{\mathrm{TDF}}] = |\Pr[W_0] - 1/2|$$

CPA语义安全模型
注意杂凑函数用建表映射来实现

Game 1



Let Z be the event that the adversary queries the random oracle at the point x in Game 1.

Clearly, Games 0 and 1 proceed identically unless Z occurs, and so by the Difference Lemma, we have:

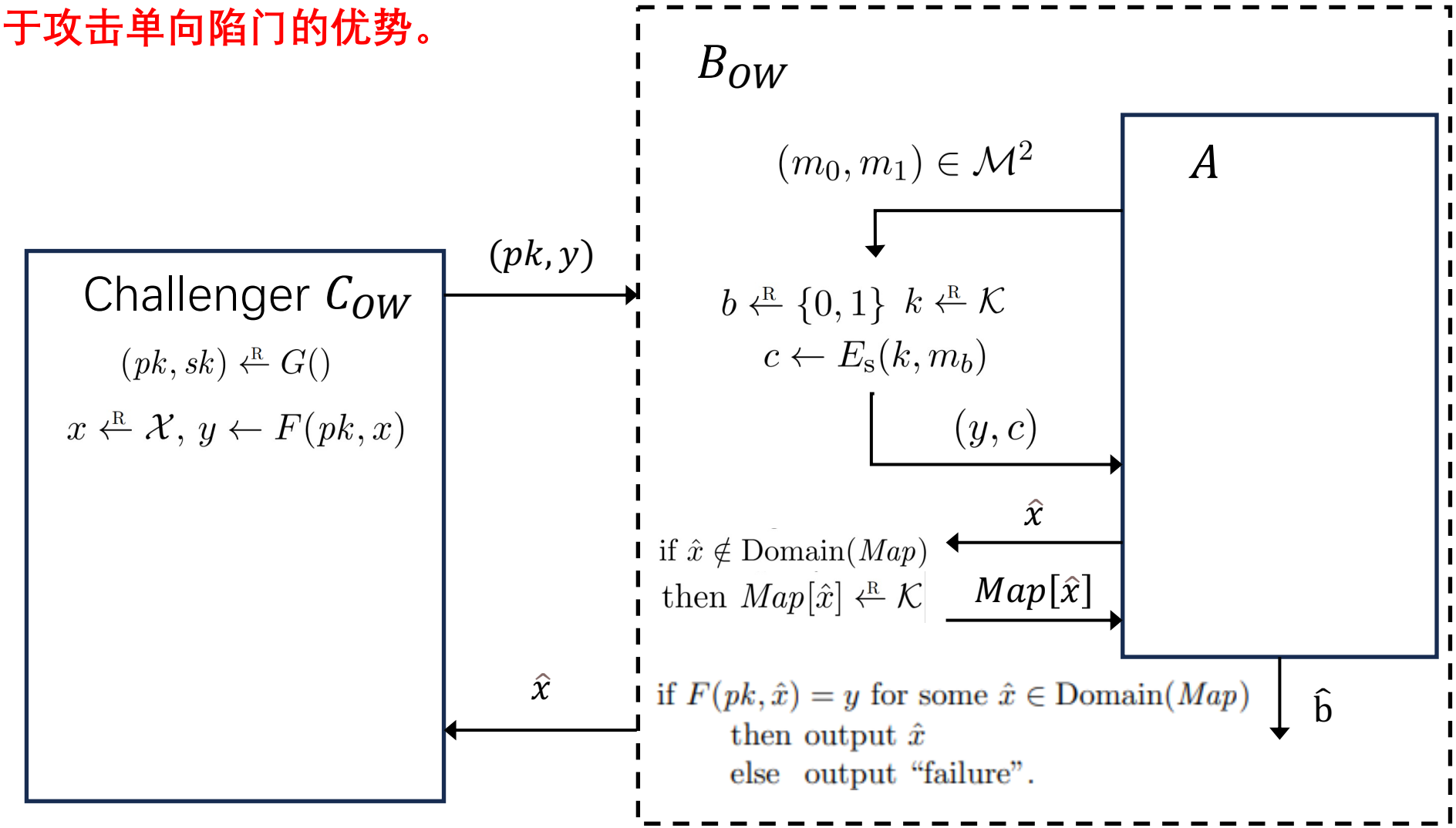
$$|\Pr[W_1] - \Pr[W_0]| \leq \Pr[Z].$$

取消x与k之间的映射关系。

Game0与Game1之间唯一的区别就是事件Z发生。

根据差分引理 $|\Pr[W_1] - \Pr[W_0]| \leq \Pr[Z].$

本页说明事件Z的发生的概率如何等同于攻击单向陷门的优势。



如果事件Z在Game1中发生，那么A一定在某次RO询问中问到了x，而x正好是公钥y对应的单向陷门函数的原像，所以就破解OW。B可以将该x直接返还C_{ow}进行作答。

Theorem 4.7 (Difference Lemma). *Let Z, W_0, W_1 be events defined over some probability space, and let $\bar{Z}$ denote the complement of the event Z. Suppose that $W_0 \wedge \bar{Z}$ occurs if and only if $W_1 \wedge \bar{Z}$ occurs. Then we have*

$$\left|\Pr[W_0] - \Pr[W_1]\right| \leq \Pr[Z].$$

Proof. This is a simple calculation. We have

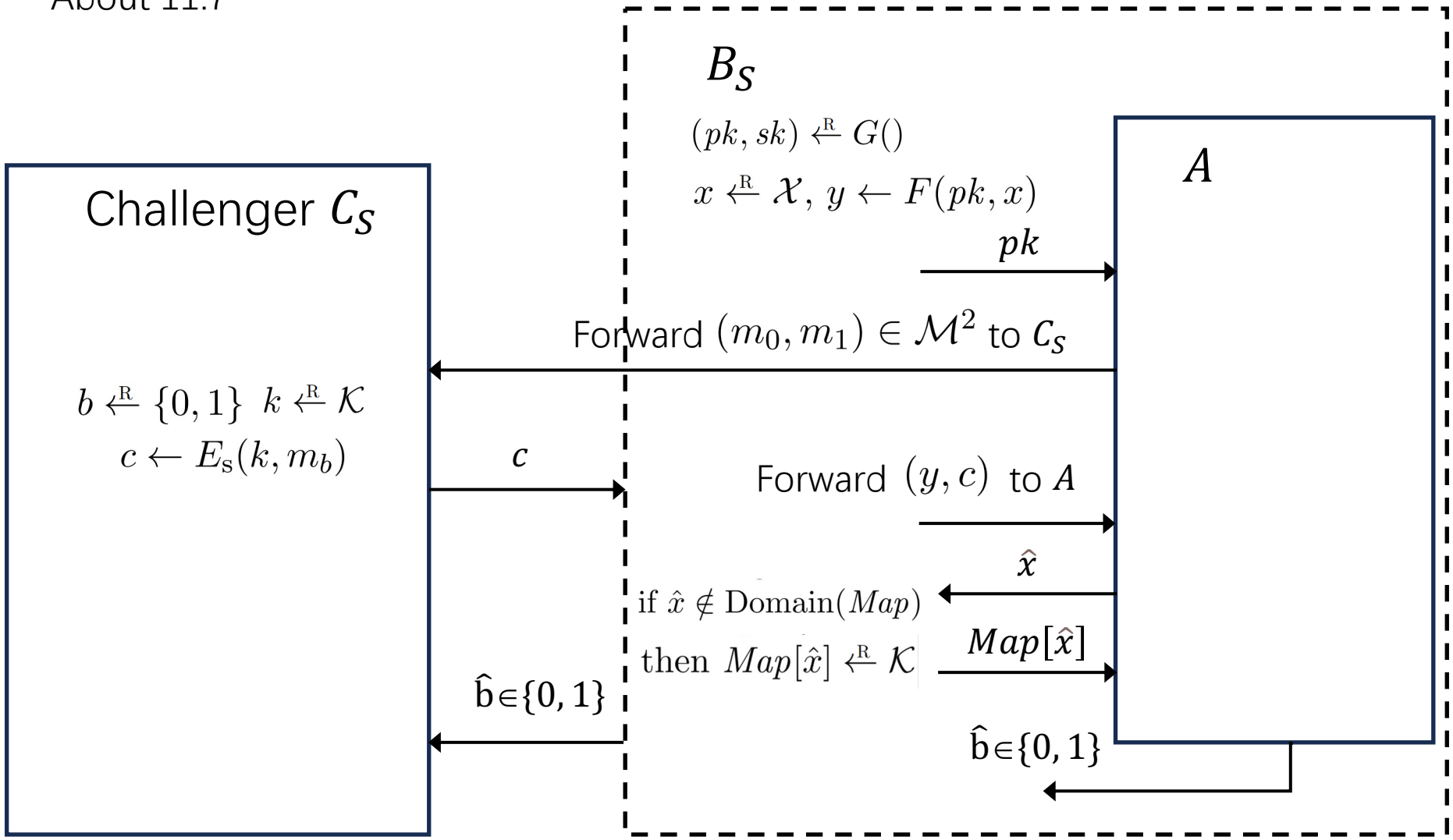
$$\begin{aligned}\left|\Pr[W_0] - \Pr[W_1]\right| &= \left|\Pr[W_0 \wedge Z] + \Pr[W_0 \wedge \bar{Z}] - \Pr[W_1 \wedge Z] - \Pr[W_1 \wedge \bar{Z}]\right| \\ &= \left|\Pr[W_0 \wedge Z] - \Pr[W_1 \wedge Z]\right| \\ &\leq \Pr[Z].\end{aligned}$$

The second equality follows from the assumption that $W_0 \wedge \bar{Z} \iff W_1 \wedge \bar{Z}$, and so in particular, $\Pr[W_0 \wedge \bar{Z}] = \Pr[W_1 \wedge \bar{Z}]$. The final inequality follows from the fact that both $\Pr[W_0 \wedge Z]$ and $\Pr[W_1 \wedge Z]$ are numbers between 0 and $\Pr[Z]$. □

To analyze $\mathcal{B}_{\text{ow}}$, we may naturally view Game 1 and the game played between $\mathcal{B}_{\text{ow}}$ and $\mathbf{C}_{\text{ow}}$ as operating on the same underlying probability space. By definition, Z occurs if and only if $x \in \text{Domain}(Map)$ when $\mathcal{B}_{\text{ow}}$ finishes its game. Therefore,

$$\Pr[Z] = \mathsf{OWadv}[\mathcal{B}_{\text{ow}}, \mathcal{T}]. \tag{11.6}$$

About 11.7


B_S
$(pk, sk) \xleftarrow{R} G()$
$x \xleftarrow{R} \mathcal{X},\ y \leftarrow F(pk, x)$
Challenger C_S
A
pk
Forward $(m_0, m_1) \in \mathcal{M}^2$ to C_S
$b \xleftarrow{R} \{0,1\}$ $k \xleftarrow{R} \mathcal{K}$
$c \leftarrow E_s(k, m_b)$
c
Forward (y, c) to A
$\hat{x}$
if $\hat{x} \notin \mathrm{Domain}(Map)$
then $Map[\hat{x}] \xleftarrow{R} \mathcal{K}$
$Map[\hat{x}]$
$\hat{b} \in \{0,1\}$
$\hat{b} \in \{0,1\}$

Observe that in Game 1, the key k is only used to encrypt the challenge plaintext. As such, the adversary is essentially attacking $\mathcal{E}_s$ as in the bit-guessing version of Attack Game 2.1 at this point. More precisely, we derive an efficient SS adversary $\mathcal{B}_s$ based on Game 1 that uses $\mathcal{A}$ as a subroutine, such that

$$|\Pr[W_1] - 1/2| = \mathsf{SSadv}^*[\mathcal{B}_s, \mathcal{E}_s]. \tag{11.7}$$

To analyze $\mathcal{B}_s$, we may naturally view Game 1 and the game played between $\mathcal{B}_s$ and $\mathbf{C}_s$ as operating on the same underlying probability space. By construction, $\mathcal{B}_s$ and $\mathcal{A}$ output the same thing, and so (11.7) holds.

Combining:

$$\mathrm{SS}^{\mathrm{ro}}\mathsf{adv}^{*}[\mathcal{A}, \mathcal{E}_{\mathrm{TDF}}] = |\Pr[W_0] - 1/2|$$

$$\left|\Pr[W_1] - \Pr[W_0]\right| \leq \Pr[Z].$$

$$\Pr[Z] = \mathrm{OW}\mathsf{adv}[\mathcal{B}_{\mathrm{ow}}, \mathcal{T}].$$

$$|\Pr[W_1] - 1/2| = \mathrm{SS}\mathsf{adv}^{*}[\mathcal{B}_{\mathrm{s}}, \mathcal{E}_{\mathrm{s}}].$$

We have:

$$\mathrm{SS}^{\mathrm{ro}}\mathsf{adv}^{*}[\mathcal{A}, \mathcal{E}_{\mathrm{TDF}}] \leq \mathrm{OW}\mathsf{adv}[\mathcal{B}_{\mathrm{ow}}, \mathcal{T}] + \mathrm{SS}\mathsf{adv}^{*}[\mathcal{B}_{\mathrm{s}}, \mathcal{E}_{\mathrm{s}}].$$