Semantic security of Encryption based on trapdoor function 11.4

Definition 10.2 (Trapdoor function scheme). *Let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. A* ***trapdoor function scheme*** *$\mathcal{T}$, defined over $(\mathcal{X}, \mathcal{Y})$, is a triple of algorithms (G, F, I), where*

- *G is a probabilistic key generation algorithm that is invoked as $(pk, sk) \overset{\mathrm{R}}{\leftarrow} G()$, where pk is called a* ***public key*** *and sk is called a* ***secret key****.*

- *F is a deterministic algorithm that is invoked as $y \leftarrow F(pk, x)$, where pk is a public key (as output by G) and x lies in $\mathcal{X}$. The output y is an element of $\mathcal{Y}$.*

- *I is a deterministic algorithm that is invoked as $x \leftarrow I(sk, y)$, where sk is a secret key (as output by G) and y lies in $\mathcal{Y}$. The output x is an element of $\mathcal{X}$.*

$\mathcal{E}_{\mathrm{TDF}}$

$\mathcal{E}_{\mathrm{TDF}}$

- a trapdoor function scheme $\mathcal{T} = (G, F, I)$, defined over $(\mathcal{X}, \mathcal{Y})$,
- a symmetric cipher $\mathcal{E}_{\mathrm{s}} = (E_{\mathrm{s}}, D_{\mathrm{s}})$, defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$,
- a hash function $H : \mathcal{X} \to \mathcal{K}$.

G: • The key generation algorithm for $\mathcal{E}_{\mathrm{TDF}}$ is the key generation algorithm for $\mathcal{T}$.

E: • For a given public key pk, and a given message $m \in \mathcal{M}$, the encryption algorithm runs as follows:

$$\begin{aligned} E(pk, m) := \quad & x \xleftarrow{\mathrm{R}} \mathcal{X}, \quad y \leftarrow F(pk, x), \quad k \leftarrow H(x), \quad c \xleftarrow{\mathrm{R}} E_{\mathrm{s}}(k, m) \\ & \text{output } (y, c). \end{aligned}$$

D: • For a given secret key sk, and a given ciphertext $(y, c) \in \mathcal{Y} \times \mathcal{C}$, the decryption algorithm runs as follows:

$$\begin{aligned} D(sk,\ (y, c)\ ) := \quad & x \leftarrow I(sk, y), \quad k \leftarrow H(x), \quad m \leftarrow D_{\mathrm{s}}(k, c) \\ & \text{output } m. \end{aligned}$$

Theorem

Theorem 11.2. *Assume $H : \mathcal{X} \to \mathcal{K}$ is modeled as a random oracle. If $\mathcal{T}$ is one-way and $\mathcal{E}_{\mathrm{s}}$ is semantically secure, then $\mathcal{E}_{\mathrm{TDF}}$ is semantically secure.*

$$\mathrm{SS}^{\mathrm{ro}}\mathsf{adv}[\mathcal{A}, \mathcal{E}_{\mathrm{TDF}}] \leq 2 \cdot \mathrm{OW}\mathsf{adv}[\mathcal{B}_{\mathrm{ow}}, \mathcal{T}] + \mathrm{SS}\mathsf{adv}[\mathcal{B}_{\mathrm{s}}, \mathcal{E}_{\mathrm{s}}].$$

Random Oracle Model

Wiki:

Random oracle (RO) is an oracle (a theoretical black box) that responds to every *unique query* with a (truly) random response chosen uniformly from its output domain. If a query is repeated, it responds the same way every time that query is submitted.

- Firstly used in rigorous cryptographic proofs in the 1993 publication by Mihir Bellare and Phillip Rogaway (1993)
- Used when the proof cannot be carried out using weaker assumptions on the cryptographic hash function.
- A system that is proven secure when every hash function is replaced by a random oracle is described as being secure in the **random oracle model**, as opposed to secure in the standard model of cryptography.
- When a random oracle is used within a security proof, it is made available to all players, including the adversaries.

Game 0

Challenger

(1) $(pk, sk) \xleftarrow{R} G(),\ x \xleftarrow{R} \mathcal{X},\ y \leftarrow F(pk, x)$

Initialize an empty associative array

$Map : \mathcal{X} \rightarrow \mathcal{K}$

(2) $k \xleftarrow{R} \mathcal{K},\ b \xleftarrow{R} \{0, 1\}$

(3) $Map[x] \leftarrow k$

(4) $c \leftarrow E_{\mathrm{s}}(k, m_b)$

if $\hat{x} \notin \mathrm{Domain}(Map)$

then $Map[\hat{x}] \xleftarrow{R} \mathcal{K}$

Adversary

Prepare $(m_0, m_1) \in \mathcal{M}^2$:

choose $\hat{x} \in \mathcal{X}$

Challenger $\xrightarrow{\text{pk}}$ Adversary

Adversary $\xrightarrow{m_0, m_1}$ Challenger

Challenger $\xrightarrow{(y, c)}$ Adversary

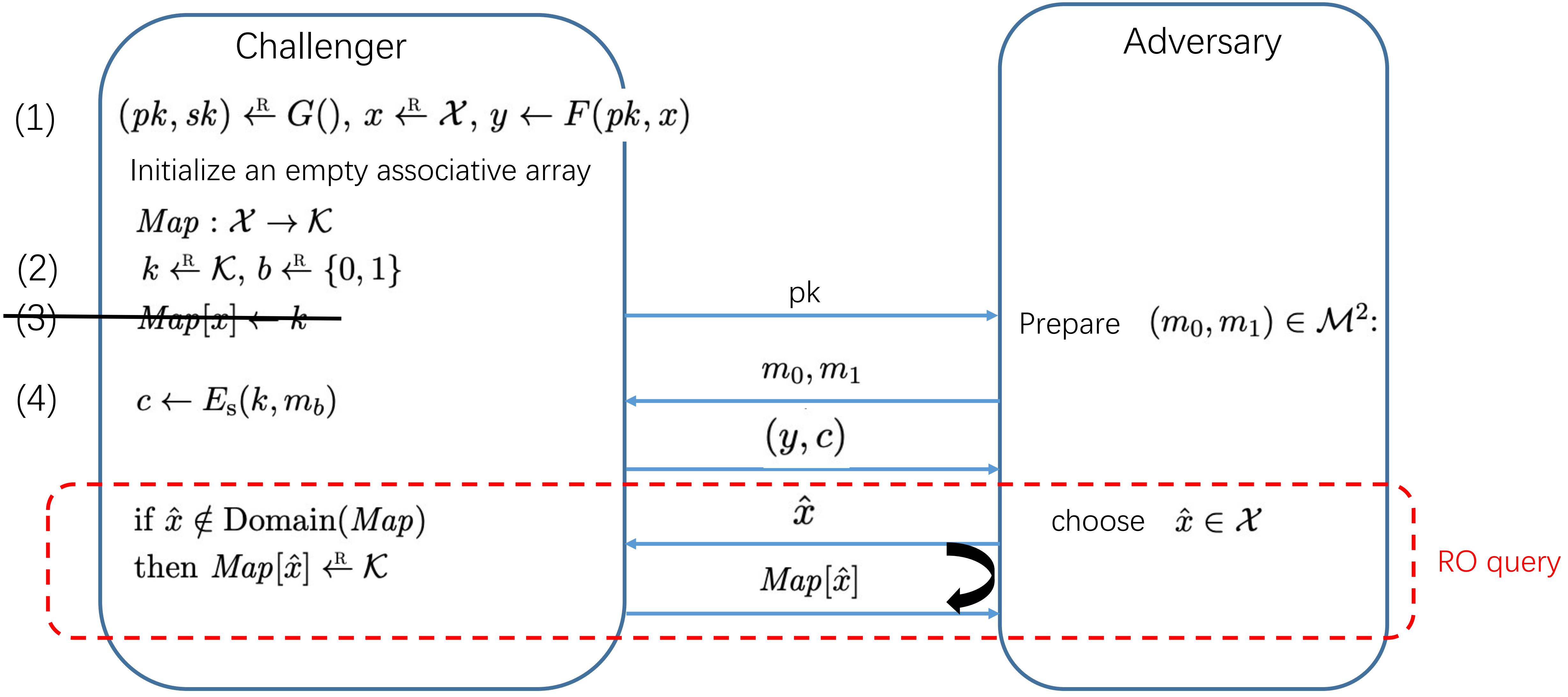
Adversary $\xrightarrow{\hat{x}}$ Challenger

Challenger $\xrightarrow{Map[\hat{x}]}$ Adversary

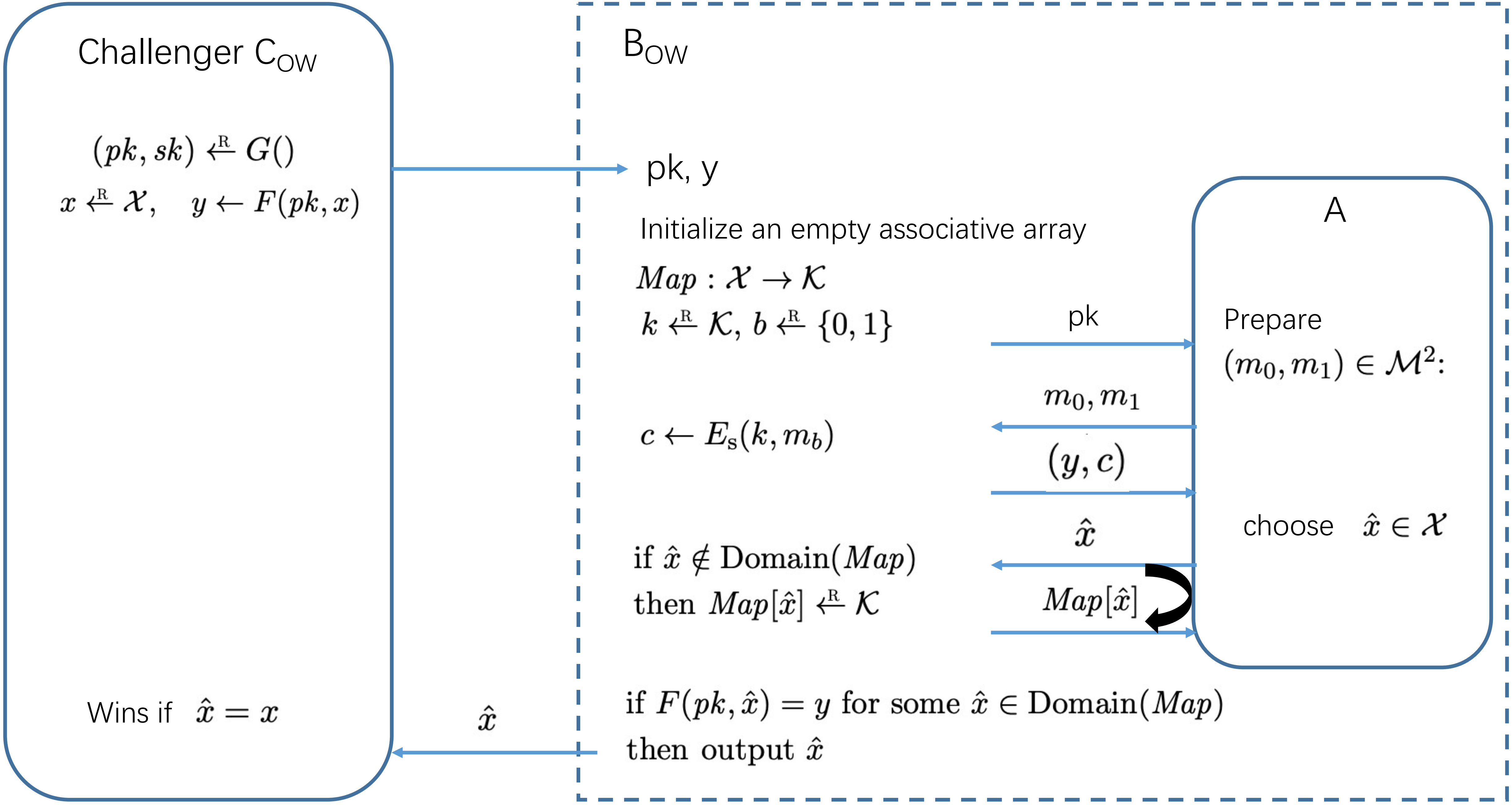
RO query

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

Game 1



Event Z: the adversary queries the random oracle at the point x $\Rightarrow$ $|\Pr[W_1] - \Pr[W_0]| \leq \Pr[Z]$



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