A generic hybrid construction of CPA encryption based on secure PRF

Pseudo-random function

F is **defined over** $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$

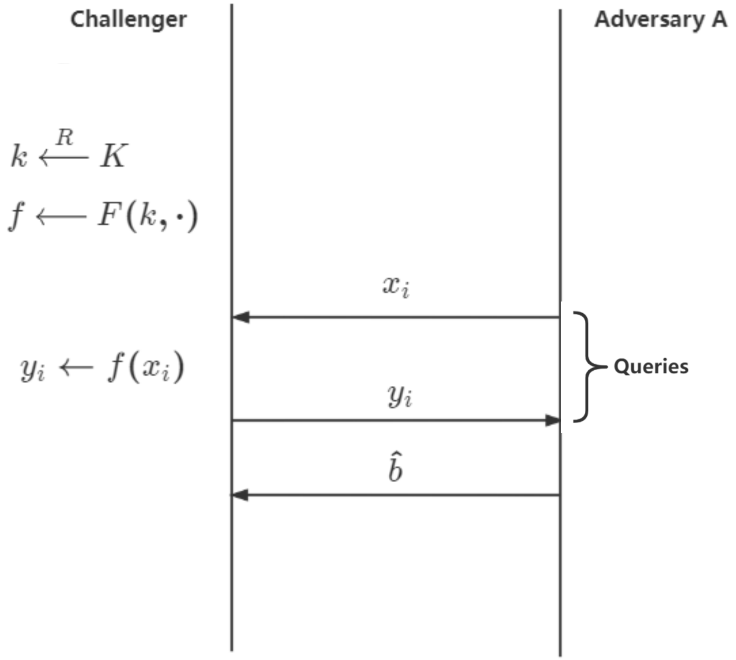
two inputs

a key k

an **input data block** x

output

$y := F(k, x)$



Attack Game 4.2 (PRF). For a given PRF F, defined over $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$, and for a given adversary $\mathcal{A}$, we define two experiments, Experiment 0 and Experiment 1. For $b = 0, 1$, we define:

Experiment b**:**

- The challenger selects $f \in \text{Funs}[\mathcal{X}, \mathcal{Y}]$ as follows:

  if $b = 0$: $k \xleftarrow{R} \mathcal{K}$, $f \leftarrow F(k, \cdot)$;
  if $b = 1$: $f \xleftarrow{R} \text{Funs}[\mathcal{X}, \mathcal{Y}]$.

- The adversary submits a sequence of queries to the challenger.

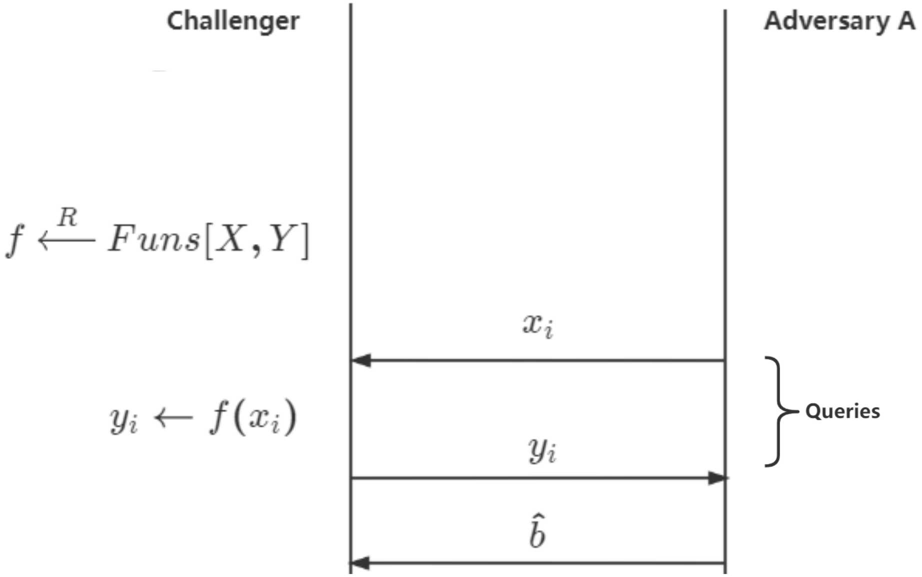
  For $i = 1, 2, \ldots,$ the ith query is an input data block $x_i \in \mathcal{X}$.

  The challenger computes $y_i \leftarrow f(x_i) \in \mathcal{Y}$, and gives y_i to the adversary.

- The adversary computes and outputs a bit $\hat{b} \in \{0, 1\}$.

For $b = 0, 1$, let W_b be the event that $\mathcal{A}$ outputs 1 in Experiment b. We define $\mathcal{A}$'s **advantage** with respect to F as

$$\text{PRFadv}[\mathcal{A}, F] := \Big|\Pr[W_0] - \Pr[W_1]\Big|. \tag{4.21}$$



Construction

- $\varepsilon = (E, D)$ be a cipher, defined over (K, M, C).
- F be a PRF defined over (K', X, K); so,the output space of F is the key space of ε.
- We define a new cipher $\varepsilon' = (E', D')$, defined over $(K', M, X \times C)$. As follows:
  - For $k' \in K'$ and $m \in M$,

$$E'(k', m) := x \xleftarrow{R} X, k \leftarrow F(k', x), c \leftarrow E(k, m), \text{ output } (x, c);$$

  - For $k' \in K'$ and $c' = (x, c) \in X \times C$,

$$D'(k', c') := k \leftarrow F(k', x), m \leftarrow D(k, c), \text{output } m.$$

Clearly,ε' is a probabilistic cipher.

Then ,ε' is CPA encryption based on secure PRF.

Theorem and proof sketch

- **Theorem. If $\boldsymbol{F}$ is a secure $\boldsymbol{PRF}$,$\boldsymbol{\varepsilon}$ is a semantically secure cipher , and $\boldsymbol{N} \coloneqq |\boldsymbol{X}|$ is super-poly, then the cipher $\boldsymbol{\varepsilon}'$described above is a $\boldsymbol{CPA}$ secure cipher.**
  - For a CPA adversary A that attacks ε', and it makes at most Q queries to its challenger, there exists a PRF adversary B_F to attacks F, and an SS adversary B_ε that attacks ε, where both B_F and B_ε are elementary wrappers around A, such that

$$CPAadv[A, \varepsilon'] \leq \frac{Q^2}{N} + 2 \cdot PRFadv[B_F, F] + Q \cdot SSadv\ [B_\varepsilon, \varepsilon]$$

- Its bit guessing version:

$$CPAadv^*[A, \varepsilon'] \leq \frac{Q^2}{2N} + PRFadv[B_F, F] + Q \cdot SSadv^*[B_\varepsilon, \varepsilon]$$

Basic strategy of the proof

- Define several games: Game 0, Game 1, Game 2, and Game 3. Each of these games is played between A and a different challenger. In each of these games, b denotes the random bit chosen by the challenger, while b'denotes the bit output by A. Also, for $j = 0, \ldots, 3$,we define W_j to be the event that $b' = b$ in Game j .
- The proof idea is to make sure for $j = 1, \ldots, 3$:

$$\left|Pr\left[W_j\right] - Pr\left[W_{j-1}\right]\right| = negligible$$

Game 0

Game 0 plays between A and the challenger in the bit-guessing version of $CPA\ security$ attack game . The challenger runs:

$b \xleftarrow{R} \{0,1\}$

$k' \xleftarrow{R} K'$

$for\ i \leftarrow 1\ to\ Q\ do$

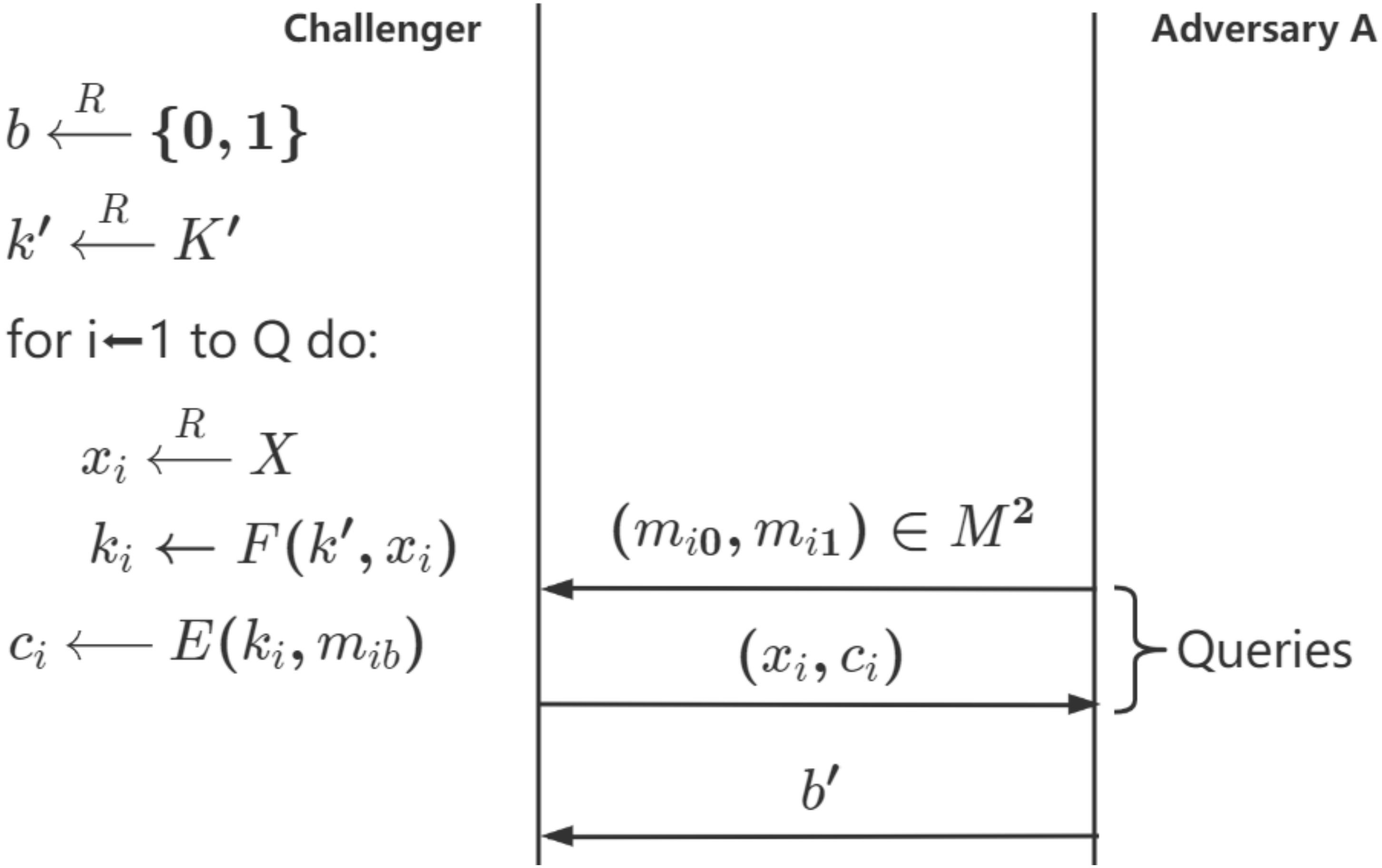
$\quad x_i \xleftarrow{R} X$

$\quad \boxed{k_i \leftarrow F(k', x_i)}$

upon receiving the ith query $(m_{i0}, m_{i1}) \in M^2$;

$\quad c_i \leftarrow E(k_i, m_{ib})$

send (x_i, c_i) to the adversary.



$$CPAadv^*[A, \varepsilon'] = |Pr[W_0] - 1/2|$$

Game 1

Game 1 plays "PRF card," replacing $F(k',\cdot)$ by a truly random function $f \in Funs[X, K]$. The challenger runs

$b \overset{R}{\leftarrow} \{0,1\}$

$f \overset{R}{\leftarrow} Funs[X, K]$.

$for\ i \leftarrow 1\ to\ Q\ do$

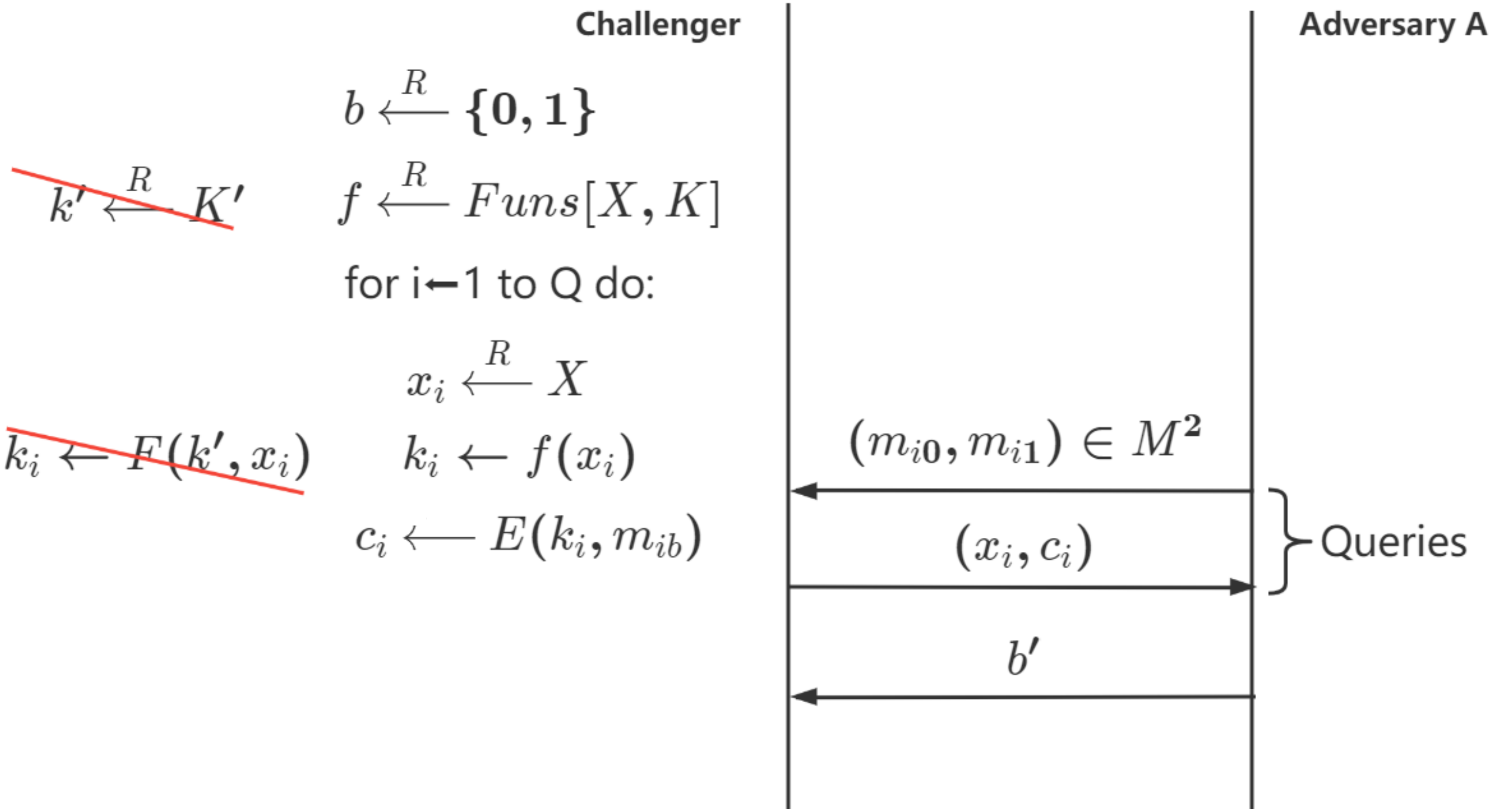
$\quad x_i \overset{R}{\leftarrow} X$

$\quad \boxed{k_i \leftarrow f(x_i)}$

upon receiving the ith query $(m_{i0}, m_{i1}) \in M^2$;

$\quad c_i \leftarrow E(k_i, m_{ib})$

$\quad$ send (x_i, c_i) to the adversary.



Claim1 : $|\Pr[W_1] - \Pr[W_0]| = PRFadv[B_F, F]$

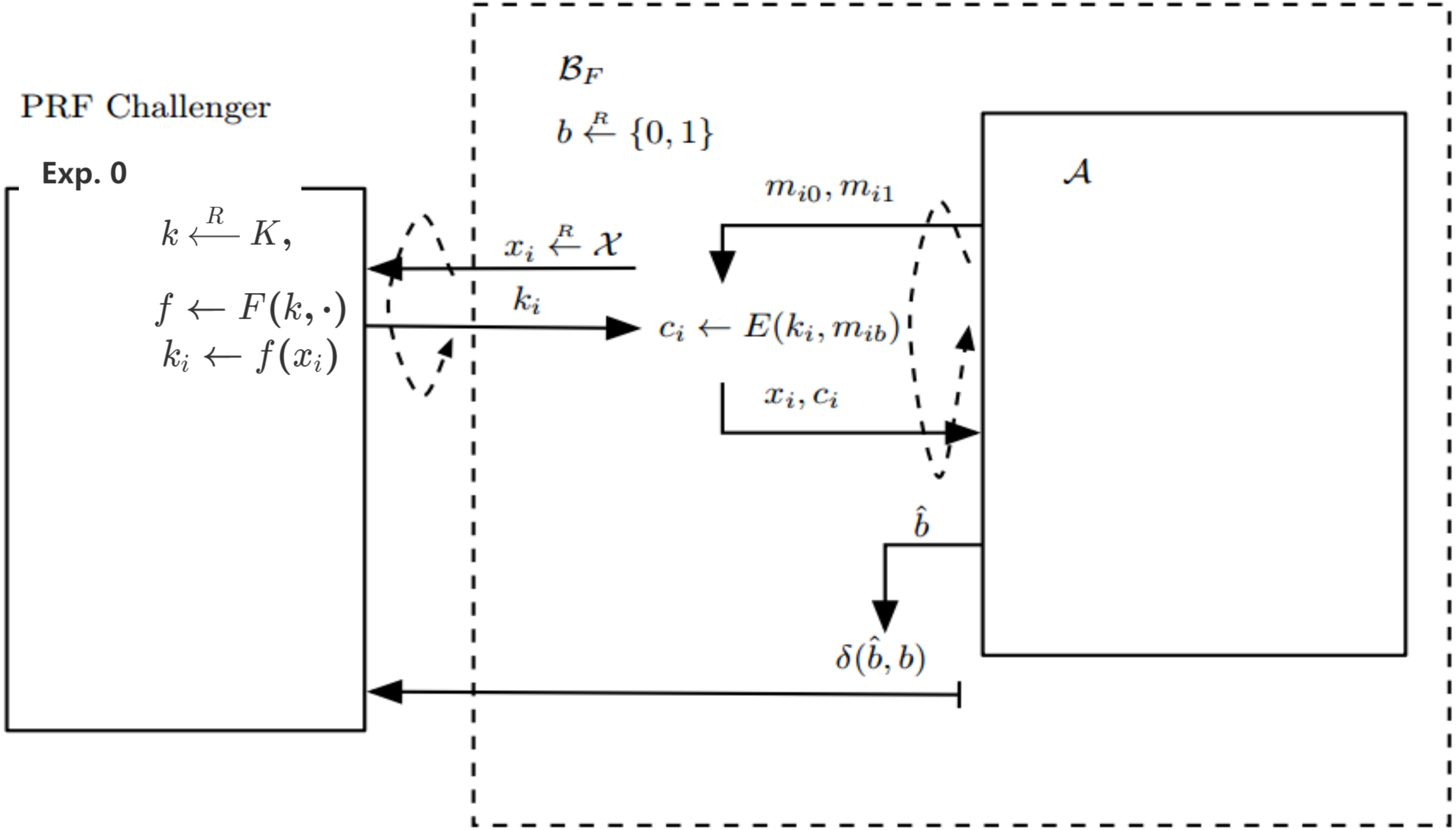
B_F is an efficient PRF adversary;

assuming that F is a secure PRF,

then $PRFadv[B_F, F]$ is negligible.

Construct B_F s.t. $|\Pr[W_1] - \Pr[W_0]| = PRFadv[B_F, F]$

- For Game 0 and Game 1,let adversary B_F plays the role of challenger to A.



- Eventually, A halts and outputs a bit b', at which time adversary B_F halts and outputs 1 if $b' = b$, and outputs 0 otherwise.

What do we have now?

$$CPAadv^*[A, \varepsilon'] = |Pr[W_0] - 1/2|$$

$$|\Pr[W_1] - \Pr[W_0]| = PRFadv[B_F, F]$$

$\Pr[W_1]$ = ?

We have played "PRF" card, we still have "SS" card.
Modify the game to the "SS" game.

Game 2

Game 2 uses “faithful gnome” idea to implement the random function f. The “gnome” has to keep track of the inputs to f, and detect if the same input is used twice. Challenger runs:

$b \xleftarrow{R} \{0,1\}$

$for\ i \leftarrow 1\ to\ Q\ do$

$\quad x_i \xleftarrow{R} X$

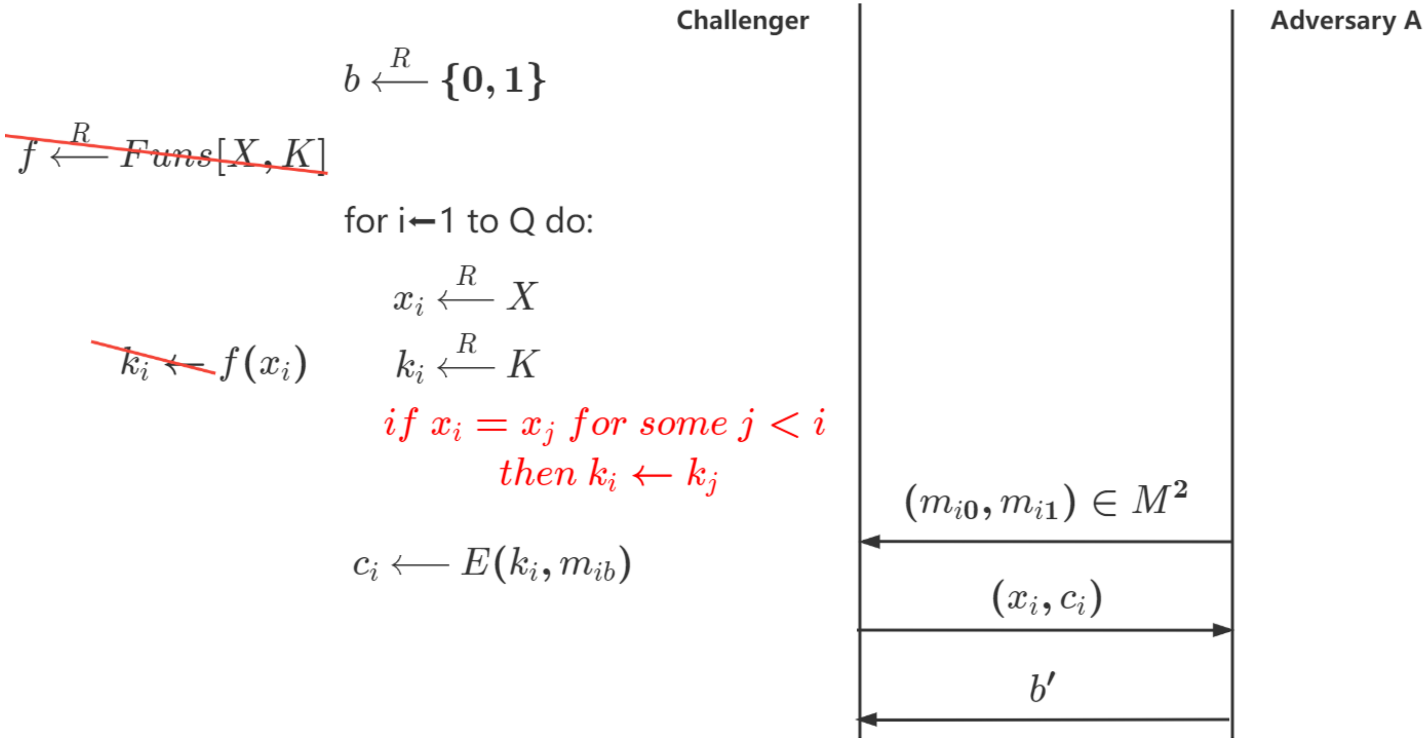
$\quad k_i \xleftarrow{R} K$

$\quad if\, x_i = x_j\ for\ some\ j < i\ then\ k_i \leftarrow k_j$

upon receiving the ith query $(m_{i0}, m_{i1}) \in M^2$;

$\qquad c_i \leftarrow E(k_i, m_{ib})$

$\qquad$send (x_i, c_i) to the adversary.



f is a faithful implementation of the random function ,then $\Pr[W_1] = \Pr[W_2]$

左边这个越来越像SS安全的方案E的CPA游戏了，还有两点不同：
1. 红色那条 2. 每次加密用不同密钥
对于1 我们去掉他构造Game 3，用差分引理证明Game 2 3可忽略
对于2 其实他符合MSS游戏，同时MSS游戏优势为Q倍SS游戏优势。

Game 3

Game3 makes that gnome "forgetful," dropping the highlight line in the previous game2:

$b \xleftarrow{R} \{0,1\}$
$for\ i \leftarrow 1\ to\ Q\ do$
$\quad x_i \xleftarrow{R} X$
$\quad k_i \xleftarrow{R} K$
upon receiving the ith query $(m_{i0}, m_{i1}) \in M^2$;
$\quad c_i \leftarrow E(k_i, m_{ib})$
$\quad$ send (x_i, c_i) to the adversary.

- Define Z to be the event that $x_i = x_j$ for some $i \neq j$. Games 2 and 3 proceed identically unless Z occurs; particularly, $W_2 \wedge \bar{Z}$ occurs if and only if $W_3 \wedge \bar{Z}$ occurs.Applying the Difference Lemma, we have

$$|\Pr[W_3] - \Pr[W_2]| \leq \Pr[Z]$$

Because there are less than $\frac{Q^2}{2}$ such events , each event occurs with probability $\frac{1}{N}$.

So , $\Pr[Z] \leq \frac{Q^2}{2N}$

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*

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

Proof. This is a simple calculation. We have

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

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 $\Pr[Z]$. $\square$

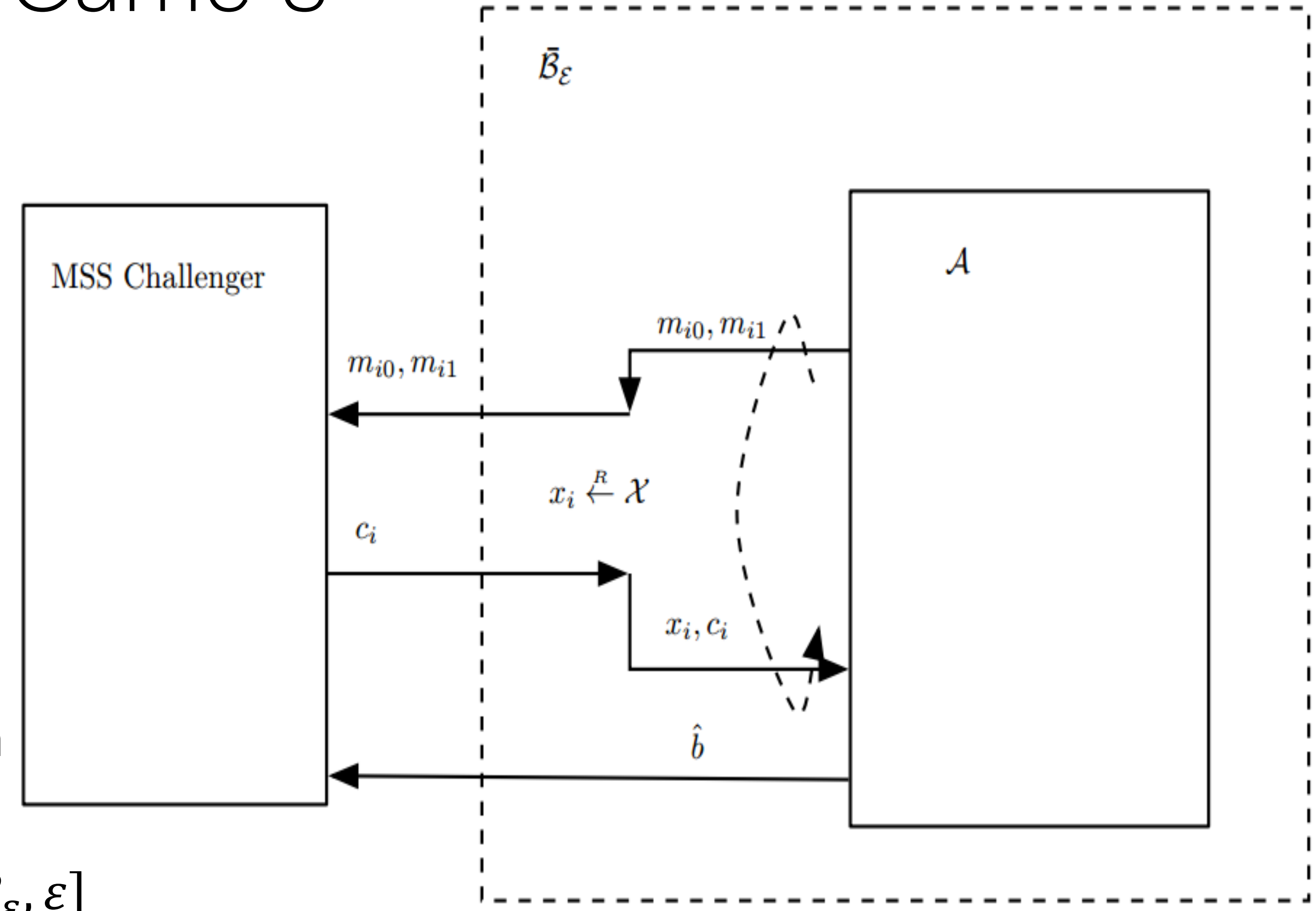
Game 3

$\bar{B}_\varepsilon$ is a multi-key semantic security adversary, playing multi-key semantic security attack with MSS challenger . It makes at most Q queries. Adversary $\bar{B}_\varepsilon$ plays the role of challenger to A.Then

$$\left|\Pr[W_3] - \frac{1}{2}\right| = MSSadv^*[\bar{B}_\varepsilon, \varepsilon]$$

Game3, independent encryption keys k_i are used to encrypt each message. So,

$$MSSadv^*[\bar{B}_\varepsilon, \varepsilon] = Q \cdot SSadv^*[B_\varepsilon, \varepsilon]$$



Putting together:

- $MSSadv^*[\bar{B}_\varepsilon, \varepsilon] = Q \cdot SSadv^*[B_\varepsilon, \varepsilon]$
- $CPAadv^*[A, \varepsilon'] = |Pr[W_0] - 1/2|$
- $|\Pr[W_1] - \Pr[W_0]| = PRFadv[B_F, F]$
- $\Pr[W_1] = \Pr[W_2]$
- $|\Pr[W_3] - \Pr[W_2]| \leq \Pr[Z]$
- $\Pr[Z] \leq \frac{Q^2}{2N}$
- $\left|\Pr[W_3] - \frac{1}{2}\right| = MSSadv^*[\bar{B}_\varepsilon, \varepsilon]$
- $\Rightarrow$ $CPAadv^*[A, \varepsilon'] \leq \frac{Q^2}{2N} + PRFadv[B_F, F] + Q \cdot SSadv^*[B_\varepsilon, \varepsilon]$