

A generic hybrid construction of CPA encryption based on secure PRF

2021.9.27

Jiageng Chen

A Graduate Course in Applied Cryptography version 0.5, Dan Boneh and Victor Shoup,
pp. 180 – 185, 5.4.1

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 $m \in M$,
$$E'(k', m) := x \stackrel{R}{\leftarrow} X, k \leftarrow F(k', x), c \stackrel{R}{\leftarrow} E(k, m), \text{ output } (x, c);$$
 - 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 idea

- **Theorem.** If F is a secure PRF , ε is a semantically secure cipher, and $N := |X|$ is super-poly, then the cipher ε' described above is a **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 $j = 0, \dots, 3$, we define W_j to be the event that $b' = b$ in Game j .
- The proof idea is to make sure for $j = 1, \dots, 3$:
$$|Pr[W_j] - Pr[W_{j-1}]| = \textit{negligible}$$

Game 0

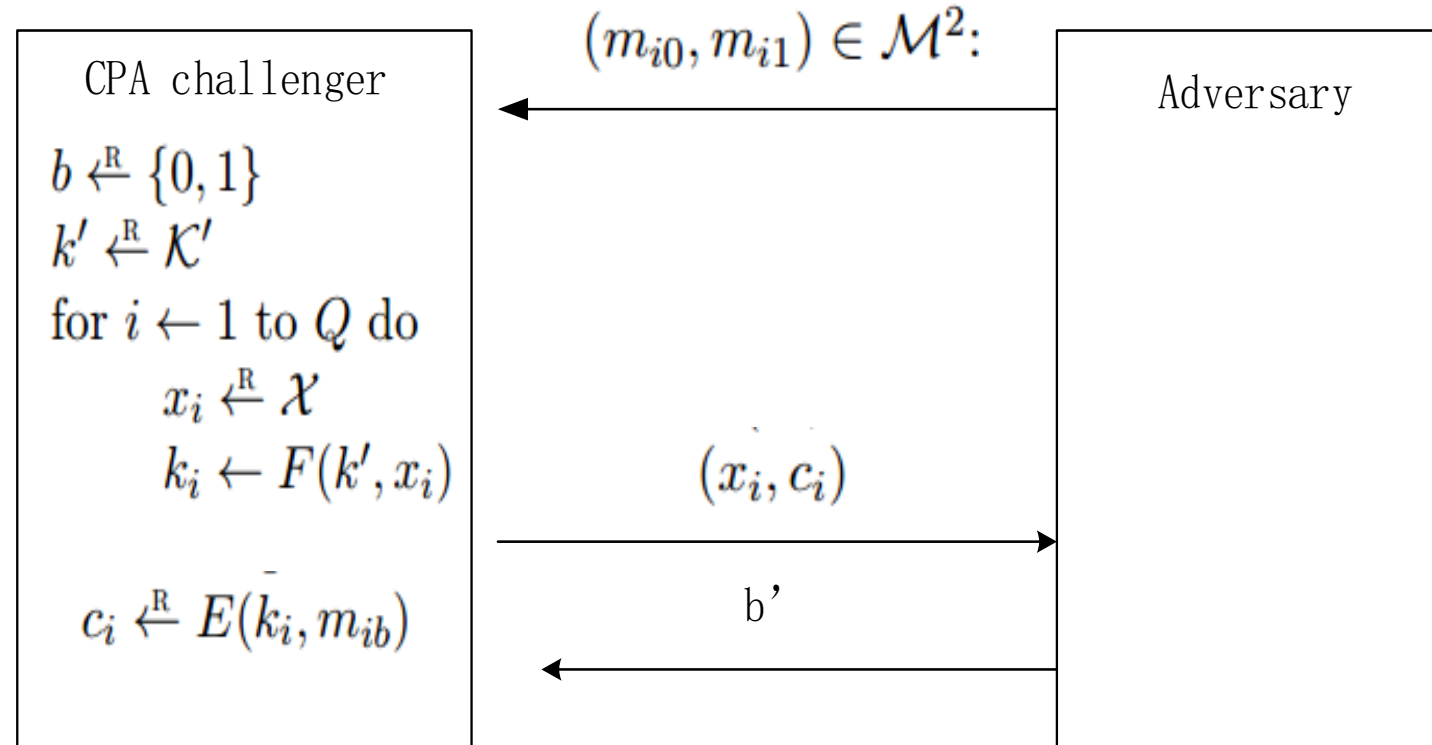
Game 0 plays between A and the challenger in the bit-guessing version of *CPA security* attack game. The challenger runs:

$b \xleftarrow{R} \{0,1\}$
 $k' \xleftarrow{R} K'$
for $i \leftarrow 1$ to Q do
 $x_i \xleftarrow{R} X$
 $k_i \leftarrow F(k', x_i)$

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

$c_i \xleftarrow{R} E(k_i, m_{ib})$

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 $f \in \text{Funs}[X, K]$. The challenger runs:

```

 $b \xleftarrow{R} \{0, 1\}$ 
 $f \xleftarrow{R} \text{Funs}[X, K]$ 
for  $i \leftarrow 1$  to  $Q$  do
     $x_i \xleftarrow{R} X$ 
     $k_i \leftarrow f(x_i)$ 

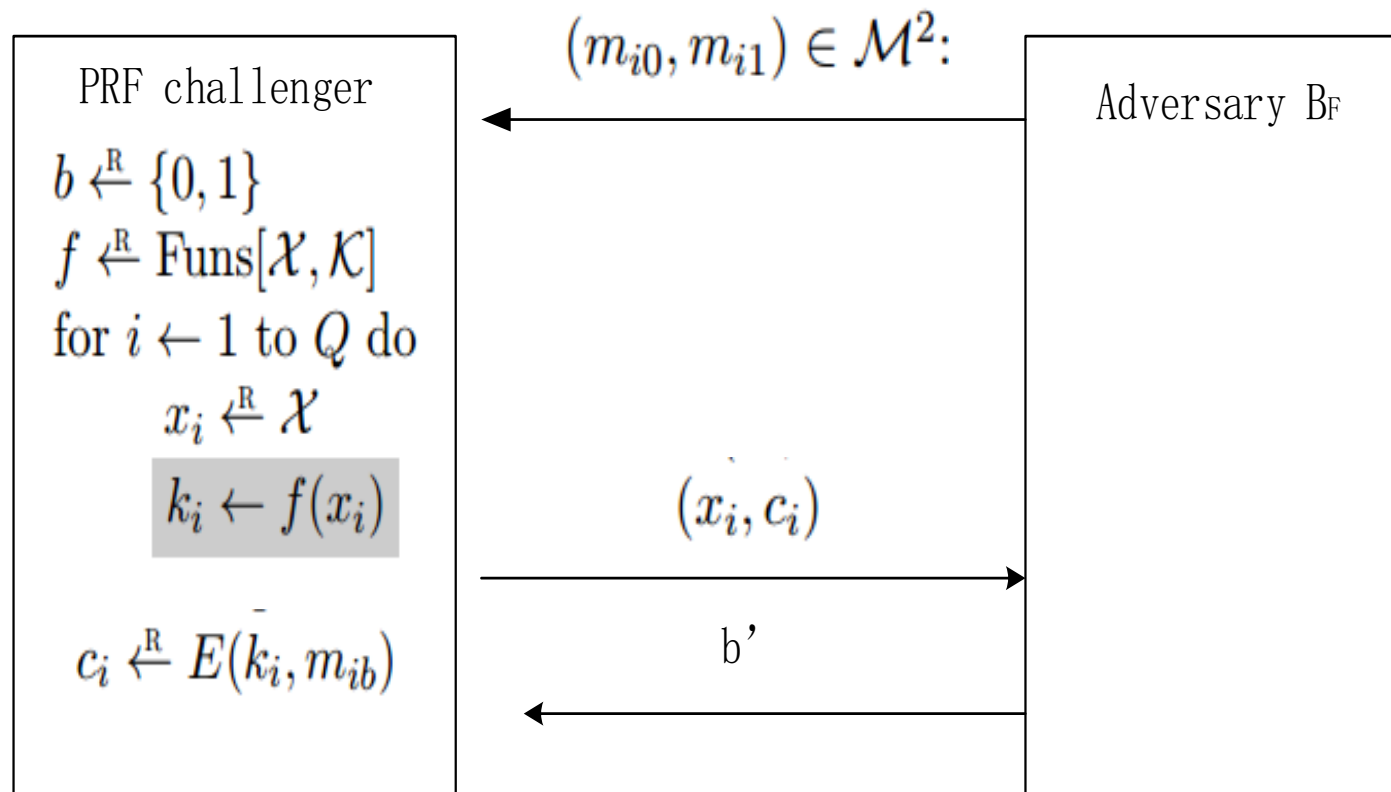
```

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

```

     $c_i \xleftarrow{R} E(k_i, m_{ib})$ 
    send  $(x_i, c_i)$  to the adversary.

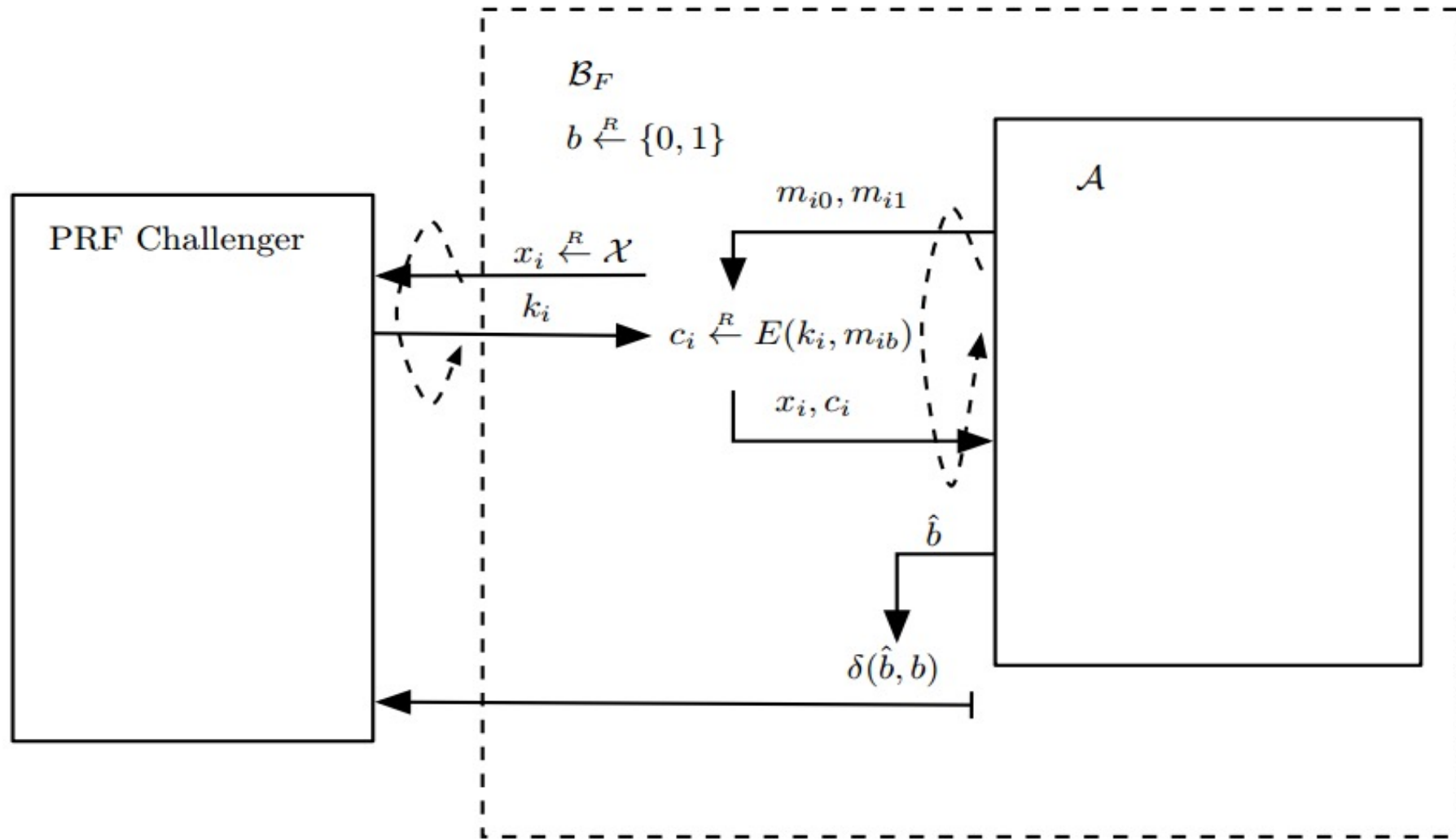
```



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

B_F is an efficient *PRF* adversary; assuming that F is a secure PRF, then $\text{PRFadv}[B_F, F]$ is negligible.

- 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.

Game 2

Game 2 implements the random function f . Challenger keeps 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*

$x_i \xleftarrow{R} X$

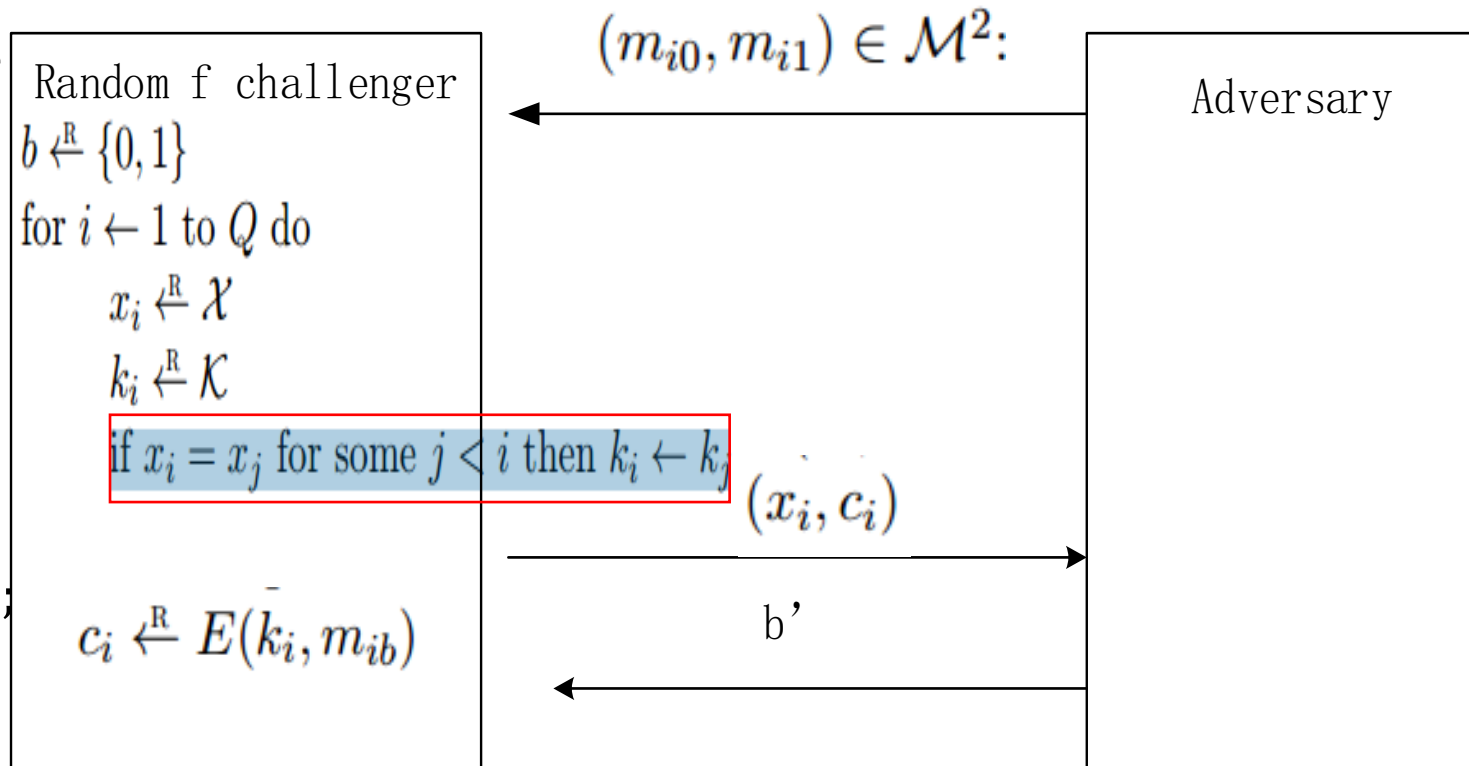
$k_i \xleftarrow{R} K$

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

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

$c_i \xleftarrow{R} E(k_i, m_{ib})$

send (x_i, c_i) to the adversary.



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

Game 3

Game3, dropping the highlight line in the previous game2:

```

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

$$\text{for } i \leftarrow 1 \text{ to } Q \text{ do}$$

$$x_i \stackrel{R}{\leftarrow} X$$

$$k_i \stackrel{R}{\leftarrow} K$$

$$\text{upon receiving the } i\text{th query}$$

$$(m_{i0}, m_{i1}) \in M^2;$$

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

$$\text{send } (x_i, c_i) \text{ to the adversary.}$$

```

- 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 $\frac{1}{N}$.

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

Game 3

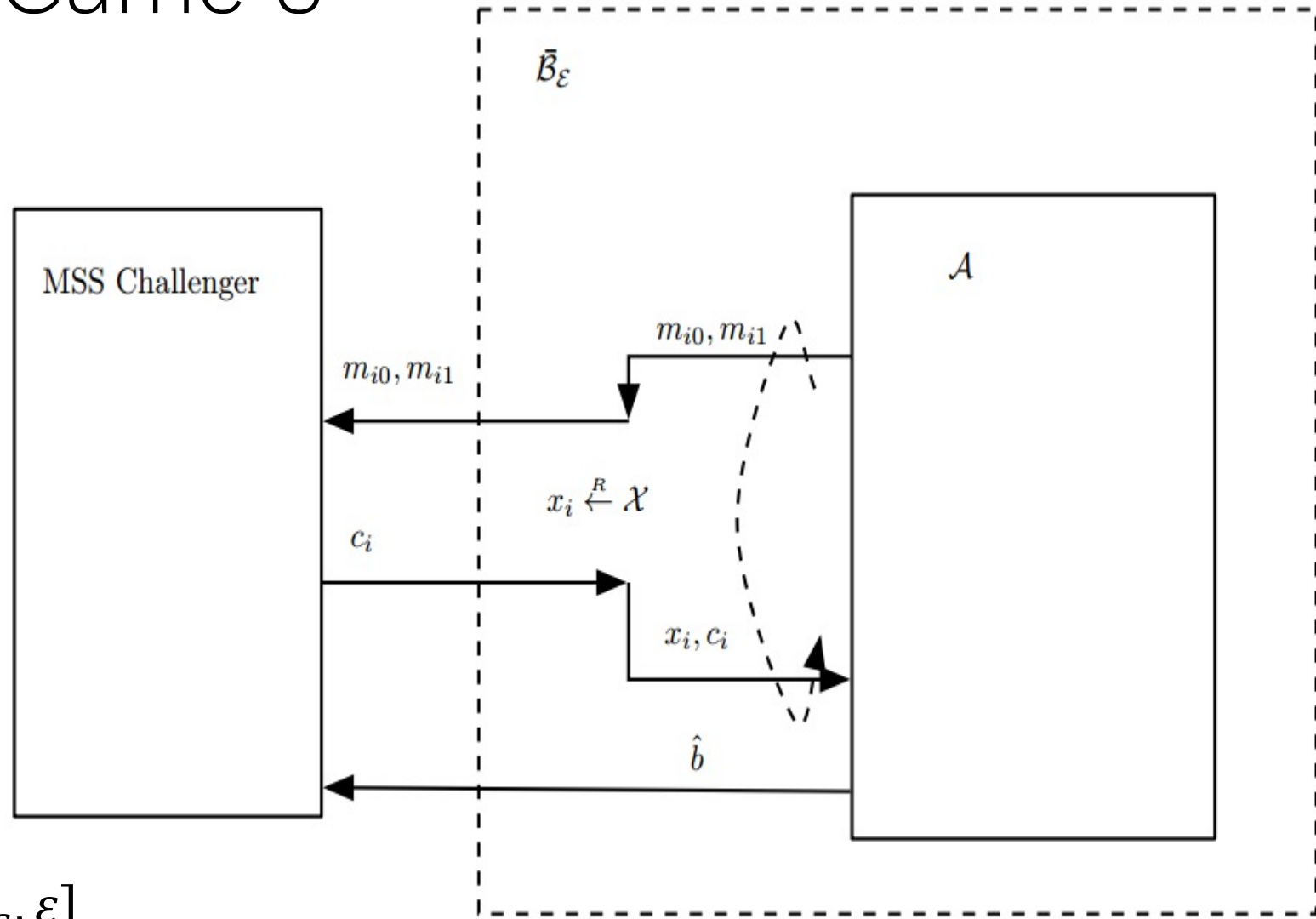
\bar{B}_ε is a multi-key semantic security adversary, playing multi-key semantic security attack with MSS challenger. It makes at most Q queries.

Adversary \bar{B}_ε 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:

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