Roadmap

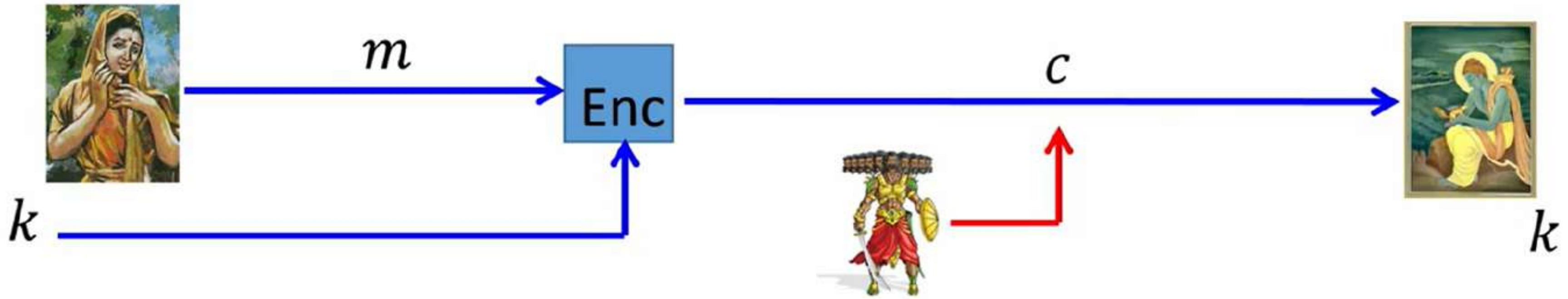
☐ Definition of semantic-security in COA attack model

☐ Equivalent indistinguishability based definition

☐ Introduction to reduction-based proofs

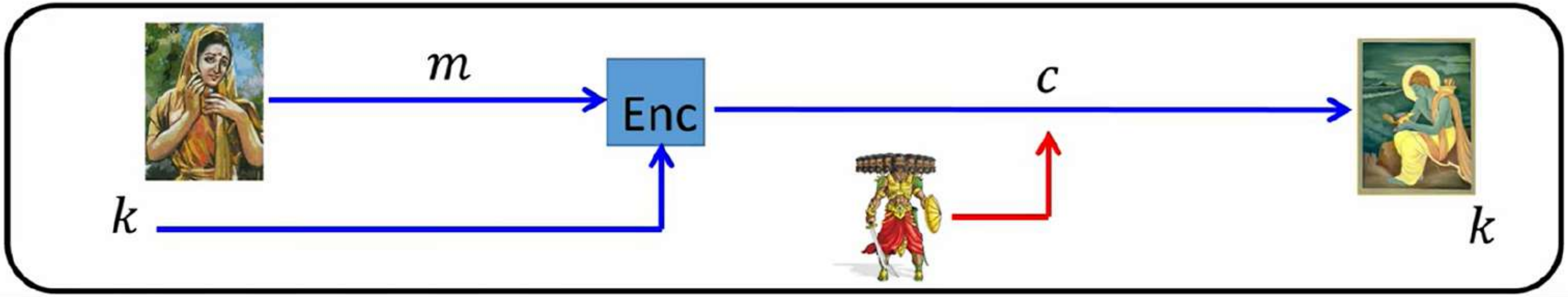
Semantic-security Definition in COA Model

- Intuition behind semantic security



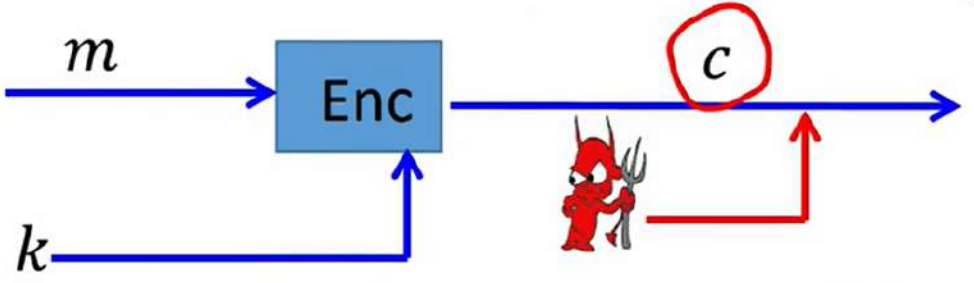
- Intuitively Enc is semantically secure, if the ciphertext does not reveal any additional information about the underlying plaintext
  - Should hold even if the adversary have any kind of prior external information about the underlying plaintext, leaked through other means
  - Extremely challenging to formalize the above intuition

Semantic-security Definition in COA Model



- ❑ Apart from the ciphertext c, adversary has access to an abstract function $h(m)$
  - ❖ Models any kind of prior external information about the underlying plaintext that might be leaked to the adversary through other means
- ❑ Goal of the adversary is to compute some function $f(m)$ of the underlying plaintext --- models the additional information that adversary wants to learn about m
- ❑ Semantic security: chances that the adversary could compute $f(m)$ using c and $h(m)$ is almost the same with which adversary could compute $f(m)$, just using $h(m)$
  - ❖ Ciphertext is of no help for the attacker in computing $f(m)$

Semantic-security Definition in COA Model



Algorithm $\mathcal{A}$: has access to c and $h(m)$

Algorithm $\mathcal{A}'$: has access to only $h(m)$

- ☐ Semantic security: Probability of $\mathcal{A}$ and $\mathcal{A}'$ computing $f(m)$ are almost the same
- ☐ Enc is semantically-secure (in the COA model) if the following holds:

$$\left| \; \underbrace{\Pr[\mathcal{A}(\mathrm{Enc}_k(m)\, h(m)) = f(m)]}_{\text{Prob. of } \mathcal{A} \text{ computing } f(m)\text{, with the aid of } c \text{ and } h(m)} - \underbrace{\Pr[\mathcal{A}'(h(m)) = f(m)]}_{\text{Prob. of } \mathcal{A}' \text{ computing } f(m)\text{, with the aid of just } h(m)} \; \right| \leq \mathrm{negl}(n)$$

Semantic Security in COA Model : Indistinguishability Based Definition

- ☐ An encryption scheme is semantically-secure (in the COA model) if the following holds:

$$\left| \Pr[\mathcal{A}(\mathsf{Enc}_k(m), h(m)) = f(m)] - \Pr[\mathcal{A}'(h(m)) = f(m)] \right| \leq \mathsf{negl}(n)$$

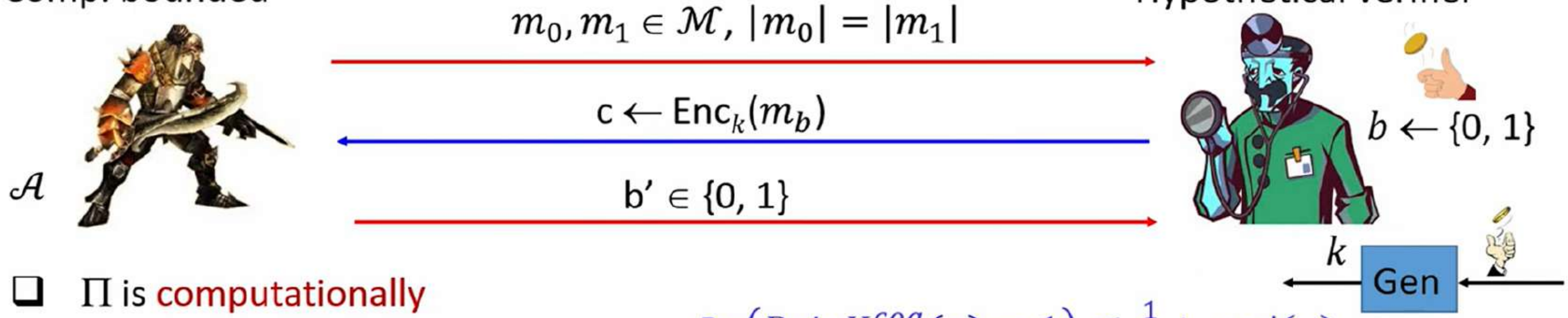
- ☐ Slightly complicated to prove semantic security as per the above definition
- ☐ Instead, we use an equivalent, indistinguishability based definition
  - ❖ Computationally-secure variant of indistinguishability based definition of perfect security

Indistinguishability Based Definition of Semantic Security in the COA Model

- ☐ Recall the indistinguishability based definition of perfect security

Publicly known scheme Π = (Gen, Enc, Dec)
over the message space $\mathcal{M}$

Experiment $PrivK^{coa}_{\mathcal{A},\Pi}(n)$



Comp. bounded

Hypothetical verifier

$m_0, m_1 \in \mathcal{M}$, $|m_0| = |m_1|$

c $\leftarrow$ Enc$_k(m_b)$

b' $\in$ {0, 1}

$\mathcal{A}$

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

k

Gen

- ☐ Π is computationally indistinguishable if for every $\mathcal{A}$:

$$\Pr\left(PrivK^{coa}_{\mathcal{A},\Pi}(n) = 1\right) \leq \frac{1}{2} + \mathsf{negl}(n)$$

Indistinguishability Based Definition of Semantic Security in the COA Model

☐ Π = (Gen, Enc, Dec) is semantically-secure (in the COA model) if the following holds:

$$\left| \quad \Pr[\mathcal{A}\left(\mathsf{Enc}_k(m), h(m)\right) = f(m)] \quad - \quad \Pr[\mathcal{A}'\left(h(m)\right) = f(m)] \quad \right| \leq \mathsf{negl}'(n)$$

$$\approx$$

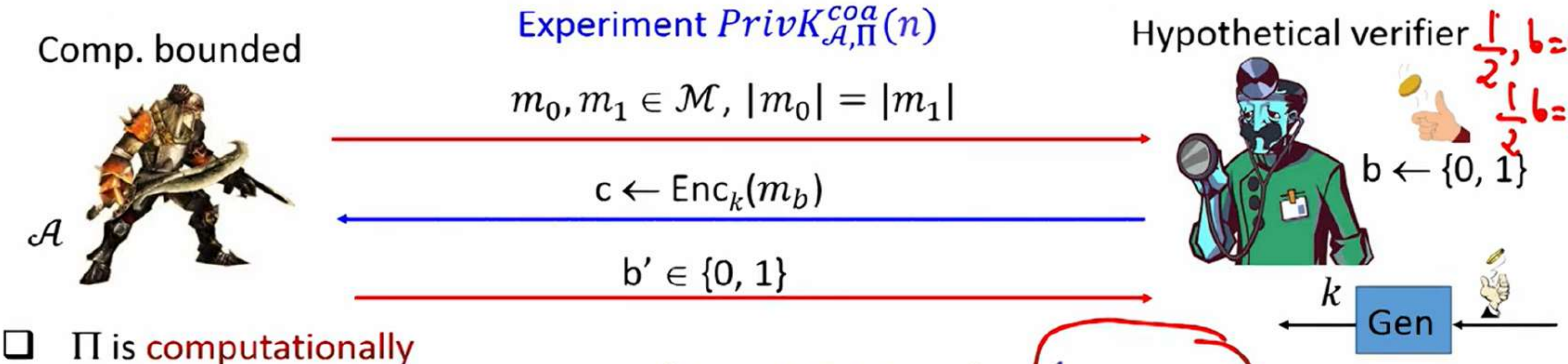
☐ Π = (Gen, Enc, Dec) is computationally indistinguishable (in the COA model) if for every $\mathcal{A}$:

$$\Pr\left(PrivK^{coa}_{\mathcal{A},\Pi}(n) = 1\right) \leq \frac{1}{2} + \mathsf{negl}(n)$$

☐ The above equivalence holds in other models as well (CPA, CCA)

- ❖ For the rest of the course, we will follow indistinguishability based security definitions

Indistinguishability Based Definition : An Equivalent Formulation



- ☐ Π is computationally indistinguishable if for every $\mathcal{A}$: $\Pr\left(PrivK^{coa}_{\mathcal{A},\Pi}(n) = 1\right) \leq \frac{1}{2} + \text{negl}(n)$

- ☐ Alternate definition : output of $\mathcal{A}$ should be the same, irrespective of b

$$\left|\ \Pr[\mathcal{A} \text{ outputs } b'=1 \mid \underline{b = 0}] \quad - \quad \Pr[\mathcal{A} \text{ outputs } b'=1 \mid \underline{b = 1}]\ \right| \leq \text{negl}'(n)$$

Indistinguishability Based Definition : An Equivalent Formulation

- A scheme Π = (Gen, Enc, Dec) over $\mathcal{M}$ is computationally indistinguishable if for every $\mathcal{A}$:

$$\Pr\left(PrivK^{coa}_{\mathcal{A},\Pi}(n) = 1\right) \leq \frac{1}{2} + \text{negl}'(n) \qquad \text{... (1)}$$

⇕

- A scheme Π = (Gen, Enc, Dec) over $\mathcal{M}$ is computationally indistinguishable if for every $\mathcal{A}$:

$$|\ \Pr[\mathcal{A} \text{ outputs } b'=1 \mid b = 0] \ - \ \Pr[\mathcal{A} \text{ outputs } b'=1 \mid b = 1]\ | \ \leq \text{negl}(n) \qquad \text{... (2)}$$

- Proof of (2) ⇒ (1)

$$\begin{aligned}
\Pr\left(PrivK^{coa}_{\mathcal{A},\Pi}(n) = 1\right) &= \frac{1}{2} . \{\Pr[\mathcal{A} \text{ outputs } b'=0 \mid b = 0] \ + \ \Pr[\mathcal{A} \text{ outputs } b'=1 \mid b = 1]\} \\
&= \frac{1}{2} . \{1 \ - \ \Pr[\mathcal{A} \text{ outputs } b'=1 \mid b = 0] \ + \ \Pr[\mathcal{A} \text{ outputs } b'=1 \mid b = 1]\} \\
&= \frac{1}{2} \ + \frac{1}{2} . \{\Pr[\mathcal{A} \text{ outputs } b'=1 \mid b = 1] - \Pr[\mathcal{A} \text{ outputs } b'=1 \mid b = 0]\} \\
&\leq \ ½ + \text{negl}'(n)
\end{aligned}$$

Significance of Indistinguishability Based Definition : An Illustration

☐ A scheme Π = (Gen, Enc, Dec) over $\mathcal{M}$ is computationally indistinguishable if for every $\mathcal{A}$:

$$\Pr\left(PrivK^{coa}_{\mathcal{A},\Pi}(n) = 1\right) \leq \frac{1}{2} + \text{negl}(n)$$

$$\approx$$

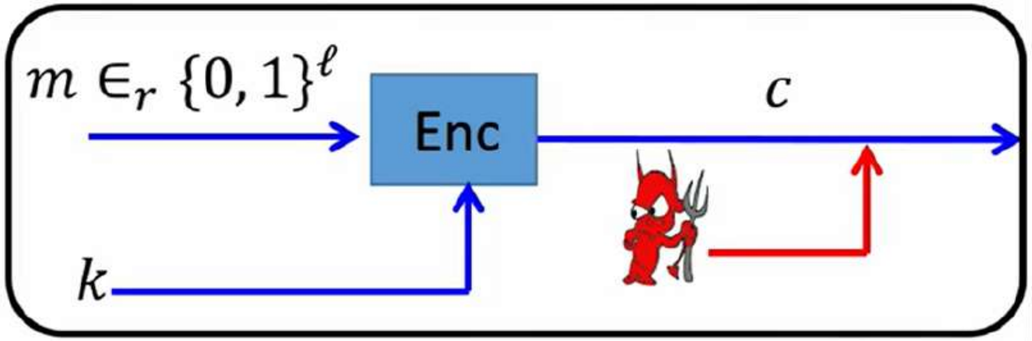
☐ Π = (Gen, Enc, Dec) is semantically-secure (in the COA model) if the following holds:

$$|\ \Pr[\mathcal{A}\left(\text{Enc}_k(m), h(m)\right) = f(m)] \quad - \quad \Pr[\mathcal{A}'\left(h(m)\right) = f(m)]| \ \leq \text{negl}(n)$$

☐ Example : we will show that if a scheme is computationally indistinguishable, then ciphertext reveals no information about the individual bits of the underlying plaintext, if $\mathcal{M} = \{0, 1\}^{\ell}$ and the plaintext is selected uniformly random

- ❖ Will introduce reduction based proofs

Significance of Indistinguishability Based Definition : An Illustration



- Claim : If Enc is computationally indistinguishable, then infeasible for the adversary to compute the ith bit of the plaintext with probability significantly better than ½
  - For each $i = 1, \ldots, \ell$:

$$\Pr[\mathcal{A}(\mathrm{Enc}_k(m)) = m^{(i)}] \leq \frac{1}{2} + \mathrm{negl}(n)$$

- Intuition : An adversary who can compute the i^{th} bit of the plaintext with probability significantly better than ½ , can significantly distinguish between encryptions of two random messages, whose i^{th} bits are different
  - The above intuition will be formalized through a reduction based proof
  - Reduction based proofs are central to cryptography

Significance of Indistinguishability Based Definition : An Illustration

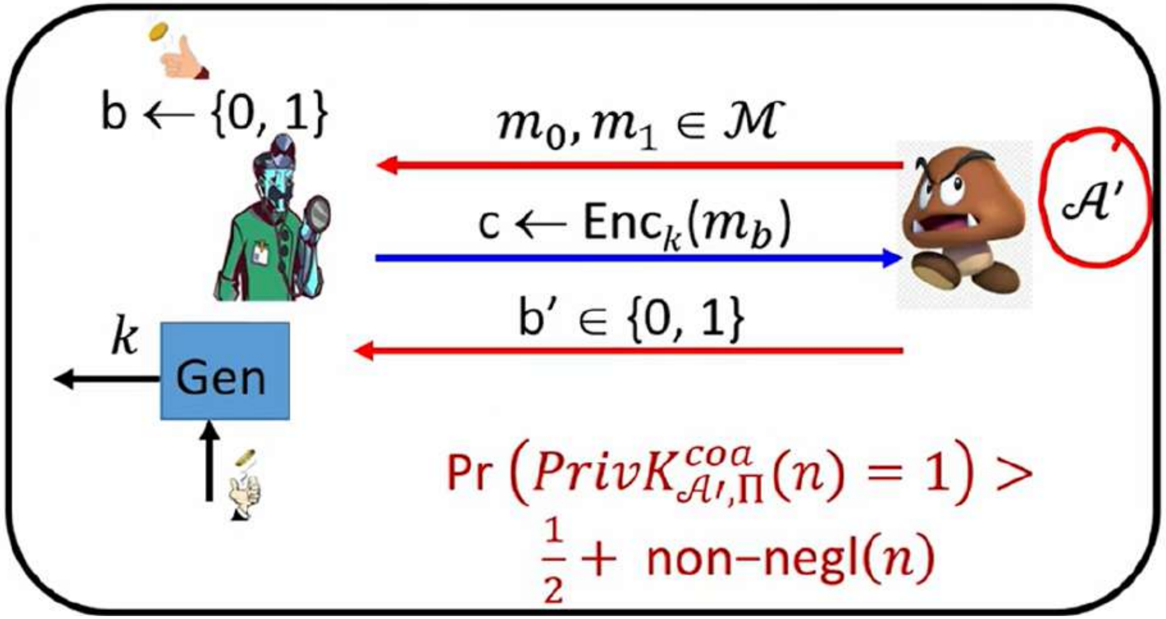
- ❑ If Π = (Gen, Enc, Dec) over $\mathcal{M} = \{0,1\}^{\ell}$ is computationally indistinguishable when the plaintext is randomly chosen from $\mathcal{M}$ $\Rightarrow$ $\Pr[\mathcal{A}(\text{Enc}_k(m)) = \underline{m^{(i)}}] \leq \frac{1}{2} + \text{negl}(n)$

- ❑ Proof by contrapositive

Significance of Indistinguishability Based Definition : An Illustration

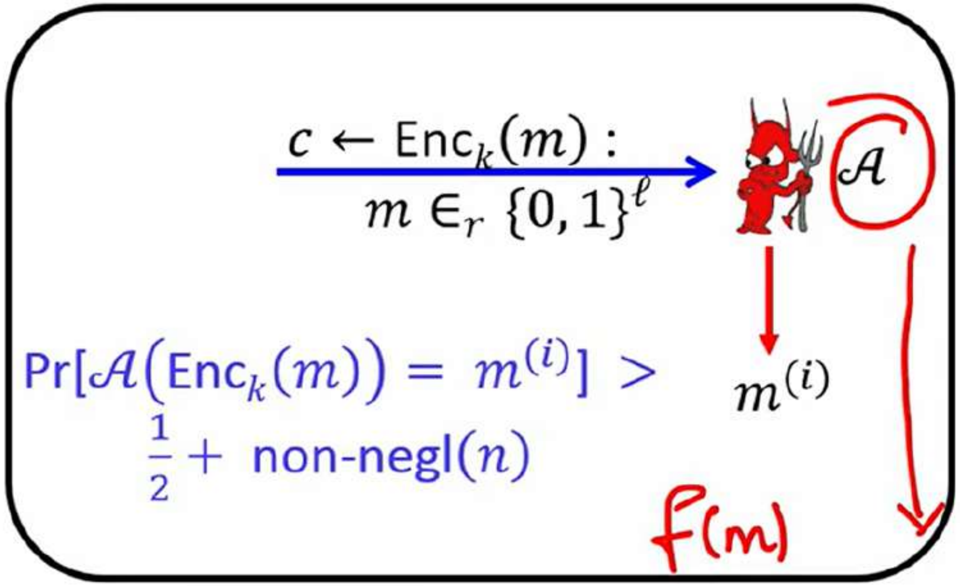
- ~~If Π = (Gen, Enc, Dec) over $\mathcal{M} = \{0,1\}^{\ell}$ is computationally indistinguishable when the plaintext is randomly chosen from $\mathcal{M}$~~ $\Rightarrow$ ~~$\Pr[\mathcal{A}(\mathsf{Enc}_k(m)) = m^{(i)}] \leq \frac{1}{2} + \mathsf{negl}(n)$~~

- Proof by contrapositive



$\Pr\left(PrivK^{coa}_{\mathcal{A}',\Pi}(n) = 1\right) > \frac{1}{2} +$ non−negl(n)

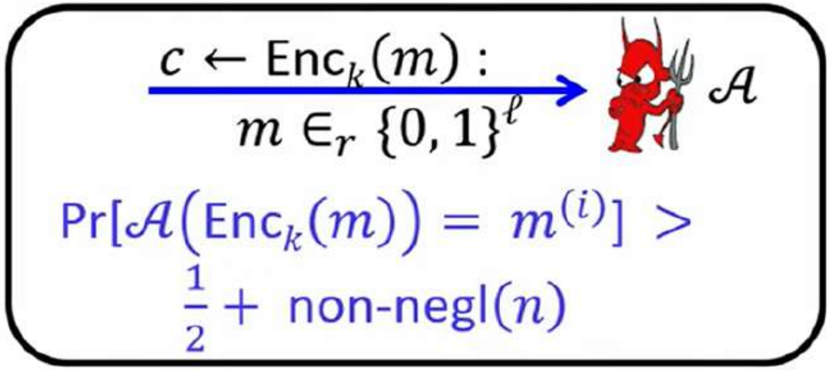
$\Leftarrow$



$\Pr[\mathcal{A}(\mathsf{Enc}_k(m)) = m^{(i)}] > \frac{1}{2} +$ non-negl(n)

Significance of Indistinguishability Based Definition : An Illustration

- ❑ Let there exist an adversary $\mathcal{A}$, who can compute the ith bit of a random plaintext by seeing the ciphertext with probability significantly better than ½

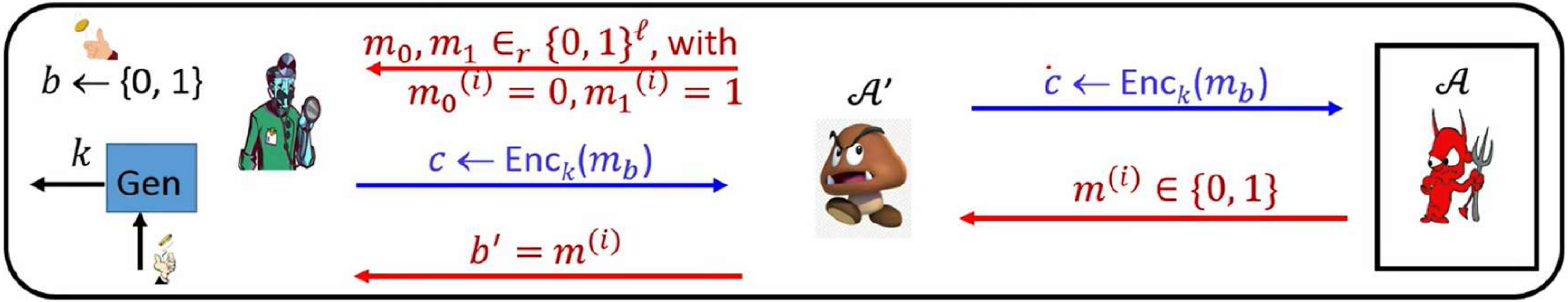


$c \leftarrow \text{Enc}_k(m)$: $m \in_r \{0,1\}^{\ell}$

$\mathcal{A}$

$\Pr[\mathcal{A}\left(\text{Enc}_k(m)\right) = m^{(i)}] > \frac{1}{2} + \text{non-negl}(n)$

- ❑ Consider the following adversary $\mathcal{A}'$, for the COA-indistinguishability game



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

k

Gen

$m_0, m_1 \in_r \{0,1\}^{\ell}$, with $m_0{}^{(i)} = 0, m_1{}^{(i)} = 1$

$c \leftarrow \text{Enc}_k(m_b)$

$b' = m^{(i)}$

$\mathcal{A}'$

$c \leftarrow \text{Enc}_k(m_b)$

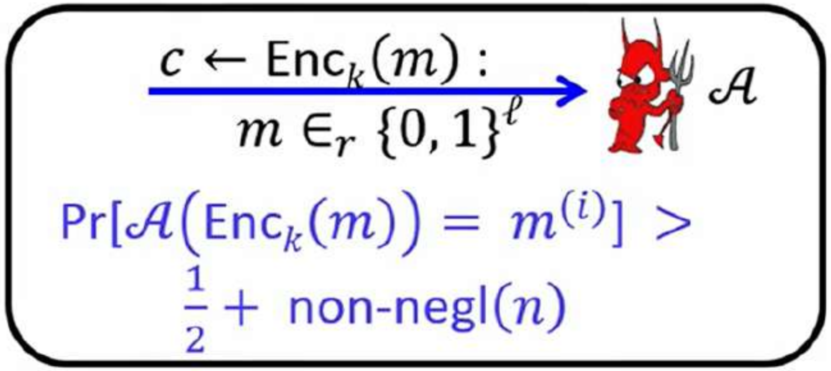
$m^{(i)} \in \{0,1\}$

$\mathcal{A}$

- ❑ Prob. that $\mathcal{A}'$ outputs $b' = b$ in the COA indistinguishability game is the same as Prob. that $\mathcal{A}$ correctly outputs $m^{(i)}$ after seeing the challenge ciphertext c

Significance of Indistinguishability Based Definition : An Illustration

- Let there exist an adversary $\mathcal{A}$, who can compute the ith bit of a random plaintext by seeing the ciphertext with probability significantly better than ½
- Consider the following adversary $\mathcal{A}'$, for the COA-indistinguishability game

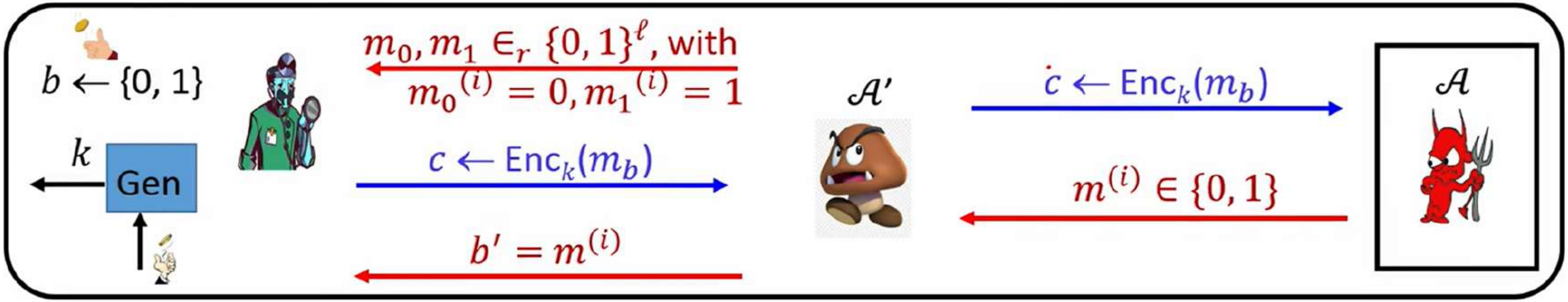


$c \leftarrow \text{Enc}_k(m)$:

$m \in_r \{0, 1\}^\ell$

$\mathcal{A}$

$\Pr[\mathcal{A}(\text{Enc}_k(m)) = m^{(i)}] > \frac{1}{2} + \text{non-negl}(n)$



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

k

Gen

$m_0, m_1 \in_r \{0, 1\}^\ell$, with $m_0{}^{(i)} = 0, m_1{}^{(i)} = 1$

$c \leftarrow \text{Enc}_k(m_b)$

$b' = m^{(i)}$

$\mathcal{A}'$

$c \leftarrow \text{Enc}_k(m_b)$

$m^{(i)} \in \{0, 1\}$

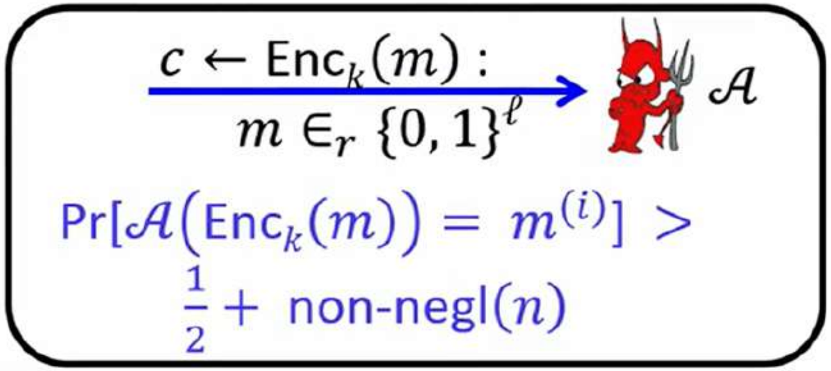
$\mathcal{A}$

$$\Pr\left(PrivK^{coa}_{\mathcal{A}',\Pi}(n) = 1\right) = \Pr[\mathcal{A}(\text{Enc}_k(m)) = m^{(i)}]$$

Significance of Indistinguishability Based Definition : An Illustration

- Let there exist an adversary $\mathcal{A}$, who can compute the ith bit of a random plaintext by seeing the ciphertext with probability significantly better than ½

- Consider the following adversary $\mathcal{A}'$, for the COA-indistinguishability game

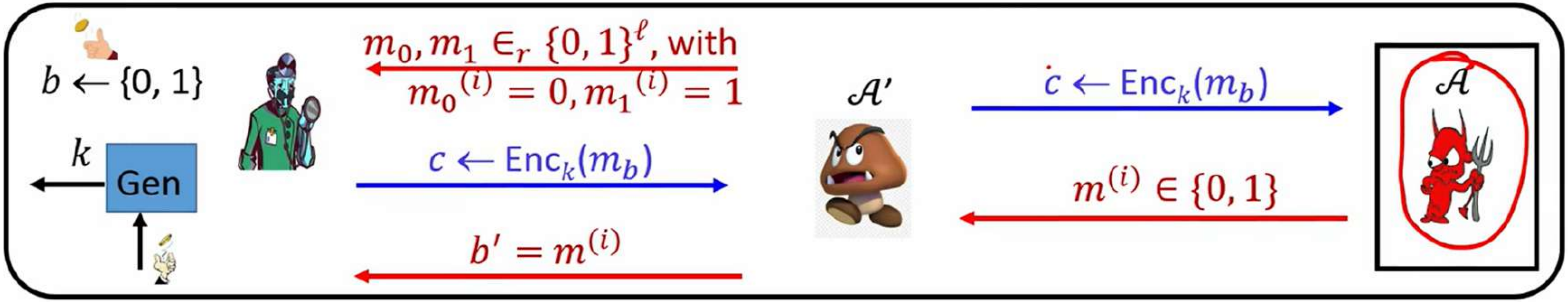


$c \leftarrow \mathrm{Enc}_k(m)$:

$m \in_r \{0,1\}^\ell$

$\mathcal{A}$

$\Pr[\mathcal{A}(\mathrm{Enc}_k(m)) = m^{(i)}] > \frac{1}{2} + \text{non-negl}(n)$



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

k

Gen

$m_0, m_1 \in_r \{0,1\}^\ell$, with $m_0{}^{(i)} = 0, m_1{}^{(i)} = 1$

$c \leftarrow \mathrm{Enc}_k(m_b)$

$b' = m^{(i)}$

$\mathcal{A}'$

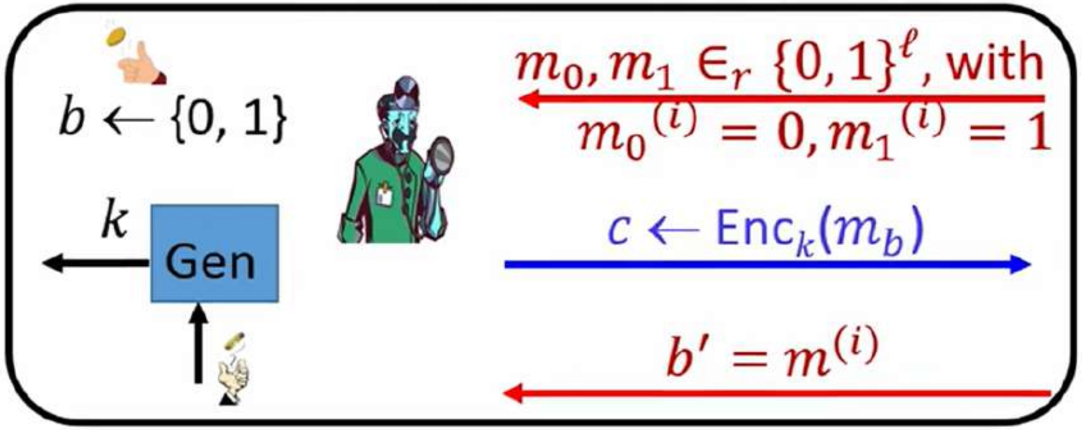
$c \leftarrow \mathrm{Enc}_k(m_b)$

$m^{(i)} \in \{0,1\}$

$\mathcal{A}$

$$\Pr\left(PrivK^{coa}_{\mathcal{A}',\Pi}(n) = 1\right) = \Pr[\mathcal{A}(\mathrm{Enc}_k(m)) = m^{(i)}] > \frac{1}{2} + \text{non-negl}(n)$$

The Reduction Based Proof : Important Details



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

k

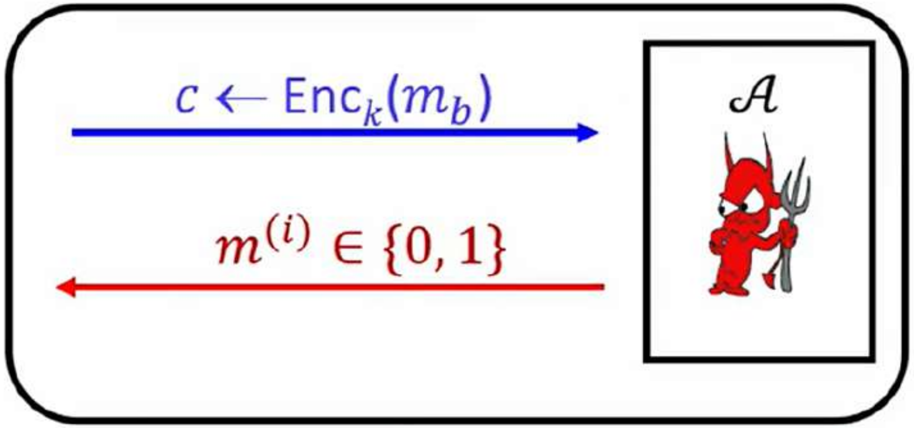
Gen

$m_0, m_1 \in_r \{0,1\}^\ell$, with $m_0^{(i)} = 0, m_1^{(i)} = 1$

$c \leftarrow \mathsf{Enc}_k(m_b)$

$b' = m^{(i)}$

$\mathcal{A}'$



$c \leftarrow \mathsf{Enc}_k(m_b)$

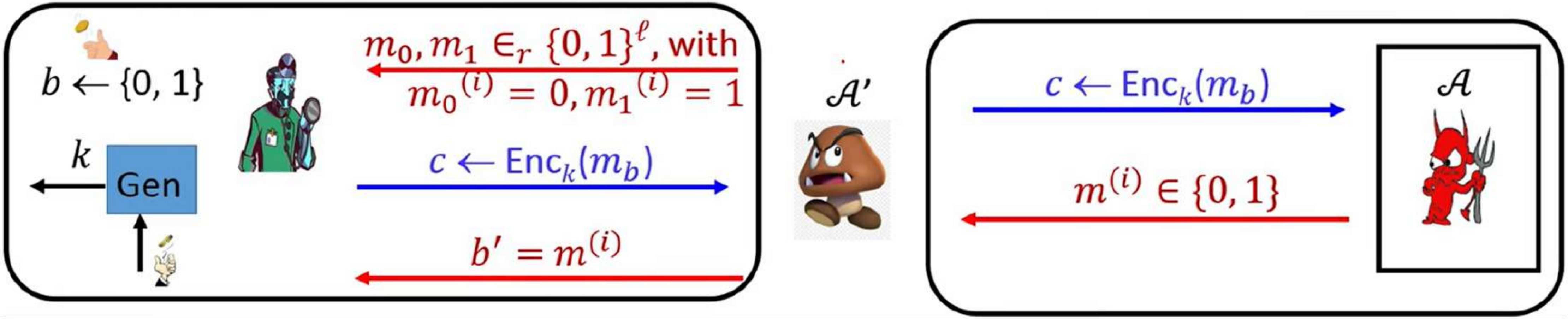
$m^{(i)} \in \{0, 1\}$

$\mathcal{A}$

← COA-experiment →

⟸ A' taking help of A

The Reduction Based Proof : Important Details



- Running time of $\mathcal{A}'$ is the same as that of $\mathcal{A}$
  - If $\mathcal{A}$ runs in polynomial time, then so does $\mathcal{A}'$

- Algorithm $\mathcal{A}'$ invokes algorithm $\mathcal{A}$ in a black-box fashion
  - $\mathcal{A}'$ knows nothing about the internal working of $\mathcal{A}$
  - Interaction with $\mathcal{A}$ handled via input/output interface
  - $\mathcal{A}'$ provides $\mathcal{A}$ with a view which is exactly the same that $\mathcal{A}$ expects at its input interface to launch its attack --- encryption of a random ℓ-bit string, with ith bit being either 0 or 1