18-733 Spring 2016
Semantic Security Review

Kyle Soska

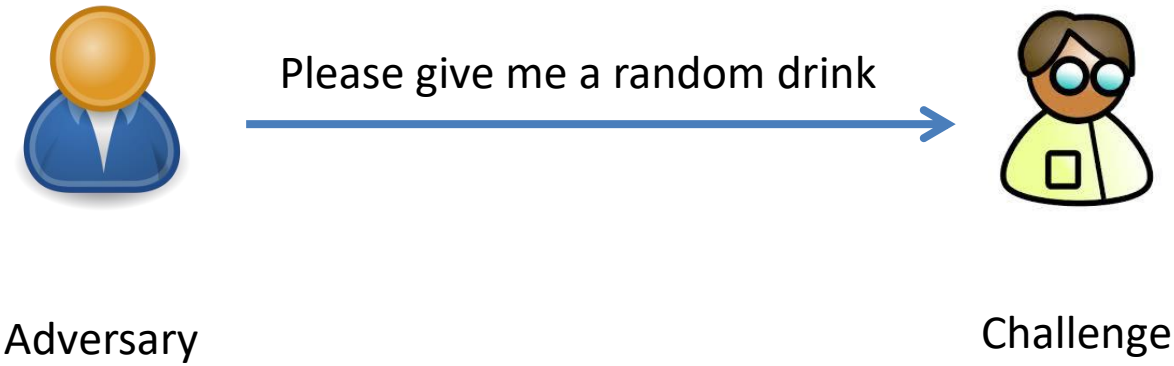
Jan 27, 2017

Topics Covered

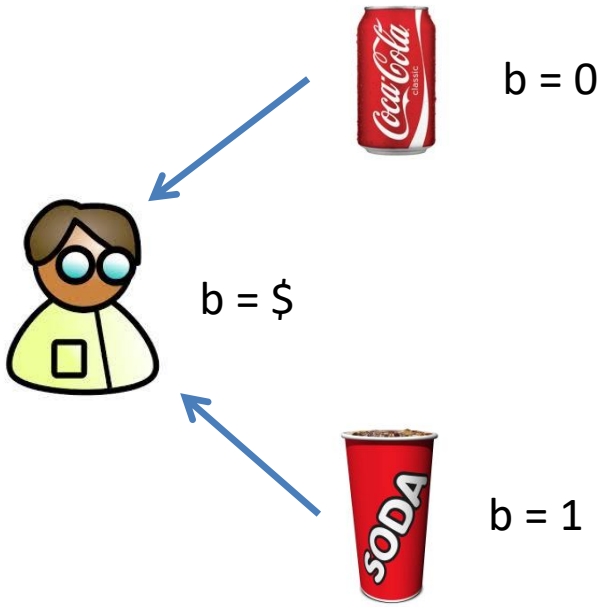
- Stream Ciphers
  - One Time Pad
  - Many Time Pad
- PRNG
  - Statistical tests
  - Security game for secure PRNG
- Perfect Secrecy
- Semantic Security
  - Security Game Definitions

Security Games – Overview

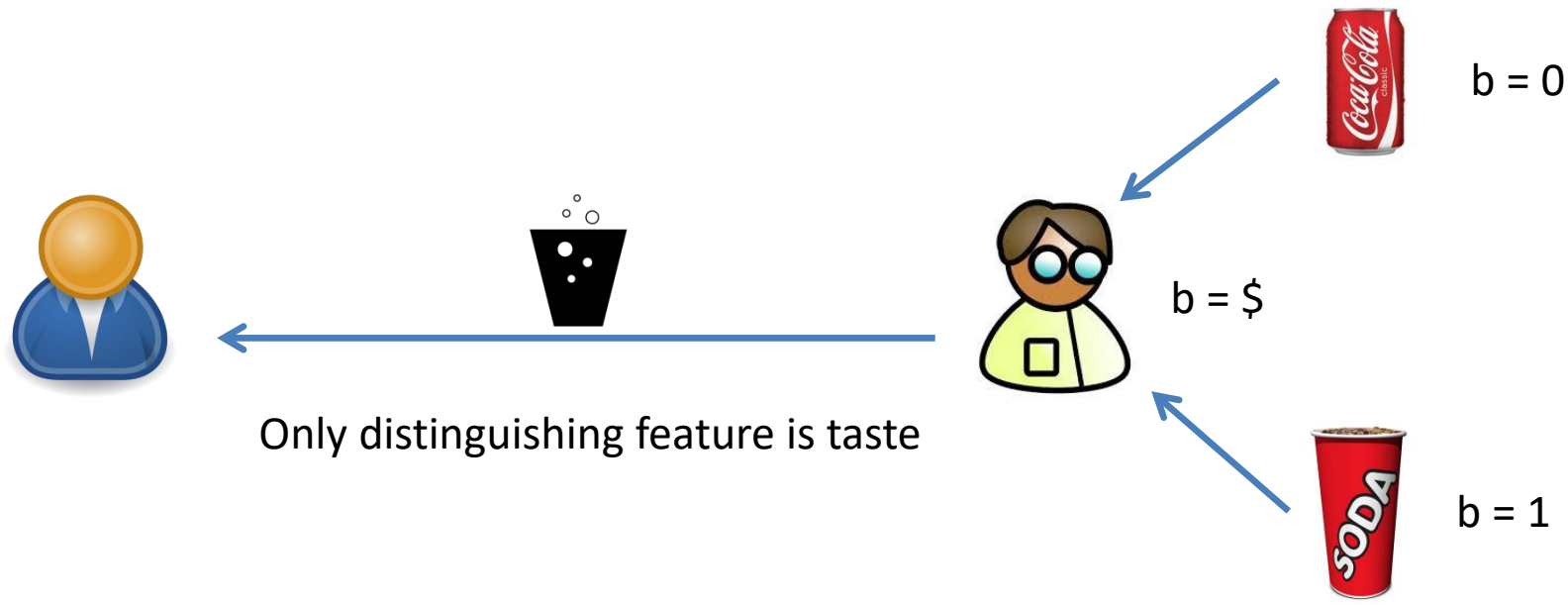
Security Games – Blind Taste Test



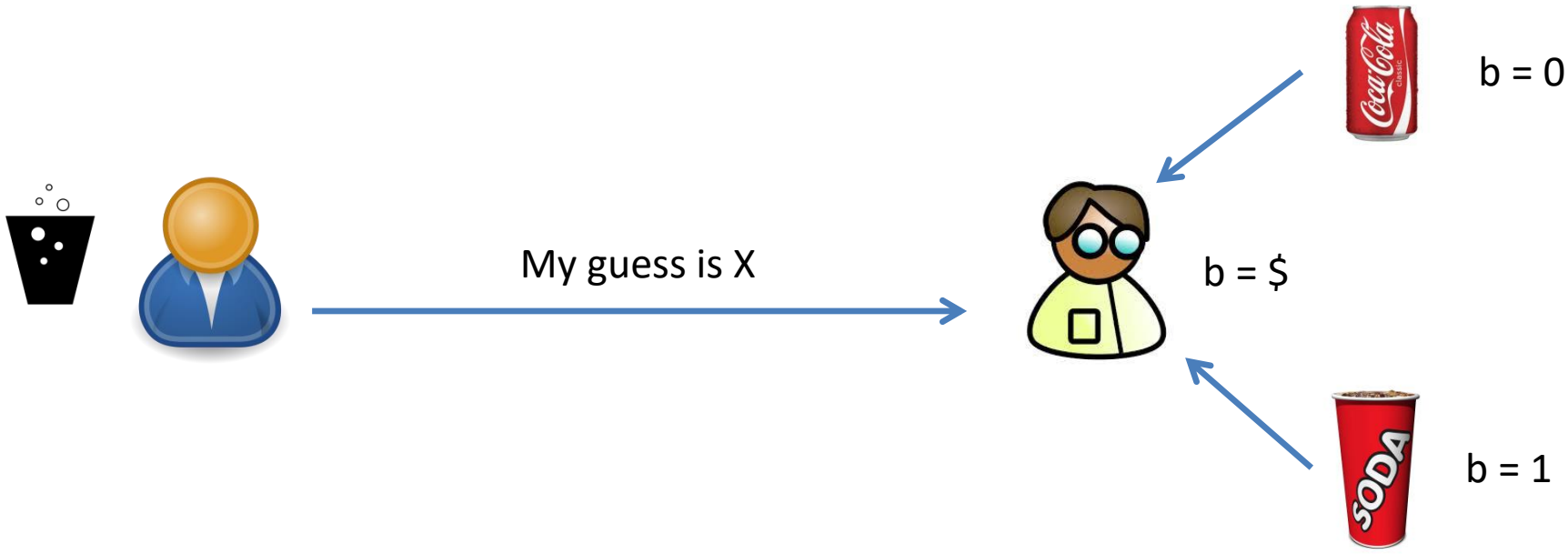
Security Games – Blind Taste Test



Security Games – Blind Taste Test



Security Games – Blind Taste Test



Security Games - Adversary

- Wine Tasting Adversaries:
  - People who have never tasted wine
  - People who sometimes drink wine
  - People who often drink wine
  - Professional wine taster (sommelier)

- Two samples w_1, w_2 are indistinguishable iff they are indistinguishable w.r.t. all reasonable adversaries

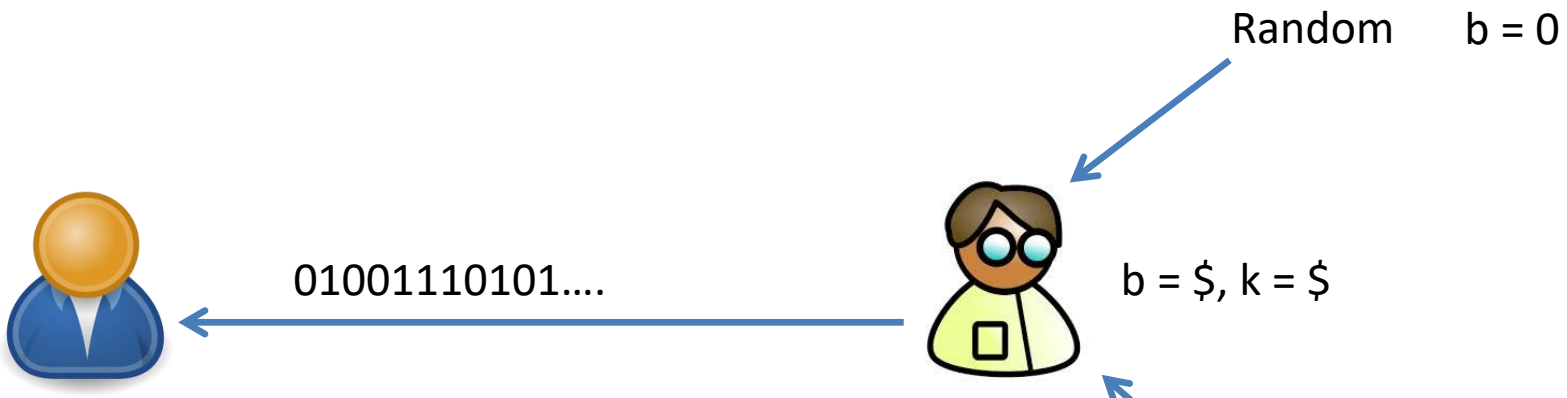
Semantic Security

- We know what properties we want our constructions to have in an ideal world

- If we can show that our real constructions are **“indistinguishable**” from these ideal constructions, then we can use them as if they have these properties

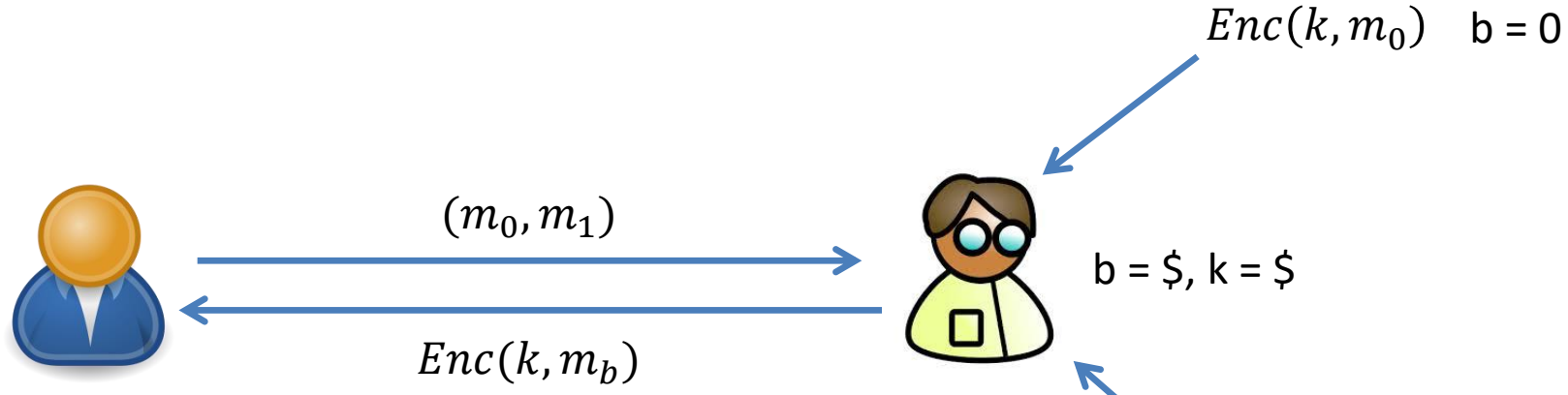
Example: PRNG

- Ideal: Sequence of truly random bits
- Actual: Pseudorandom sequence of bits



$$Adv(A) = \Pr[A(G(k)) = 1] - \Pr[A(r) = 1]$$

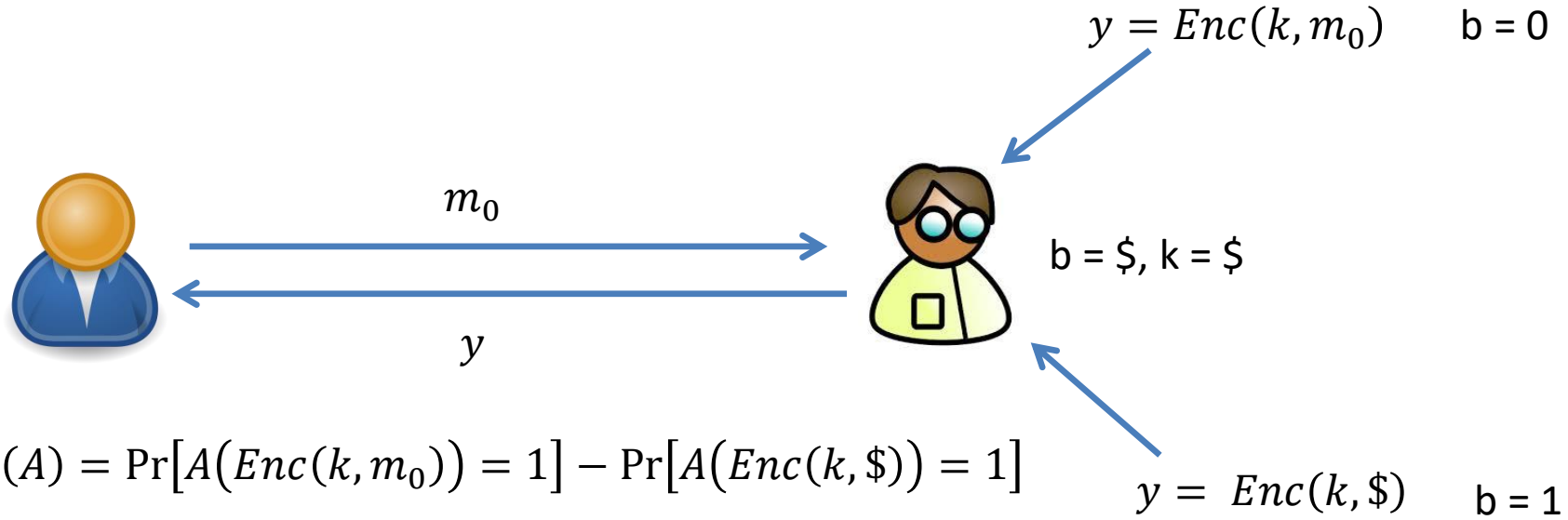
Example: IND-CPA (Indistinguishable with respect to Chosen Plaintext Attack)



$$Adv(A) = \Pr\left[A\left(Enc(k, m_0)\right) = 1\right] - \Pr\left[A\left(Enc(k, m_1)\right) = 1\right]$$

Example Homework Question (IND-CPA$)

- Consider the following game



$$Adv(A) = \Pr\left[A\left(Enc(k, m_0)\right) = 1\right] - \Pr\left[A\left(Enc(k, \$)\right) = 1\right]$$

Question: Let Enc be an IND-CPA secure encryption scheme, is Enc IND-CPA$ secure?

Question: Let Enc be an IND-CPA$ secure encryption scheme, is Enc IND-CPA secure?

IND-CPA => IND-CPA$?

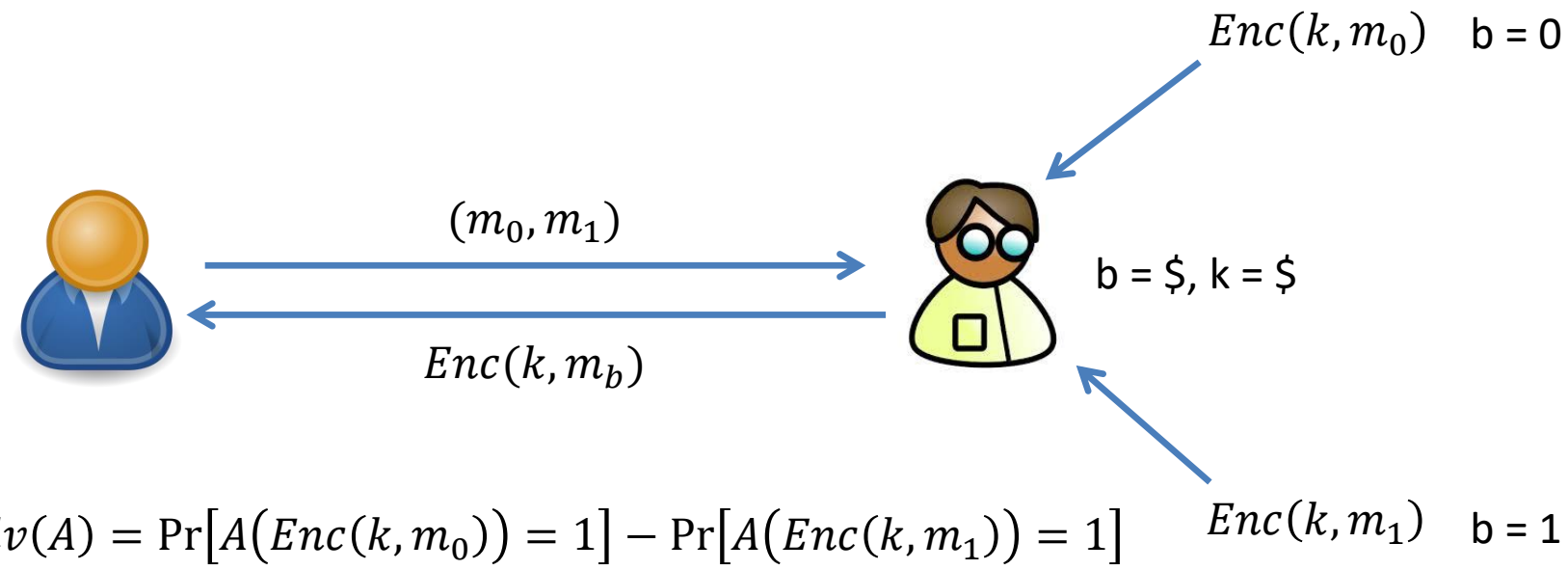
- $\mathrm{p} \Rightarrow q \equiv \neg q \Rightarrow \neg p$ (contrapositive)
- $\mathrm{IND-CPA} \Rightarrow \mathrm{IND-CPA\$} \equiv \neg\mathrm{IND-CPA\$} \Rightarrow \neg\mathrm{IND-CPA}$

Forwards or backwards, which direction is more appealing?

What is implied by $\neg\mathrm{IND-CPA\$}$?

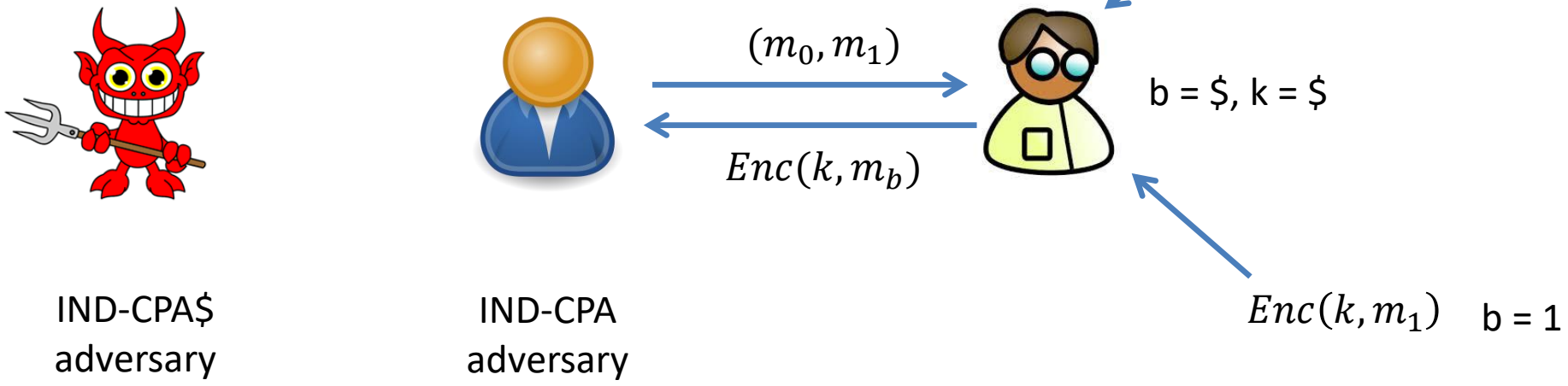
$\neg IND - CPA\$ \Rightarrow \neg IND - CPA$?

Can be break this game with the help of an adversary that breaks IND-CPA$?

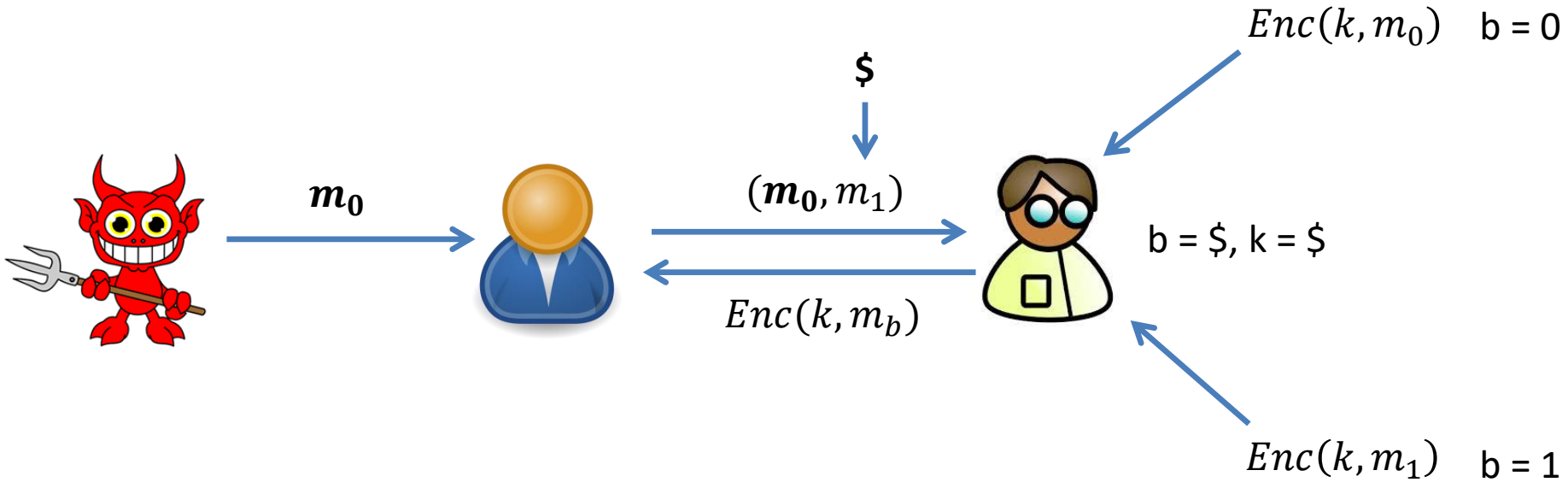


$$Adv(A) = \Pr\left[A\left(Enc(k, m_0)\right) = 1\right] - \Pr\left[A\left(Enc(k, m_1)\right) = 1\right]$$

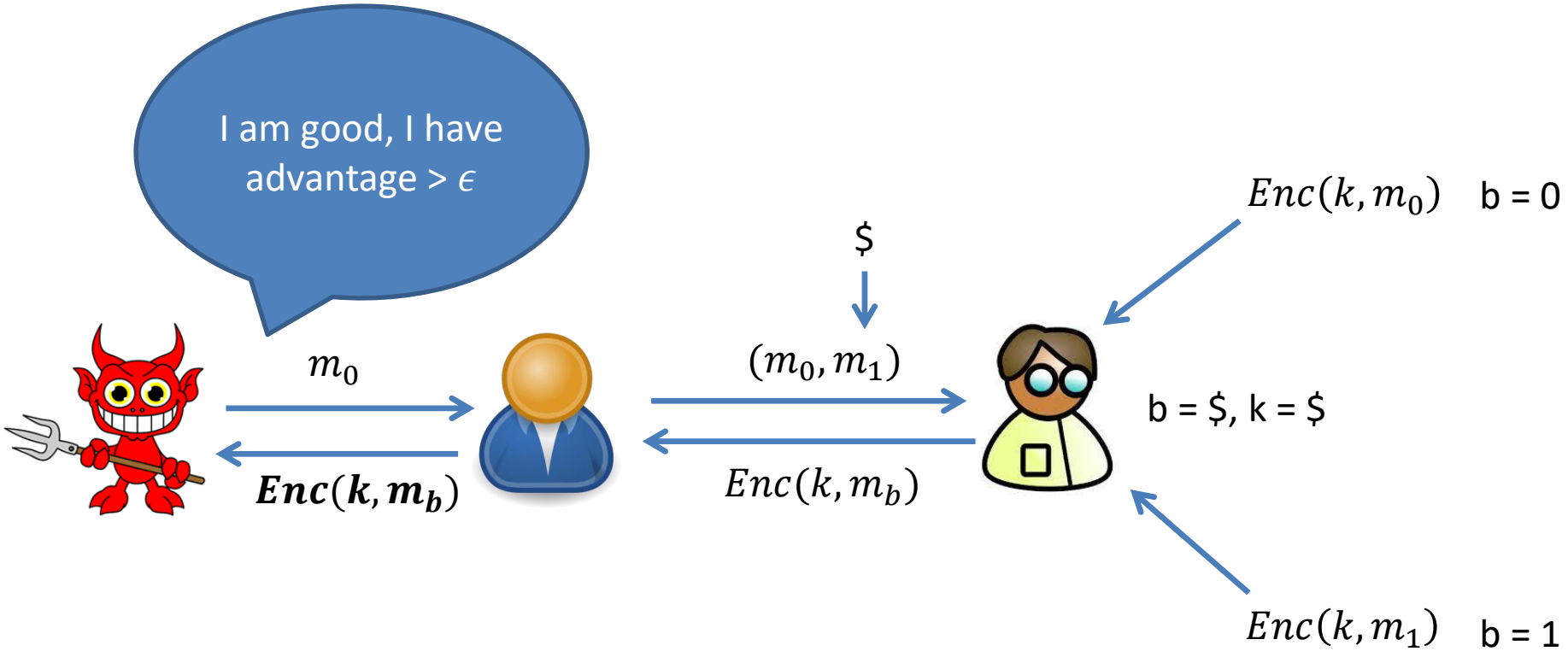
$\neg IND - CPA\$ \Rightarrow \neg IND - CPA$?



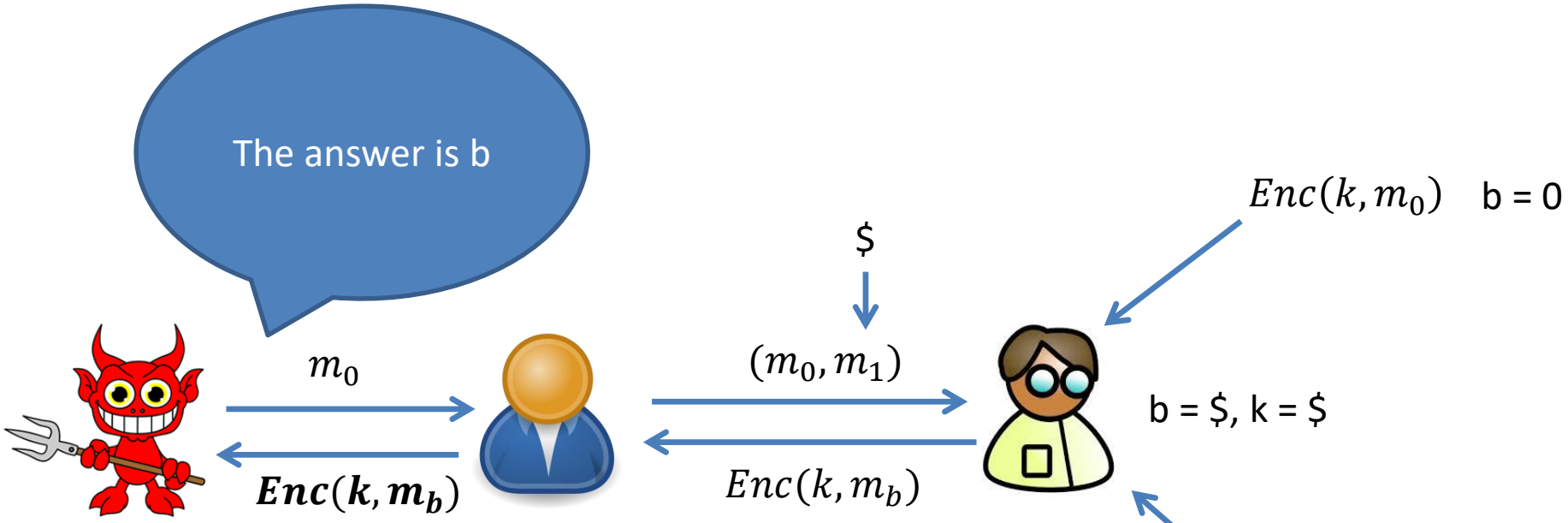
$\neg IND - CPA\$ \Rightarrow \neg IND - CPA$?



$\neg IND - CPA\$ \Rightarrow \neg IND - CPA$?

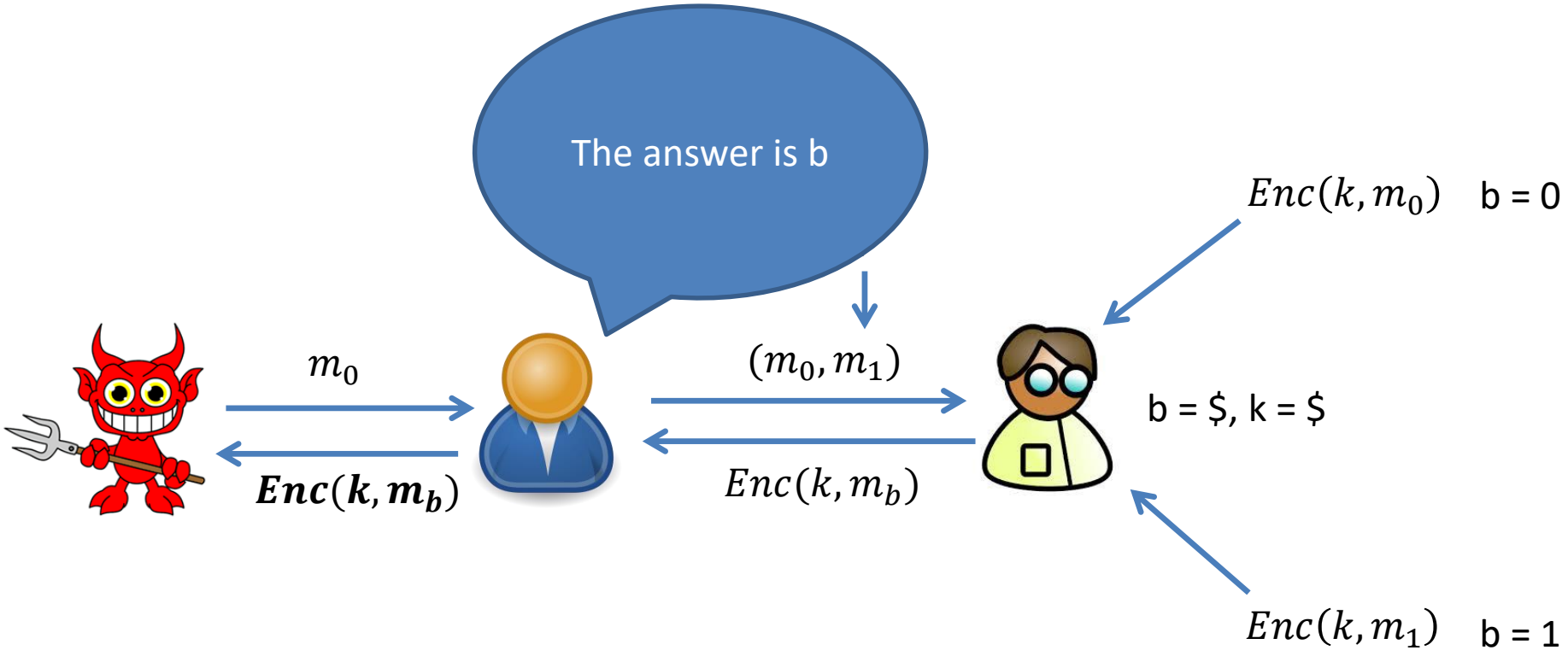


$\neg IND - CPA\$ \Rightarrow \neg IND - CPA$?



If b = 0: $Adv = \epsilon$
If b = 1: $Adv = \epsilon$

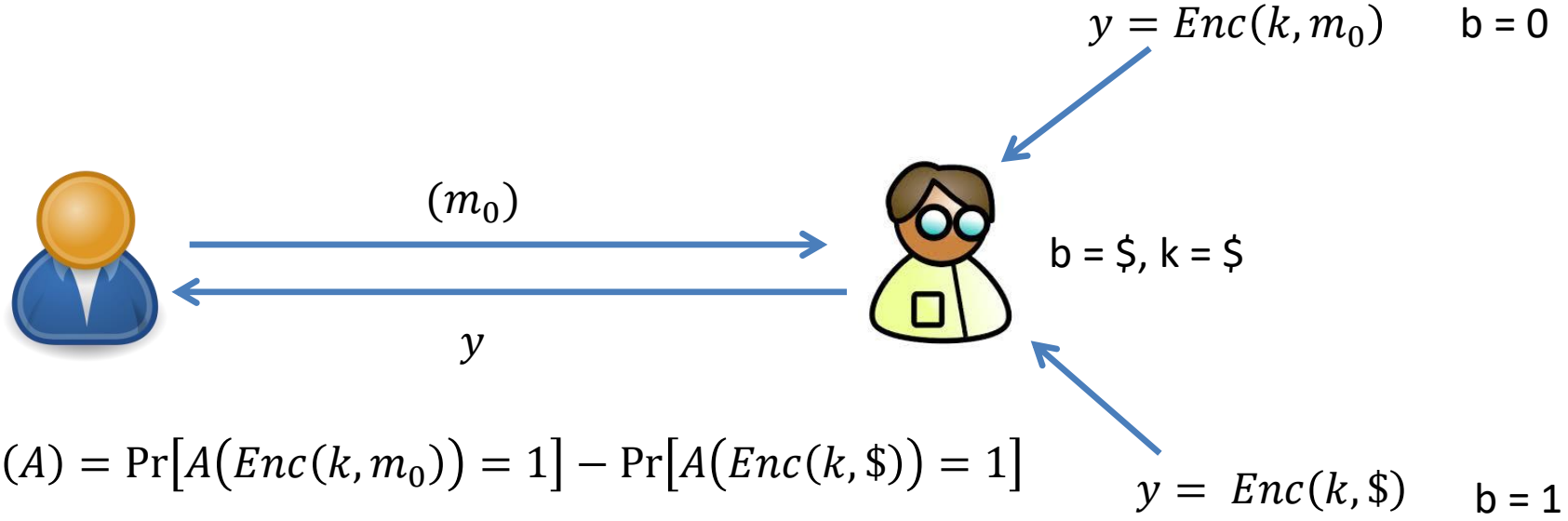
$\neg IND - CPA\$ \Rightarrow \neg IND - CPA$?



$$\boldsymbol{Adv(A) = \Pr\left[A\left(Enc(k, m_0)\right) = 1\right] - \Pr\left[A\left(Enc(k, m_1)\right) = 1\right] = Adv(\neg IND - CPA\$)}$$

Example Homework Question (IND-CPA$)

- Consider the following game



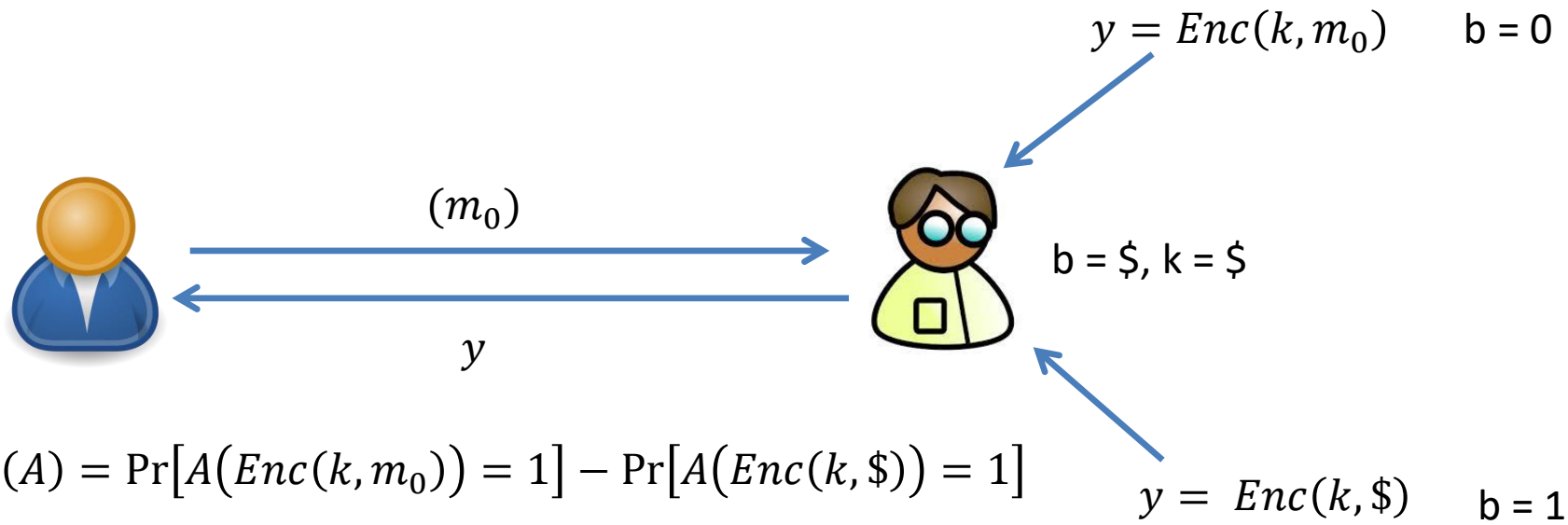
$$Adv(A) = \Pr\left[A\left(Enc(k, m_0)\right) = 1\right] - \Pr\left[A\left(Enc(k, \$)\right) = 1\right]$$

Question: Let Enc be an IND-CPA secure encryption scheme, is Enc IND-CPA$ secure?

Yes!

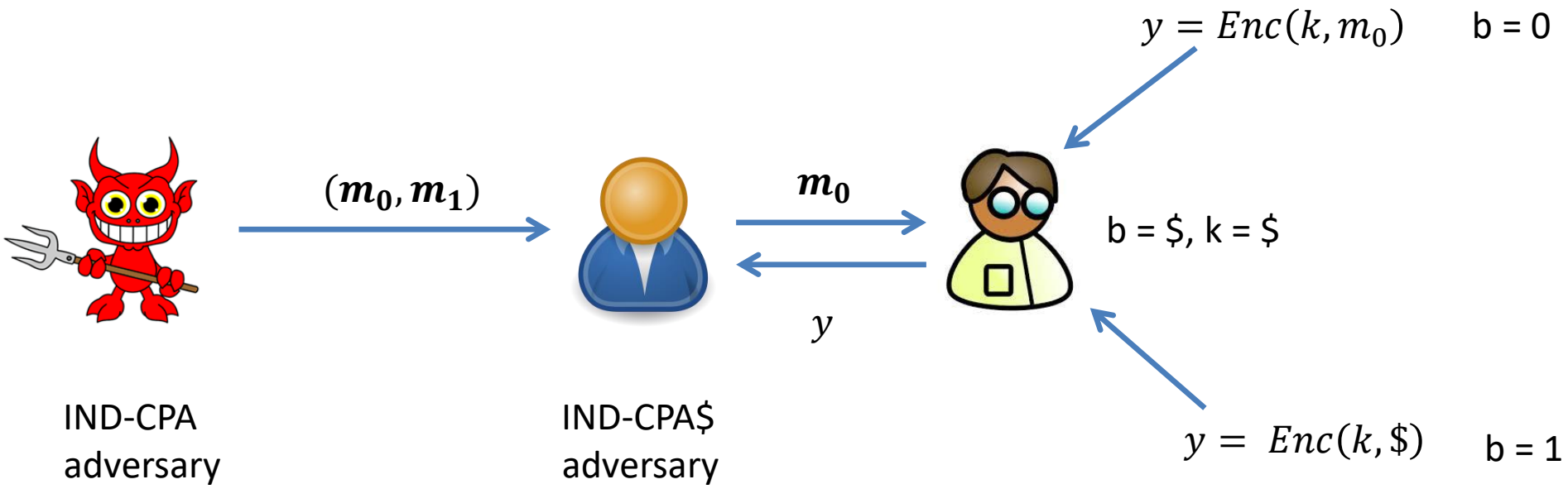
Question: Let Enc be an IND-CPA$ secure encryption scheme, is Enc IND-CPA secure?

$\neg IND - CPA \Rightarrow \neg IND - CPA\$$?

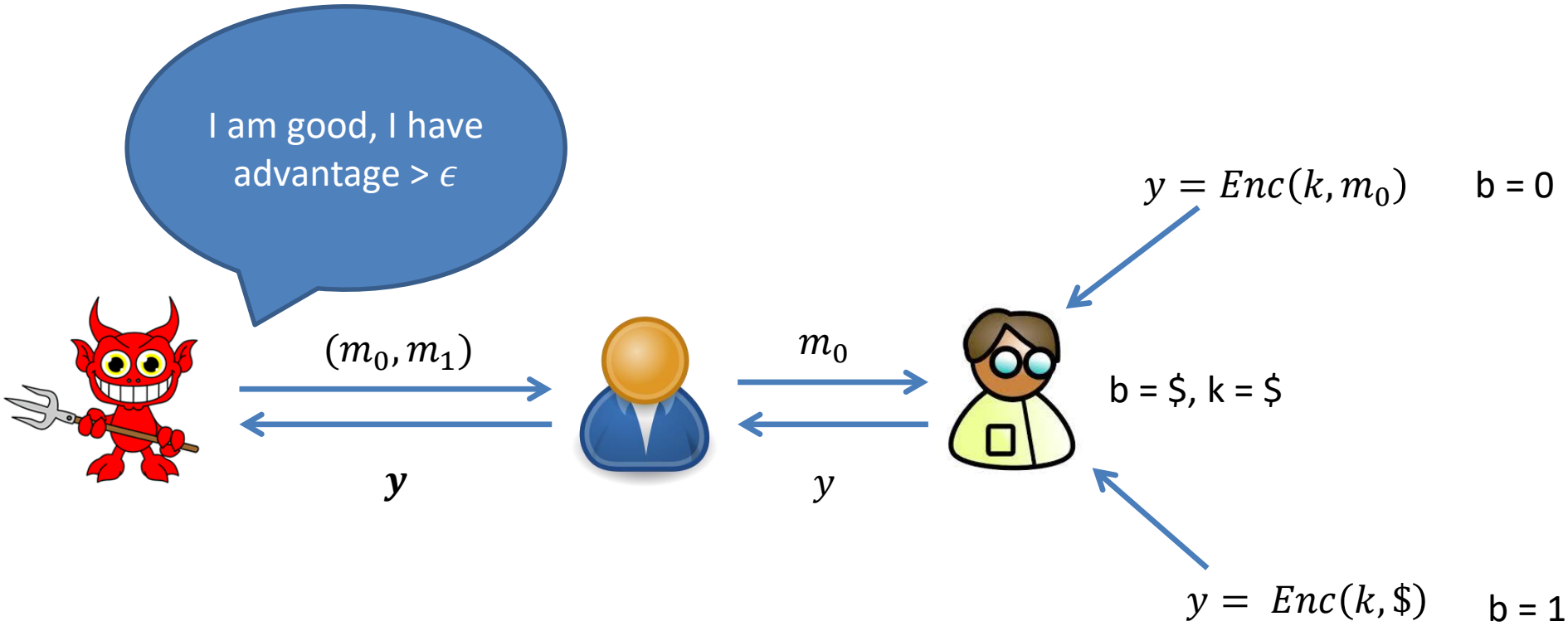


$$Adv(A) = \Pr\left[A\left(Enc(k, m_0)\right) = 1\right] - \Pr\left[A\left(Enc(k, \$)\right) = 1\right]$$

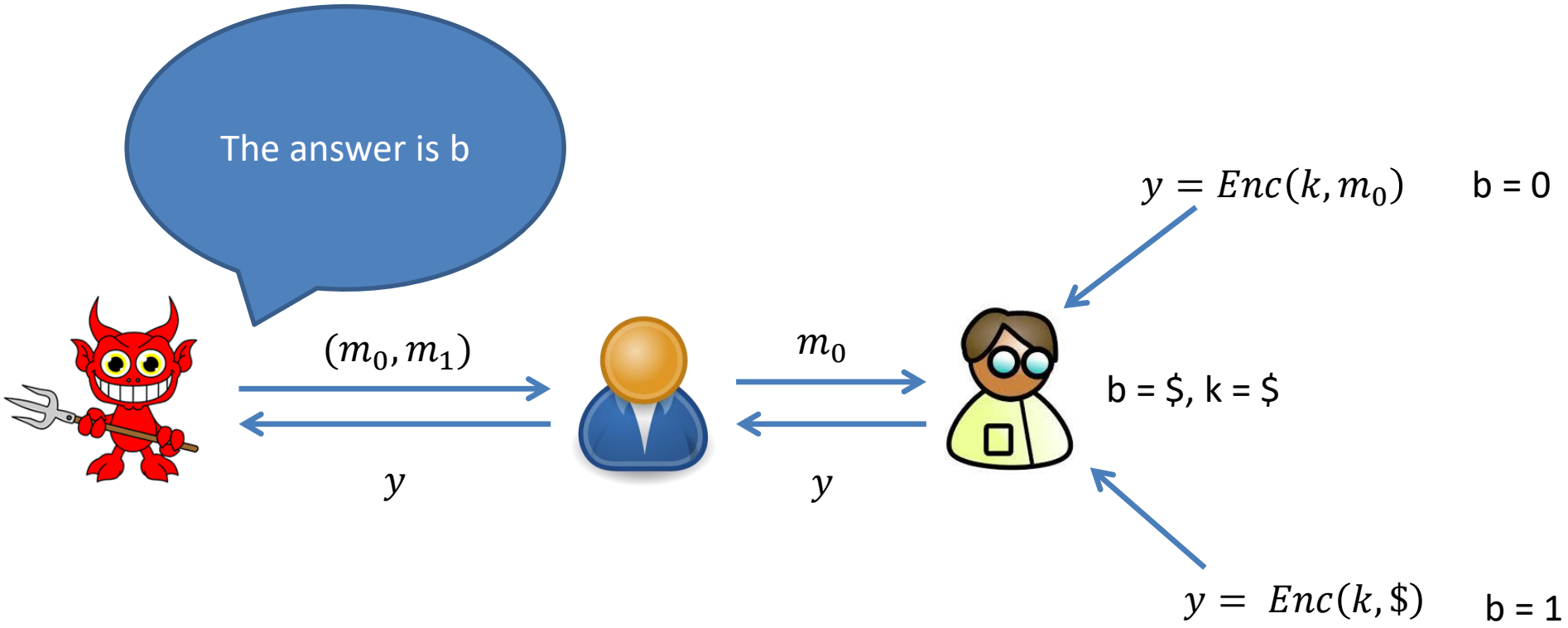
$\neg IND - CPA \Rightarrow \neg IND - CPA\$\ ?$



$\neg IND - CPA \Rightarrow \neg IND - CPA\$$?



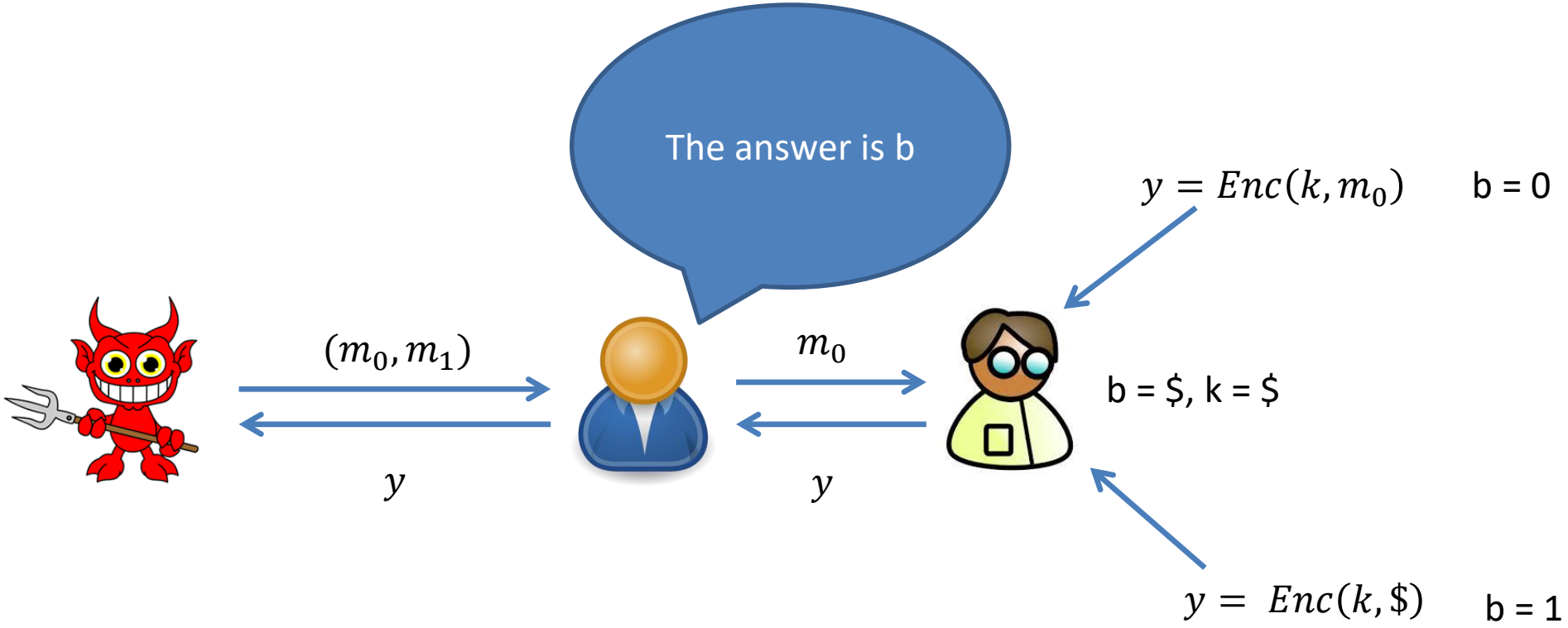
$\neg IND - CPA \Rightarrow \neg IND - CPA\$$?



If b = 0: This is identical to the IND-CPA game, oracle has $Adv = \epsilon$

if b = 1: This oracle was given input that it is not designed to handle, in the worst case it has no advantage at all, just random guessing

$\neg IND - CPA \Rightarrow \neg IND - CPA\$$?



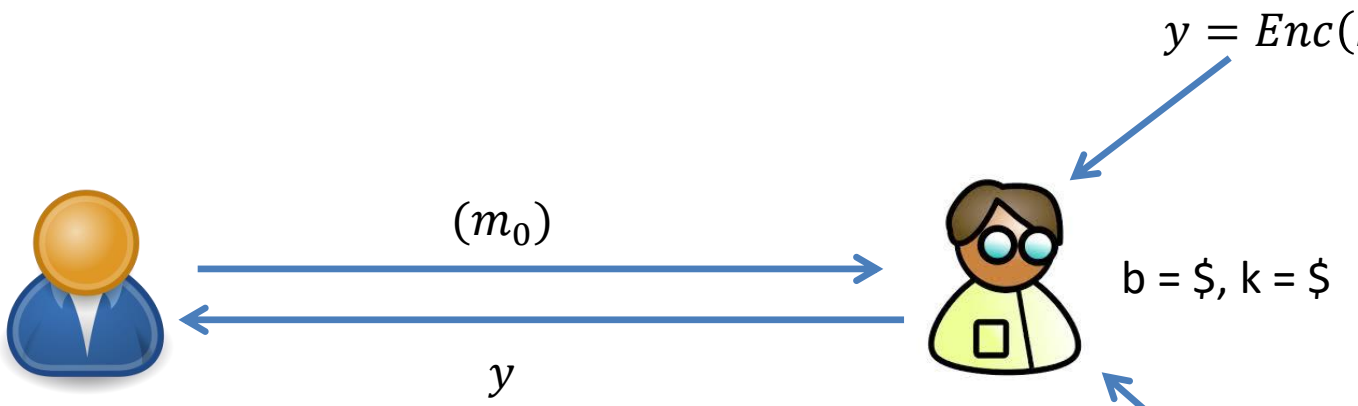
$$\boldsymbol{Adv(A) = \Pr\left[A\left(Enc(k, m_0)\right) = 1\right] - \Pr\left[A\left(Enc(k, \$)\right) = 1\right] = \frac{Adv(\neg IND - CPA)}{2}}$$

Takeaway

- There are other equivalent definitions of the IND-CPA security game
  - Left or Right (LoR)
  - Real or Random (RoR)

- Are there stronger definitions?

Real or Random String (IND$-CPA)



$$Adv(A) = \Pr\left[A\left(Enc(k, m_0)\right) = 1\right] - \Pr\left[A\left(Enc(k, \$)\right) = 1\right]$$

Question: Let Enc be an IND-CPA secure encryption scheme, is Enc IND$-CPA secure?

$\mathrm{IND} - \mathrm{CPA} \not\Rightarrow \mathrm{IND\$} - \mathrm{CPA}$

- Let **Enc** be an IND-CPA secure encryption scheme that always appends the bit ‘0’ to the ciphertext

- An adversary A can check the last bit of the ciphertext and guess “real” if it is 0, “random” if it is 1

$$Adv(A) = \Pr\left[A\left(Enc(k, m_0)\right) = 1\right] - \Pr[A(\$) = 1] = 1 - \frac{1}{2} = \frac{1}{2}$$