Modern symmetric-key Encryption

Computational Security

- What does it mean to be pseudo-random
  - Things can look random when they are not

- This can be used to achieve secure encryption while using short keys

Security

- A scheme is secure if:

  Every Probabilistic Polynomial Time Adversary succeeds in breaking the scheme with only negligible probability.

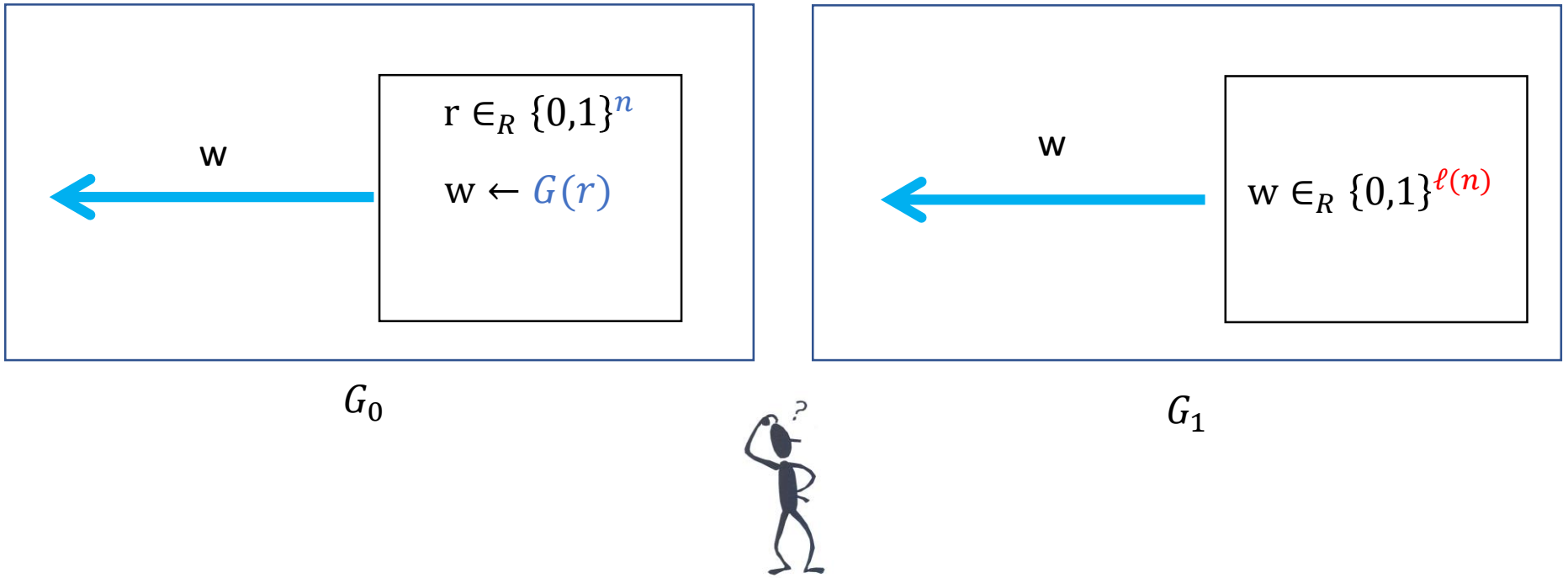
Insecurity of a scheme

- A scheme is broken if

  there exists a p.p.t. adversary which succeeds in breaking the scheme with probability greater $1/p(n)$ where p is a polynomial

Definition of Pseudo-random generator

- A function $G : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$ is a PRG if
  - Expansion: $\ell(n) > n$ (trivial if $\ell(n) \leq n$)
  - Pseudo-random: following two games are computationally indistinguishable



Pseudo-random generator exercise

- Make groups of two where each player takes a role
  - Game
  - Distinguisher

Pseudo-random generator exercise

- Instructions
  - $\mathrm{Z}_{23} \leftarrow \{0, \ldots, 22\}$
  - Game
    - Choose a function G from Z_{23} to $Z_{23} \times Z_{23}$ (easy to compute by hand)
    - Write down 2 random points $x_1, x_2 \in Z_{23}$
    - Write down 2 random points $y_1, y_2 \in Z_{23} \times Z_{23}$
    - Compute $z_1 \leftarrow G(x_1),\ z_2 \leftarrow G(x_2)$
    - Give the description G to Distinguisher
    - Sample a random bit $r \in \{0,1\}$ (don't tell distinguisher)
    - If r=0 then send (y_1, y_2) else send (z_1, z_2)
  - Distinguisher
    - Give a guess b on what r was.
    - Win if $b = r$.

Questions on generators

- $G' : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ is a PRG
- $b \in \{0,1\}$
- $||$ denote concatenation

1. Is $G(b||r) \coloneqq b||G'(r)$ a PRG? Yes
2. Is $G(r) \coloneqq G'(r \oplus 5)$ a PRG? Yes
3. If G_1, G_2 are PRG is $G_1(r) \oplus G_2(r \oplus 0^{n-3}101)$ a PRG?

Pseudo-random function exercise

- Instructions
  - $\mathrm{Z}_{23} \leftarrow \{0, \ldots, 22\}$
  - Game
    - Choose a function F from Z_{23} to Z_{23} (easy to compute by hand, don't show to distinguisher)
    - Write down 2 random points $y_1, y_2 \in Z_{23}$
  - Distinguisher
    - Choose two points $x_1, x_2 \in Z_{23}$ and give them to Game
  - Game
    - Compute $\mathrm{z}_1, \mathrm{z}_2 \leftarrow F(x_1)$,
    - Choose a bit r at random
    - If $r = 0$ then give (y_1, y_2) to distinguisher, otherwise give z_1, z_2
  - Distinguisher
    - Give a guess b on what r was.
    - Win if $b = r$.

CPA-secure encryption scheme from PRF

- $Keygen(\{1\}^s)$
  - $k \in_R \{0,1\}^s$
- $Enc_k(m)$
  - $r \in_R \{0,1\}^n$
  - $c \leftarrow (r, F_k(r) \oplus m)$
- $Dec_k(c)$
  - $(r, d) \leftarrow c$
  - $m \leftarrow F_k(r) \oplus d$

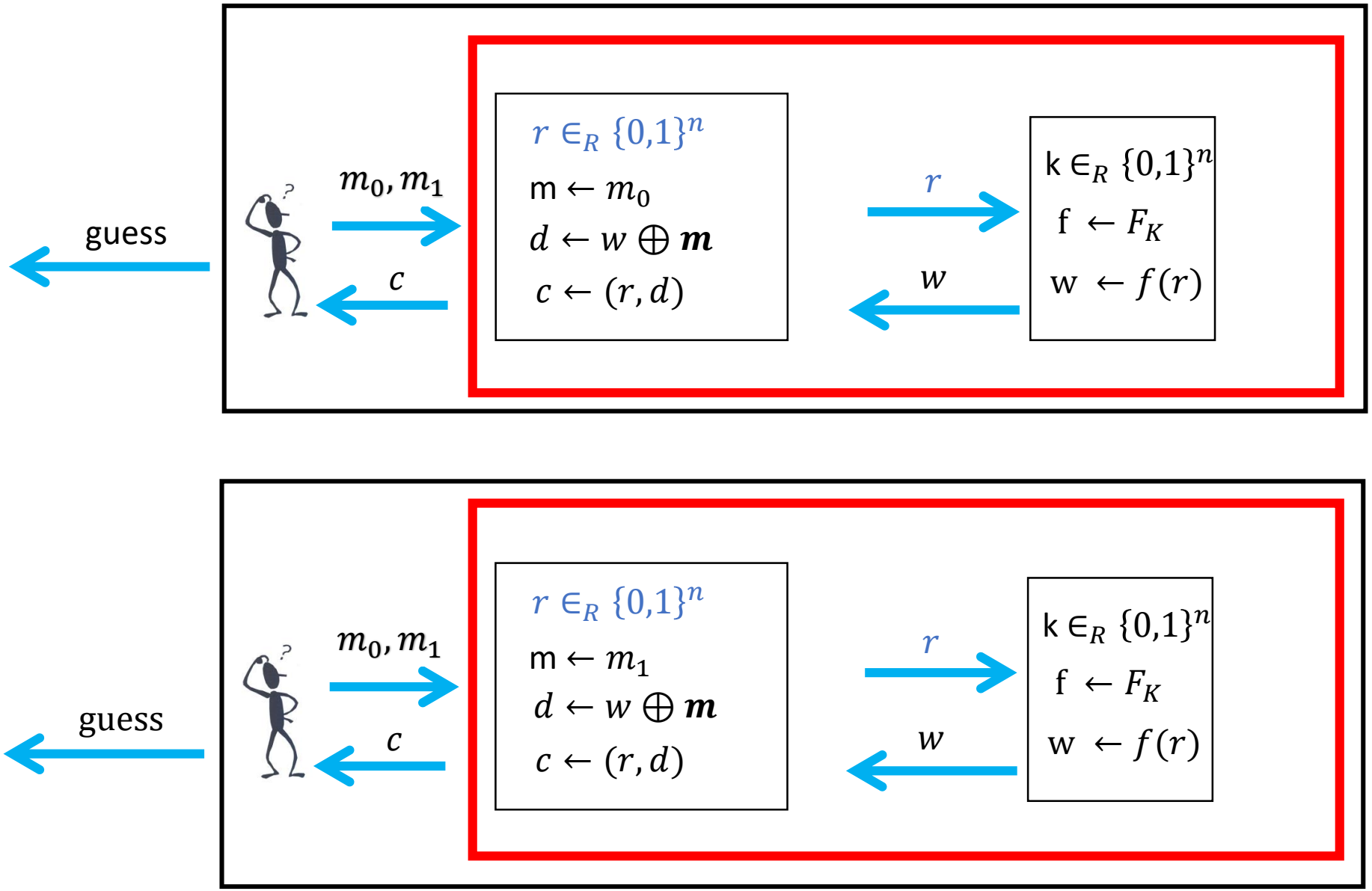
Proving security of encryption from PRG

- We will use the distinguisher for the encryption scheme to build a distinguisher which distinguisher between a random function and the PRF.

- This would thus imply that the function is not PRF and therefore the construction is secure when instantiated as a PRF.

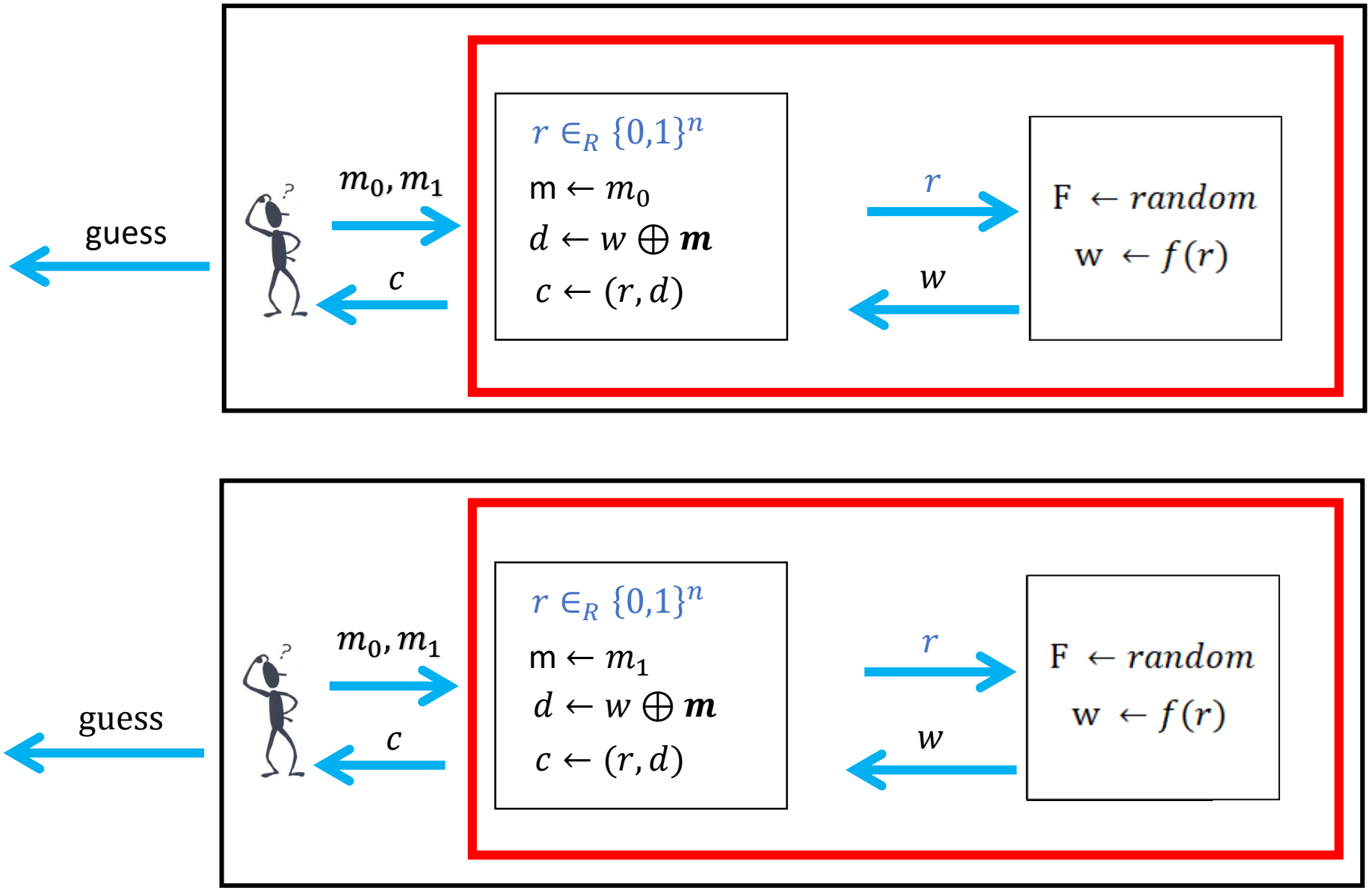
Building a distinguisher for the PRF using a distinguisher for the encryption scheme

Since the red part is an encryption of the message the distinguisher will guess which game he is in with good probability



Building a distinguisher for the PRF using a distinguisher for the encryption scheme

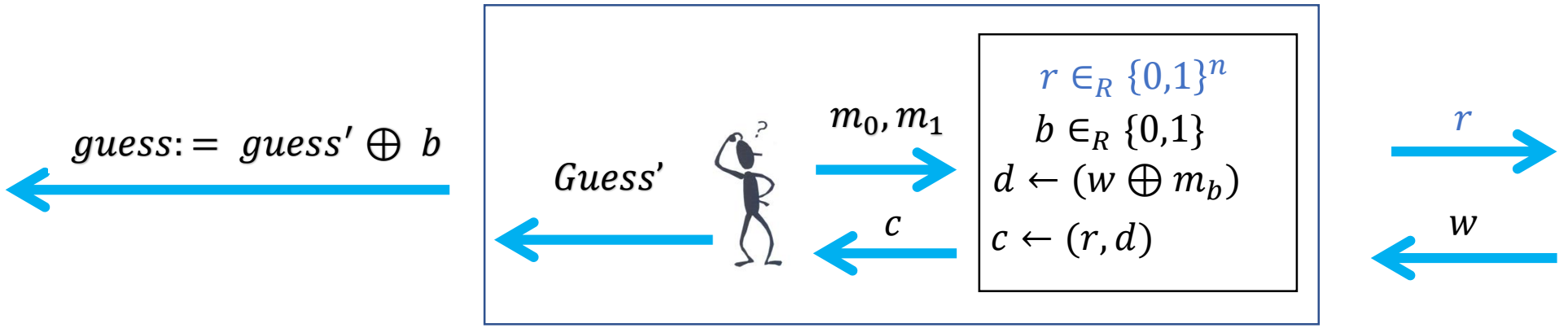
Since the red part is **random** **no distinguisher** can distinguish between these two games.



Building a distinguisher for the PRF using a distinguisher for the encryption scheme

- When using PRF
  - There exists a distinguisher which distinguishes between
    - Game where $m = m_0$
    - Game where $m = m_1$
- When using random functions
  - No distinguisher can distinguish between
    - Game where $m = m_0$
    - Game where $m = m_1$

Building a distinguisher for the PRF using a distinguisher for the encryption scheme



$:= distinguisher\ for\ the\ encryption\ scheme$

Result

- With a PRF, the distinguisher guesses correctly with good probability
- With a random function, the distinguisher guesses correctly about half to the time
- Therefore the distinguisher can distinguish between PRF and random function. Therefore the function is not a PRF.