Logistics

- HW3 due today
- Midterm on Tuesday
  - Questions similar to homework, Boneh-Shoup exercises 4.1 and 3.7
- Definitions sheet on class website

Pseudorandom Functions

Pseudorandom Functions

But, what are we distinguishing between?

Pseudorandom Functions

But, what are we distinguishing between?

> *Descriptions* of the functions wouldn't work. We just said that random functions are way bigger than what we're building

Pseudorandom Functions

But, what are we distinguishing between?

Descriptions of the functions wouldn't work. We just said that random functions are way bigger than what we're building

Idea: Get to *query* the function and try and distinguish by its *outputs*

Pseudorandom Functions

But, what are we distinguishing between?

Descriptions of the functions wouldn't work. We just said that random functions are way bigger than what we're building

Idea: Get to *query* the function and try and distinguish by its *outputs*

Problem: We can't keep the *description* of the PRF secret (Kerckoff's principal)

Pseudorandom Functions

But, what are we distinguishing between?

Descriptions of the functions wouldn’t work. We just said that random functions are way bigger than what we’re building

Idea: Get to *query* the function and try and distinguish by its *outputs*

Problem: We can’t keep the *description* of the PRF secret (Kerckoff’s principal)

Solution: PRFs will be *keyed*, and we’ll keep the key secret!

Pseudorandom Functions

But, what are we distinguishing between?

Descriptions of the functions wouldn't work. We just said that random functions are way bigger than what we're building

Idea: Get to *query* the function and try and distinguish by its *outputs*

$$F : \{0,1\}^\lambda \times X \to Y$$

Problem: We can't keep the *description* of the PRF secret (Kerckoff's principal)

Solution: PRFs will be *keyed*, and we'll keep the key secret!

Pseudorandom Functions

But, what are we distinguishing between?

Descriptions of the functions wouldn't work. We just said that random functions are way bigger than what we're building

Idea: Get to *query* the function and try and distinguish by its *outputs*

$$F : \{0,1\}^{\lambda} \times X \to Y$$

$$F(k, x) \to y$$

Problem: We can't keep the *description* of the PRF secret (Kerckoff's principal)

Solution: PRFs will be *keyed*, and we'll keep the key secret!

Pseudorandom Functions

But, what are we distinguishing between?

Descriptions of the functions wouldn't work. We just said that random functions are way bigger than what we're building

Idea: Get to *query* the function and try and distinguish by its *outputs*

$$F : \{0,1\}^\lambda \times X \to Y$$

$$F(k, x) \to y$$

Problem: We can't keep the *description* of the PRF secret (Kerckoff's principal)

Can also view this as a *family* of functions

Solution: PRFs will be *keyed*, and we'll keep the key secret!

Pseudorandom Functions

But, what are we distinguishing between?

Descriptions of the functions wouldn't work. We just said that random functions are way bigger than what we're building

Idea: Get to *query* the function and try and distinguish by its *outputs*

$$F : \{0,1\}^\lambda \times X \to Y$$

$$F(k, x) \to y$$

Problem: We can't keep the *description* of the PRF secret (Kerckoff's principal)

Can also view this as a *family* of functions

Solution: PRFs will be *keyed*, and we'll keep the key secret!

$$\{F_k\}_{k \in \{0,1\}^\lambda}$$

Pseudorandom Functions

But, what are we distinguishing between?

Descriptions of the functions wouldn't work. We just said that random functions are way bigger than what we're building

Idea: Get to *query* the function and try and distinguish by its *outputs*

$$F : \{0,1\}^\lambda \times X \to Y$$

$$F(k, x) \to y$$

Problem: We can't keep the *description* of the PRF secret (Kerckoff's principal)

Can also view this as a *family* of functions

Solution: PRFs will be *keyed*, and we'll keep the key secret!

$$\{F_k\}_{k \in \{0,1\}^\lambda} \qquad F_k : X \to Y$$

Pseudorandom Functions

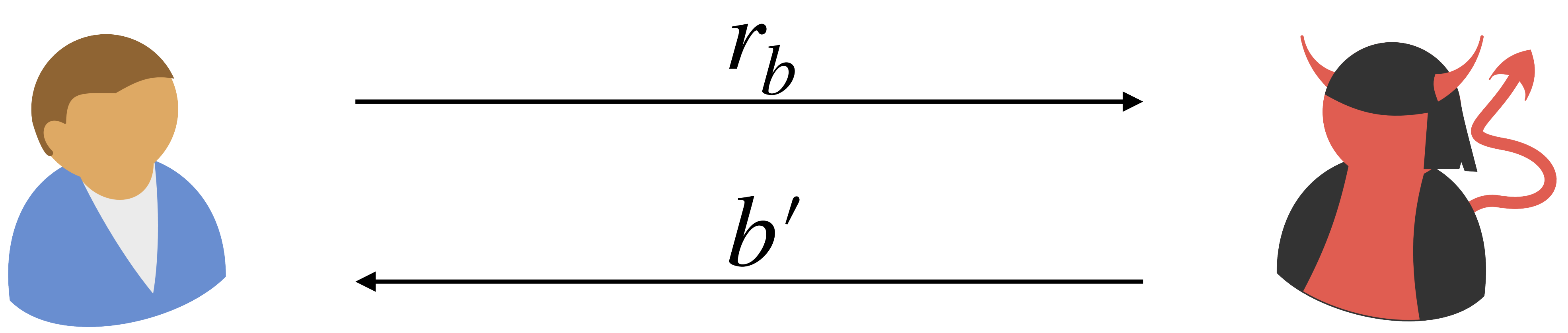
Recap: PRG Game

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

$$s \xleftarrow{\$} \{0,1\}^{\lambda}$$

$$r_0 \xleftarrow{\$} \{0,1\}^{\ell(\lambda)}$$

$$r_1 := G(s)$$



Wins if $b' = b$

Pseudorandom Functions

Now: PRF Game

Pseudorandom Functions

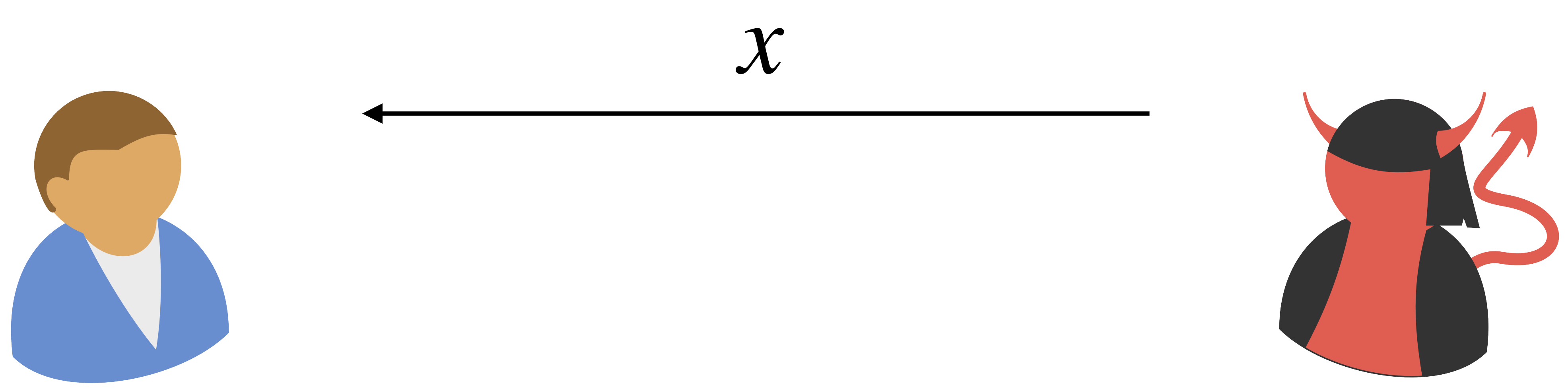
Now: PRF Game

$$b \xleftarrow{\$} \{0,1\}$$
$$k \xleftarrow{\$} \{0,1\}^{\lambda}$$
$$T := \{\}$$

Pseudorandom Functions

Now: PRF Game

$$b \xleftarrow{\$} \{0,1\}$$
$$k \xleftarrow{\$} \{0,1\}^\lambda$$
$$T := \{\}$$



Pseudorandom Functions

Now: PRF Game

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

$k \xleftarrow{\$} \{0,1\}^\lambda$

$T := \{\}$

if $b = 0$

$y = F_k(x)$

x

Pseudorandom Functions

Now: PRF Game

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

$k \xleftarrow{\$} \{0,1\}^\lambda$

$T := \{\}$

if $b = 0$

$y = F_k(x)$

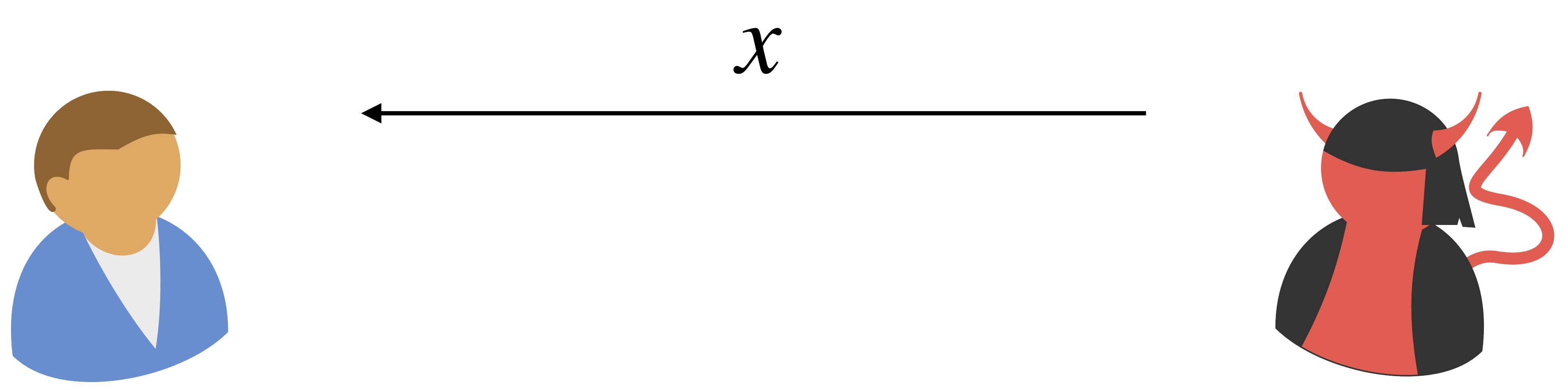
else

if $x \notin T$

$r \xleftarrow{\$} \{0,1\}^\lambda$

$T[x] = r$

$y = T[x]$



Pseudorandom Functions

Now: PRF Game

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

$k \xleftarrow{\$} \{0,1\}^\lambda$

$T := \{\}$

if $b = 0$

$y = F_k(x)$

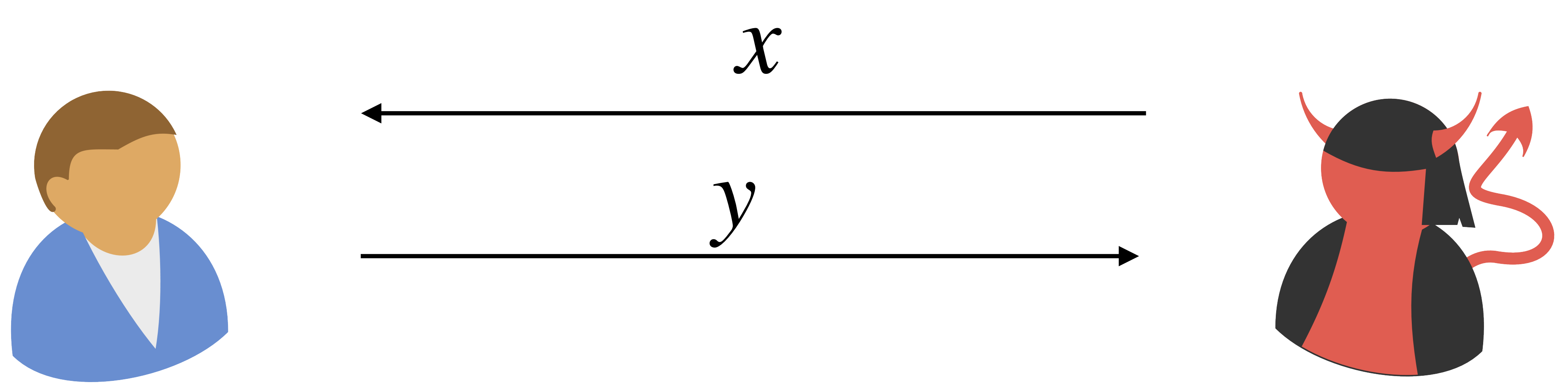
else

if $x \notin T$

$r \xleftarrow{\$} \{0,1\}^\lambda$

$T[x] = r$

$y = T[x]$



Pseudorandom Functions

Now: PRF Game

Repeat as much as $\mathscr{A}$ wants!

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

$k \xleftarrow{\$} \{0,1\}^\lambda$

$T := \{\}$

if $b = 0$

$\quad y = F_k(x)$

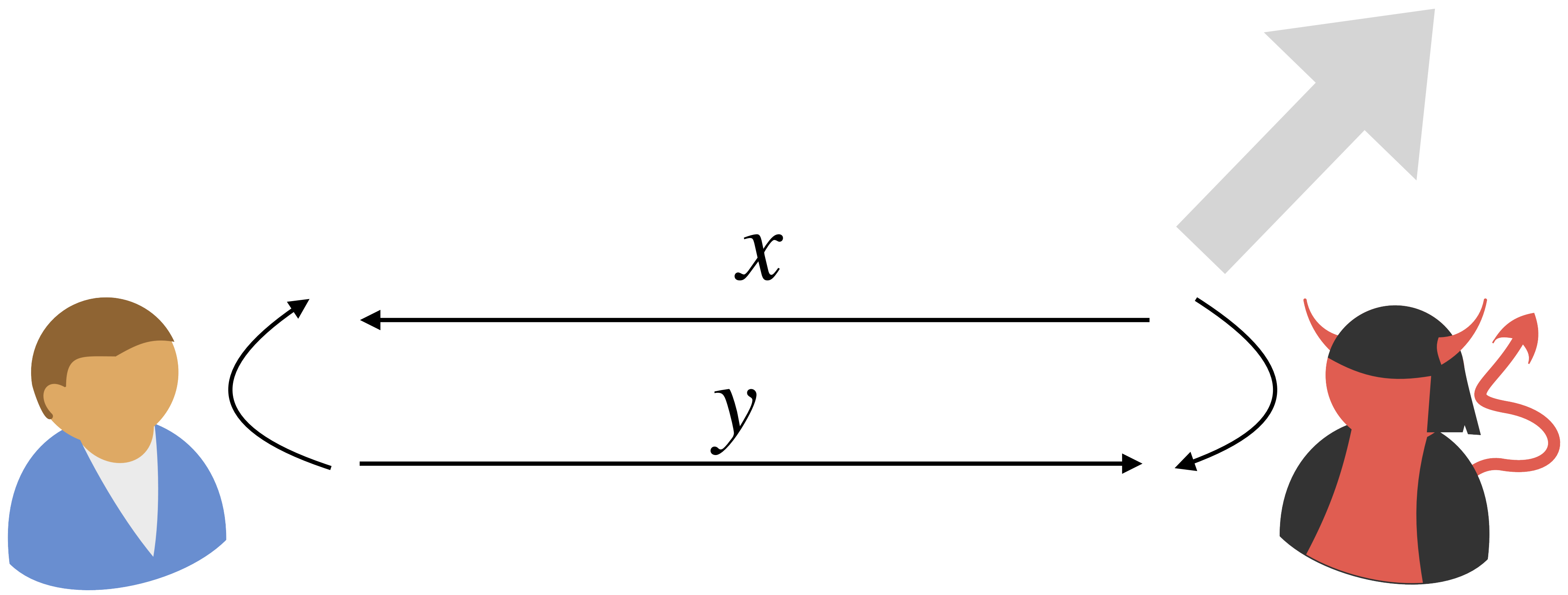
else

$\quad$ **if** $x \notin T$

$\quad\quad r \xleftarrow{\$} \{0,1\}^\lambda$

$\quad\quad T[x] = r$

$\quad y = T[x]$



Pseudorandom Functions

Now: PRF Game

Repeat as much as $\mathscr{A}$ wants!

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

$k \xleftarrow{\$} \{0,1\}^\lambda$

$T := \{\}$

if $b = 0$

$y = F_k(x)$

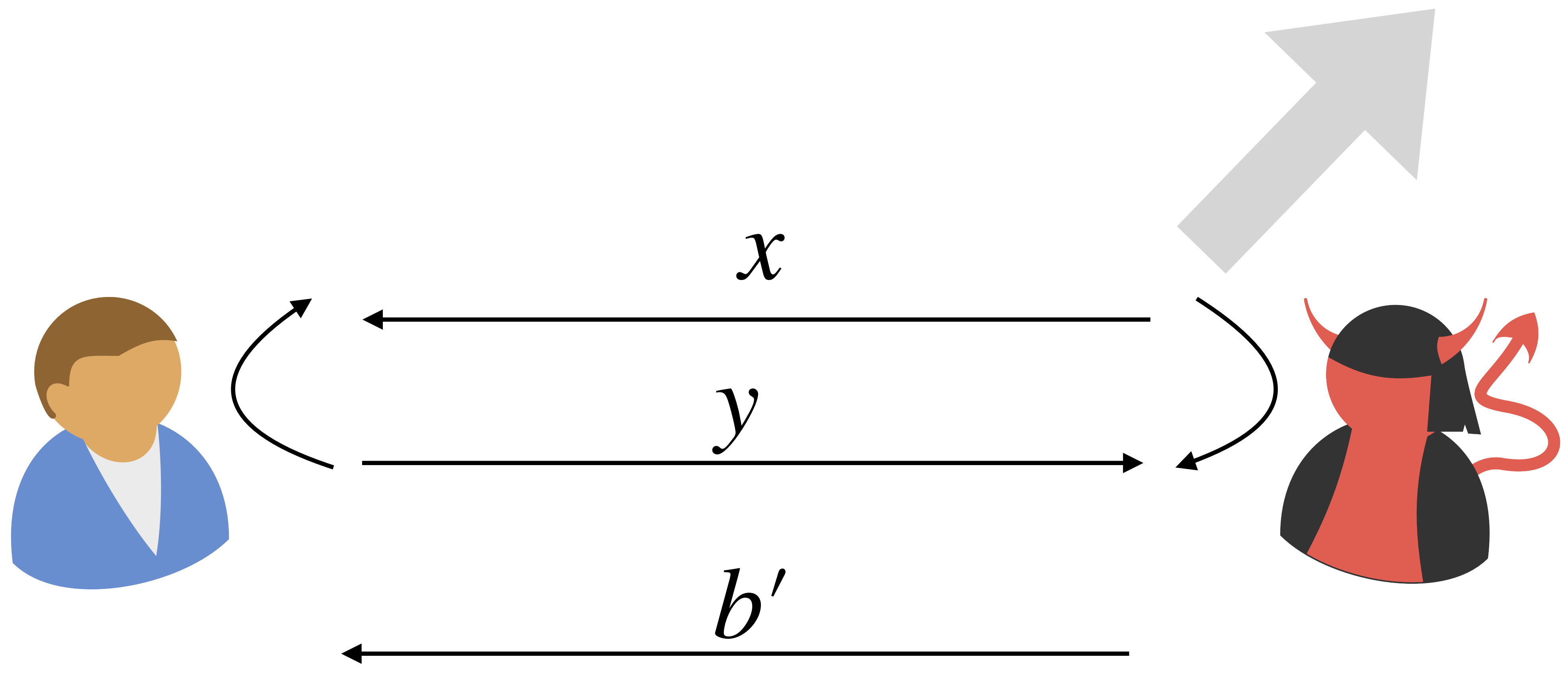
else

if $x \notin T$

$r \xleftarrow{\$} \{0,1\}^\lambda$

$T[x] = r$

$y = T[x]$



Pseudorandom Functions

Now: PRF Game

Repeat as much as $\mathscr{A}$ wants!

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

$k \xleftarrow{\$} \{0,1\}^\lambda$

$T := \{\}$

if $b = 0$

  $y = F_k(x)$

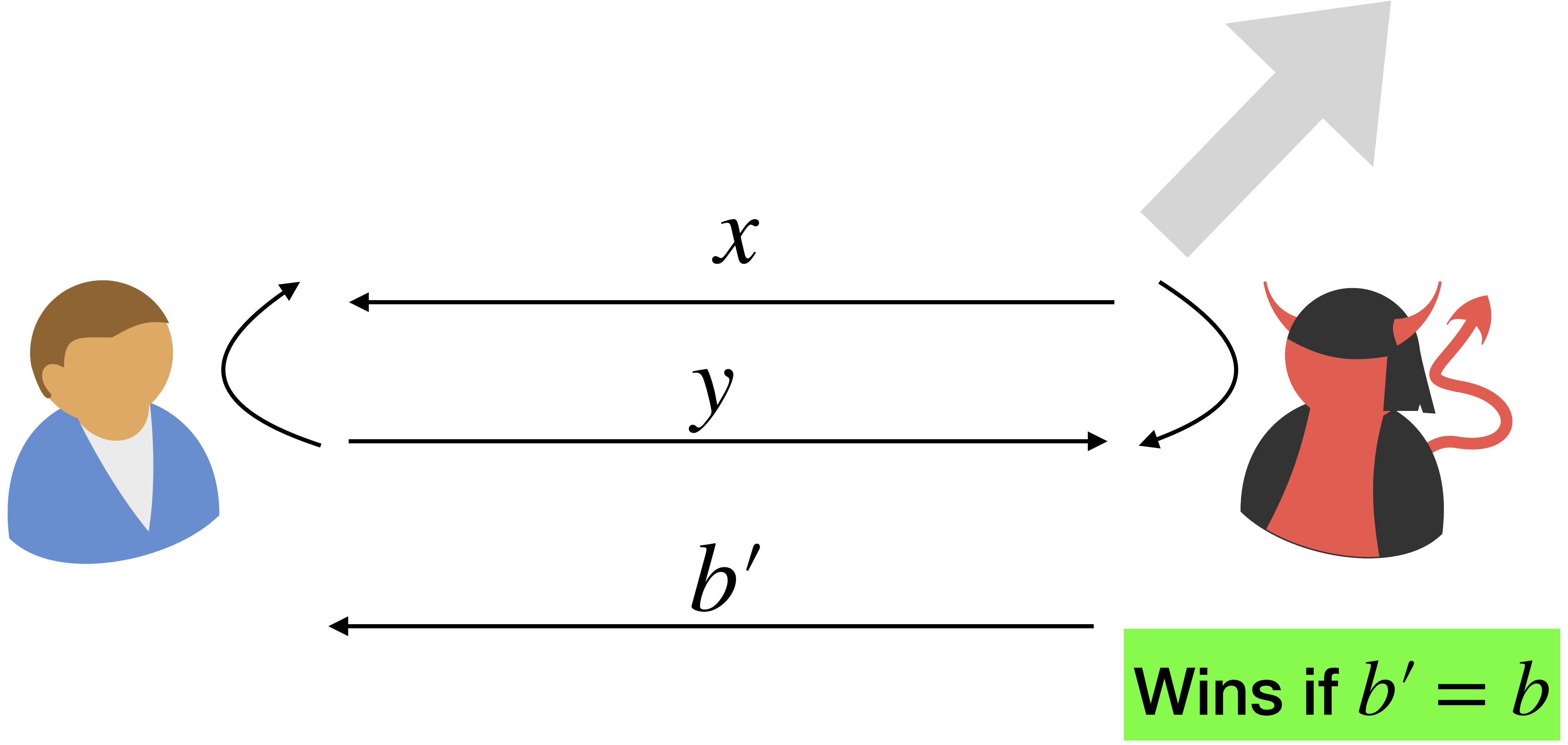
else

  if $x \notin T$

    $r \xleftarrow{\$} \{0,1\}^\lambda$

    $T[x] = r$

  $y = T[x]$



Pseudorandom Functions

Pseudorandom Function

Pseudorandom Functions

Pseudorandom Function

A deterministic family of functions $\{F_k\}_{k \in \{0,1\}^\lambda}$ where $F_k : X \to Y$ for all k is *pseudorandom* if:

Pseudorandom Functions

Pseudorandom Function

A deterministic family of functions $\{F_k\}_{k \in \{0,1\}^\lambda}$ where $F_k : X \to Y$ for all k is *pseudorandom* if:

- $F_k(x)$ can be computed in polynomial time

Pseudorandom Functions

Pseudorandom Function

A deterministic family of functions $\{F_k\}_{k \in \{0,1\}^\lambda}$ where $F_k : X \to Y$ for all k is *pseudorandom* if:

- $F_k(x)$ can be computed in polynomial time
- For all NUPPT $\mathscr{A}$, there exists a negligible function ν such that $\forall \lambda \in \mathbb{N}$,

Pseudorandom Functions

Pseudorandom Function

A deterministic family of functions $\{F_k\}_{k \in \{0,1\}^\lambda}$ where $F_k : X \to Y$ for all k is *pseudorandom* if:

- $F_k(x)$ can be computed in polynomial time
- For all NUPPT $\mathscr{A}$, there exists a negligible function ν such that $\forall \lambda \in \mathbb{N}$,

$$\Pr[\mathscr{A} \text{ wins GuessGame}] \leq \frac{1}{2} + \nu(\lambda)$$

Pseudorandom Functions

Pseudorandom Function

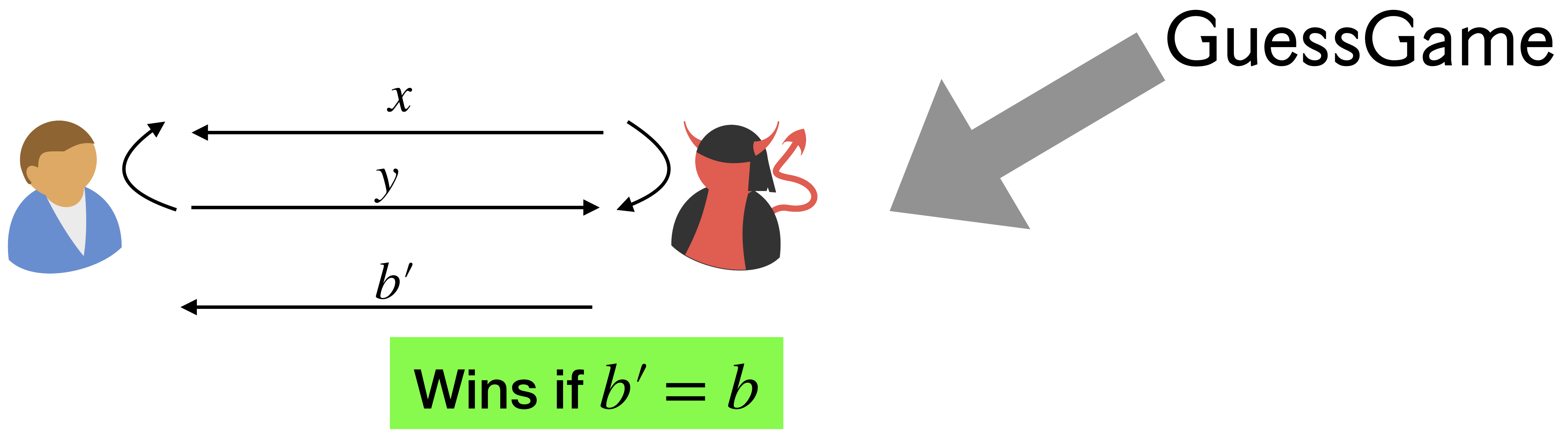
A deterministic family of functions $\{F_k\}_{k \in \{0,1\}^\lambda}$ where $F_k : X \to Y$ for all k is *pseudorandom* if:

- $F_k(x)$ can be computed in polynomial time
- For all NUPPT $\mathscr{A}$, there exists a negligible function ν such that $\forall \lambda \in \mathbb{N}$,

$$\Pr[\mathscr{A} \text{ wins GuessGame}] \leq \frac{1}{2} + \nu(\lambda)$$

$b \xleftarrow{\$} \{0,1\}$
$k \xleftarrow{\$} \{0,1\}^\lambda$
$T := \{\}$

if $b = 0$
  $y = F_k(x)$
else
  if $x \notin T$
    $r \xleftarrow{\$} \{0,1\}^\lambda$
    $T[x] = r$
  $y = T[x]$



Pseudorandom Functions

Pseudorandom Function

A deterministic family of functions $\{F_k\}_{k \in \{0,1\}^\lambda}$ where $F_k : X \to Y$ for all k is *pseudorandom* if:

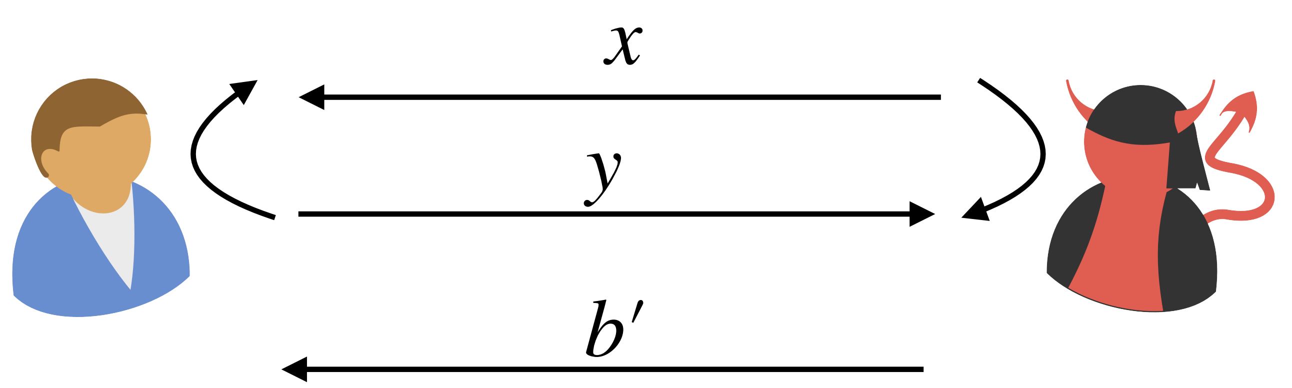
- $F_k(x)$ can be computed in polynomial time
- For all NUPPT $\mathscr{A}$, there exists a negligible function ν such that $\forall \lambda \in \mathbb{N}$,

$$\Pr[\mathscr{A} \text{ wins GuessGame}] \leq \frac{1}{2} + \nu(\lambda)$$

GuessGame

$b \xleftarrow{\$} \{0,1\}$
$k \xleftarrow{\$} \{0,1\}^\lambda$
$T := \{\}$

if $b = 0$
  $y = F_k(x)$
else
  if $x \notin T$
    $r \xleftarrow{\$} \{0,1\}^\lambda$
    $T[x] = r$
  $y = T[x]$



Wins if $b' = b$

This is the first security definition that we have seen that is *adaptive*, the adversary gets to choose its queries based on the responses it gets.

Pseudorandom Functions

Pseudorandom Function

A deterministic family of functions $\{F_k\}_{k \in \{0,1\}^\lambda}$ where $F_k : X \rightarrow Y$ for all k is *pseudorandom* if:

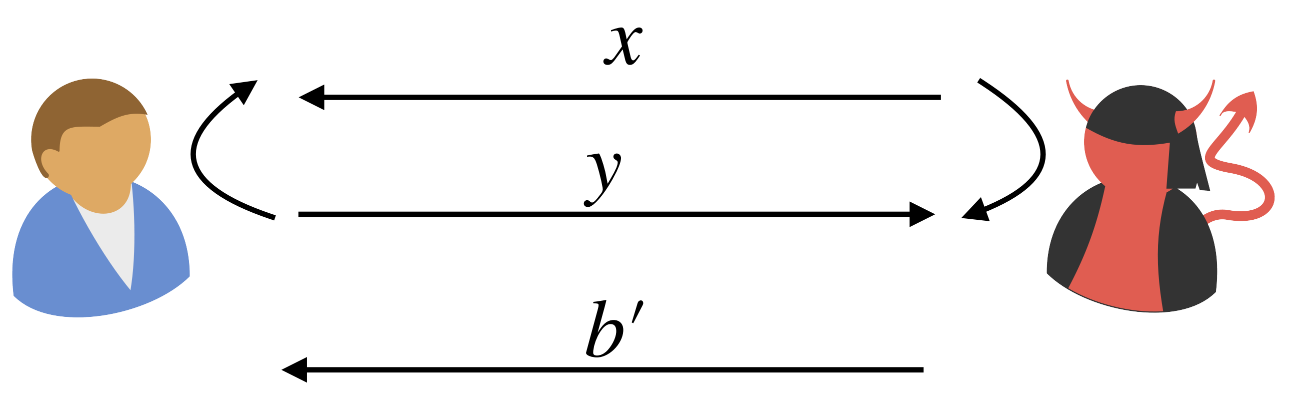
- $F_k(x)$ can be computed in polynomial time
- For all NUPPT $\mathscr{A}$, there exists a negligible function ν such that $\forall \lambda \in \mathbb{N}$,

$$\Pr[\mathscr{A} \text{ wins GuessGame}] \leq \frac{1}{2} + \nu(\lambda)$$

GuessGame

$b \xleftarrow{\$} \{0,1\}$
$k \xleftarrow{\$} \{0,1\}^\lambda$
$T := \{\}$

if $b = 0$
  $y = F_k(x)$
else
  if $x \notin T$
    $r \xleftarrow{\$} \{0,1\}^\lambda$
    $T[x] = r$
  $y = T[x]$



Wins if $b' = b$

This is the first security definition that we have seen that is *adaptive*, the adversary gets to choose its queries based on the responses it gets.

One of the benefits of thinking in terms of *games* is easily expressing things like this!

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

$k \xleftarrow{\$} \{0,1\}^\lambda$

$T := \{\}$

if $b = 0$

$y = F_k(x)$

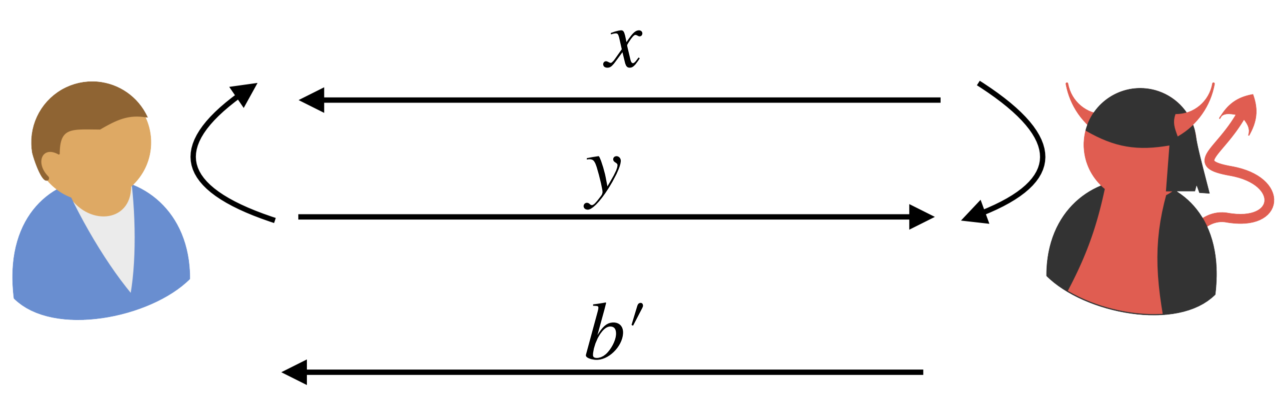
else

if $x \notin T$

$r \xleftarrow{\$} \{0,1\}^\lambda$

$T[x] = r$

$y = T[x]$



Wins if $b' = b$

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

$k \xleftarrow{\$} \{0,1\}^\lambda$

$T := \{\}$

if $b = 0$

$y = F_k(x)$

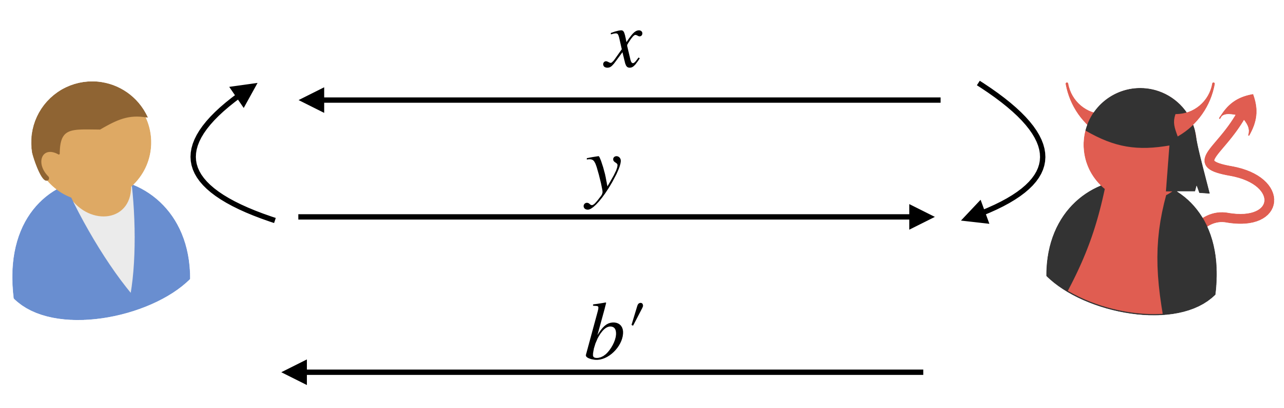
else

if $x \notin T$

$r \xleftarrow{\$} \{0,1\}^\lambda$

$T[x] = r$

$y = T[x]$



Wins if $b' = b$

$$\Pr[\mathscr{A} \text{ wins GuessGame}] \le \frac{1}{2} + \nu(\lambda)$$

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

$k \xleftarrow{\$} \{0,1\}^\lambda$

$T := \{\}$

if $b = 0$

  $y = F_k(x)$

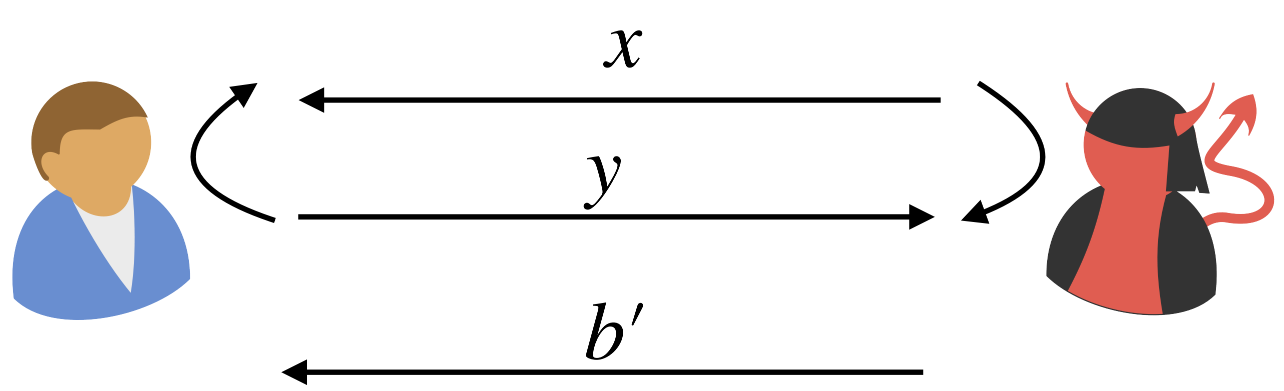
else

  if $x \notin T$

    $r \xleftarrow{\$} \{0,1\}^\lambda$

    $T[x] = r$

  $y = T[x]$

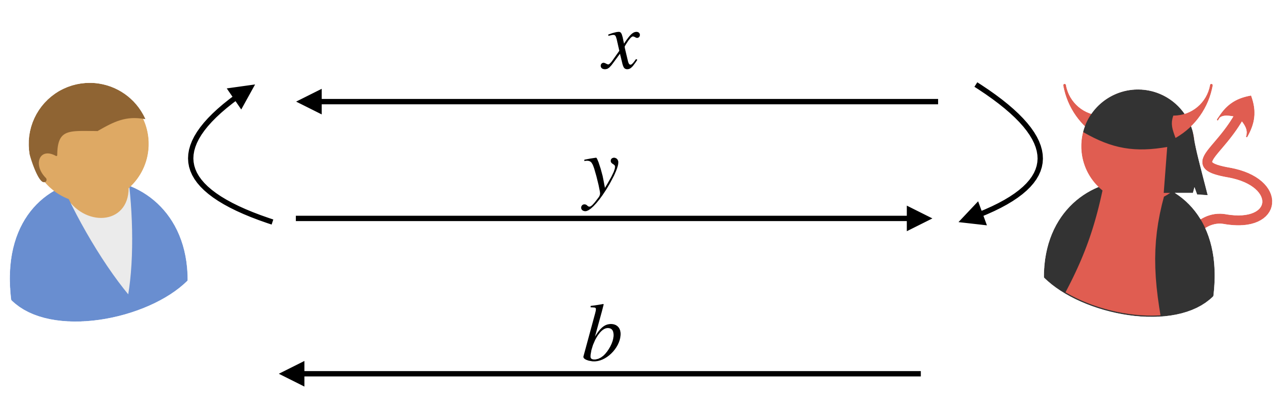


Wins if $b' = b$

$$\Pr[\mathscr{A} \text{ wins GuessGame}] \leq \frac{1}{2} + \nu(\lambda)$$

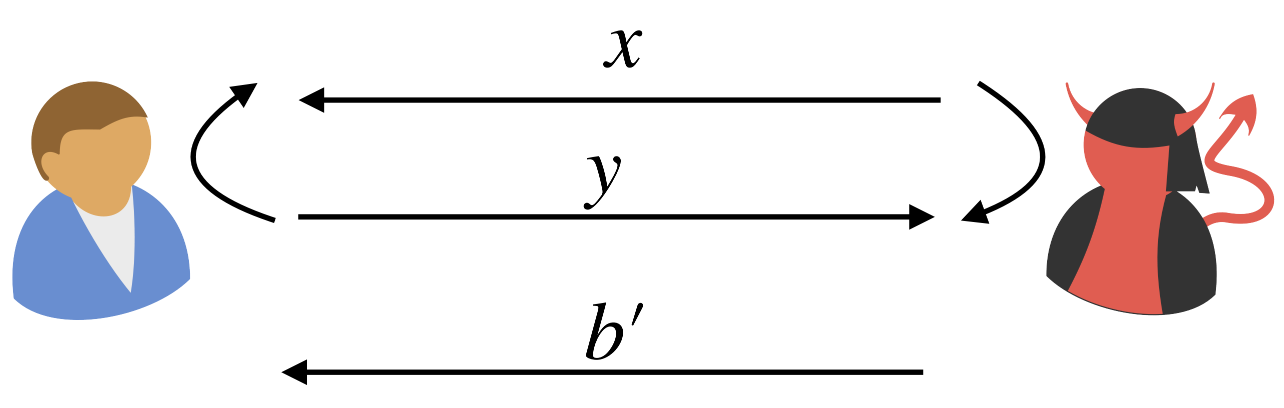
Game_0

$k \xleftarrow{\$} \{0,1\}^\lambda$ $\quad y = F_k(x)$



$b \xleftarrow{\$} \{0,1\}$
$k \xleftarrow{\$} \{0,1\}^\lambda$
$T := \{\}$

if $b = 0$
 $y = F_k(x)$
else
 if $x \notin T$
  $r \xleftarrow{\$} \{0,1\}^\lambda$
  $T[x] = r$
 $y = T[x]$

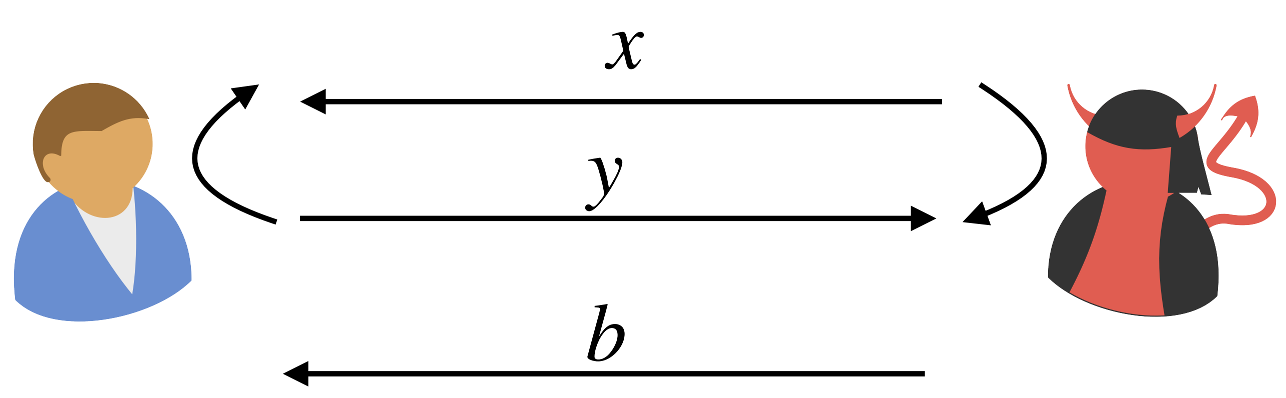


Wins if $b' = b$

$$\Pr[\mathscr{A} \text{ wins GuessGame}] \leq \frac{1}{2} + \nu(\lambda)$$

Game_0

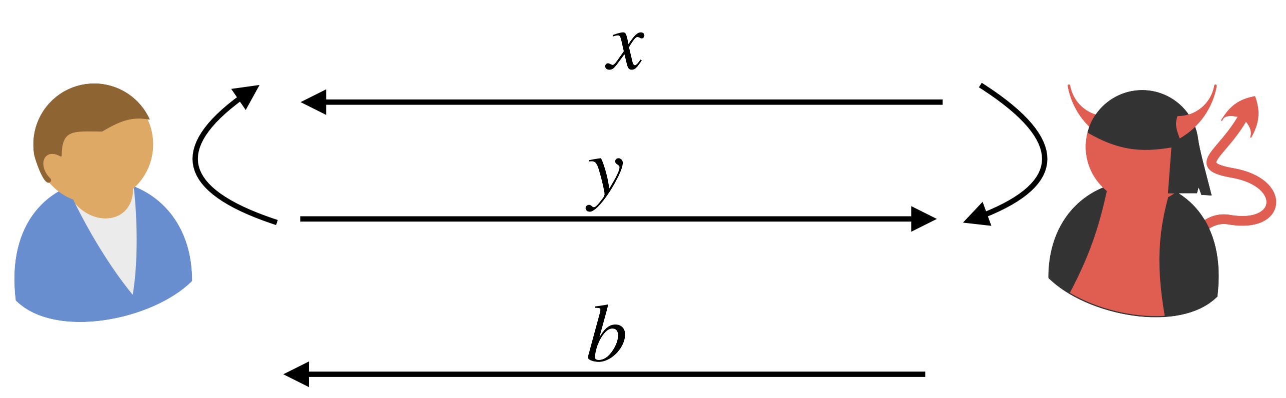
$k \xleftarrow{\$} \{0,1\}^\lambda$ $y = F_k(x)$



Game_1

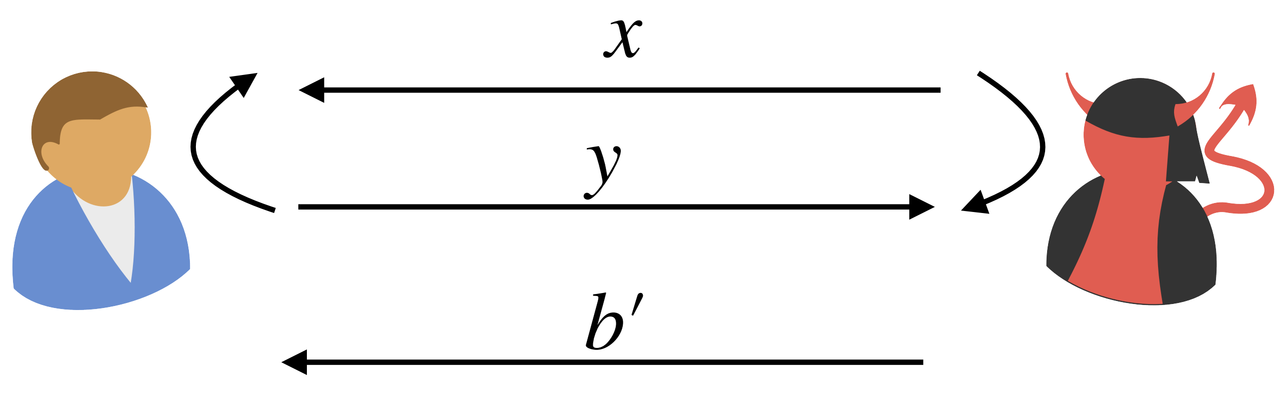
$T := \{\}$

if $x \notin T$
 $r \xleftarrow{\$} \{0,1\}^\lambda$
 $T[x] = r$
$y := T[x]$



$b \xleftarrow{\$} \{0,1\}$
$k \xleftarrow{\$} \{0,1\}^\lambda$
$T := \{\}$

if $b = 0$
  $y = F_k(x)$
else
  if $x \notin T$
    $r \xleftarrow{\$} \{0,1\}^\lambda$
    $T[x] = r$
  $y = T[x]$

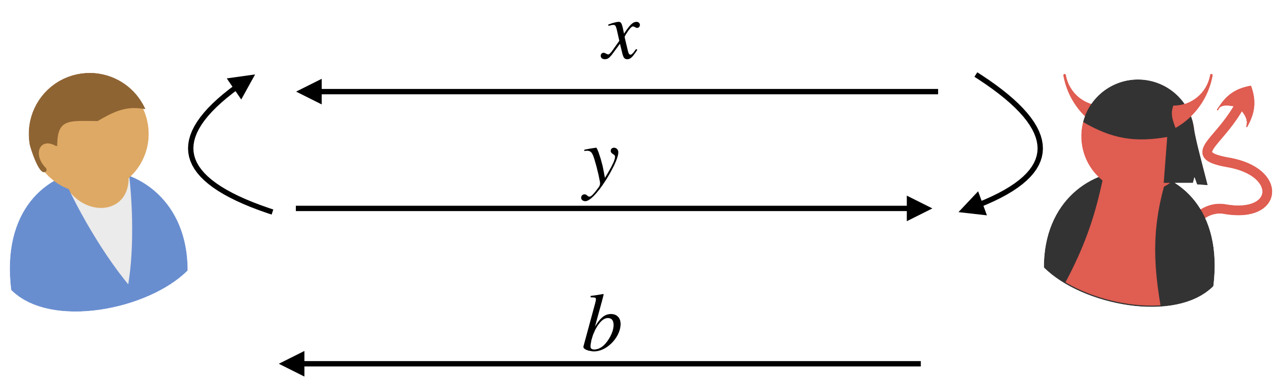


Wins if $b' = b$

$$\Pr[\mathscr{A} \text{ wins GuessGame}] \leq \frac{1}{2} + \nu(\lambda)$$

Game_0

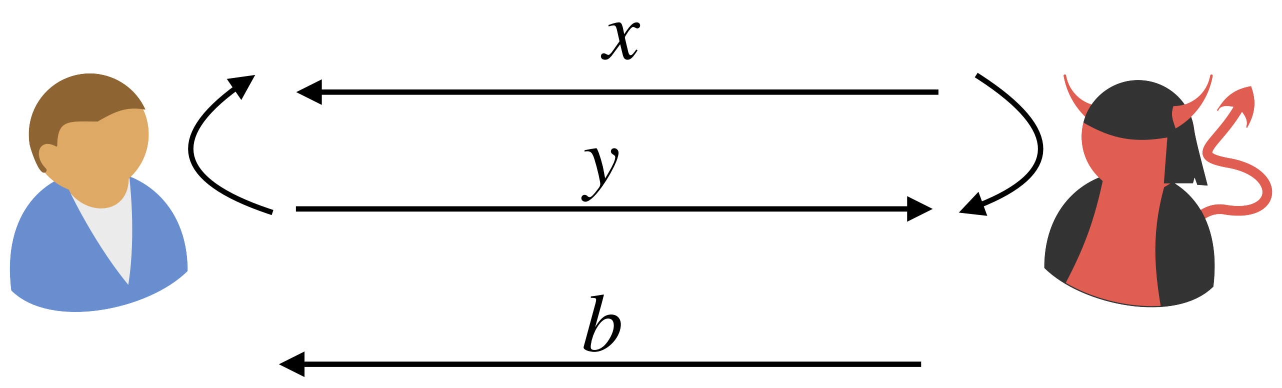
$k \xleftarrow{\$} \{0,1\}^\lambda$ $y = F_k(x)$



Game_1

$T := \{\}$

if $x \notin T$
  $r \xleftarrow{\$} \{0,1\}^\lambda$
  $T[x] = r$
$y := T[x]$



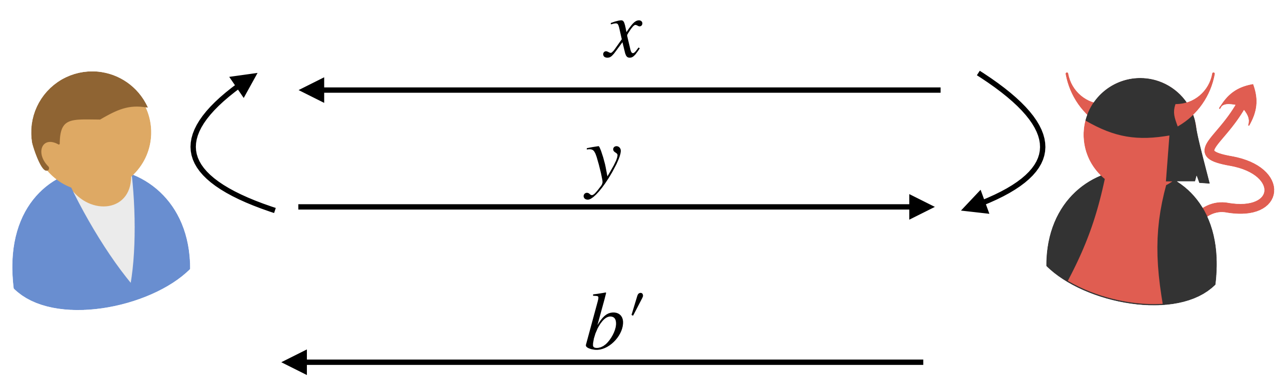
Let W_b be the event that $\mathscr{A}$ outputs 1 in Game_b

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

$k \xleftarrow{\$} \{0,1\}^\lambda$

$T := \{\}$

if $b = 0$
  $y = F_k(x)$
else
  if $x \notin T$
    $r \xleftarrow{\$} \{0,1\}^\lambda$
    $T[x] = r$
  $y = T[x]$

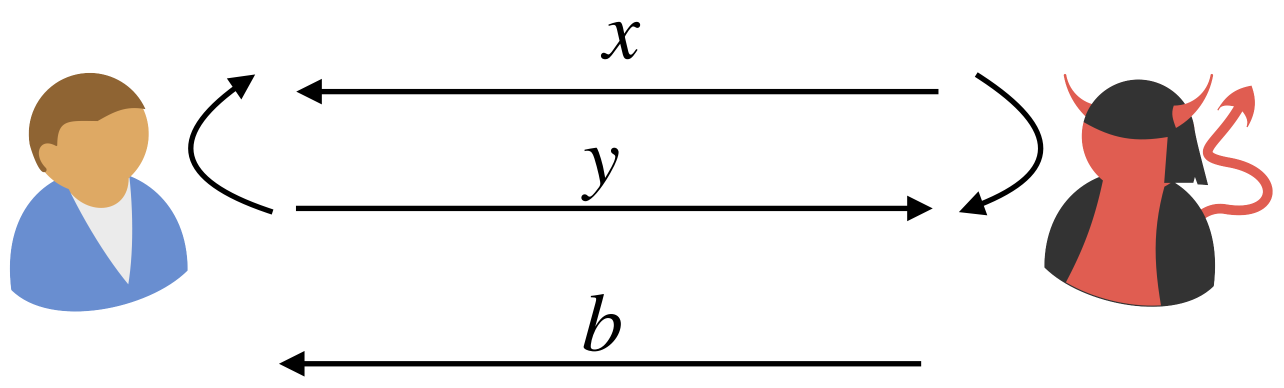


Wins if $b' = b$

$$\Pr[\mathscr{A} \text{ wins GuessGame}] \leq \frac{1}{2} + \nu(\lambda)$$

Game_0

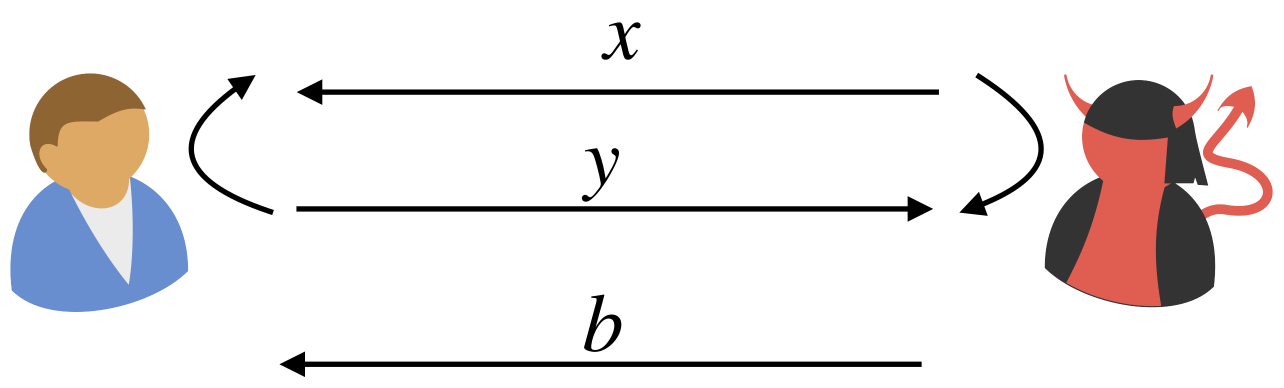
$k \xleftarrow{\$} \{0,1\}^\lambda$ $\quad y = F_k(x)$



Game_1

$T := \{\}$

if $x \notin T$
  $r \xleftarrow{\$} \{0,1\}^\lambda$
  $T[x] = r$
$y := T[x]$



Let W_b be the event that $\mathscr{A}$ outputs 1 in Game_b

$$\left| \Pr[W_0] - \Pr[W_1] \right| \leq \text{negl}(\lambda)$$

Pseudorandom Functions

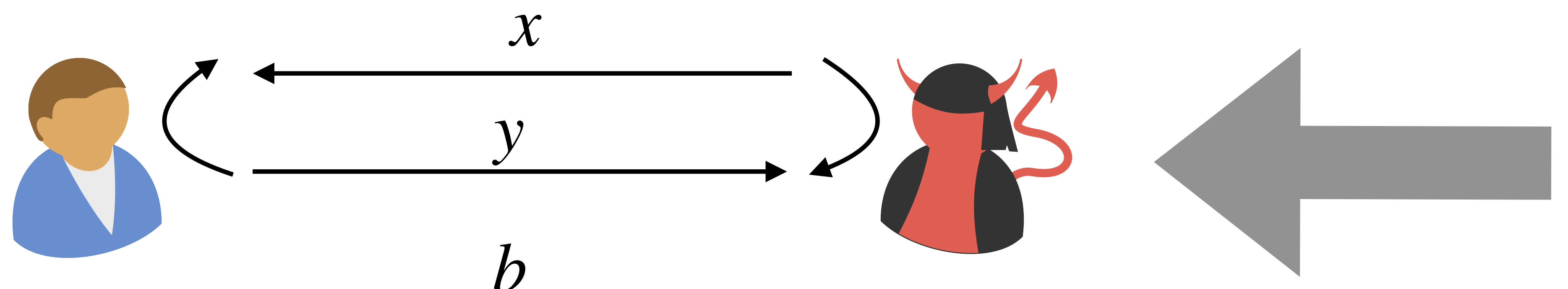
Pseudorandom Function

A deterministic family of functions $\{F_k\}_{k \in \{0,1\}^\lambda}$ where $F_k : \{0,1\}^\lambda \to \{0,1\}^\lambda$ for all k is *pseudorandom* if:

- $F_k(x)$ can be computed in polynomial time
- For all NUPPT $\mathscr{A}$, there exists a negligible function ν such that $\forall \lambda \in \mathbb{N}$,

$$\left| \Pr[\mathscr{A} \text{ outputs } 1 \text{ in Game}_0] - \Pr[\mathscr{A} \text{ outputs } 1 \text{ in Game}_1] \right| \leq \nu(\lambda)$$

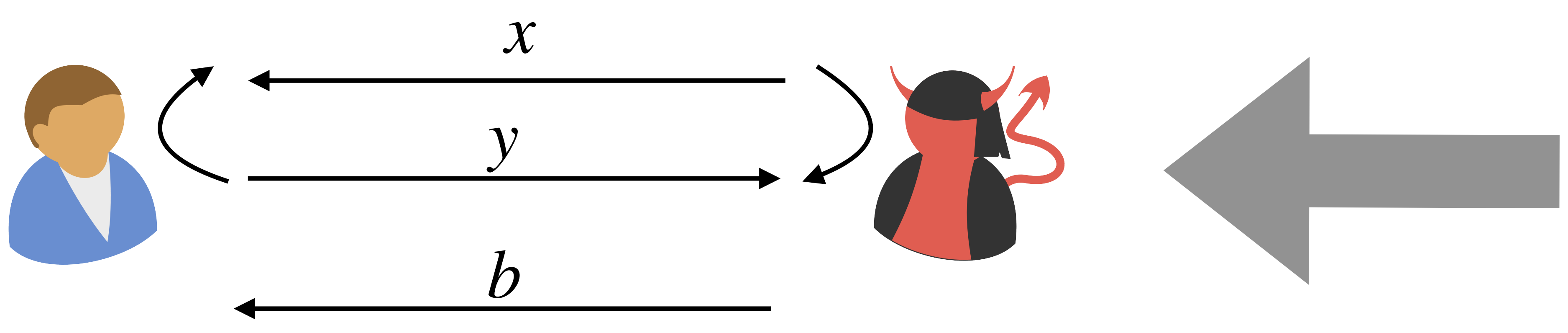
$k \xleftarrow{\$} \{0,1\}^\lambda \quad y = F_k(x)$



Game$_0$

$T := \{\}$

if $x \notin T$
$\quad r \xleftarrow{\$} \{0,1\}^\lambda$
$\quad T[x] = r$
$y := T[x]$



Game$_1$