Oblivious Transfer

CS 598 DH

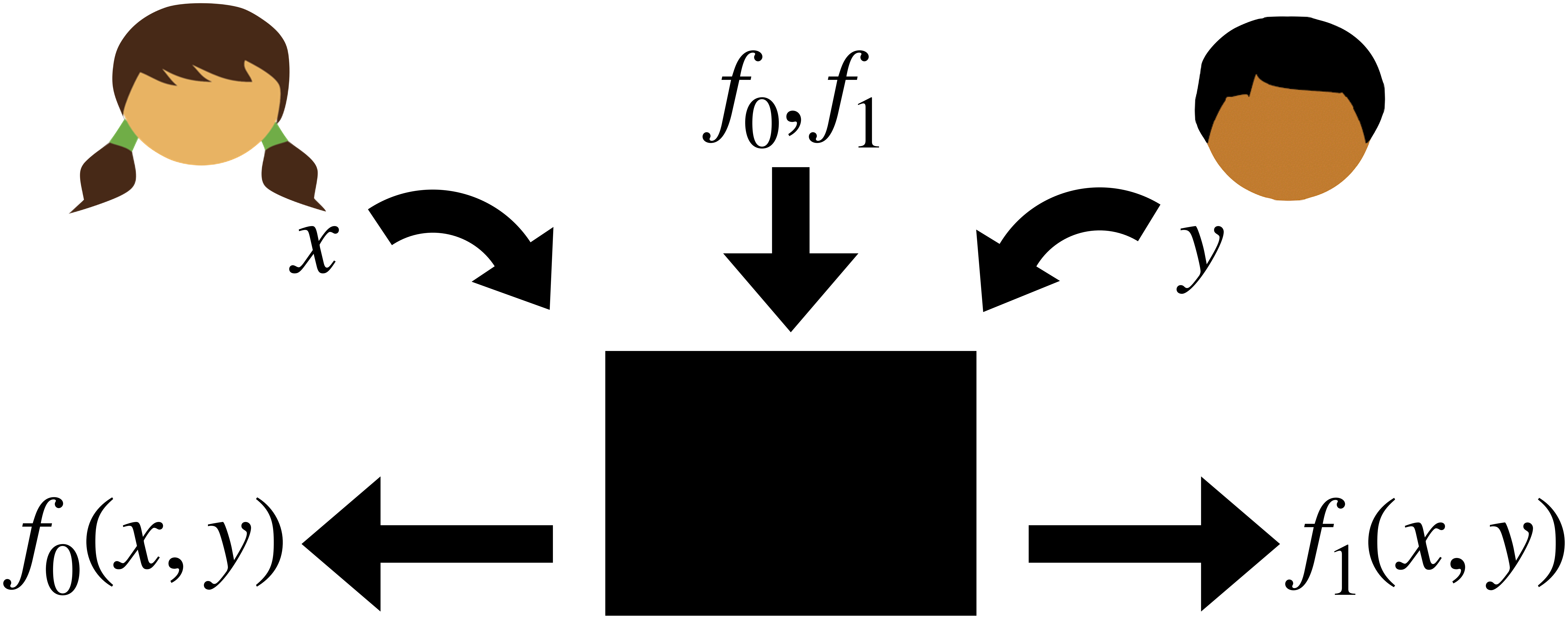
Today’s objectives

Review semi-honest security

Introduce **oblivious transfer (OT)**

Build OT from DDH

See an end-to-end security proof



f_0, f_1

x

y

$f_0(x, y)$

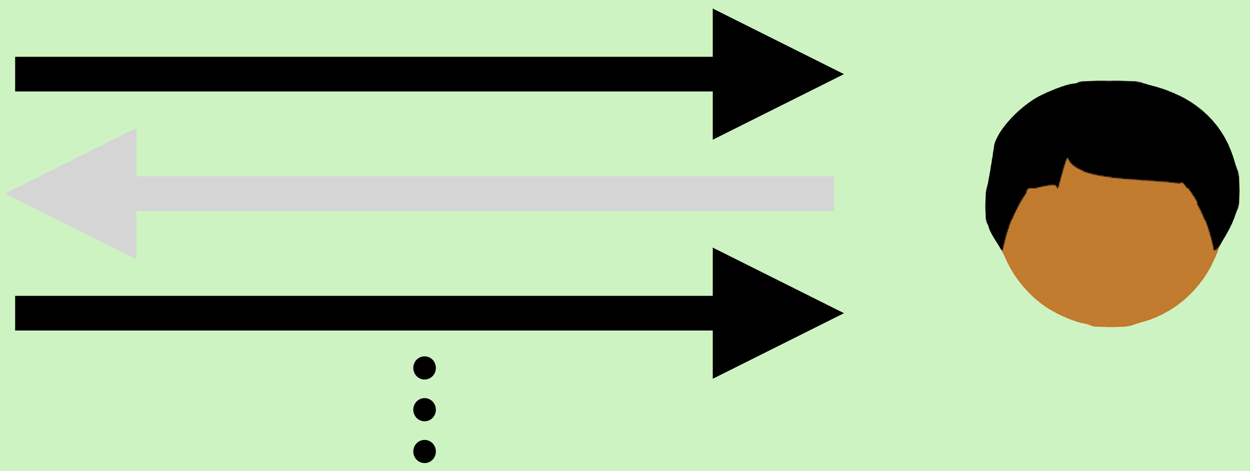
$f_1(x, y)$

Two-Party Semi-Honest Security
for deterministic functionalities

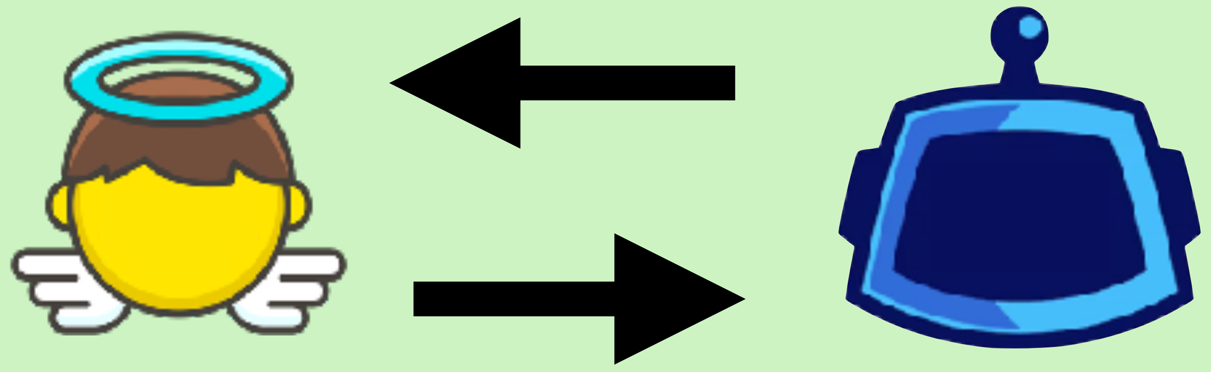
Let f_0,f_1 be functions. We say that a protocol Π securely computes f_0,f_1 in the presence of a semi-honest adversary if for each party $i \in \{0,1\}$ there exists a polynomial time simulator $\mathcal{S}_i$ *such that for all inputs x_0, x_1:*

$$\text{View}_i^{\Pi}(x_0, x_1) \overset{c}{=} \mathcal{S}_i(x_i, f_i(x_0, x_1))$$

Semi-honest Security



$\text{View}^{\Pi}_{\text{Bob}}(x, y) = \{\ y, m_0, m_1, \ldots\ \}$



$\text{Output}^{\text{Sim}}_{\text{Bob}}(x, y) = \{\ y, m_0, m_1, \ldots\ \}$

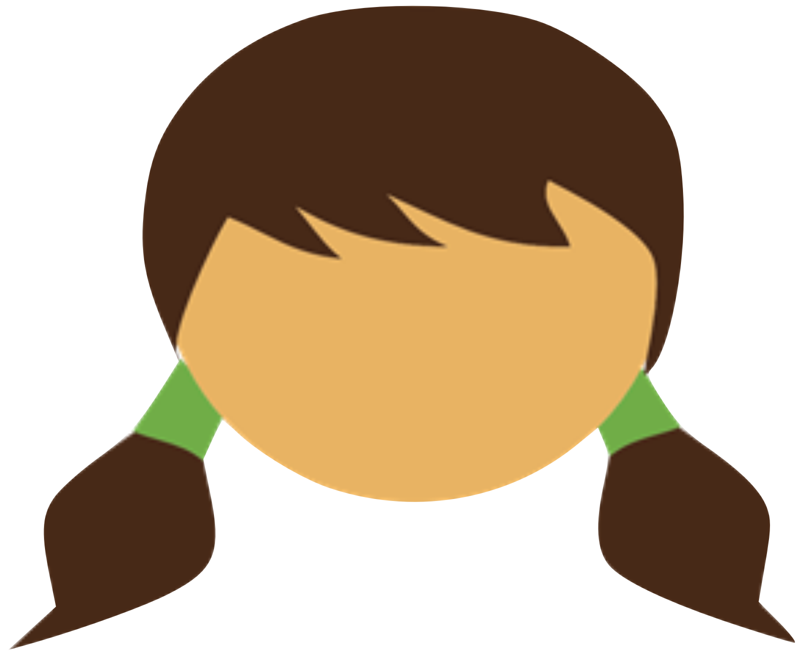
Three notions of “hard to tell apart”

$X \equiv Y$ Identically distributed

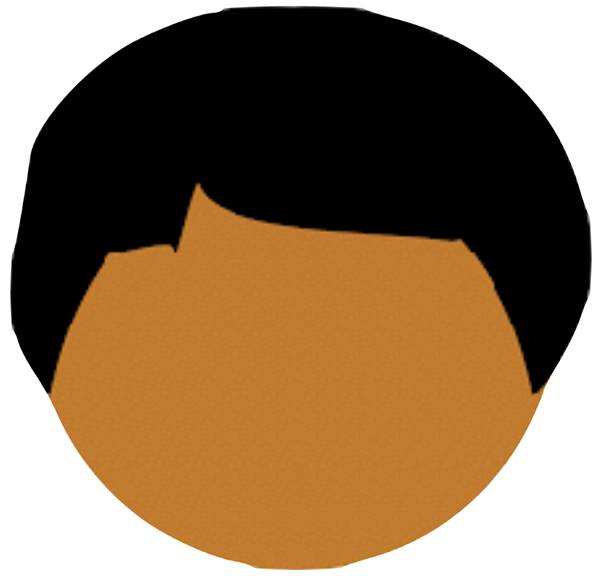
$X \approx Y$ Statistically close As we increase a parameter, the distributions **quickly** become close together.

$X \overset{c}{=} Y$ Indistinguishable As we increase a parameter, it **quickly** becomes difficult for programs to tell the distributions apart.

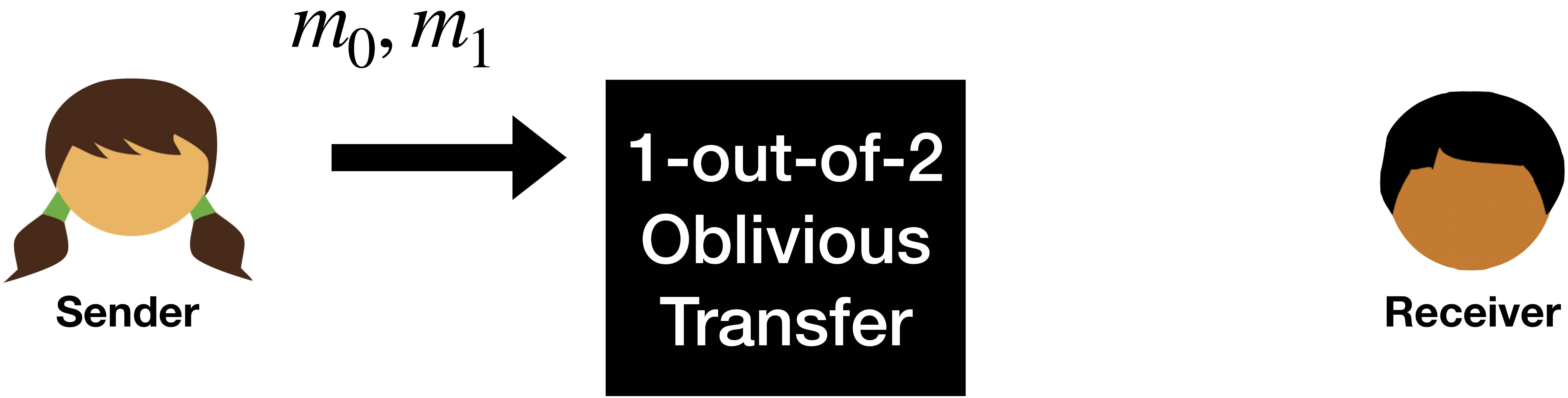
Oblivious Transfer



Sender



Receiver

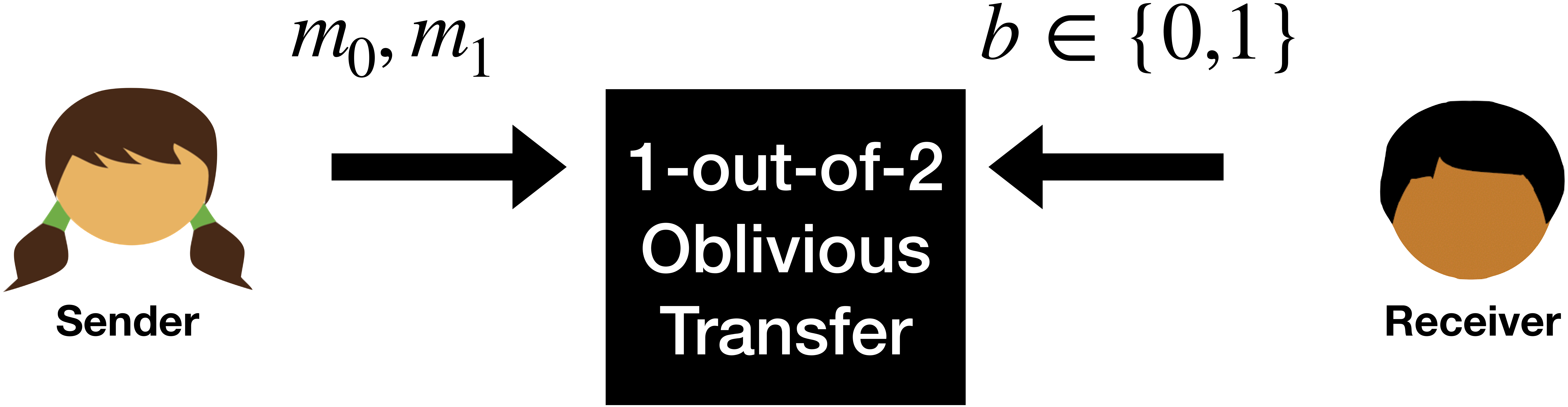


m_0, m_1

1-out-of-2 Oblivious Transfer

Sender

Receiver



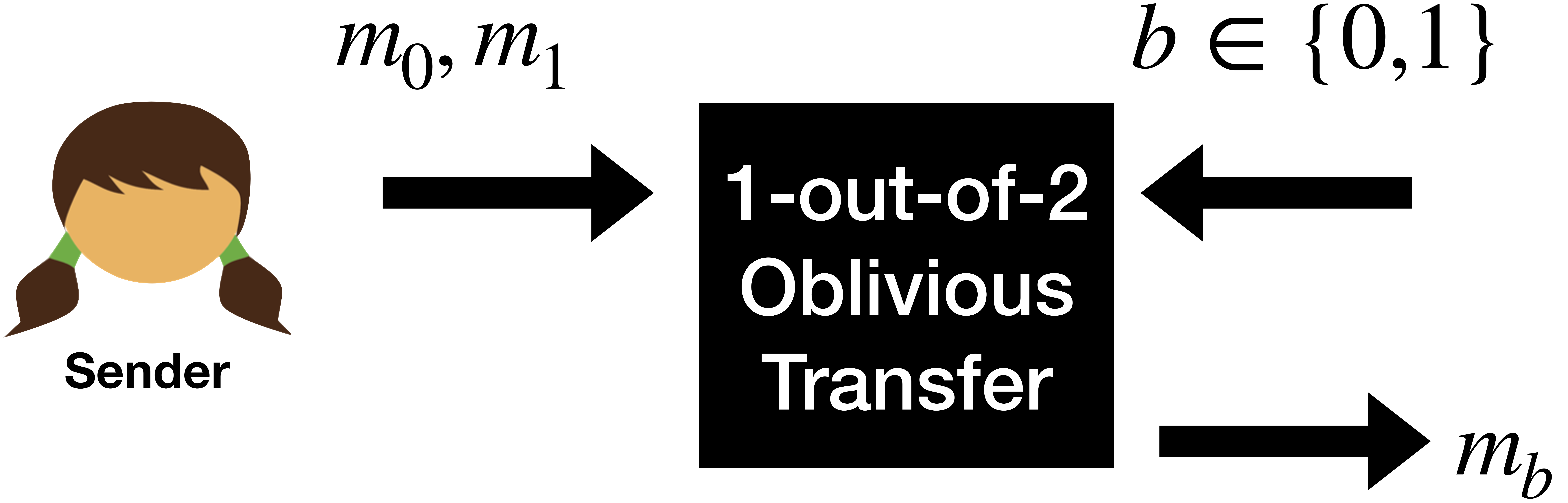
m_0, m_1

Sender

1-out-of-2 Oblivious Transfer

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

Receiver



m_0, m_1

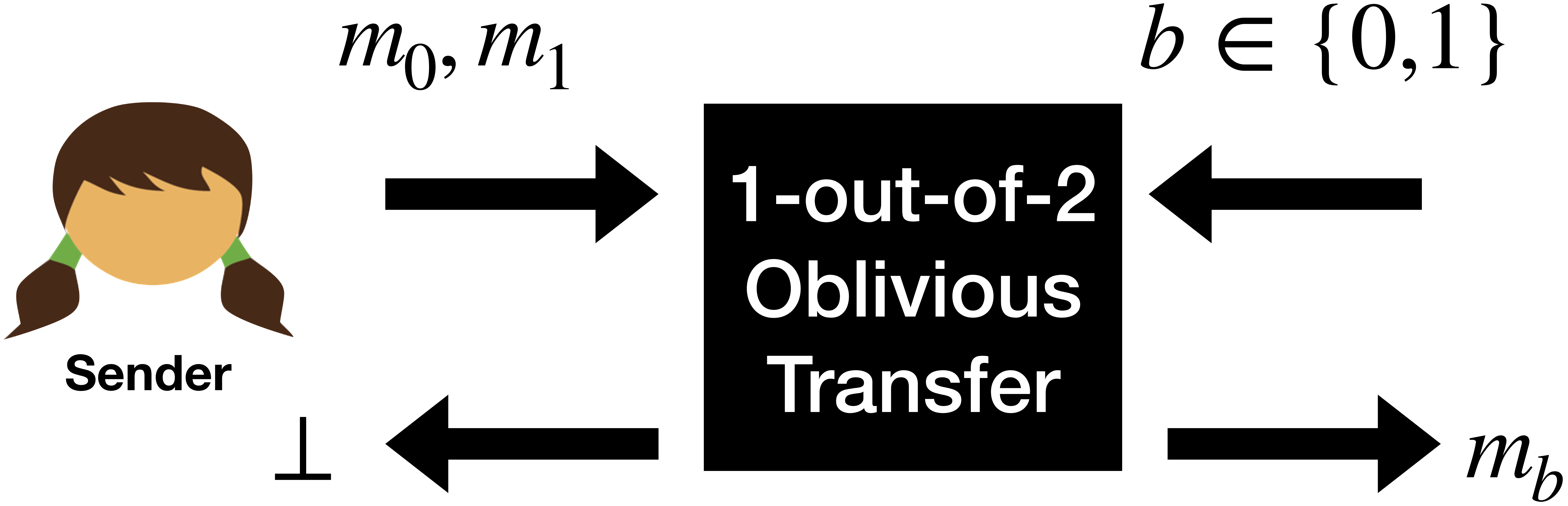
$b \in \{0,1\}$

1-out-of-2 Oblivious Transfer

Sender

Receiver

m_b



m_0, m_1

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

1-out-of-2 Oblivious Transfer

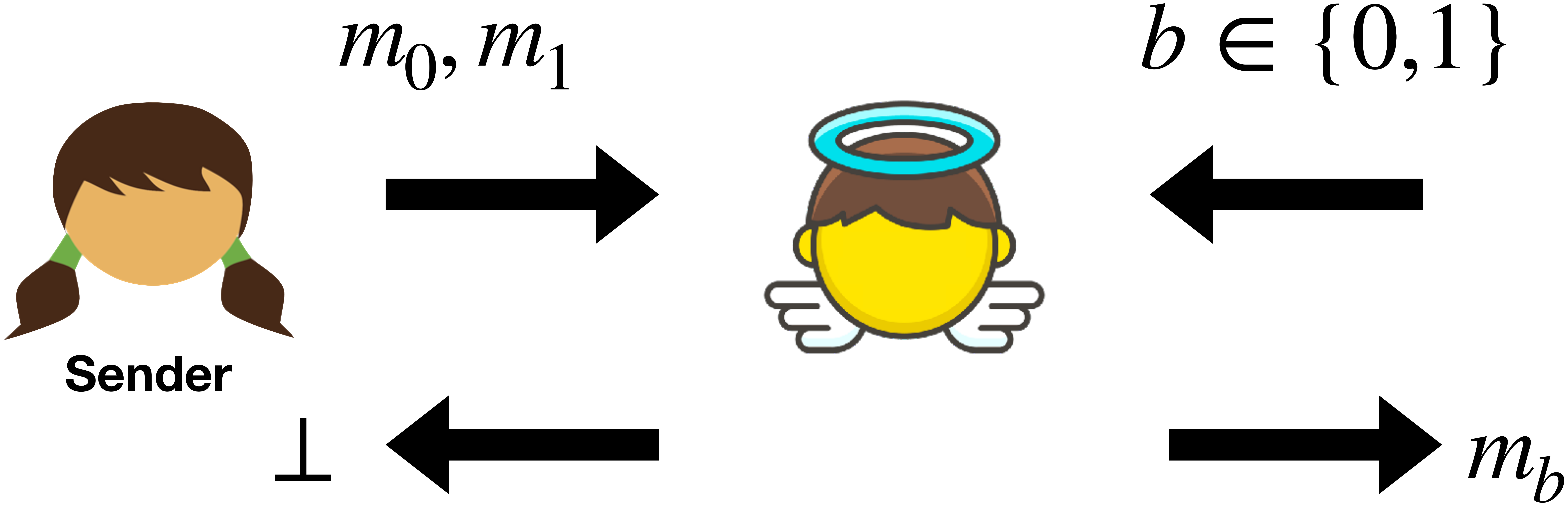
Sender

Receiver

$\perp$

m_b

1-out-of-2 OT Ideal Functionality



m_0, m_1

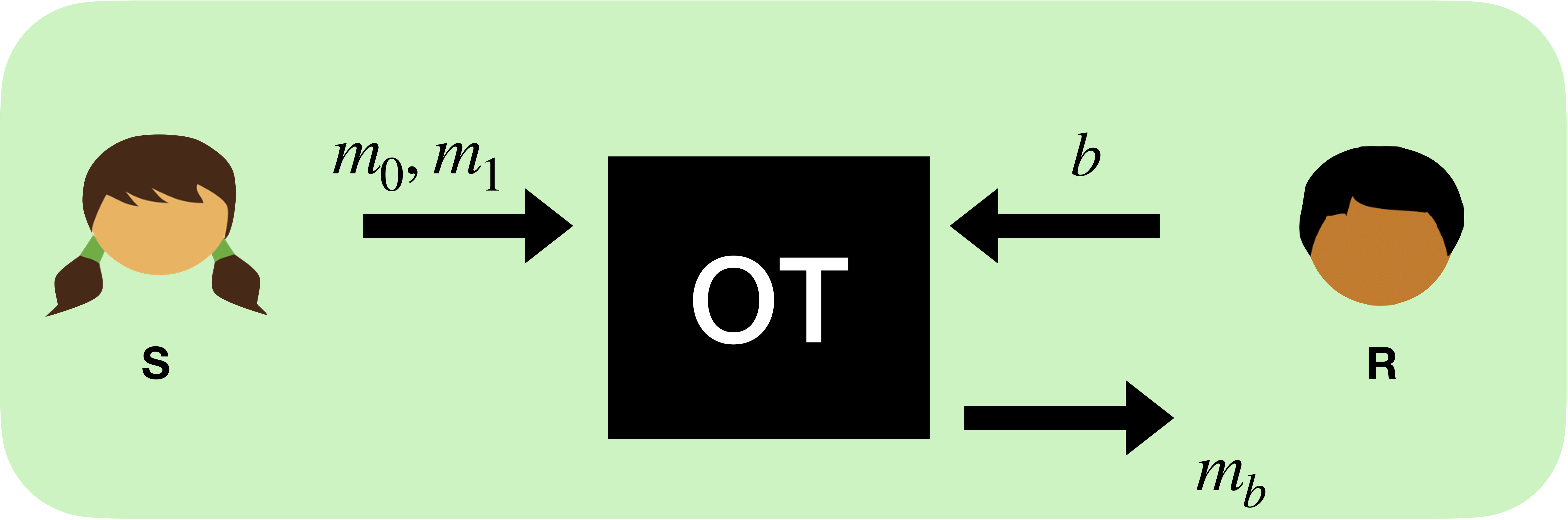
$b \in \{0,1\}$

Sender

Receiver

$\perp$

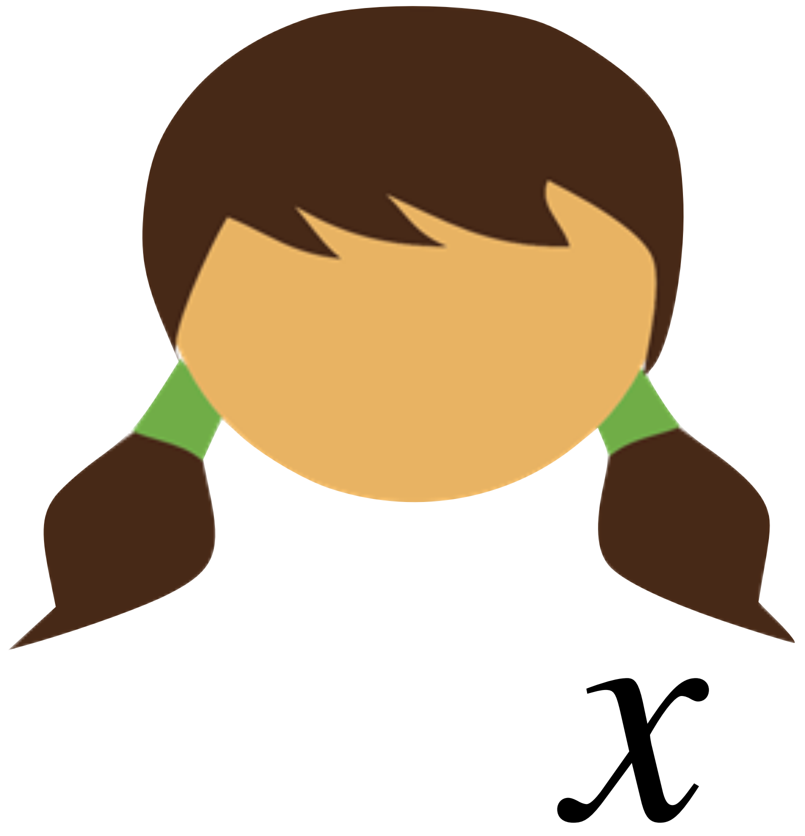
m_b

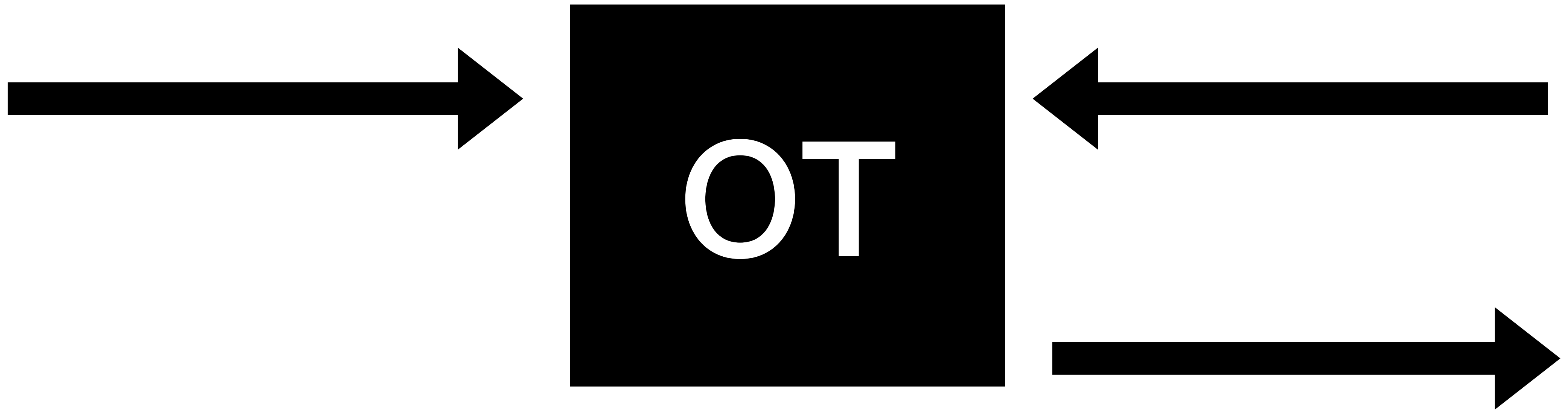


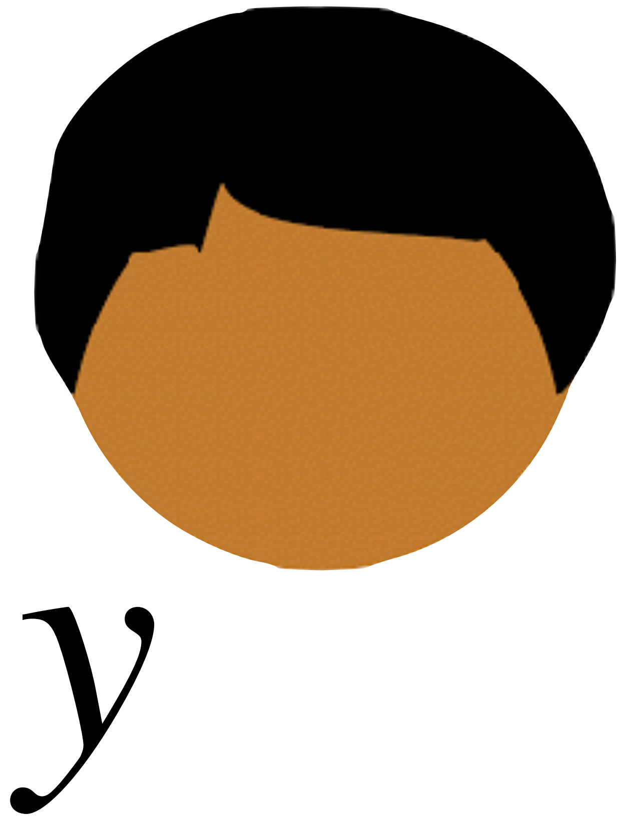
OT is an extremely powerful tool

Given enough OTs, we can build a semi-honest protocol for *any* computable function

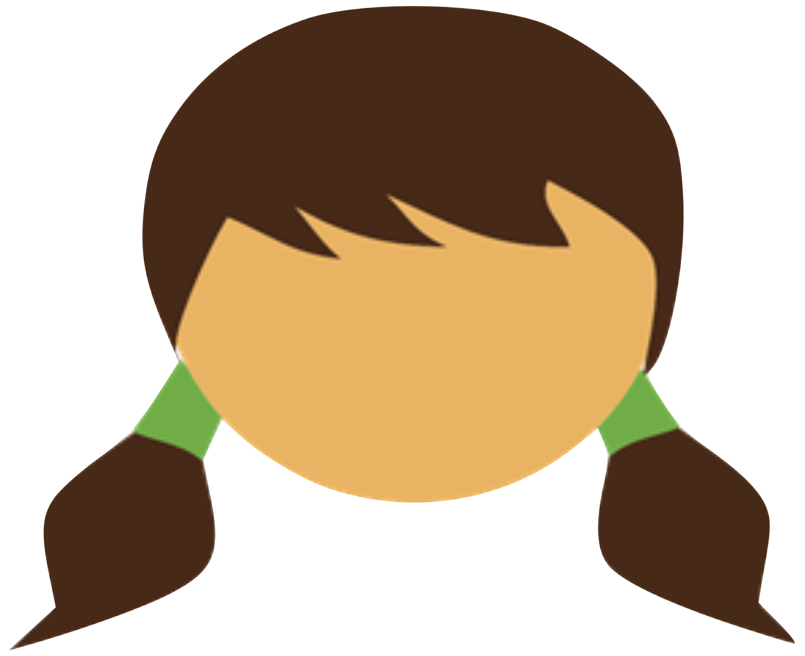
Secure AND



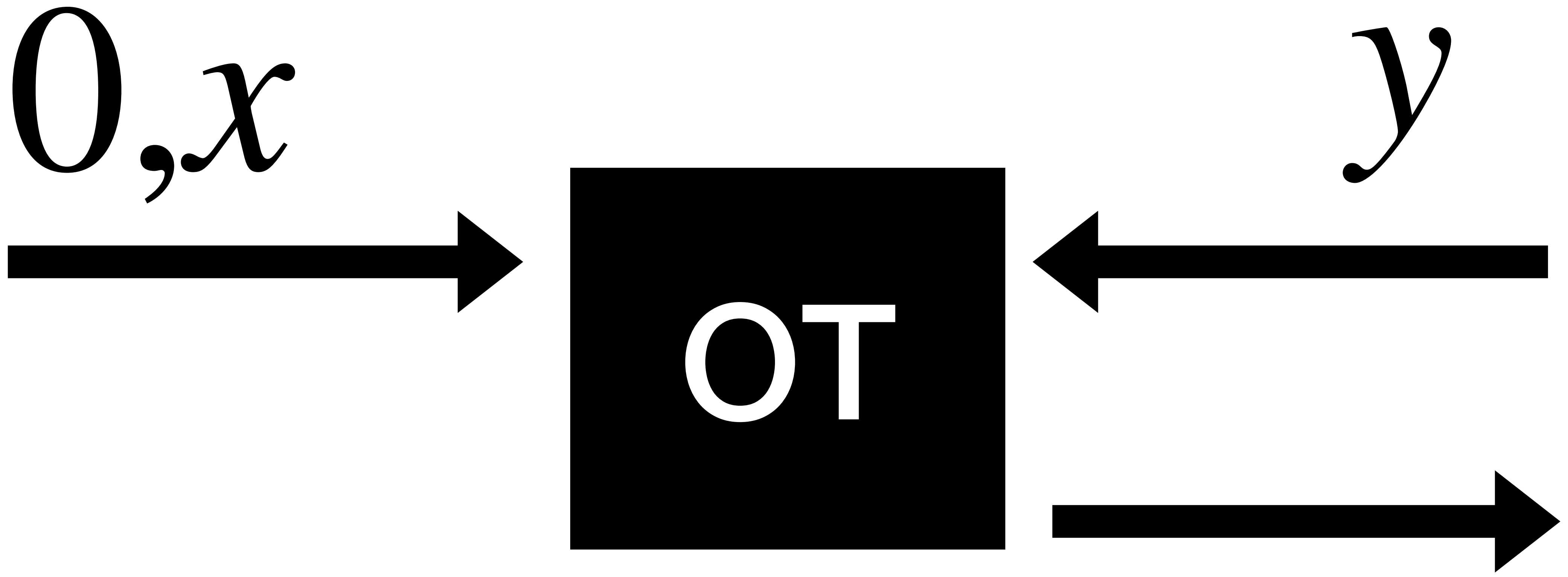




Secure AND



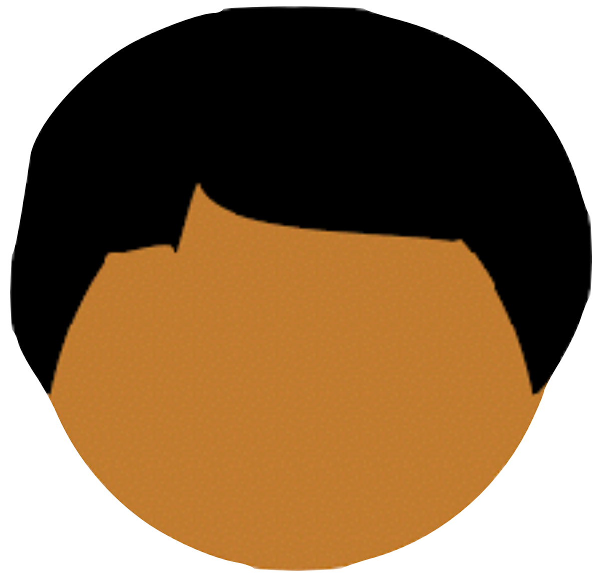
x



$0,x$

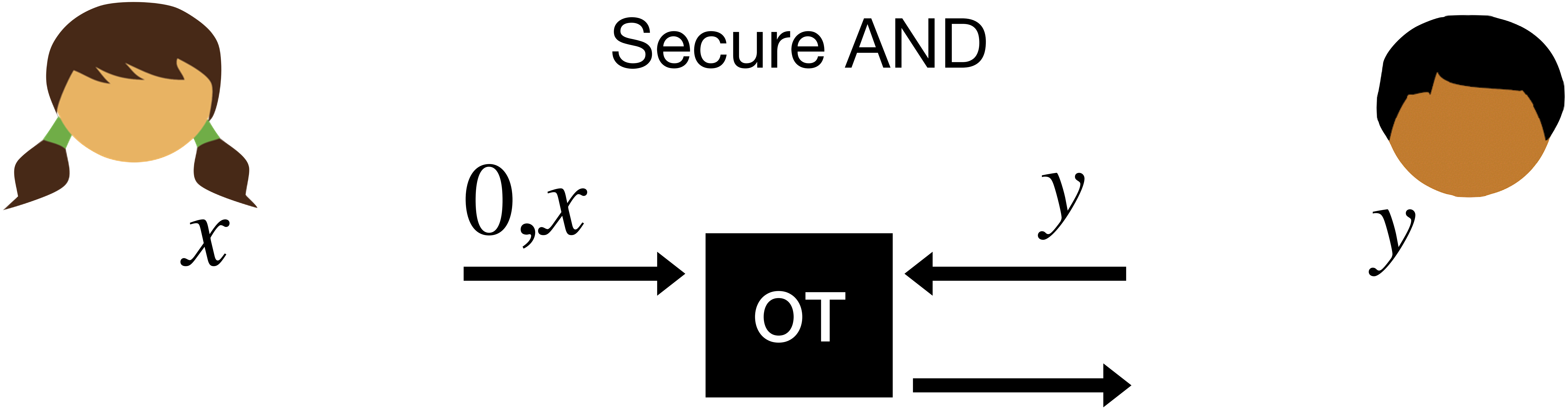
OT

y



y

Secure AND



x

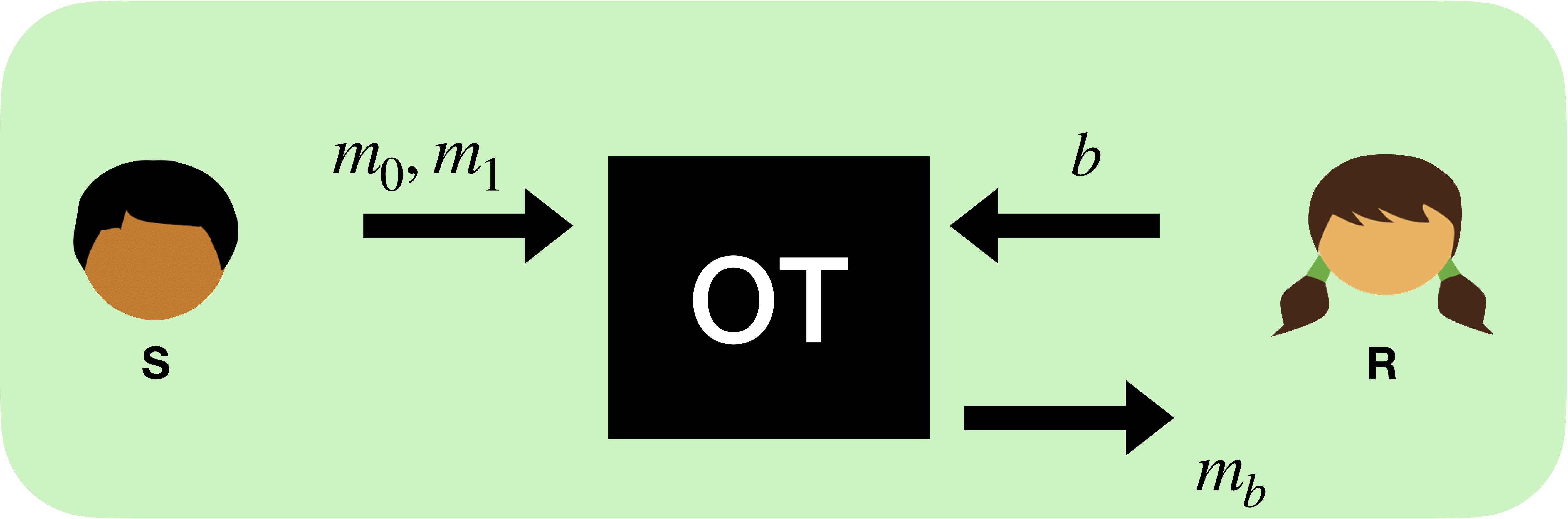
$0, x$

OT

y

y

$$\left(\begin{cases} 0 & \text{if } y = 0 \\ x & \text{if } y = 1 \end{cases}\right) = x \wedge y$$

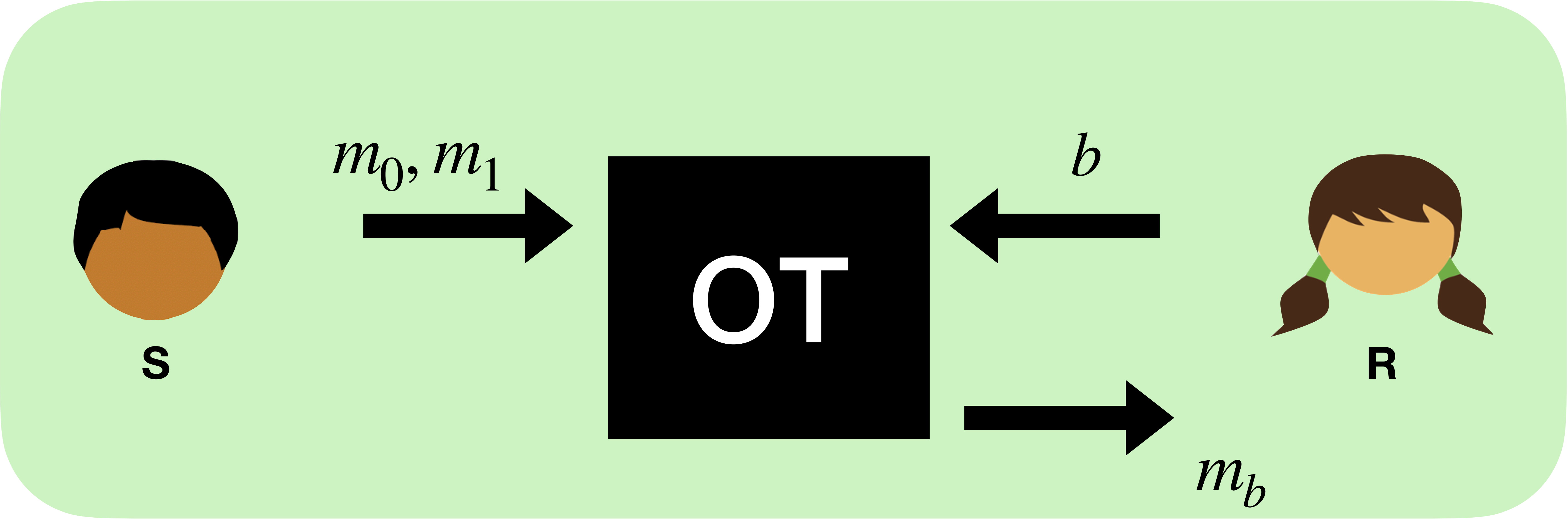


Public Key Encryption Scheme

Generating a key makes a public key, private key pair pk, sk

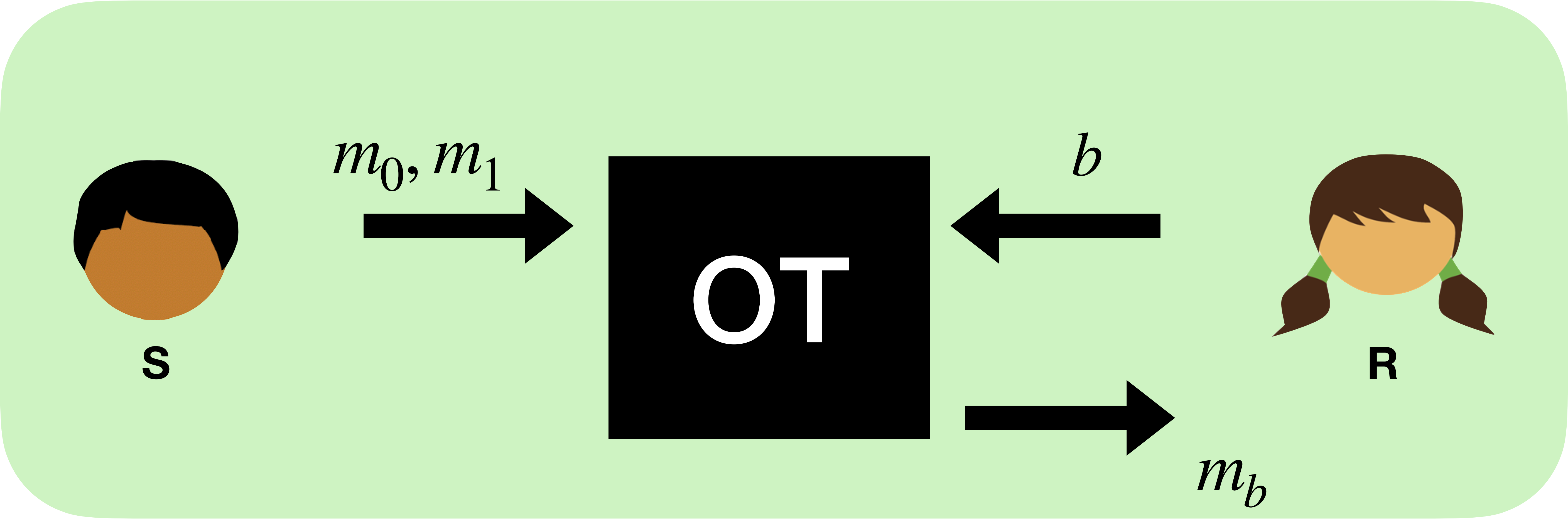
Anyone with pk can encrypt messages

Only those with sk can decrypt



Intuitive Idea for OT

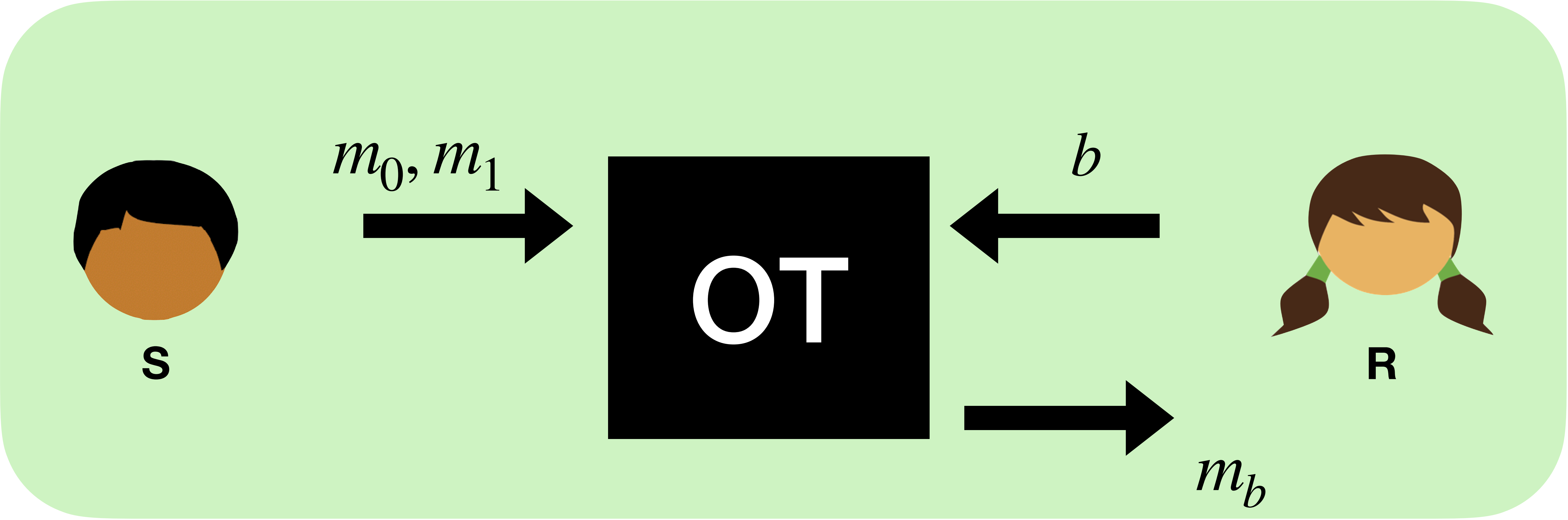
Receiver makes two public keys, but only one has a matching private key



Intuitive Idea for OT

Receiver makes two public keys, but only one has a matching private key

Receiver sends each public key to Sender

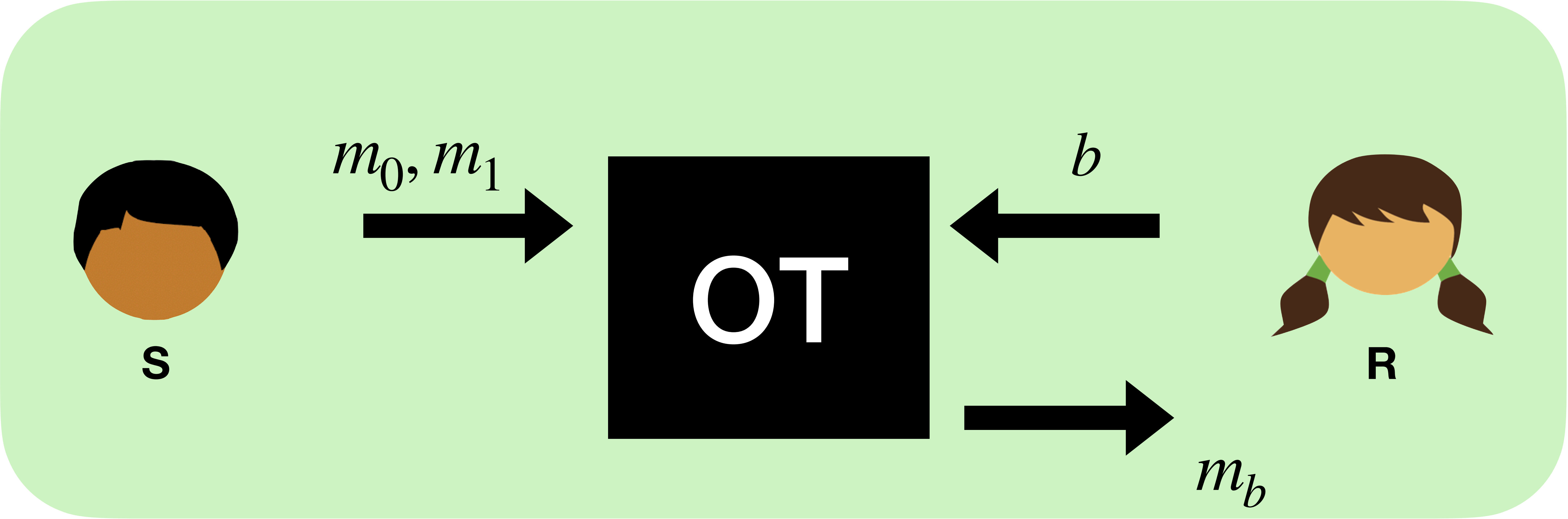


Intuitive Idea for OT

Receiver makes two public keys, but only one has a matching private key

Receiver sends each public key to Sender

Sender encrypts one message per key



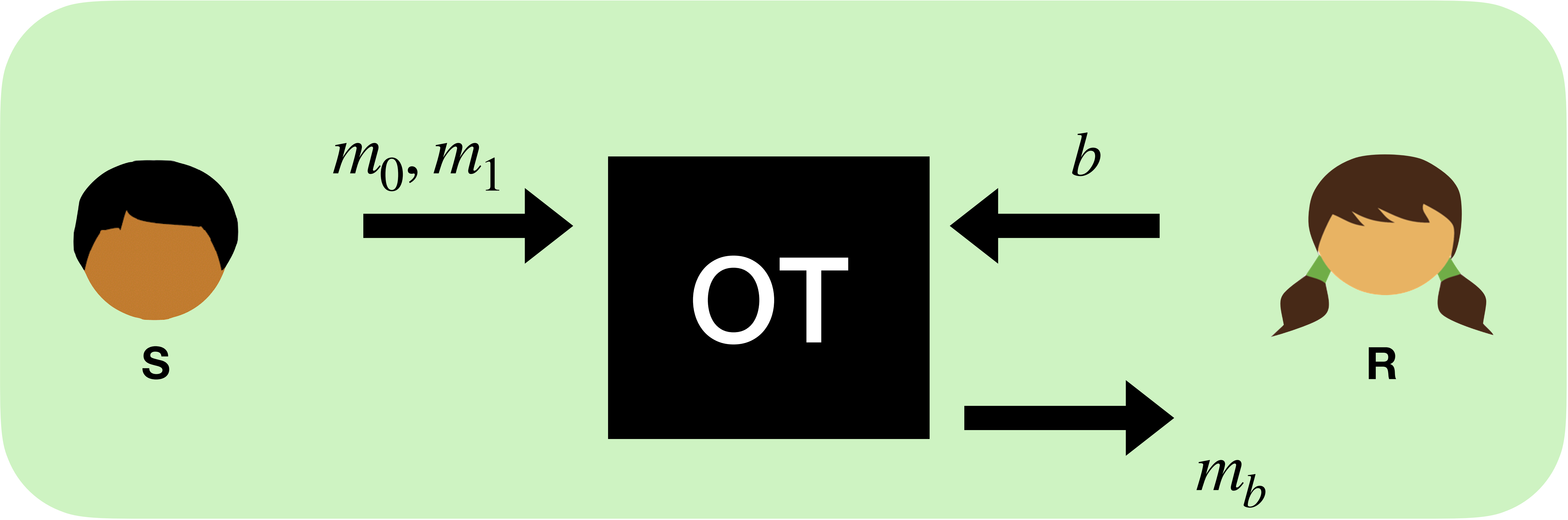
Intuitive Idea for OT

Receiver makes two public keys, but only one has a matching private key

Receiver sends each public key to Sender

Sender encrypts one message per key

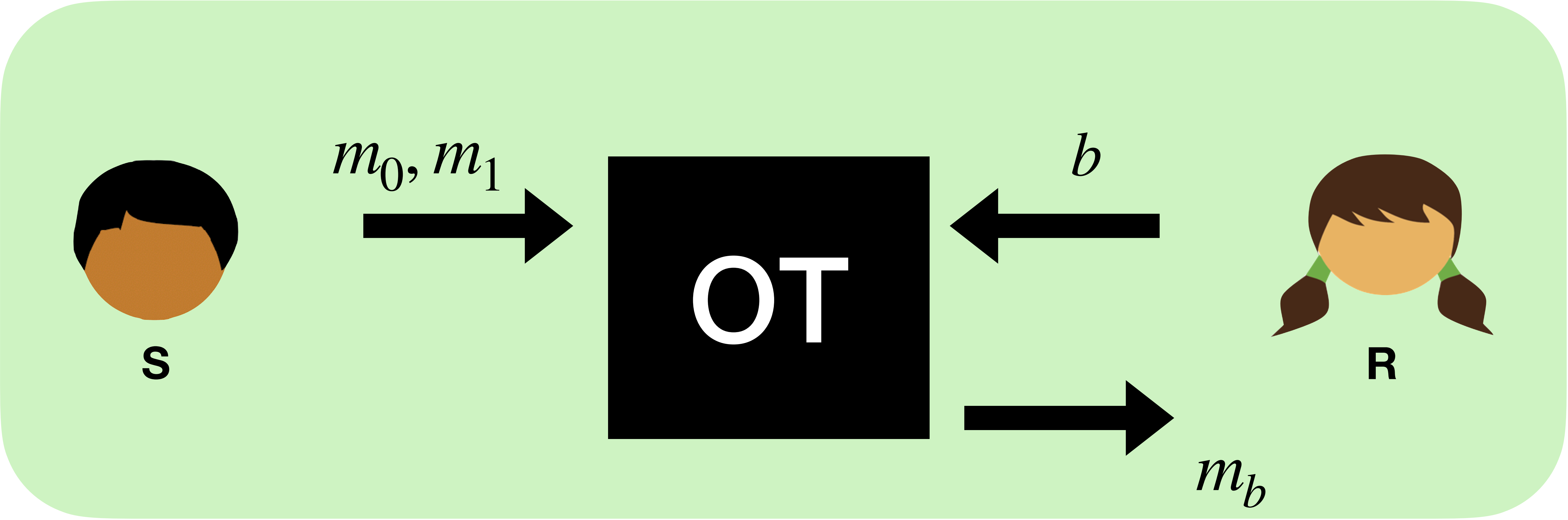
Receiver decrypts (only) the desired message



Goal:

Correctness

Semi-honest Security



Goal:

- Correctness
- Semi-honest Security

$$\mathrm{View}_S^{\mathrm{OT}}(m_0, m_1, b) \approx \mathcal{S}_S(m_0, m_1, \perp)$$

$$\mathrm{View}_R^{\mathrm{OT}}(m_0, m_1, b) \approx \mathcal{S}_R(b, m_b)$$

Decisional Diffie-Hellman Assumption

“It is hard to compute logarithms in certain mathematical sets”

Decisional Diffie-Hellman Assumption

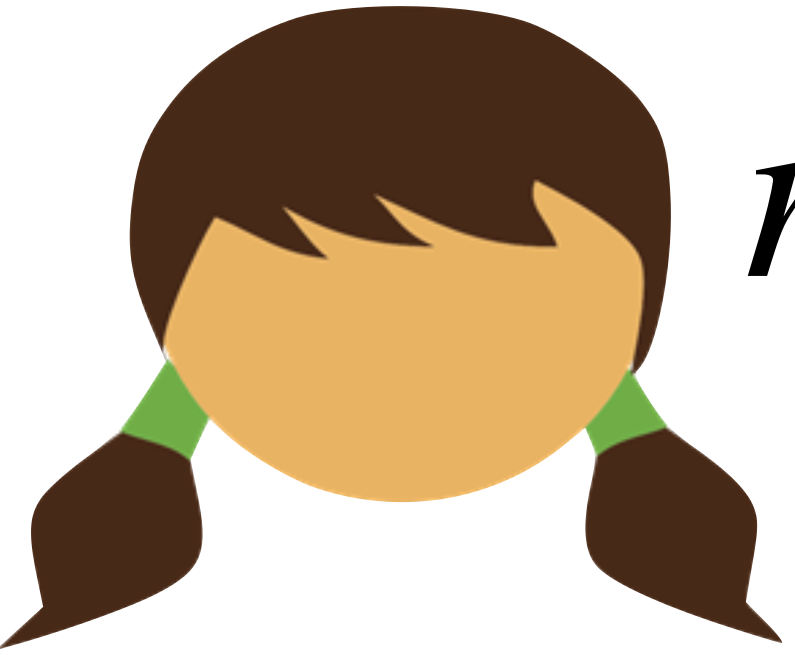
“It is hard to compute logarithms in certain mathematical sets”

Let G be a cyclic group of order q with generator g

```
Real( ):
    $a \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $b \overset{\$}{\leftarrow} \mathbb{Z}_q$
    return $\{g^a, g^b, g^{a \cdot b}\}$
```

$$\overset{c}{=}$$

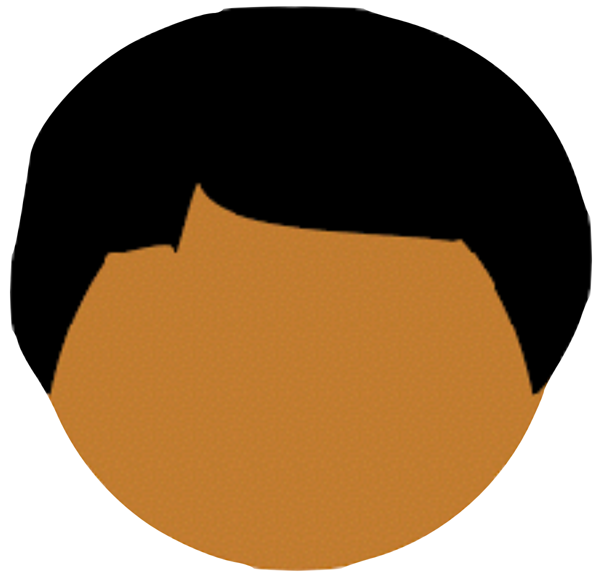
```
Ideal( ):
    $a \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $b \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $c \overset{\$}{\leftarrow} \mathbb{Z}_q$
    return $\{g^a, g^b, g^c\}$
```



m_0, m_1

Sender

b



Receiver

$$a \xleftarrow{\$} \mathbb{Z}_q$$

$$h_b \leftarrow g^a$$

$$h_{1-b} \xleftarrow{\$} G$$

m_0, m_1

Sender

b

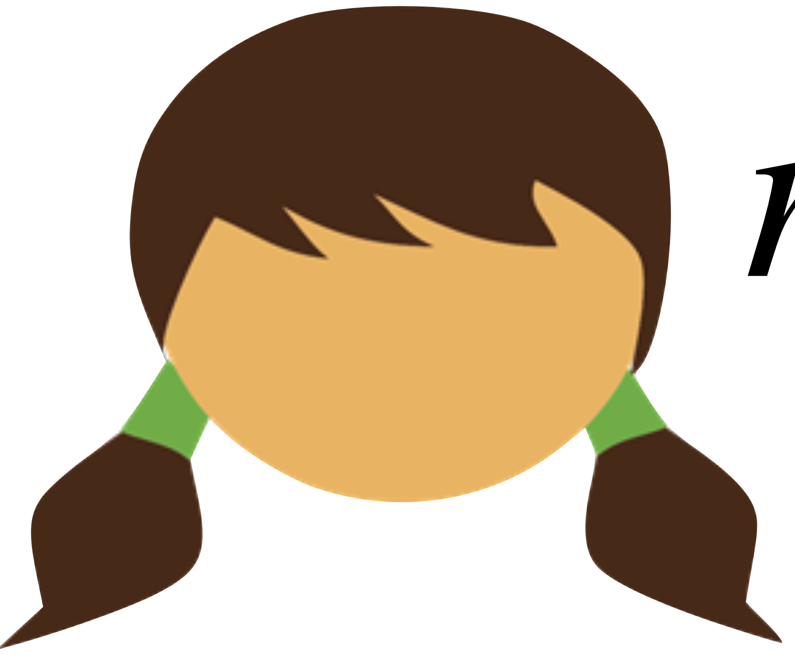
Receiver

$a \xleftarrow{\$} \mathbb{Z}_q$

$h_b \leftarrow g^a$

$h_{1-b} \xleftarrow{\$} G$

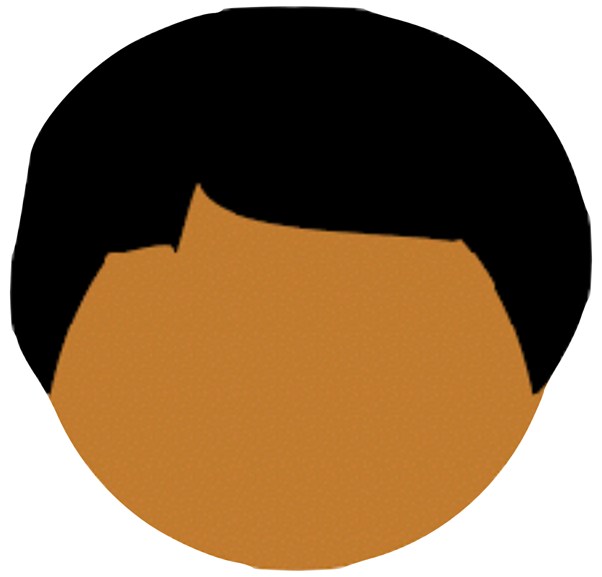
h_0, h_1



m_0, m_1

Sender

b



Receiver

$a \xleftarrow{\$} \mathbb{Z}_q$

$h_b \leftarrow g^a$

$h_{1-b} \xleftarrow{\$} G$

$$\xleftarrow{\quad h_0, h_1 \quad}$$

$r_0 \xleftarrow{\$} \mathbb{Z}_q$

$r_1 \xleftarrow{\$} \mathbb{Z}_q$

m_0, m_1

b

Sender

Receiver

$a \xleftarrow{\$} \mathbb{Z}_q$

$h_b \leftarrow g^a$

$h_{1-b} \xleftarrow{\$} G$

h_0, h_1

$r_0 \xleftarrow{\$} \mathbb{Z}_q$

$r_1 \xleftarrow{\$} \mathbb{Z}_q$

g^{r_0} g^{r_1}

$h_0^{r_0} \cdot m_0$ $h_1^{r_1} \cdot m_1$

$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a}$$

m_0, m_1

Sender

$r_0 \overset{\$}{\leftarrow} \mathbb{Z}_q$

$r_1 \overset{\$}{\leftarrow} \mathbb{Z}_q$

h_0, h_1

$g^{r_0} \quad g^{r_1}$

$h_0^{r_0} \cdot m_0 \quad h_1^{r_1} \cdot m_1$

b

Receiver

$a \overset{\$}{\leftarrow} \mathbb{Z}_q$

$h_b \leftarrow g^a$

$h_{1-b} \overset{\$}{\leftarrow} G$

$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a}$$

$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a}$$

m_0, m_1

Sender

$r_0 \xleftarrow{\$} \mathbb{Z}_q$

$r_1 \xleftarrow{\$} \mathbb{Z}_q$

h_0, h_1

g^{r_0} $\quad$ g^{r_1}

$h_0^{r_0} \cdot m_0$ $\quad$ $h_1^{r_1} \cdot m_1$

$a \xleftarrow{\$} \mathbb{Z}_q$

$h_b \leftarrow g^a$

$h_{1-b} \xleftarrow{\$} G$

b

Receiver

$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a}$$

$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a} = \frac{(g^a)^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a}$$

Sender m_0, m_1

Receiver b

$a \xleftarrow{\$} \mathbb{Z}_q$

$h_b \leftarrow g^a$

$h_{1-b} \xleftarrow{\$} G$

h_0, h_1

$r_0 \xleftarrow{\$} \mathbb{Z}_q$

$r_1 \xleftarrow{\$} \mathbb{Z}_q$

g^{r_0} g^{r_1}

$h_0^{r_0} \cdot m_0$ $h_1^{r_1} \cdot m_1$

$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a}$$

$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a} = \frac{(g^a)^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a} = \frac{g^{a \cdot r_b} \cdot m_b}{g^{a \cdot r_b}}$$

Sender

m_0, m_1

$r_0 \overset{\$}{\leftarrow} \mathbb{Z}_q$

$r_1 \overset{\$}{\leftarrow} \mathbb{Z}_q$

Receiver

b

$a \overset{\$}{\leftarrow} \mathbb{Z}_q$

$h_b \leftarrow g^a$

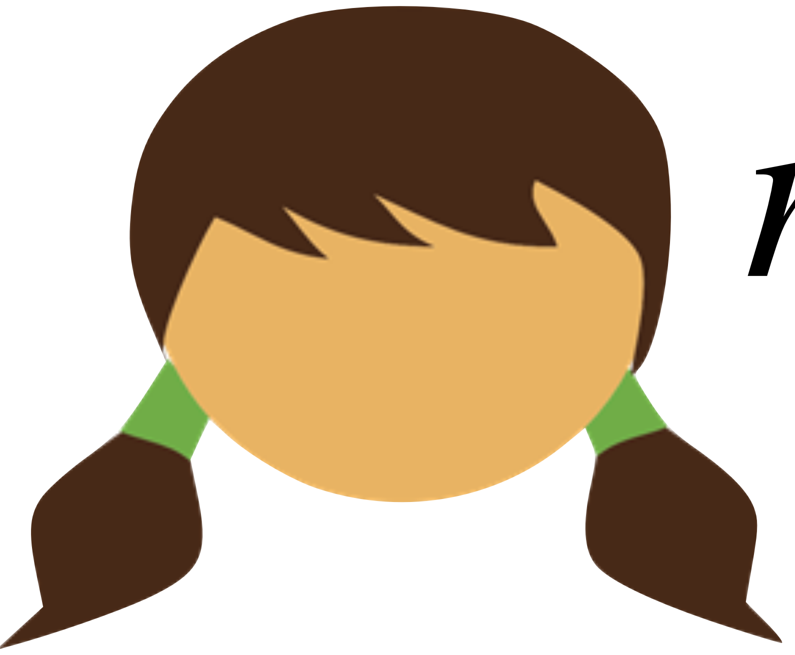
$h_{1-b} \overset{\$}{\leftarrow} G$

$$\xleftarrow{h_0, h_1}$$

$$\xrightarrow{g^{r_0} \quad g^{r_1} \quad h_0^{r_0} \cdot m_0 \quad h_1^{r_1} \cdot m_1}$$

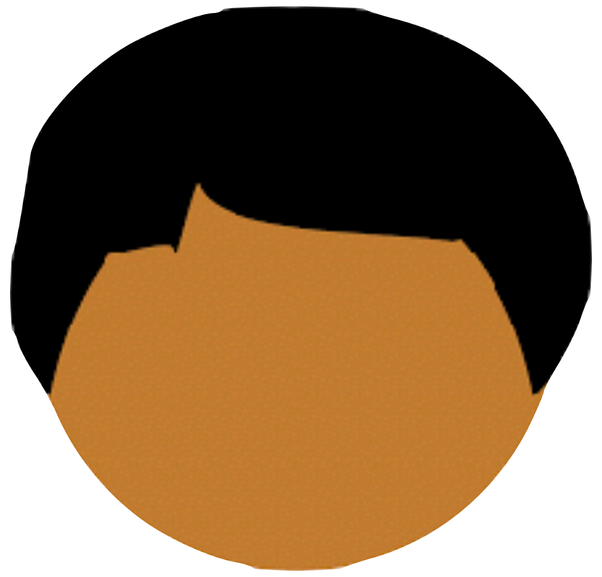
$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a}$$

$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a} = \frac{(g^a)^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a} = \frac{g^{a \cdot r_b} \cdot m_b}{g^{a \cdot r_b}} = m_b$$



m_0, m_1

Sender



b

Receiver

$a \xleftarrow{\$} \mathbb{Z}_q$

$h_b \leftarrow g^a$

$h_{1-b} \xleftarrow{\$} G$

$$\xleftarrow{\quad h_0, h_1 \quad}$$

$r_0 \xleftarrow{\$} \mathbb{Z}_q$

$r_1 \xleftarrow{\$} \mathbb{Z}_q$

$$\xrightarrow[\quad h_0^{r_0} \cdot m_0 \qquad h_1^{r_1} \cdot m_1 \quad]{\quad g^{r_0} \qquad g^{r_1} \quad}$$

$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a}$$

$$\text{View}_S^{\text{OT}}(m_0, m_1, b) = \cdots$$

m_0, m_1

Sender

b

Receiver

$a \xleftarrow{\$} \mathbb{Z}_q$

$h_b \leftarrow g^a$

$h_{1-b} \xleftarrow{\$} G$

h_0, h_1

$r_0 \xleftarrow{\$} \mathbb{Z}_q$

$r_1 \xleftarrow{\$} \mathbb{Z}_q$

g^{r_0} g^{r_1}

$h_0^{r_0} \cdot m_0$ $h_1^{r_1} \cdot m_1$

$\dfrac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a}$

$$\mathrm{View}_S^{\mathrm{OT}}(m_0, m_1, b) = \{m_0, m_1, h_0, h_1, r_0, r_1\}$$

$$\equiv$$

```
$\mathcal{S}_S(m_0, m_1, \perp)$:
  $h_0, h_1, r_0, r_1 \xleftarrow{\$} G$
  return $\{m_0, m_1, h_0, h_1, r_0, r_1\}$
```

m_0, m_1

Sender

$r_0 \xleftarrow{\$} \mathbb{Z}_q$

$r_1 \xleftarrow{\$} \mathbb{Z}_q$

b

Receiver

$a \xleftarrow{\$} \mathbb{Z}_q$

$h_b \leftarrow g^a$

$h_{1-b} \xleftarrow{\$} G$

h_0, h_1

g^{r_0} g^{r_1}

$h_0^{r_0} \cdot m_0$ $h_1^{r_1} \cdot m_1$

$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a}$$

$$\text{View}_R^{\text{OT}}(m_0, m_1, b) = \{b, a, h_{1-b}, g^{r_0}, g^{r_1}, h_b^{r_b} \cdot m_b, h_{1-b}^{r_{1-b}} \cdot m_{1-b}\}$$

```
$\mathcal{S}_R(b, m_b)$:
    $r_0, r_1, a, k, s \xleftarrow{\$} \mathbb{Z}_q$
    return $\{b, a, g^k, g^{r_0}, g^{r_1}, g^{a \cdot r_b} \cdot m_b, g^s\}$
```

m_0, m_1

Sender

$r_0 \xleftarrow{\$} \mathbb{Z}_q$

$r_1 \xleftarrow{\$} \mathbb{Z}_q$

b

$a \xleftarrow{\$} \mathbb{Z}_q$

$h_b \leftarrow g^a$

$h_{1-b} \xleftarrow{\$} G$

Receiver

h_0, h_1

g^{r_0} g^{r_1}

$h_0^{r_0} \cdot m_0$ $h_1^{r_1} \cdot m_1$

$$\frac{h_b^{r_b} \cdot m_b}{\left(g^{r_b}\right)^a}$$

$$\text{View}_R^{\text{OT}}(m_0, m_1, b) = \{b, a, h_{1-b}, g^{r_0}, g^{r_1}, h_b^{r_b} \cdot m_b, h_{1-b}^{r_{1-b}} \cdot m_{1-b}\}$$

```
$\mathcal{S}_R(b, m_b)$:
    $r_0, r_1, a, k, s \xleftarrow{\$} \mathbb{Z}_q$
    return $\{b, a, g^k, g^{r_0}, g^{r_1}, g^{a \cdot r_b} \cdot m_b, g^s\}$
```

$$\text{View}_R^{\text{OT}}(m_0, m_1, b) = \{b, a, h_{1-b}, g^{r_0}, g^{r_1}, h_b^{r_b} \cdot m_b, h_{1-b}^{r_{1-b}} \cdot m_{1-b}\}$$

"DDH implies that $h_{1-b}^{r_{1-b}}$ "looks random", and $h_{1-b}^{r_{1-b}}$ masks message m_{1-b}"

```
$\mathcal{S}_R(b, m_b)$:
    $r_0, r_1, a, k, s \overset{\$}{\leftarrow} \mathbb{Z}_q$
    return $\{b, a, g^k, g^{r_0}, g^{r_1}, g^{a \cdot r_b} \cdot m_b, g^s\}$
```

```
Hyb0($m_0, m_1, b$):
    $a, r_0, r_1 \xleftarrow{\$} \mathbb{Z}_q$
    $h_b \leftarrow g^a$
    $h_{1-b} \xleftarrow{\$} G$
    return $\{b, a, h_{1-b}, g^{r_0}, g^{r_1}, h_b^{r_b} \cdot m_b, h_{1-b}^{r_{1-b}} \cdot m_{1-b}\}$
```

WLOG, suppose $b = 0$

```
Hyb0($m_0, m_1, b$):
    $a, r_0, r_1 \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \overset{\$}{\leftarrow} G$
    return $\{b, a, h_1, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_b, h_1^{r_1} \cdot m_1\}$
```

WLOG, suppose $b = 0$

```
Hyb0($m_0, m_1, b$):
    $a, r_0, r_1 \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \xleftarrow{\$} G$
    return $\{b, a, h_1, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_b, h_1^{r_1} \cdot m_1\}$
```

R’s input

WLOG, suppose $b = 0$

```
Hyb0($m_0, m_1, b$):
    $a, r_0, r_1 \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \xleftarrow{\$} G$
    return $\{b, \underbrace{a, h_1}, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_b, h_1^{r_1} \cdot m_1\}$
```

R’s input

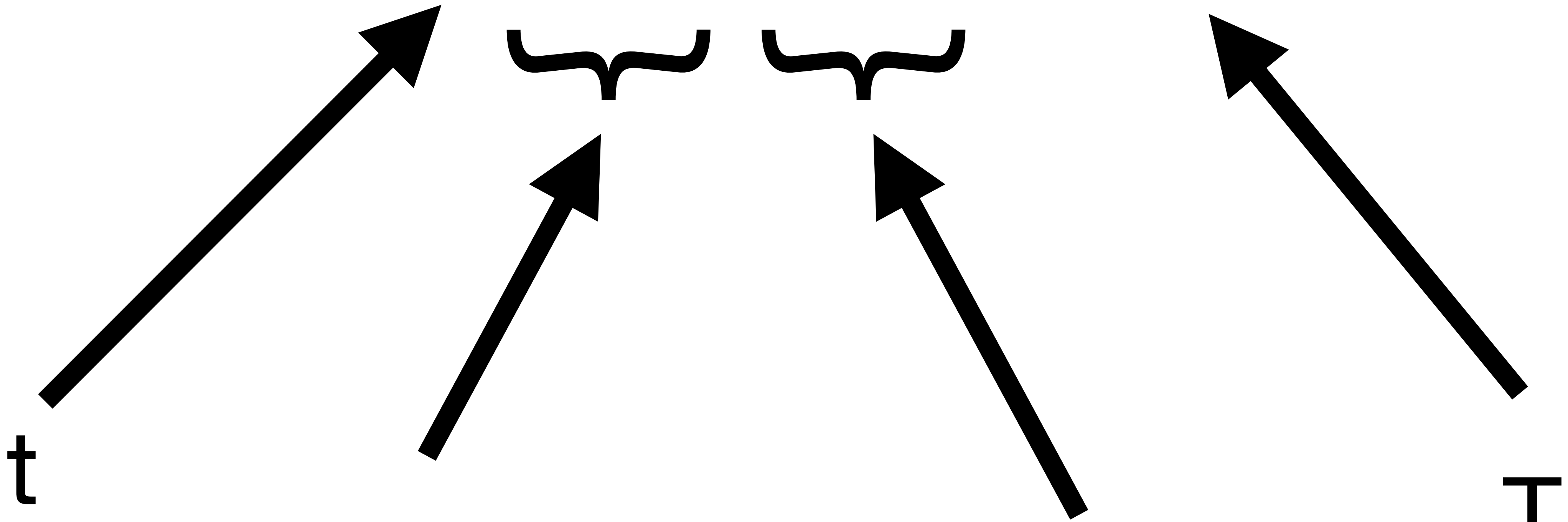
R’s randomness

WLOG, suppose $b = 0$

```
Hyb0($m_0, m_1, b$):
    $a, r_0, r_1 \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \xleftarrow{\$} G$
    return $\{\underset{\text{R's input}}{b}, \underbrace{a,}_{\text{R's randomness}} \underbrace{h_1,}_{\text{S's random messages}} g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_b, h_1^{r_1} \cdot m_1\}$
```

WLOG, suppose $b = 0$

```
Hyb0($m_0, m_1, b$):
    $a, r_0, r_1 \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \xleftarrow{\$} G$
    return $\{b, a, h_1, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_b, h_1^{r_1} \cdot m_1\}$
```



R's input

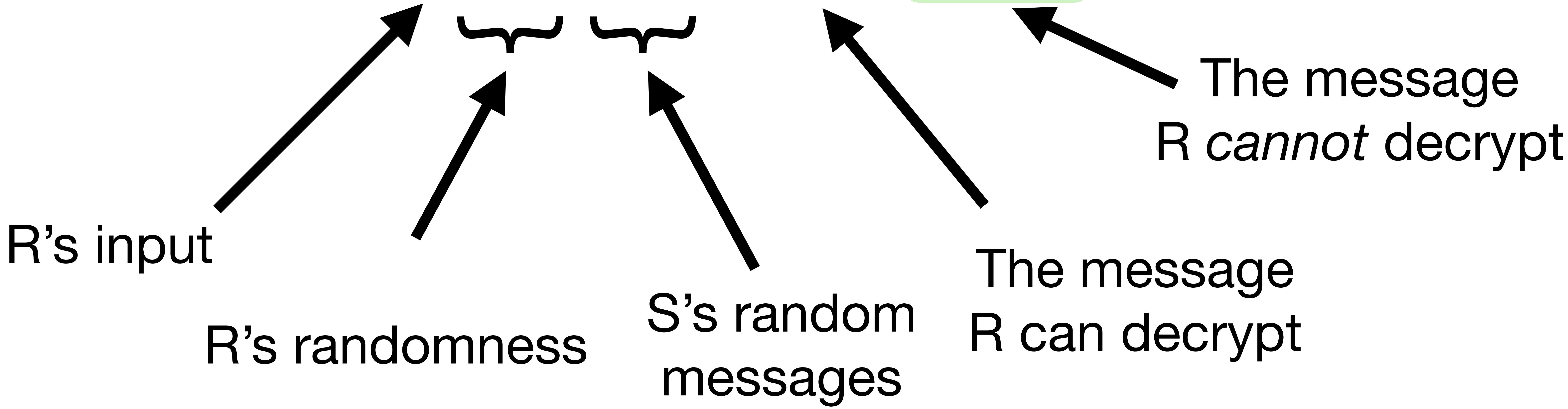
R's randomness

S's random messages

The message R can decrypt

WLOG, suppose $b = 0$

```
Hyb0($m_0, m_1, b$):
    $a, r_0, r_1 \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \xleftarrow{\$} G$
    return $\{b, a, h_1, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_b, h_1^{r_1} \cdot m_1\}$
```



R's input

R's randomness

S's random messages

The message R can decrypt

The message R *cannot* decrypt

```
Hyb0($m_0, m_1, b$):
    $a, r_0, r_1 \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \xleftarrow{\$} G$
    return $\{b, a, h_1, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, h_1^{r_1} \cdot m_1\}$
```

$$=$$

```
Hyb1($m_0, m_1, b$):
    $a, r_0, r_1, k \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    return $\{b, a, h_1, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, h_1^{r_1} \cdot m_1\}$
```

```
Hyb1($m_0, m_1, b$):
    $a, r_0, r_1, k \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    return $\{b, a, h_1, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, h_1^{r_1} \cdot m_1\}$
```

```
Hyb2($m_0, m_1, b$):
    $a, r_0, r_1, k \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    $\text{mask} \leftarrow h_1^{r_1}$
    return $\{b, a, h_1, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

$$=$$

```
Hyb1($m_0, m_1, b$):
    $a, r_0, r_1, k \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    return $\{b, a, h_1, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, h_1^{r_1} \cdot m_1\}$
```

```
Hyb2($m_0, m_1, b$):
    $a, r_0, r_1, k \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    $\text{mask} \leftarrow h_1^{r_1}$
    return $\{b, a, h_1, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

```
Hyb2($m_0, m_1, b$):
    $a, r_0, r_1, k \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    mask $\leftarrow h_1^{r_1}$
    return $\{b, a, h_1, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

$$=$$

```
Hyb3($m_0, m_1, b$):
    $a, r_0, r_1, k \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    $g' \leftarrow g^{r_1}$
    mask $\leftarrow g^{k \cdot r_1}$
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

```
Hyb3($m_0, m_1, b$):
    $a, r_0, r_1, k \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    $g' \leftarrow g^{r_1}$
    $\text{mask} \leftarrow g^{k \cdot r_1}$
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

```
Hyb3($m_0, m_1, b$):
    $a, r_0, r_1, k \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    $g' \leftarrow g^{r_1}$
    $\mathrm{mask} \leftarrow g^{k \cdot r_1}$
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \mathrm{mask} \cdot m_1\}$
```

$$=$$

```
Hyb4($m_0, m_1, b$):
    $a, r_0 \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $\{h_1, g', \mathrm{mask}\} \leftarrow$ Real()
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \mathrm{mask} \cdot m_1\}$
```

```
Real():
    $k, r_1 \overset{\$}{\leftarrow} \mathbb{Z}_q$
    return $\{g^k, g^{r_1}, g^{k \cdot r_1}\}$
```

Decisional Diffie-Hellman Assumption

“It is hard to compute logarithms in certain mathematical sets”

Let G be a cyclic group of order q with generator g

```
Real( ):
    $a \xleftarrow{\$} \mathbb{Z}_q$
    $b \xleftarrow{\$} \mathbb{Z}_q$
    return $\{g^a, g^b, g^{a \cdot b}\}$
```

$$\overset{c}{=}$$

```
Ideal( ):
    $a \xleftarrow{\$} \mathbb{Z}_q$
    $b \xleftarrow{\$} \mathbb{Z}_q$
    $c \xleftarrow{\$} \mathbb{Z}_q$
    return $\{g^a, g^b, g^c\}$
```

```
Hyb4($m_0, m_1, b$):
    $a, r_0 \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $\{h_1, g', \mathrm{mask}\} \leftarrow$ Real()
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \mathrm{mask} \cdot m_1\}$
```

```
Real():
    $k, r_1 \overset{\$}{\leftarrow} \mathbb{Z}_q$
    return $\{g^k, g^{r_1}, g^{k \cdot r_1}\}$
```

```
Hyb4($m_0, m_1, b$):
    $a, r_0 \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $\{h_1, g', \text{mask}\} \leftarrow$ Real()
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

```
Real():
    $k, r_1 \xleftarrow{\$} \mathbb{Z}_q$
    return $\{g^k, g^{r_1}, g^{k \cdot r_1}\}$
```

$\overset{c}{=}$ [By DDH]

```
Hyb5($m_0, m_1, b$):
    $a, r_0 \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $\{h_1, g', \text{mask}\} \leftarrow$ Ideal()
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

```
Ideal():
    $k, r_1, s \xleftarrow{\$} \mathbb{Z}_q$
    return $\{g^k, g^{r_1}, g^s\}$
```

```
Hyb5($m_0, m_1, b$):
    $a, r_0 \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $\{h_1, g', \text{mask}\} \leftarrow$ Ideal()
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

```
Ideal():
    $k, r_1, s \overset{\$}{\leftarrow} \mathbb{Z}_q$
    return $\{g^k, g^{r_1}, g^s\}$
```

```
Hyb5($m_0, m_1, b$):
    $a, r_0 \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $\{h_1, g', \text{mask}\} \leftarrow$ Ideal()
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

```
Ideal():
    $k, r_1, s \xleftarrow{\$} \mathbb{Z}_q$
    return $\{g^k, g^{r_1}, g^s\}$
```

$$=$$

```
Hyb5($m_0, m_1, b$):
    $a, r_0, r_1, k, s \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    $g' \leftarrow g^{r_1}$
    $\text{mask} \leftarrow g^s$
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

```
Hyb5($m_0, m_1, b$):
    $a, r_0, r_1, k, s \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    $g' \leftarrow g^{r_1}$
    $\text{mask} \leftarrow g^s$
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

```
Hyb6($m_0, m_1, b$):
    $a, r_0, r_1, k, s \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    return $\{b, a, g^k, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, g^s \cdot m_1\}$
```

$$=$$

```
Hyb5($m_0, m_1, b$):
    $a, r_0, r_1, k, s \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    $h_1 \leftarrow g^k$
    $g' \leftarrow g^{r_1}$
    $\text{mask} \leftarrow g^s$
    return $\{b, a, h_1, g^{r_0}, g', h_0^{r_0} \cdot m_0, \text{mask} \cdot m_1\}$
```

```
Hyb6($m_0, m_1, b$):
    $a, r_0, r_1, k, s \overset{\$}{\leftarrow} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    return $\{b, a, g^k, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, g^s \cdot m_1\}$
```

```
Hyb6($m_0, m_1, b$):
    $a, r_0, r_1, k, s \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    return $\{b, a, g^k, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, g^s \cdot m_1\}$
```

$=$ [By one-time-pad]

```
Hyb7($m_0, m_1, b$):
    $a, r_0, r_1, k, s \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    return $\{b, a, g^k, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, g^s\}$
```

```
Hyb7($m_0, m_1, b$):
    $a, r_0, r_1, k, s \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    return $\{b, a, g^k, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, g^s\}$
```

```
$\mathcal{S}_R(b, m_0)$:
    $a, r_0, r_1, k, s \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    return $\{b, a, g^k, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, g^s\}$
```

$$=$$

```
Hyb7($m_0, m_1, b$):
    $a, r_0, r_1, k, s \xleftarrow{\$} \mathbb{Z}_q$
    $h_0 \leftarrow g^a$
    return $\{b, a, g^k, g^{r_0}, g^{r_1}, h_0^{r_0} \cdot m_0, g^s\}$
```

Today's objectives

Review semi-honest security

Introduce **oblivious transfer (OT)**

Build OT from DDH

See an end-to-end security proof