Homework 2 Review

CS 598 DH

Setting

Semi-honest Security

Malicious Security

Zero Knowledge

General-Purpose Tools

GMW Protocol

- Multi-party
- Multi-round

Garbled Circuit

- Constant Round
- Two Party

Primitives

Oblivious Transfer

Pseudorandom functions/encryption

Commitments

ORAM

Setting

Semi-honest Security

Malicious Security

Zero Knowledge

General-Purpose Tools

GMW Protocol

- Multi-party
- Multi-round

Garbled Circuit

- Constant Round
- Two Party

Primitives

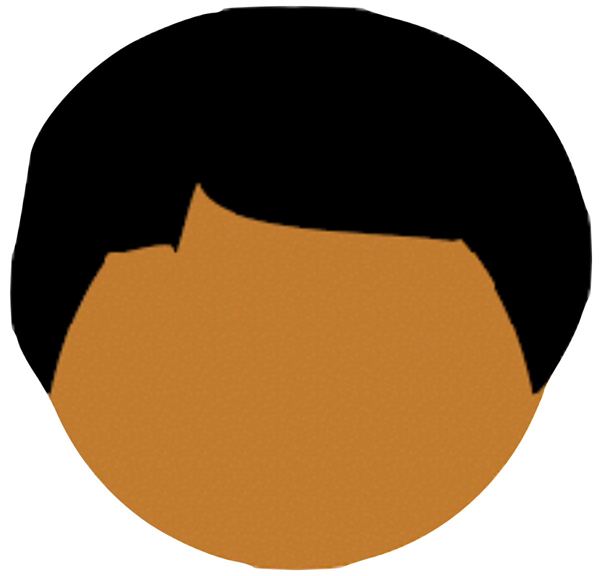
Oblivious Transfer

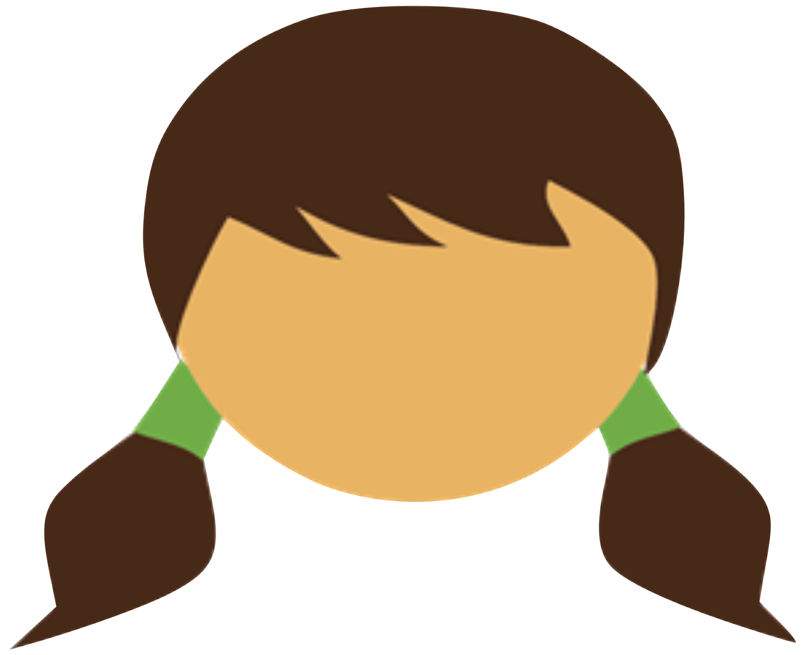
Pseudorandom functions/encryption

Commitments

ORAM

$$f(\cdot) = \{\ r \mid r \xleftarrow{\$} \{0,1\}\ \}$$

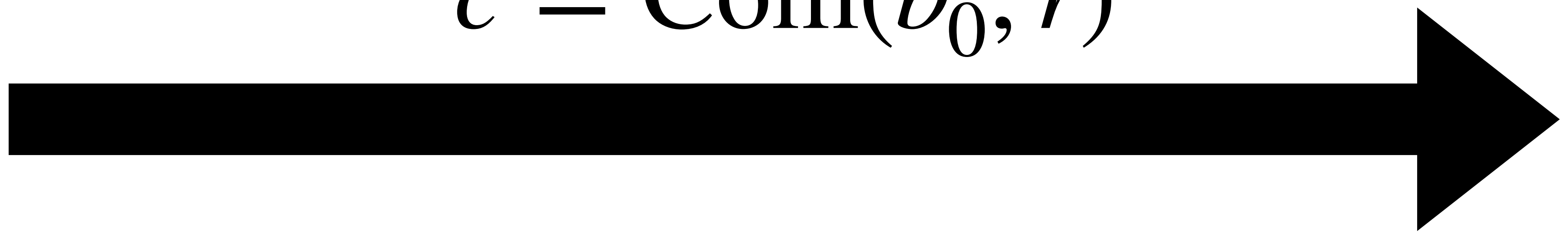




$b_0 \xleftarrow{\$} \{0,1\}$

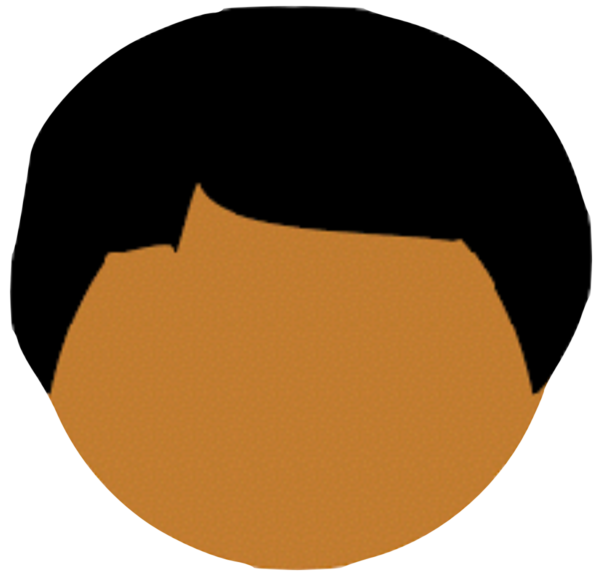
$r \xleftarrow{\$} \{0,1\}^\lambda$

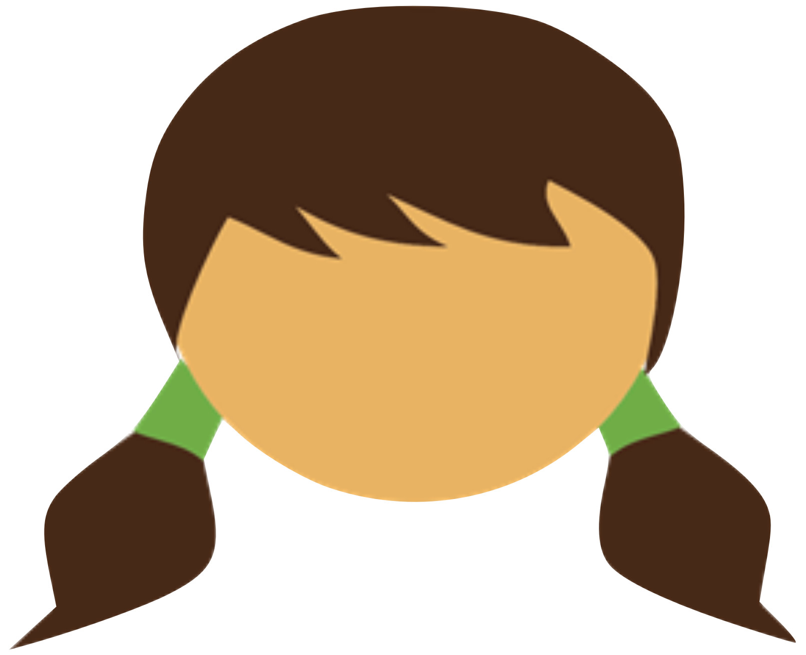
$c = \mathrm{Com}(b_0; r)$



$b_1 \xleftarrow{\$} \{0,1\}$

$$f(\cdot) = \{\ r \mid r \xleftarrow{\$} \{0,1\}\ \}$$

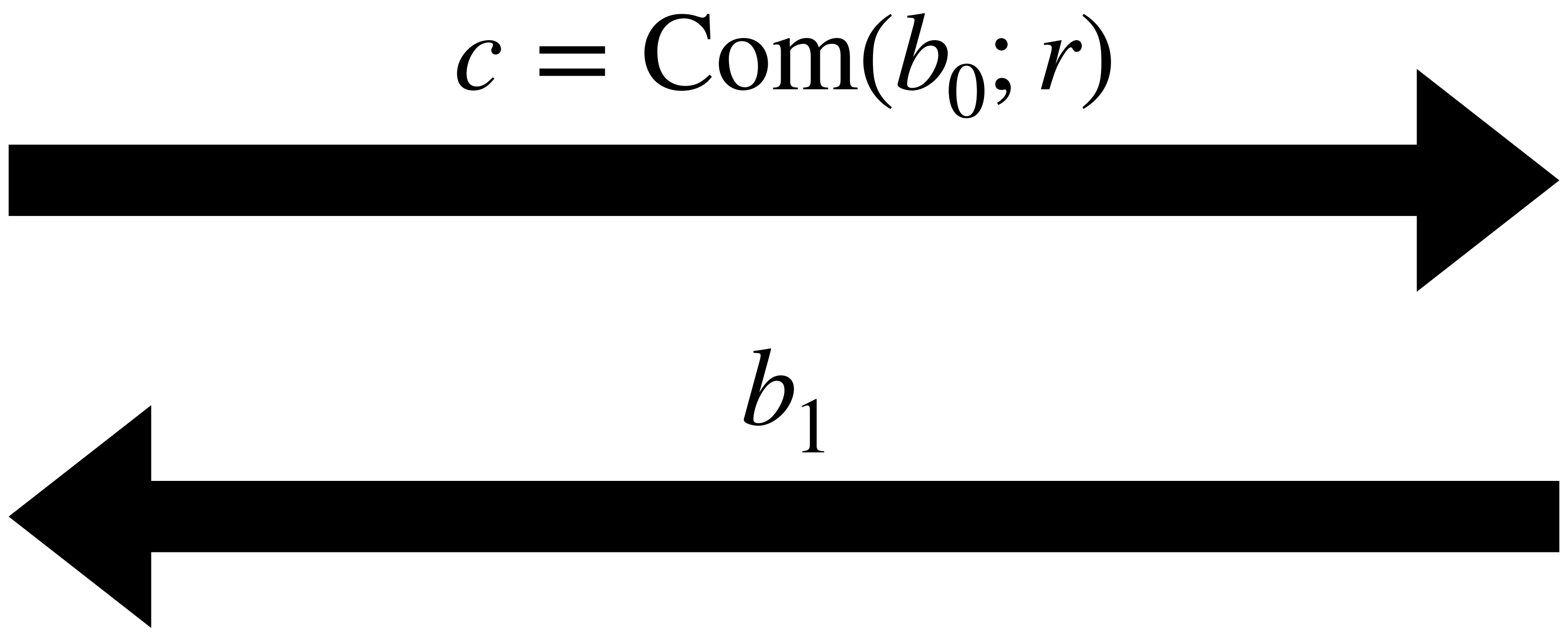




$b_0 \xleftarrow{\$} \{0,1\}$

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

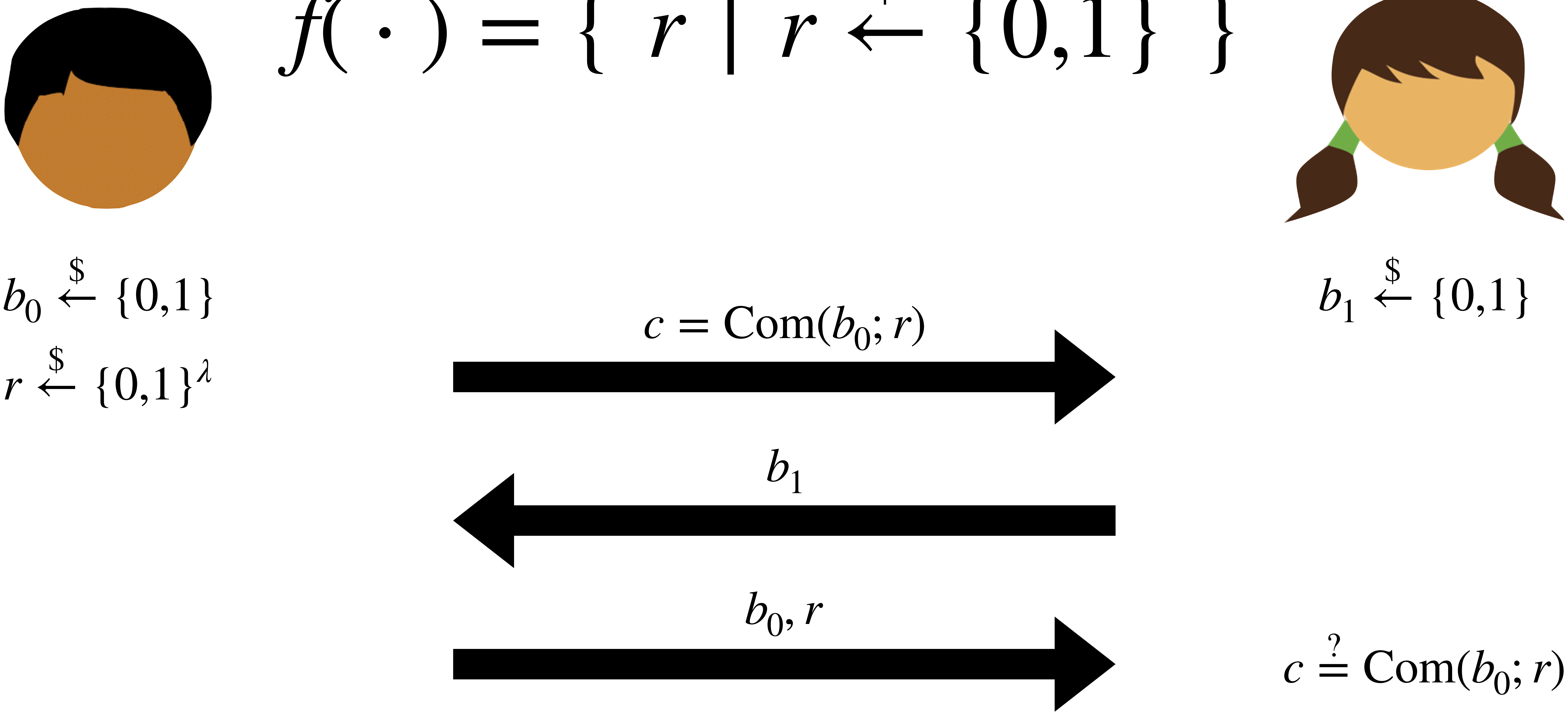
$b_1 \xleftarrow{\$} \{0,1\}$



$c = \mathrm{Com}(b_0; r)$

b_1

$$f(\cdot) = \{\ r \mid r \overset{\$}{\leftarrow} \{0,1\}\ \}$$



$b_0 \overset{\$}{\leftarrow} \{0,1\}$

$r \overset{\$}{\leftarrow} \{0,1\}^{\lambda}$

$b_1 \overset{\$}{\leftarrow} \{0,1\}$

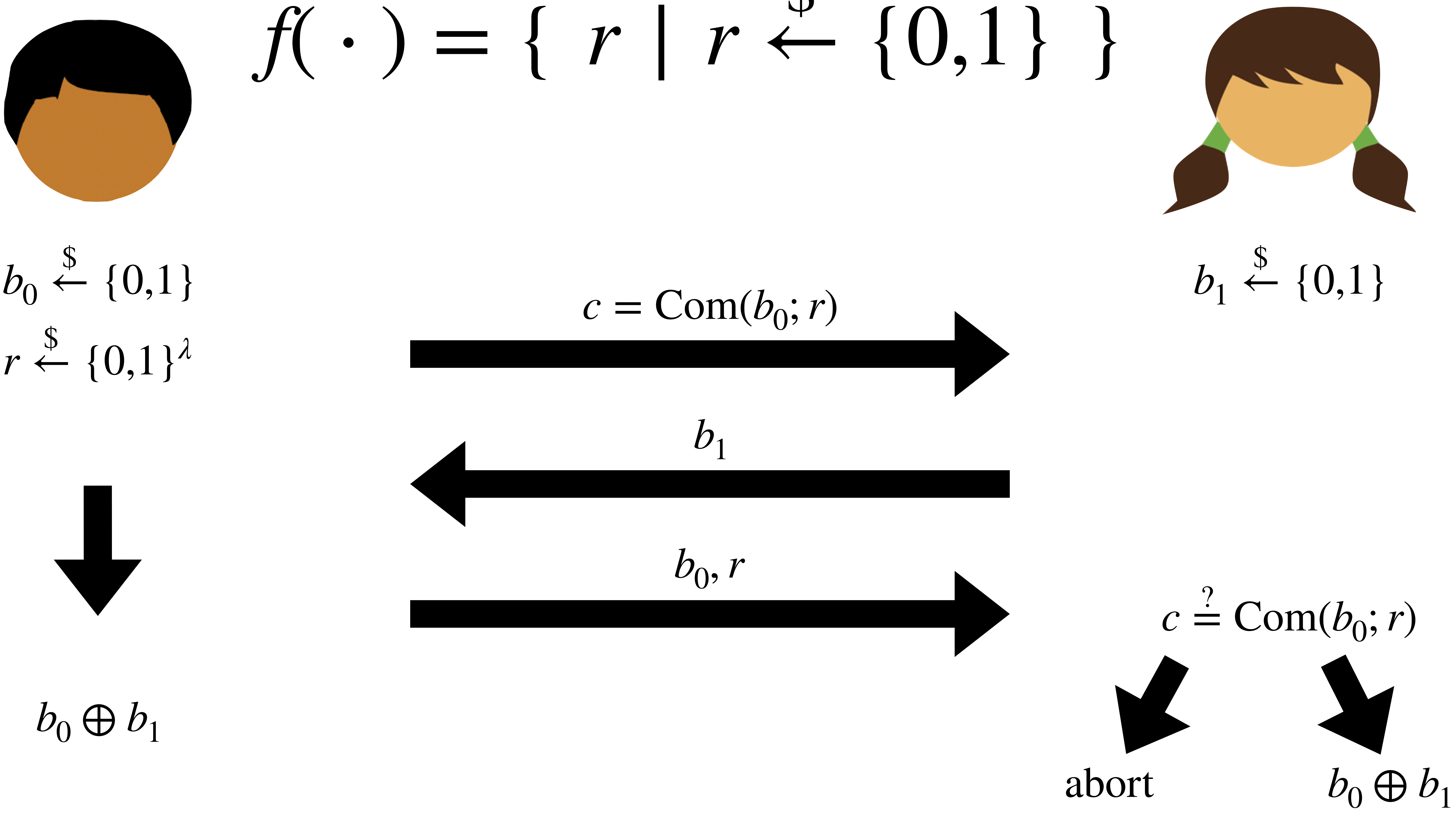
$c = \mathrm{Com}(b_0; r)$

b_1

b_0, r

$c \overset{?}{=} \mathrm{Com}(b_0; r)$

$$f(\cdot) = \{ \, r \mid r \xleftarrow{\$} \{0,1\} \, \}$$



$b_0 \xleftarrow{\$} \{0,1\}$

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

$c = \mathrm{Com}(b_0; r)$

$b_1 \xleftarrow{\$} \{0,1\}$

b_1

b_0, r

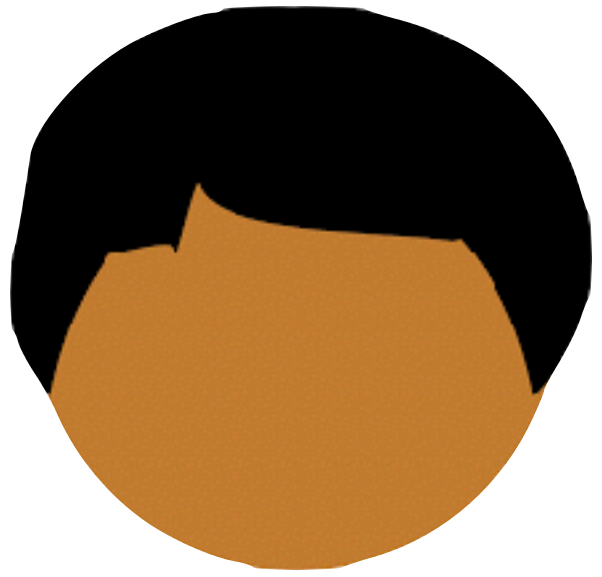
$c \overset{?}{=} \mathrm{Com}(b_0; r)$

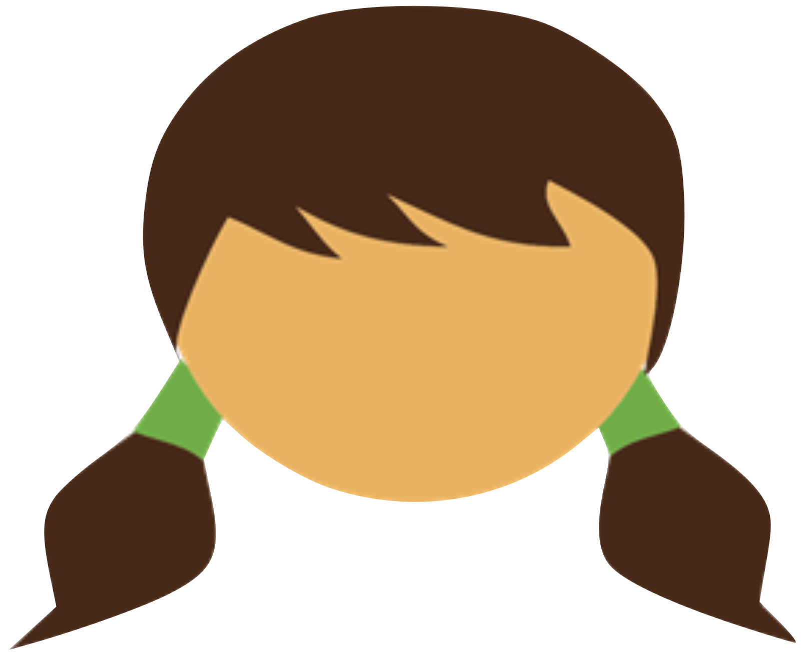
$b_0 \oplus b_1$

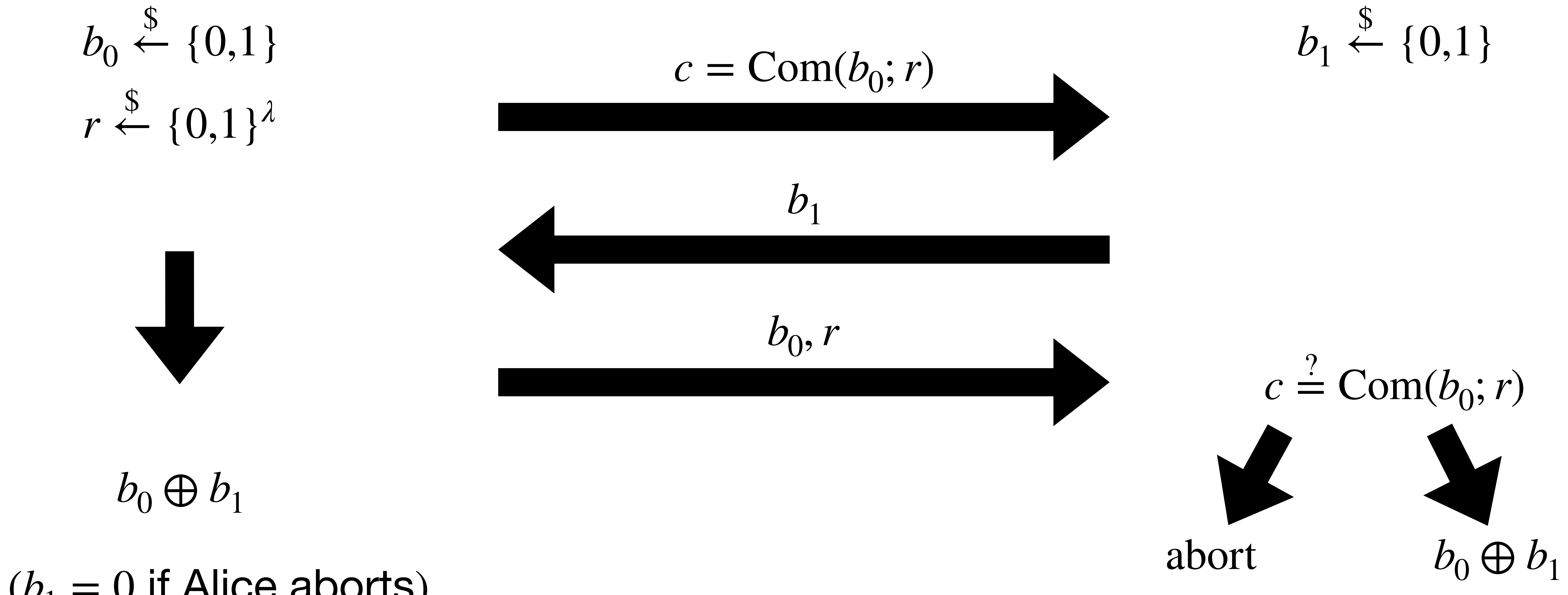
abort

$b_0 \oplus b_1$

$$f(\cdot) = \{\ r \mid r \overset{\$}{\leftarrow} \{0,1\}\ \}$$







$b_0 \overset{\$}{\leftarrow} \{0,1\}$

$r \overset{\$}{\leftarrow} \{0,1\}^\lambda$

$c = \mathrm{Com}(b_0; r)$

b_1

b_0, r

$b_0 \oplus b_1$

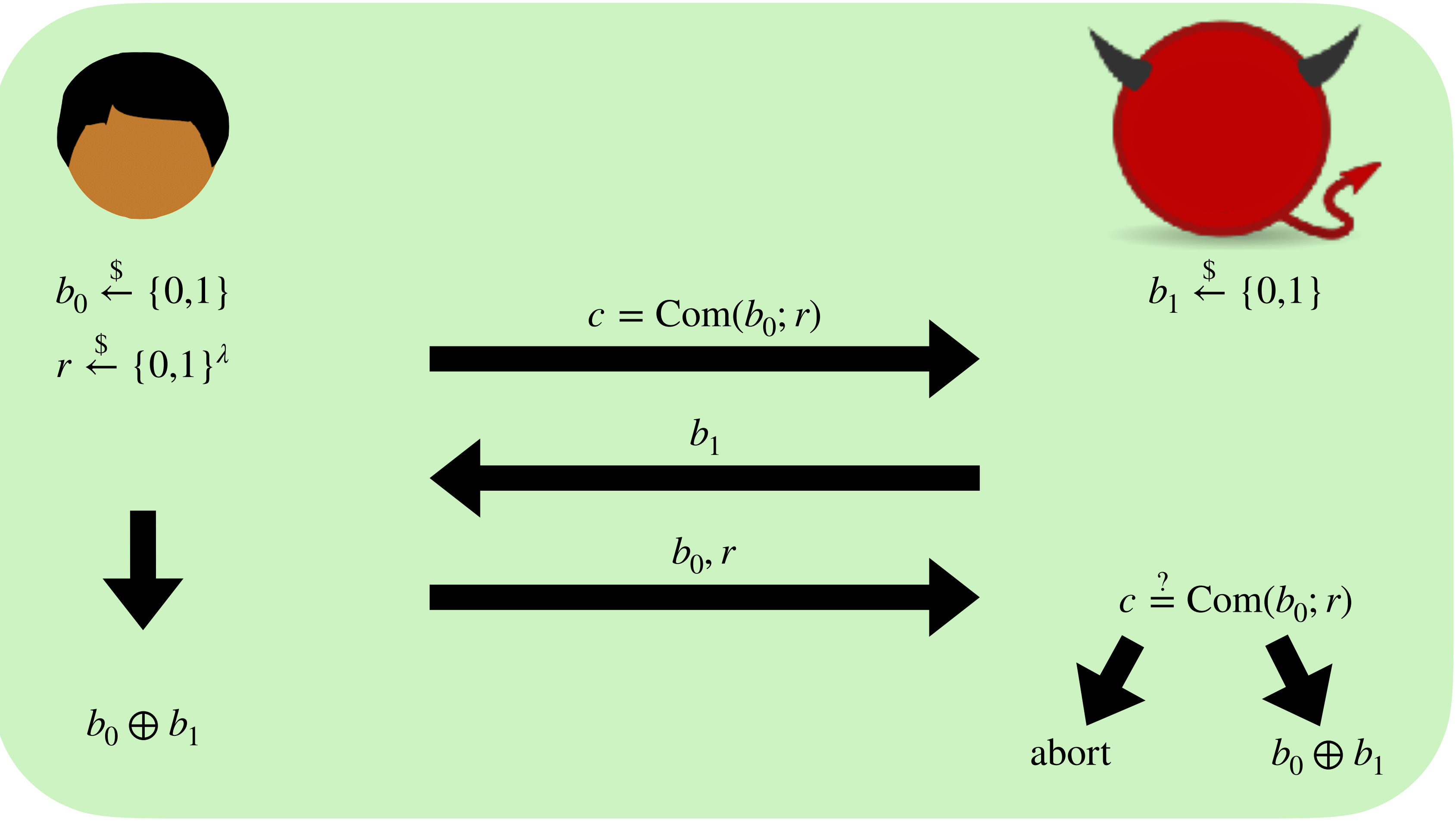
($b_1 = 0$ if Alice aborts)

$b_1 \overset{\$}{\leftarrow} \{0,1\}$

$c \overset{?}{=} \mathrm{Com}(b_0; r)$

abort

$b_0 \oplus b_1$



$b_0 \xleftarrow{\$} \{0,1\}$

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

$c = \mathrm{Com}(b_0; r)$

$b_1 \xleftarrow{\$} \{0,1\}$

b_1

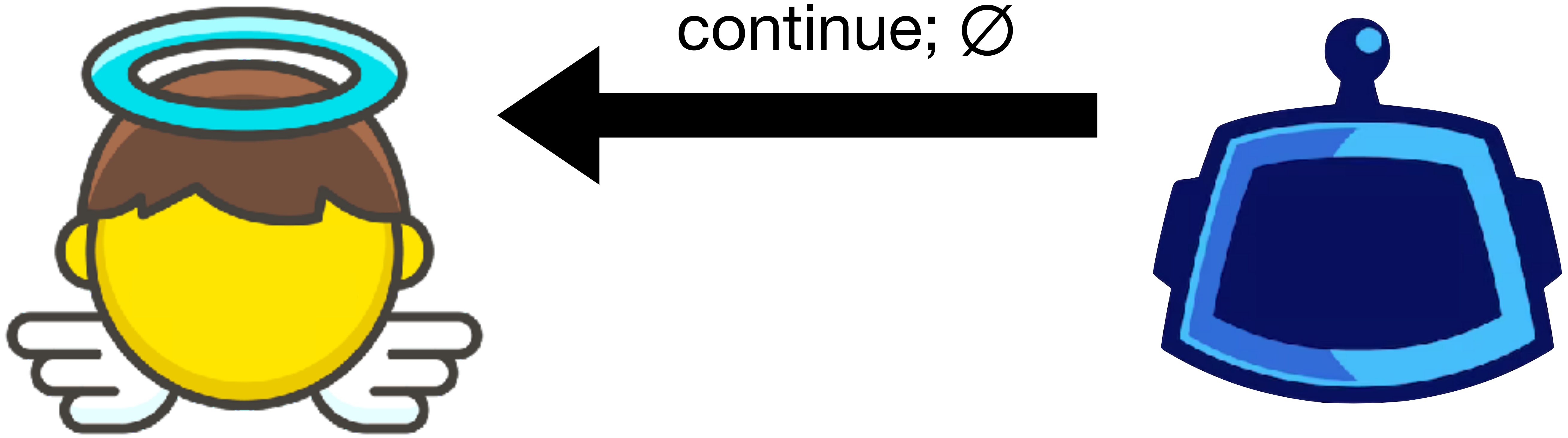
b_0, r

$c \overset{?}{=} \mathrm{Com}(b_0; r)$

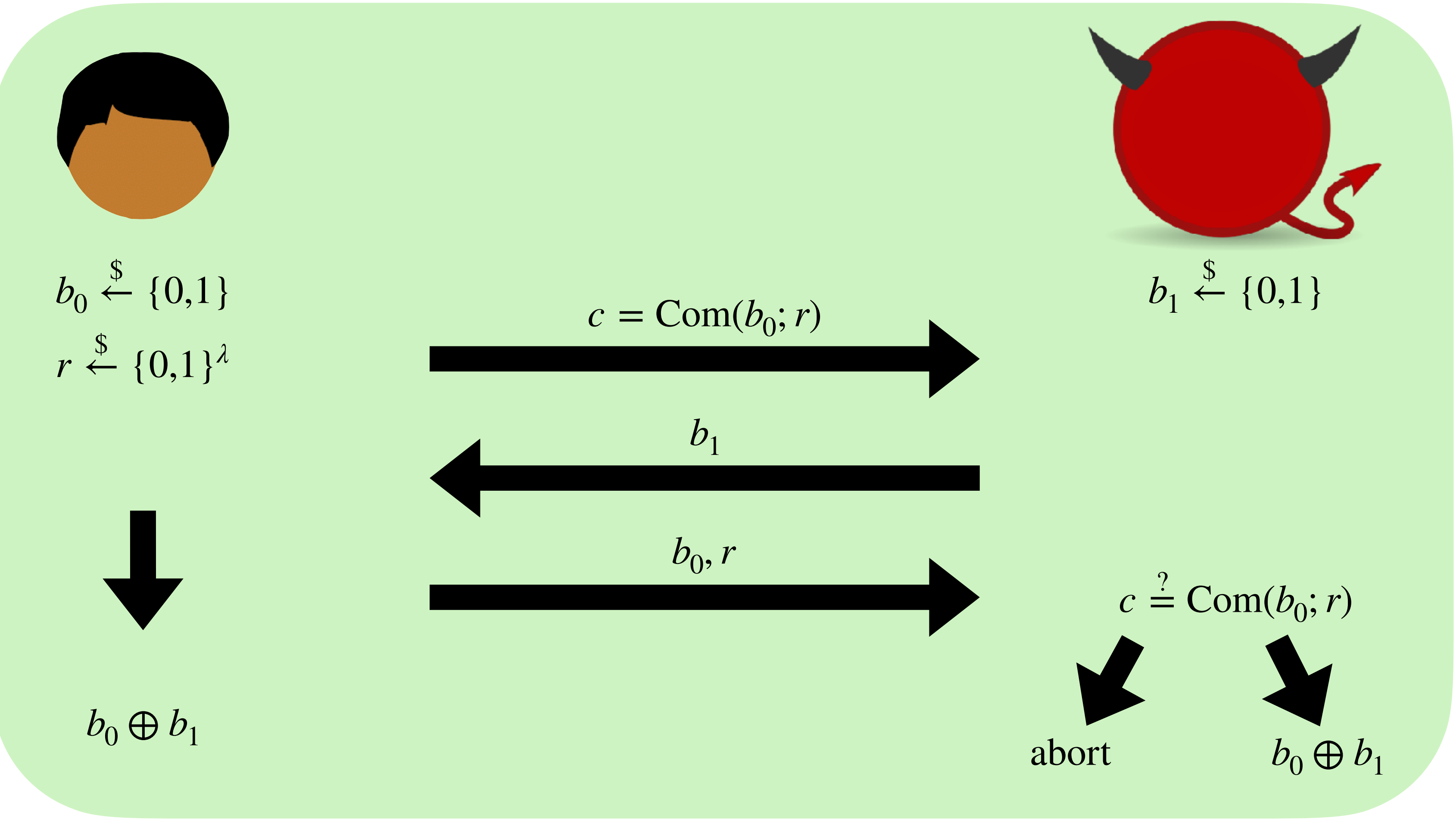
$b_0 \oplus b_1$

abort

$b_0 \oplus b_1$



continue; ∅



$b_0 \xleftarrow{\$} \{0,1\}$

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

$c = \mathrm{Com}(b_0; r)$

$b_1 \xleftarrow{\$} \{0,1\}$

b_1

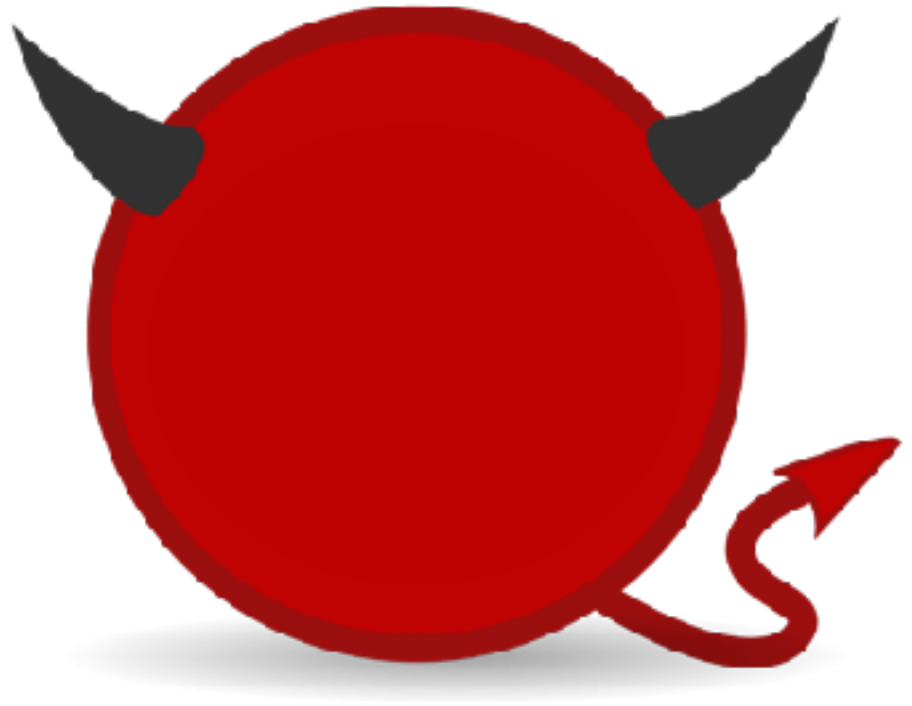
b_0, r

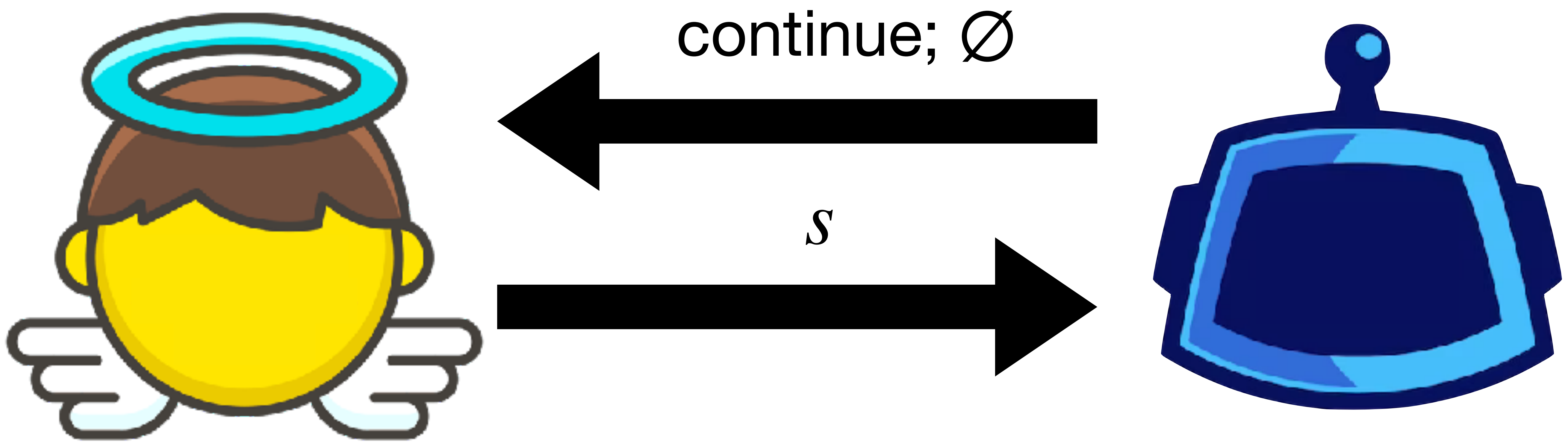
$c \stackrel{?}{=} \mathrm{Com}(b_0; r)$

$b_0 \oplus b_1$

abort

$b_0 \oplus b_1$

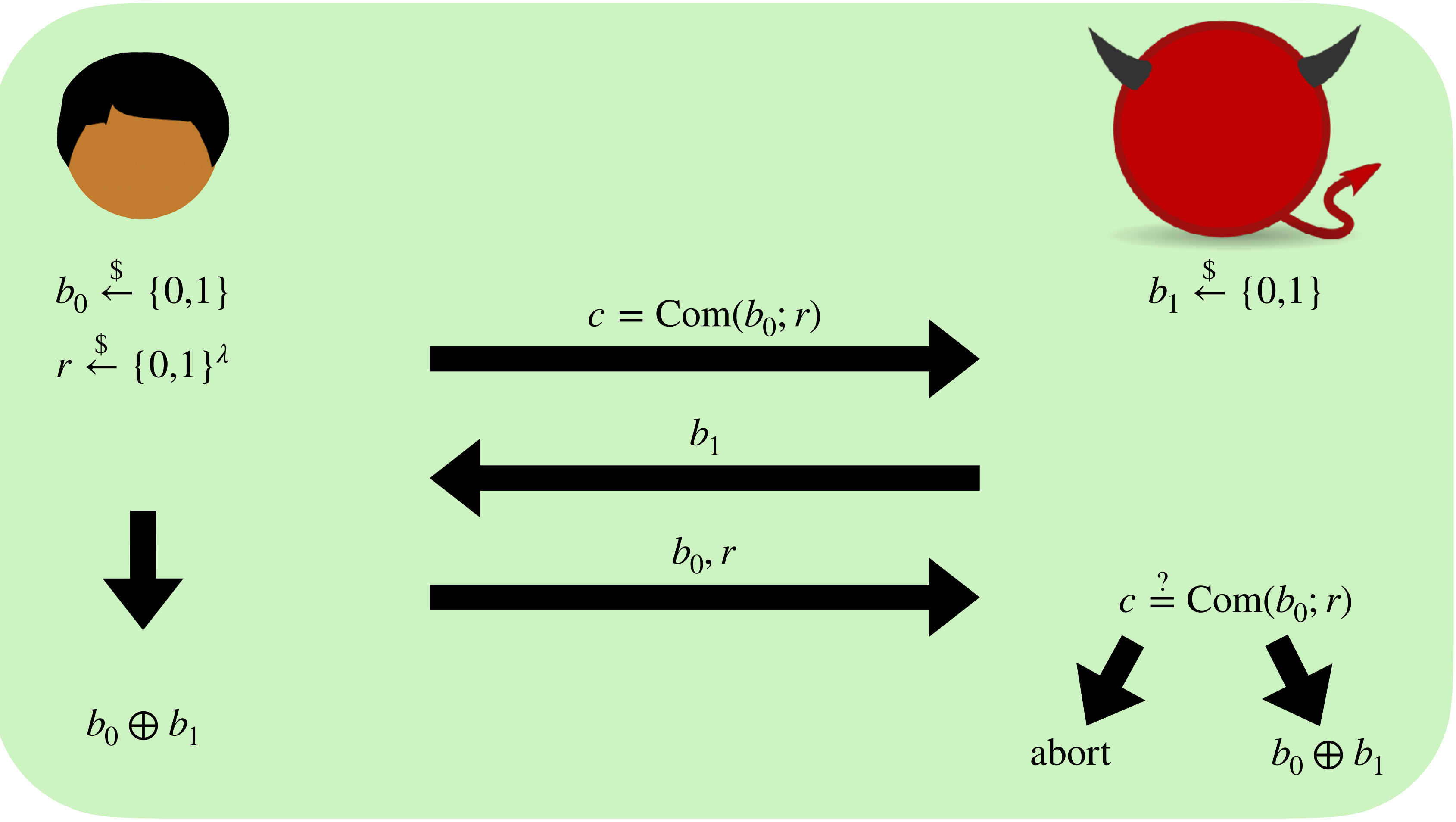




continue; ∅

s

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



$b_0 \xleftarrow{\$} \{0,1\}$

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

$c = \mathrm{Com}(b_0; r)$

$b_1 \xleftarrow{\$} \{0,1\}$

b_1

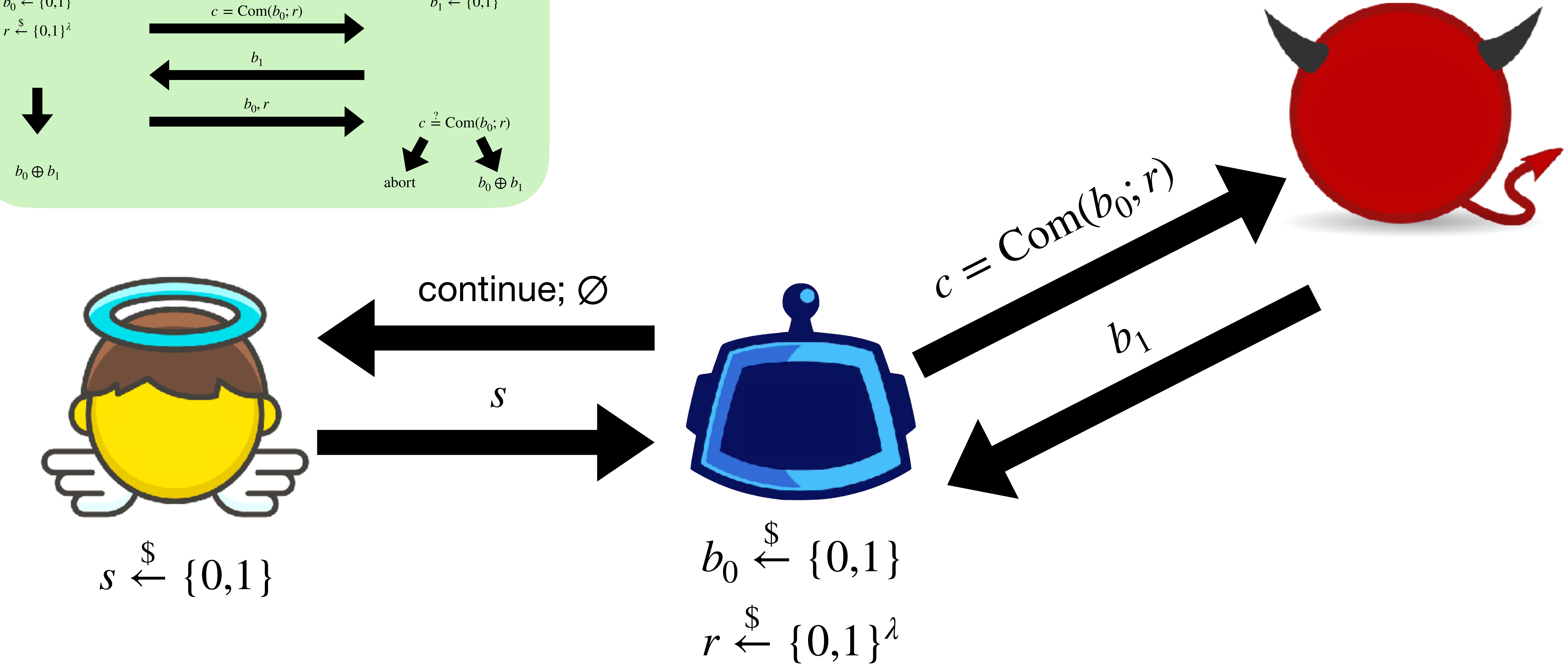
b_0, r

$c \stackrel{?}{=} \mathrm{Com}(b_0; r)$

$b_0 \oplus b_1$

abort

$b_0 \oplus b_1$



continue; ∅

s

$c = \mathrm{Com}(b_0; r)$

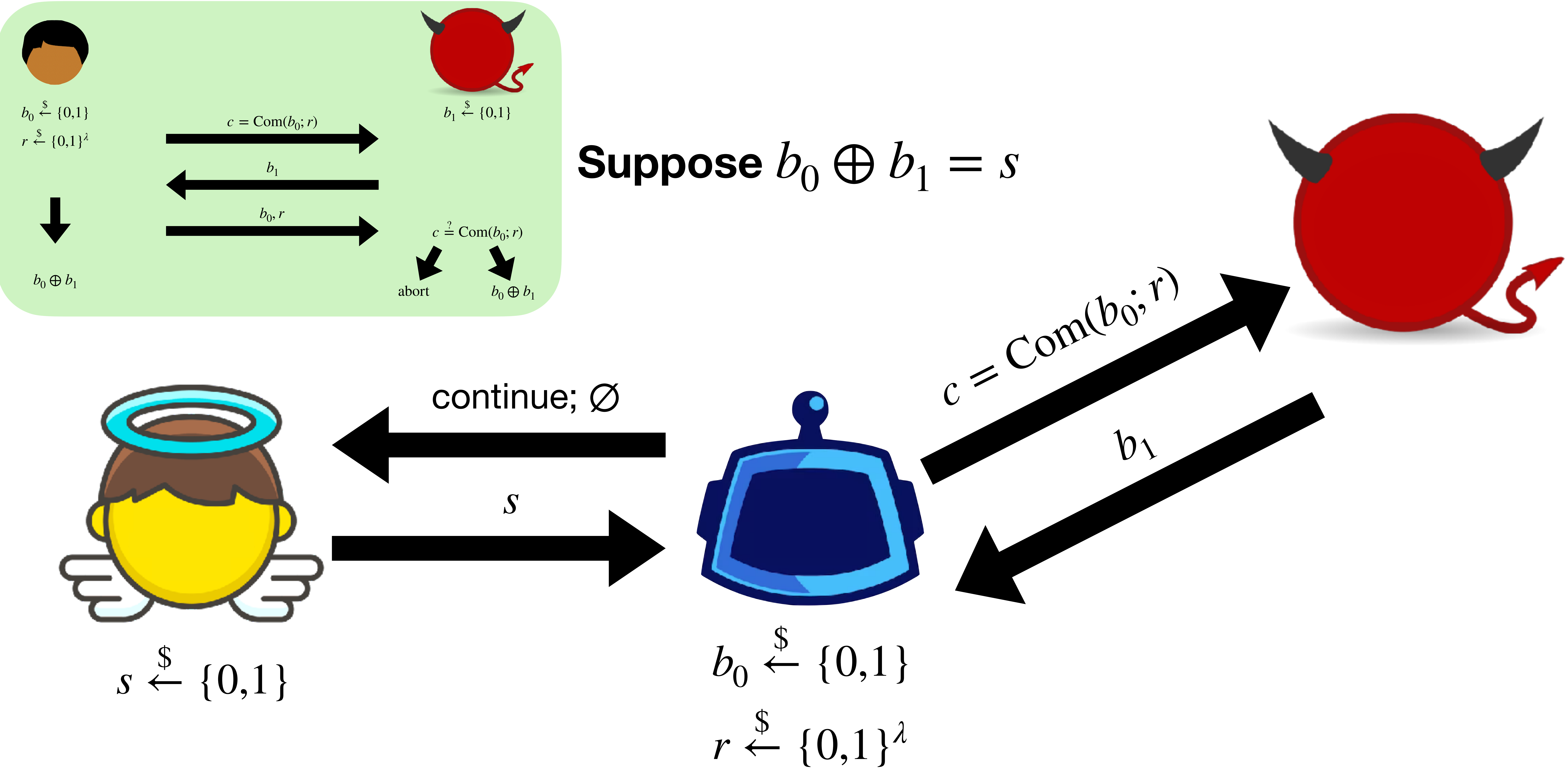
b_1

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

$b_0 \xleftarrow{\$} \{0,1\}$

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

Suppose $b_0 \oplus b_1 = s$



$b_0 \xleftarrow{\$} \{0,1\}$

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

$c = \mathrm{Com}(b_0; r)$

$b_1 \xleftarrow{\$} \{0,1\}$

b_1

b_0, r

$c \overset{?}{=} \mathrm{Com}(b_0; r)$

$b_0 \oplus b_1$

abort

$b_0 \oplus b_1$

continue; ∅

s

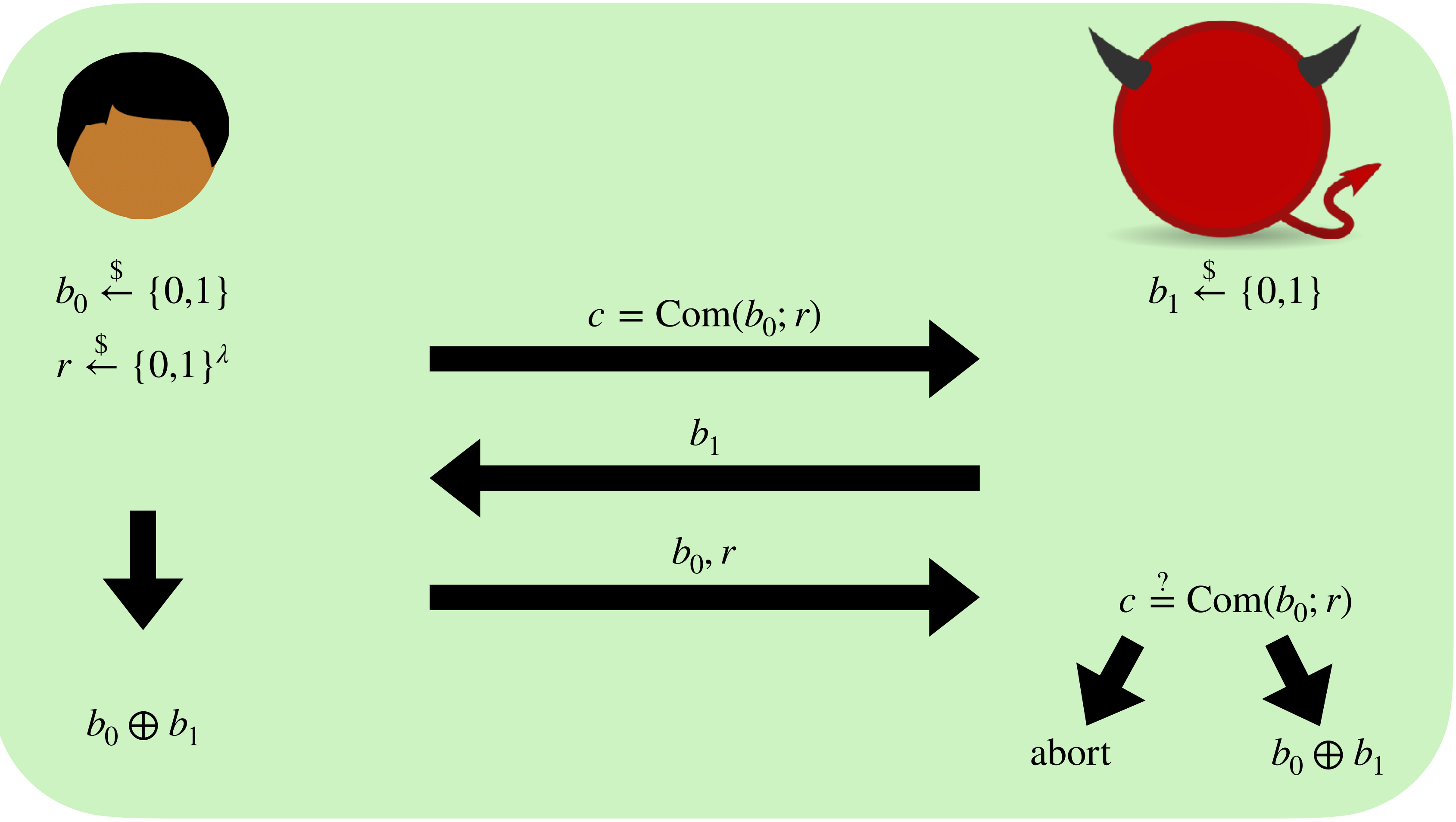
$c = \mathrm{Com}(b_0; r)$

b_1

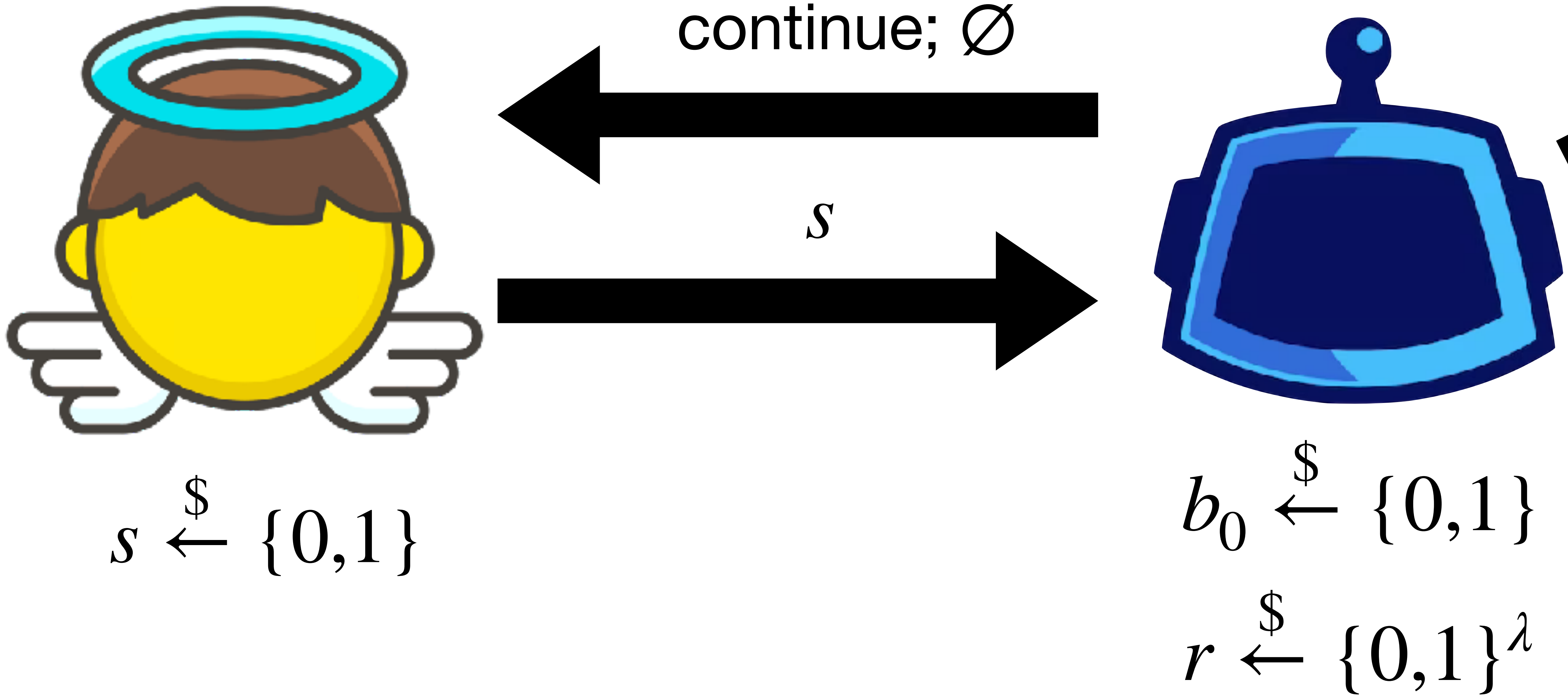
$s \xleftarrow{\$} \{0,1\}$

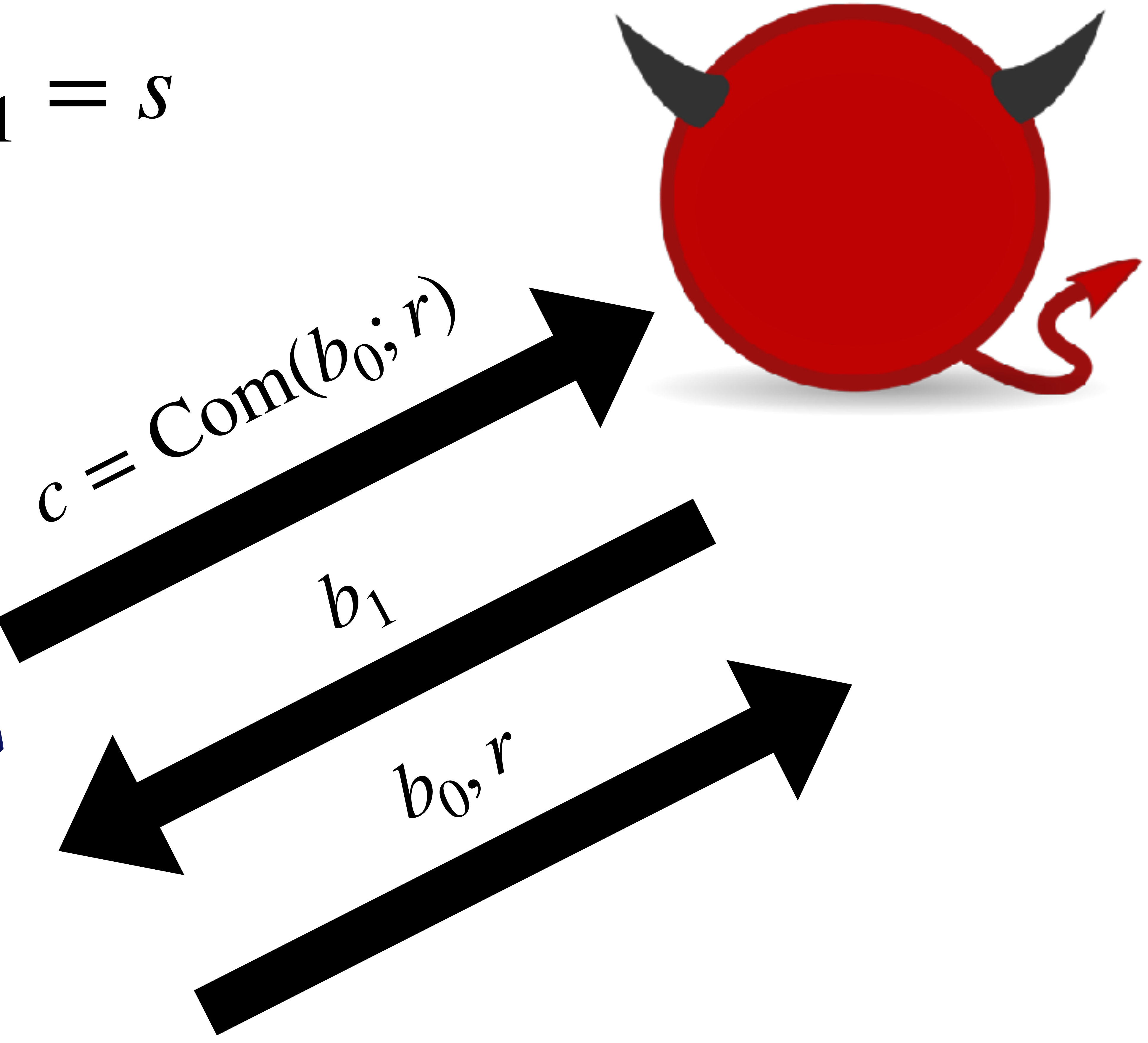
$b_0 \xleftarrow{\$} \{0,1\}$

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

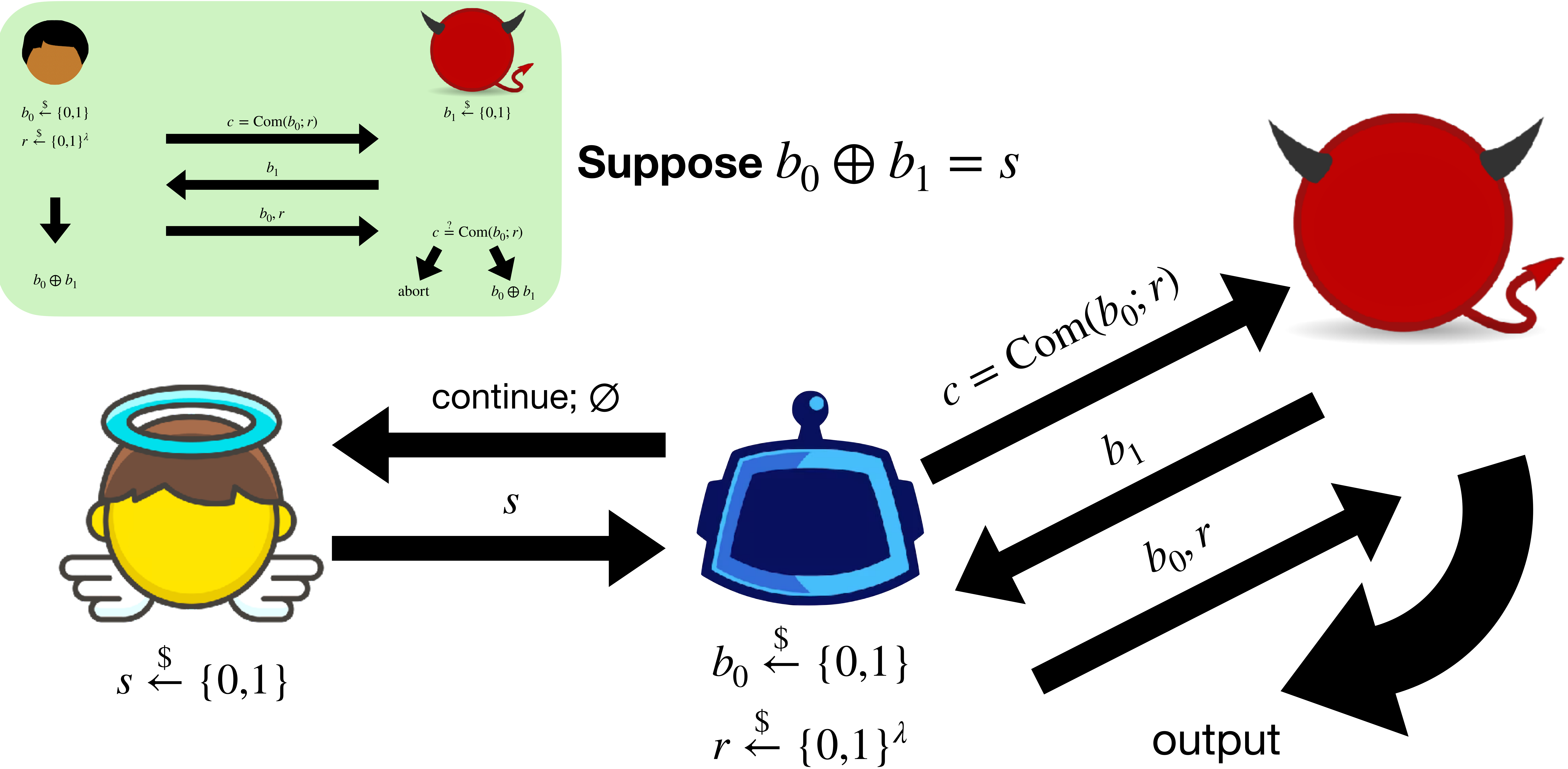

$b_0 \xleftarrow{\$} \{0,1\}$
$r \xleftarrow{\$} \{0,1\}^\lambda$
$b_1 \xleftarrow{\$} \{0,1\}$
$c = \mathrm{Com}(b_0; r)$
b_1
b_0, r
$c \overset{?}{=} \mathrm{Com}(b_0; r)$
$b_0 \oplus b_1$
abort
$b_0 \oplus b_1$

Suppose $b_0 \oplus b_1 = s$

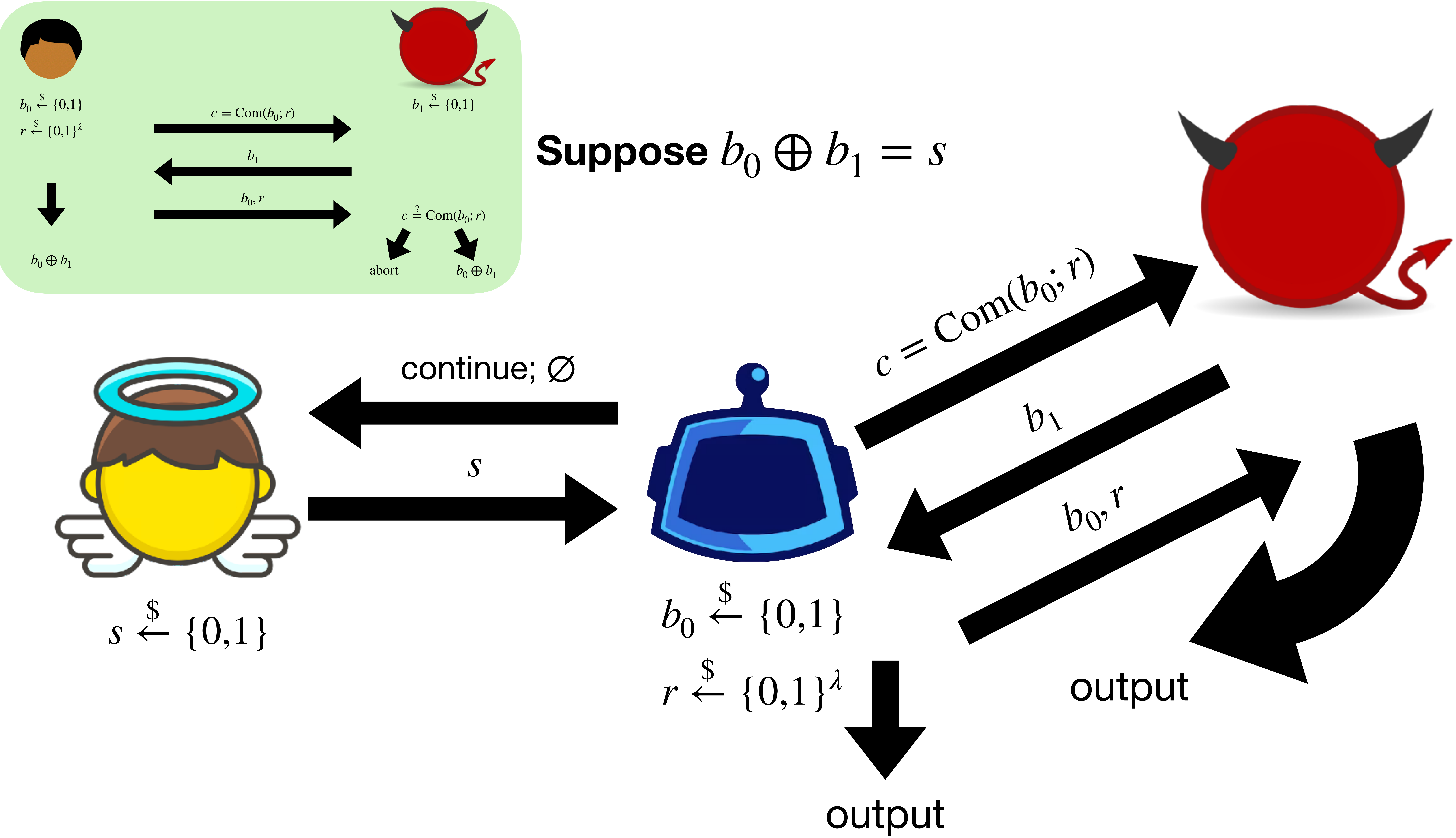

continue; $\varnothing$
s
$s \xleftarrow{\$} \{0,1\}$
$b_0 \xleftarrow{\$} \{0,1\}$
$r \xleftarrow{\$} \{0,1\}^\lambda$



Suppose $b_0 \oplus b_1 = s$


$b_0 \xleftarrow{\$} \{0,1\}$
$r \xleftarrow{\$} \{0,1\}^\lambda$
$c = \mathrm{Com}(b_0; r)$
$b_1 \xleftarrow{\$} \{0,1\}$
b_1
b_0, r
$c \overset{?}{=} \mathrm{Com}(b_0; r)$
$b_0 \oplus b_1$
abort
$b_0 \oplus b_1$
continue; ∅
s
$s \xleftarrow{\$} \{0,1\}$
$b_0 \xleftarrow{\$} \{0,1\}$
$r \xleftarrow{\$} \{0,1\}^\lambda$
$c = \mathrm{Com}(b_0; r)$
b_1
b_0, r
output

Suppose $b_0 \oplus b_1 = s$



$b_0 \xleftarrow{\$} \{0,1\}$

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

$c = \mathrm{Com}(b_0; r)$

b_1

b_0, r

$b_0 \oplus b_1$

$b_1 \xleftarrow{\$} \{0,1\}$

$c \overset{?}{=} \mathrm{Com}(b_0; r)$

abort

$b_0 \oplus b_1$

continue; ∅

s

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

$c = \mathrm{Com}(b_0; r)$

b_1

b_0, r

$b_0 \xleftarrow{\$} \{0,1\}$

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

output

output

Suppose $b_0 \oplus b_1 = s$

$b_0 \overset{\$}{\leftarrow} \{0,1\}$

$r \overset{\$}{\leftarrow} \{0,1\}^\lambda$

$c = \mathrm{Com}(b_0; r)$

$b_1 \overset{\$}{\leftarrow} \{0,1\}$

b_1

b_0, r

$c \overset{?}{=} \mathrm{Com}(b_0; r)$

abort

$b_0 \oplus b_1$

$b_0 \oplus b_1$

continue; ∅

s

s

continue

$s \overset{\$}{\leftarrow} \{0,1\}$

s

$b_0 \overset{\$}{\leftarrow} \{0,1\}$

$r \overset{\$}{\leftarrow} \{0,1\}^\lambda$

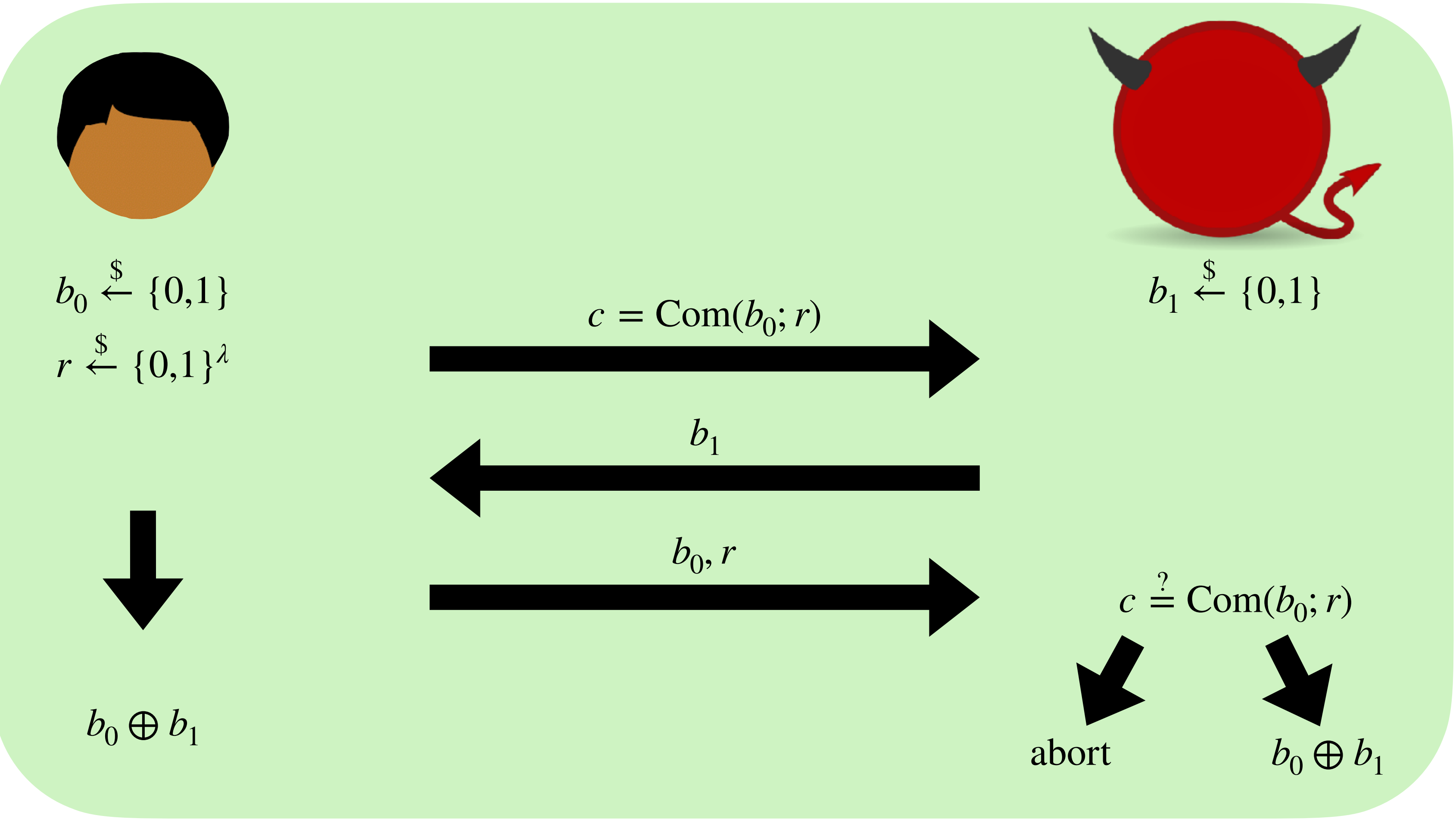
$c = \mathrm{Com}(b_0; r)$

b_1

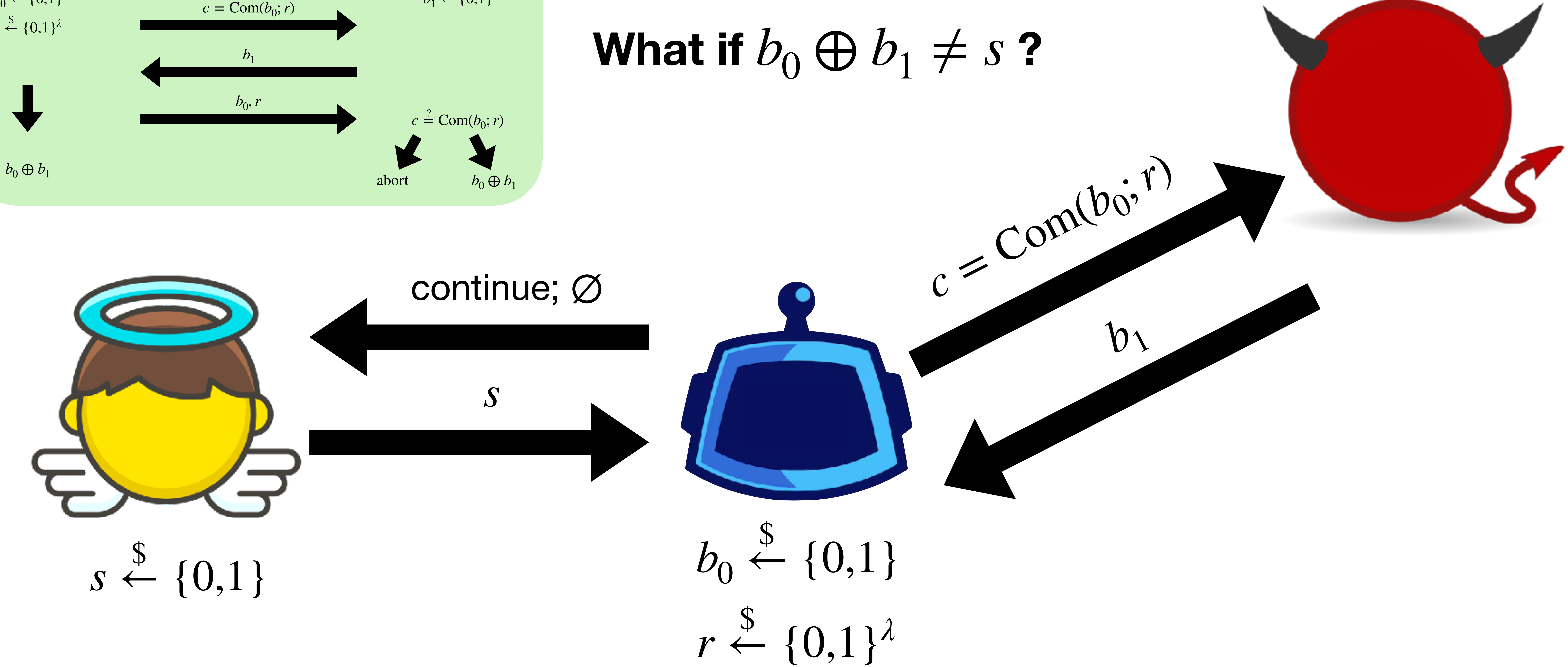
b_0, r

output

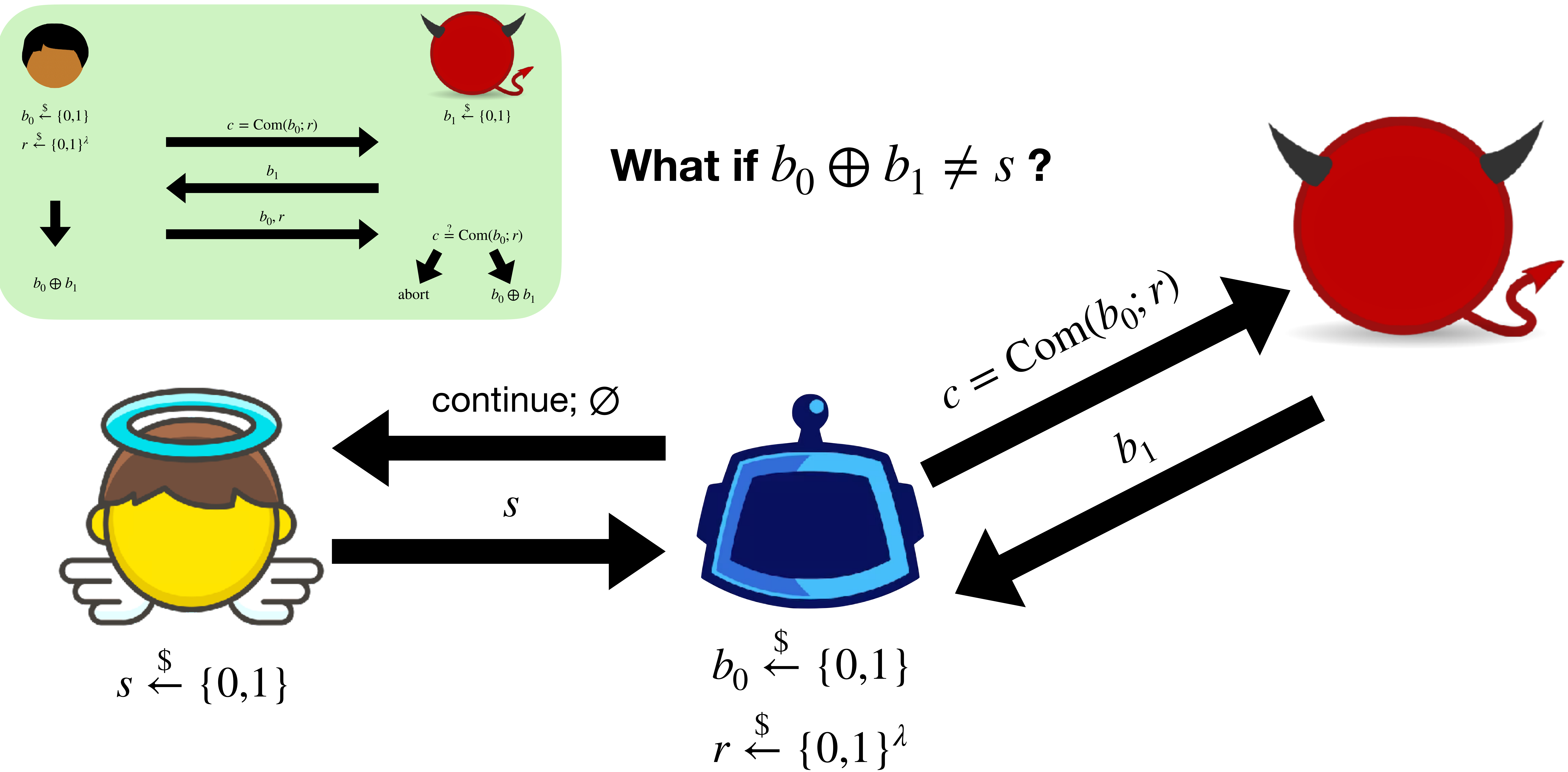
output


$b_0 \xleftarrow{\$} \{0,1\}$
$r \xleftarrow{\$} \{0,1\}^\lambda$
$b_1 \xleftarrow{\$} \{0,1\}$
$c = \mathrm{Com}(b_0; r)$
b_1
b_0, r
$c \overset{?}{=} \mathrm{Com}(b_0; r)$
$b_0 \oplus b_1$
abort
$b_0 \oplus b_1$

What if $b_0 \oplus b_1 \neq s$?


continue; $\varnothing$
s
$c = \mathrm{Com}(b_0; r)$
b_1
$s \xleftarrow{\$} \{0,1\}$
$b_0 \xleftarrow{\$} \{0,1\}$
$r \xleftarrow{\$} \{0,1\}^\lambda$

What if $b_0 \oplus b_1 \neq s$?



$b_0 \overset{\$}{\leftarrow} \{0,1\}$

$r \overset{\$}{\leftarrow} \{0,1\}^\lambda$

$c = \mathrm{Com}(b_0; r)$

$b_1 \overset{\$}{\leftarrow} \{0,1\}$

b_1

b_0, r

$c \overset{?}{=} \mathrm{Com}(b_0; r)$

$b_0 \oplus b_1$

abort

$b_0 \oplus b_1$

continue; $\varnothing$

s

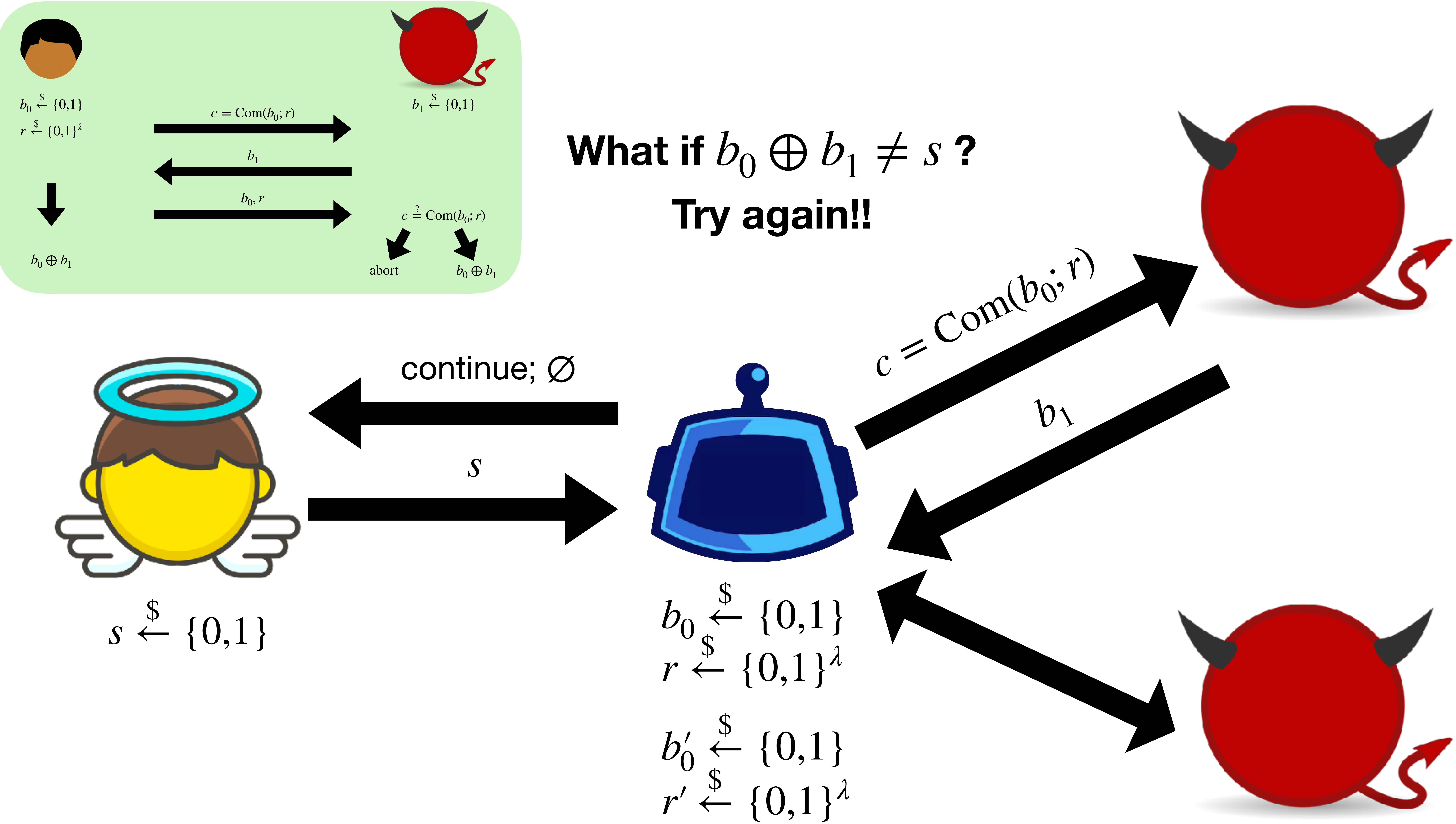
$c = \mathrm{Com}(b_0; r)$

b_1

$s \overset{\$}{\leftarrow} \{0,1\}$

$b_0 \overset{\$}{\leftarrow} \{0,1\}$

$r \overset{\$}{\leftarrow} \{0,1\}^\lambda$



$b_0 \overset{\$}{\leftarrow} \{0,1\}$
$r \overset{\$}{\leftarrow} \{0,1\}^\lambda$
$b_1 \overset{\$}{\leftarrow} \{0,1\}$
$c = \mathrm{Com}(b_0; r)$
b_1
b_0, r
$c \overset{?}{=} \mathrm{Com}(b_0; r)$
$b_0 \oplus b_1$
abort
$b_0 \oplus b_1$

What if $b_0 \oplus b_1 \neq s$?

Try again!!

continue; ∅
s
$s \overset{\$}{\leftarrow} \{0,1\}$
$c = \mathrm{Com}(b_0; r)$
b_1
$b_0 \overset{\$}{\leftarrow} \{0,1\}$
$r \overset{\$}{\leftarrow} \{0,1\}^\lambda$
$b_0' \overset{\$}{\leftarrow} \{0,1\}$
$r' \overset{\$}{\leftarrow} \{0,1\}^\lambda$