Just How Fair is an Unreactive World?

Srinivasan Raghuraman, Visa Research and MIT
Yibin Yang, Georgia Tech

Just How Fair is an Unreactive World?

Just How Fair is an Unreactive World?

Fair

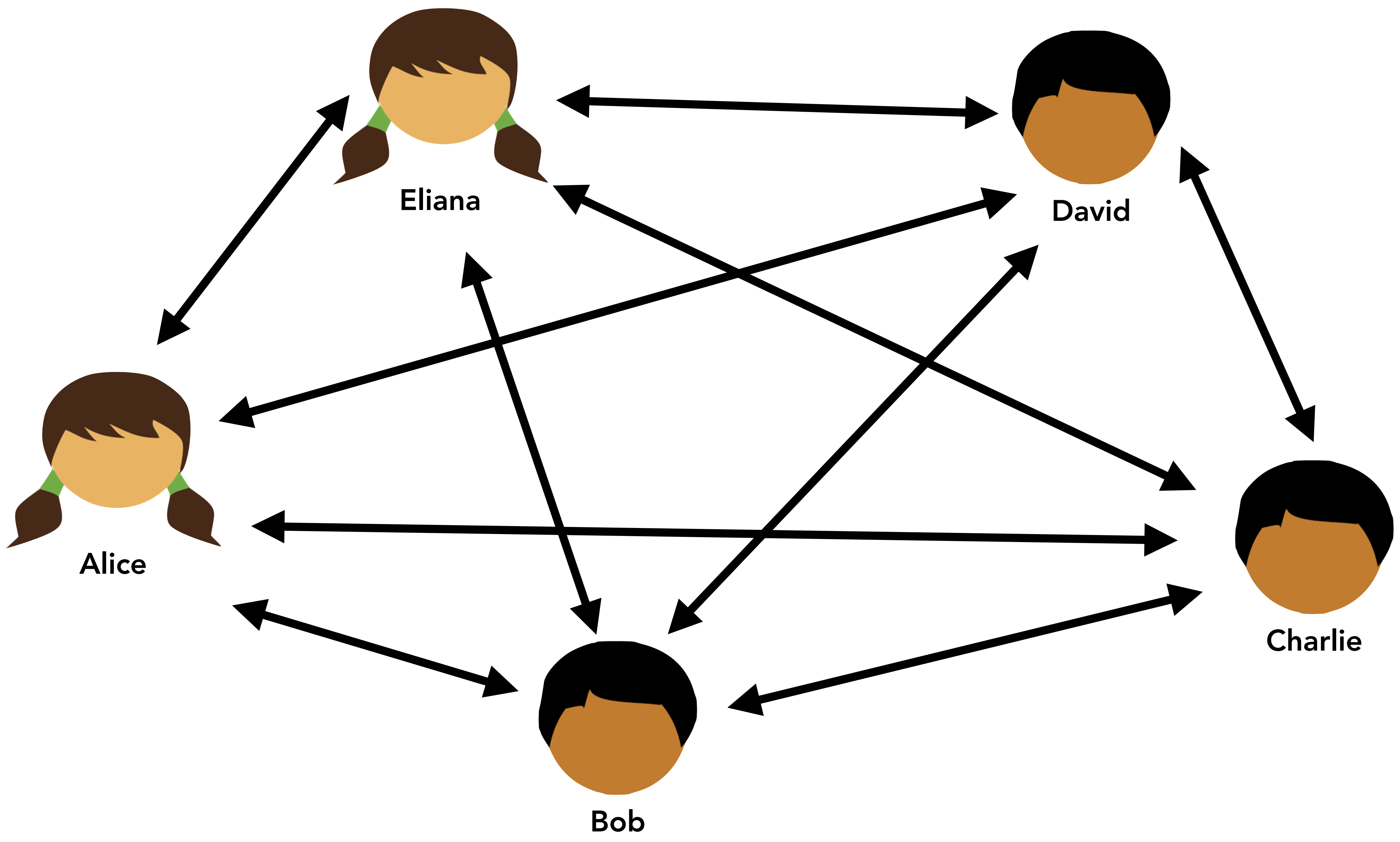
Fair Secure Multiparty Computation

Fair Secure Multiparty Computation

Let’s recall what MPC is

Fair Secure Multiparty Computation

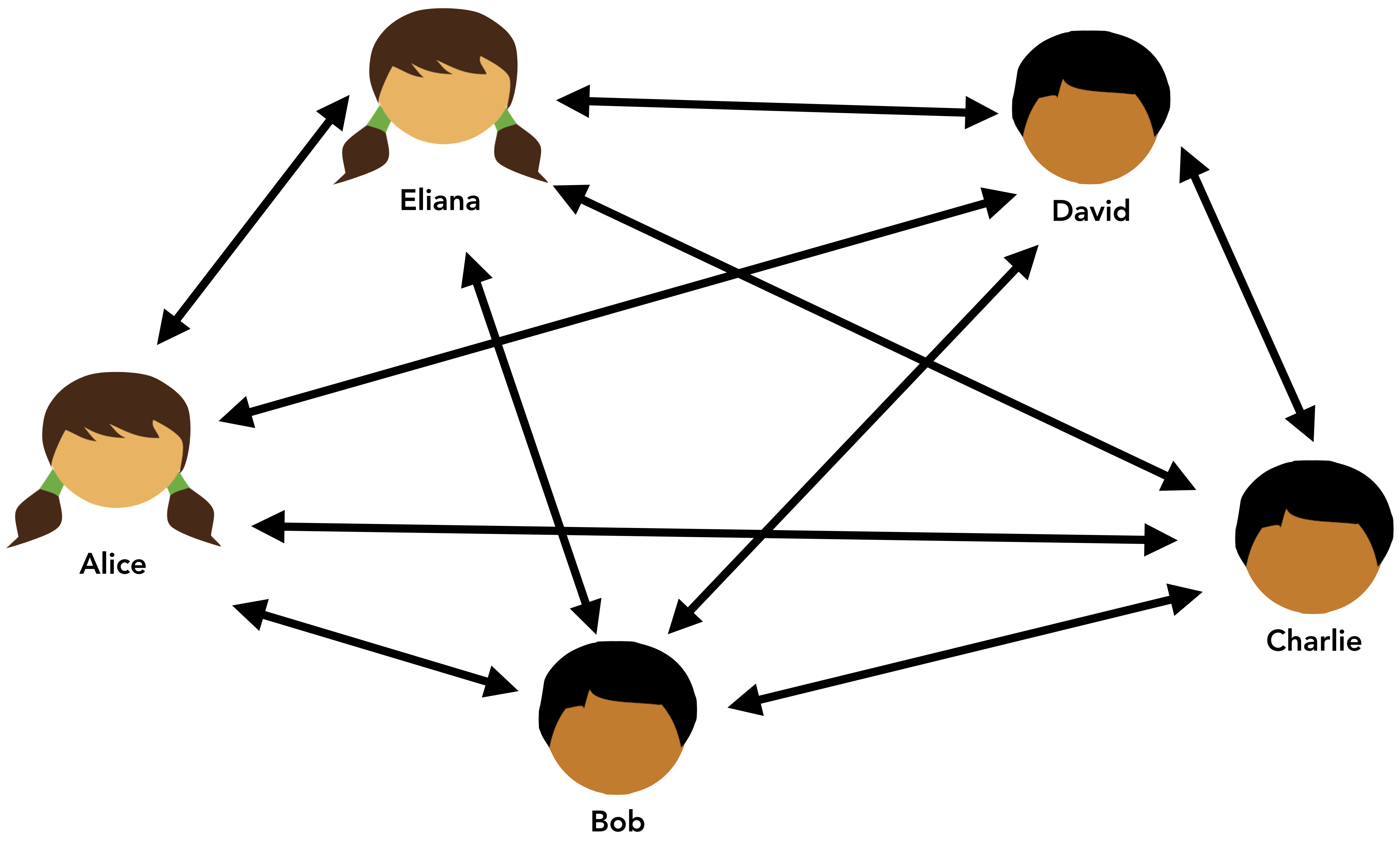
Let’s recall what MPC is



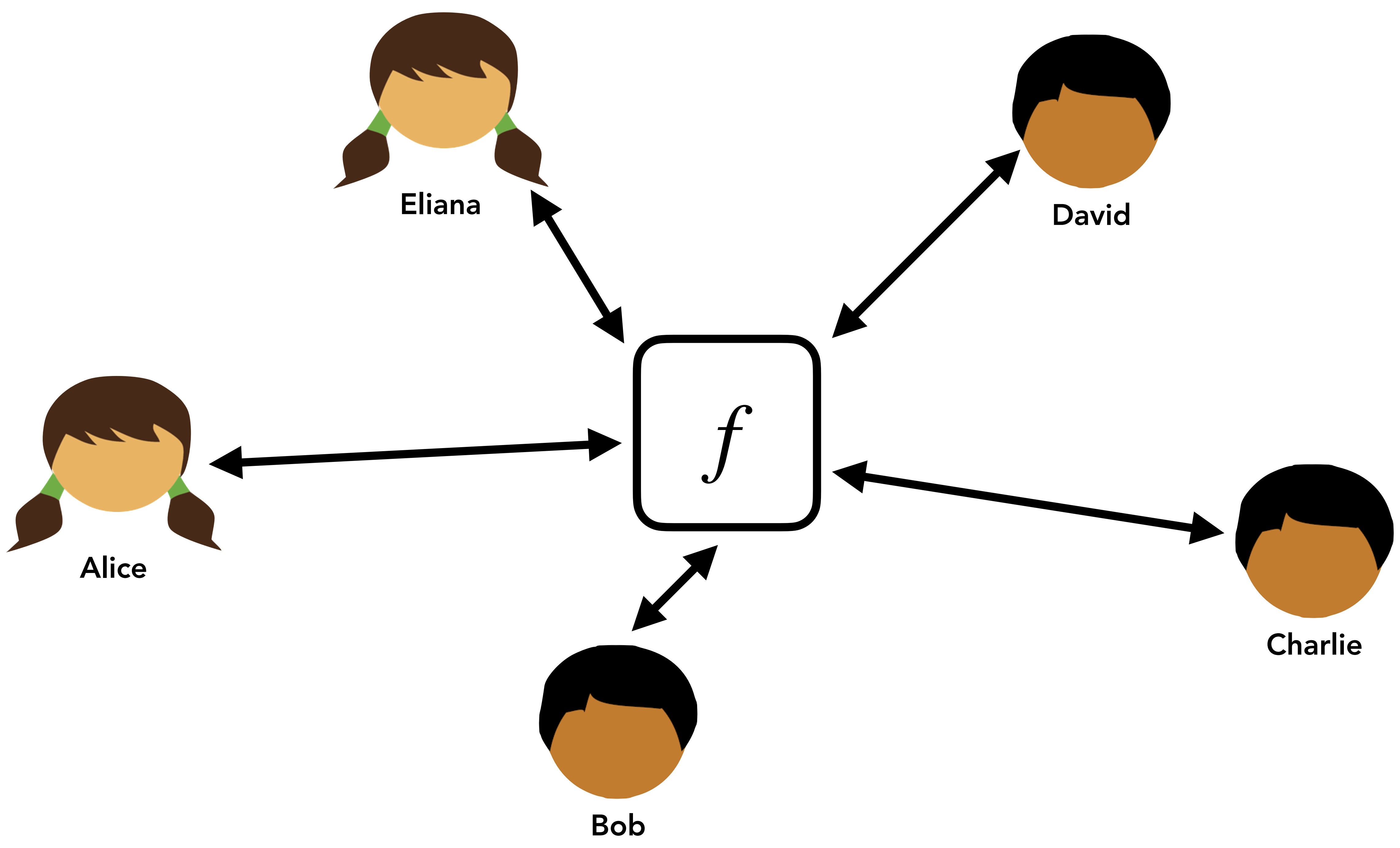
Fair Secure Multiparty Computation

Let's recall what MPC is

Real World

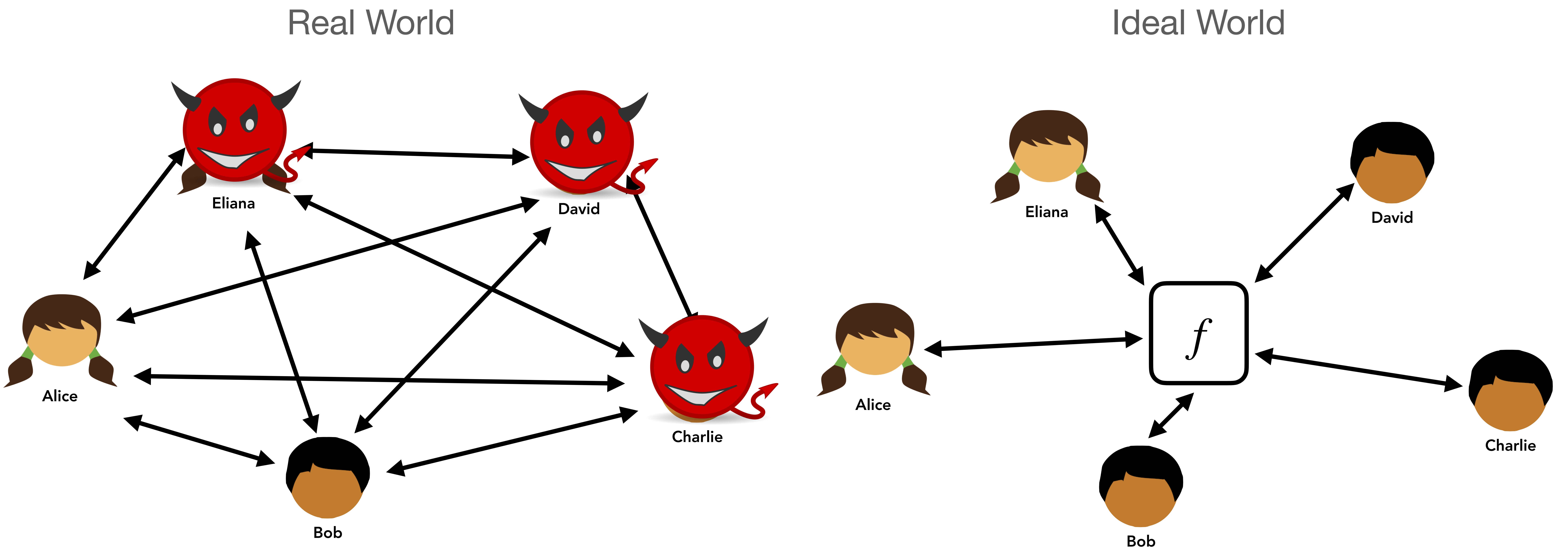


Ideal World



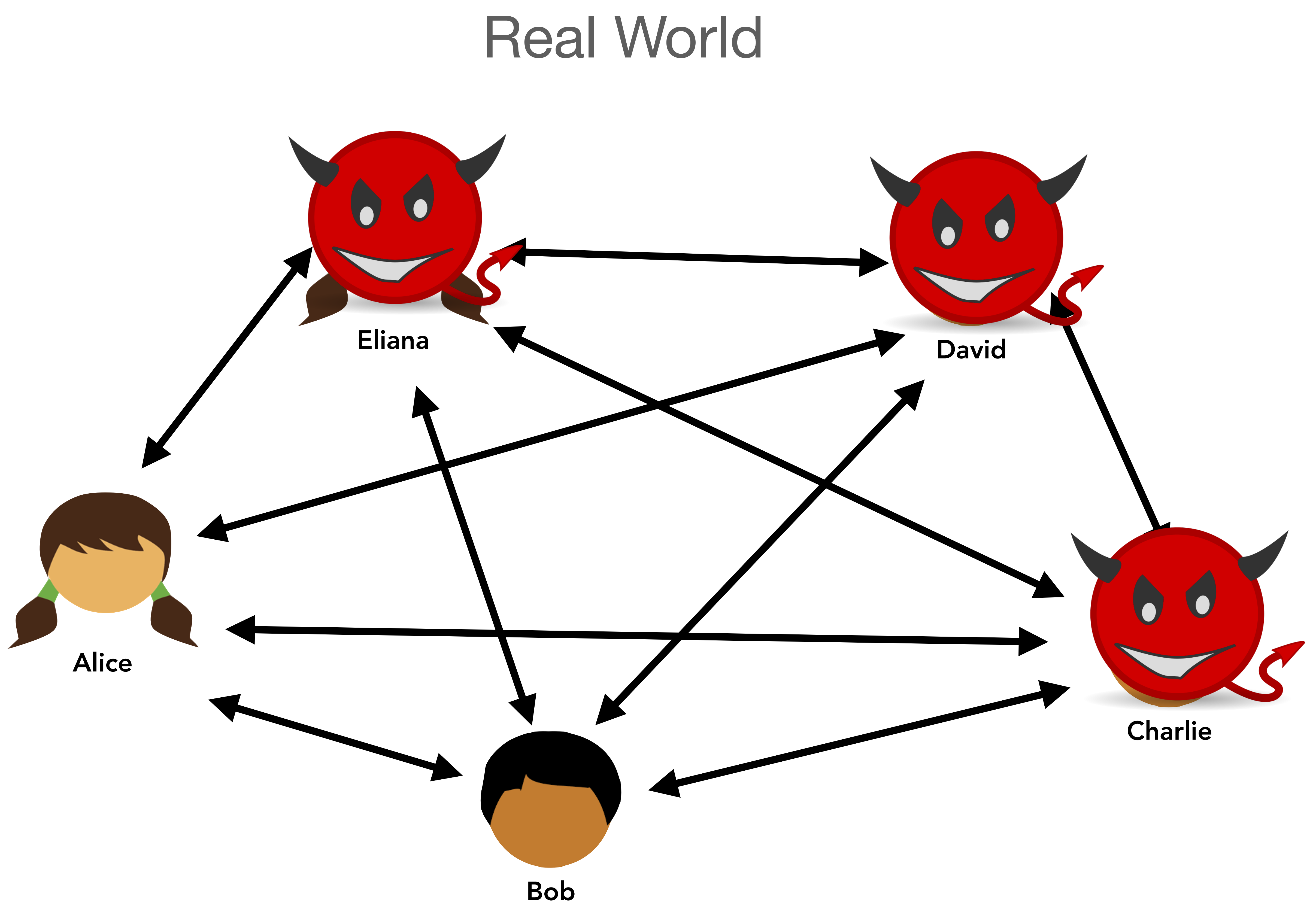
Fair Secure Multiparty Computation

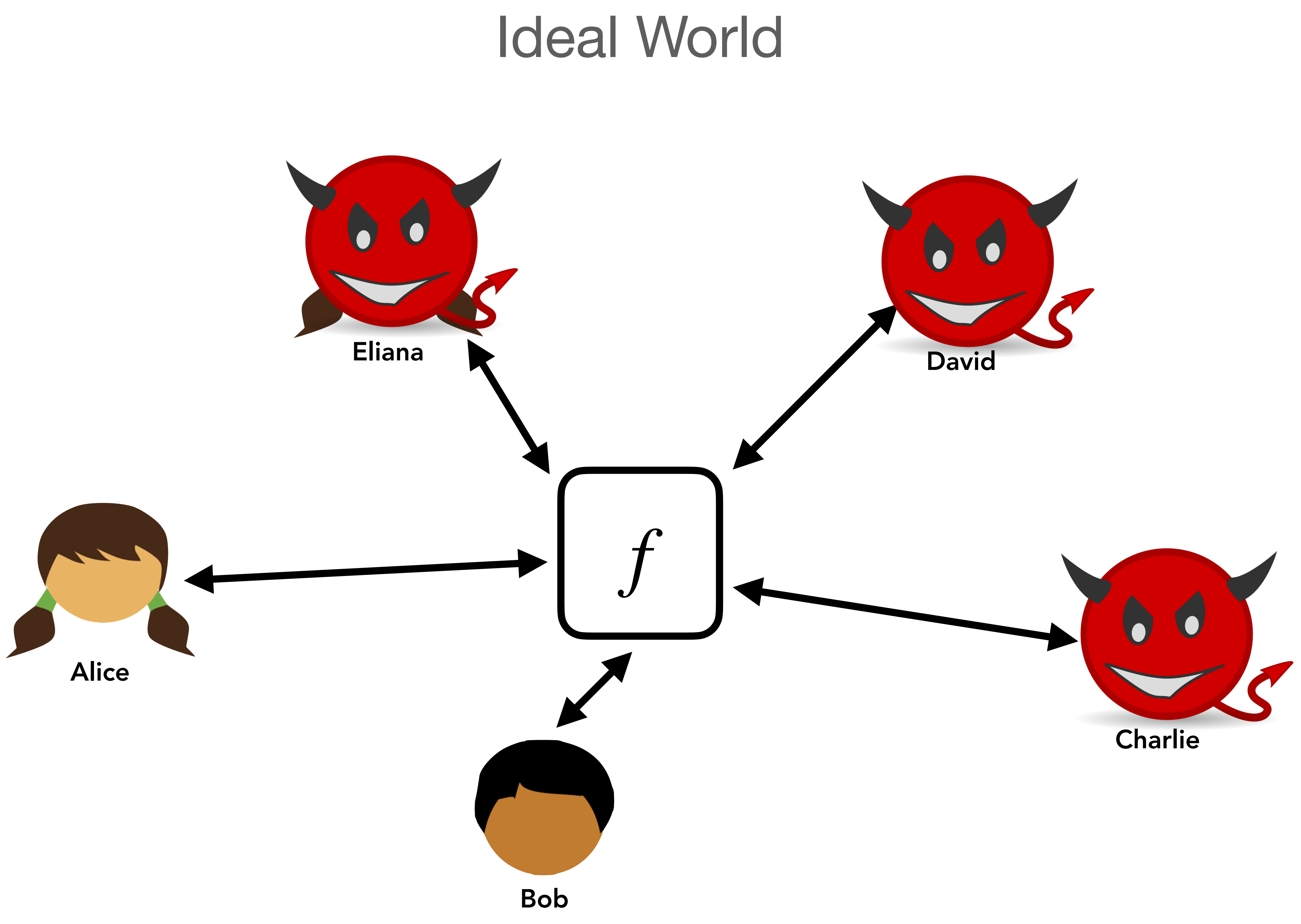
Let's recall what MPC is



Fair Secure Multiparty Computation

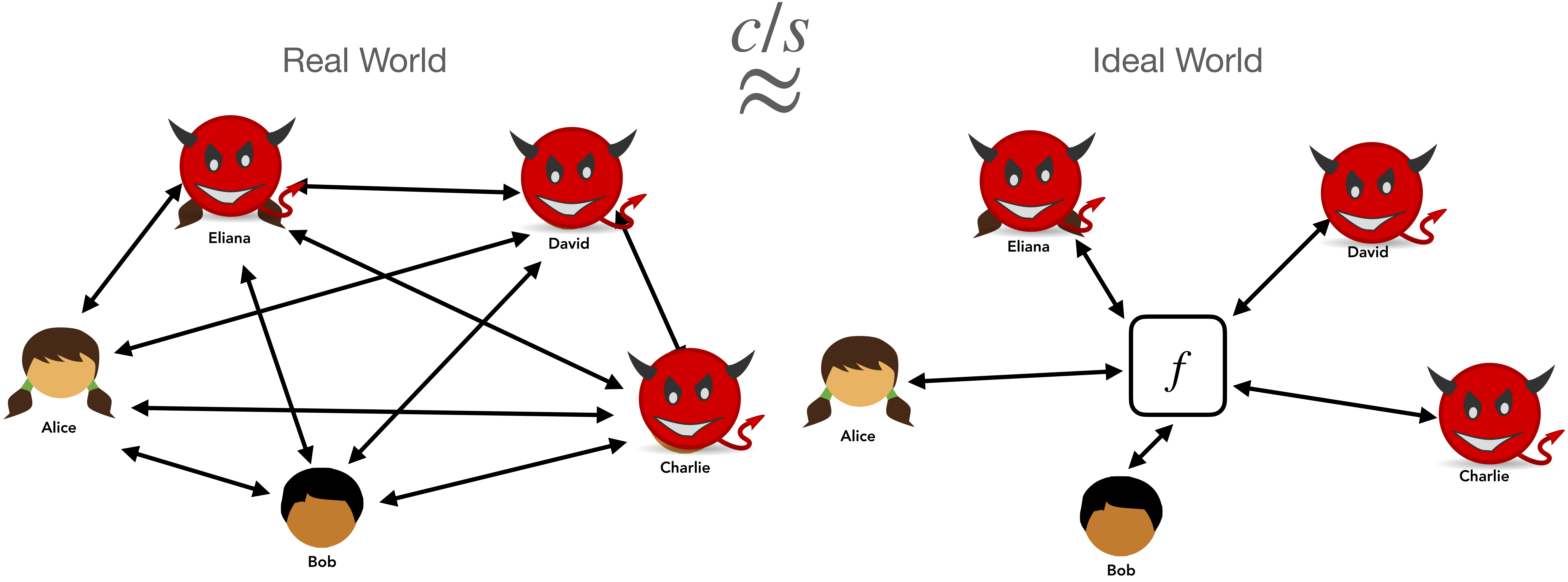
Let's recall what MPC is





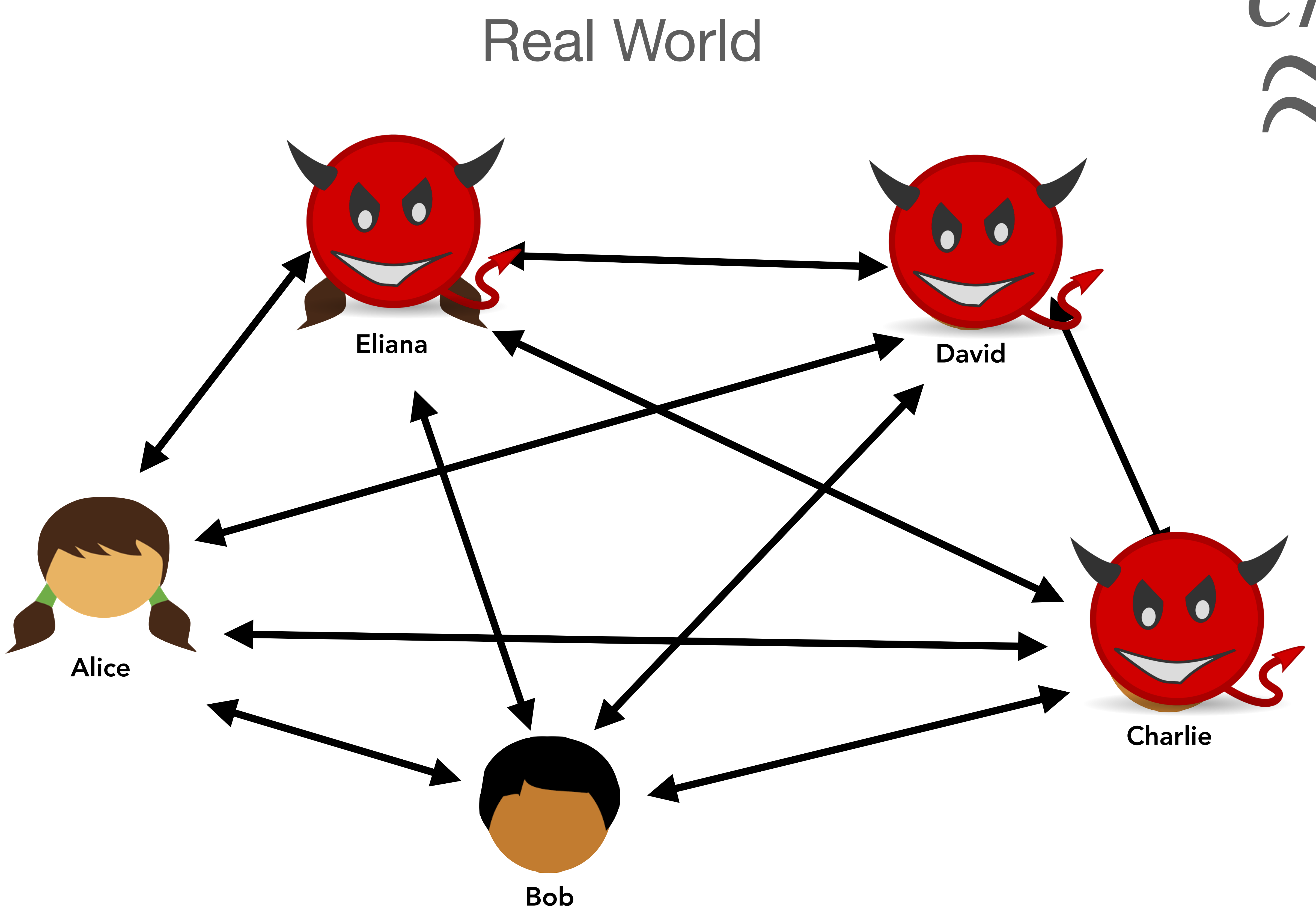
Fair Secure Multiparty Computation

Let's recall what MPC is

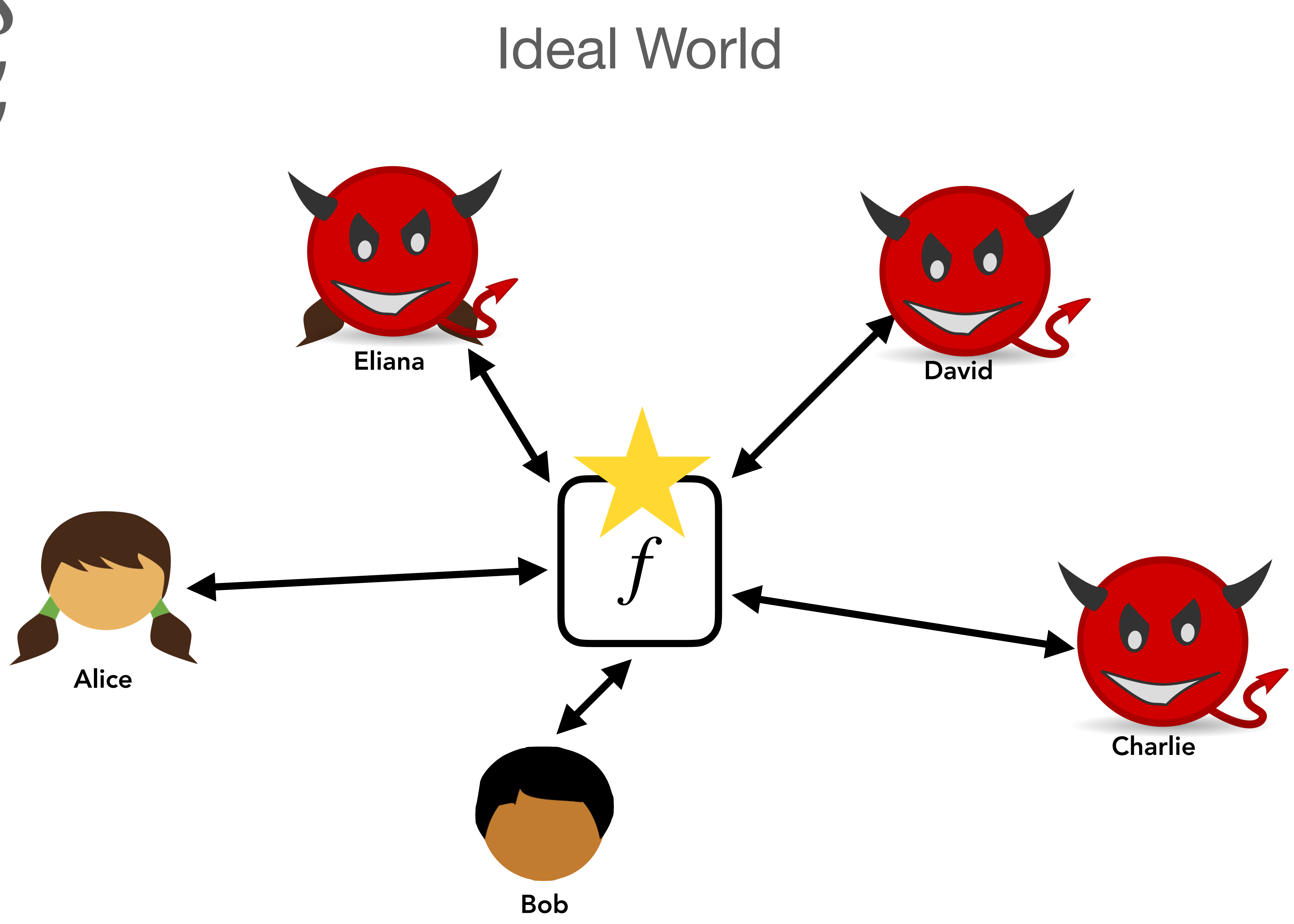


Fair Secure Multiparty Computation

Let's recall what MPC is



$\overset{c/s}{\approx}$



We consider ***active, malicious majority***

Different Security Levels

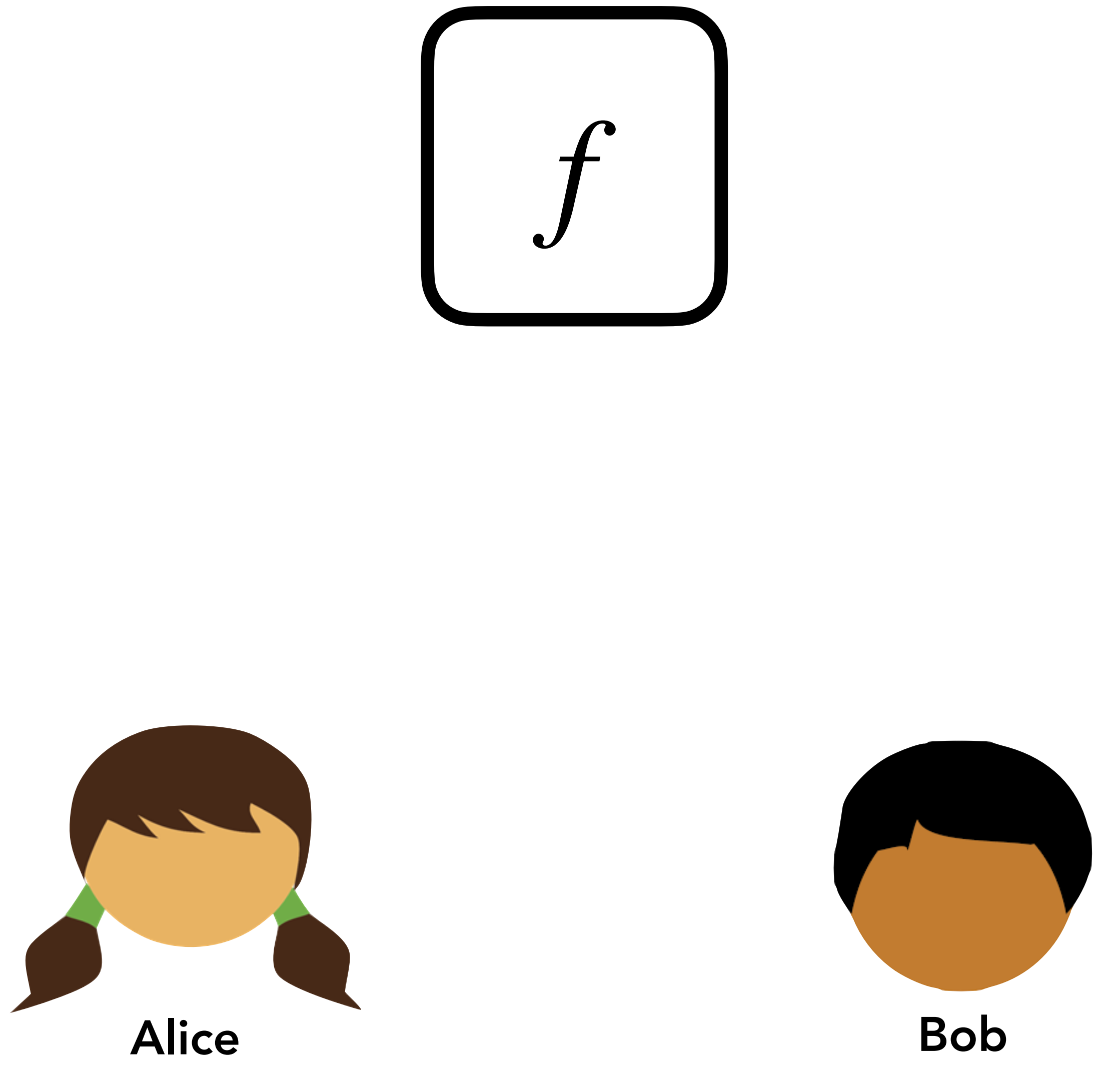
Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

We consider ***active, malicious majority***

Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

Security with Abort

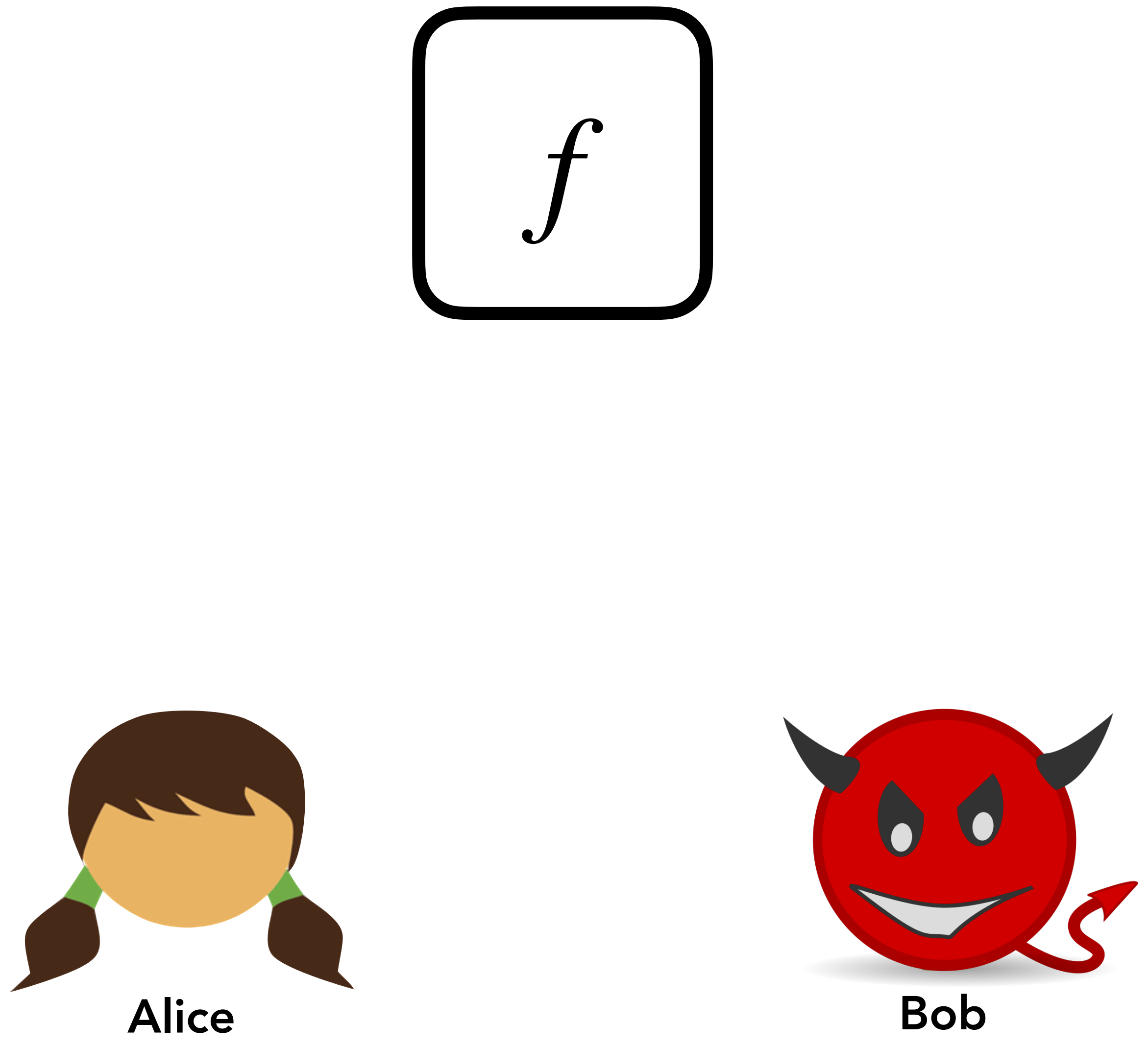


We consider ***active, malicious majority***

Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

Security with Abort

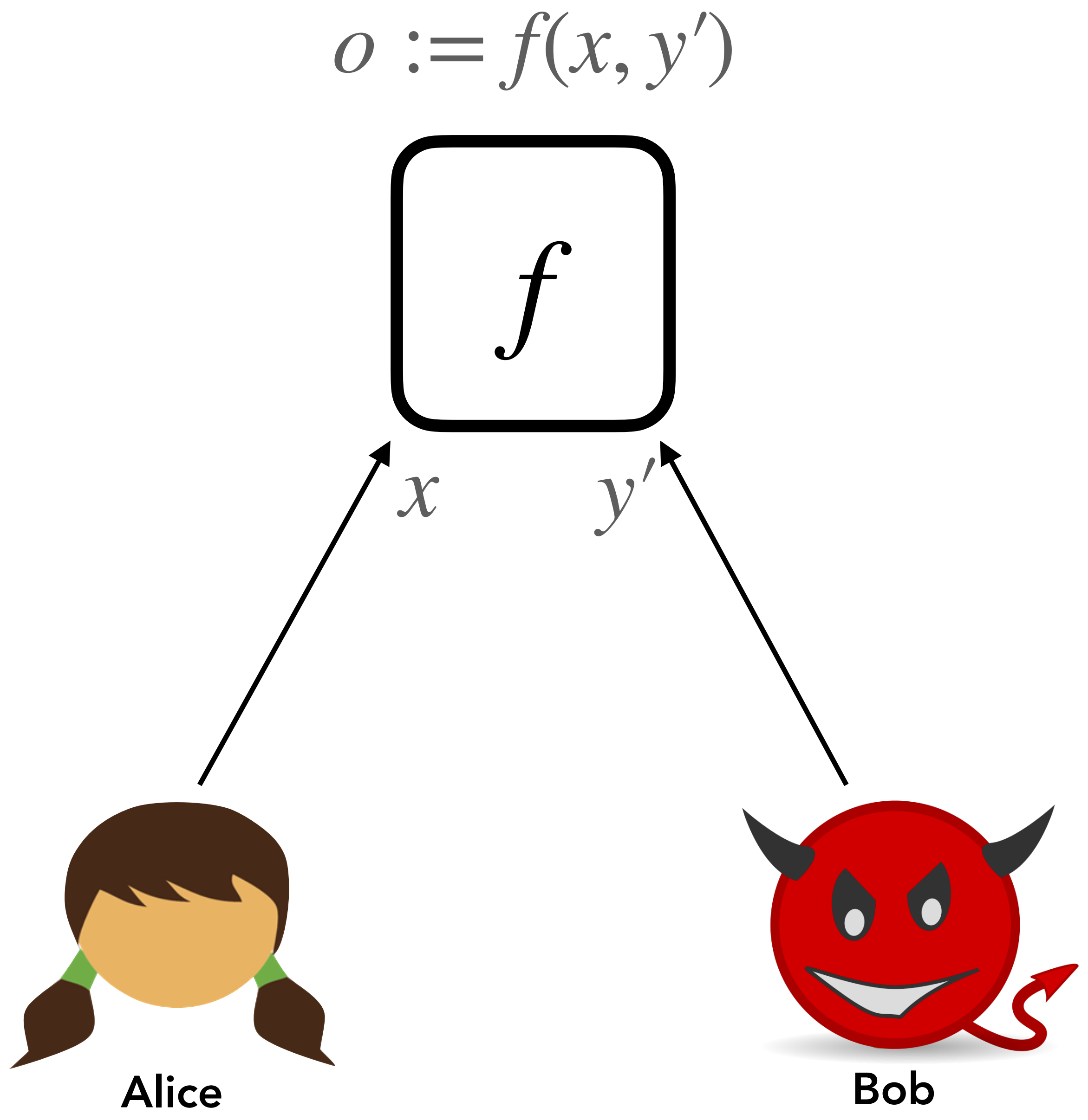


We consider ***active, malicious majority***

Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

Security with Abort

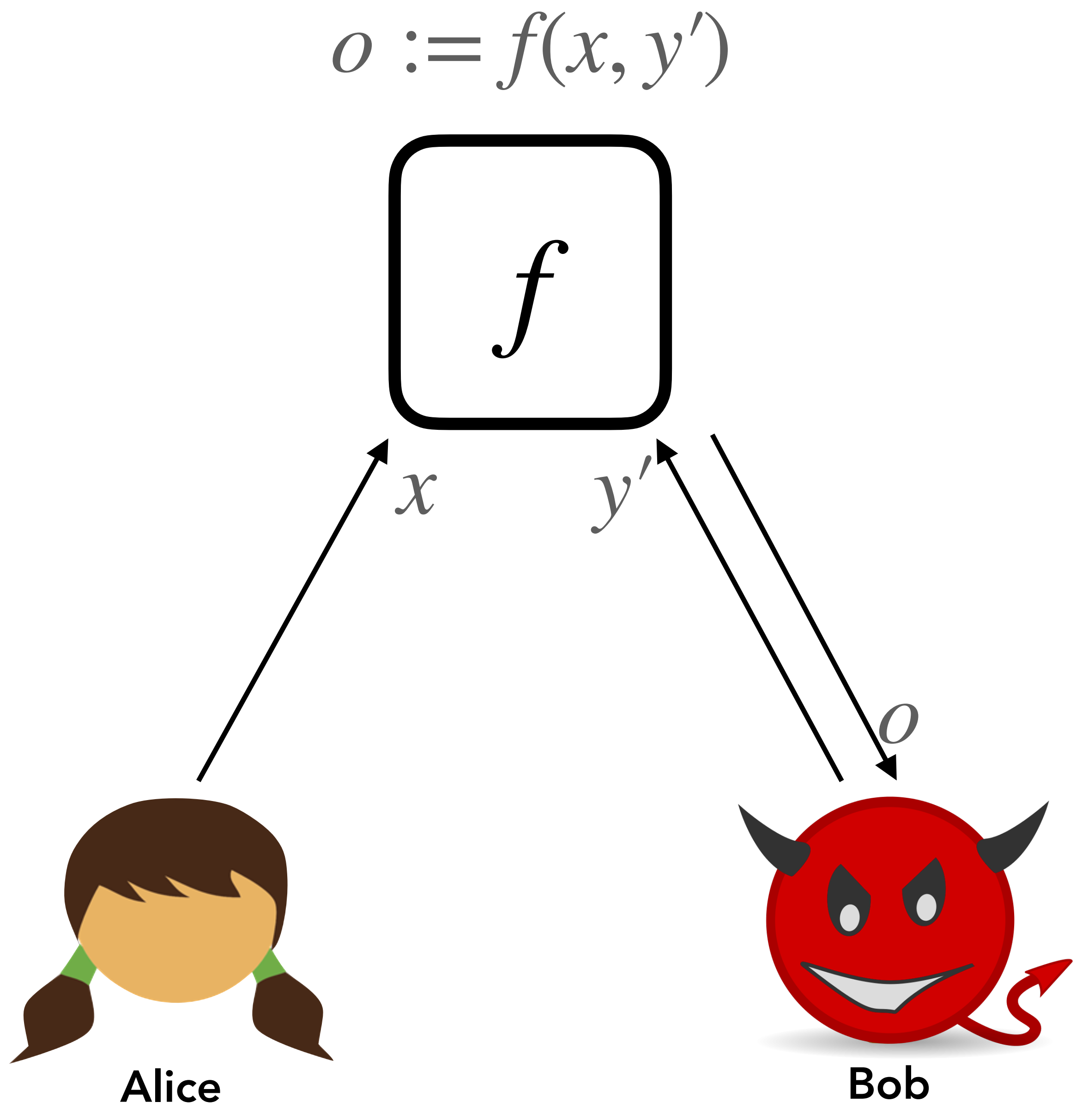


We consider ***active, malicious majority***

Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

Security with Abort

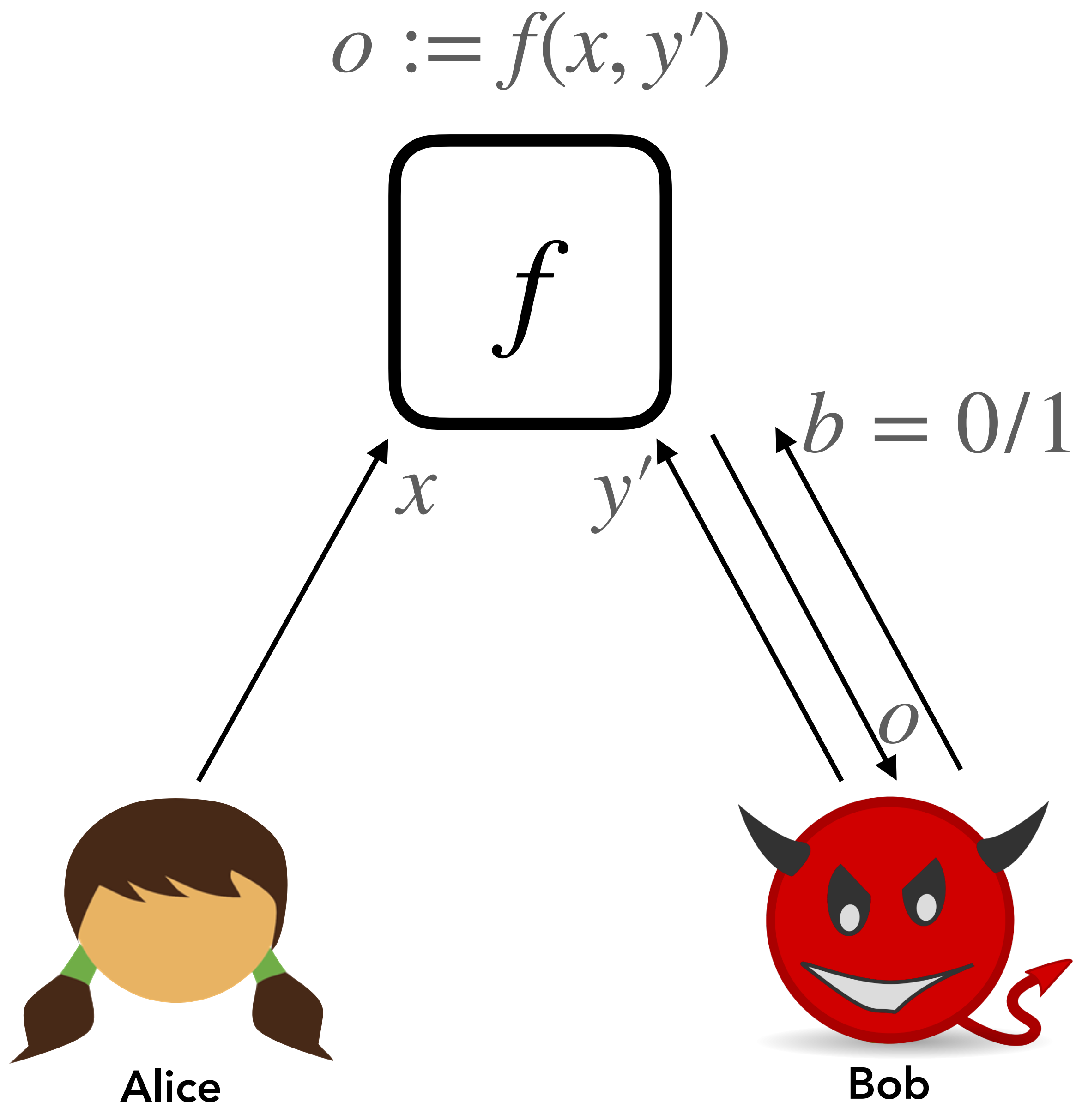


We consider ***active, malicious majority***

Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

Security with Abort

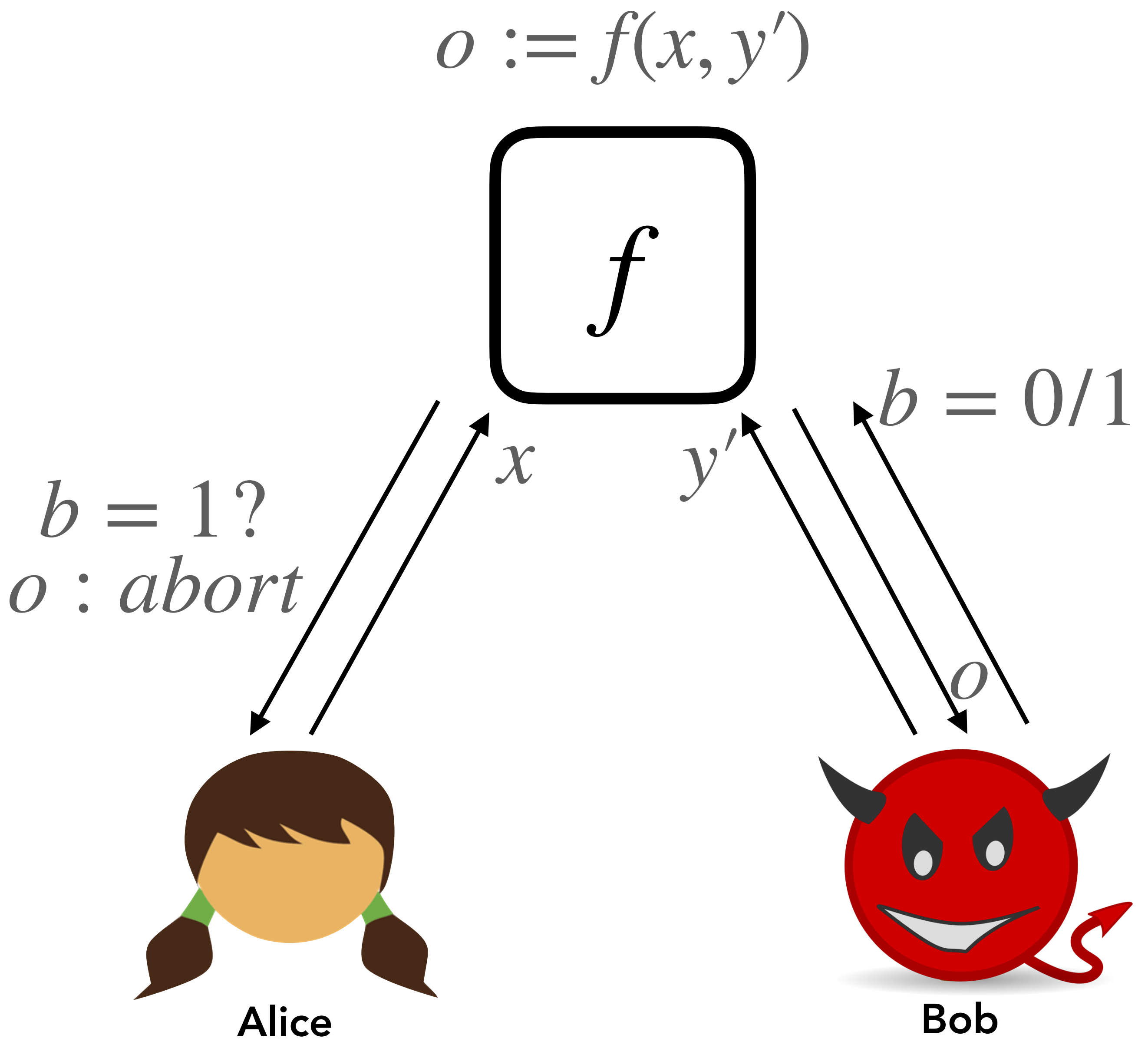


We consider ***active, malicious majority***

Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

Security with Abort

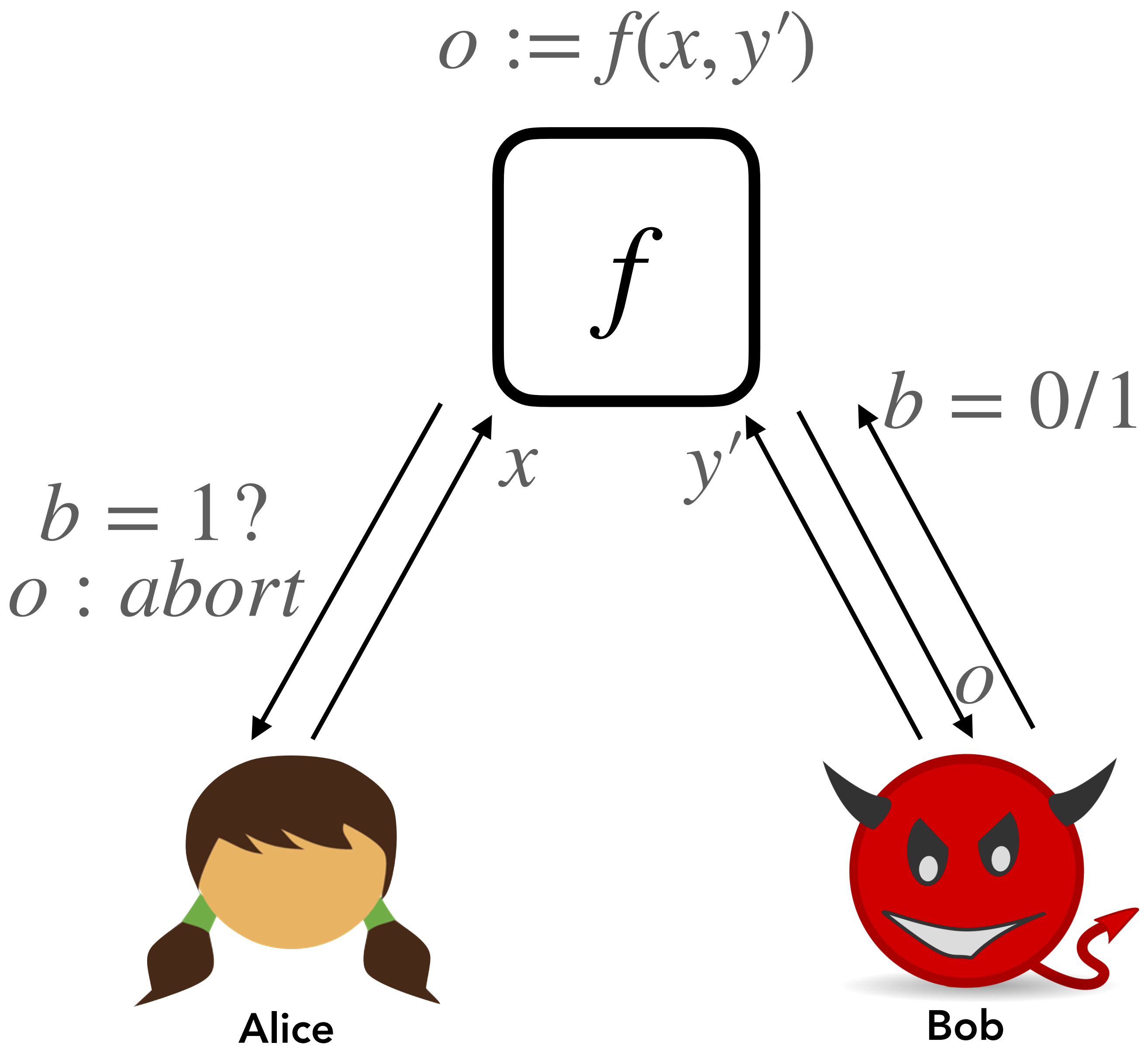


We consider ***active, malicious majority***

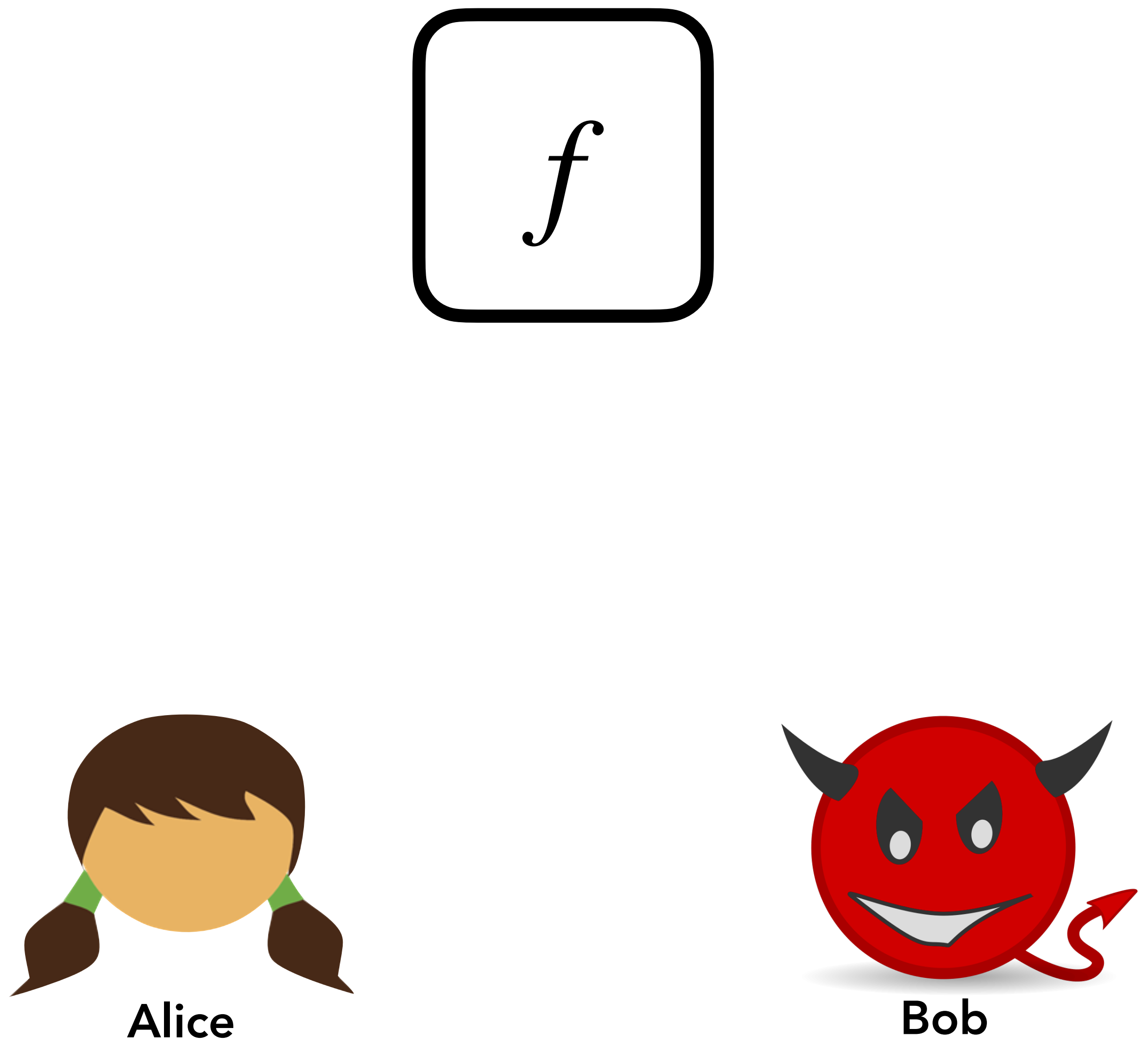
Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

Security with Abort



Guaranteed Output Delivery

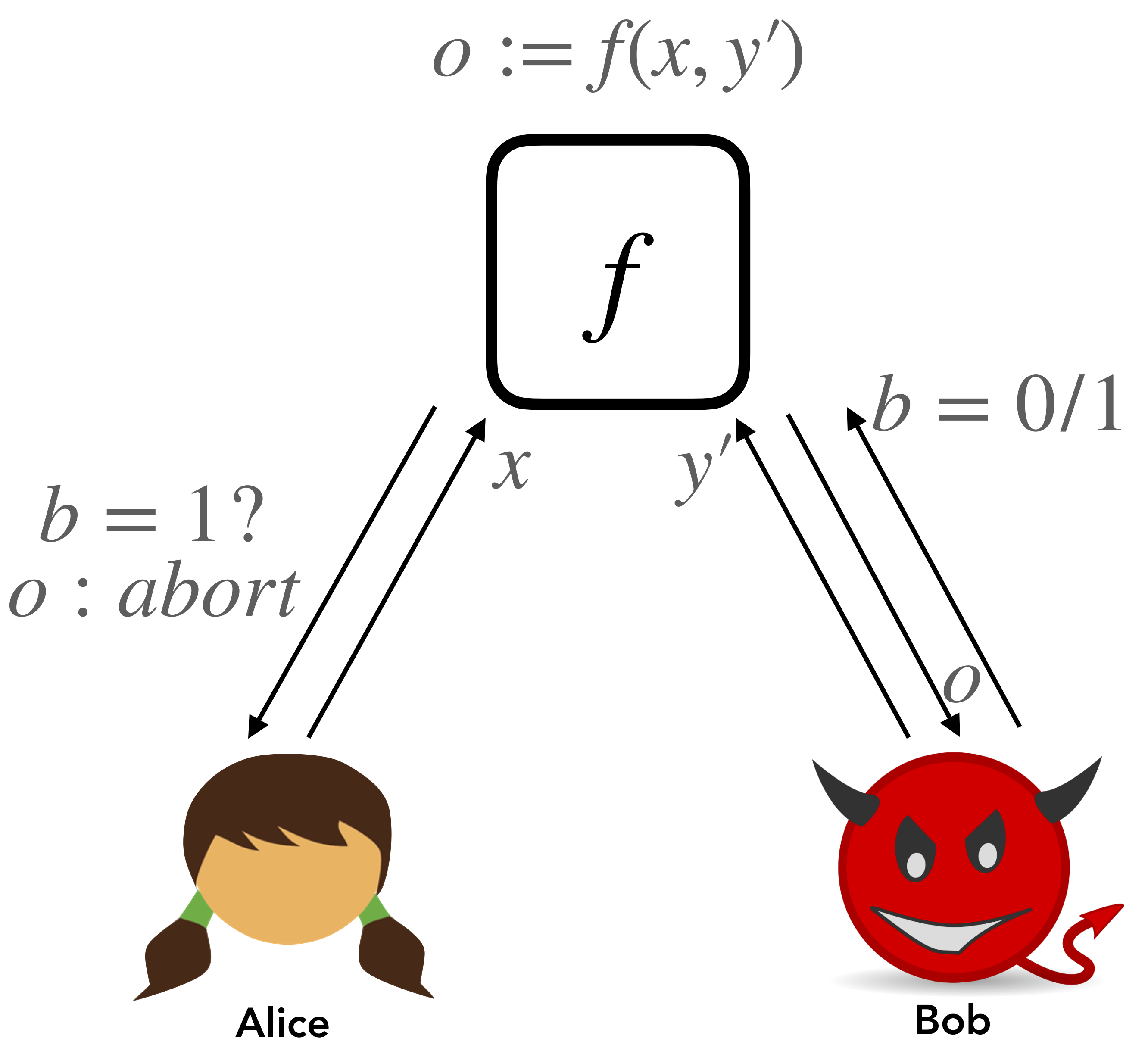


We consider ***active, malicious majority***

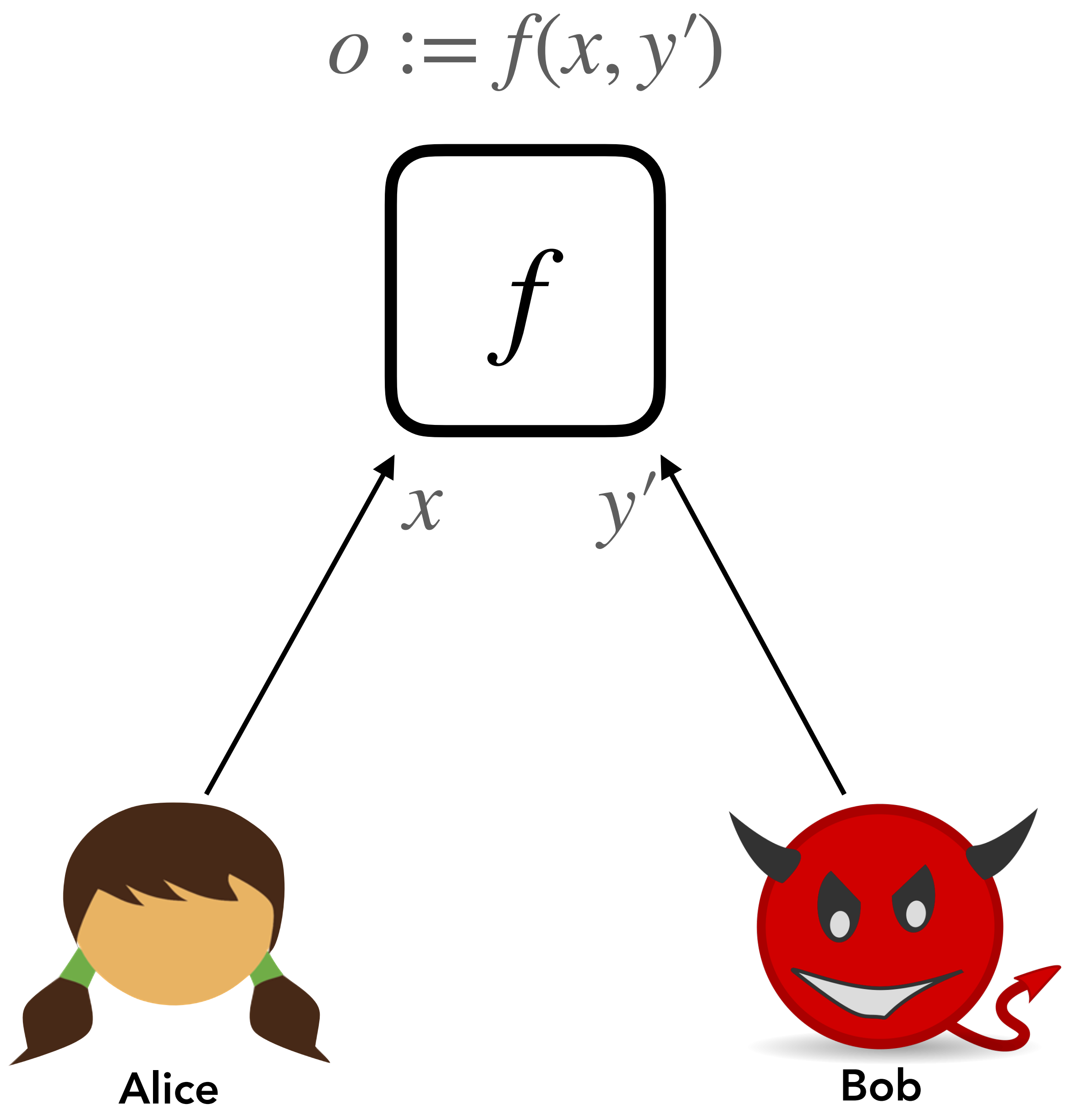
Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

Security with Abort



Guaranteed Output Delivery

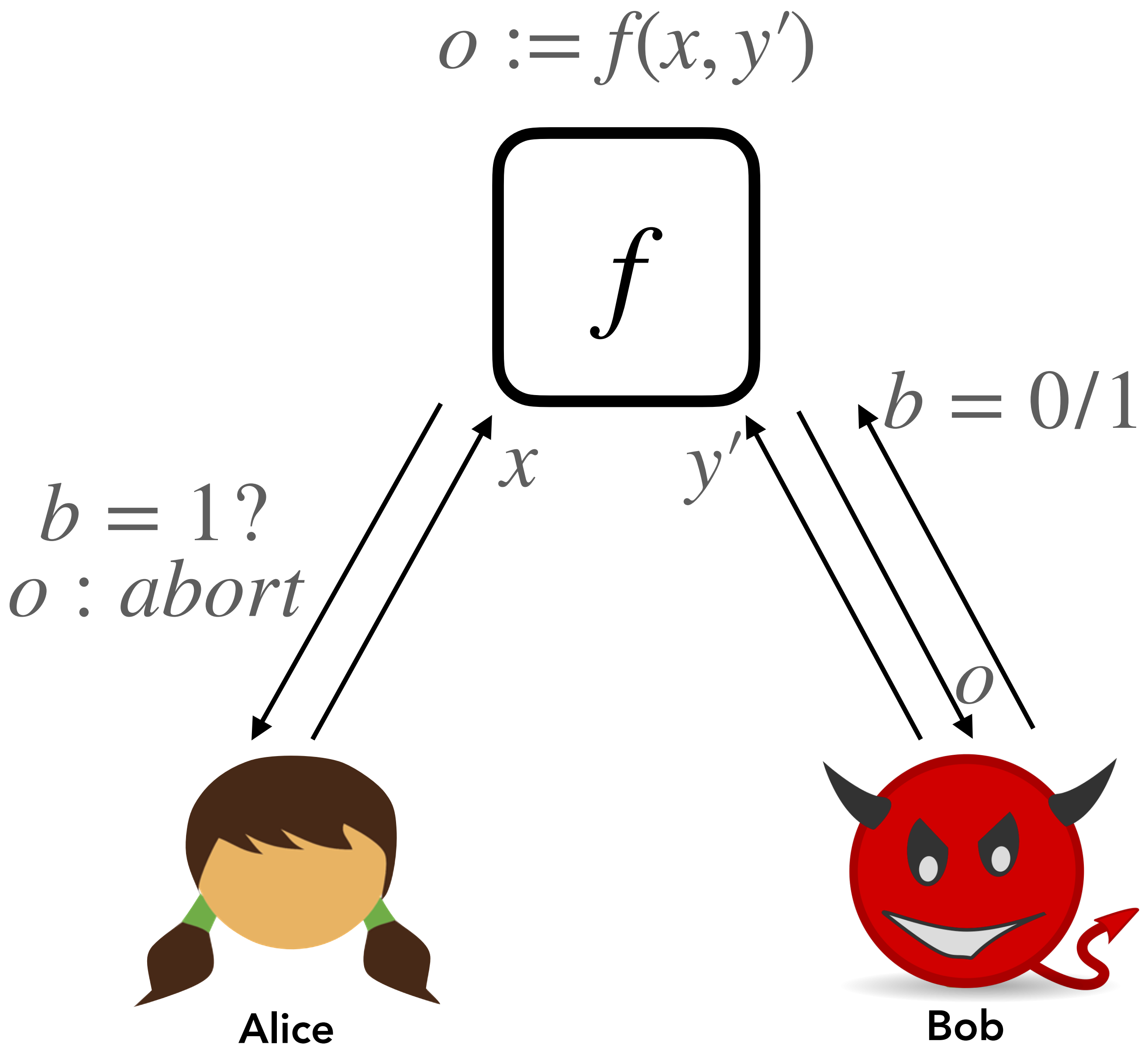


We consider ***active, malicious majority***

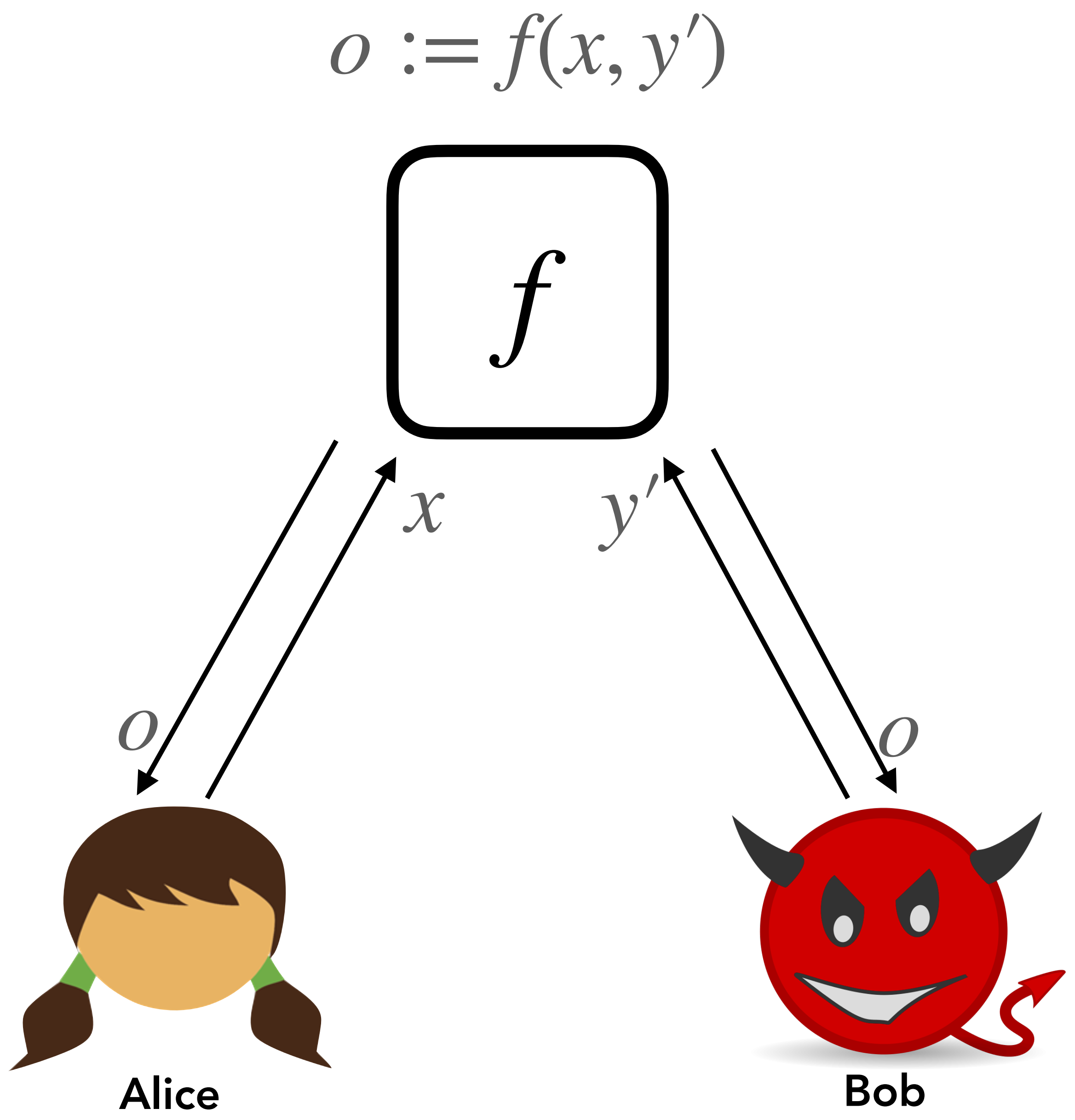
Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

Security with Abort



Guaranteed Output Delivery

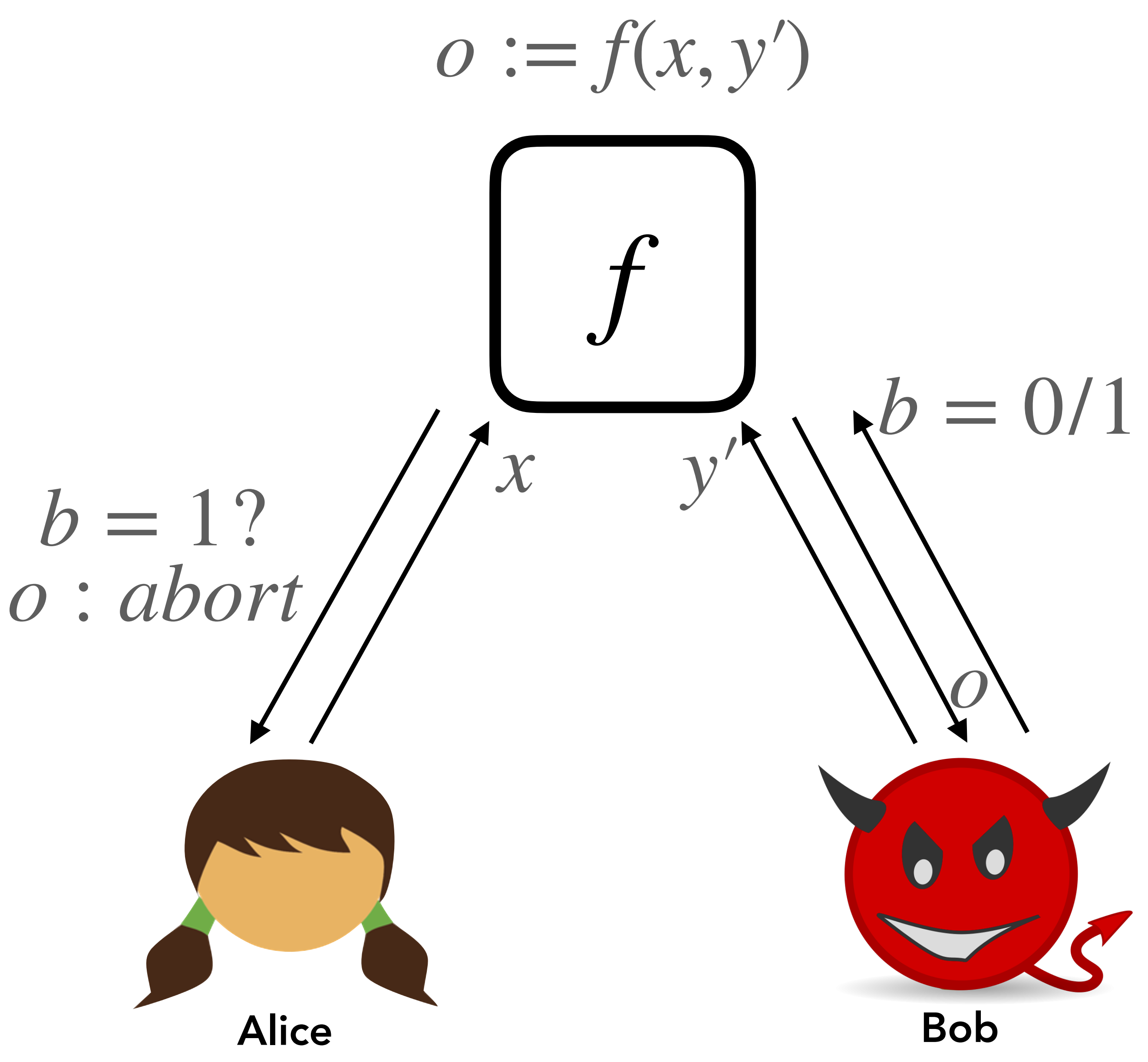


We consider ***active, malicious majority***

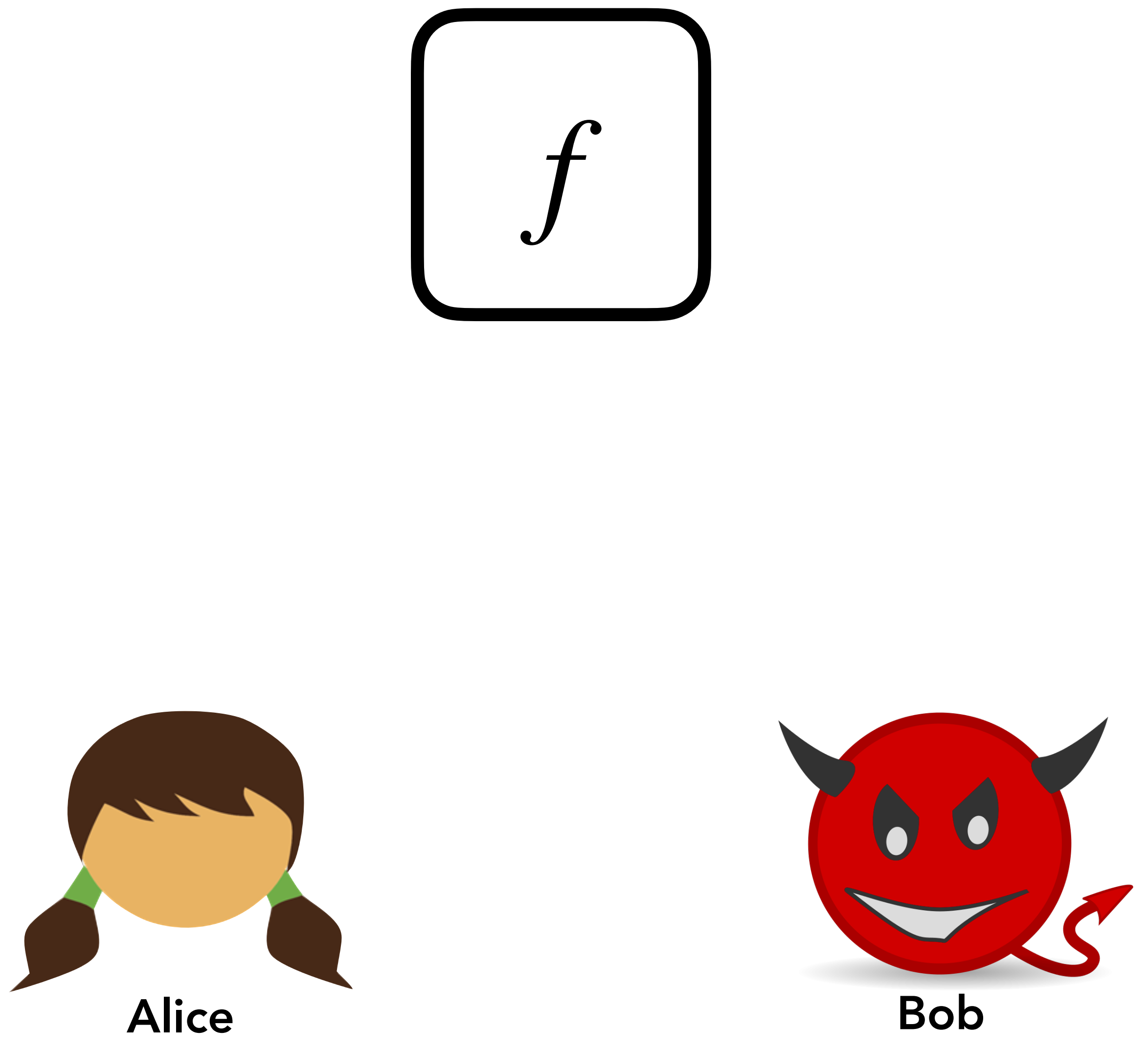
Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

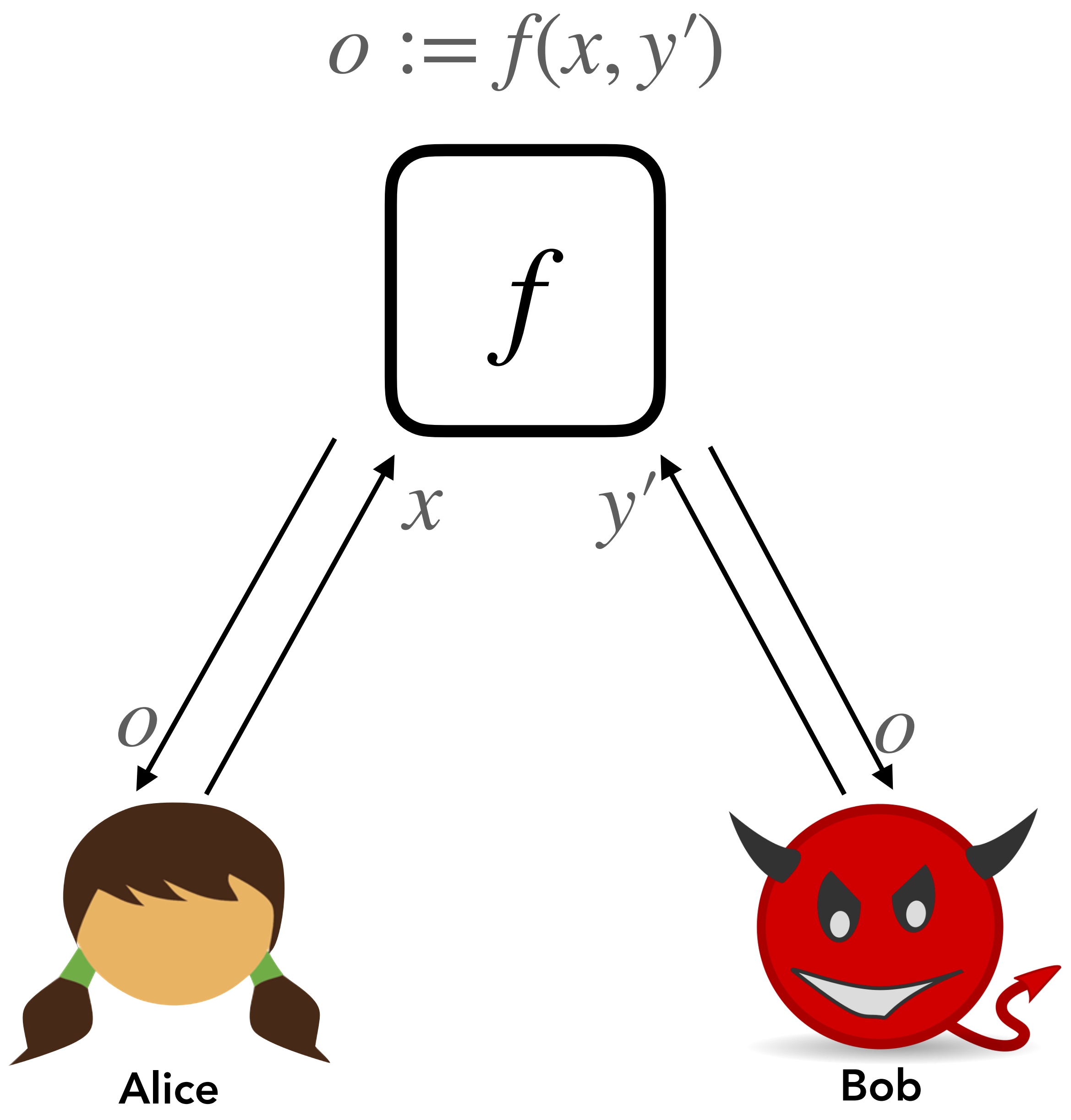
Security with Abort



Fairness



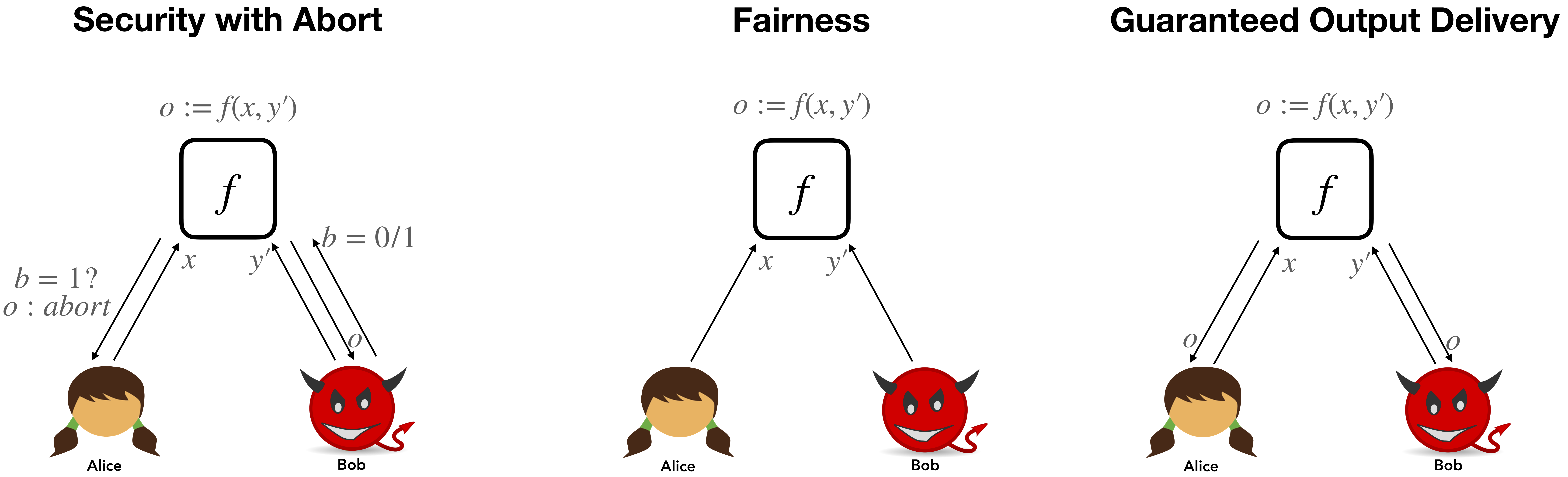
Guaranteed Output Delivery



We consider ***active, malicious majority***

Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

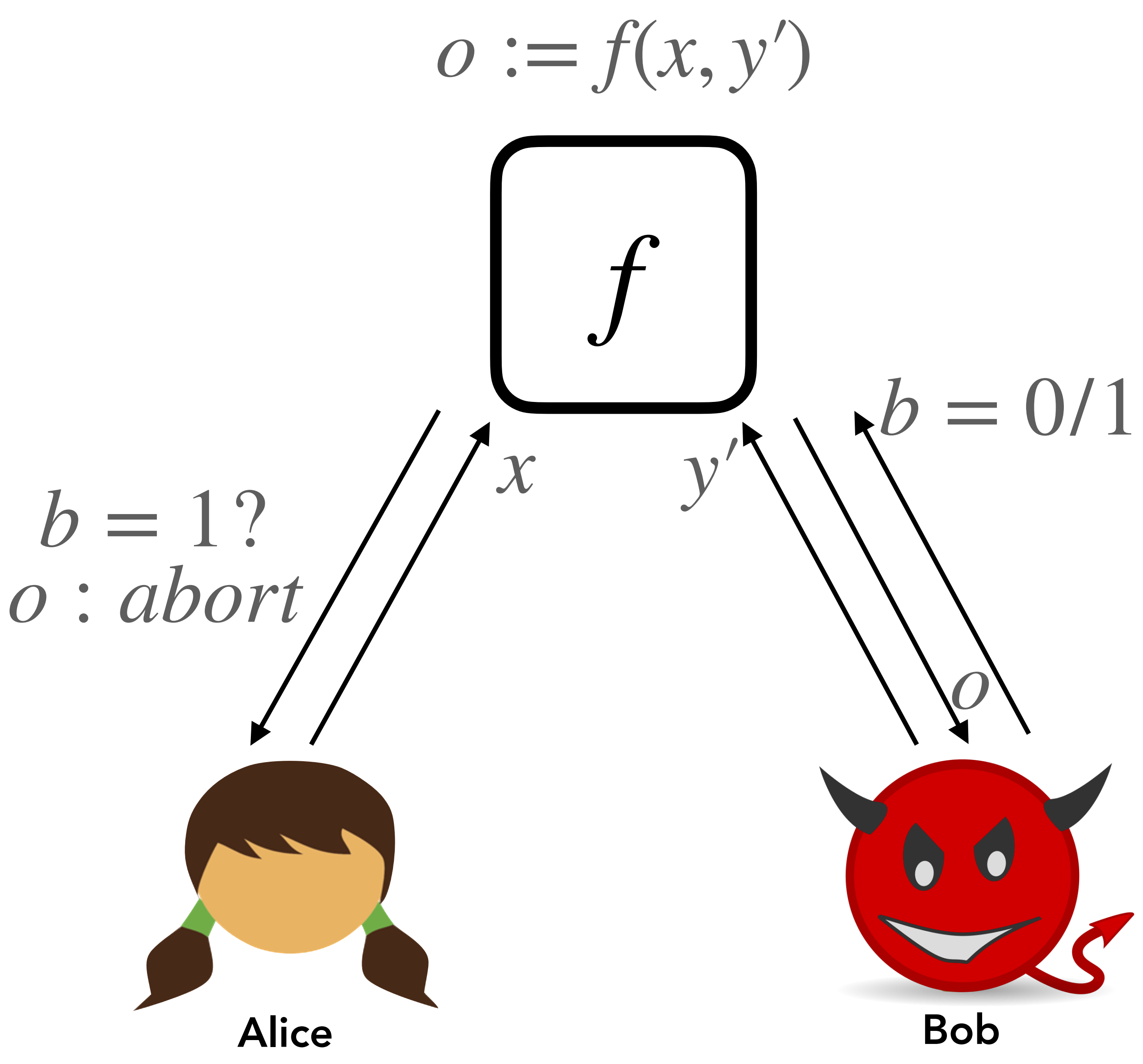


We consider ***active, malicious majority***

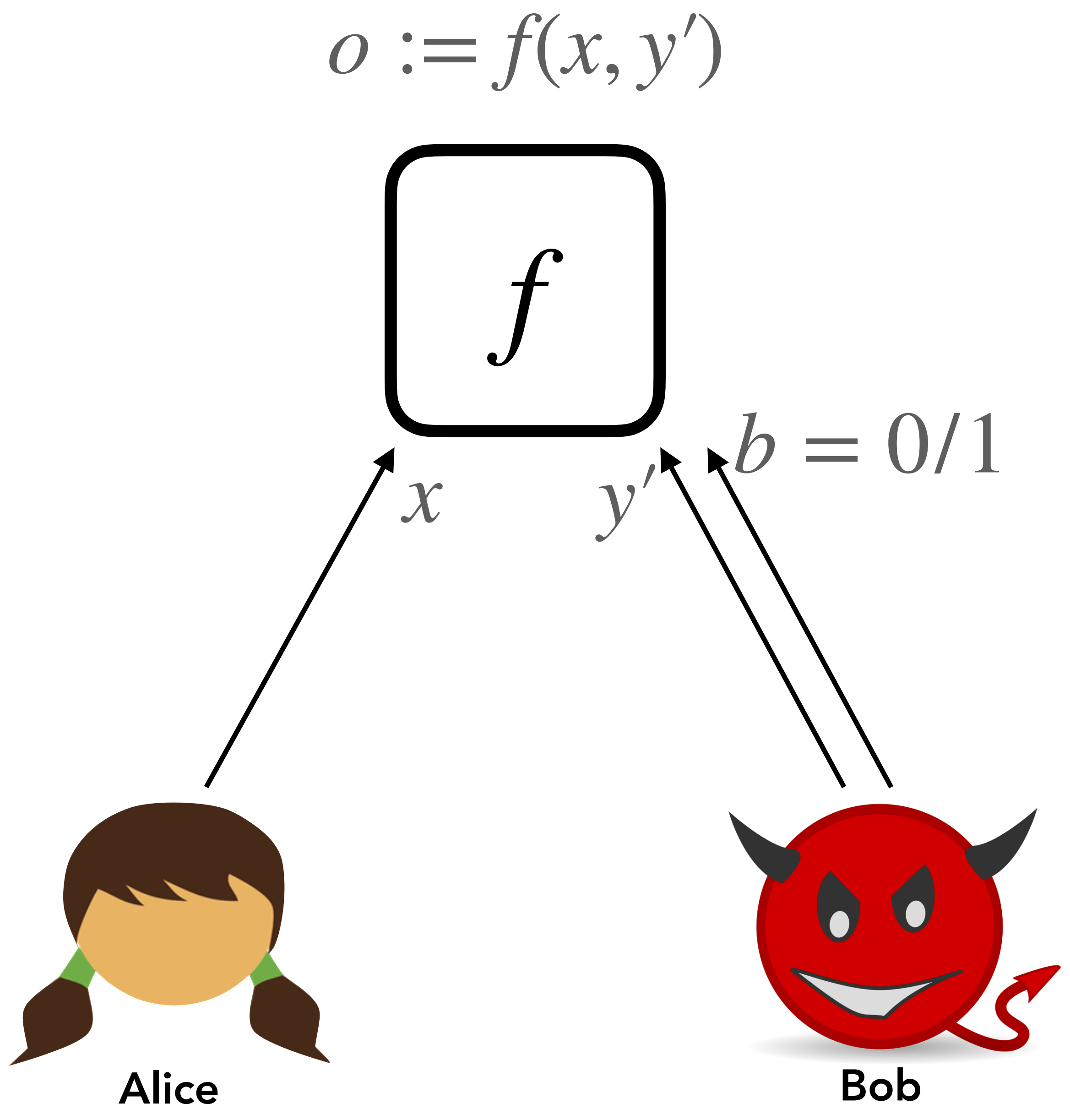
Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

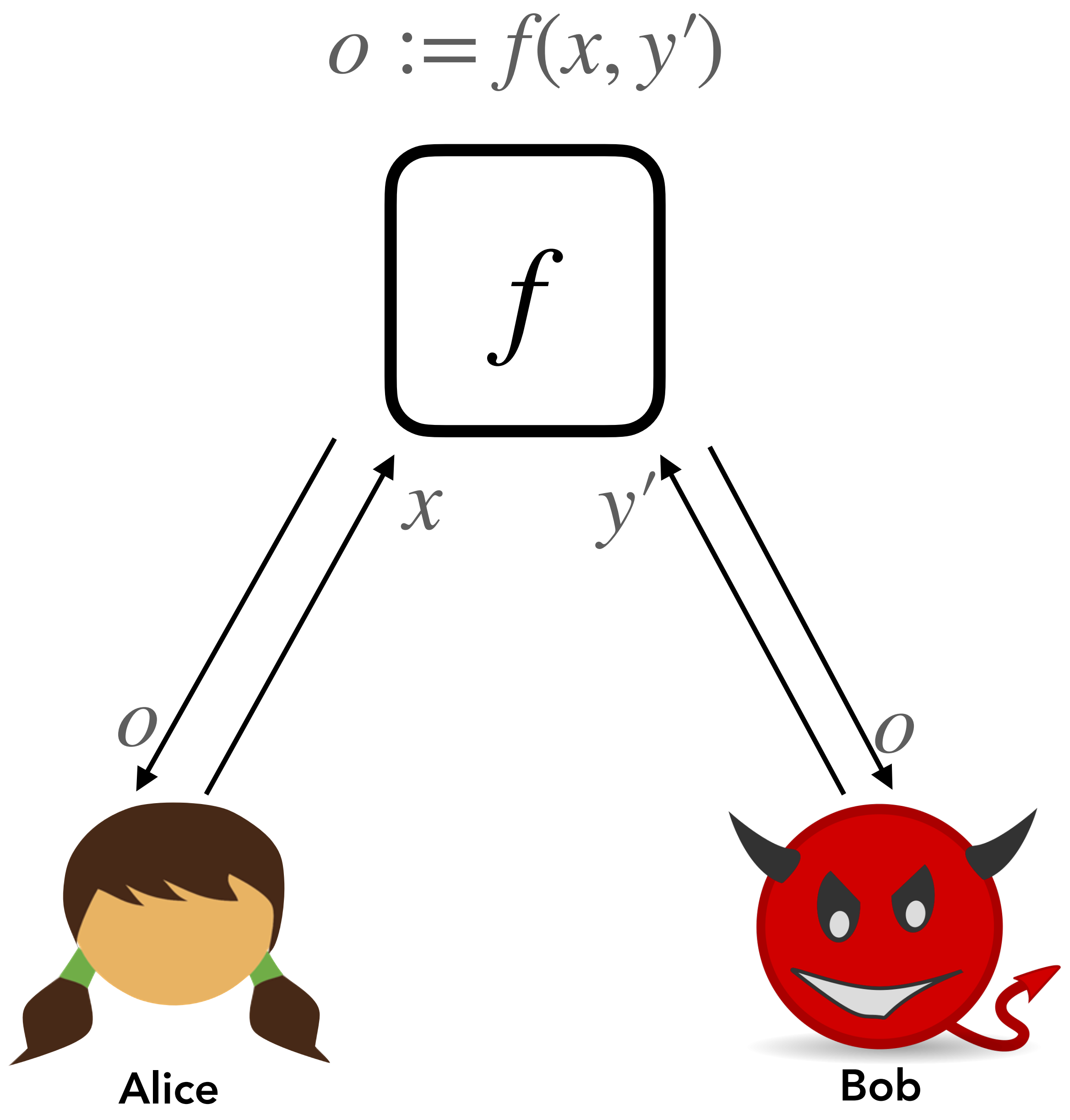
Security with Abort



Fairness



Guaranteed Output Delivery

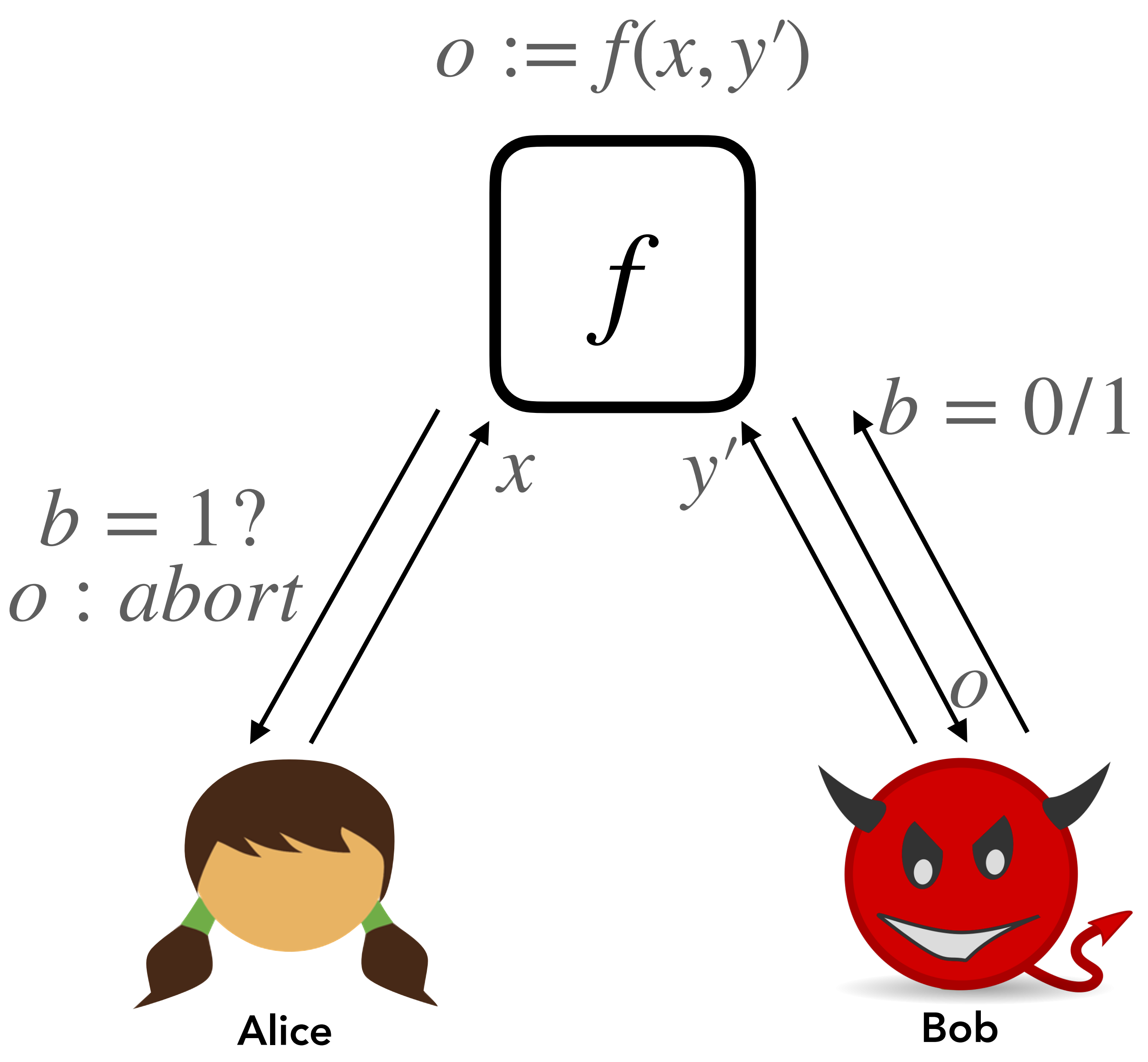


We consider ***active, malicious majority***

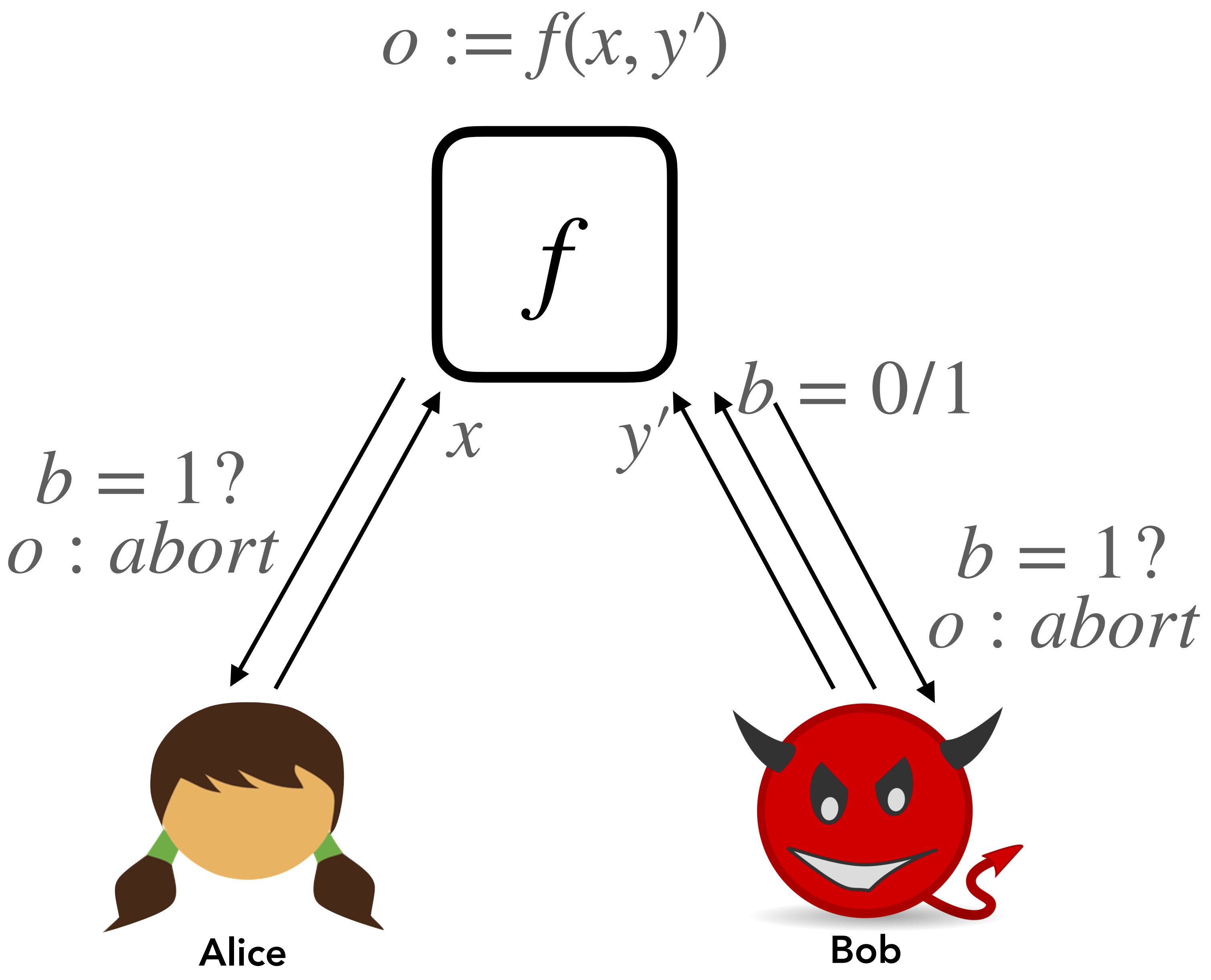
Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

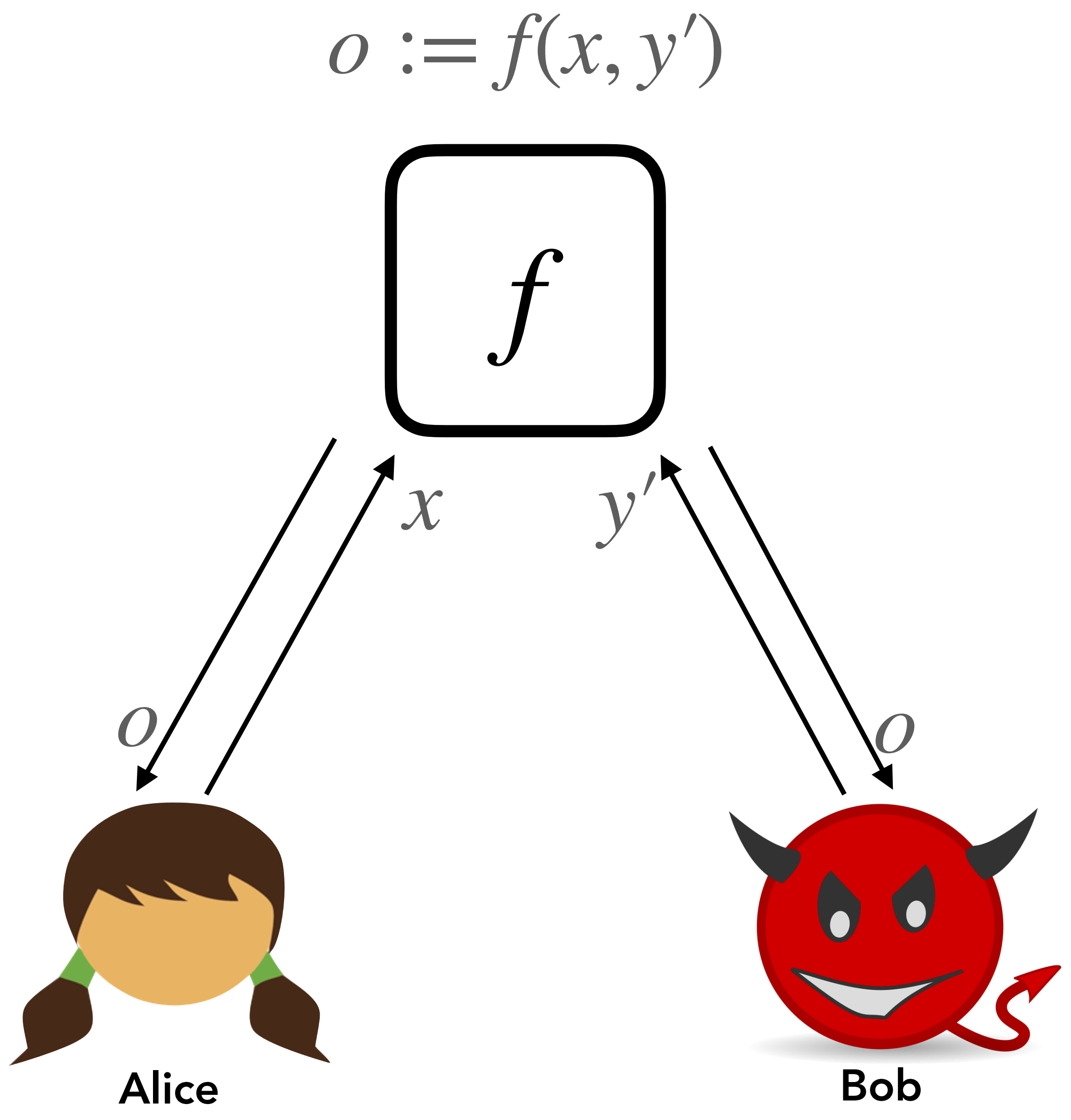
Security with Abort



Fairness



Guaranteed Output Delivery

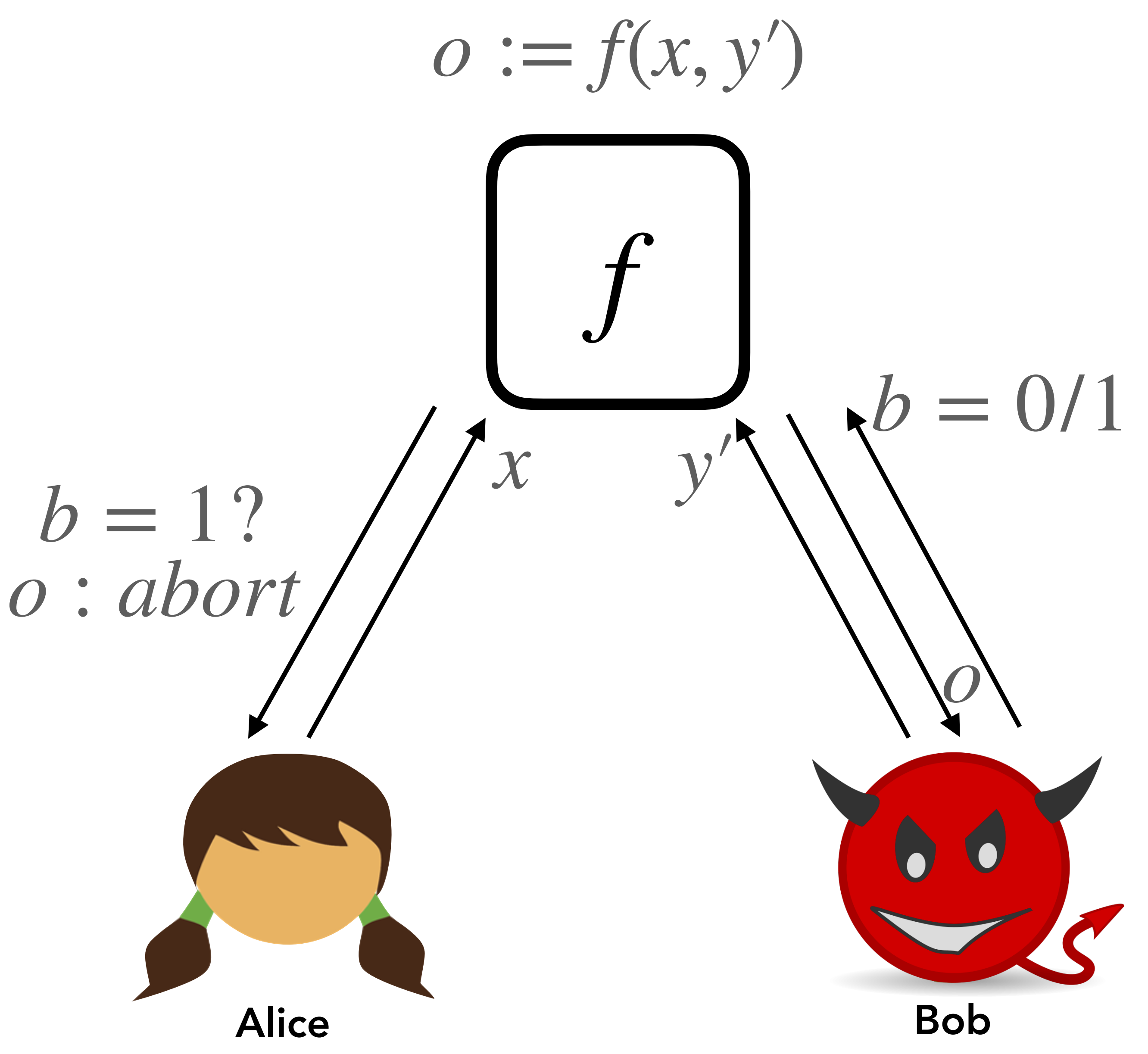


We consider ***active, malicious majority***

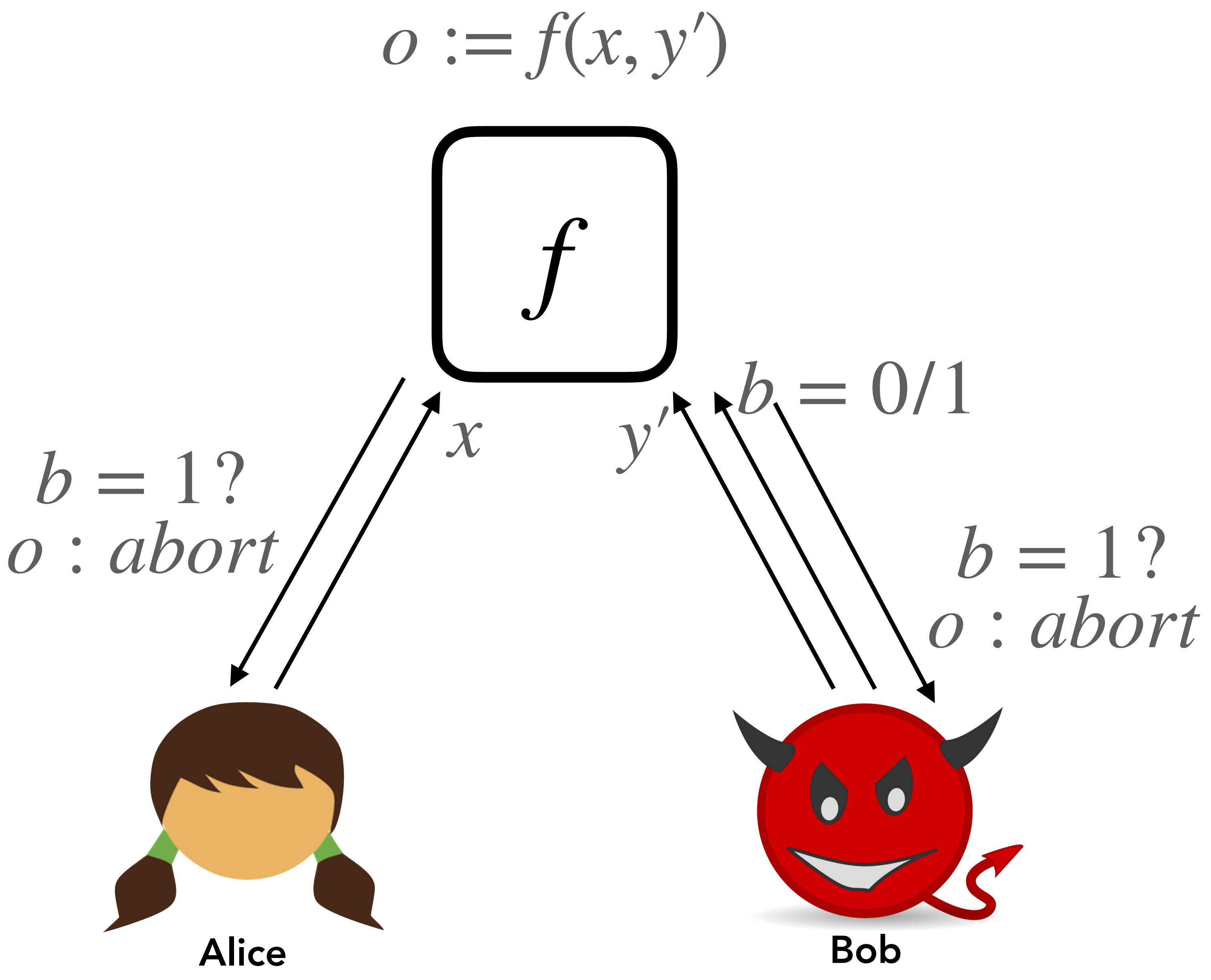
Different Security Levels

Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

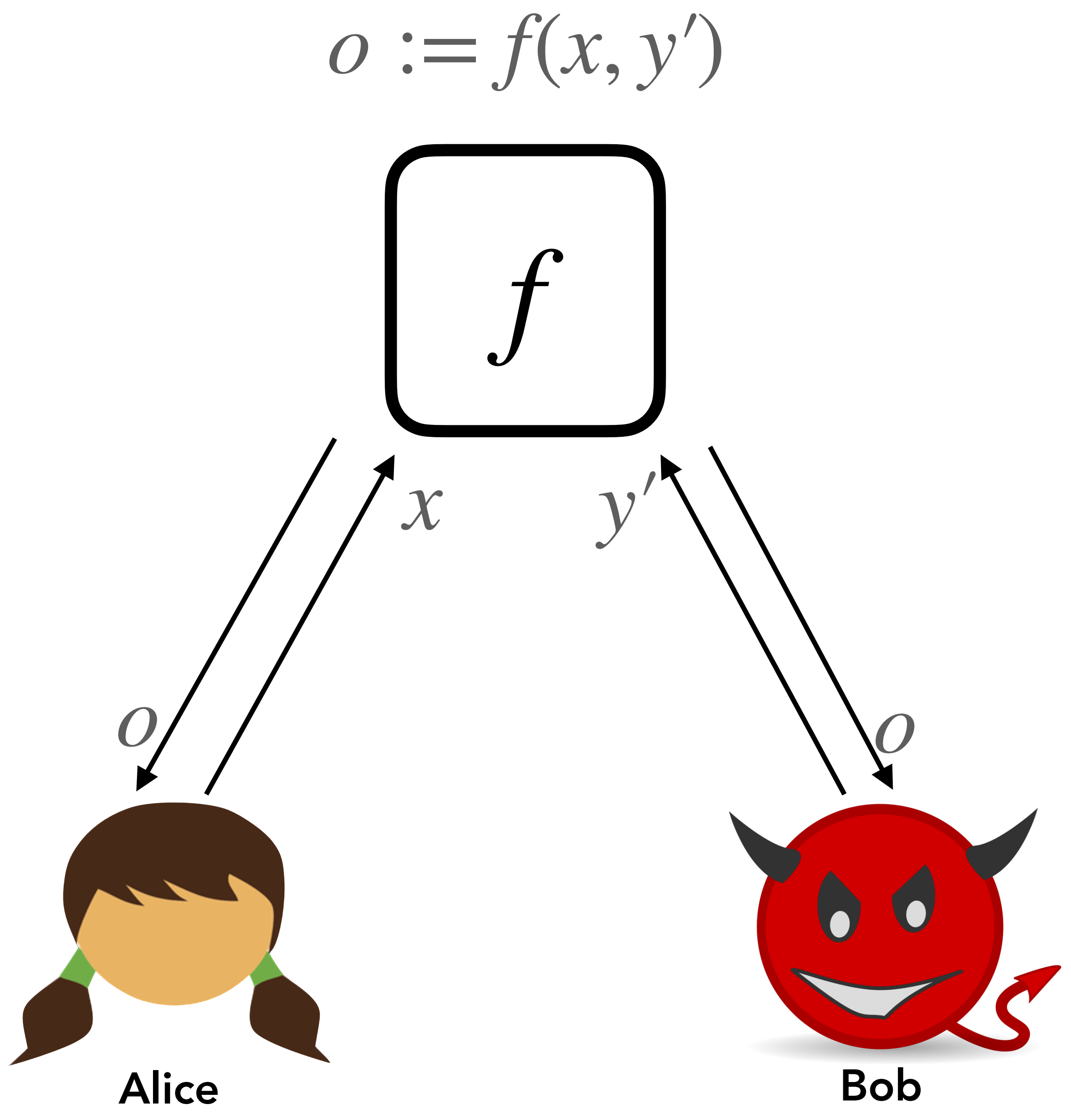
Security with Abort



Fairness



Guaranteed Output Delivery



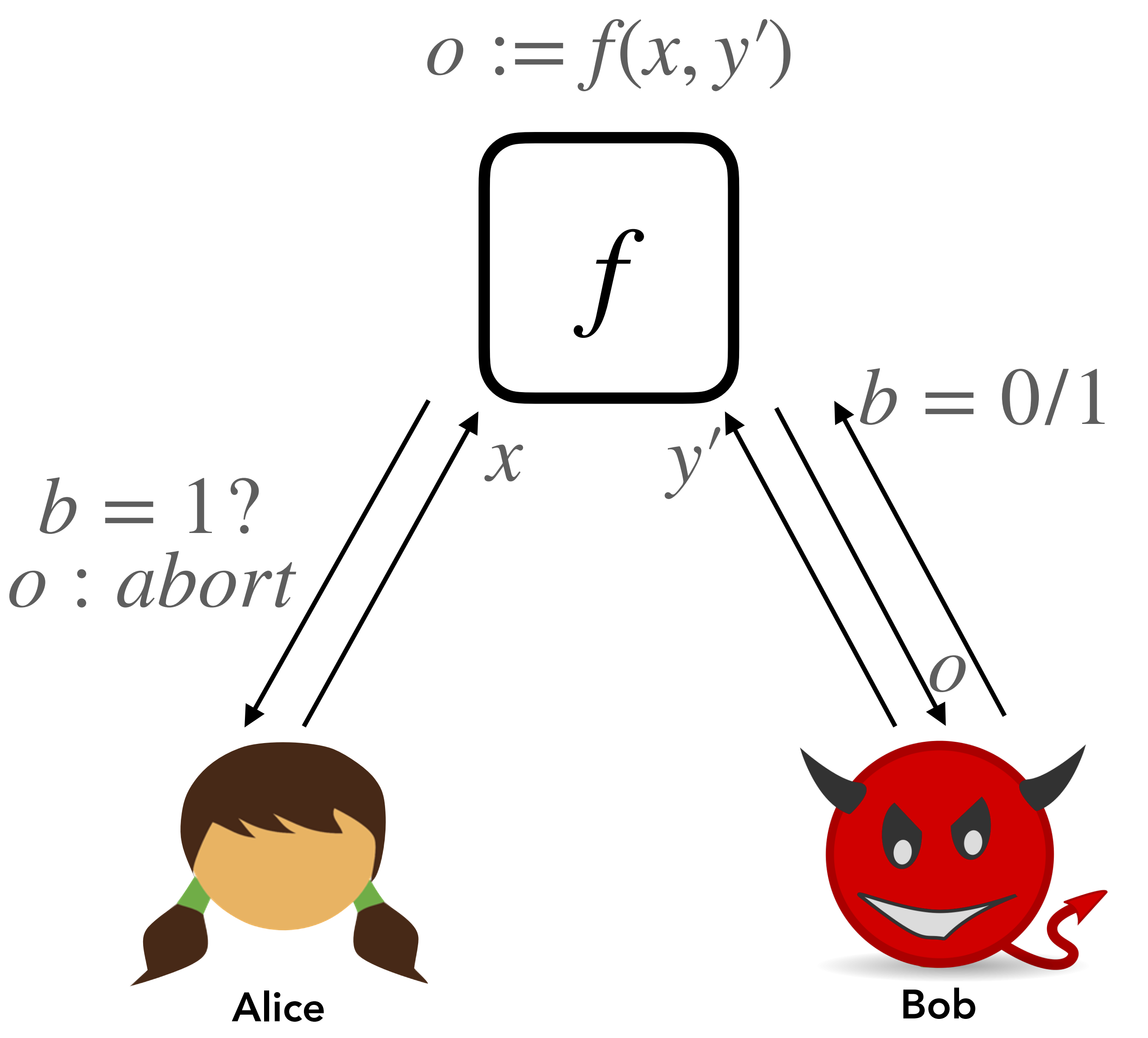
We consider ***active, malicious majority***

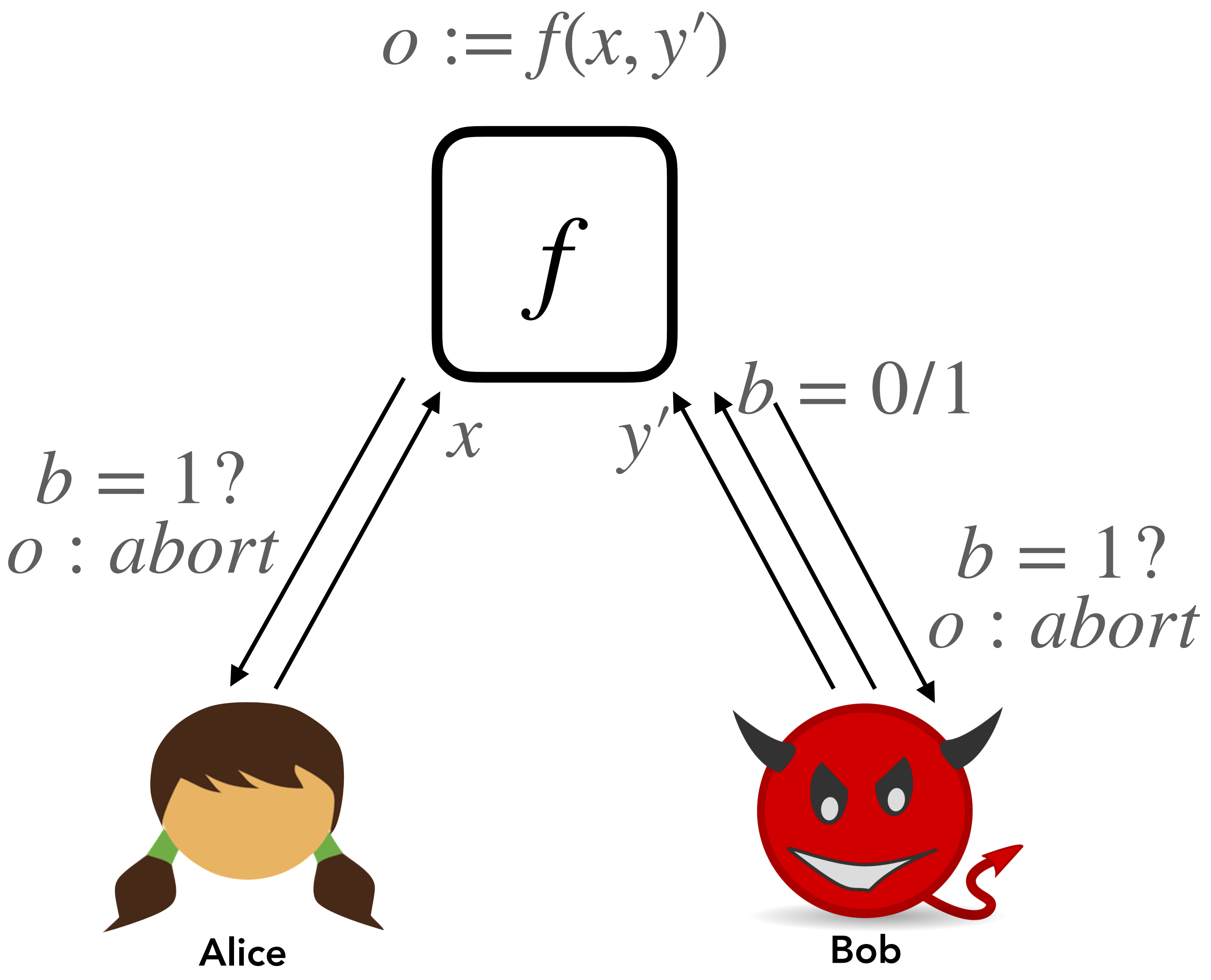
Different Security Levels

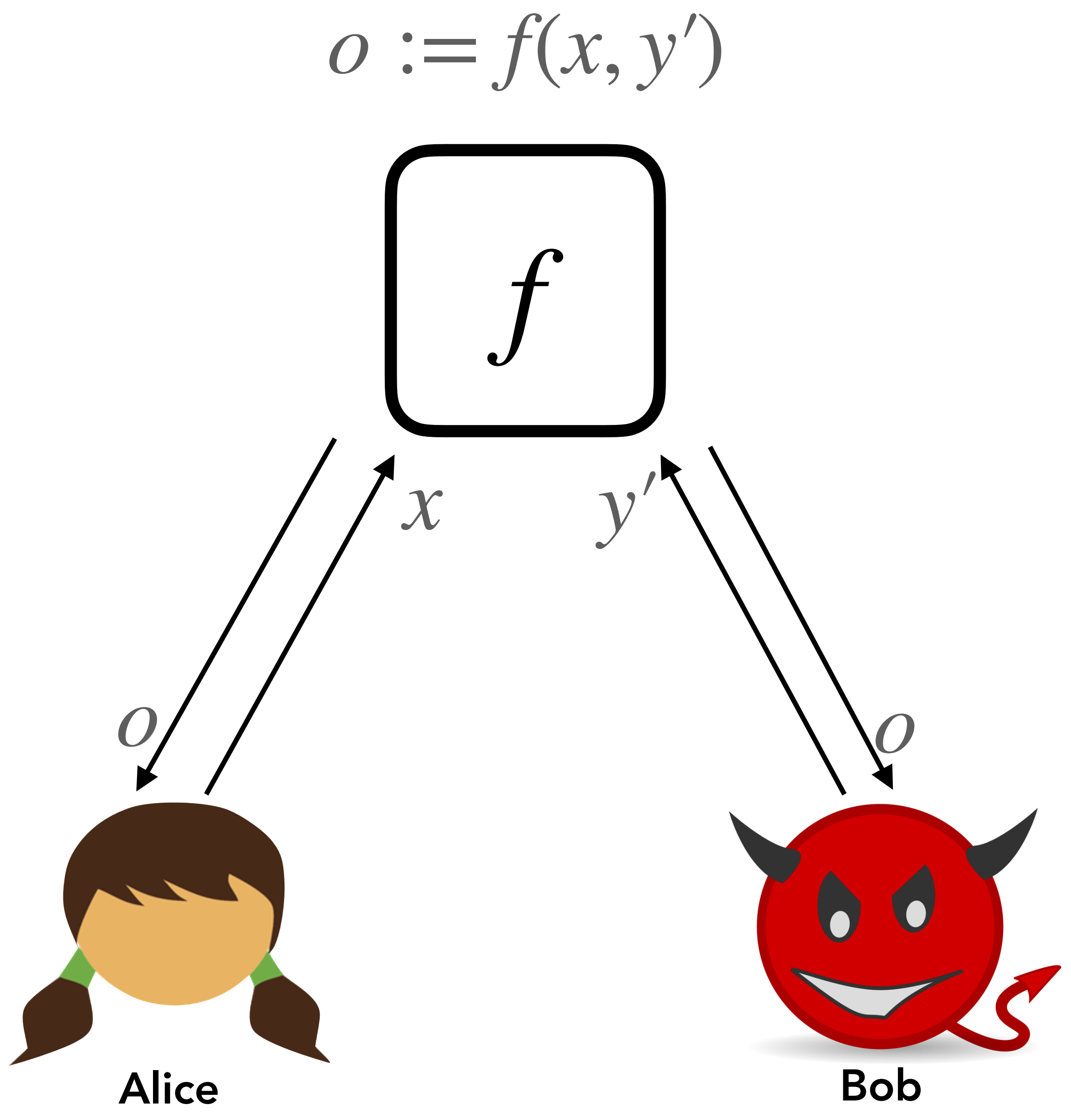
Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

[Cleve86]

Security with Abort	Fairness	Guaranteed Output Delivery
✓	✗	✗







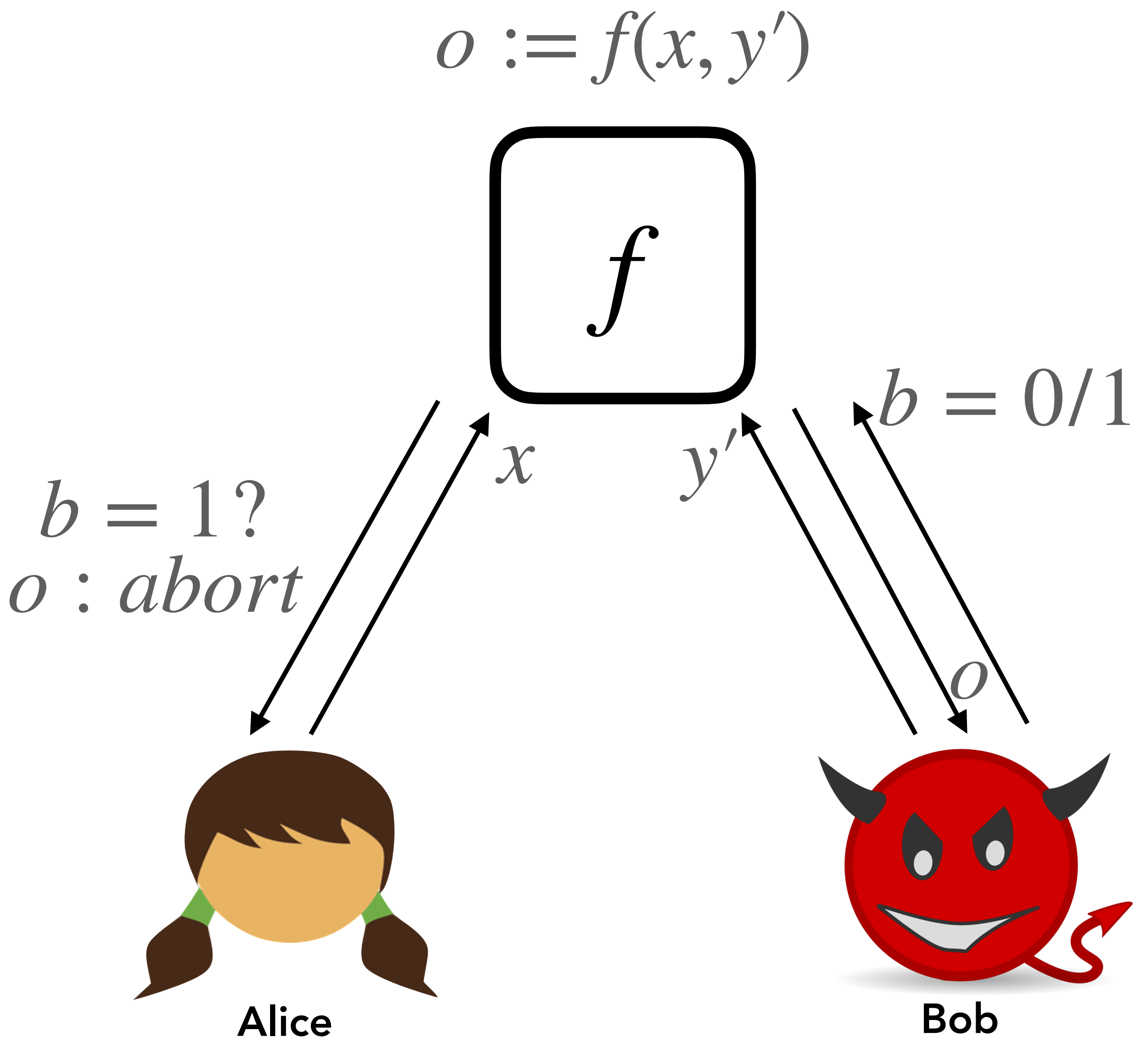
We consider ***active, malicious majority***

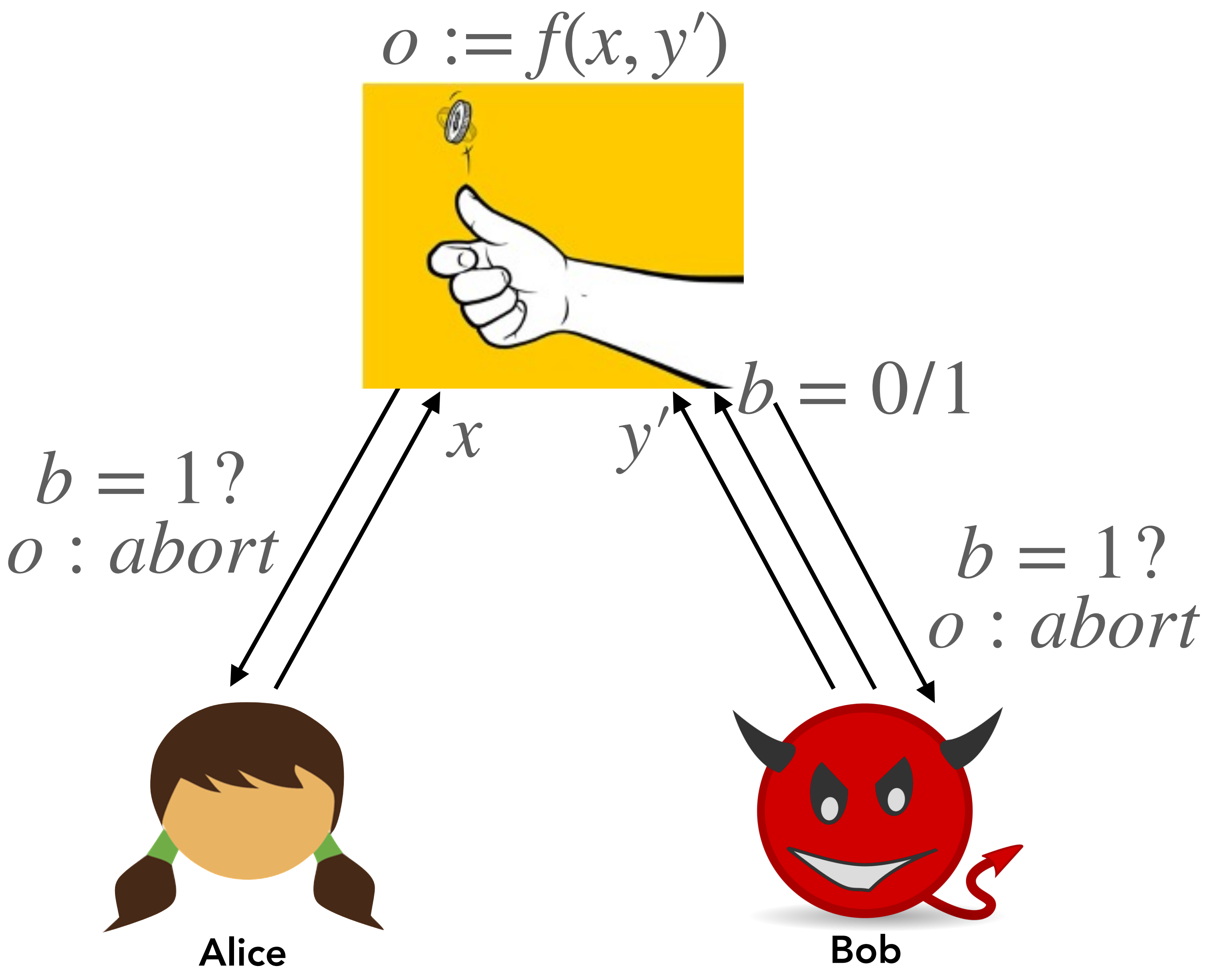
Different Security Levels

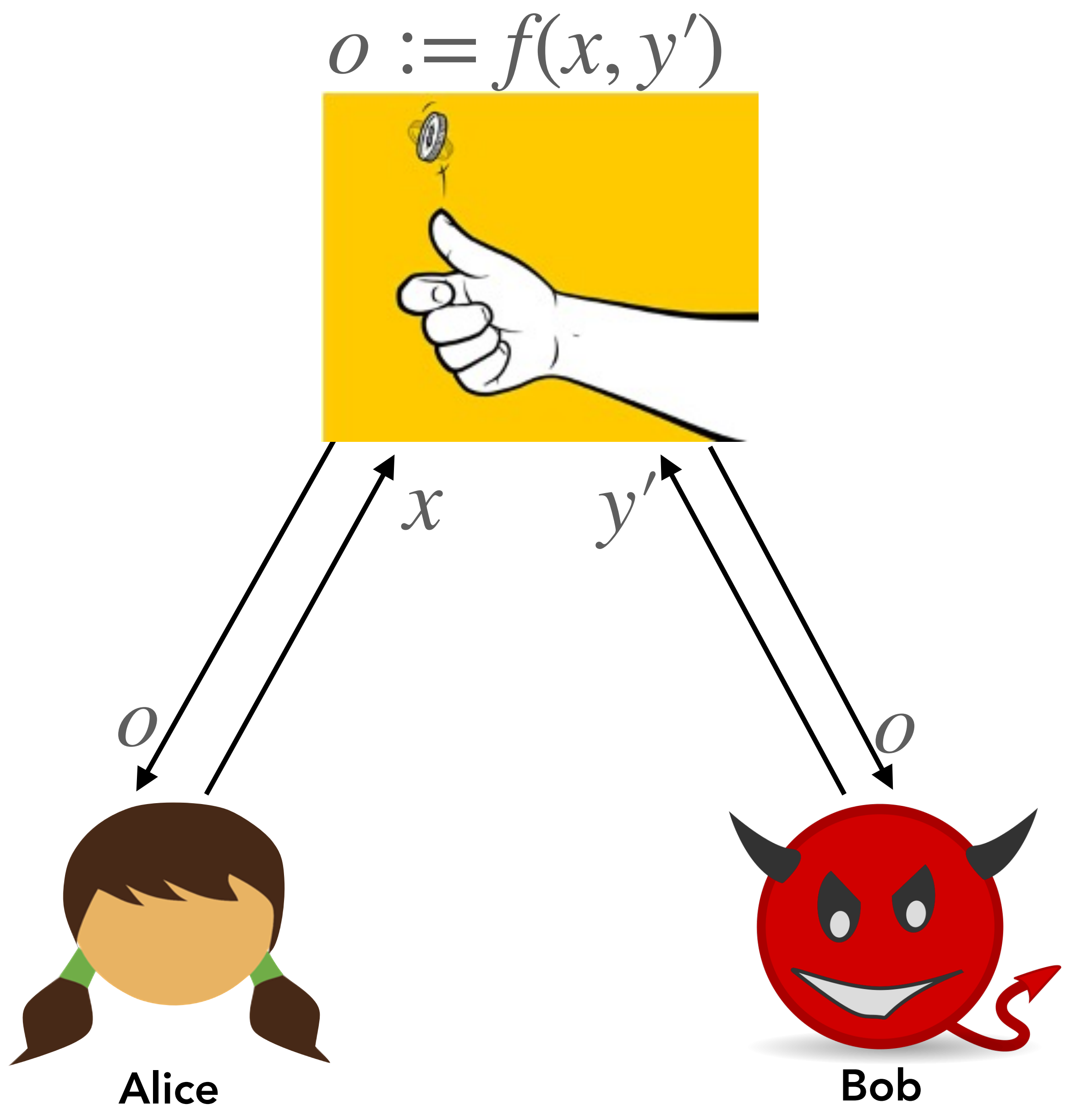
Security with Abort v.s. Fairness v.s. Guaranteed Output Delivery

[Cleve86]

Security with Abort | **Fairness** | **Guaranteed Output Delivery**

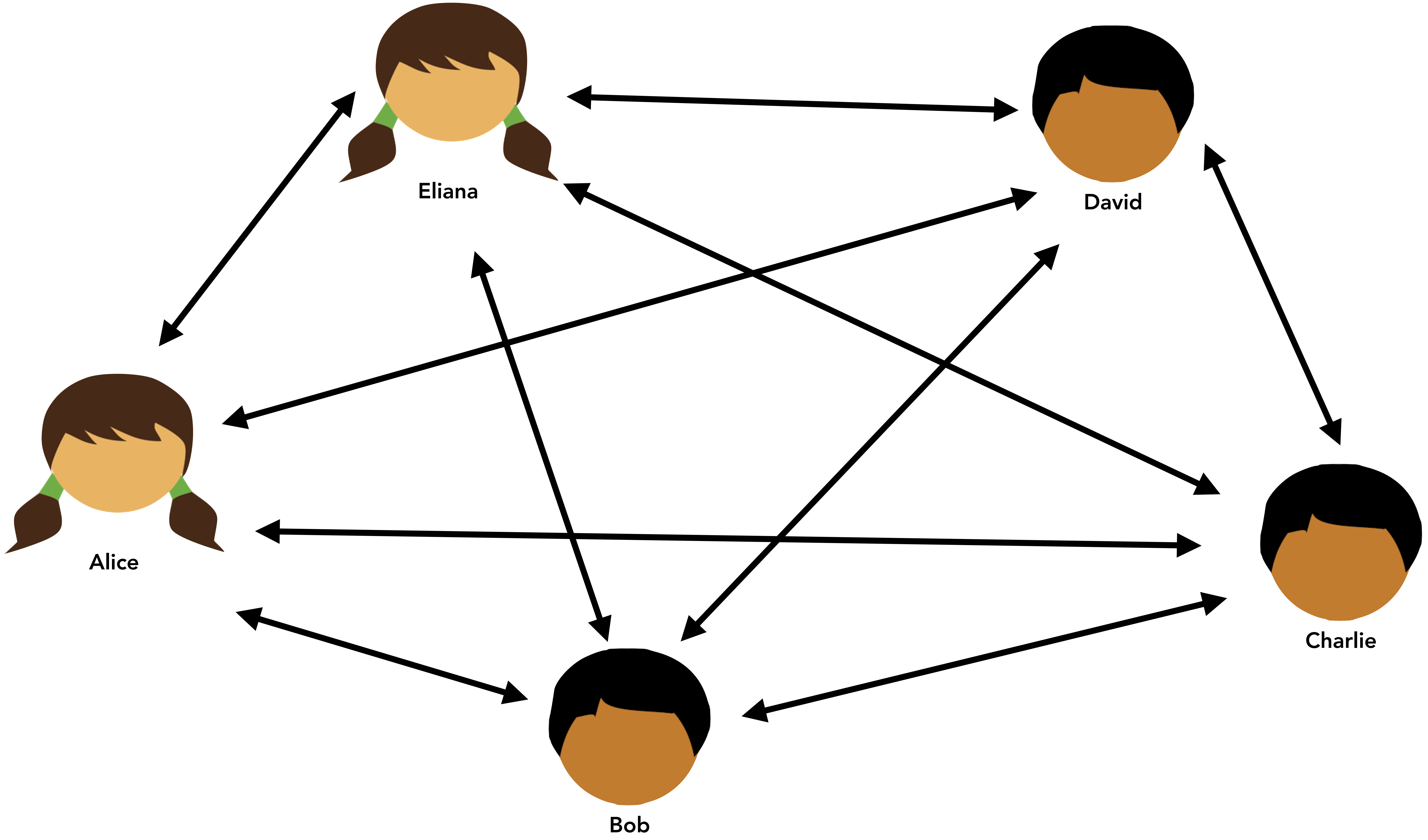






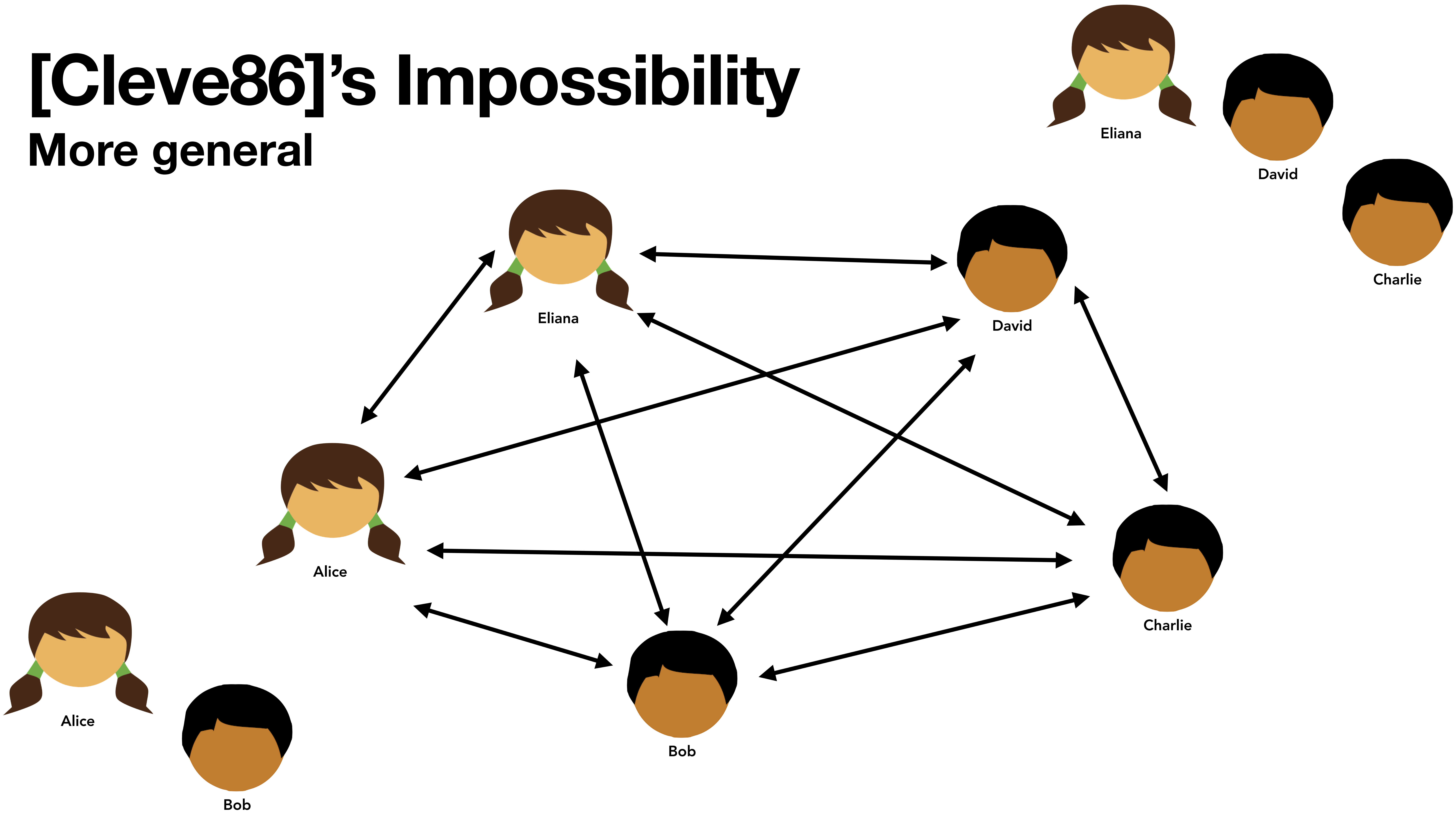
[Cleve86]'s Impossibility

More general



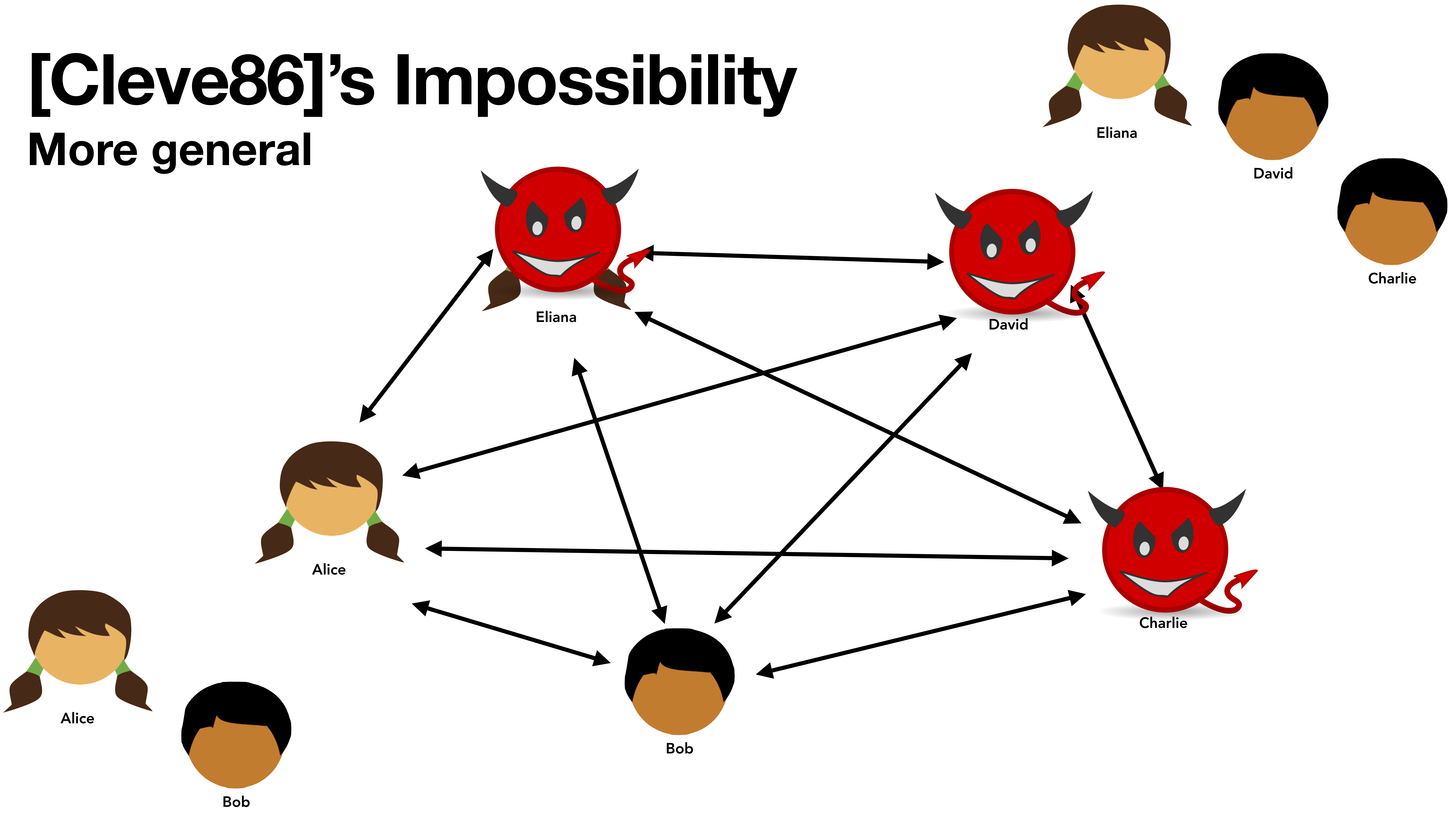
[Cleve86]'s Impossibility

More general



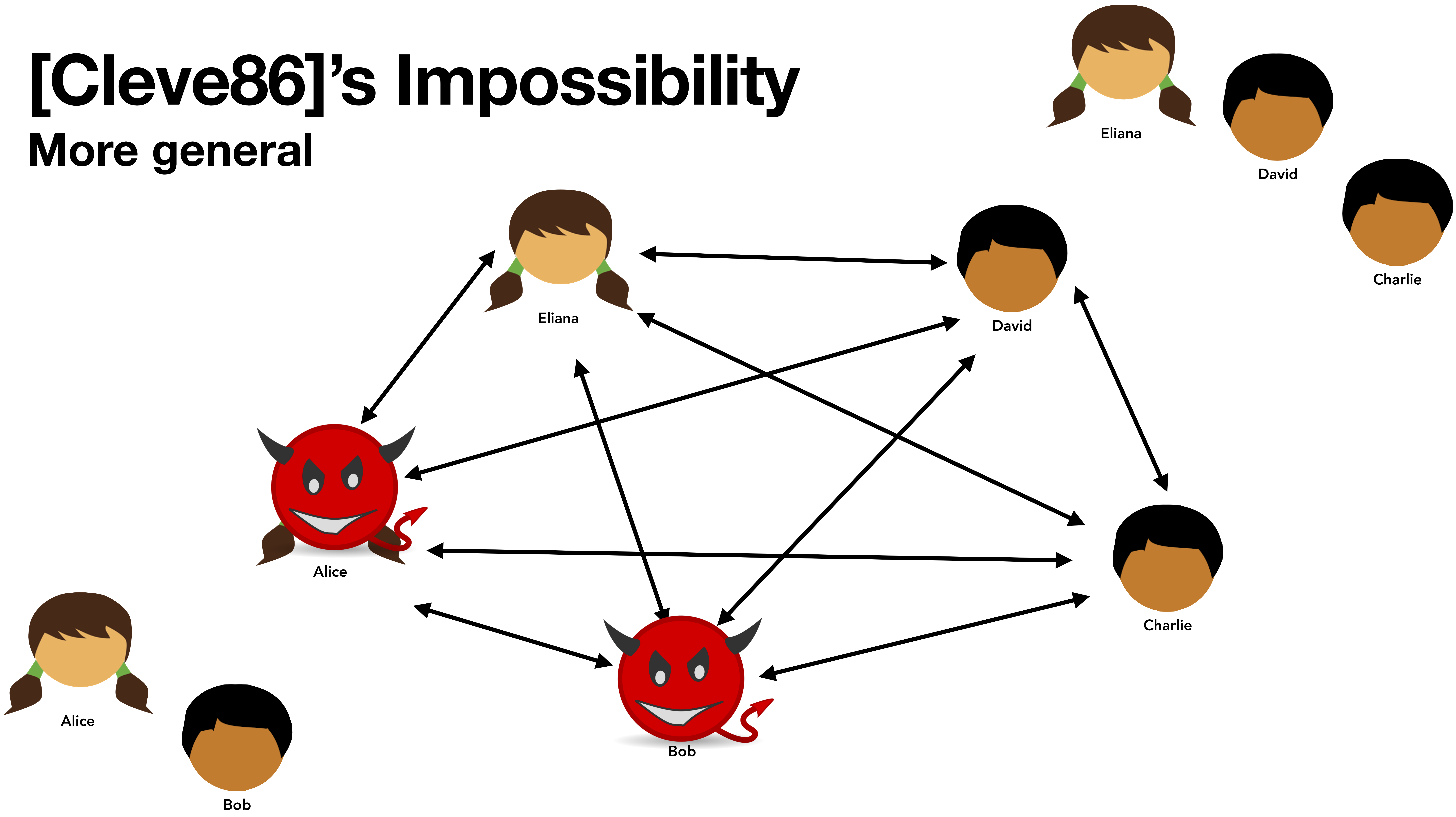
[Cleve86]'s Impossibility

More general



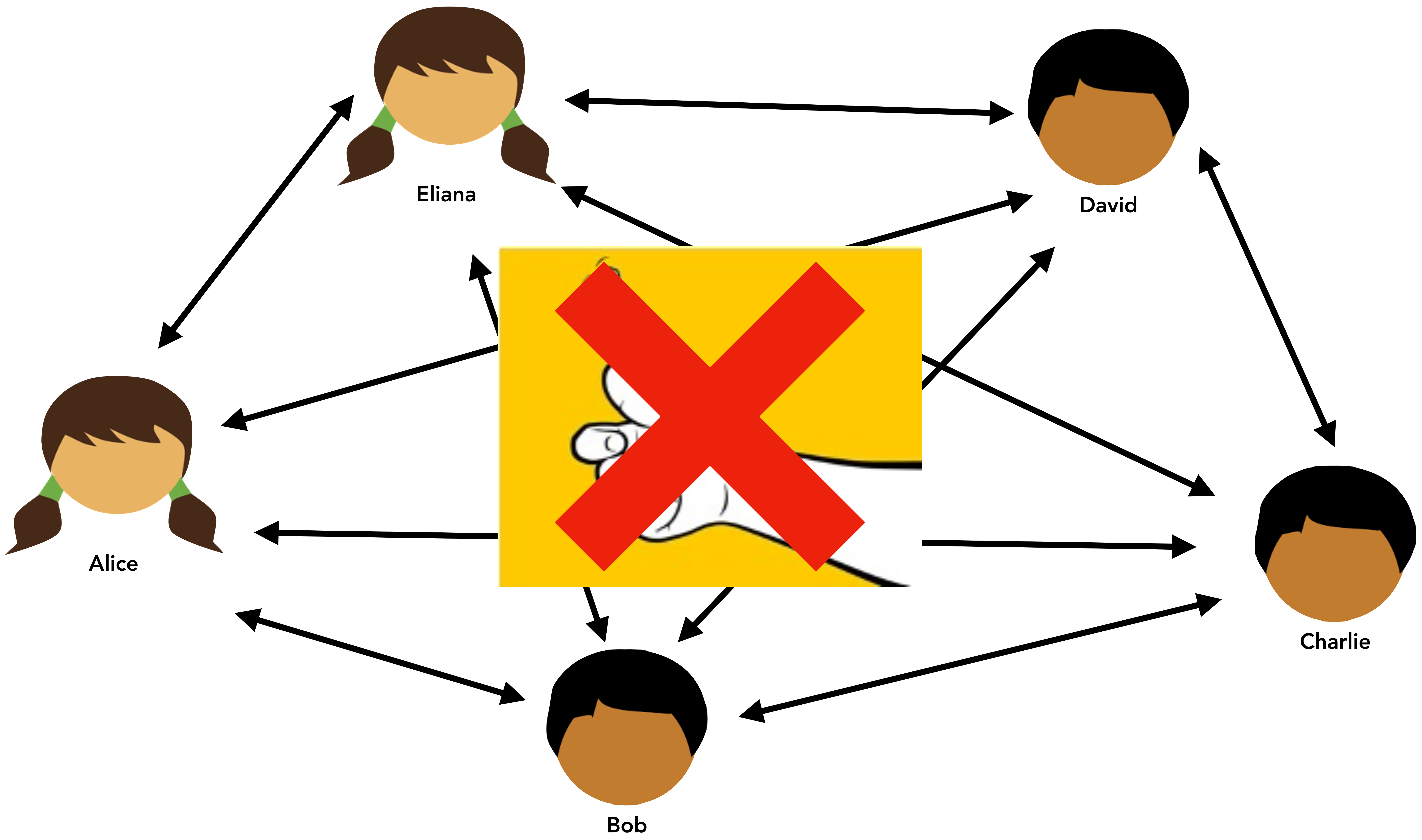
[Cleve86]'s Impossibility

More general



[Cleve86]'s Impossibility

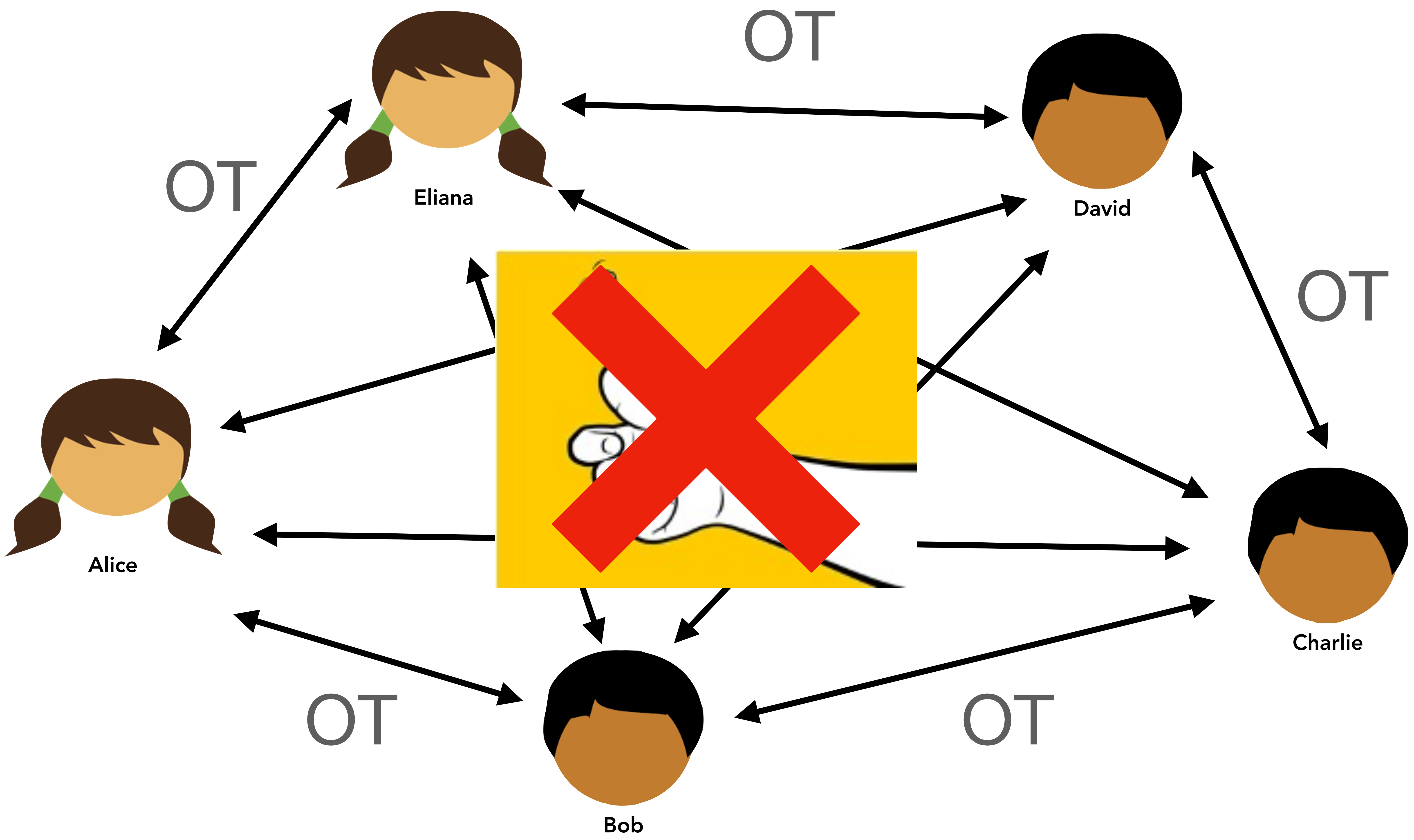
More general



[Cleve86]'s Impossibility

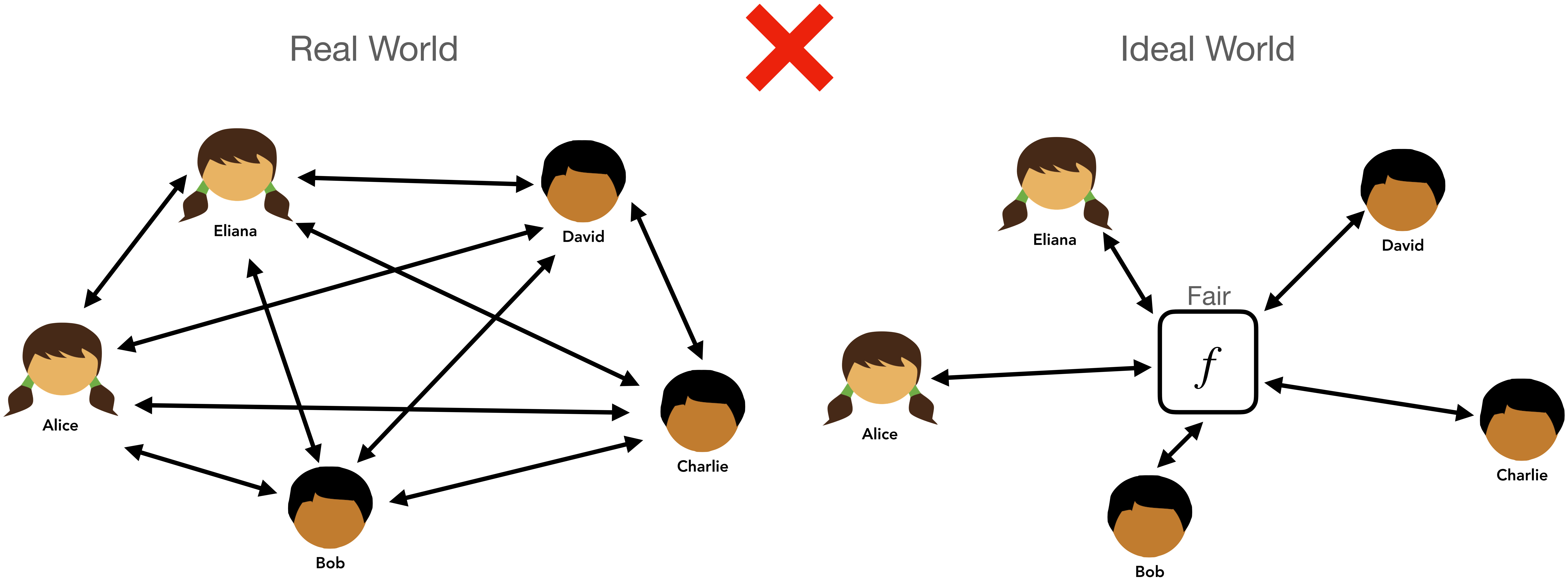
More general

Any one-way channels, e.g, OTs



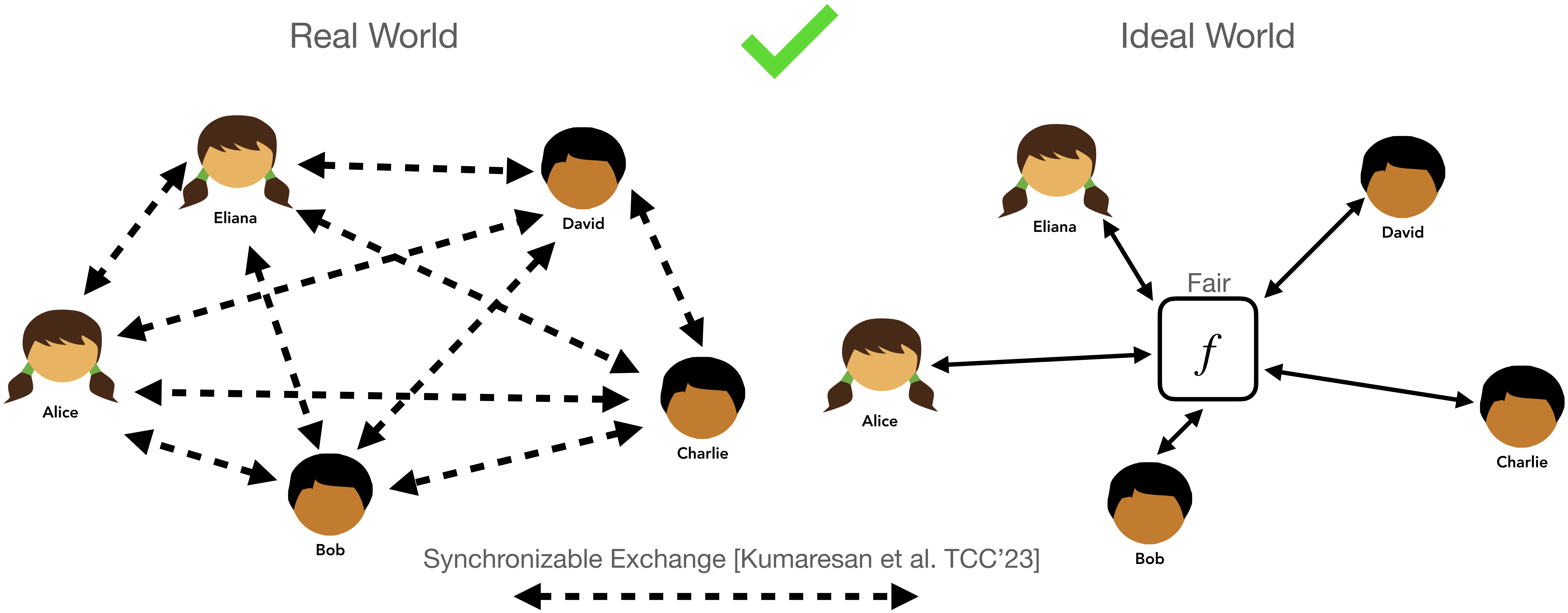
Bypassing [Cleve86] to Achieve Fair MPC

Via augmenting “stronger” communication channels



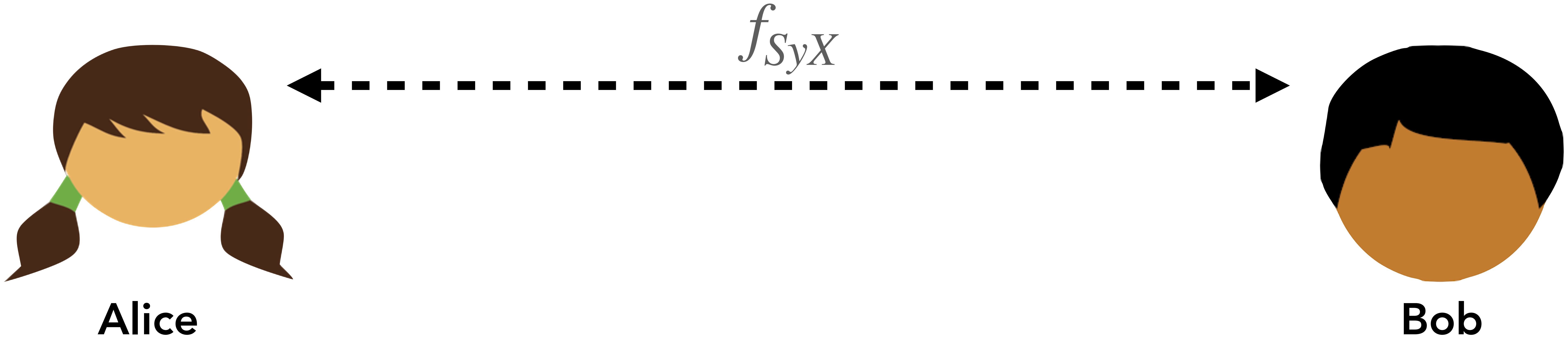
Bypassing [Cleve86] to Achieve Fair MPC

Via augmenting "stronger" communication channels

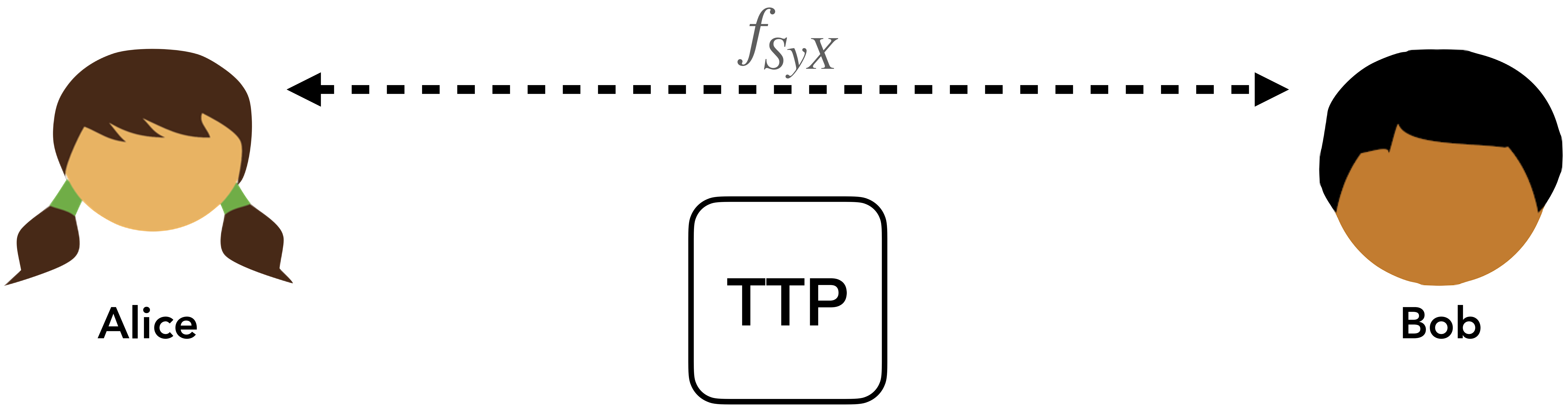


Synchronizable Exchange

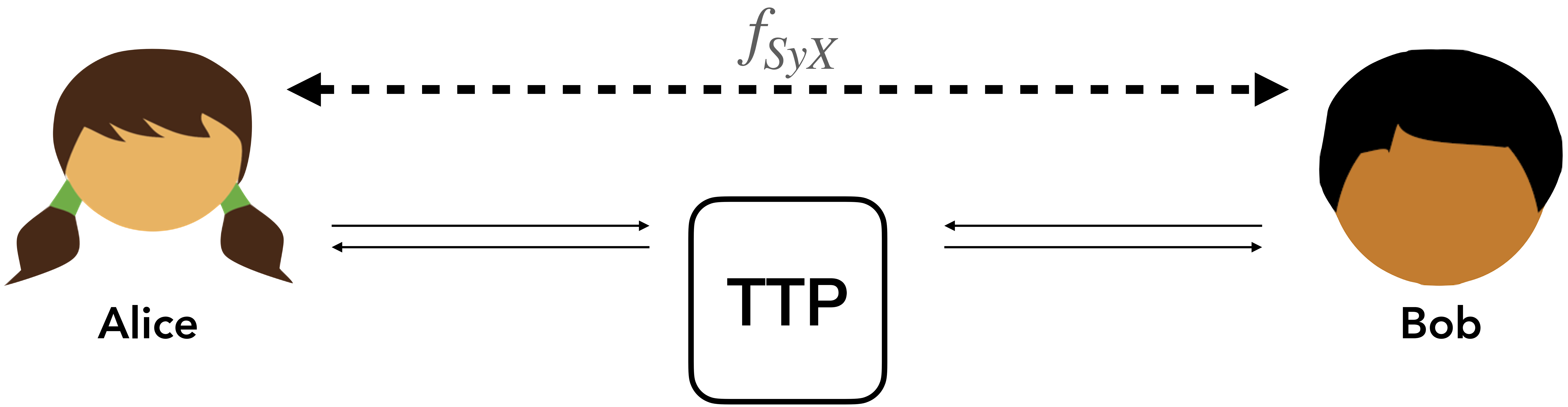
[Kumaresan et al. TCC'23]



Synchronizable Exchange
[Kumaresan et al. TCC'23]

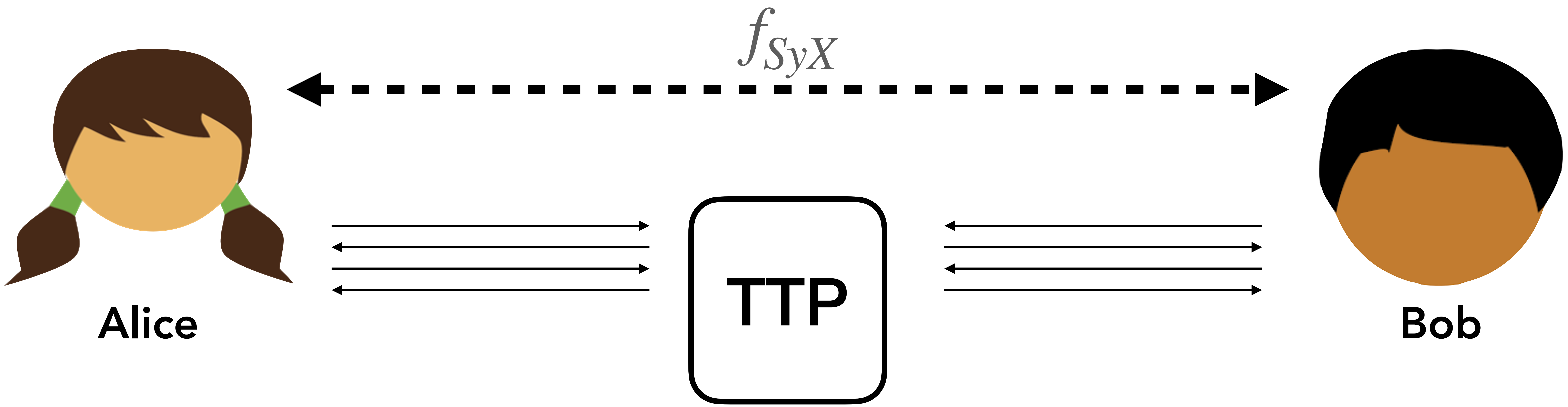


Synchronizable Exchange
[Kumaresan et al. TCC'23]



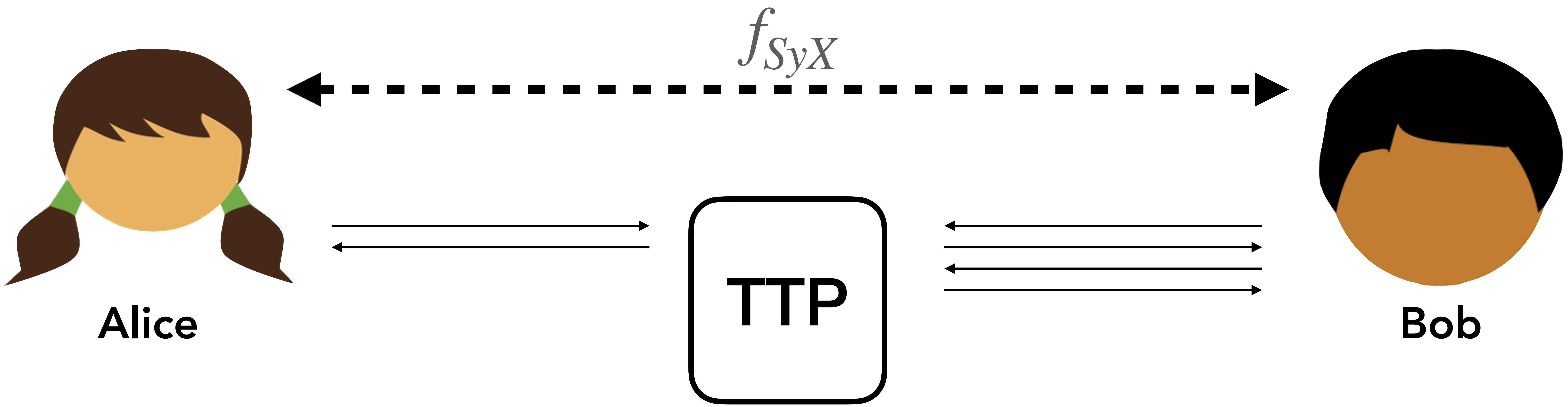
Synchronizable Exchange

[Kumaresan et al. TCC'23]



Synchronizable Exchange

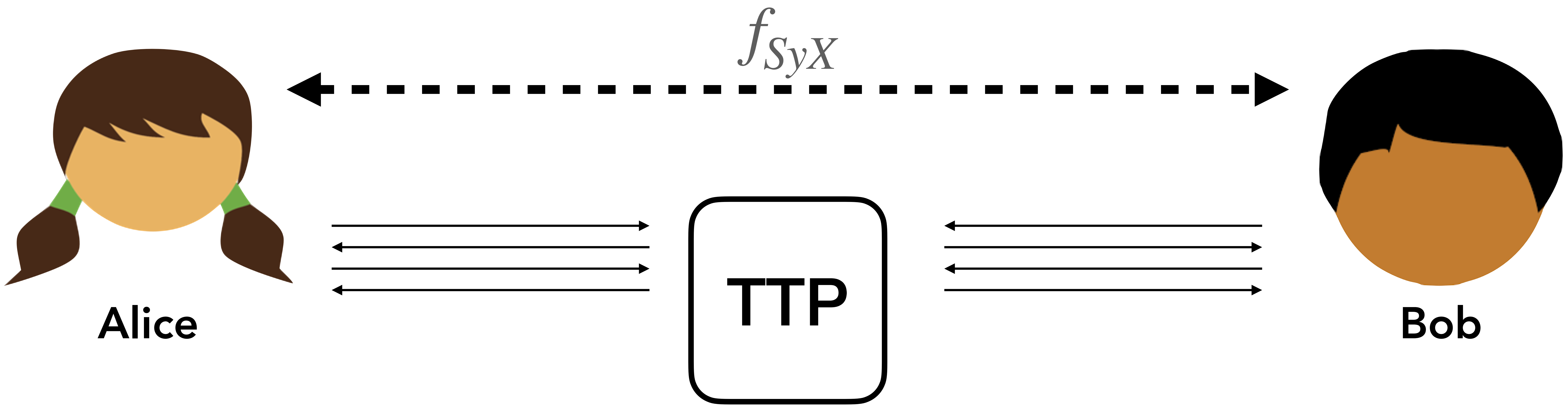
[Kumaresan et al. TCC'23]



Synchronizable Exchange

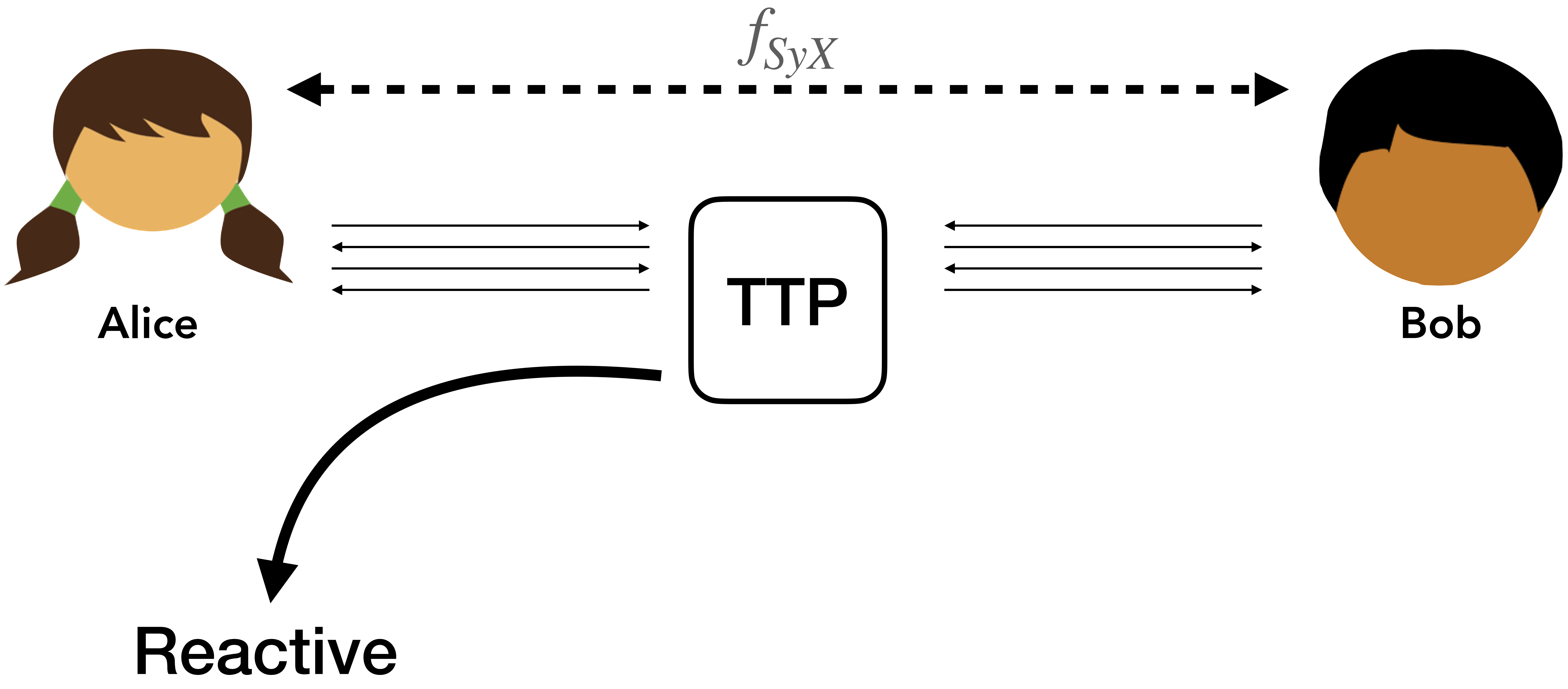
[Kumaresan et al. TCC'23]

No longer a one-way channel



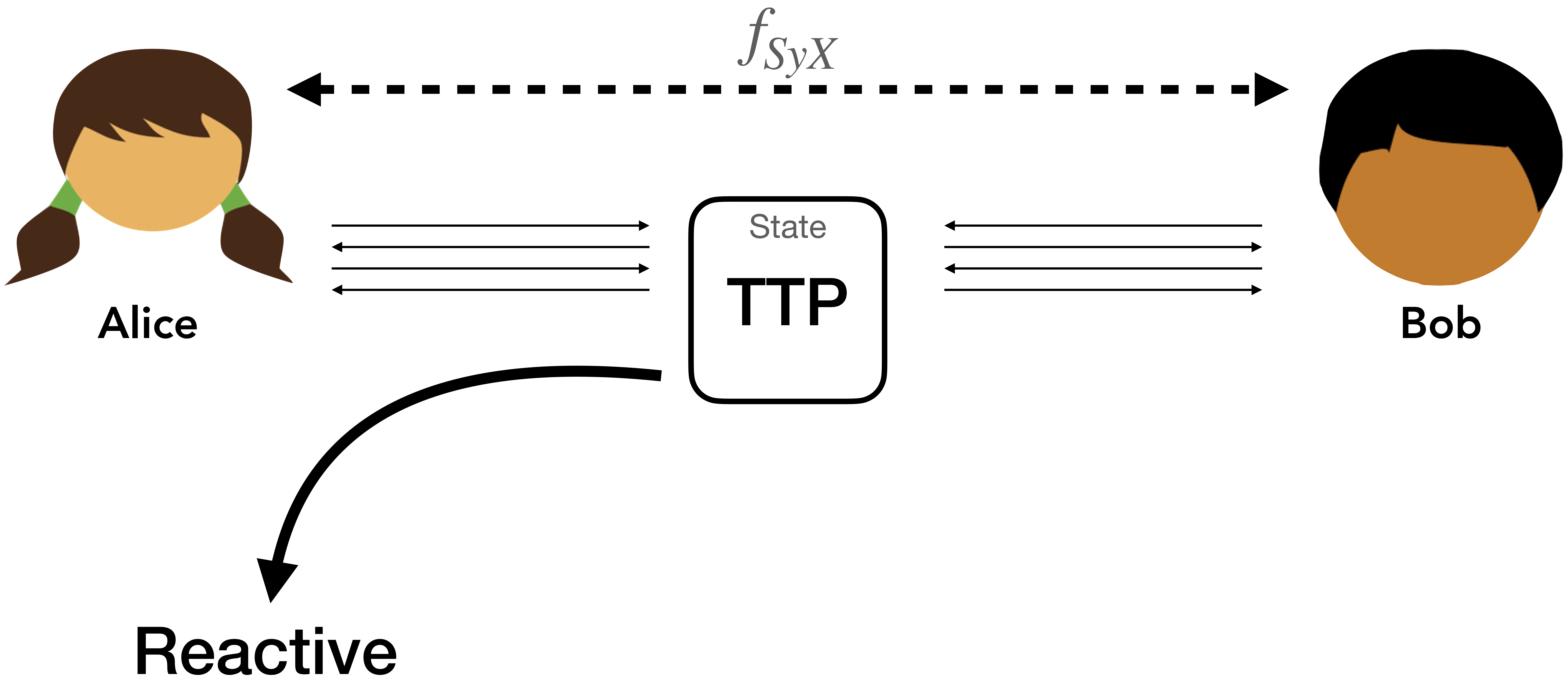
Synchronizable Exchange
[Kumaresan et al. TCC'23]

No longer a one-way channel



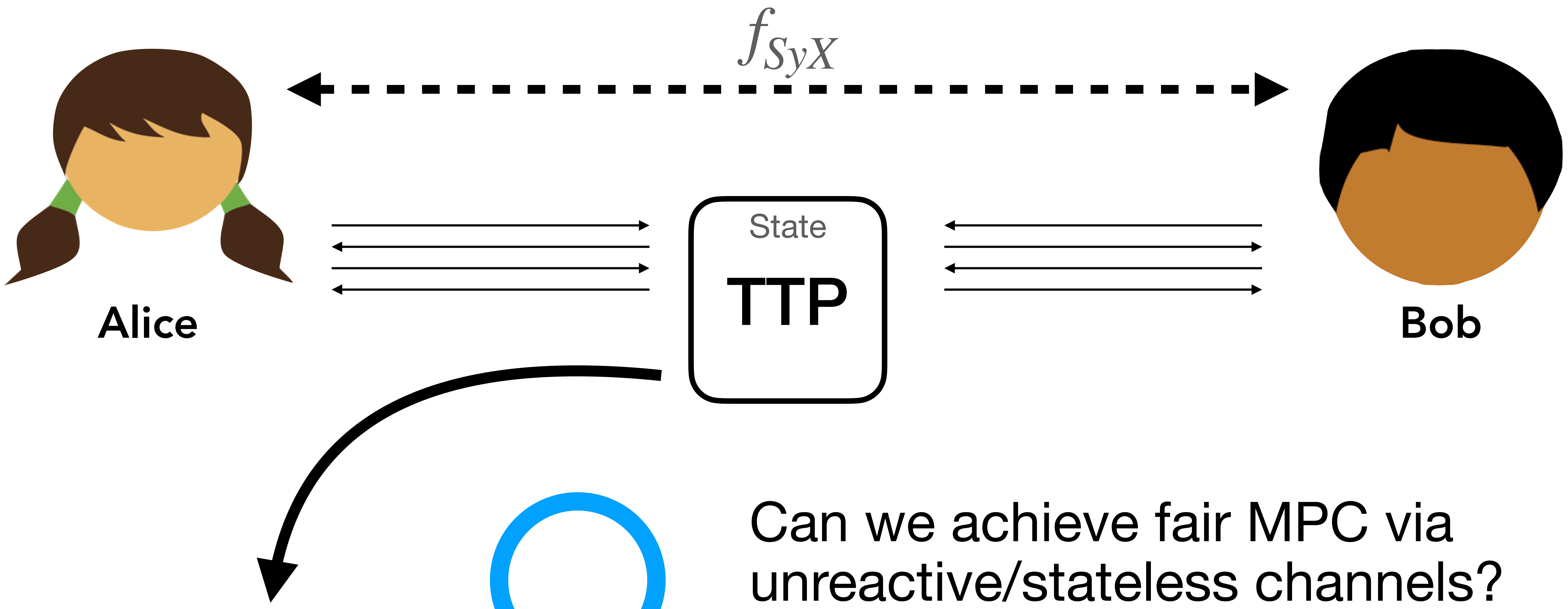
Synchronizable Exchange
[Kumaresan et al. TCC'23]

No longer a one-way channel



Synchronizable Exchange
[Kumaresan et al. TCC'23]

No longer a one-way channel



Reactive

Can we achieve fair MPC via unreactive/stateless channels?

Just how fair is an unreactive world?

Just How Fair is an Unreactive World?

Just How Fair is an Unreactive World?

We completely address this question.

Just How Fair is an Unreactive World?

We completely address this question.
$t =$ #corruption, $n =$ #party

Just How Fair is an Unreactive World?

We completely address this question.
t = #corruption, n = #party

Table 1: Our contributions.

t	Insufficient functionalities for fair coin tossing	Sufficient functionalities for fair MPC
$t < \frac{n}{2}$	–	Local computation [FGMvR02]
$t = \frac{n}{2}$	Local computation [Cle86]	2-wise fair exchange **[ours]**
$t > \frac{n}{2}$	Arbitrary unreactive t-wise **[ours]**	$(t+1)$-wise fair exchange[a] **[ours]**

Just How Fair is an Unreactive World?

We completely address this question.
t = #corruption, n = #party

Not very fair ☹

Table 1: Our contributions.

t	**Insufficient functionalities for fair coin tossing**	**Sufficient functionalities for fair MPC**
$t < \frac{n}{2}$	–	Local computation [FGMvR02]
$t = \frac{n}{2}$	Local computation [Cle86]	2-wise fair exchange [**ours**]
$t > \frac{n}{2}$	Arbitrary unreactive t-wise [**ours**]	$(t+1)$-wise fair exchange[a] [**ours**]

Just How Fair is an Unreactive World?

We completely address this question.
t = #corruption, n = #party

Not very fair ☹

Table 1: Our contributions.

t	**Insufficient functionalities for fair coin tossing**	**Sufficient functionalities for fair MPC**
$t < \frac{n}{2}$	–	Local computation [FGMvR02]
$t = \frac{n}{2}$	Local computation [Cle86]	2-wise fair exchange **[ours]**
$t > \frac{n}{2}$	Arbitrary unreactive t-wise **[ours]**	$(t+1)$-wise fair exchange[a] **[ours]**

[Cohen and Lindel, Asiacrypt 14]:

1. Fairness with broadcast →Fairness without broadcast
2. No G.O.D. with broadcast →No fairness (even) with broadcast

Just How Fair is an Unreactive World?

We completely address this question.
t = #corruption, n = #party

Not very fair ☹

Table 1: Our contributions.

t	**Insufficient functionalities for fair coin tossing**	**Sufficient functionalities for fair MPC**
$t < \frac{n}{2}$	–	Local computation [FGMvR02]
$t = \frac{n}{2}$	Local computation [Cle86]	2-wise fair exchange [**ours**]
$t > \frac{n}{2}$	Arbitrary unreactive t-wise [**ours**]	$(t+1)$-wise fair exchange[a] [**ours**]

[Cohen and Lindel, Asiacrypt 14]:

1. Fairness with broadcast → Fairness without broadcast
2. No G.O.D. with broadcast → No fairness (even) with broadcast

Example: Our Upper Bound

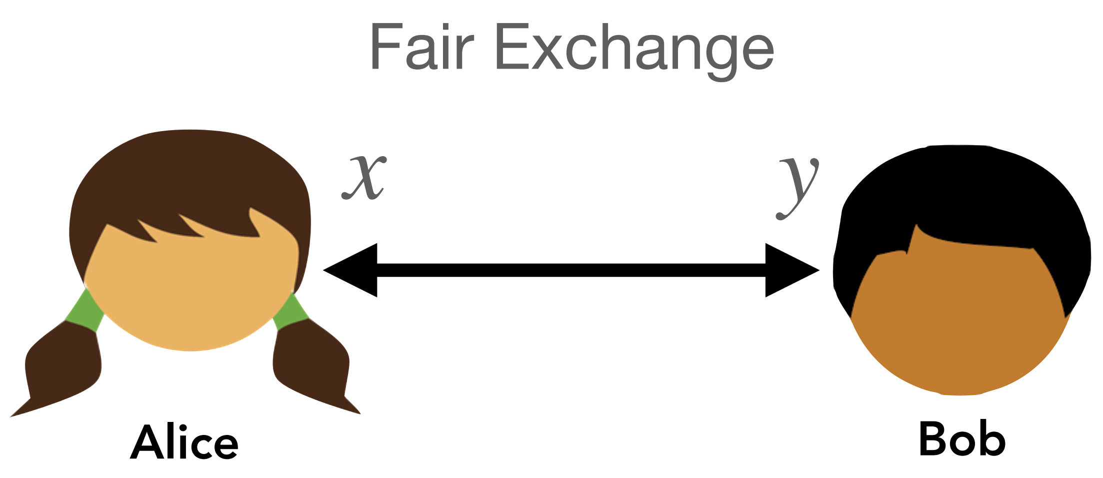
$t = \frac{n}{2}, 2$**-wise fair exchange**

Example: Our Upper Bound

$t = \frac{n}{2}, 2$**-wise fair exchange**

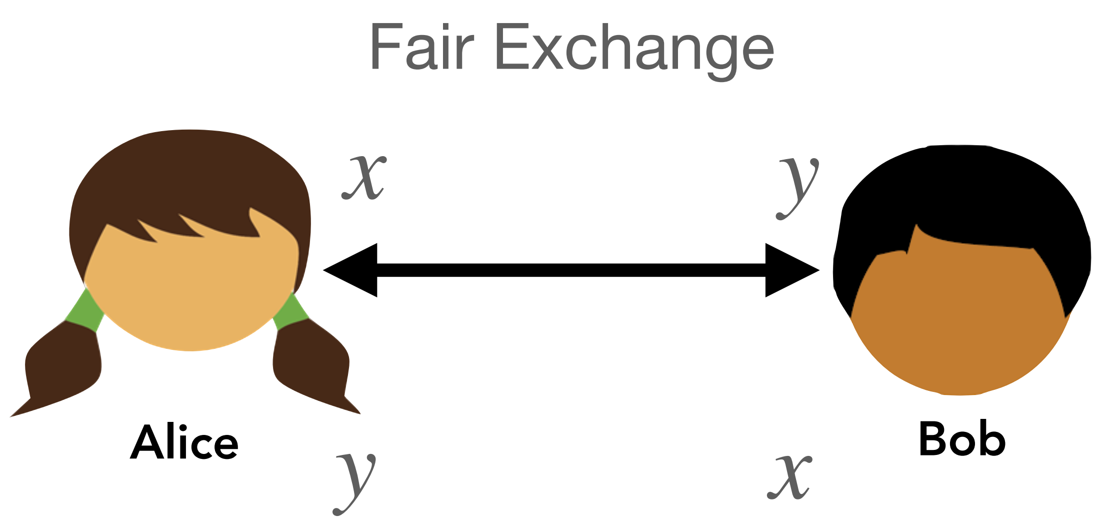
Example: Our Upper Bound

$t = \frac{n}{2}, 2$-wise fair exchange



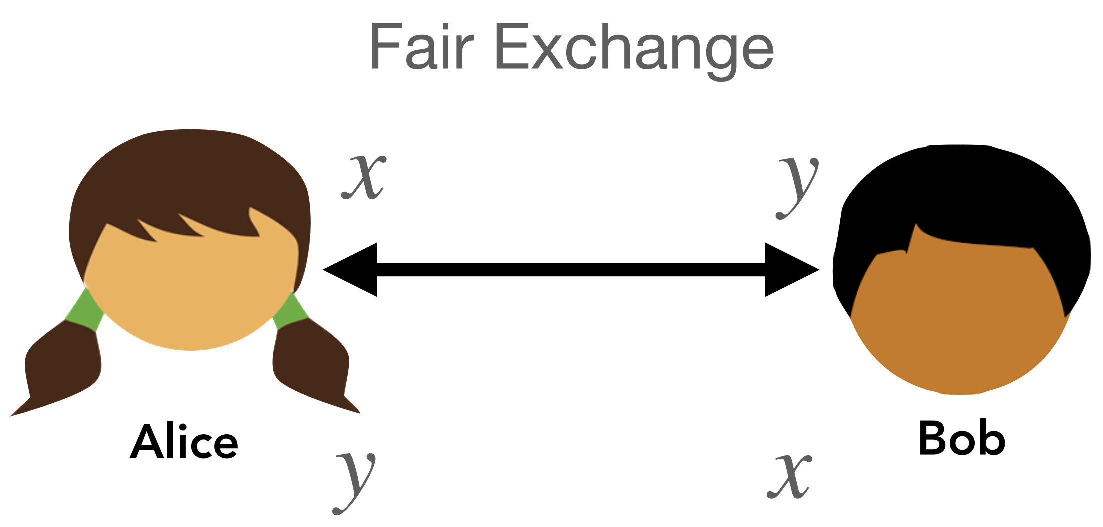
Example: Our Upper Bound

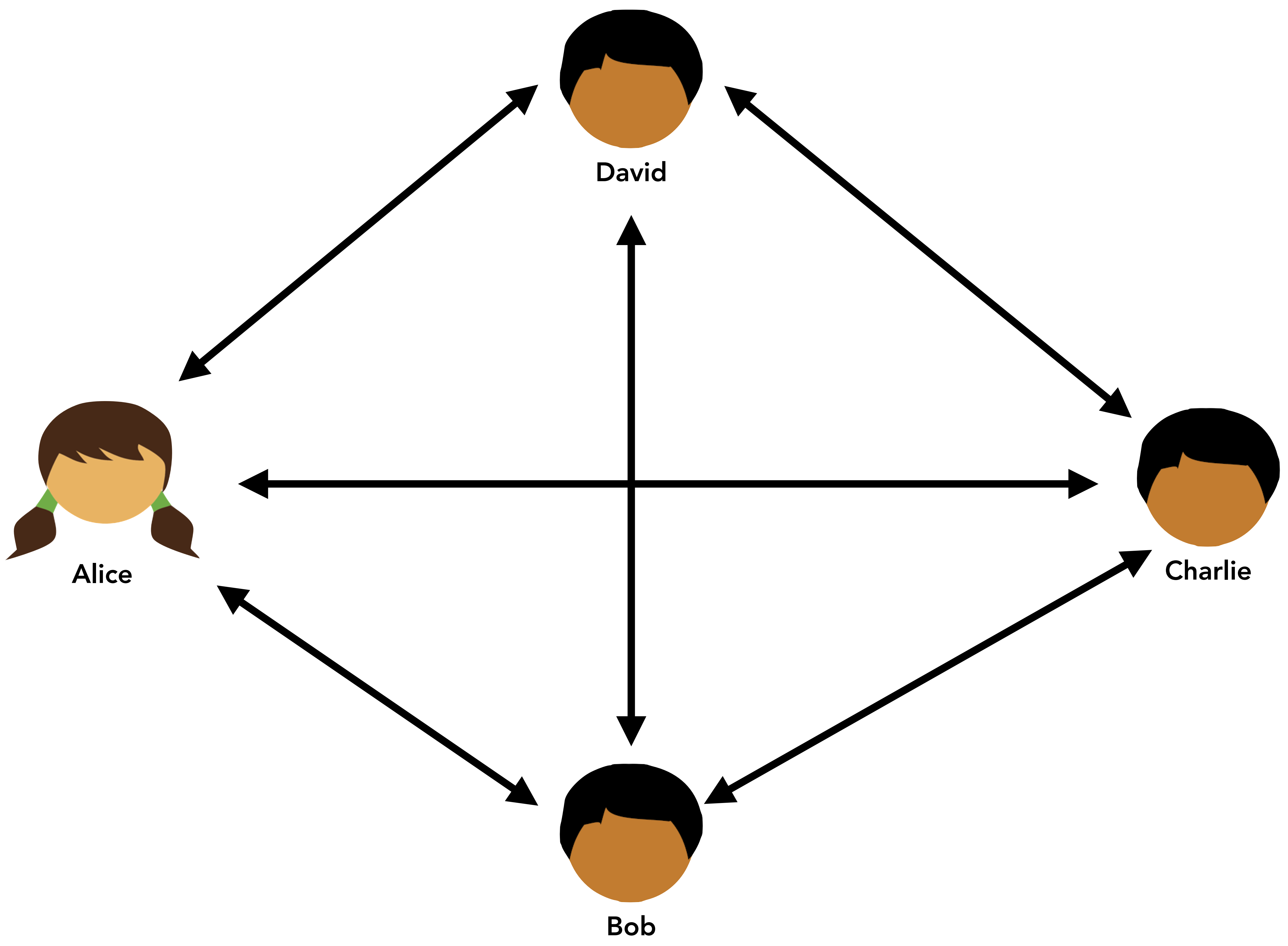
$t = \frac{n}{2}$, 2-**wise fair exchange**



Example: Our Upper Bound

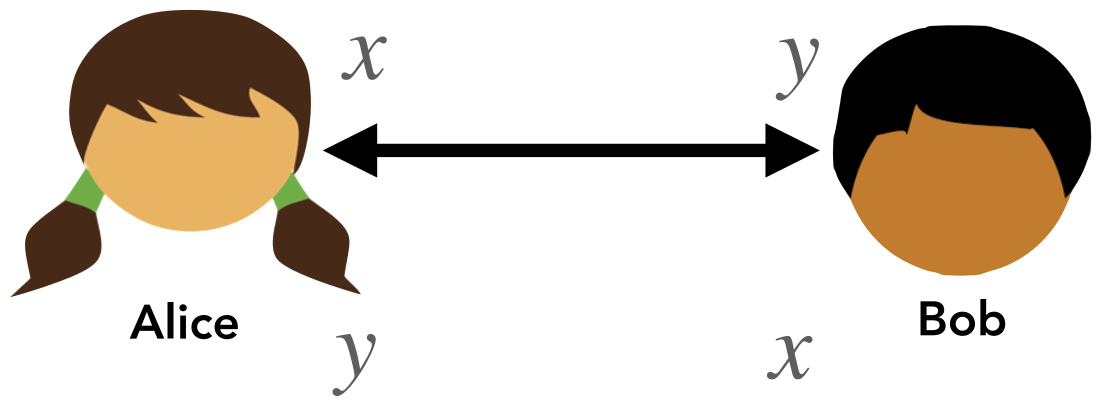
$t = \frac{n}{2}$, 2-wise fair exchange, $n = 4$

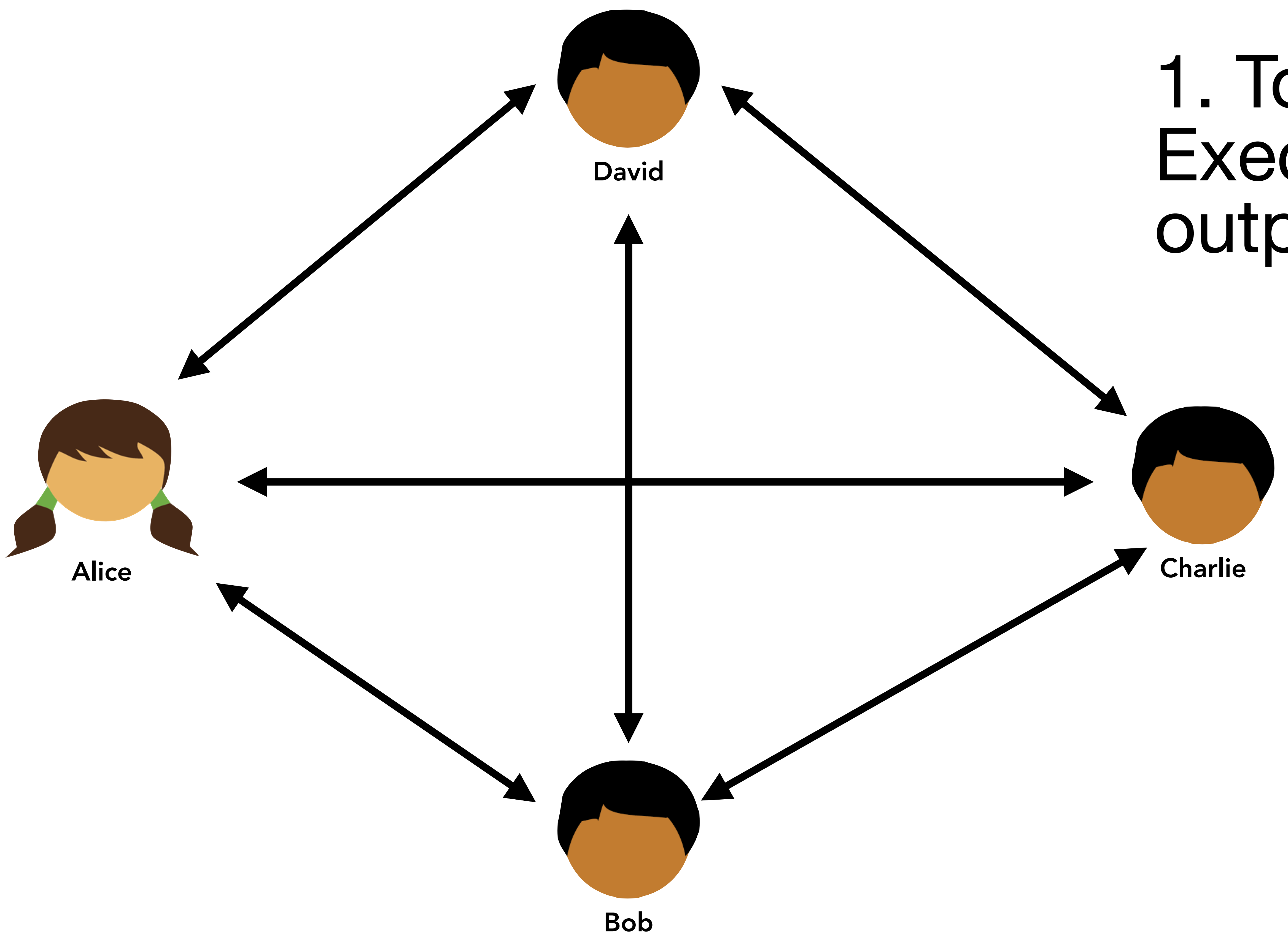




Example: Our Upper Bound

$t = \frac{n}{2}$, 2-**wise fair exchange,** $n = 4$

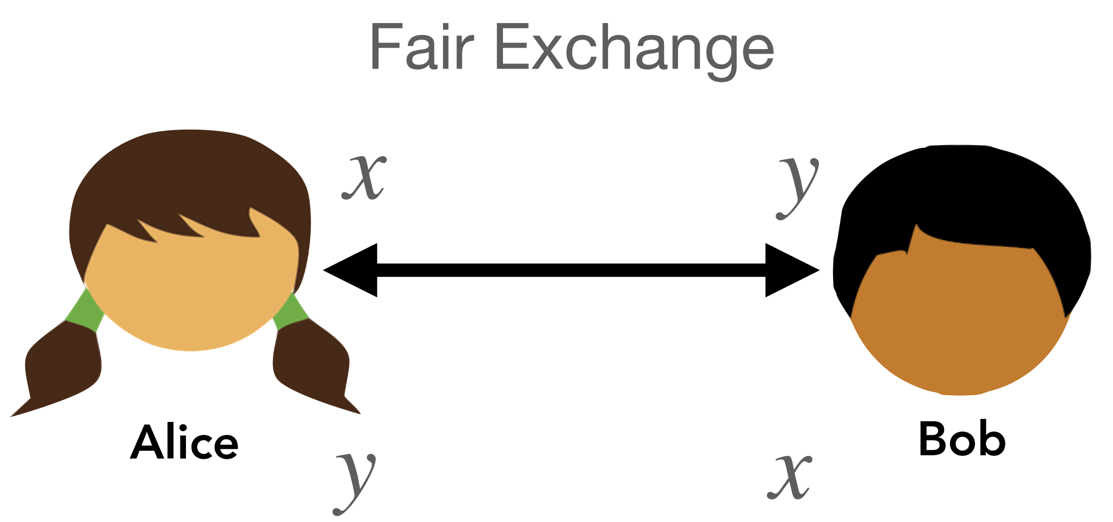


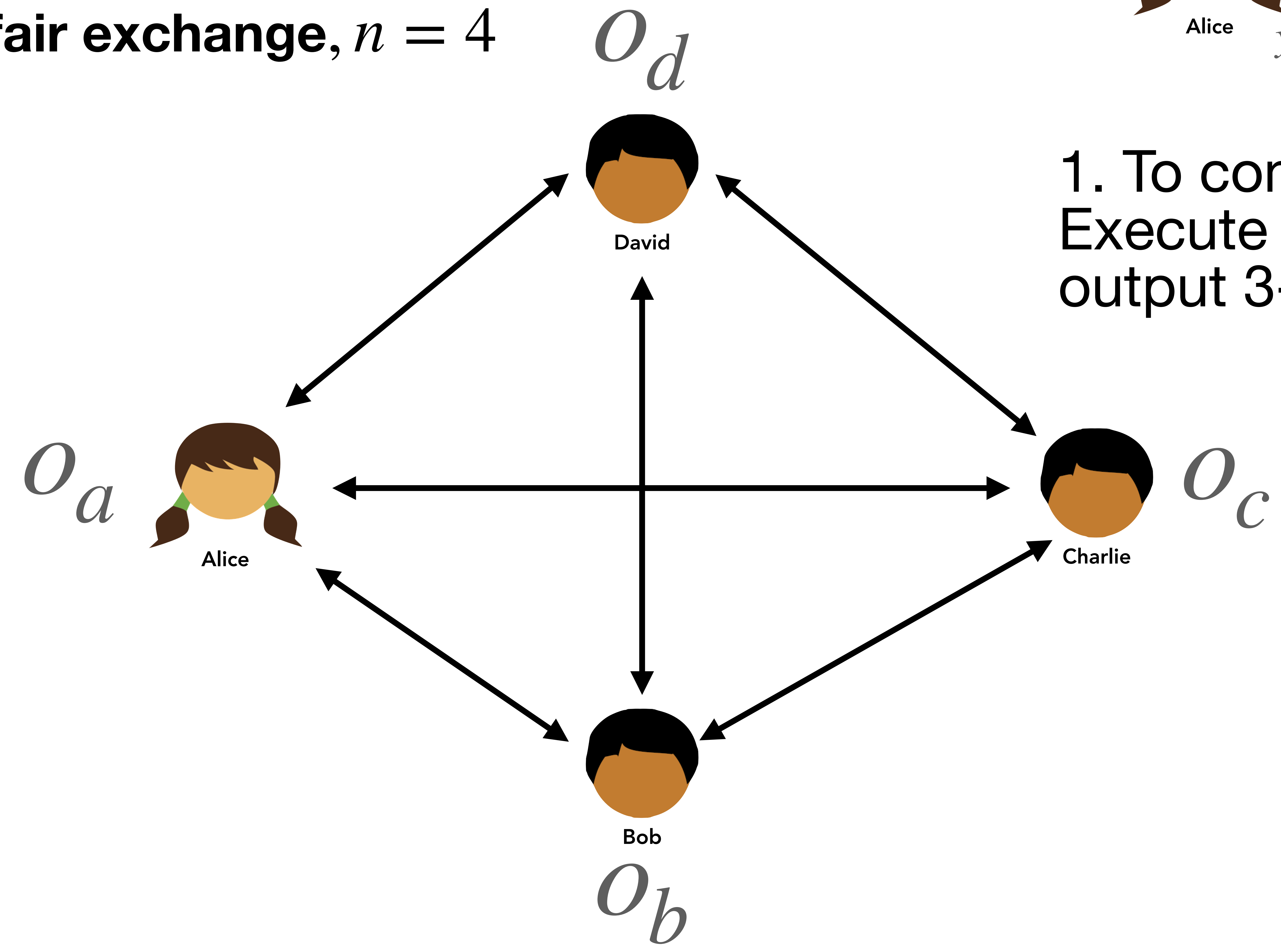


1. To compute f:
Execute some SwA MPC,
output 3-out-of-4 SS.

Example: Our Upper Bound

$t = \frac{n}{2}$, 2-wise fair exchange, $n = 4$

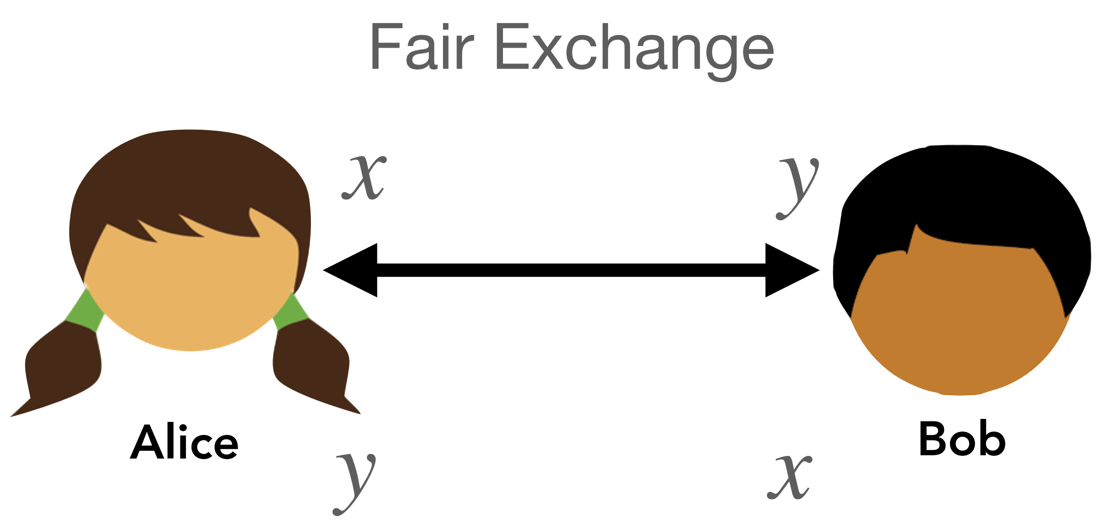


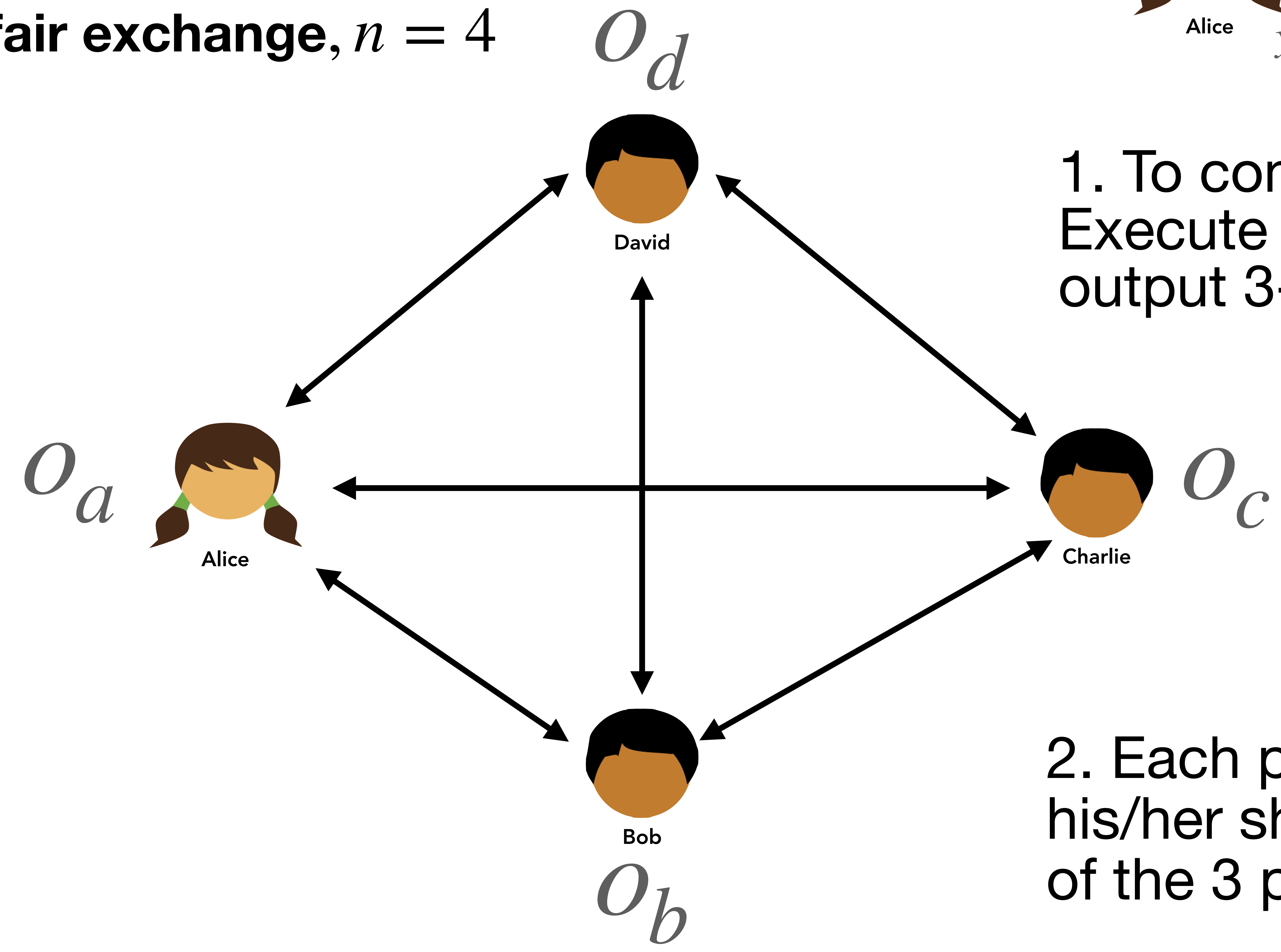


1. To compute f:
Execute some SwA MPC, output 3-out-of-4 SS.

Example: Our Upper Bound

$t = \frac{n}{2}$, 2-wise fair exchange, $n = 4$



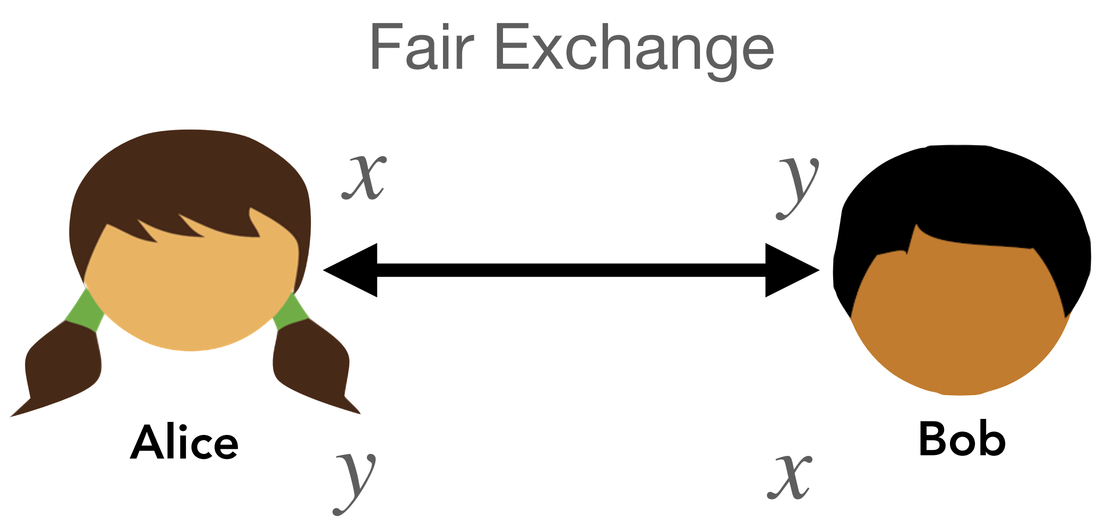


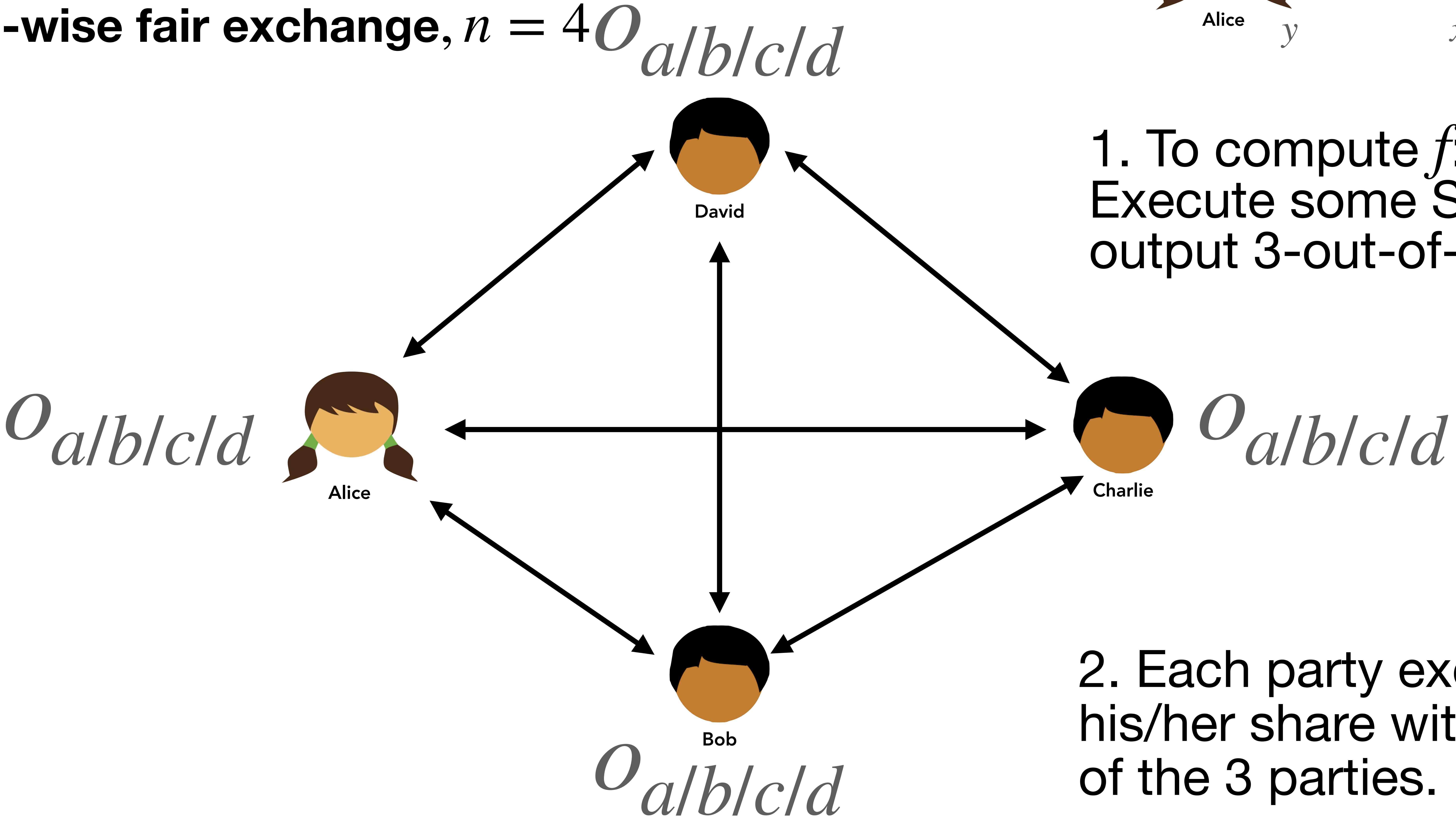
1. To compute f: Execute some SwA MPC, output 3-out-of-4 SS.

2. Each party exchanges his/her share with the rest of the 3 parties.

Example: Our Upper Bound

$t = \frac{n}{2}$, 2-wise fair exchange, $n = 4$



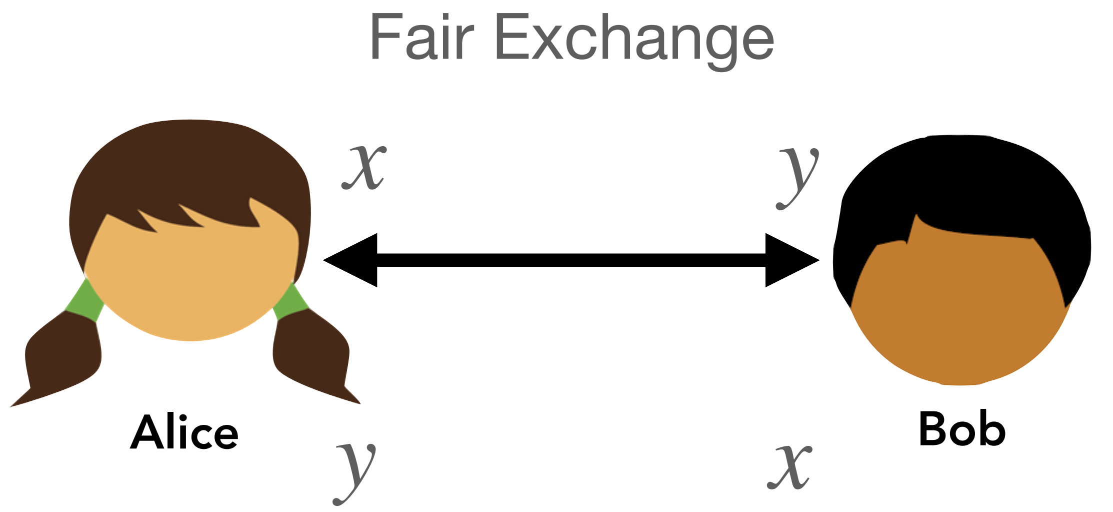


1. To compute f: Execute some SwA MPC, output 3-out-of-4 SS.

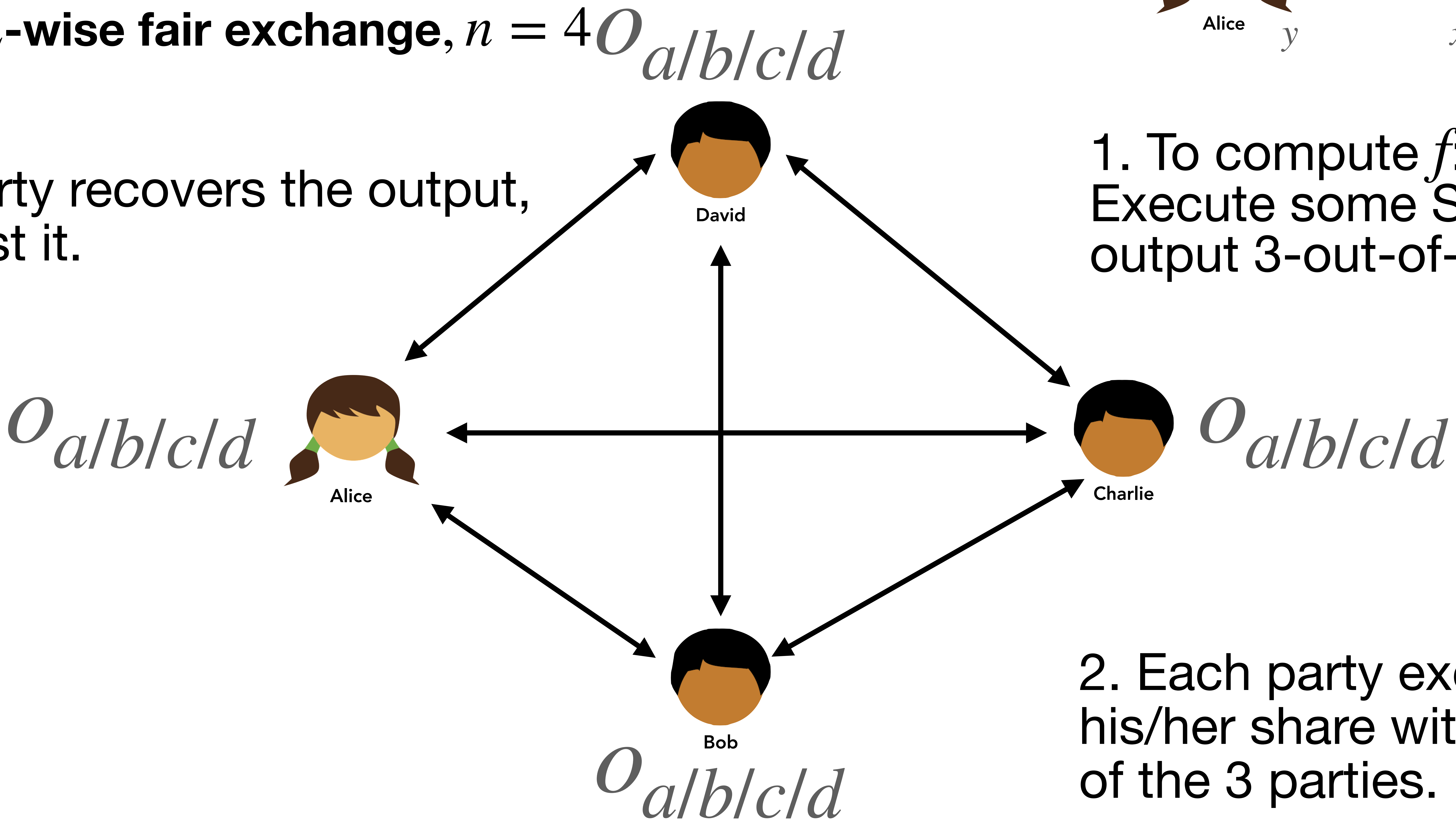
2. Each party exchanges his/her share with the rest of the 3 parties.

Example: Our Upper Bound

$t = \frac{n}{2}$, 2-**wise fair exchange**, $n = 4$



1. To compute f: Execute some SwA MPC, output 3-out-of-4 SS.

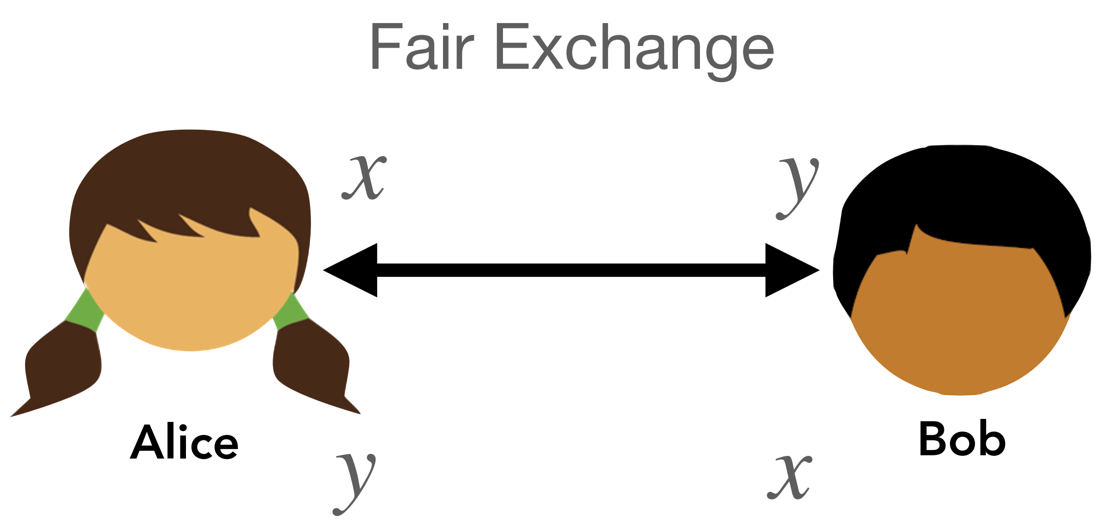


2. Each party exchanges his/her share with the rest of the 3 parties.

3. If a party recovers the output, broadcast it.

Example: Our Upper Bound

$t = \frac{n}{2}$, 2-wise fair exchange, $n = 4$

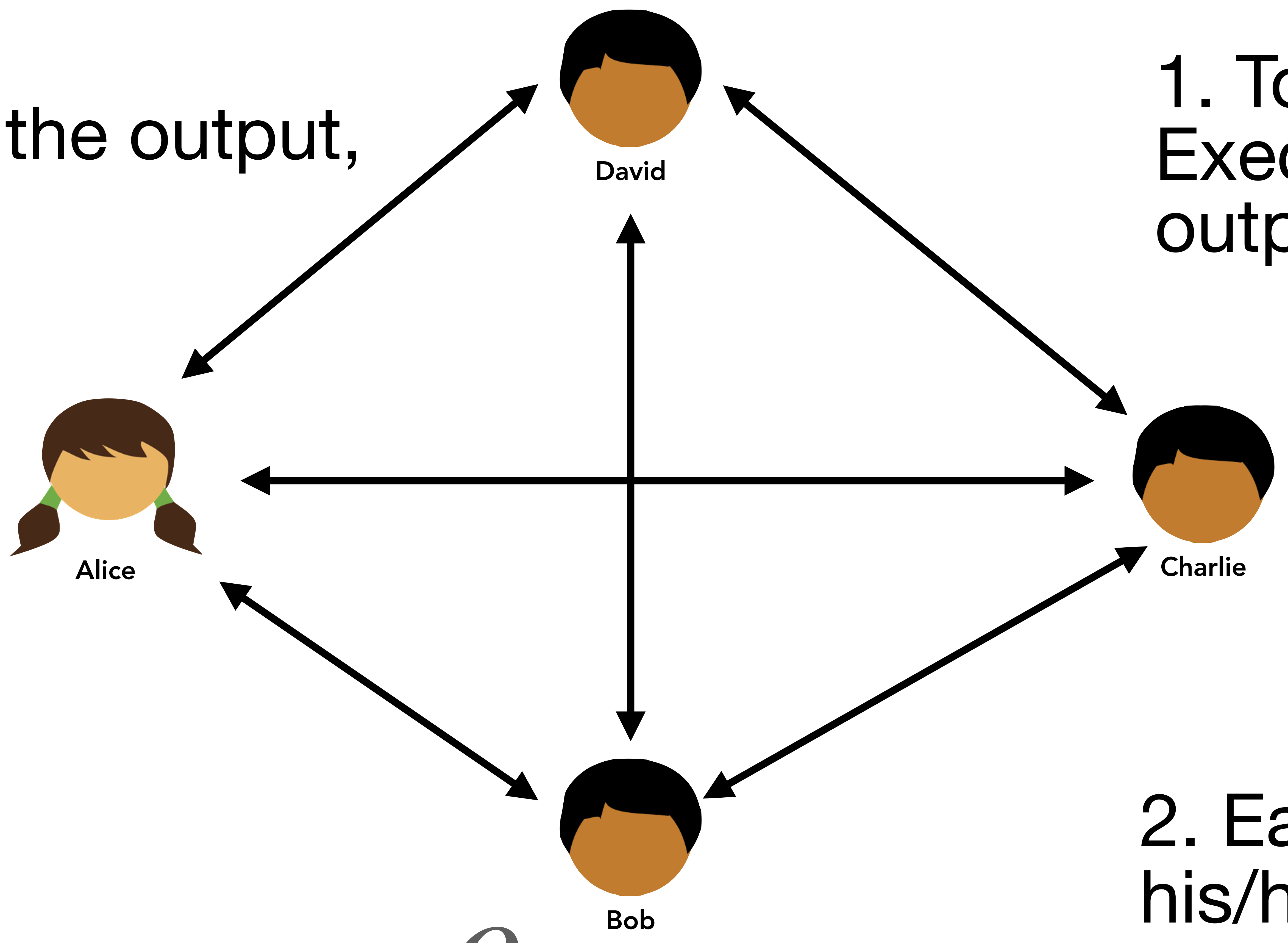


1. To compute f: Execute some SwA MPC, output 3-out-of-4 SS.

2. Each party exchanges his/her share with the rest of the 3 parties.

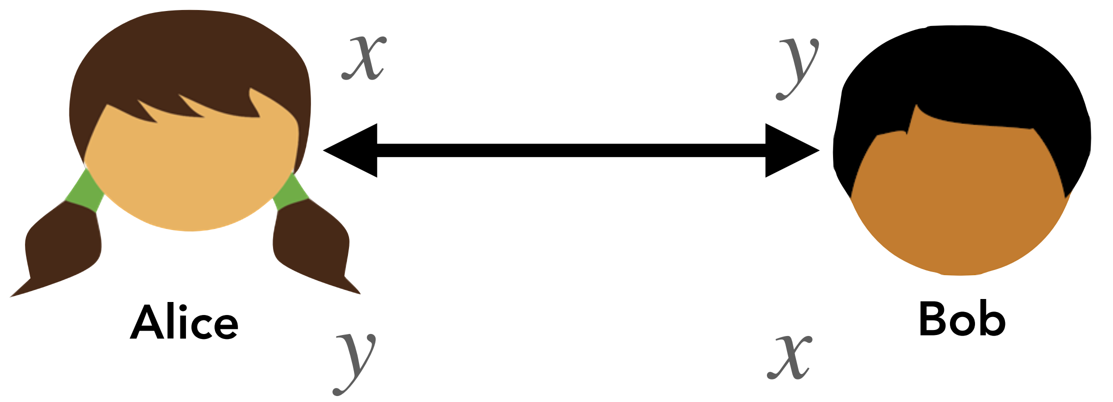
3. If a party recovers the output, broadcast it.

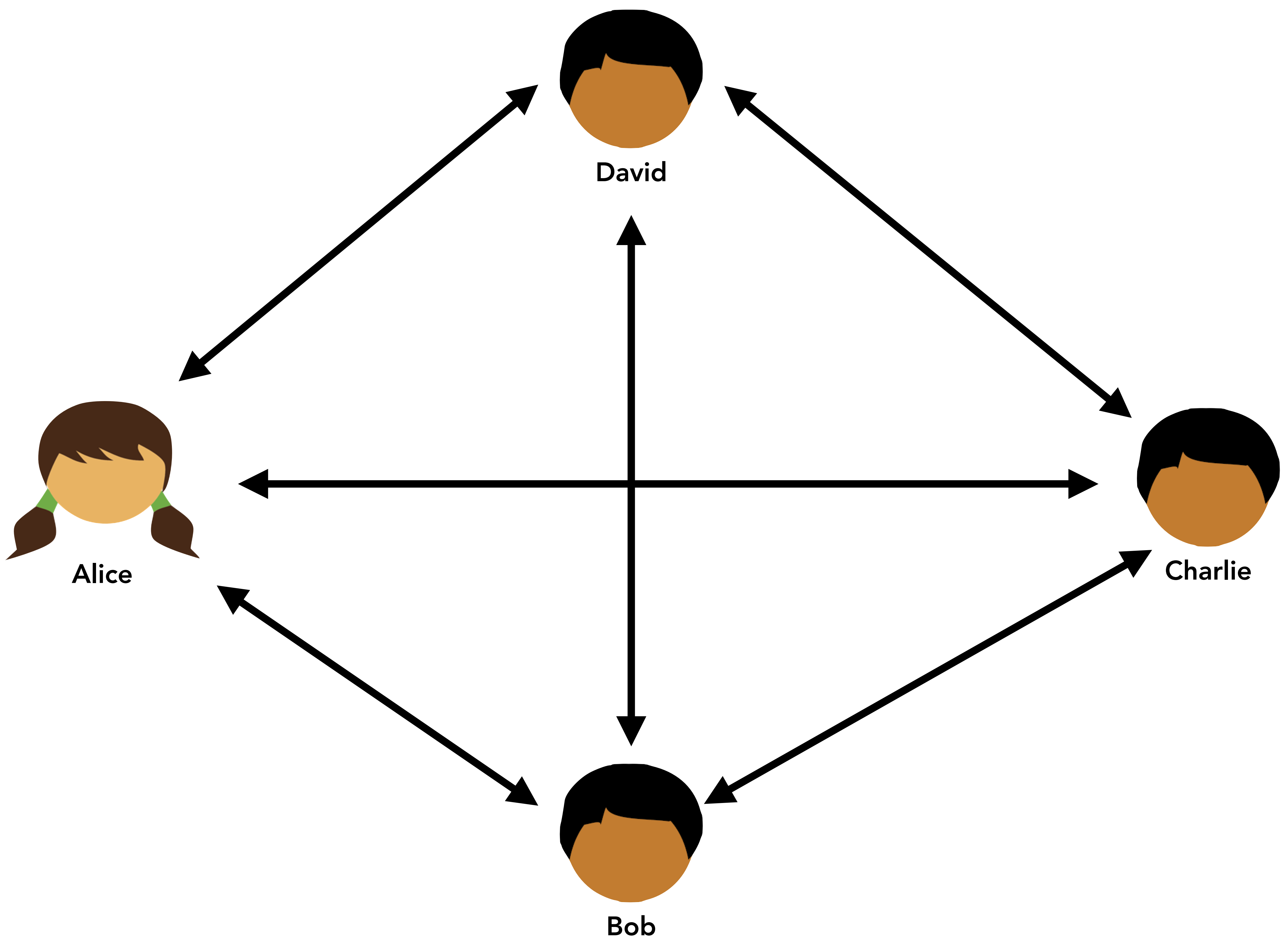
4. Output the result.



Why Fair?

$t = \frac{n}{2}$, 2-**wise fair exchange,** $n = 4$

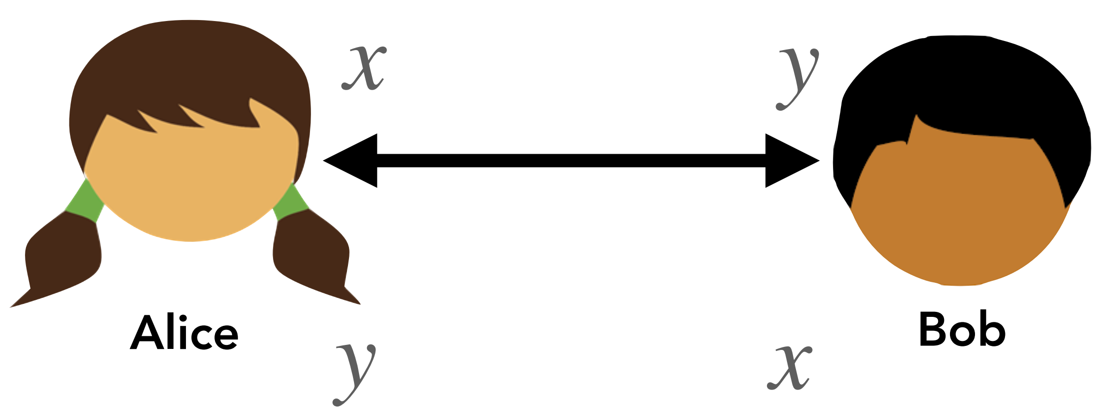


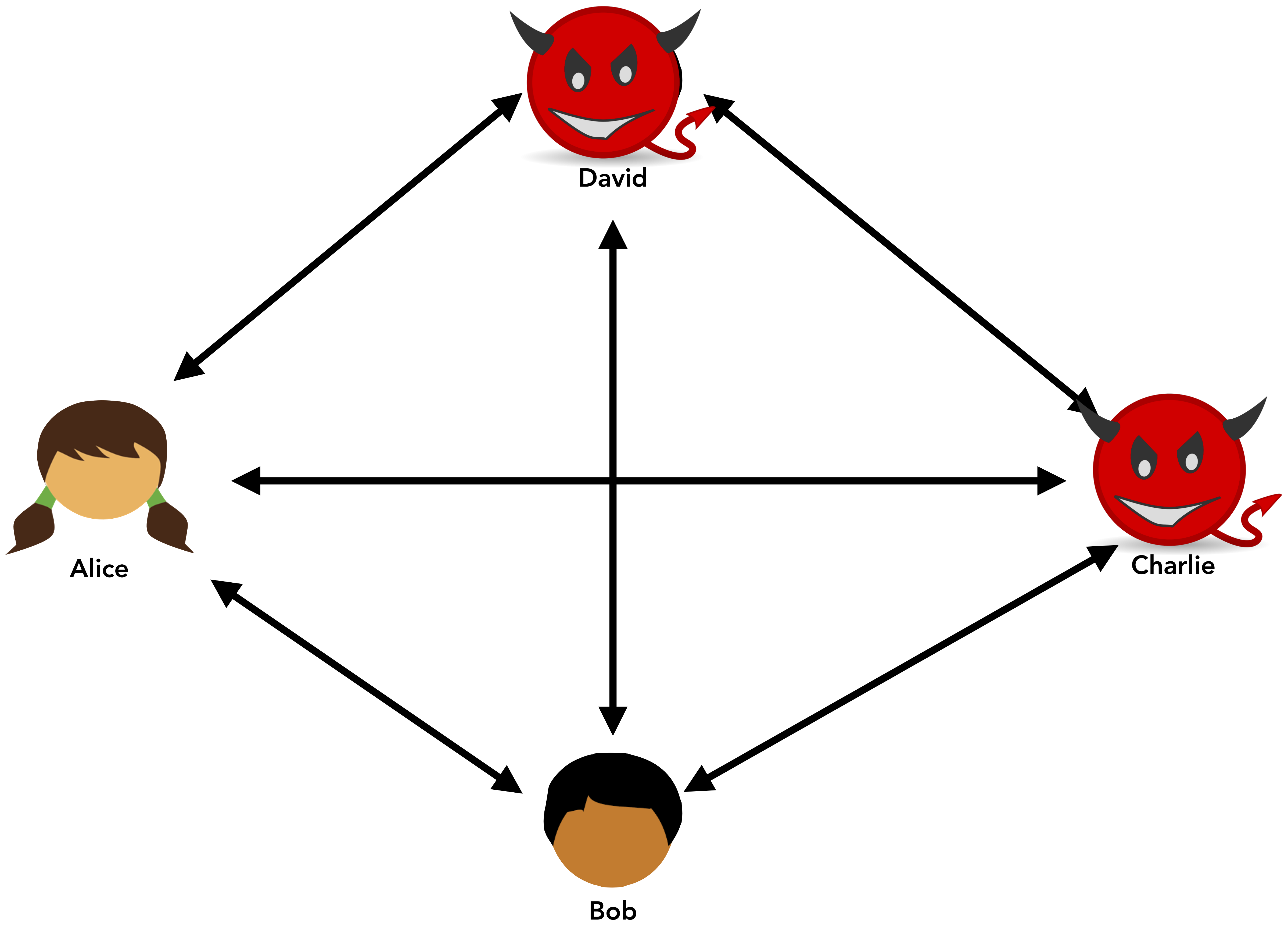


Why Fair?

$t = \frac{n}{2}$, 2-wise fair exchange, $n = 4$

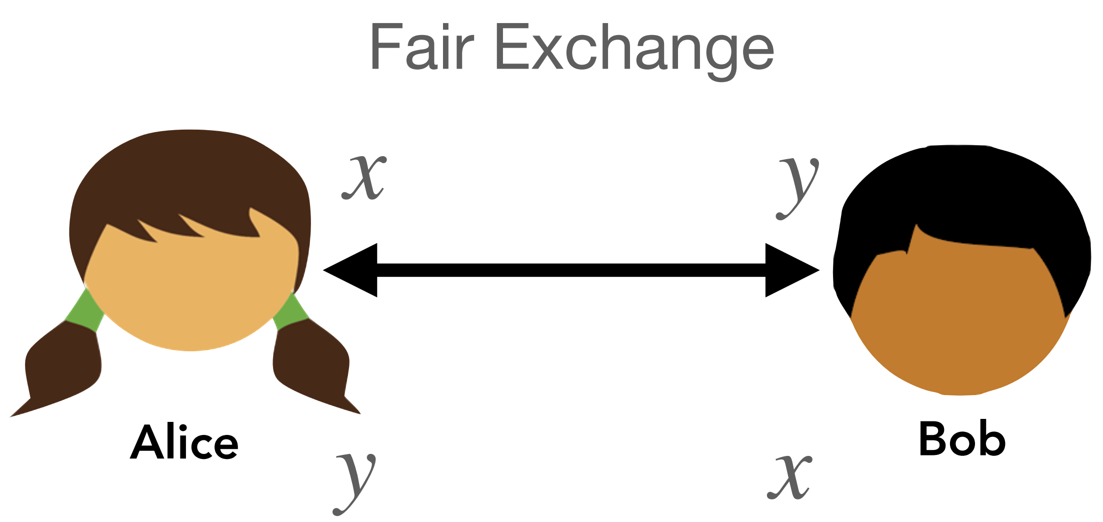
Fair Exchange

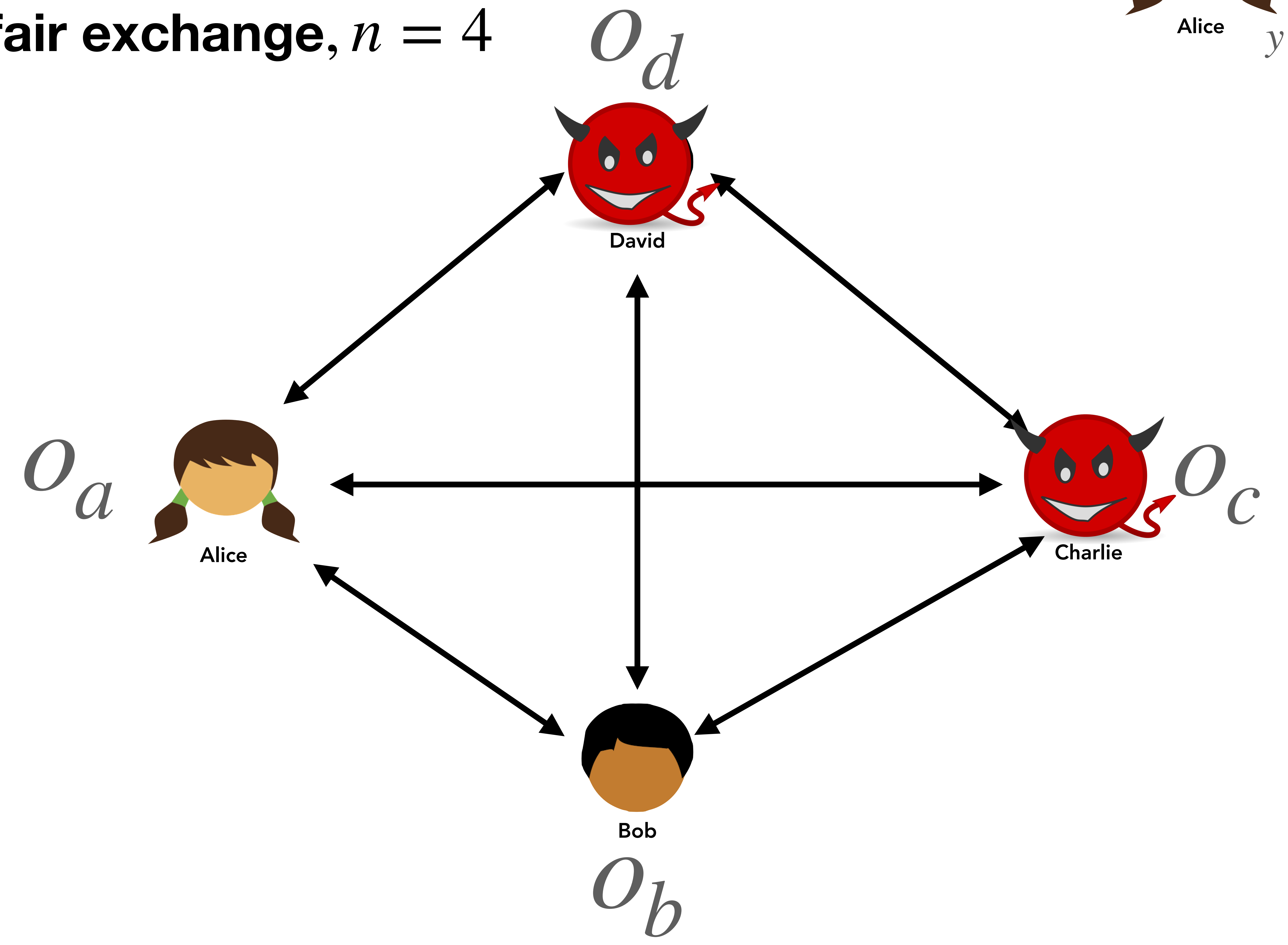




Why Fair?

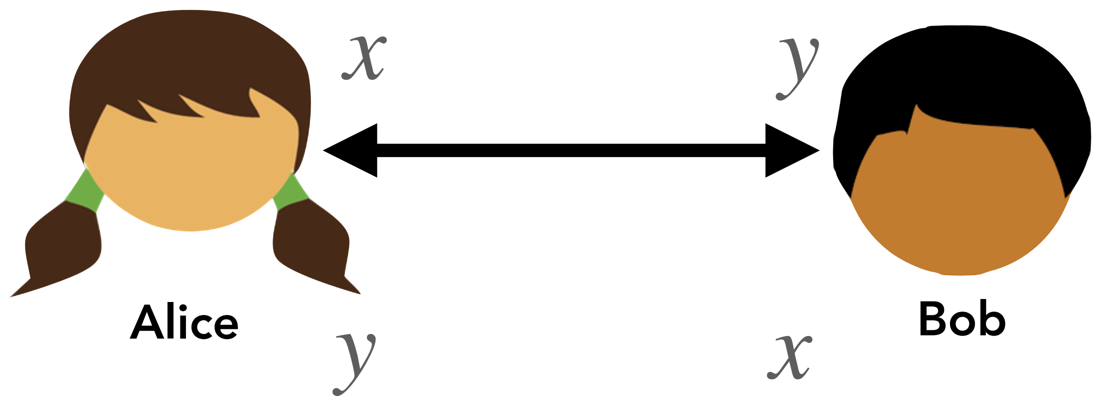
$t = \frac{n}{2}$, 2-wise fair exchange, $n = 4$



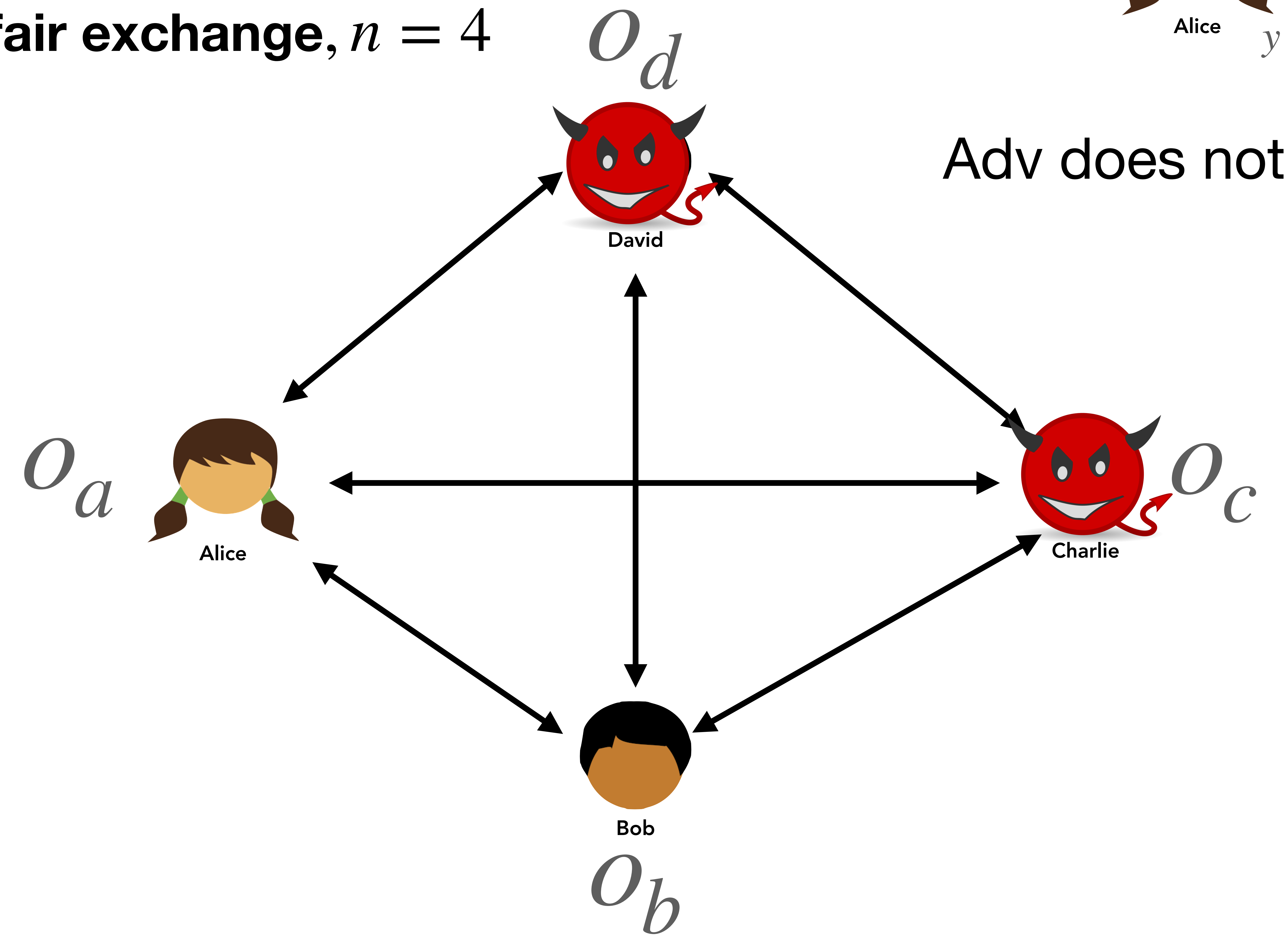


Why Fair?

$t = \frac{n}{2}$, 2-wise fair exchange, $n = 4$

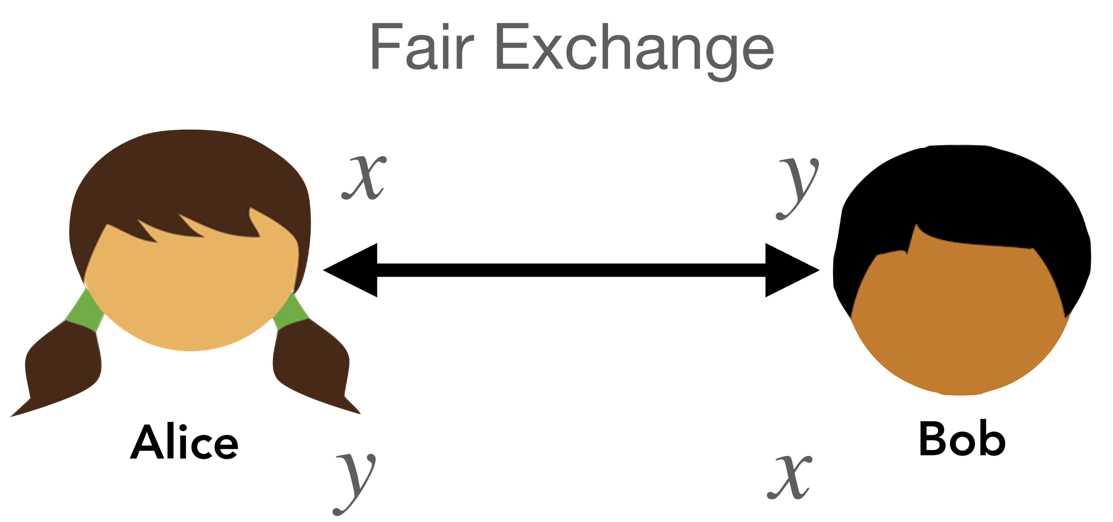


Adv does not learn the output.

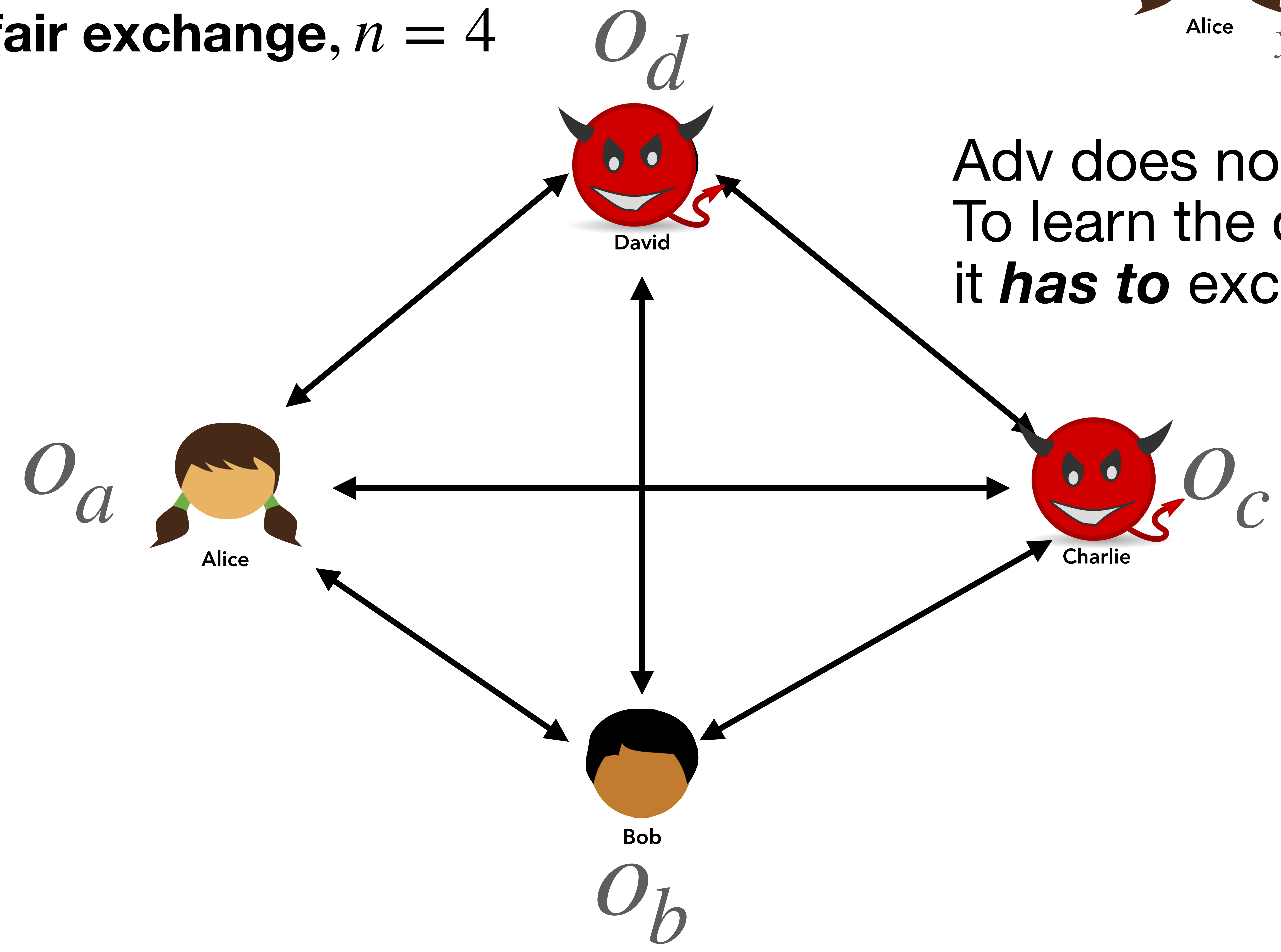


Why Fair?

$t = \frac{n}{2}$, 2-wise fair exchange, $n = 4$

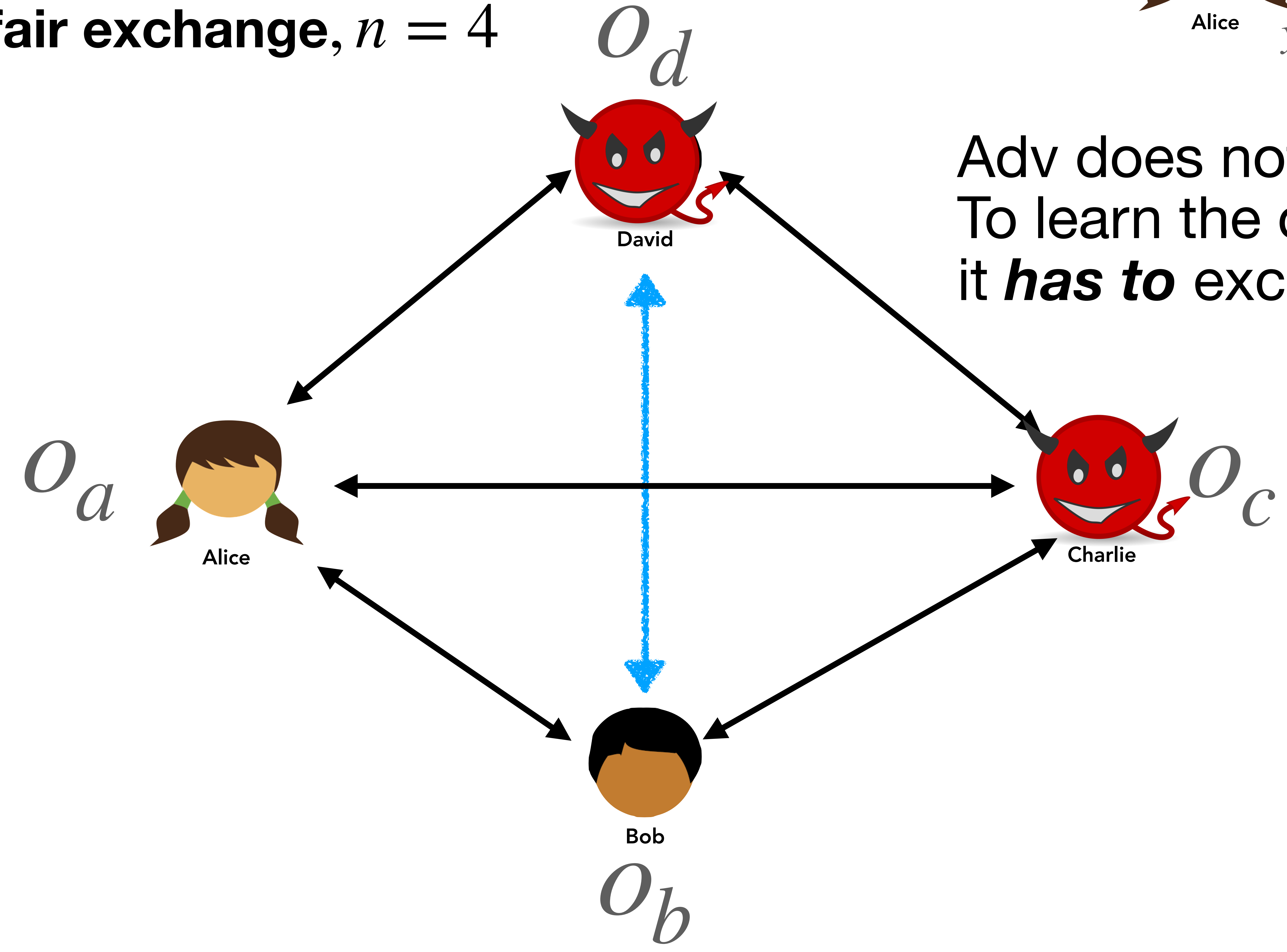


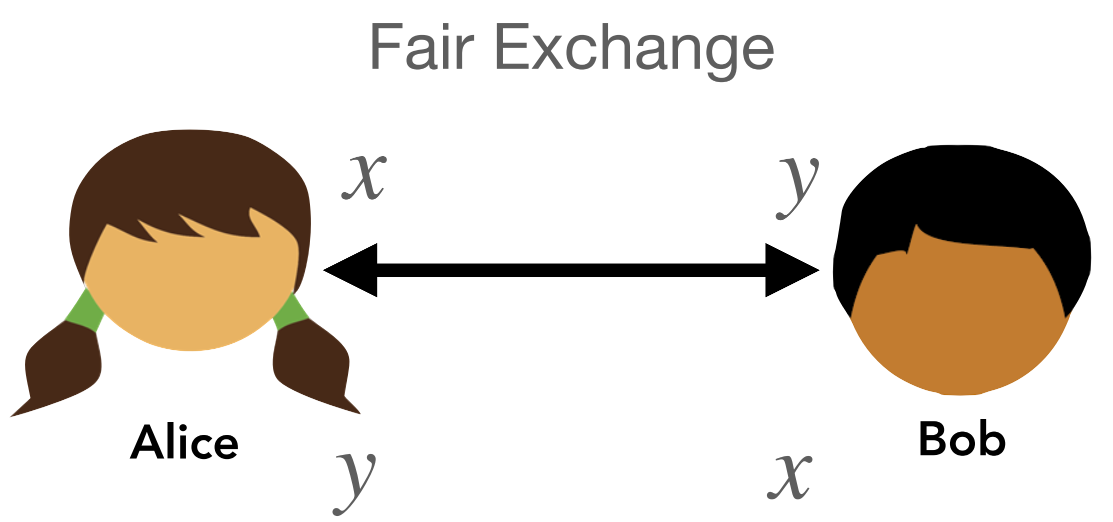
Adv does not learn the output.
To learn the output,
it ***has to*** exchange.



Why Fair?

$t = \frac{n}{2}$, 2-wise fair exchange, $n = 4$

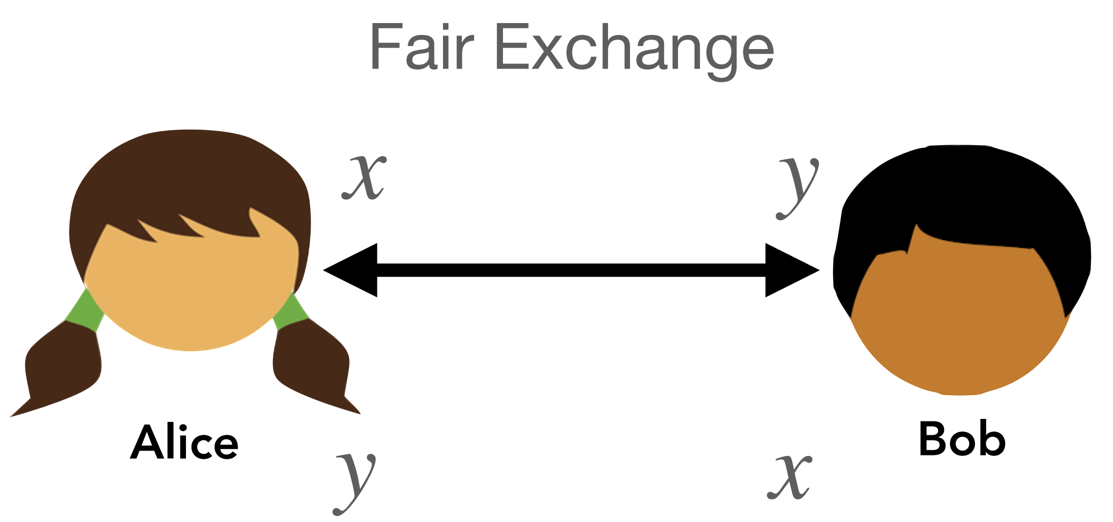


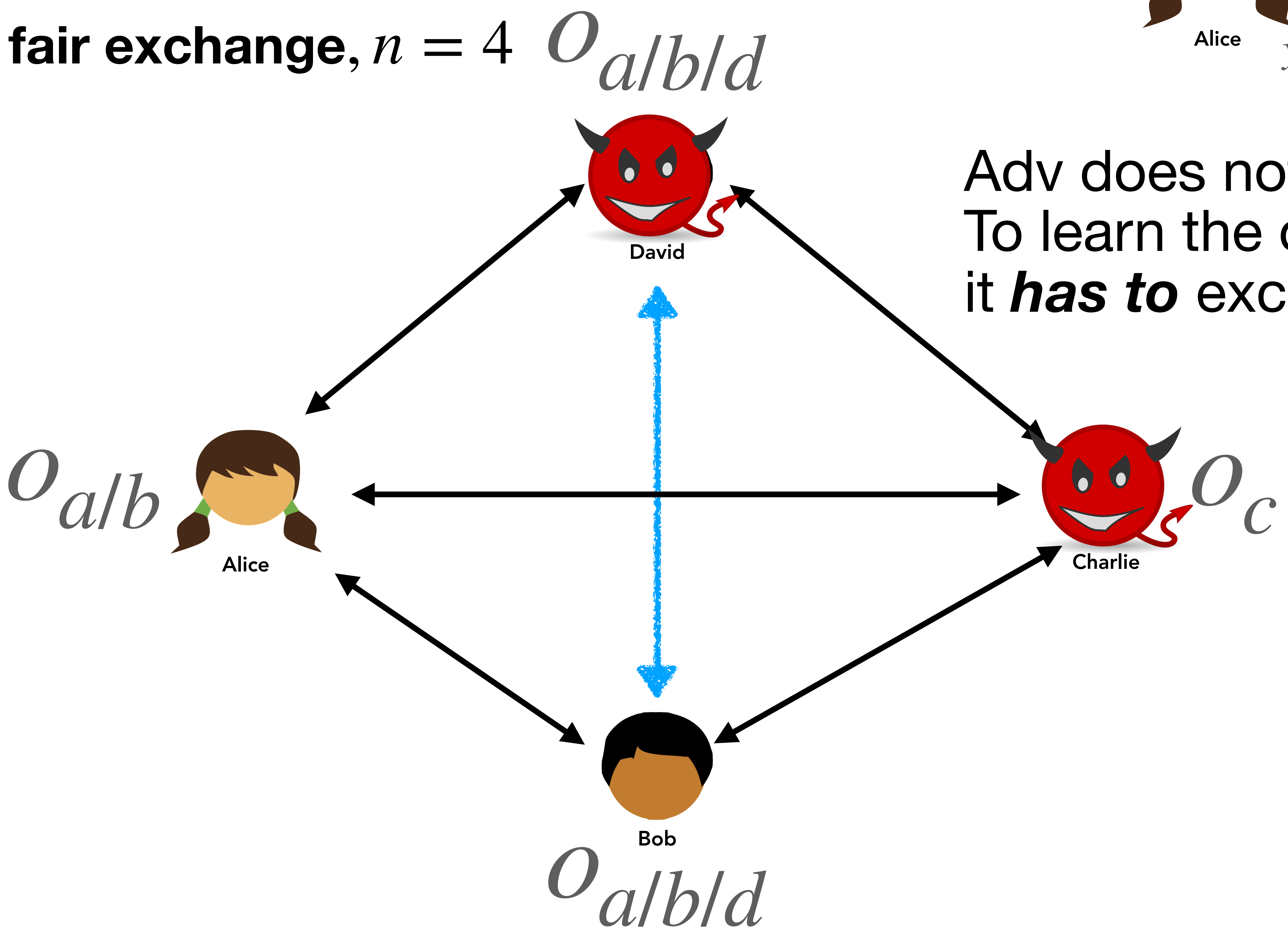


Adv does not learn the output.
To learn the output,
it ***has to*** exchange.

Why Fair?

$t = \frac{n}{2}$, 2-wise fair exchange, $n = 4$

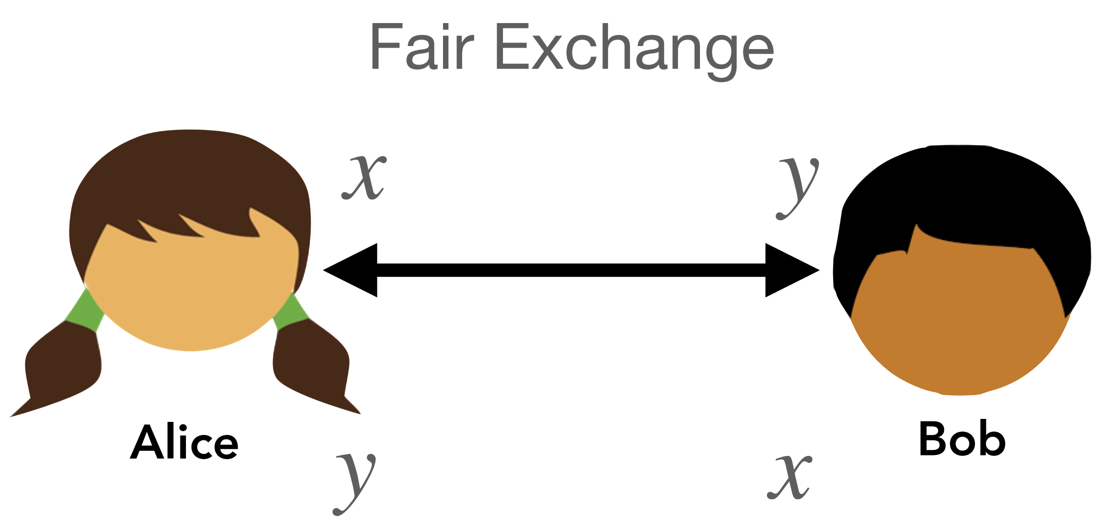


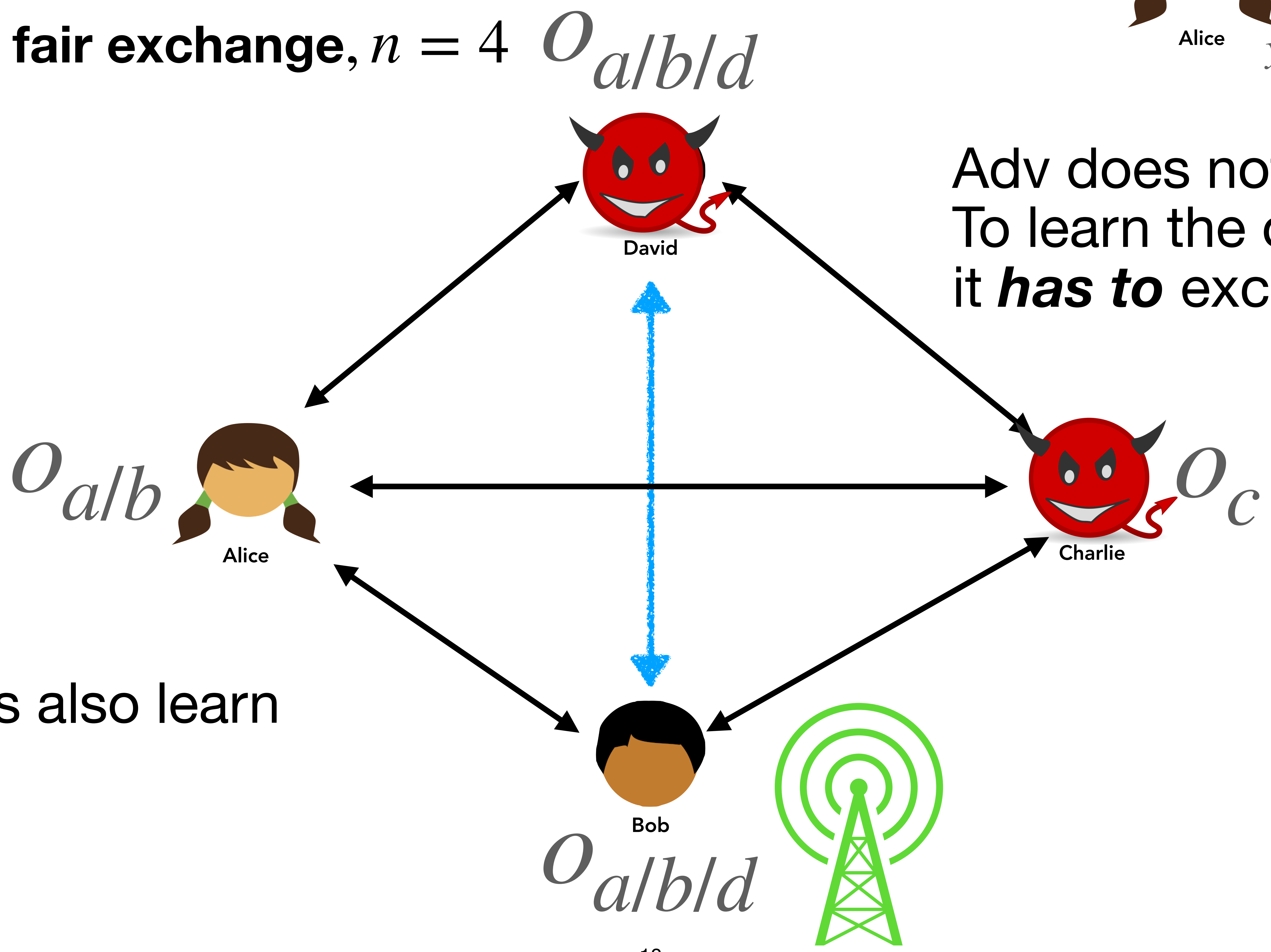


Adv does not learn the output.
To learn the output,
it ***has to*** exchange.

Why Fair?

$t = \frac{n}{2}$, 2-**wise fair exchange,** $n = 4$





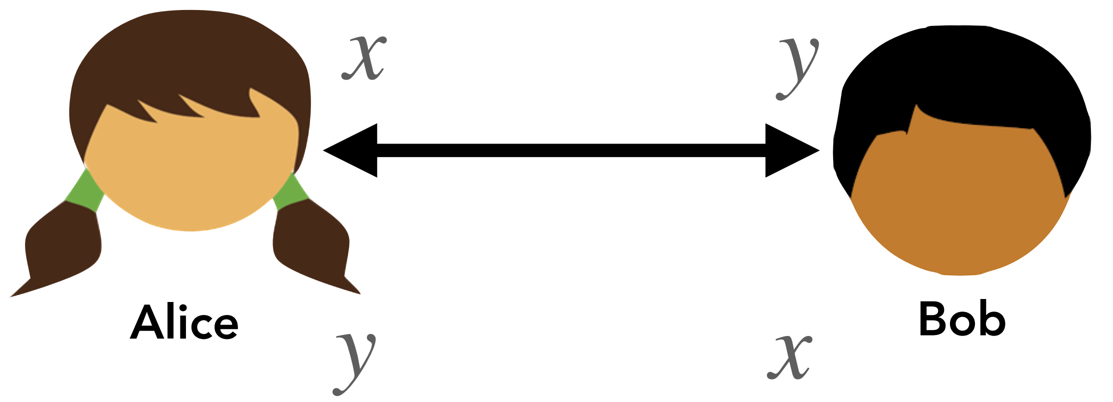
Adv does not learn the output.
To learn the output,
it ***has to*** exchange.

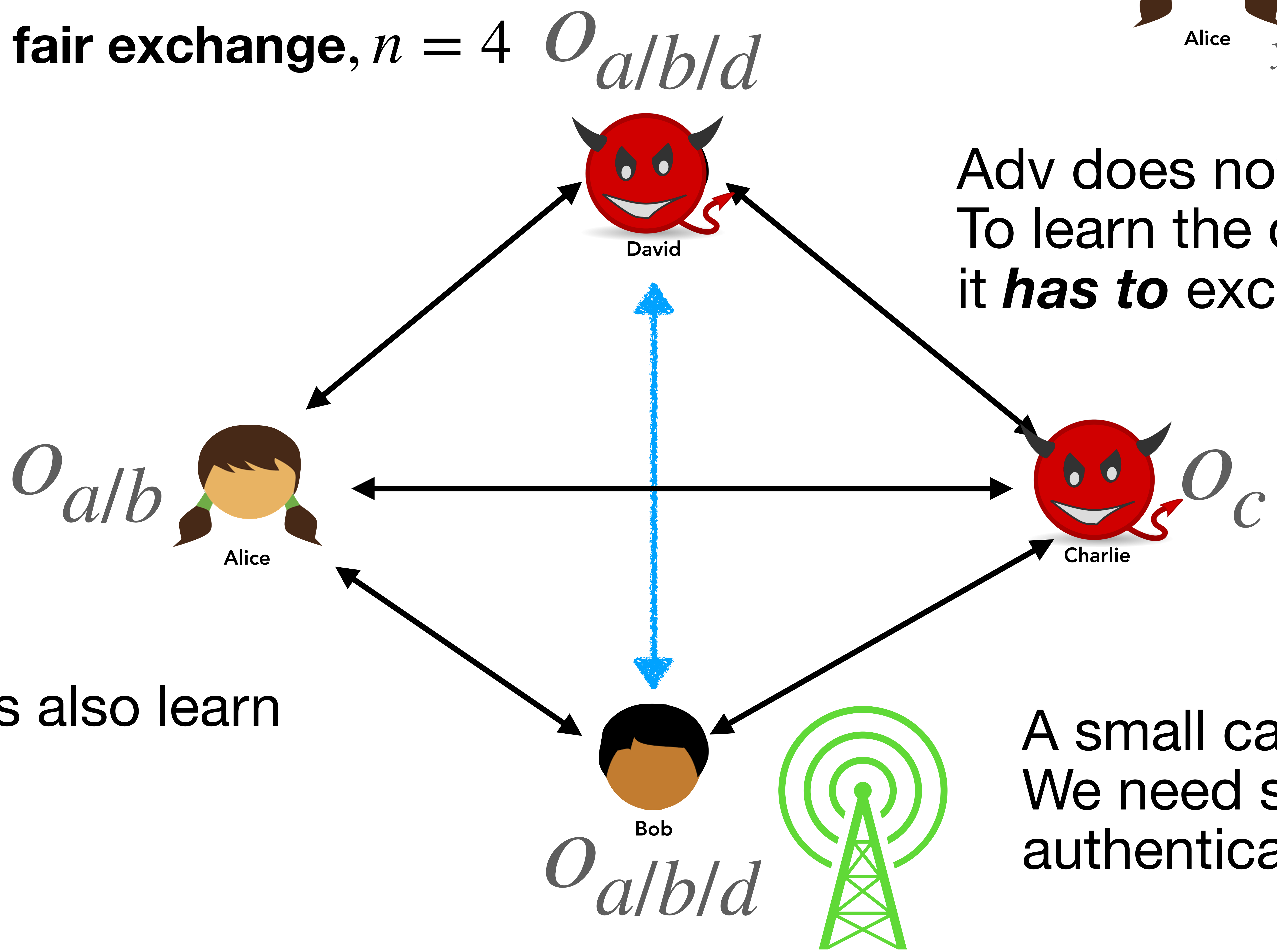
Honest parties also learn the output.

Why Fair?

$t = \frac{n}{2}$, 2-**wise fair exchange,** $n = 4$

Fair Exchange





Adv does not learn the output.
To learn the output,
it ***has to*** exchange.

Honest parties also learn the output.

A small caveat:
We need some authentication mechanism.

Just How Fair is an Unreactive World?

We completely address this question.
t = #corruption, n = #party

Not very fair ☹

Table 1: Our contributions.

t	Insufficient functionalities for fair coin tossing	Sufficient functionalities for fair MPC
$t < \frac{n}{2}$	–	Local computation [FGMvR02]
$t = \frac{n}{2}$	Local computation [Cle86]	2-wise fair exchange **[ours]**
$t > \frac{n}{2}$	Arbitrary unreactive t-wise **[ours]**	$(t+1)$-wise fair exchange[a] **[ours]**

[Cohen and Lindel, Asiacrypt 14]:

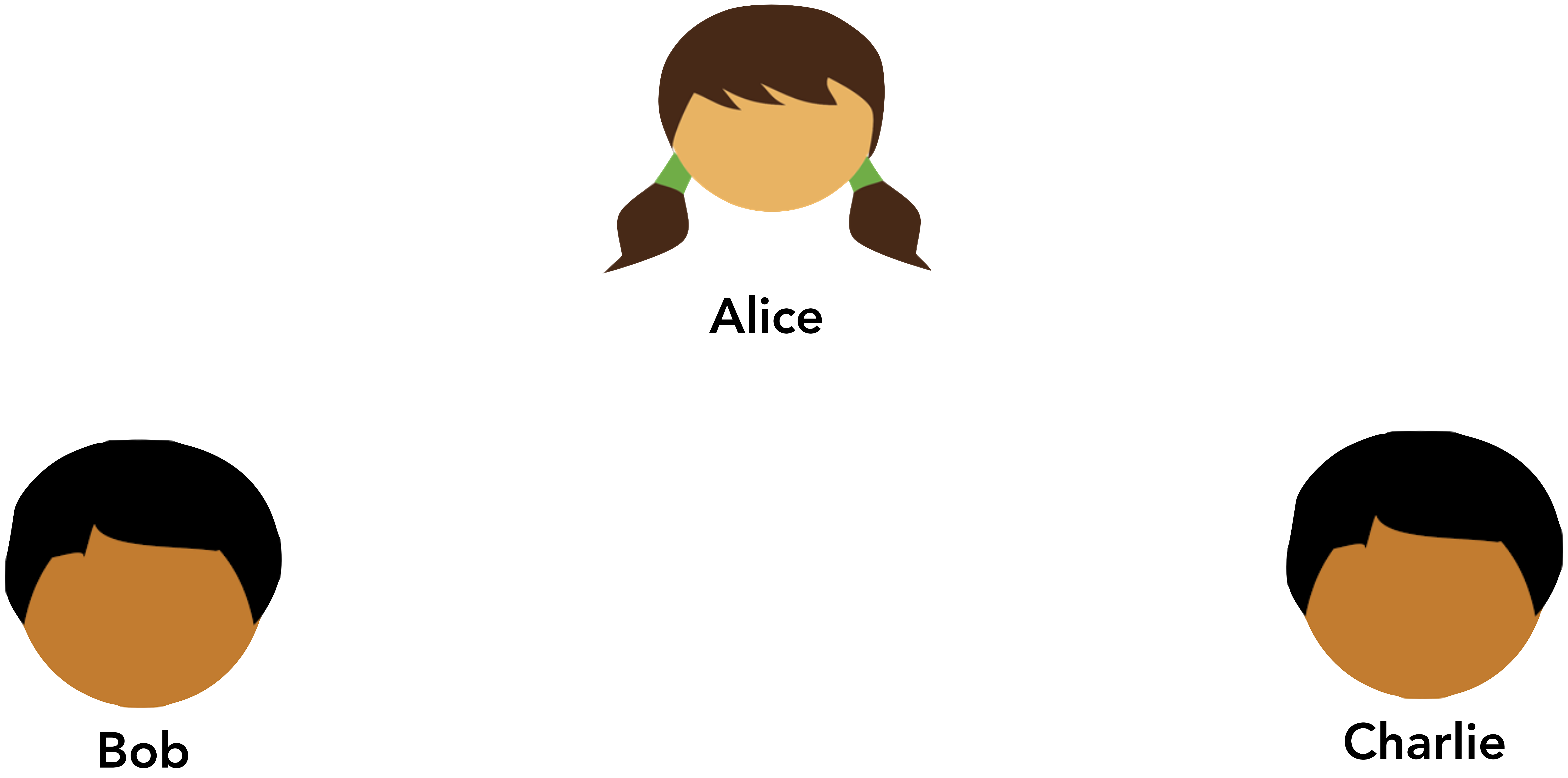
1. Fairness with broadcast →Fairness without broadcast
2. No G.O.D. with broadcast →No fairness (even) with broadcast

Example: Our Lower Bound

$n = 3, t = 2,$ **any** 2**-wise unreactive functionality**

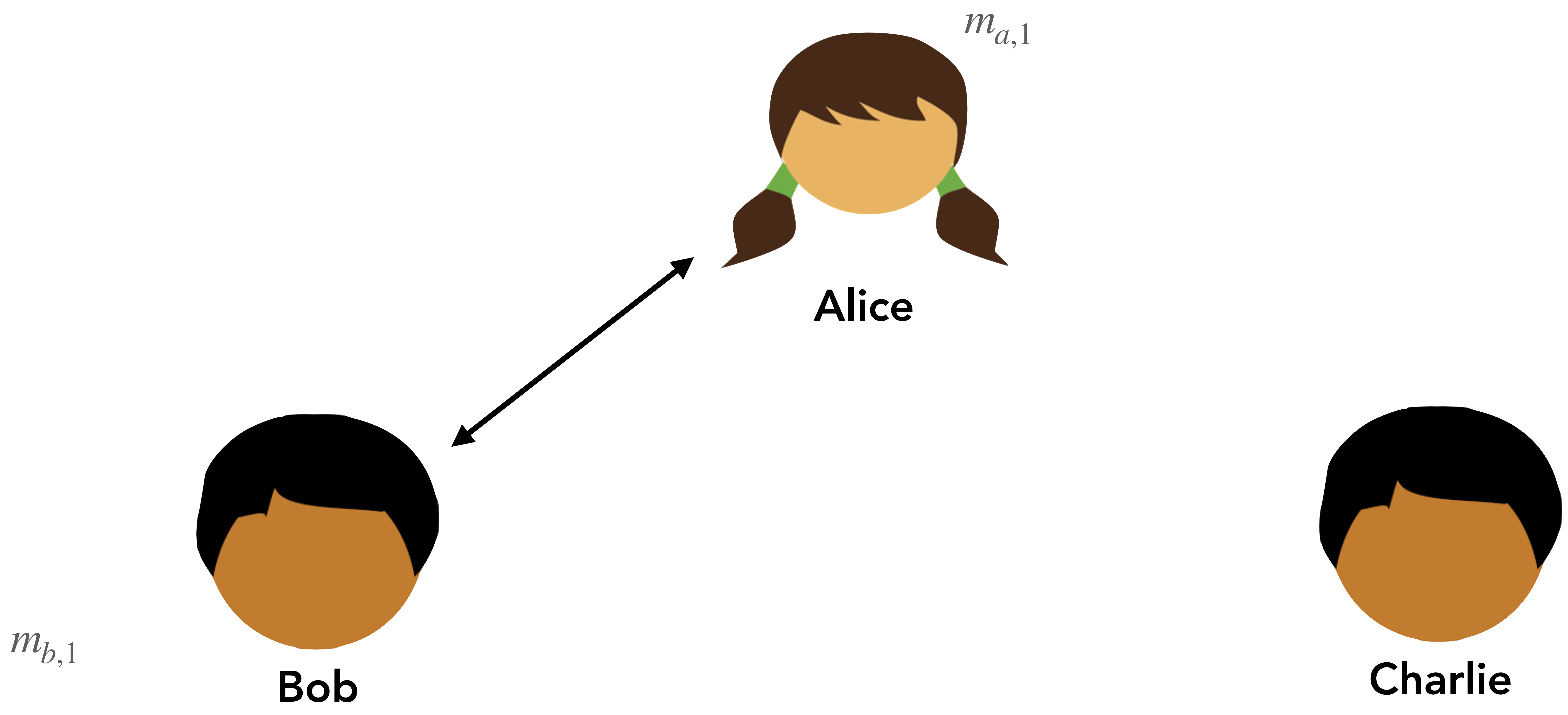
Example: Our Lower Bound

$n = 3$, $t = 2$, any 2-wise unreactive functionality



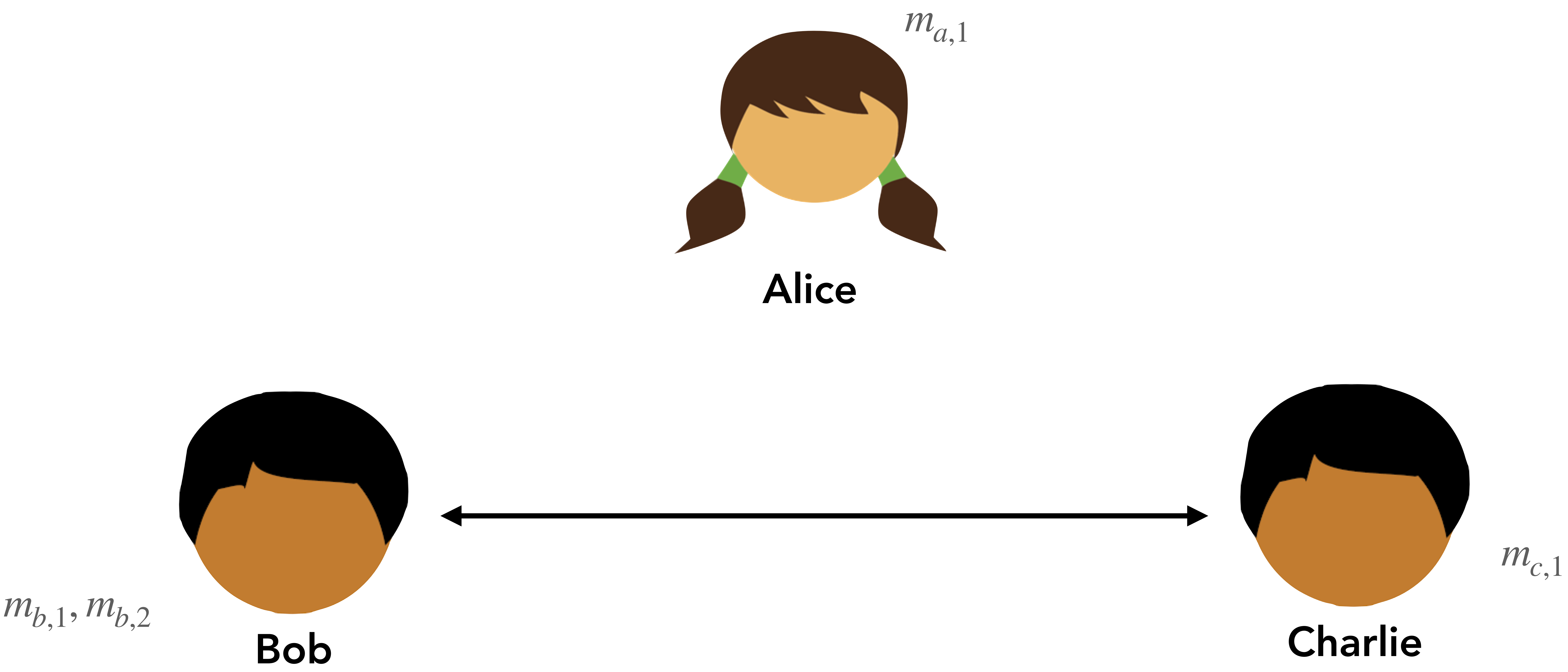
Example: Our Lower Bound

$n = 3, t = 2$, any 2-wise unreactive functionality



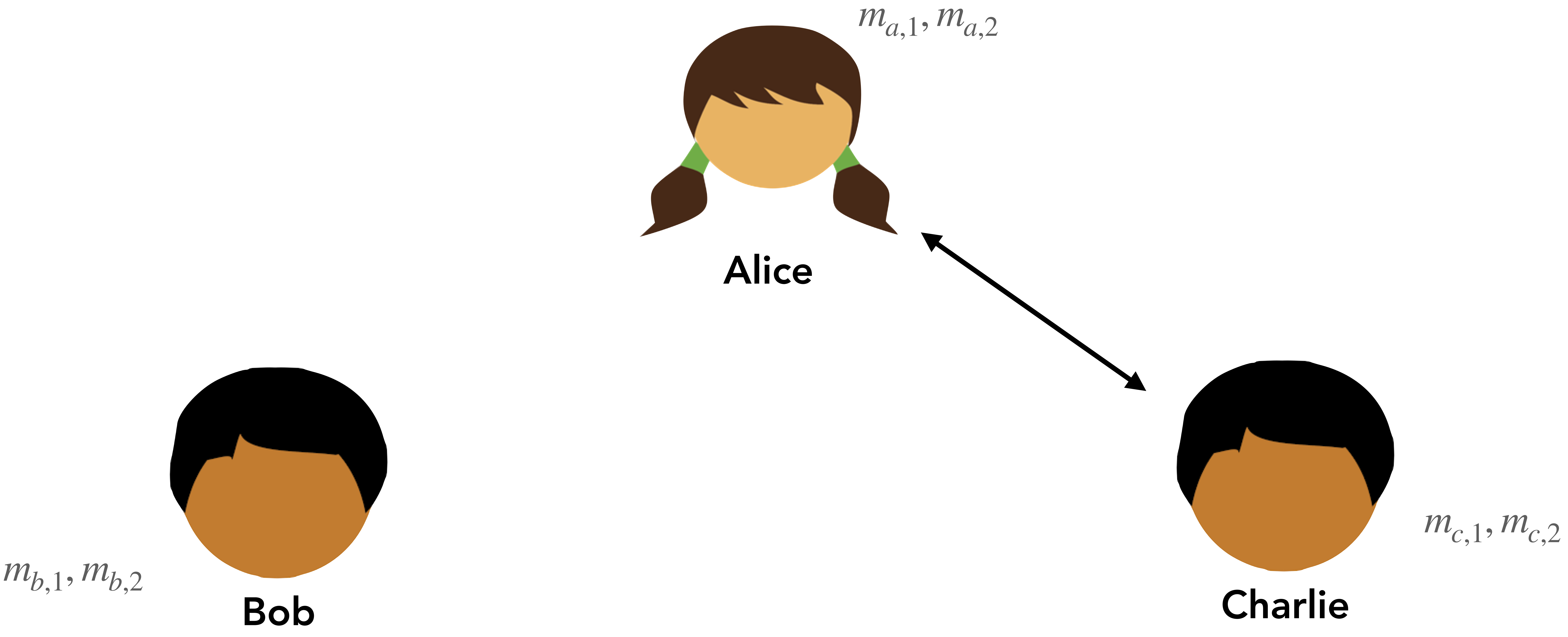
Example: Our Lower Bound

$n = 3, t = 2$, **any 2-wise unreactive functionality**



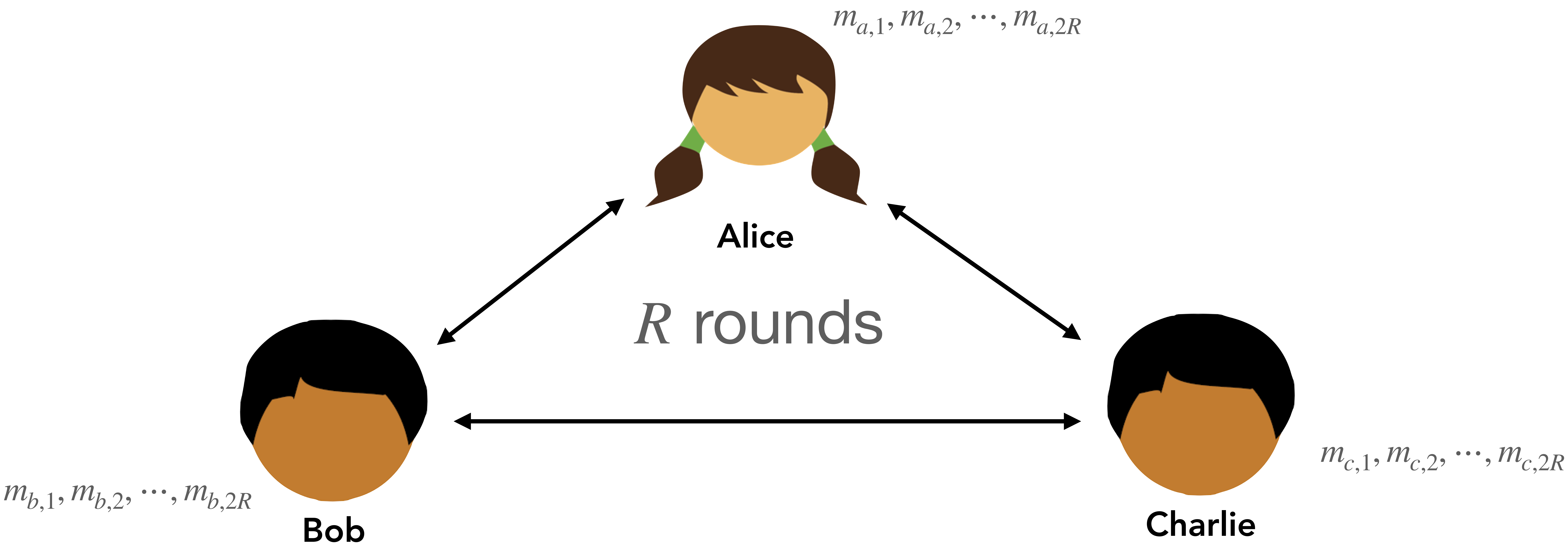
Example: Our Lower Bound

$n = 3, t = 2$, any 2-wise unreactive functionality



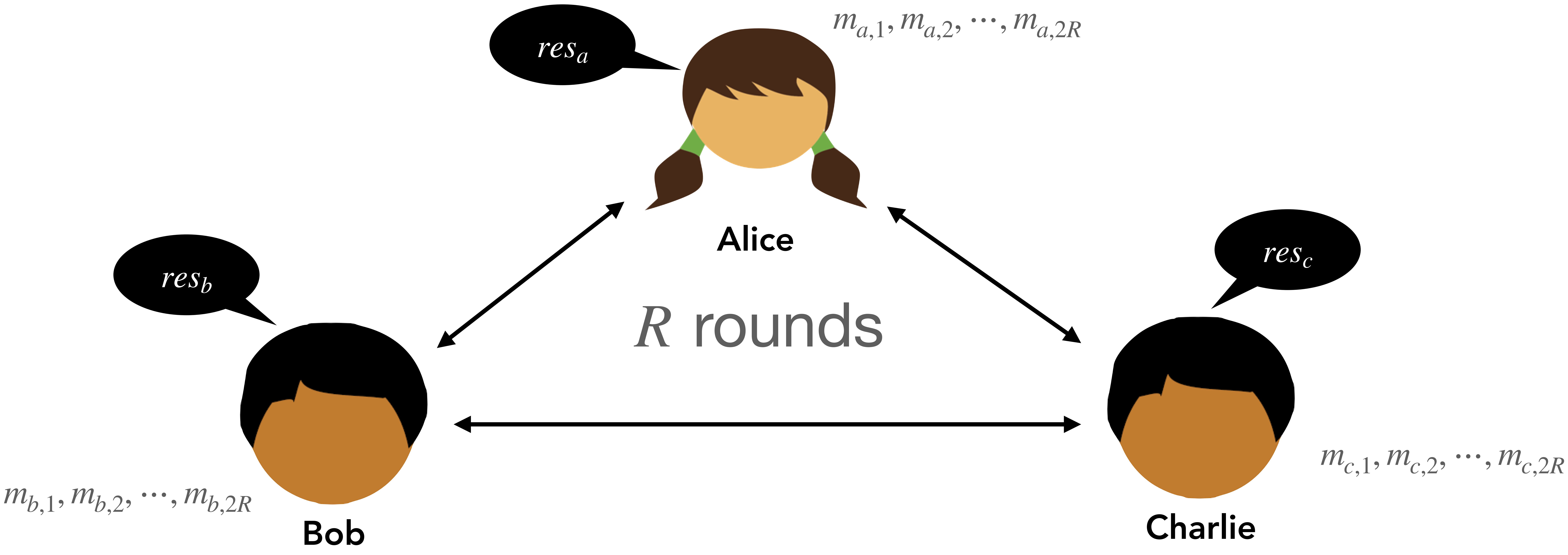
Example: Our Lower Bound

$n = 3, t = 2,$ any 2-wise unreactive functionality



Example: Our Lower Bound

$n = 3, t = 2$, any 2-wise unreactive functionality

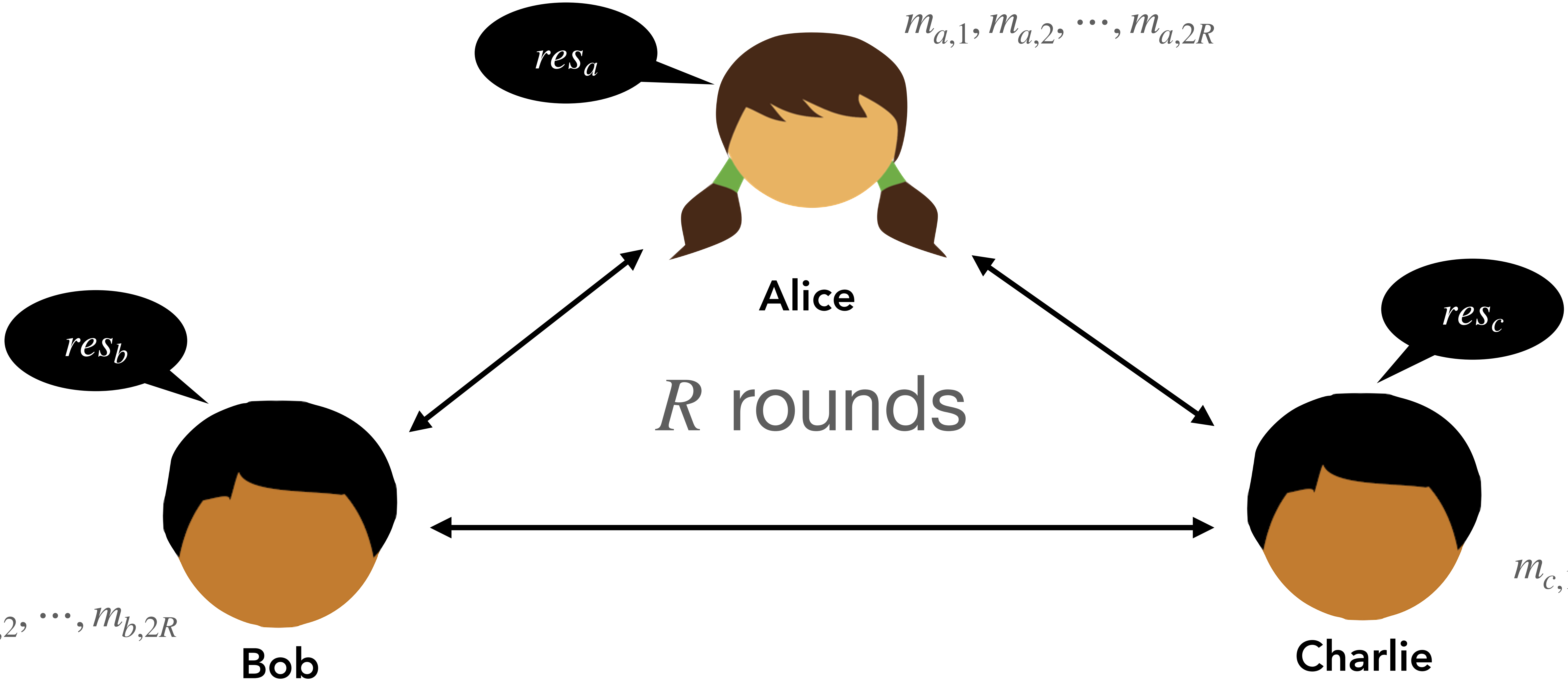


Example: Our Lower Bound

$n = 3, t = 2,$ **any** 2**-wise unreactive functionality**

$$\Pr[res_a = res_b = res_c] = 1$$

$$\Pr[res_a / res_b / res_c = 0] = \frac{1}{2}$$

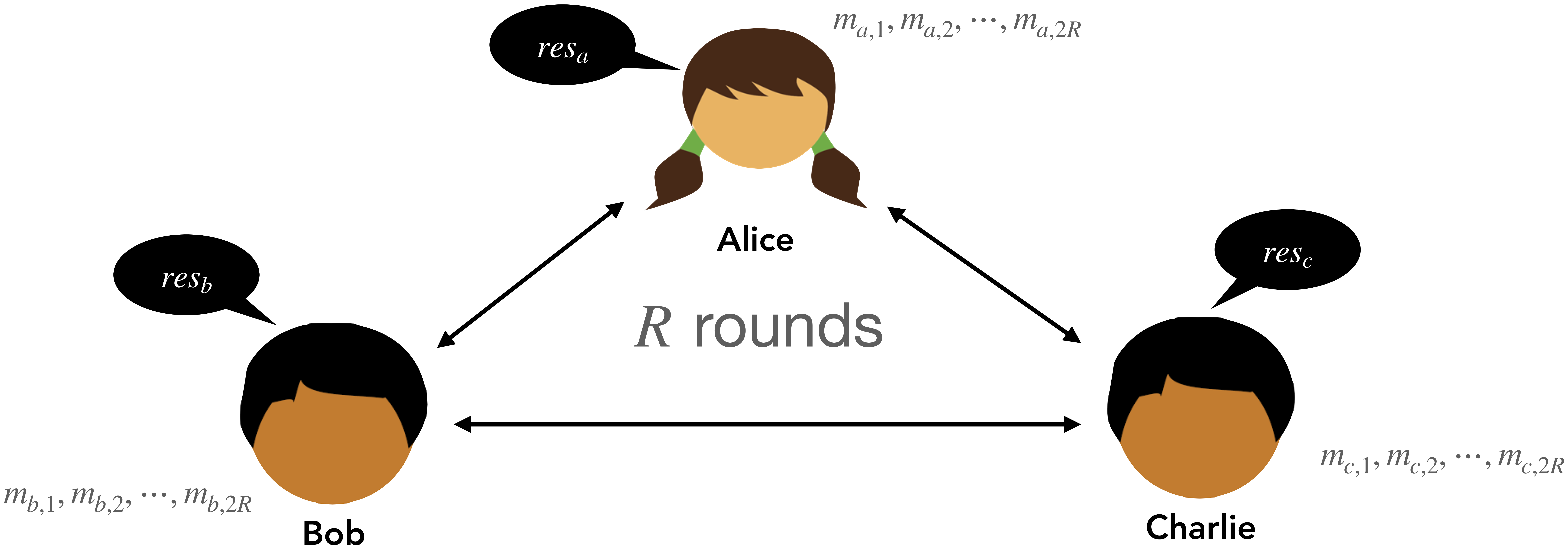


Example: Our Lower Bound

$n = 3, t = 2,$ **any** 2**-wise unreactive functionality**

$$\Pr[\overbrace{res_a = res_b = res_c}^{res}] = 1$$

$$\Pr[res_a / res_b / res_c = 0] = \frac{1}{2}$$

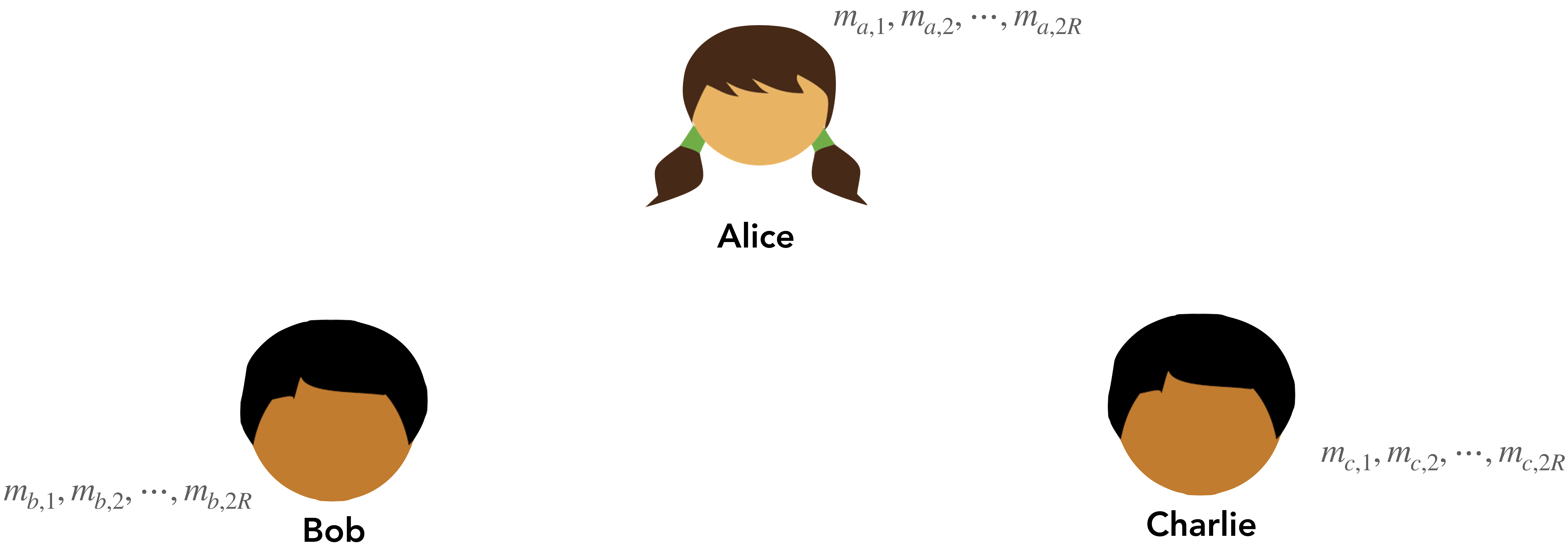


Example: Our Lower Bound

Predictor — Known as “backup” coin

$$\Pr[\overbrace{res_a = res_b = res_c}^{res}] = 1$$

$$\Pr[res_a / res_b / res_c = 0] = \frac{1}{2}$$



Example: Our Lower Bound

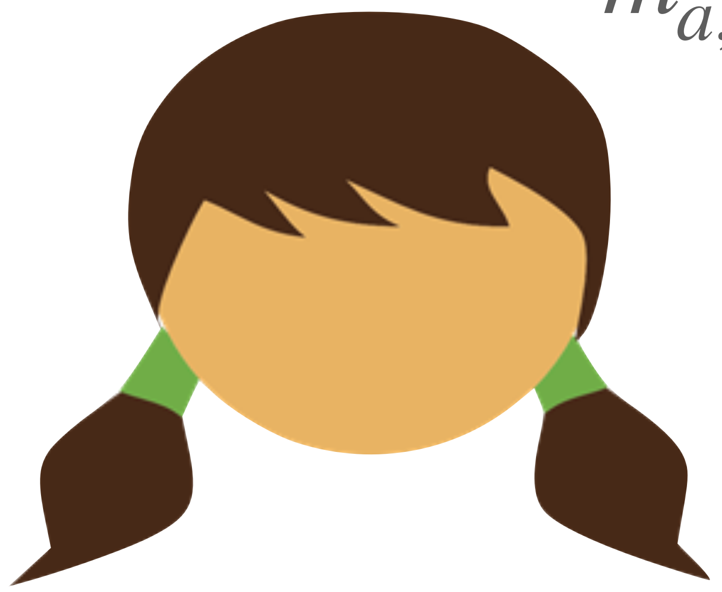
Predictor — Known as "backup" coin

$$\Pr[\overbrace{res_a = res_b = res_c}^{res}] = 1$$

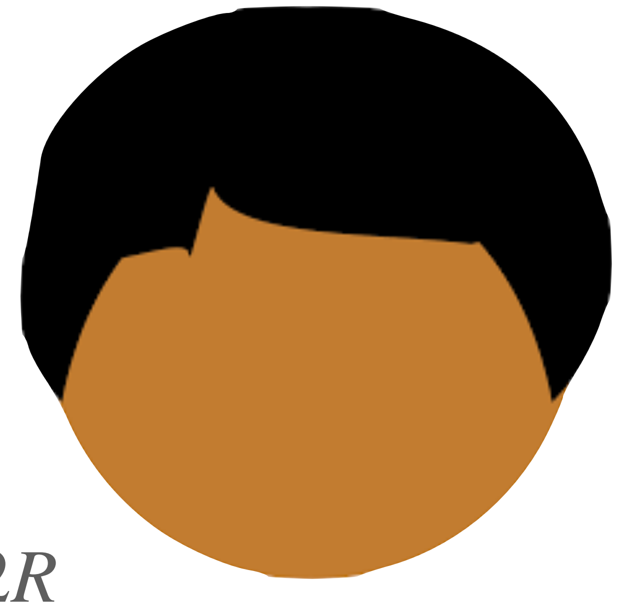
$$\Pr[res_a / res_b / res_c = 0] = \frac{1}{2}$$

$m_{a,1}, m_{a,2}, \cdots, m_{a,2R}$

$\Pi_{a,0}, \Pi_{a,1}, \Pi_{a,2}, \cdots, \Pi_{a,2R}$



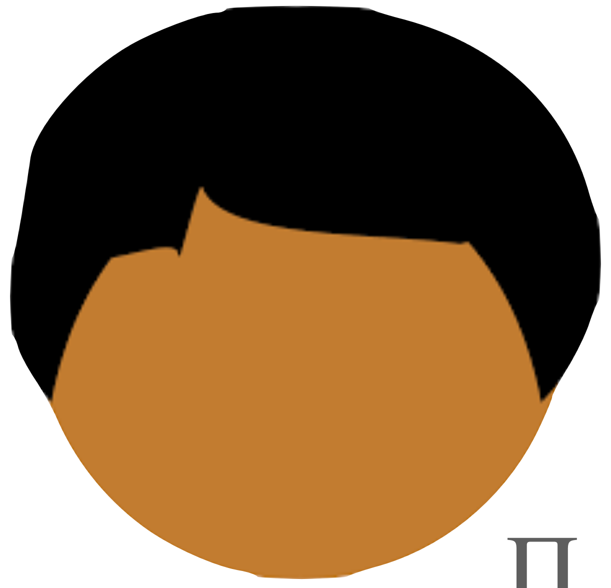
Alice



$m_{b,1}, m_{b,2}, \cdots, m_{b,2R}$

$\Pi_{b,0}, \Pi_{b,1}, \Pi_{b,2}, \cdots, \Pi_{b,2R}$

Bob



$m_{c,1}, m_{c,2}, \cdots, m_{c,2R}$

$\Pi_{c,0}, \Pi_{c,1}, \Pi_{c,2}, \cdots, \Pi_{c,2R}$

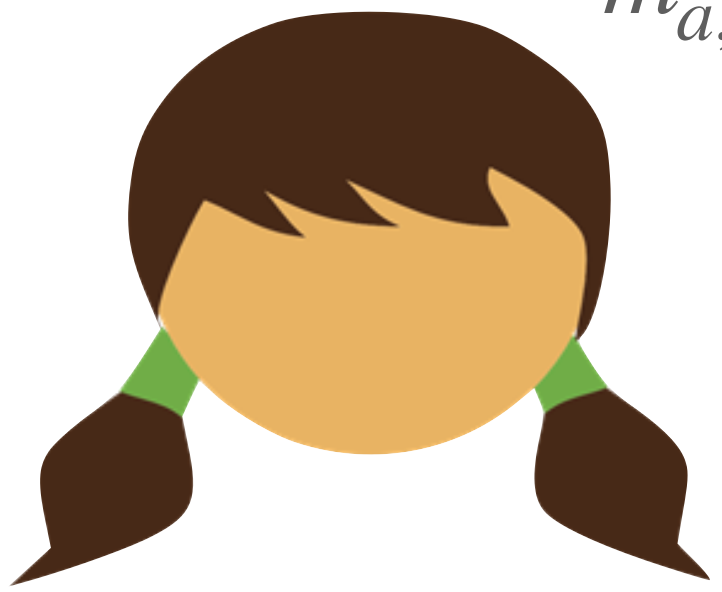
Charlie

Example: Our Lower Bound

Predictor — Known as “backup” coin

$$\Pr[\overbrace{res_a = res_b = res_c}^{res}] = 1$$

$$\Pr[res_a / res_b / res_c = 0] = \frac{1}{2}$$



$m_{a,1}, m_{a,2}, \cdots, m_{a,2R}$

$\Pi_{a,0}, \Pi_{a,1}, \Pi_{a,2}, \cdots, \Pi_{a,2R}$

Alice

Predictability

$\Pr[\Pi_{a,0} = res] = \frac{1}{2}$

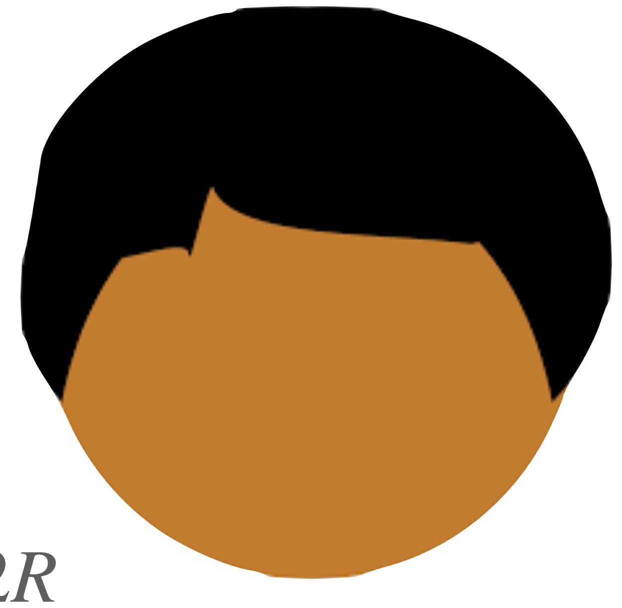
$\Pr[\Pi_{a,2R} = res] = 1$

$\Pr[\Pi_{b,0} = res] = \frac{1}{2}$

$\Pr[\Pi_{b,2R} = res] = 1$

$\Pr[\Pi_{c,0} = res] = \frac{1}{2}$

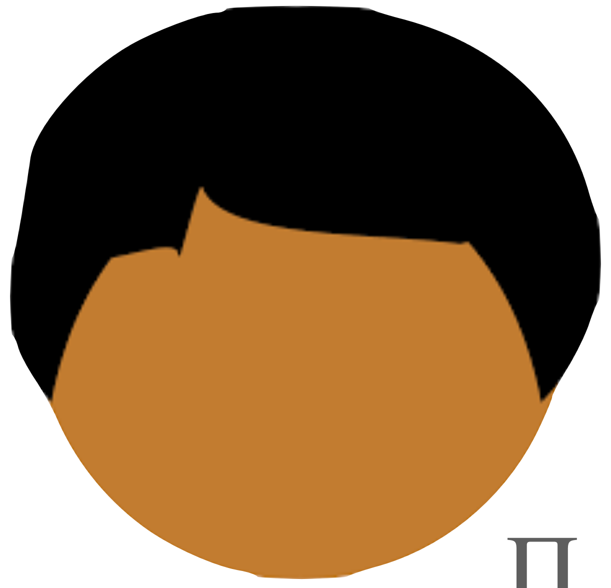
$\Pr[\Pi_{c,2R} = res] = 1$



$m_{b,1}, m_{b,2}, \cdots, m_{b,2R}$

$\Pi_{b,0}, \Pi_{b,1}, \Pi_{b,2}, \cdots, \Pi_{b,2R}$

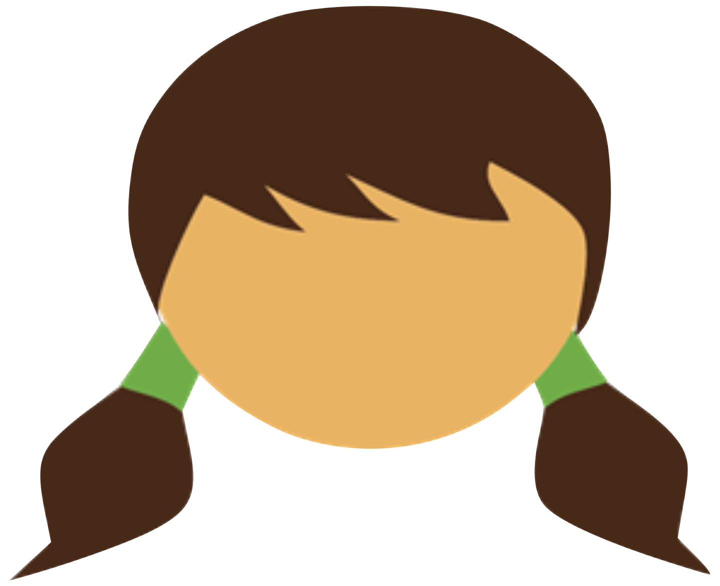
Bob



$m_{c,1}, m_{c,2}, \cdots, m_{c,2R}$

$\Pi_{c,0}, \Pi_{c,1}, \Pi_{c,2}, \cdots, \Pi_{c,2R}$

Charlie



Alice

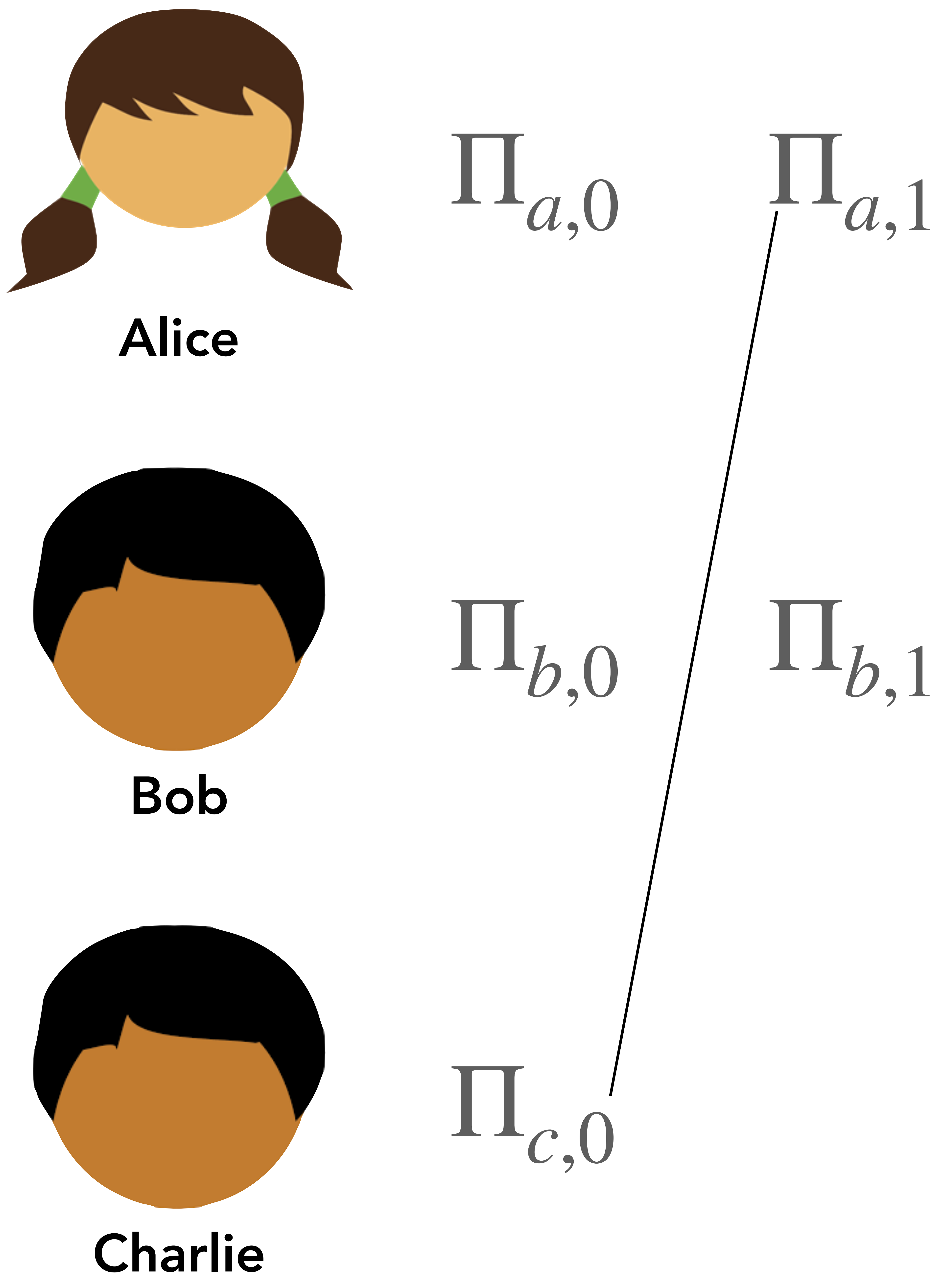
$$\Pi_{a,0}$$

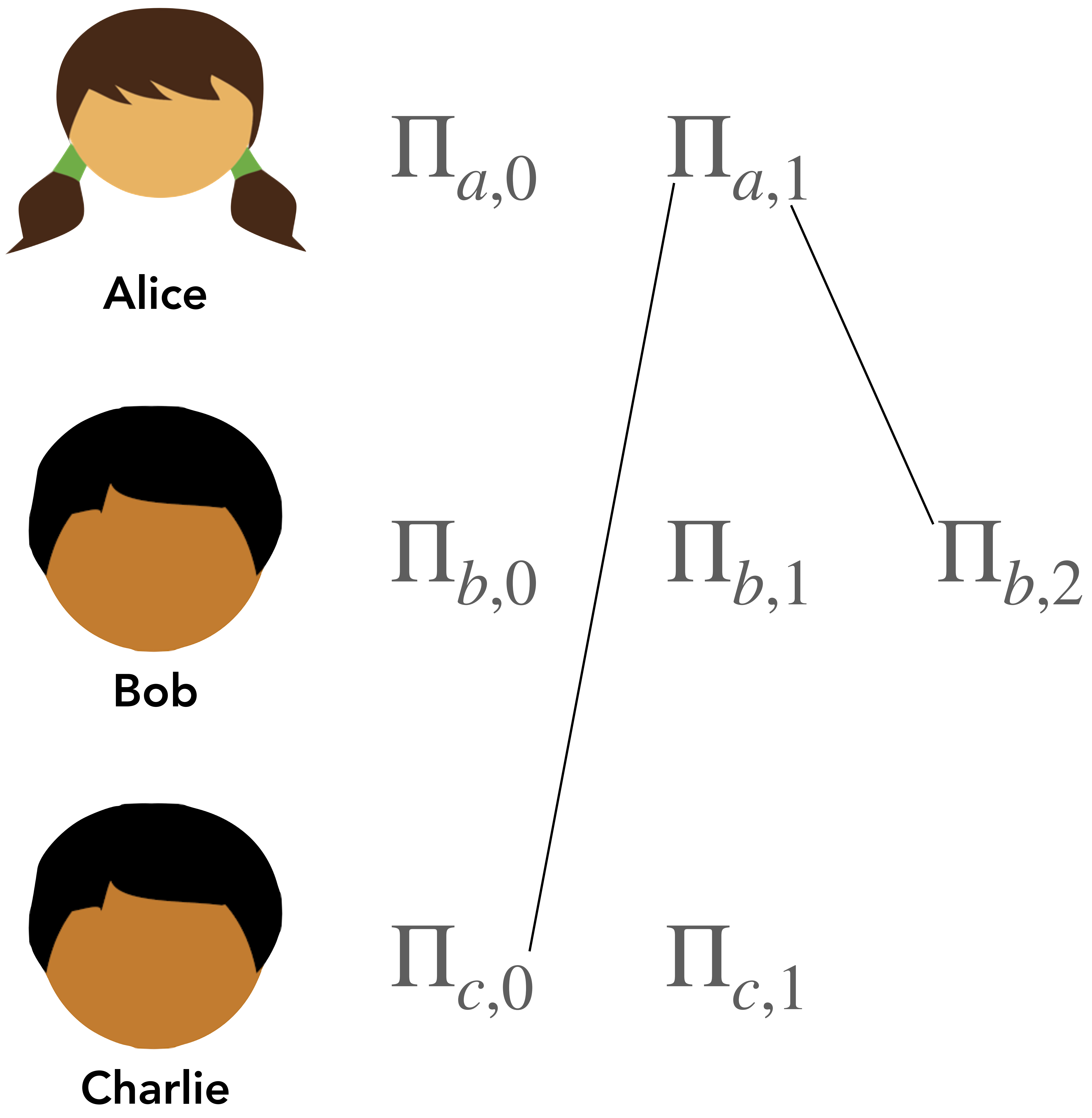
Bob

$$\Pi_{b,0}$$

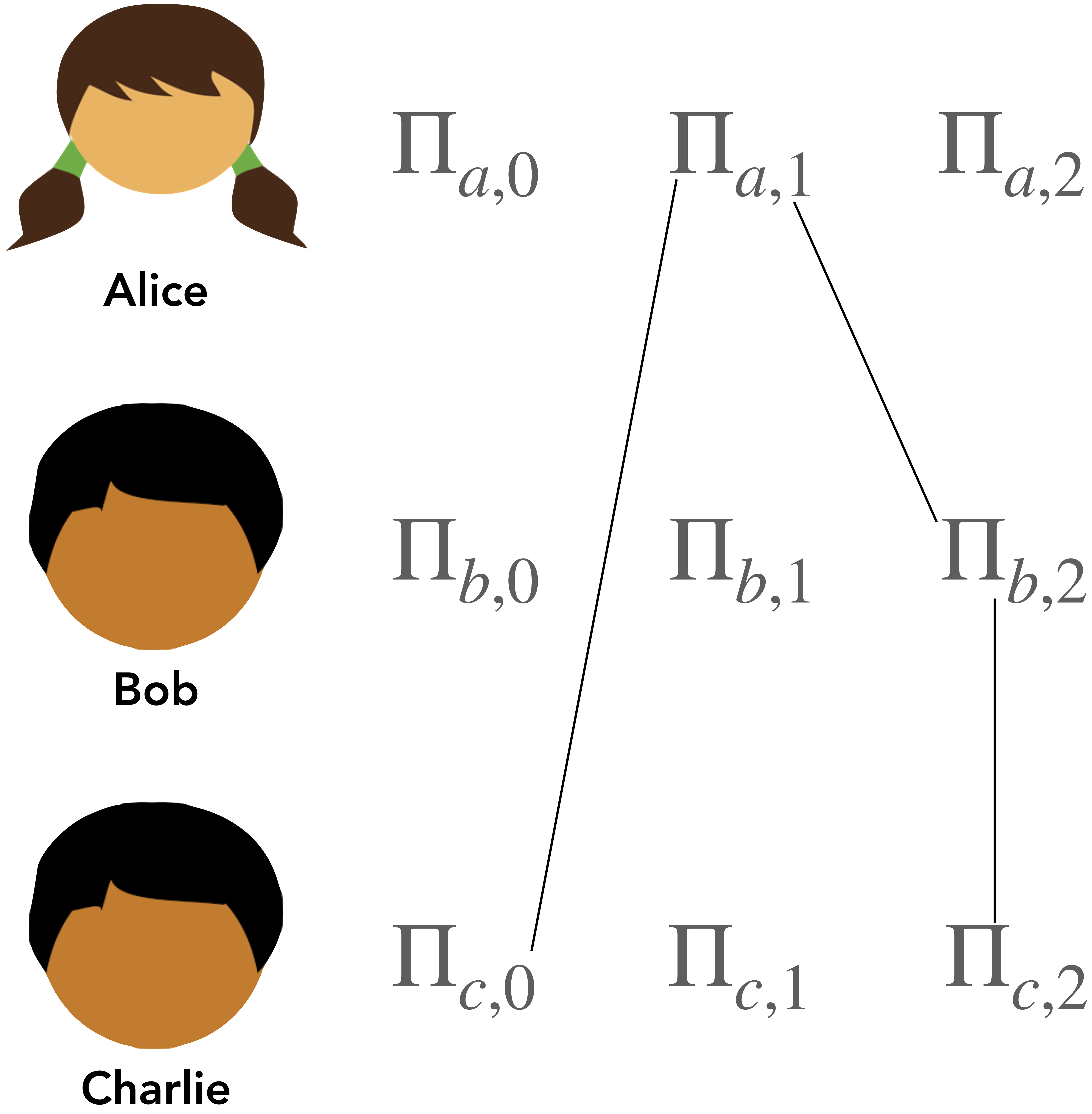
Charlie

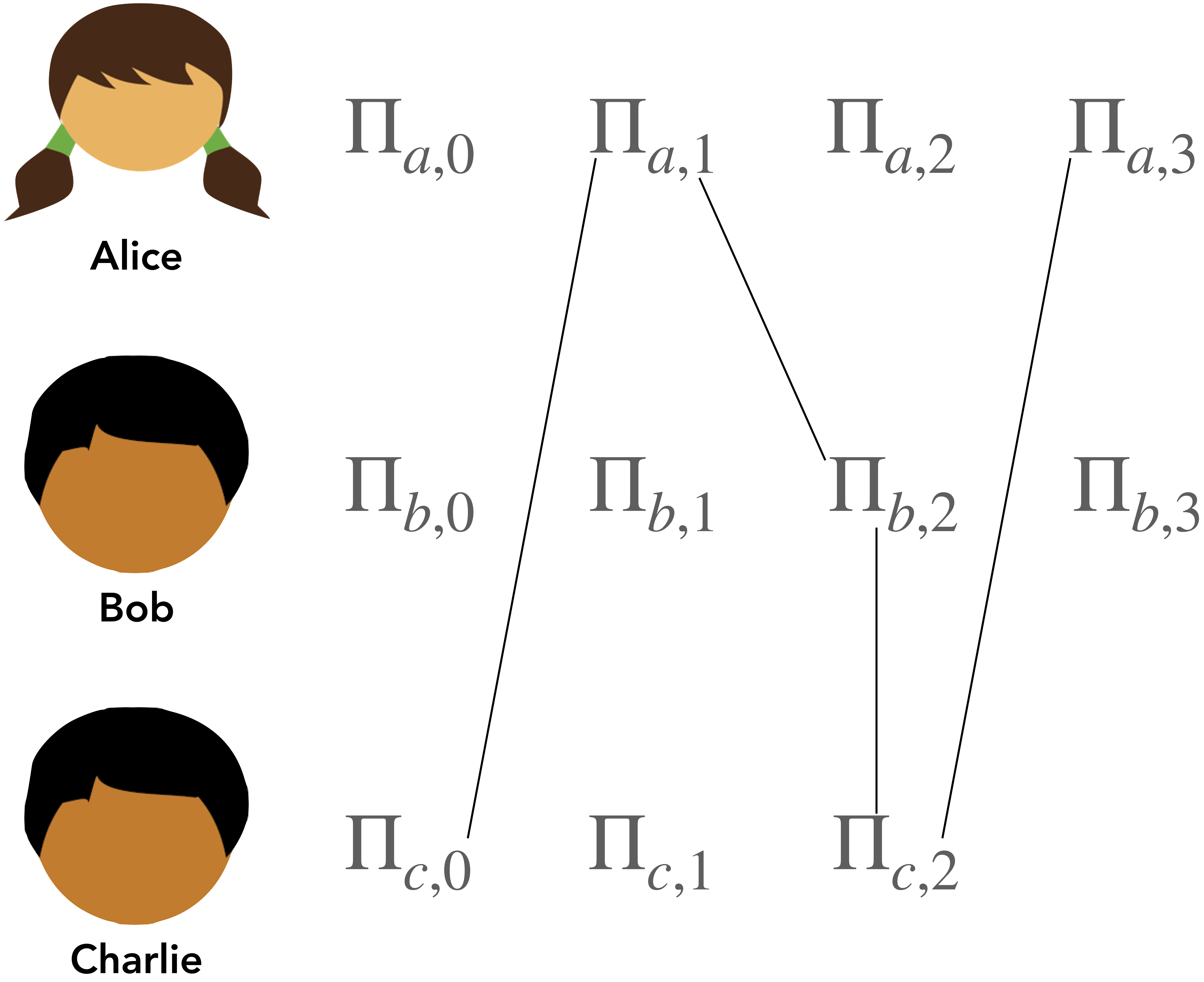
$$\Pi_{c,0}$$

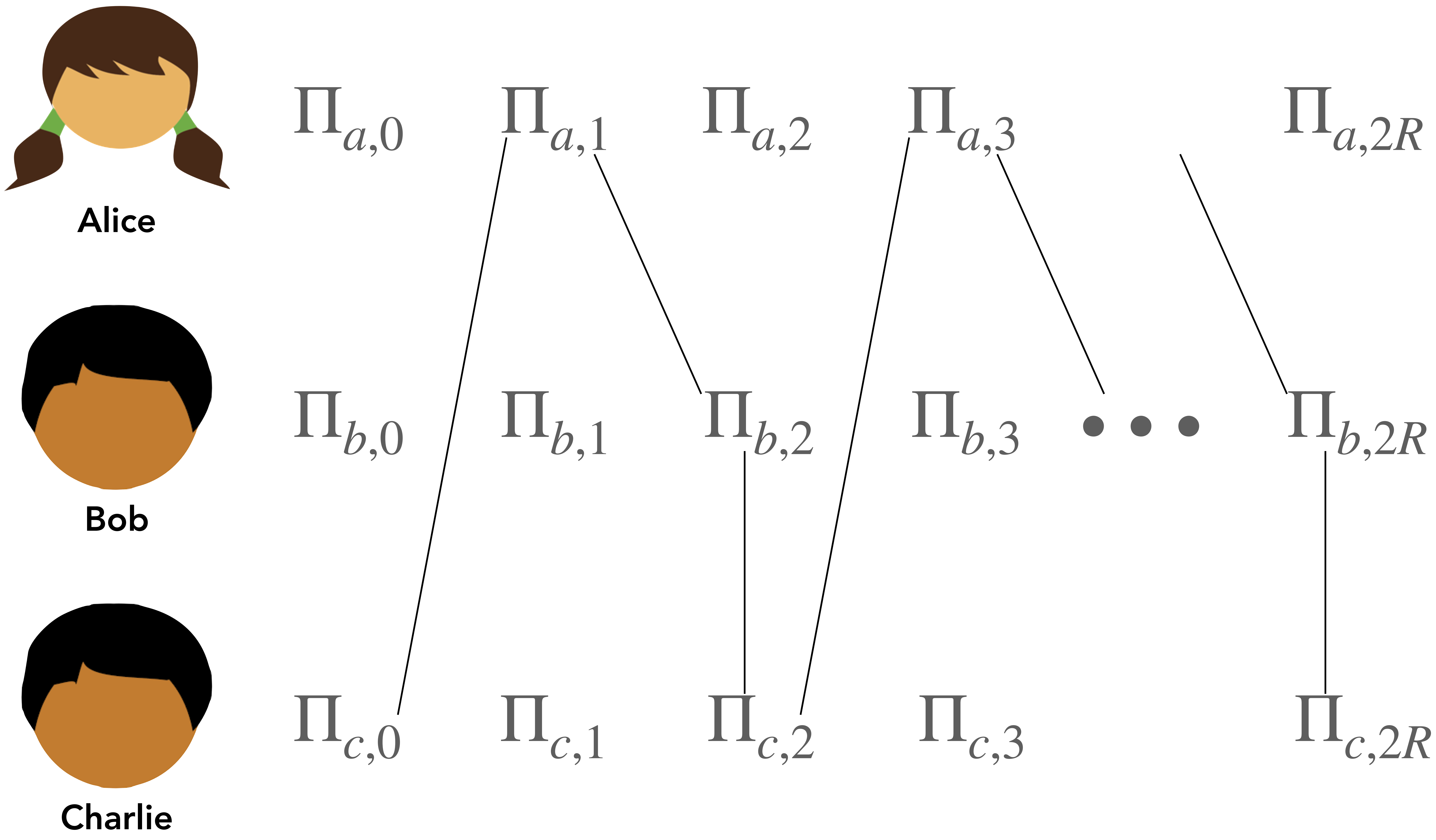

Alice
Bob
Charlie
$\Pi_{a,0}$
$\Pi_{a,1}$
$\Pi_{b,0}$
$\Pi_{b,1}$
$\Pi_{c,0}$



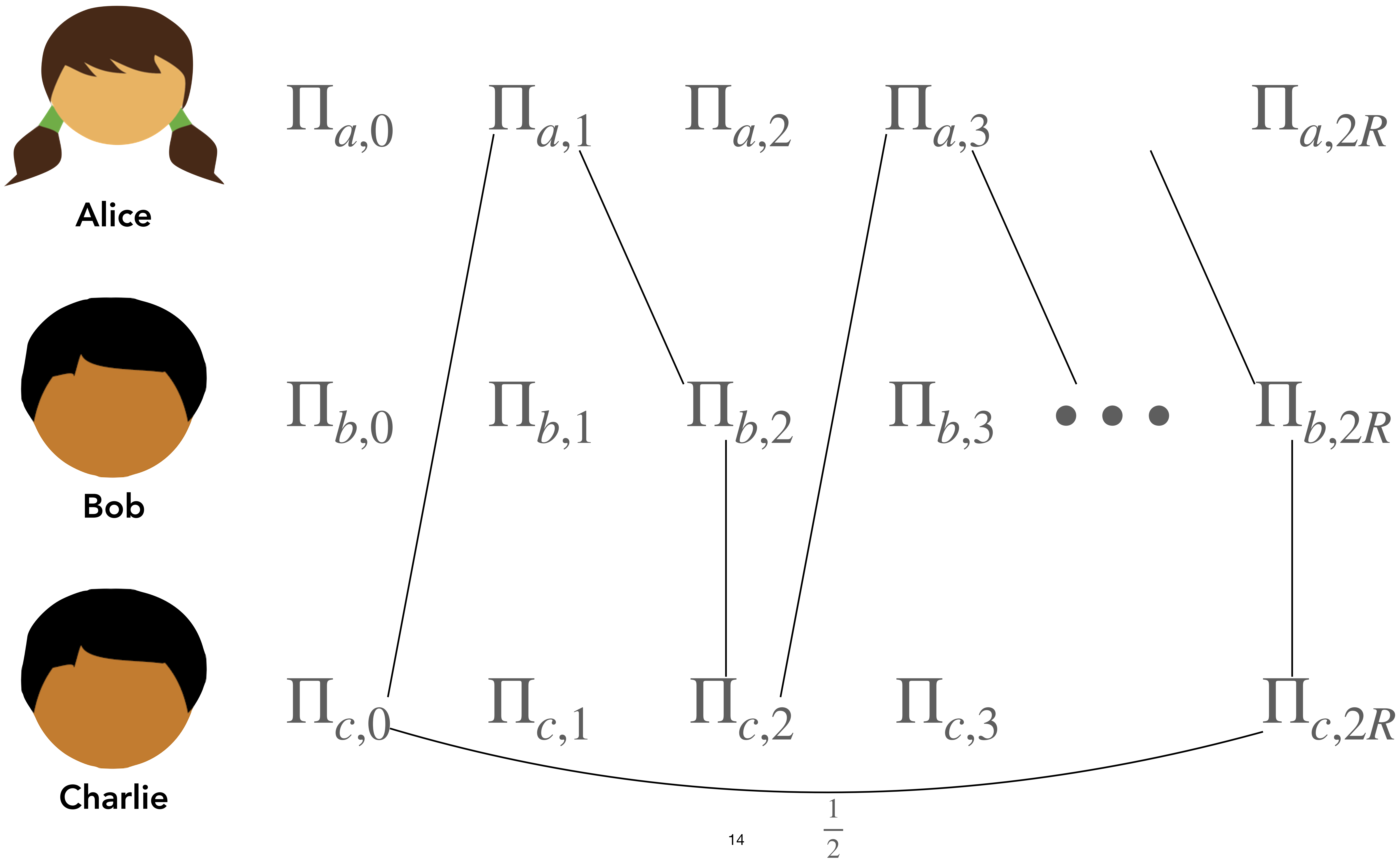
Alice
Bob
Charlie
$\Pi_{a,0}$
$\Pi_{a,1}$
$\Pi_{b,0}$
$\Pi_{b,1}$
$\Pi_{b,2}$
$\Pi_{c,0}$
$\Pi_{c,1}$


Alice
Bob
Charlie
$\Pi_{a,0}$
$\Pi_{a,1}$
$\Pi_{a,2}$
$\Pi_{b,0}$
$\Pi_{b,1}$
$\Pi_{b,2}$
$\Pi_{c,0}$
$\Pi_{c,1}$
$\Pi_{c,2}$

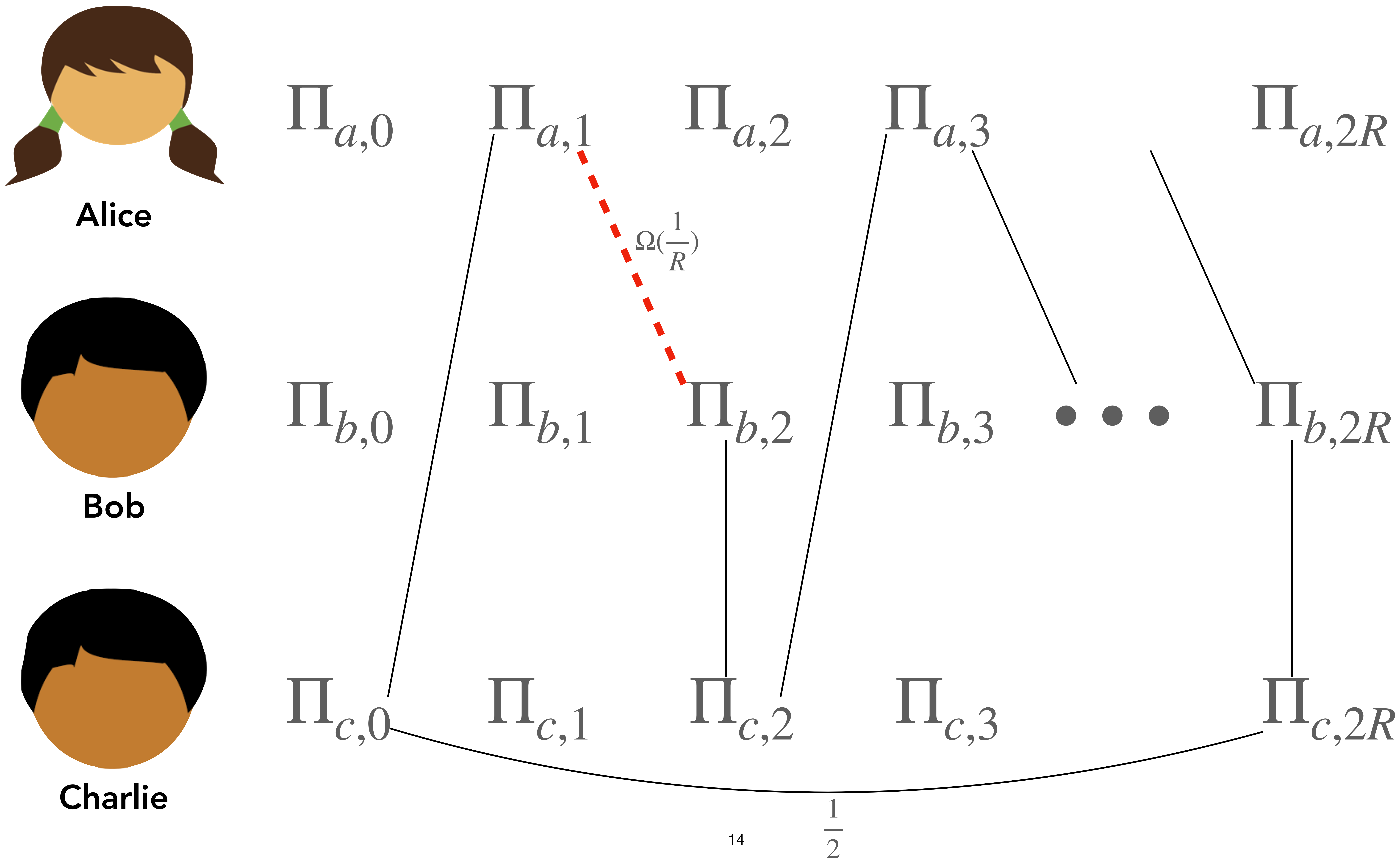

Alice
Bob
Charlie
$\Pi_{a,0}$ $\Pi_{a,1}$ $\Pi_{a,2}$ $\Pi_{a,3}$
$\Pi_{b,0}$ $\Pi_{b,1}$ $\Pi_{b,2}$ $\Pi_{b,3}$
$\Pi_{c,0}$ $\Pi_{c,1}$ $\Pi_{c,2}$



Alice
Bob
Charlie
$\Pi_{a,0}$ $\Pi_{a,1}$ $\Pi_{a,2}$ $\Pi_{a,3}$ $\Pi_{a,2R}$
$\Pi_{b,0}$ $\Pi_{b,1}$ $\Pi_{b,2}$ $\Pi_{b,3}$ $\Pi_{b,2R}$
$\Pi_{c,0}$ $\Pi_{c,1}$ $\Pi_{c,2}$ $\Pi_{c,3}$ $\Pi_{c,2R}$



Alice
Bob
Charlie
$\Pi_{a,0}$ $\Pi_{a,1}$ $\Pi_{a,2}$ $\Pi_{a,3}$ $\Pi_{a,2R}$
$\Pi_{b,0}$ $\Pi_{b,1}$ $\Pi_{b,2}$ $\Pi_{b,3}$ $\cdots$ $\Pi_{b,2R}$
$\Pi_{c,0}$ $\Pi_{c,1}$ $\Pi_{c,2}$ $\Pi_{c,3}$ $\Pi_{c,2R}$
$\frac{1}{2}$


Alice
Bob
Charlie
$\Pi_{a,0}$
$\Pi_{a,1}$
$\Pi_{a,2}$
$\Pi_{a,3}$
$\Pi_{a,2R}$
$\Omega(\frac{1}{R})$
$\Pi_{b,0}$
$\Pi_{b,1}$
$\Pi_{b,2}$
$\Pi_{b,3}$
$\Pi_{b,2R}$
$\Pi_{c,0}$
$\Pi_{c,1}$
$\Pi_{c,2}$
$\Pi_{c,3}$
$\Pi_{c,2R}$
$\frac{1}{2}$

Future Work

Does an unreactive world enable more fair functionalities?

Can we fairly toss a coin that agrees with $\frac{1}{2} + \text{non-negl}(\lambda)$ probability?

How to instantiate our upper bound protocols?

Q/A

ePrint: https://eprint.iacr.org/2022/1655