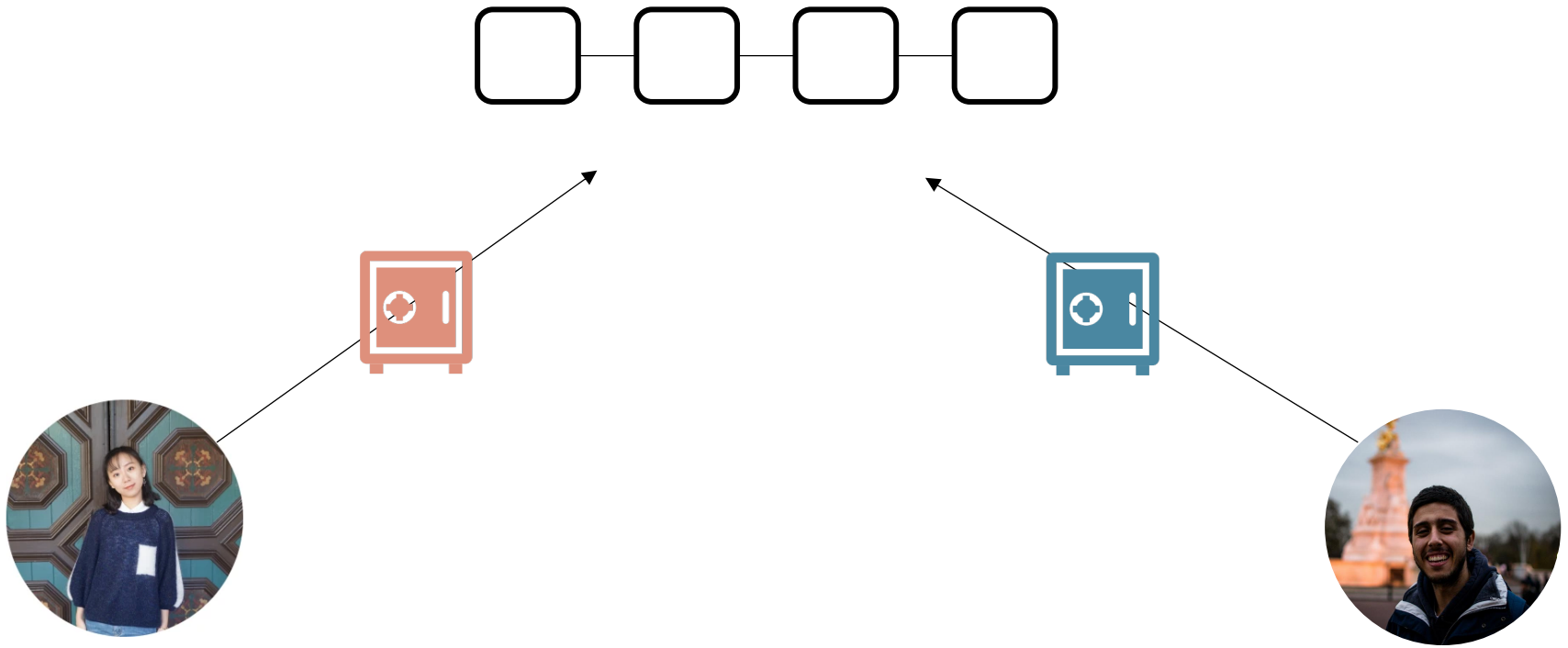
A Complete Characterization of Game-Theoretically Fair, Multi-Party Coin Toss

Gilad Asharov, Elaine Shi, and **Ke Wu**

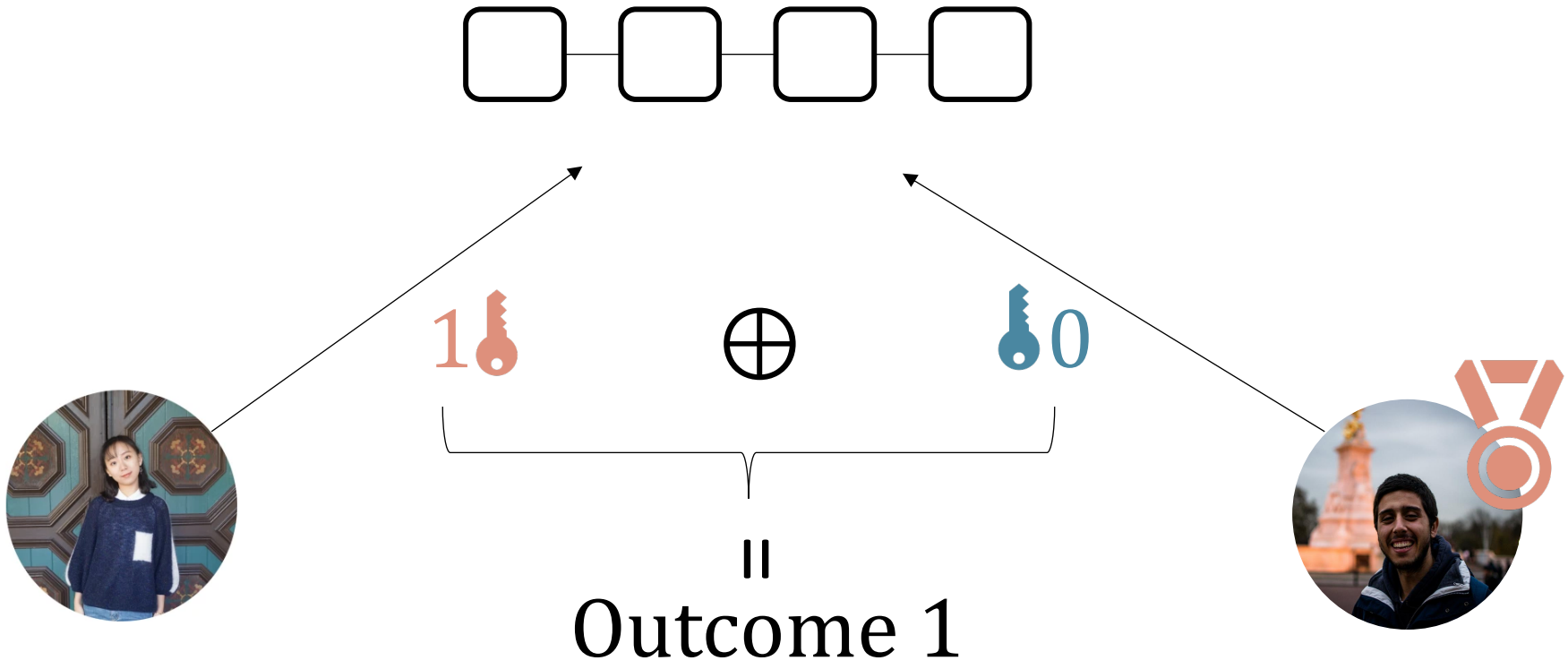
What to eat for crypto seminar?

Sushi!

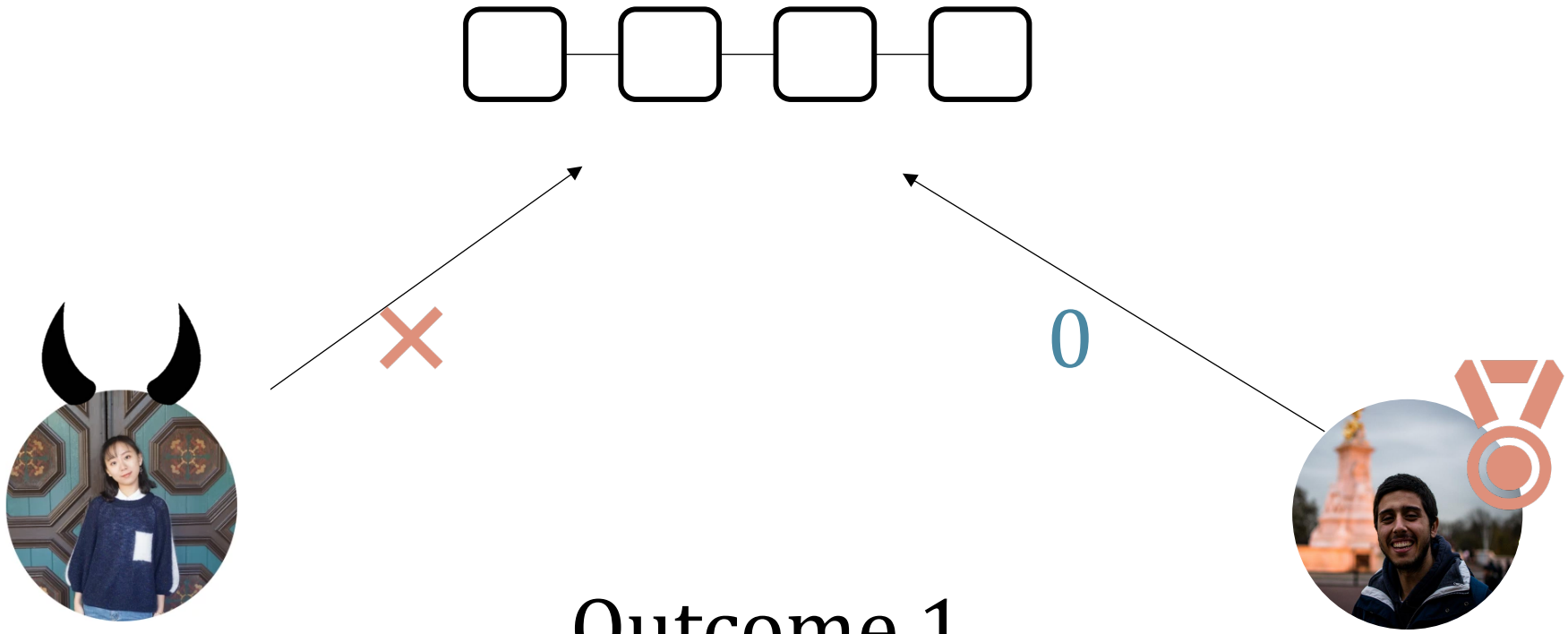
Cake!



[Blum 83]



[Blum 83]



[Blum 83]

Coin toss protocol

- Correctness: if all honest, output is uniformly random.

- Strong fairness: strategic player cannot bias the output. ✗

Impossible due to [Cle86]

Coin toss protocol

- Correctness: if all honest, output is uniformly random.

- Game-theoretic fairness: strategic player cannot benefit herself.

? Game-theoretic fair n-party coin toss?

Coalition

Sushi!

Cake!

$$\text{Utility}=\begin{cases}1, & \text{if I like output}\\ 0, & \text{otherwise}\end{cases}$$

Multi-party coin toss protocol

- Correctness: if all honest, output is uniformly random.

- Game-theoretic fairness: a coalition cannot increase its expected utility.

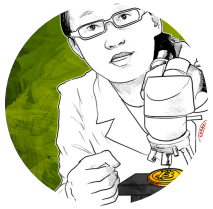
Honest protocol is a Nash equilibrium!

Why we care?

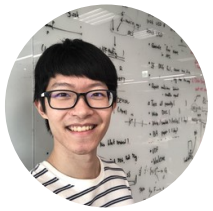
Strong fairness is impossible if half sized coalition.

Want fairness against majority sized coalition.

? Game-theoretic fair n-party coin toss?

Sushi!





Cake!

☹ Impossible against $(n-1)$-coalition due to [CGL+18].

Smaller coalition

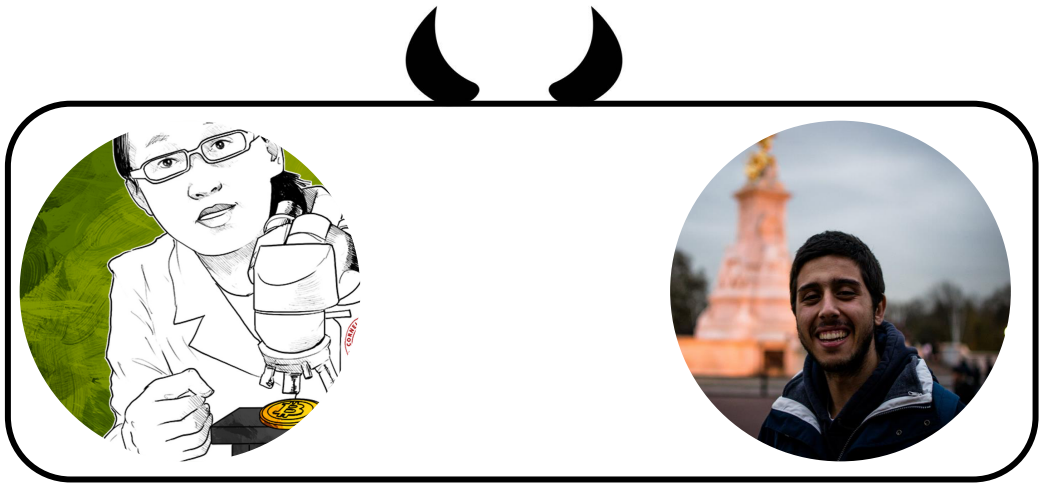
? Game-theoretic fair n-party coin toss against $< n - 1$?

Yes!

A strawman solution

Sushi!

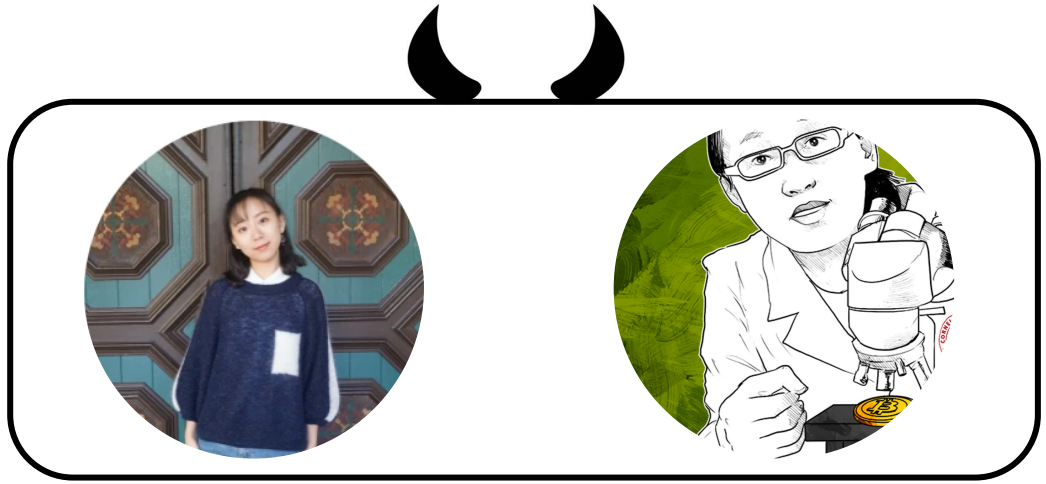
Cake!



Sushi!

Cake!

No preference



Sushi!

Cake!

Cannot benefit

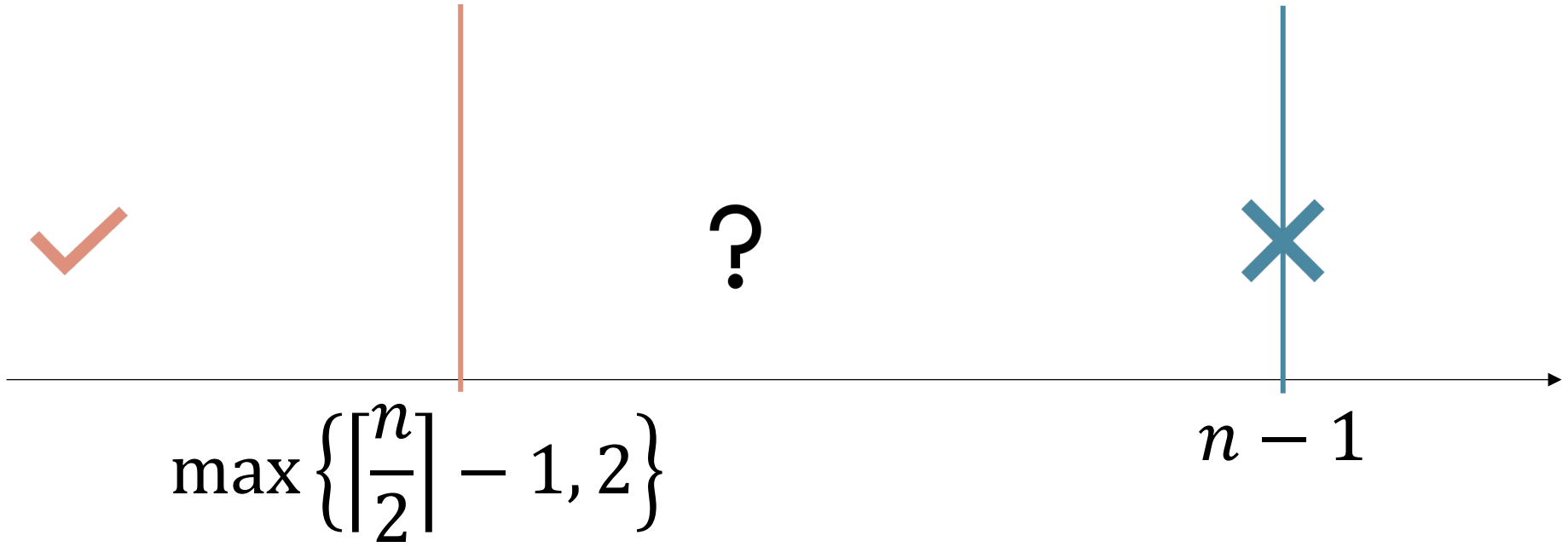
Sushi!

Cake!

Cannot tolerate coalition of size 3

Feasible region?

Under what size of coalition is it possible to achieve game-theoretic fairness?



Complete characterization

- A game-theoretic fair coin toss against t-coalition.

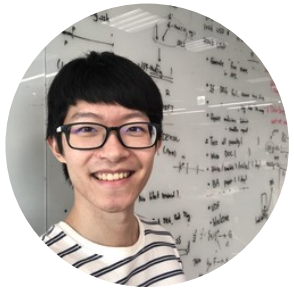
- Game-theoretic fairness is impossible against $(t + 1)$-coalition.

Protocol

Sushi!

Cake!

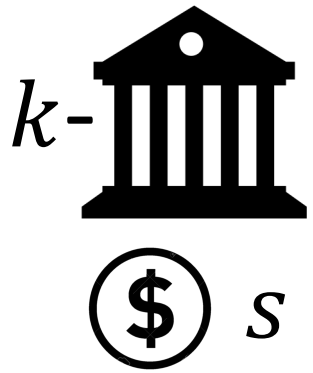




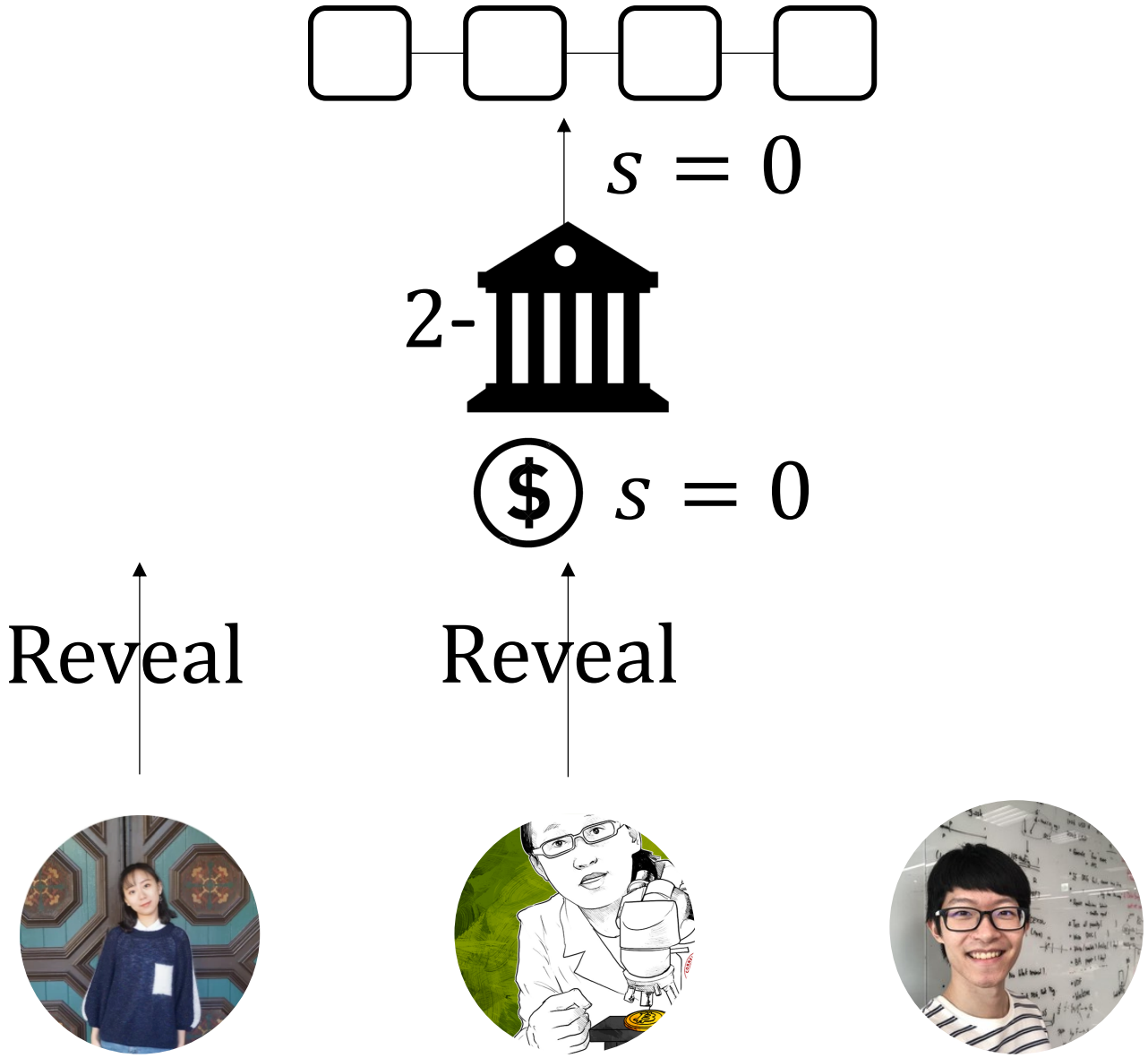

s_0 $\oplus$ s_1

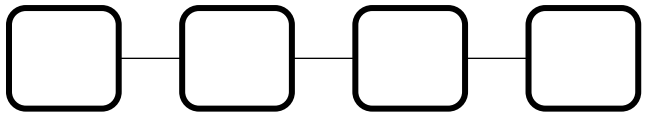
Outcome

Secret sharing trusted authority



- Only $\geq k$ players can ask to reveal s.
- Any $\geq k$ players can rewrite s;

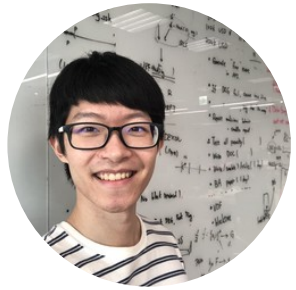

$s = 0$
2-
$
$s = 0$
Reveal
Reveal



2- 

 $s = 0$

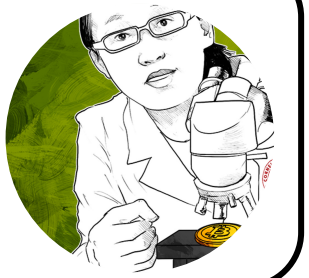
Reveal

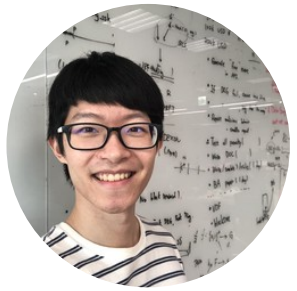


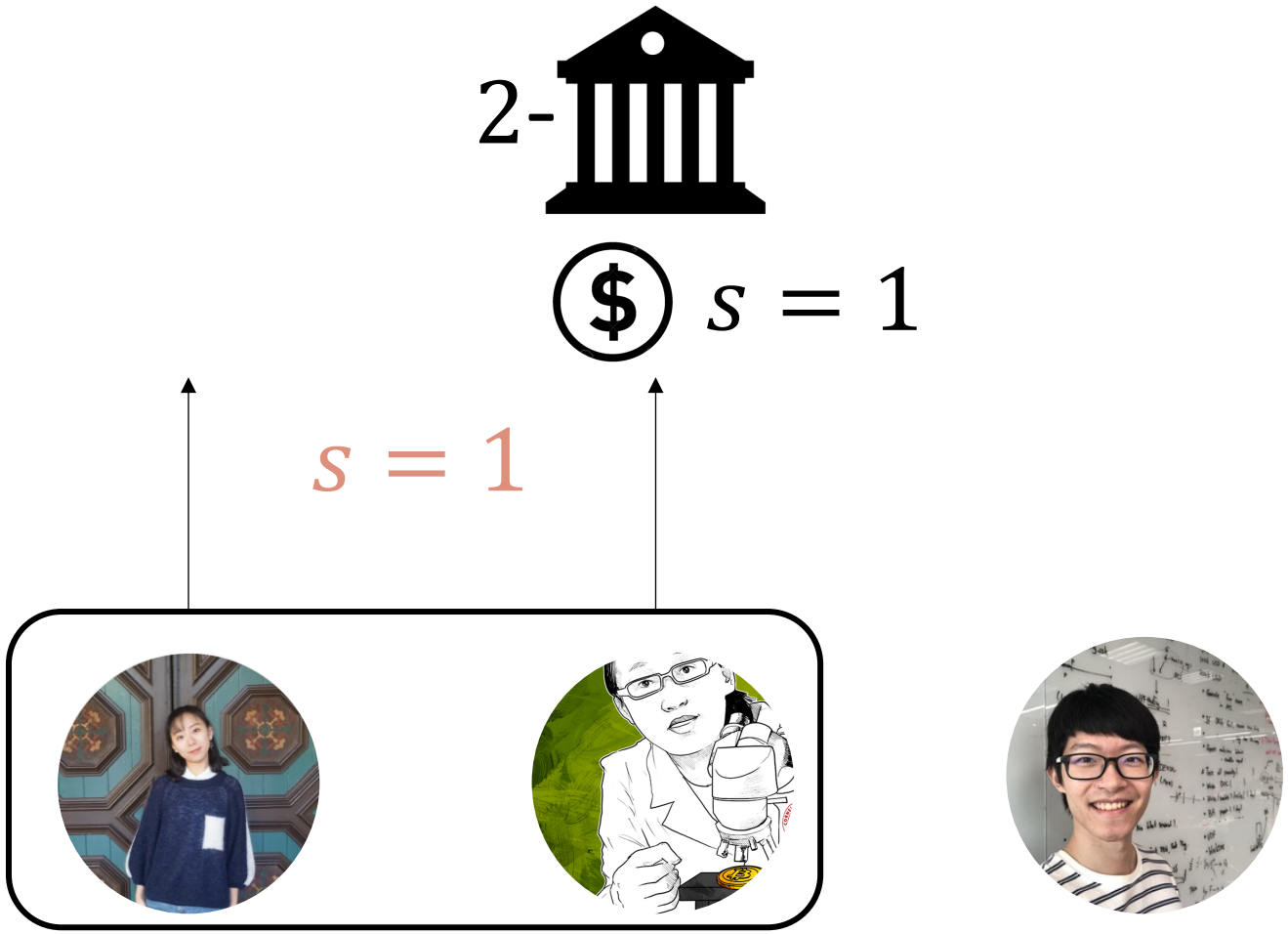
2-

$s = 0$

$s = 1$

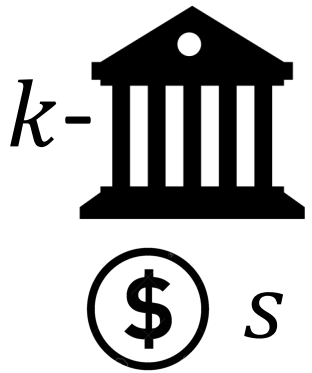






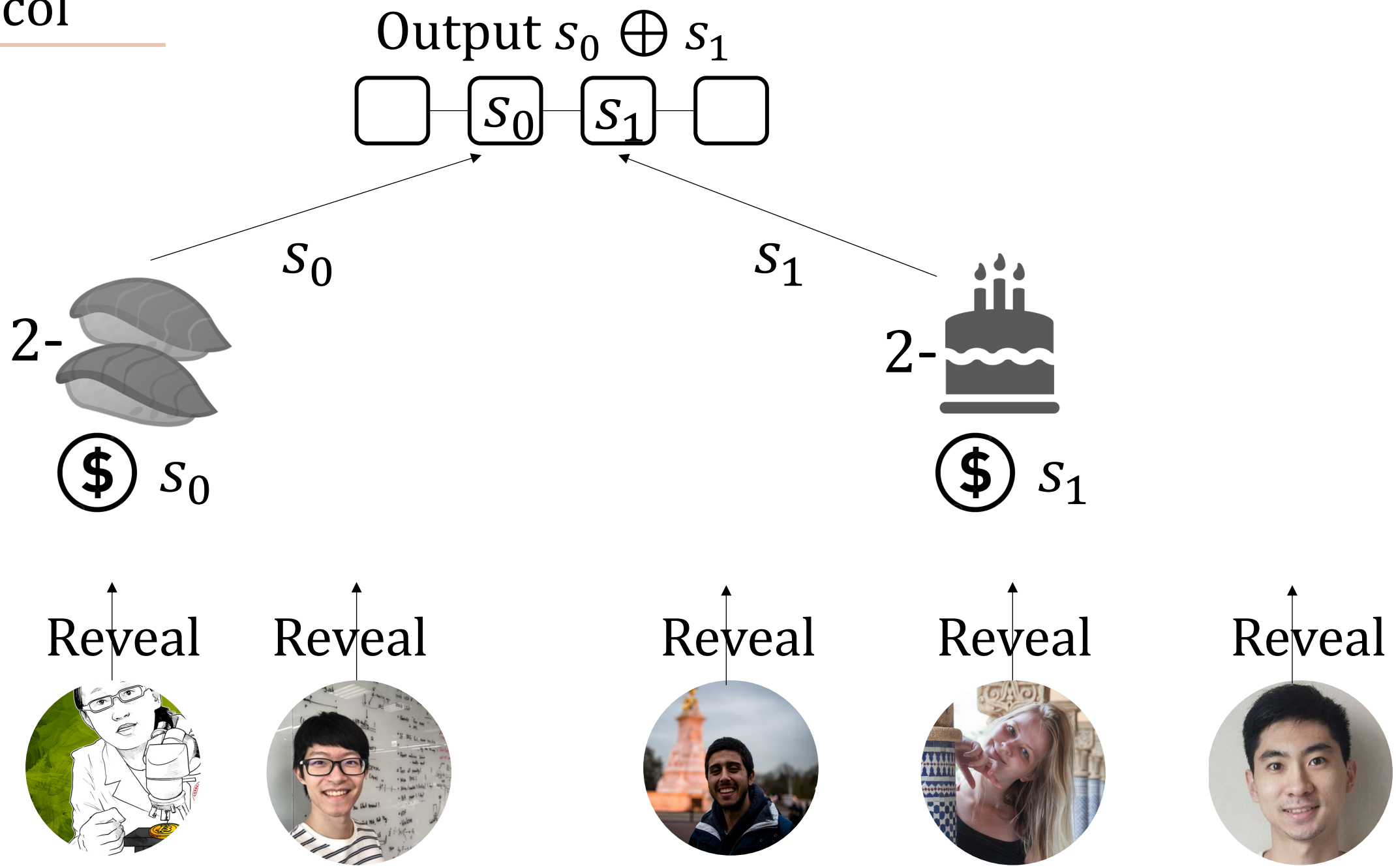
Only rewrite once before any reveal request.

Summary of trusted authority

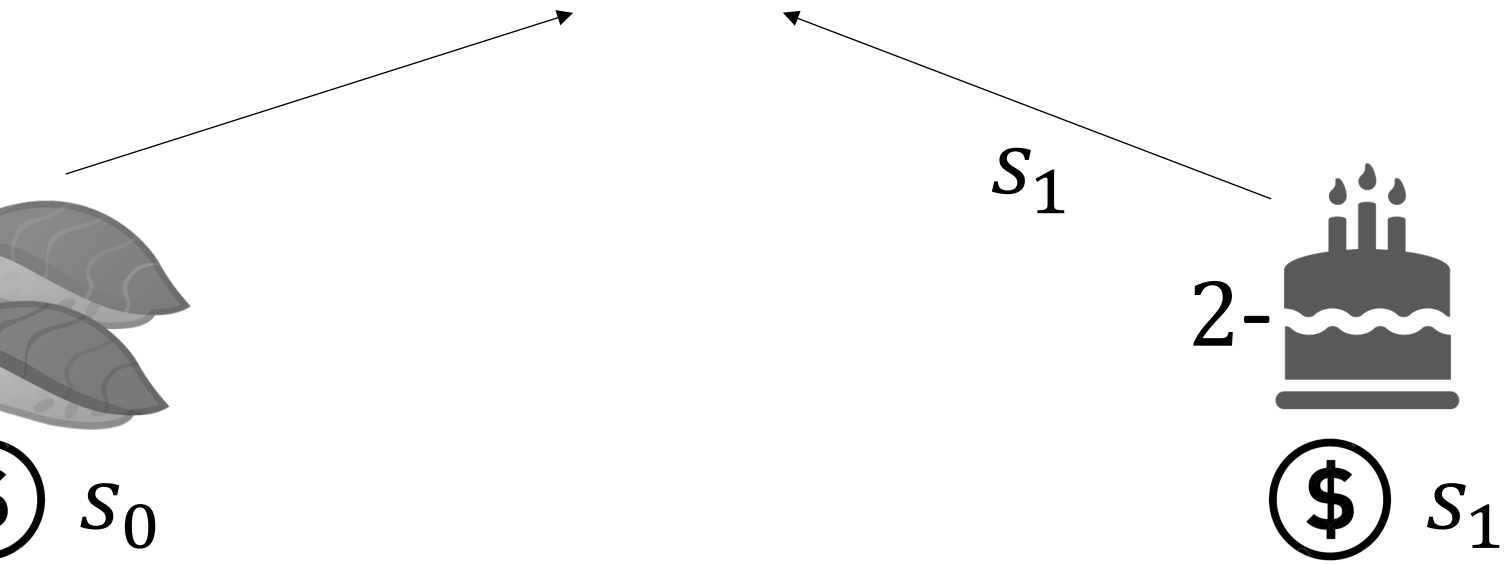


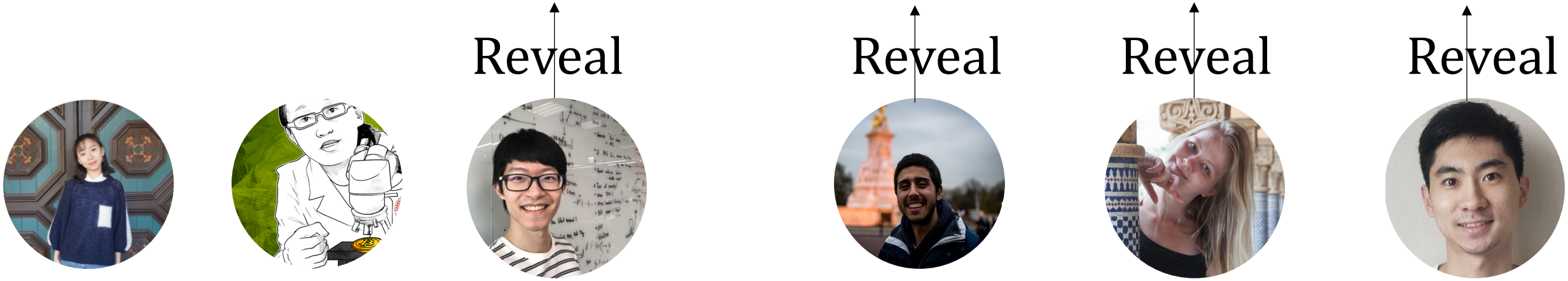
- Only $\geq k$ players can ask to reveal s.
- Any $\geq k$ players can rewrite s before reveal;

Our protocol

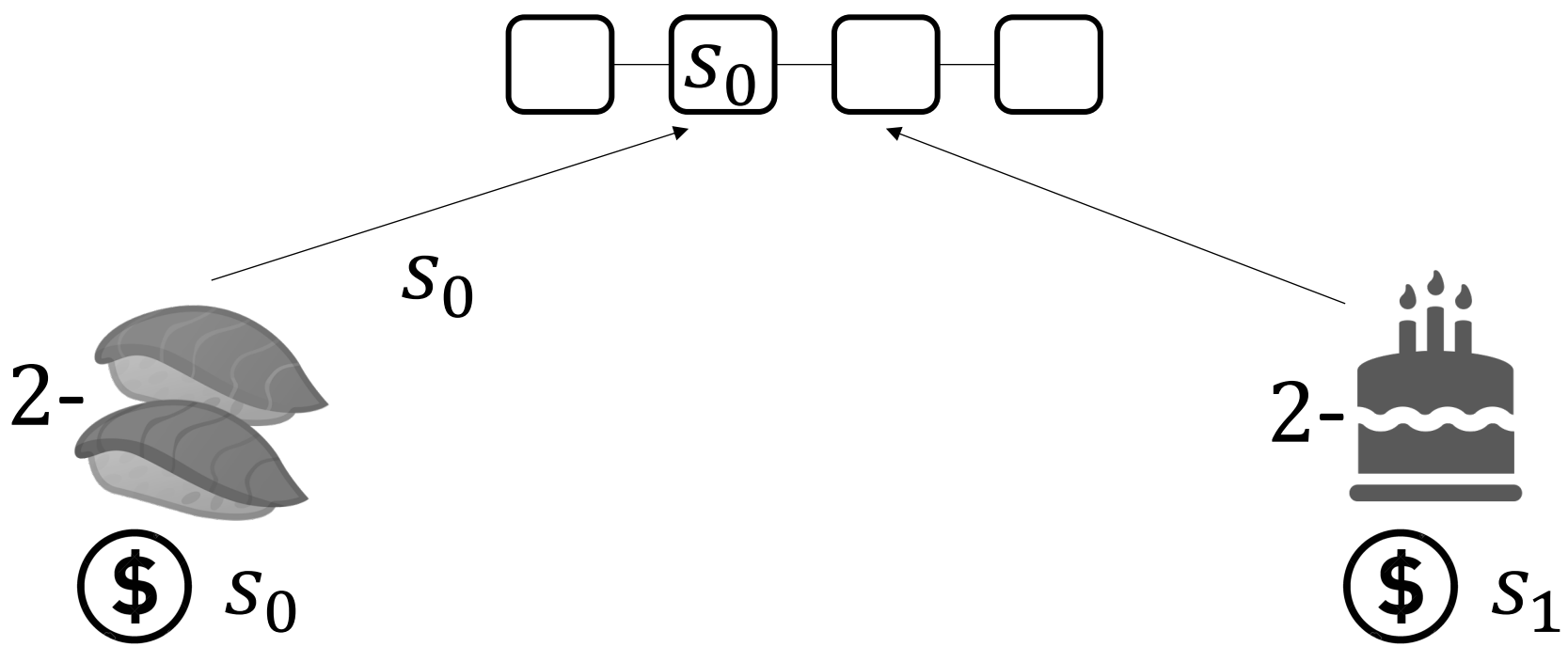


Output s_1



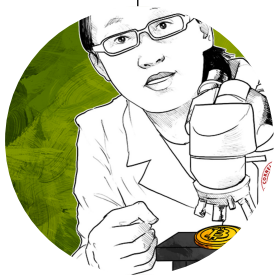


Output s_0?

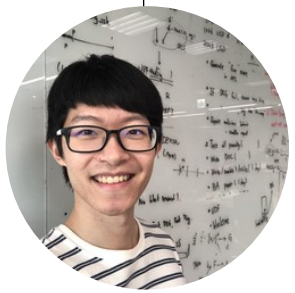


Reveal

Reveal

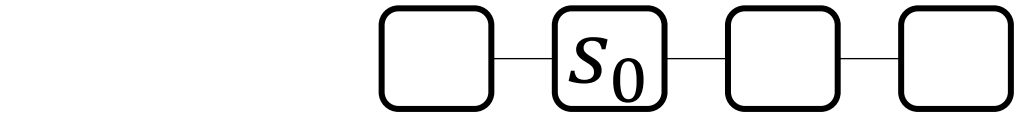


Reveal



Reveal

Output 0!

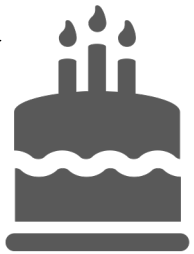


s_0

2-

$ s_0

2-

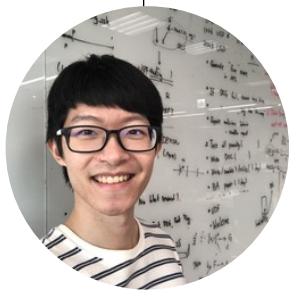


$ s_1

Reveal

Reveal

Reveal

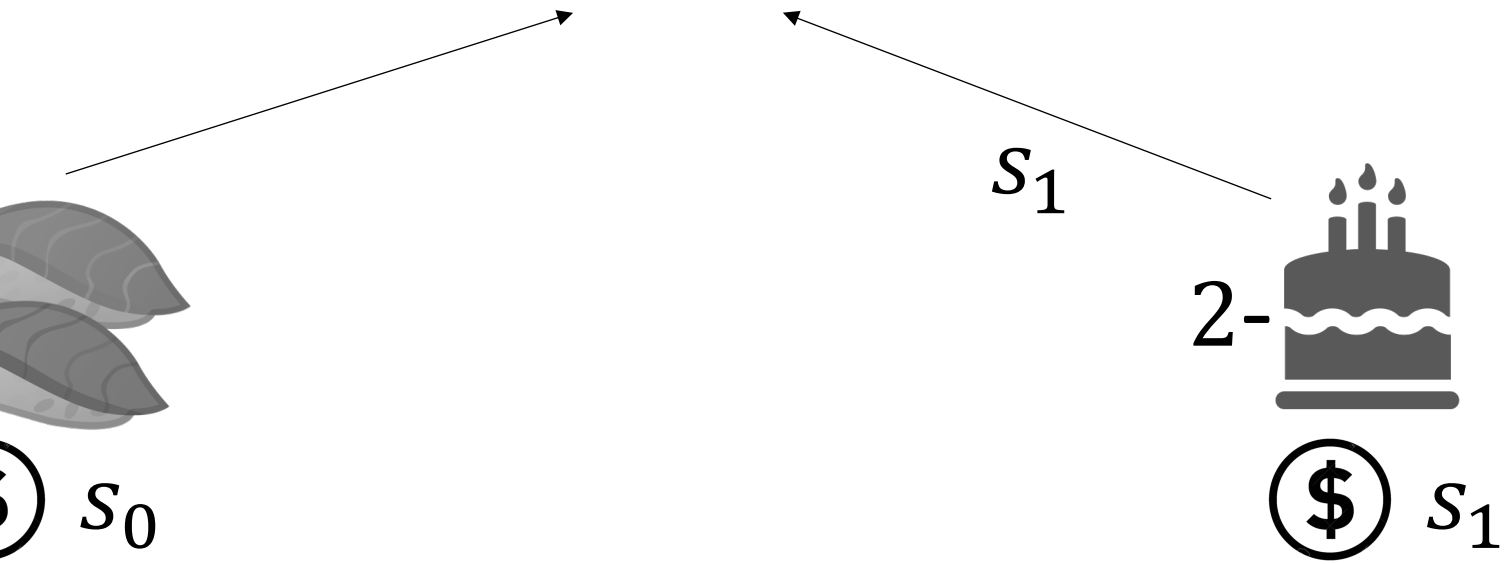


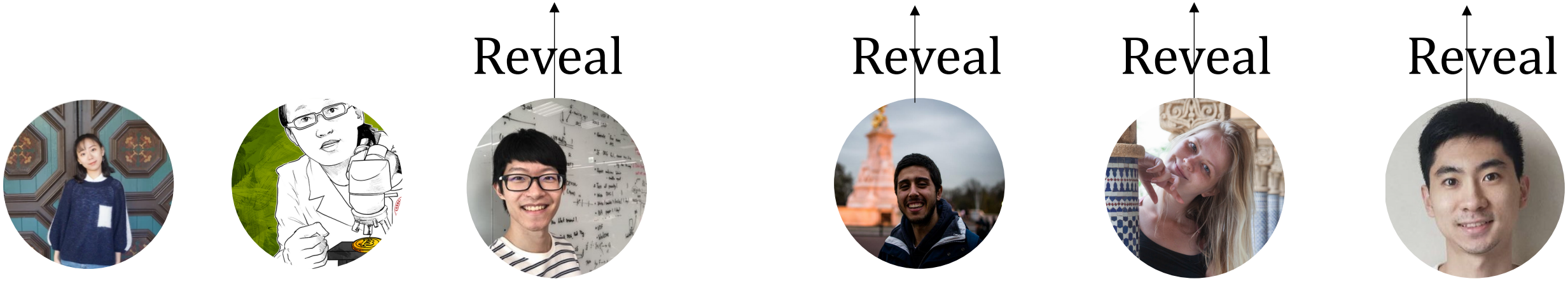
Reveal

Asymmetric

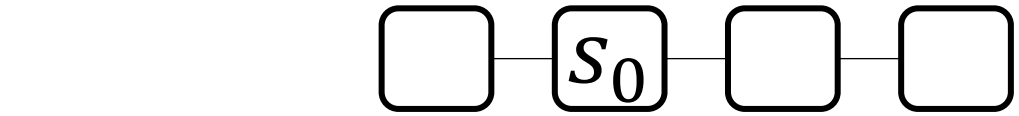
Why is this protocol asymmetric?

Output s_1





Output 0!

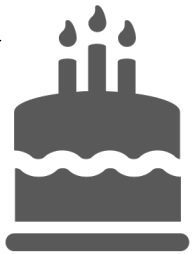


s_0

2-

$ s_0

2-

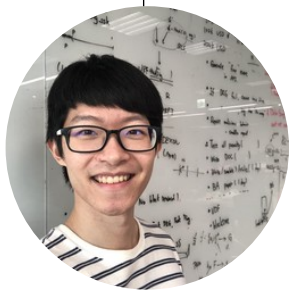


$ s_1

Reveal

Reveal

Reveal

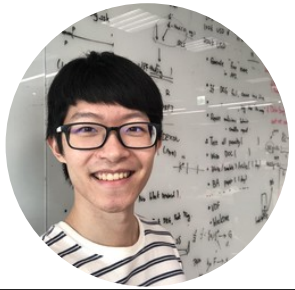


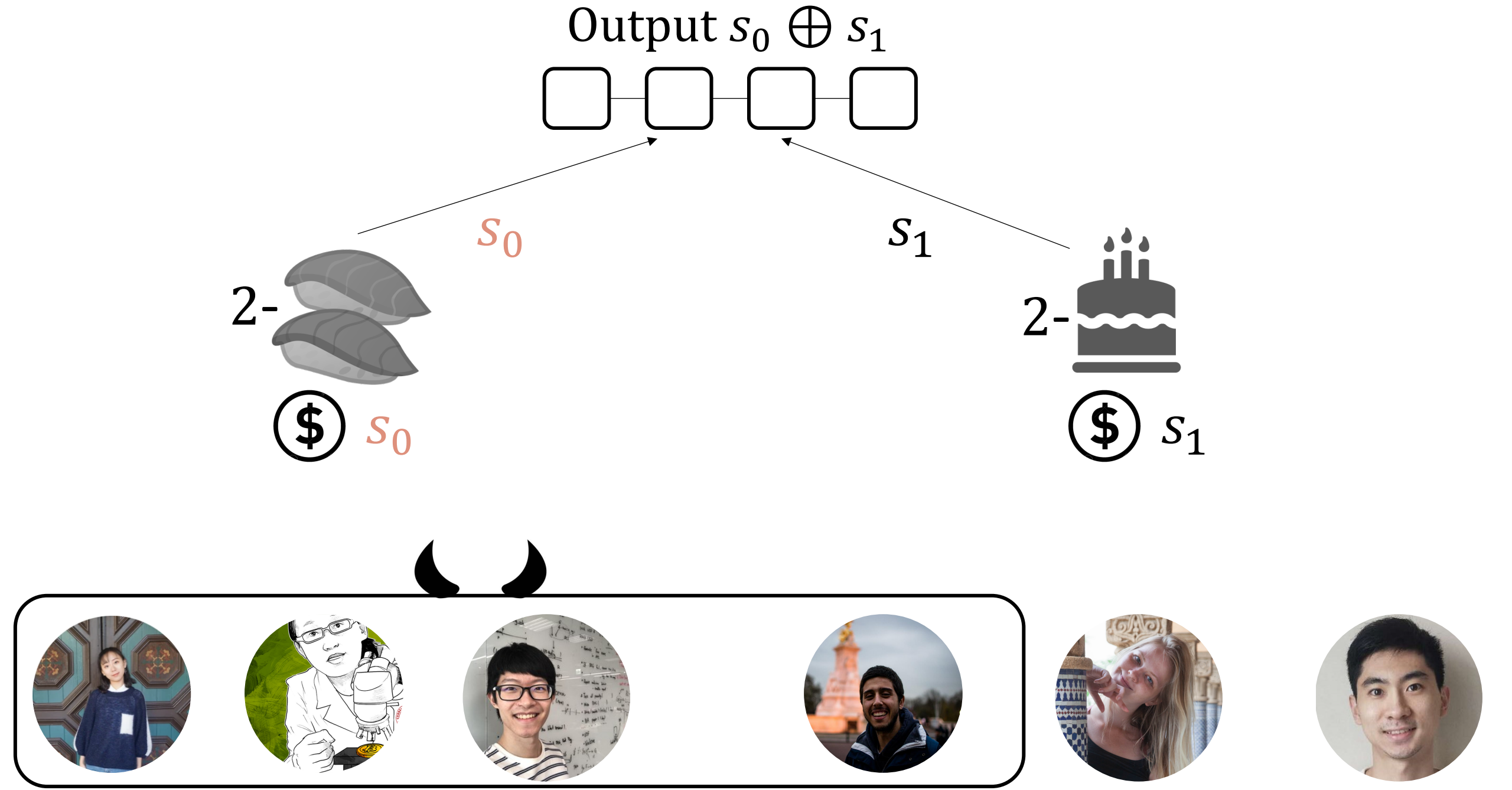
Reveal

Fairness against coalition of size 4

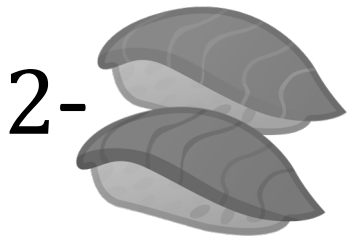
No preference







Output $s_0 \oplus s_1$
s_0
s_1
2-
2-
s_0
s_1

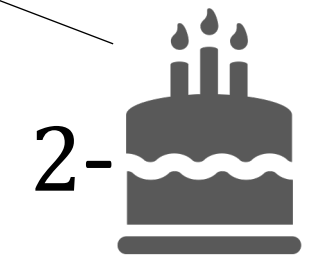
Output s_1



2-

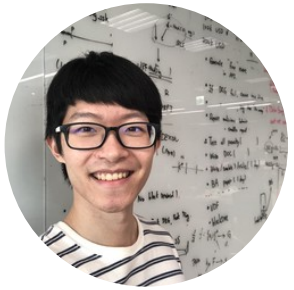
s_0

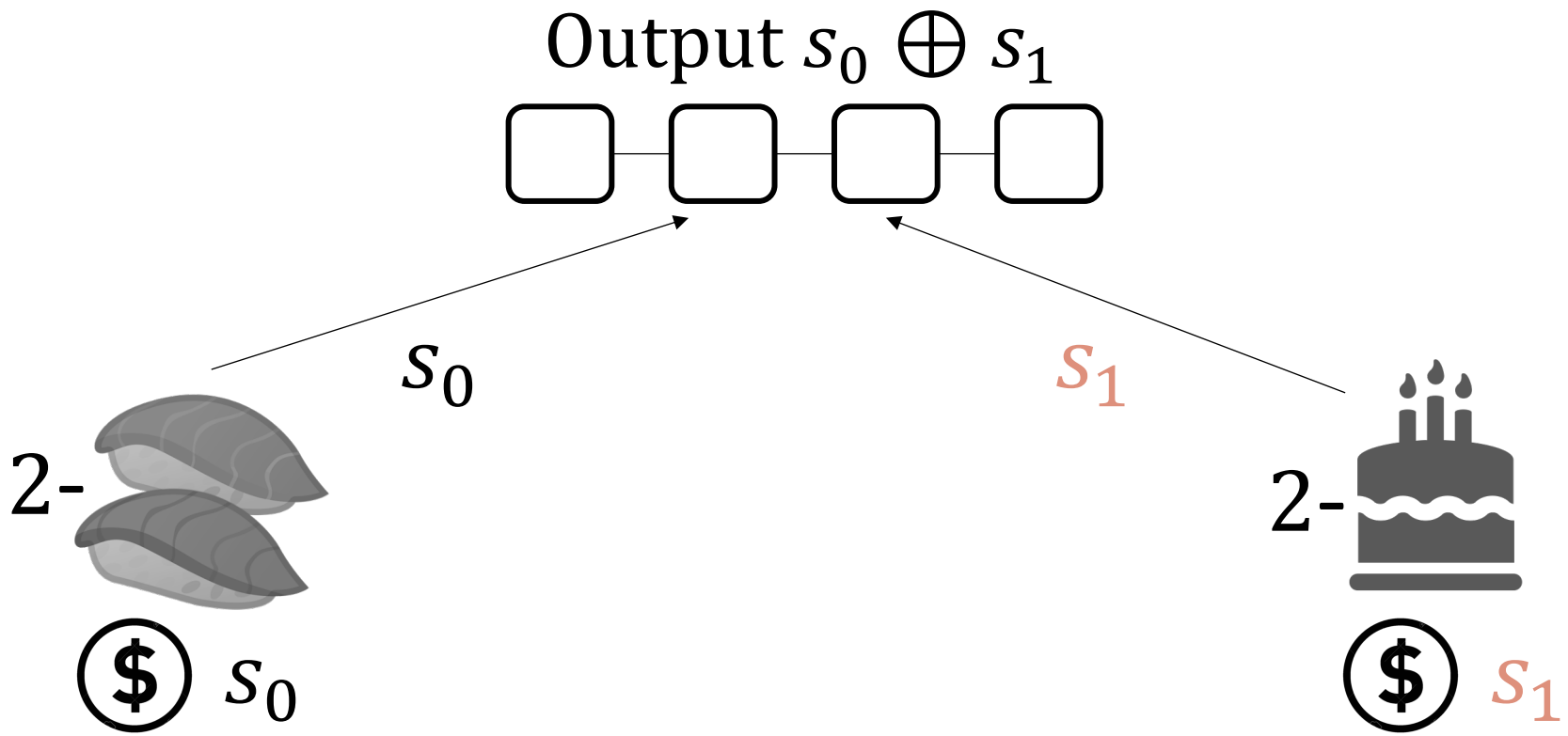
s_1

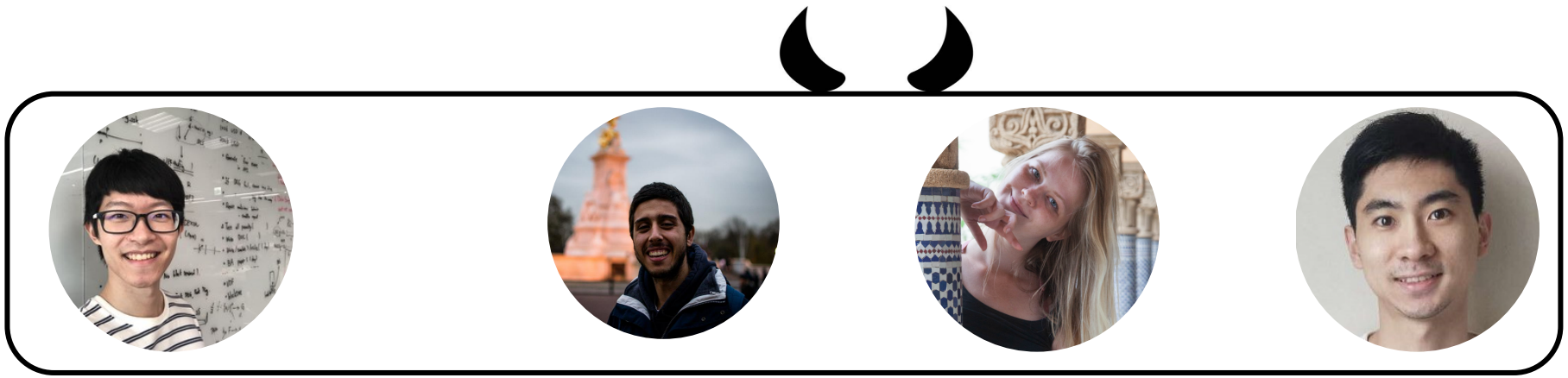


2-

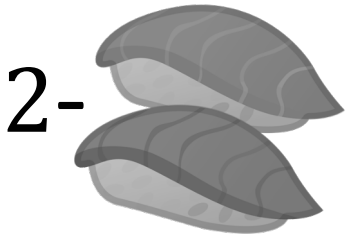
s_1




Output $s_0 \oplus s_1$
s_0
s_1
2-
2-
s_0
s_1



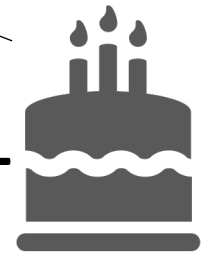
Output 0!



2-

s_0

s_0



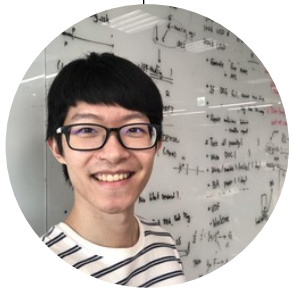
2-

s_1

Reveal

Reveal

Reveal



Reveal

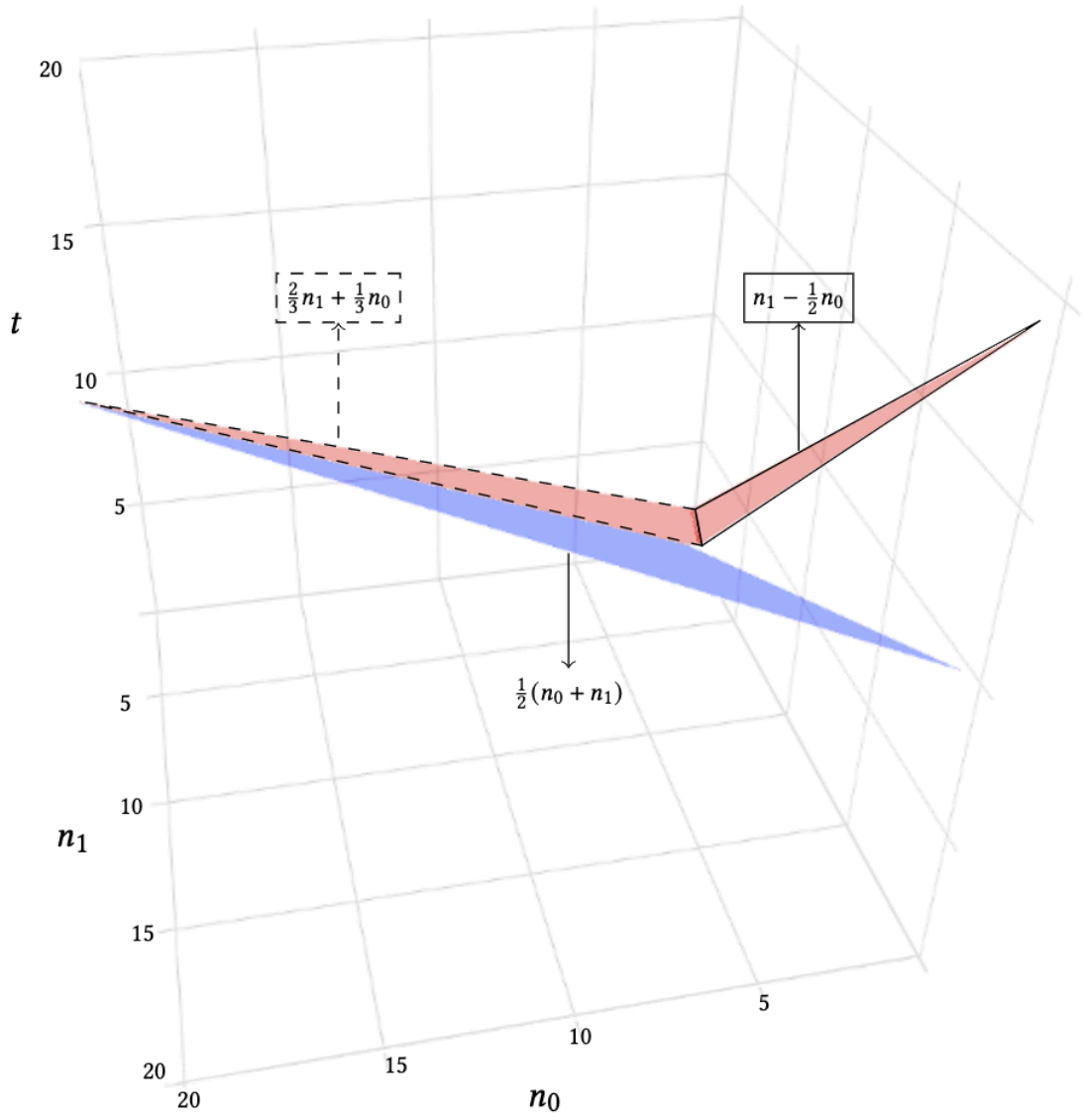
This protocol is game-theoretic fair again coalition of size 4.

Can we generalize?

Achievability	Coalition size t
$if\ n_1 \geq \frac{5}{2} n_0$	$n_1 - \frac{1}{2} n_0$
$otherwise$	$\frac{2}{3} n_1 + \frac{1}{3} n_0$

Game-theoretic fairness is impossible against $(t + 1)$-coalition.

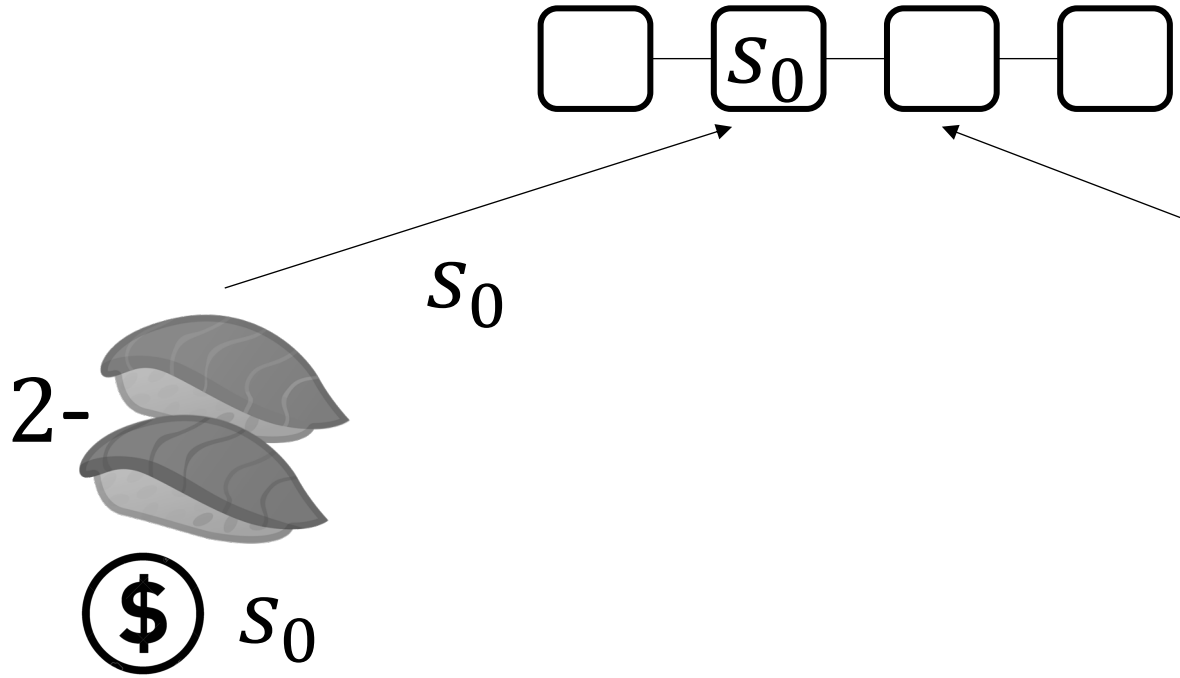
Landscape


20
15
t
10
5
5
10
n_1
15
20
20
15
10
5
n_0
$\frac{2}{3}n_1 + \frac{1}{3}n_0$
$n_1 - \frac{1}{2}n_0$
$\frac{1}{2}(n_0 + n_1)$

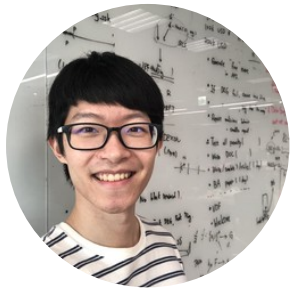
Phase Transition

Achievability	Coalition size t
$if\ n_1 \geq \frac{5}{2} n_0$	$n_1 - \frac{1}{2} n_0$
$otherwise$	$\frac{2}{3} n_1 + \frac{1}{3} n_0$

Output 0!

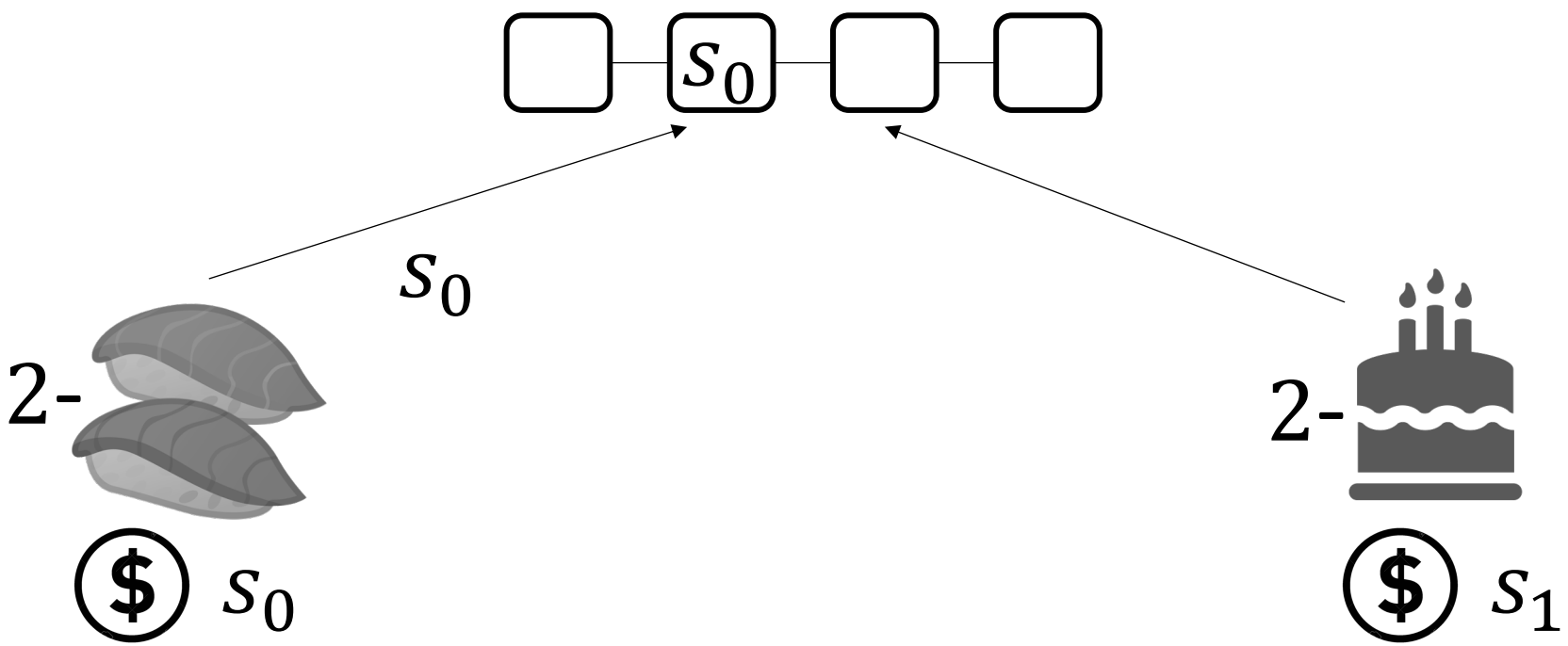




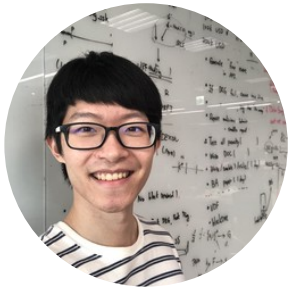




Output 0!



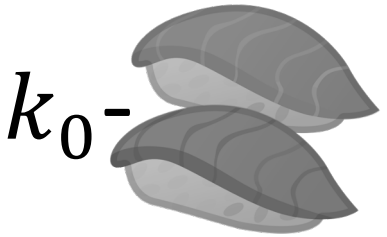


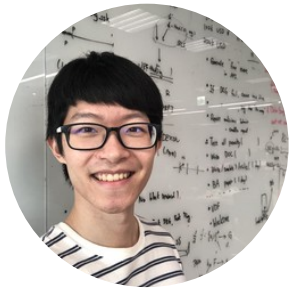




How to choose the threshold in general?

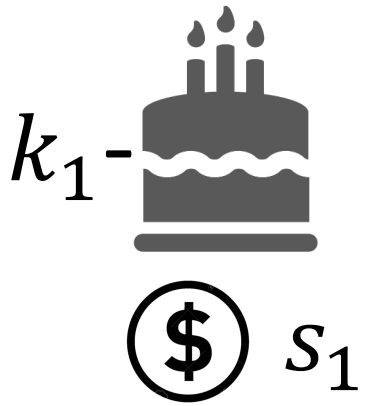

Sushi!



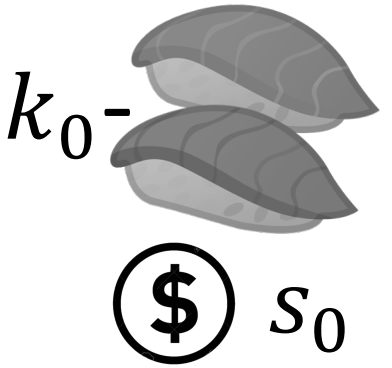


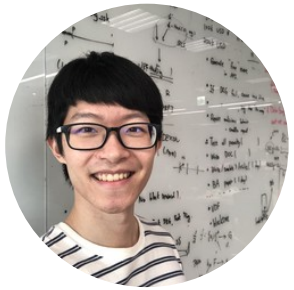


Cake!

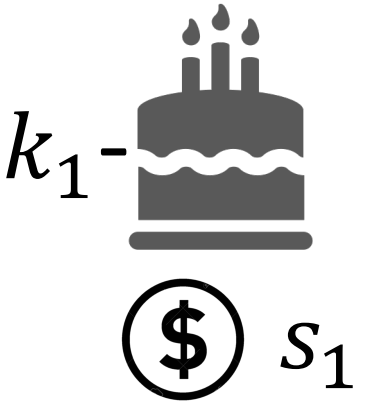


- <u>Condition 1</u>: Coalition cannot control both coins.

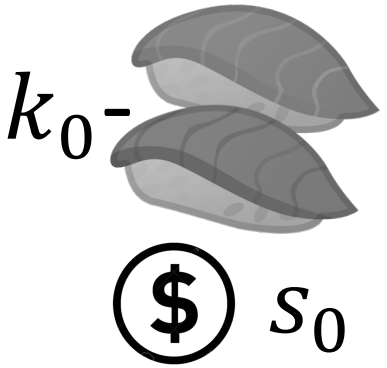


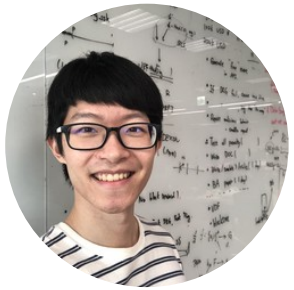




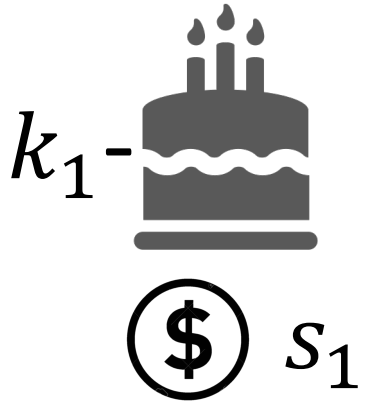
$$t \leq k_0 + k_1$$

- <u>Condition 2</u>: If control s_1, cannot fail reconstruction of s_0.

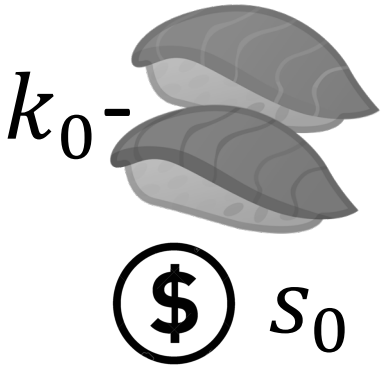


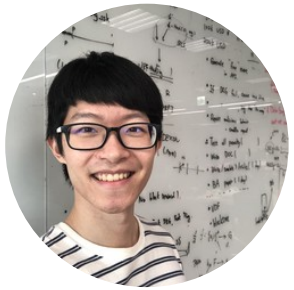




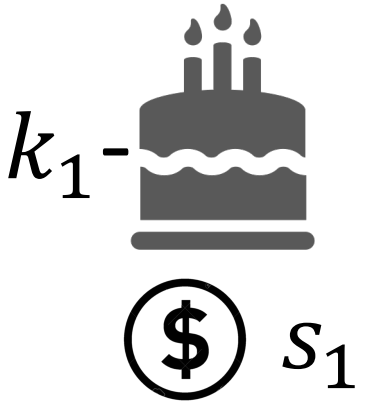
$$t \leq (n_0 - k_0 + 1) + k_1$$

- <u>Condition 3</u>: If can fail reconstruction of s_1, must not prefer 0.







$$\text{If } n_1 - k_1 < n_0, t \leq 2(n_1 - k_1)$$

Achievability: optimization

Maximize t

Subject to $t < (k_0 + 1) + (k_1 + 1)$

$$t < (n_0 - k_0) + (k_1 + 1)$$

If $n_1 - k_1 < n_0, t \leq 2(n_1 - k_1)$

	k_0	k_1	t
$if\ n_1 \geq \frac{5}{2}n_0$	$\frac{1}{2}n_0$	$n_1 - n_0$	$n_1 - \frac{1}{2}n_0$
$otherwise$	$\frac{1}{2}n_0$	$\frac{2}{3}n_1 - \frac{1}{6}n_0$	$\frac{2}{3}n_1 + \frac{1}{3}n_0$

Three conditions imply fairness

- Condition 1: Coalition cannot control both coins.
- Condition 2: If control s_1, cannot fail reconstruction of s_0.
- Condition 3: If can fail reconstruction of s_1, must not prefer 0.

Conclusion

1. We can construct game-theoretic fair coin toss against coalition of size

$$t = \begin{cases} n_1 - \left\lfloor \frac{1}{2} n_0 \right\rfloor, & if\ n_1 \geq \frac{5}{2} n_0, \\ \left\lceil \frac{1}{2} n_0 \right\rceil + \left\lfloor \frac{2}{3} n_1 - \frac{1}{6} n_0 \right\rfloor, & otherwise. \end{cases}$$

2. There is no game-theoretic fair coin toss against $(t + 1)$-sized coalition.

More result

1. Complete characterization of another fairness notion: no coalition can harm honest individual.

2. Complete characterization under other utility.

References

[Cle 86] Richard Cleve. *Limits on the security of coin flips when half the processors are faulty.* In STOC, 1986.

[Blu83] Manuel Blum. *Coin flipping by telephone.* In CRYPTO, 1981.

[CGL+18] Kai-Min Chung, Yue Guo, Wei-Kai Lin, Rafael Pass, and Elaine Shi. *Game theoretic notions of fairness in multi-party coin toss.* In TCC, 2018.