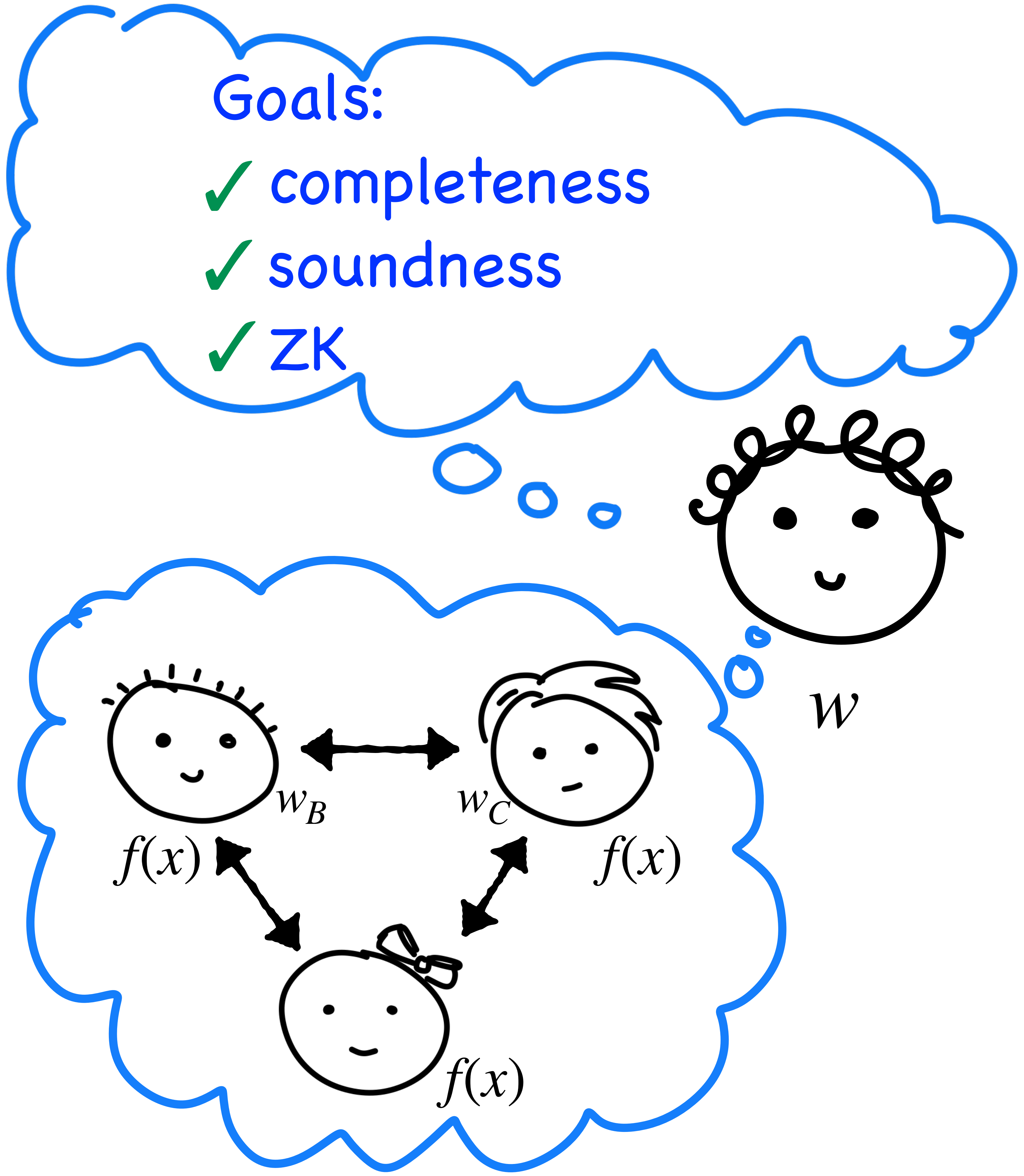
ZKP and MPC: Day 2

- **Recap**
- A Concrete Lightweight MPC Scheme
- Reducing Rounds
- Better Communication Efficiency
- MPC from ZK

Sophia Yakoubov

ZKP from MPC

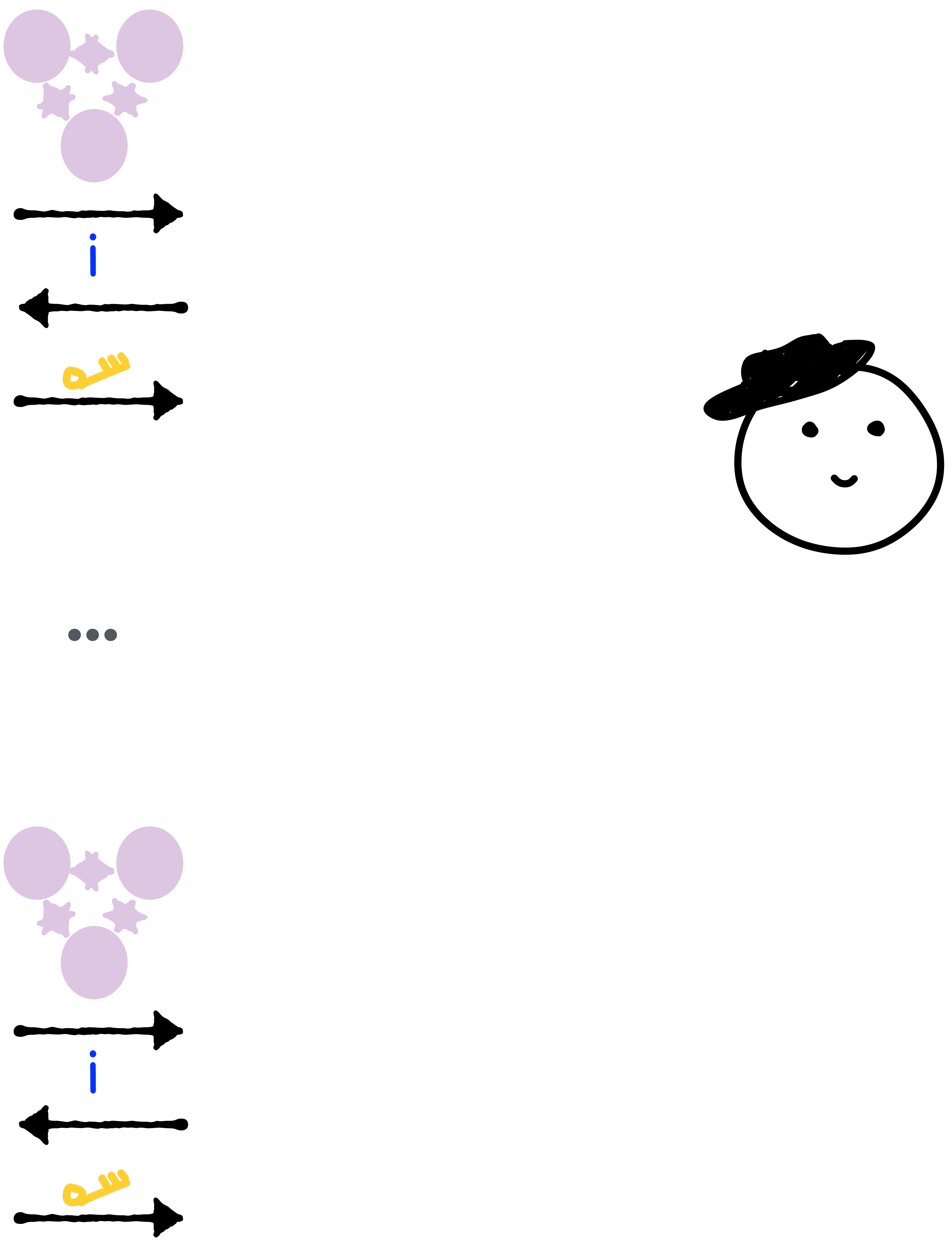


Goals:

✓ completeness

✓ soundness

✓ ZK



MPC for $f(w_B, w_C, \perp) = R(x, w_B + w_C)$ with:

- 1-privacy
- perfect correctness

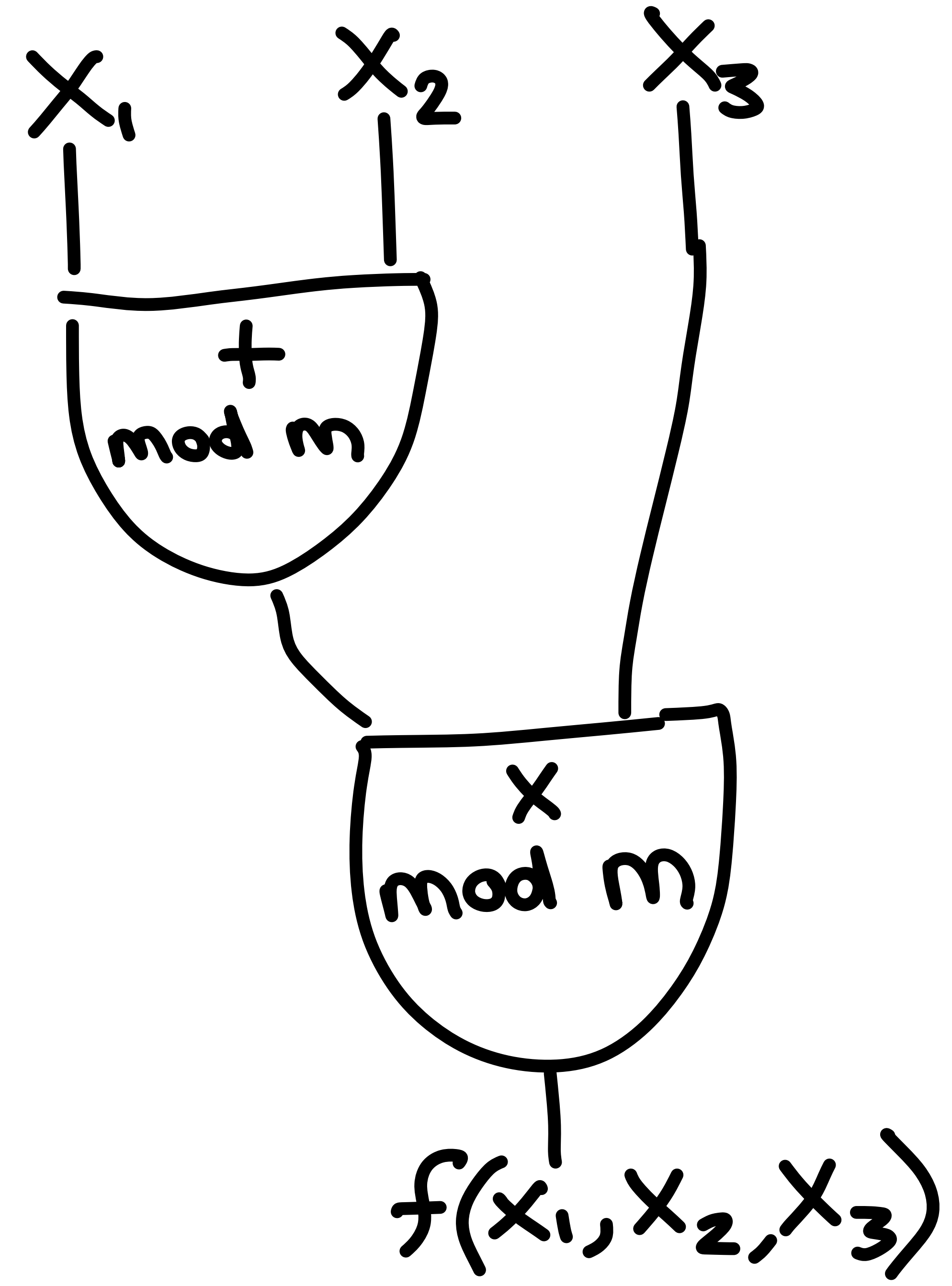
ZKP and MPC: Day 2

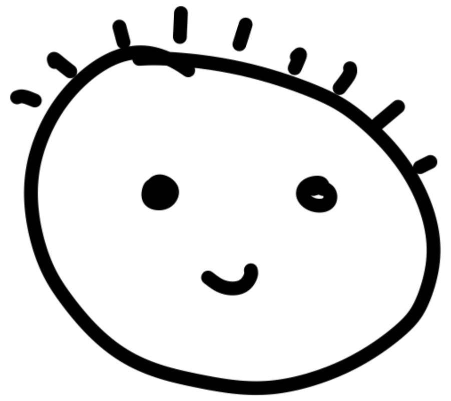
- Recap
- **A Concrete Lightweight MPC Scheme**
- Reducing Rounds
- Better Communication Efficiency
- MPC from ZK

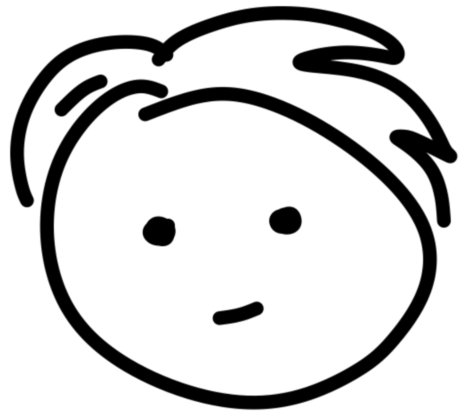
Sophia Yakoubov

MPC from Correlated Randomness

Step 1: express f as a circuit







Invariant: for wire value x, we have $x = x_B + x_C$ (mod m)

Input x: secret share x

Open x: $\xrightarrow{x_B}$ $\xleftarrow{x_C}$

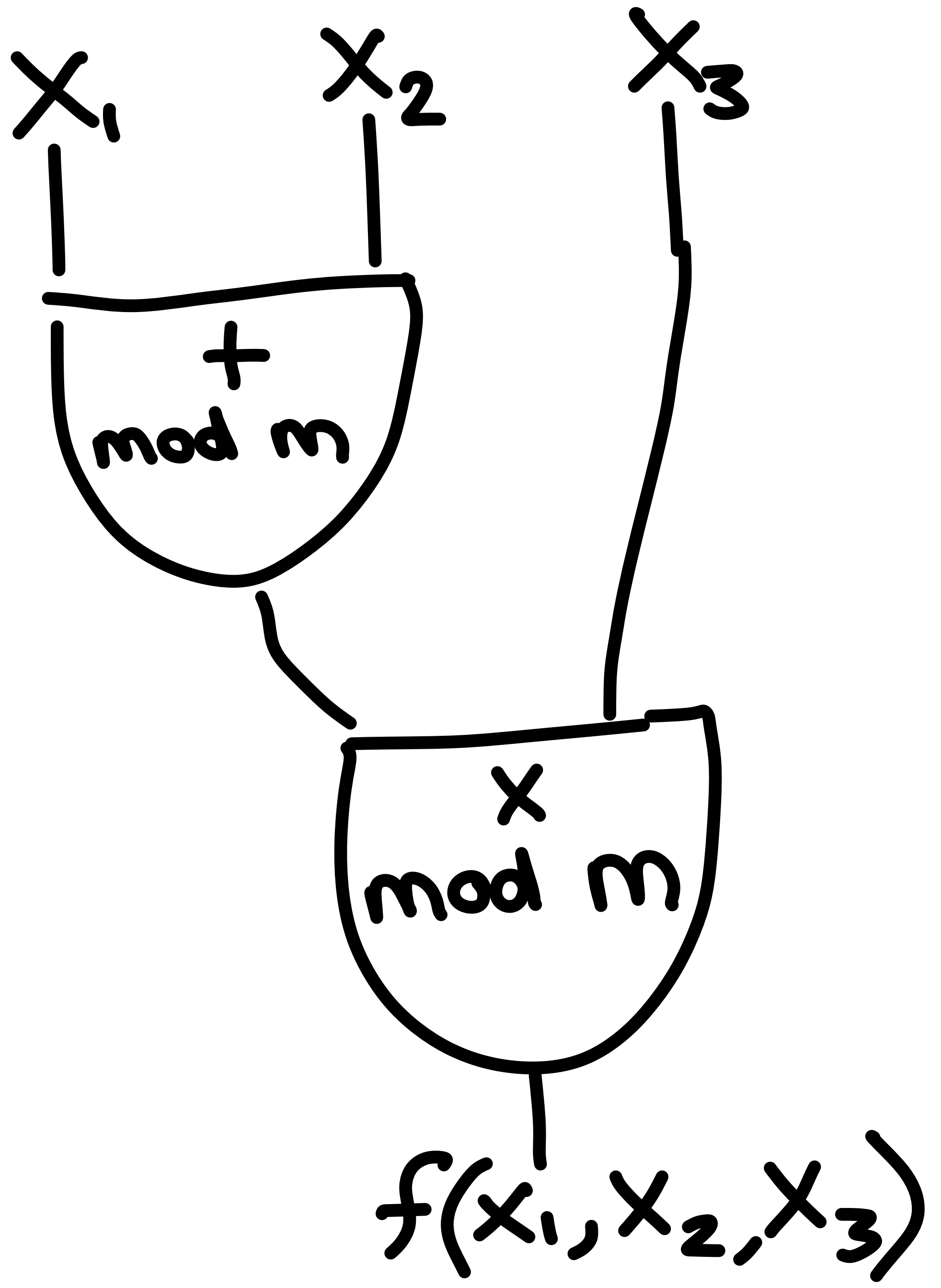
Add x and y: x_B, y_B $\quad$ x_C, y_C

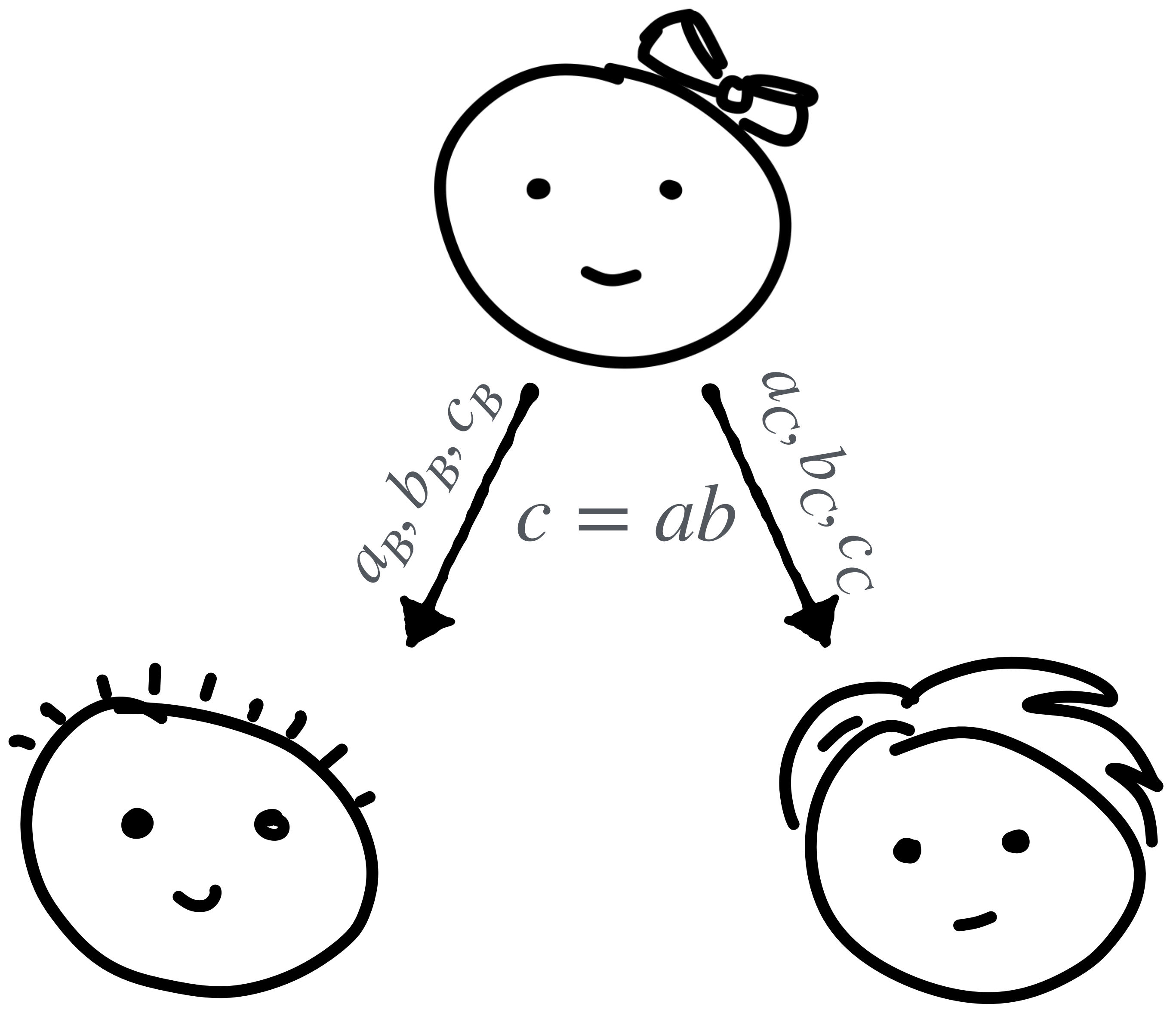
$z_B = x_B + y_B$ $\quad$ $z_C = x_C + y_C$

$$\begin{aligned} z_B + z_C &= (x_B + y_B) + (x_C + y_C) \\ &= (x_B + x_C) + (y_B + y_C) \\ &= x + y \end{aligned}$$ (mod m)

MPC from Correlated Randomness

Step 1: express f as a circuit





a_B, b_B, c_B

$c = ab$

a_C, b_C, c_C

Invariant: for wire value x, we have $x =$ x_B + x_C (mod m)

Input x: secret share x

Open x: $\underset{x_C}{\overset{x_B}{\rightleftarrows}}$

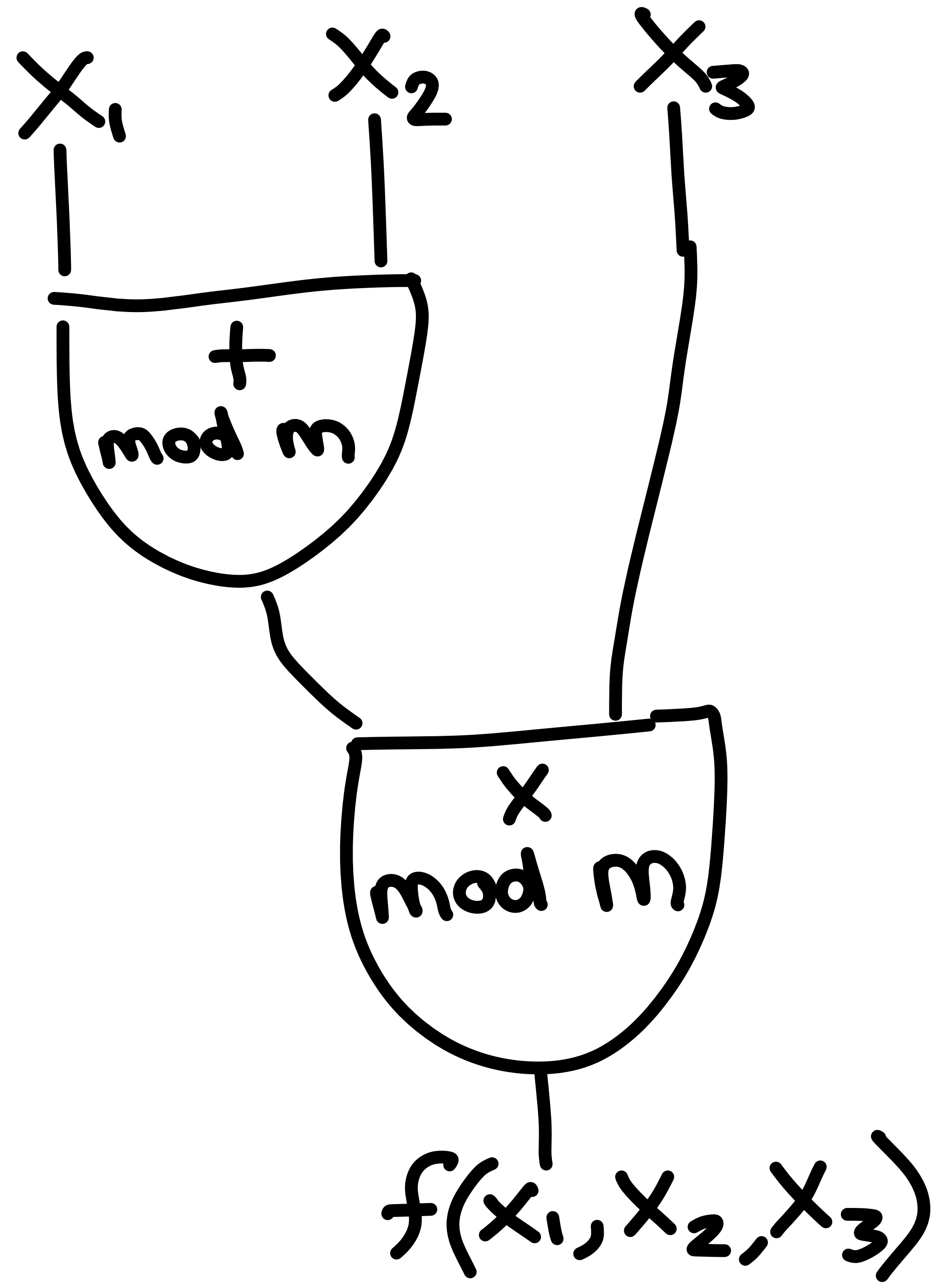
Add x and y: $z_B = x_B + y_B$ $z_C = x_C + y_C$

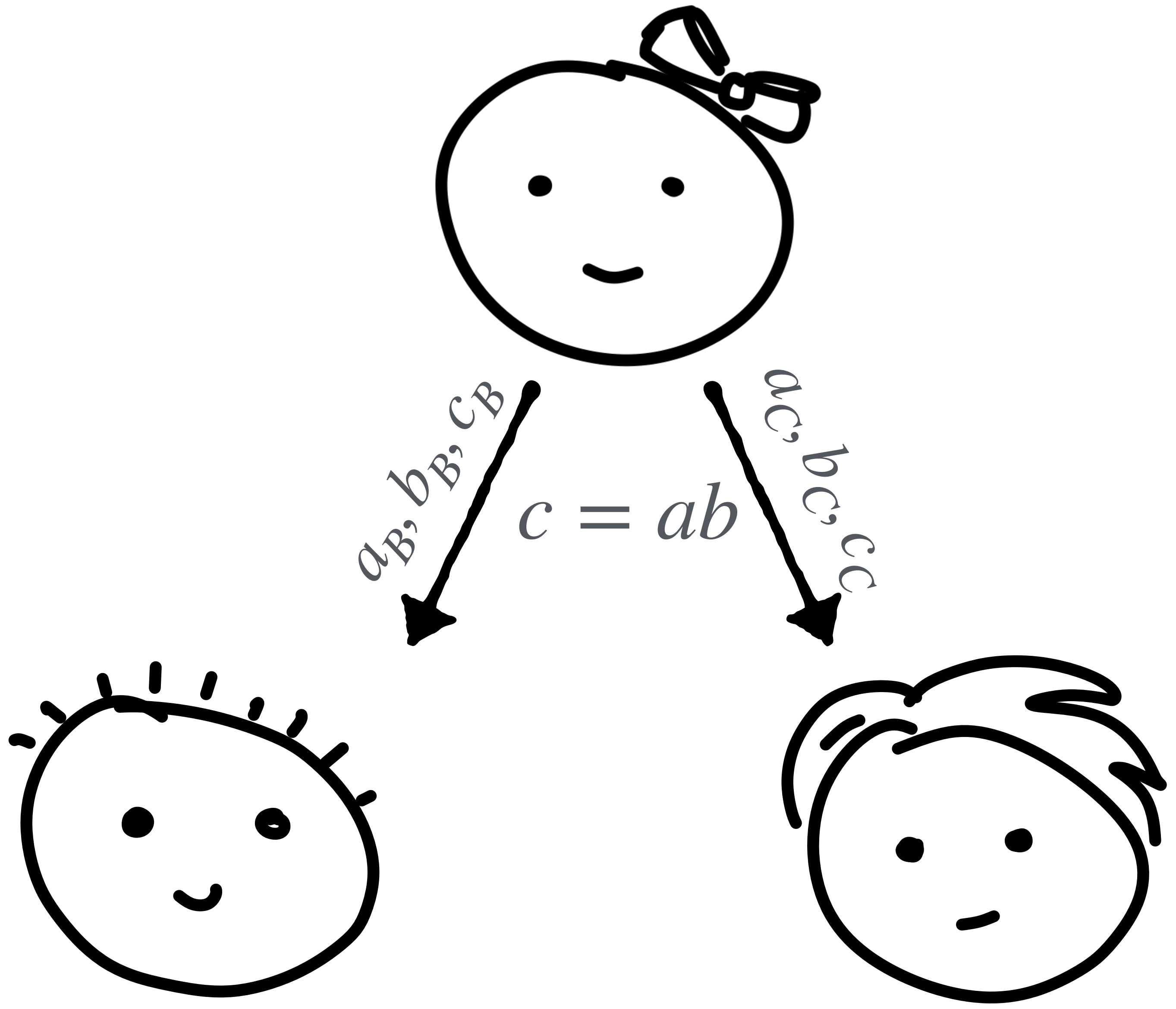
Mult x and y: $z = xy = (x_B + x_C)(y_B + y_C)$

$= x_B y_B + x_C y_C + x_B y_C + x_C y_B$

MPC from Correlated Randomness

Step 1: express f as a circuit





Invariant: for wire value x, we have $x =$ x_B $+$ x_C (mod m)

Input x: secret share x

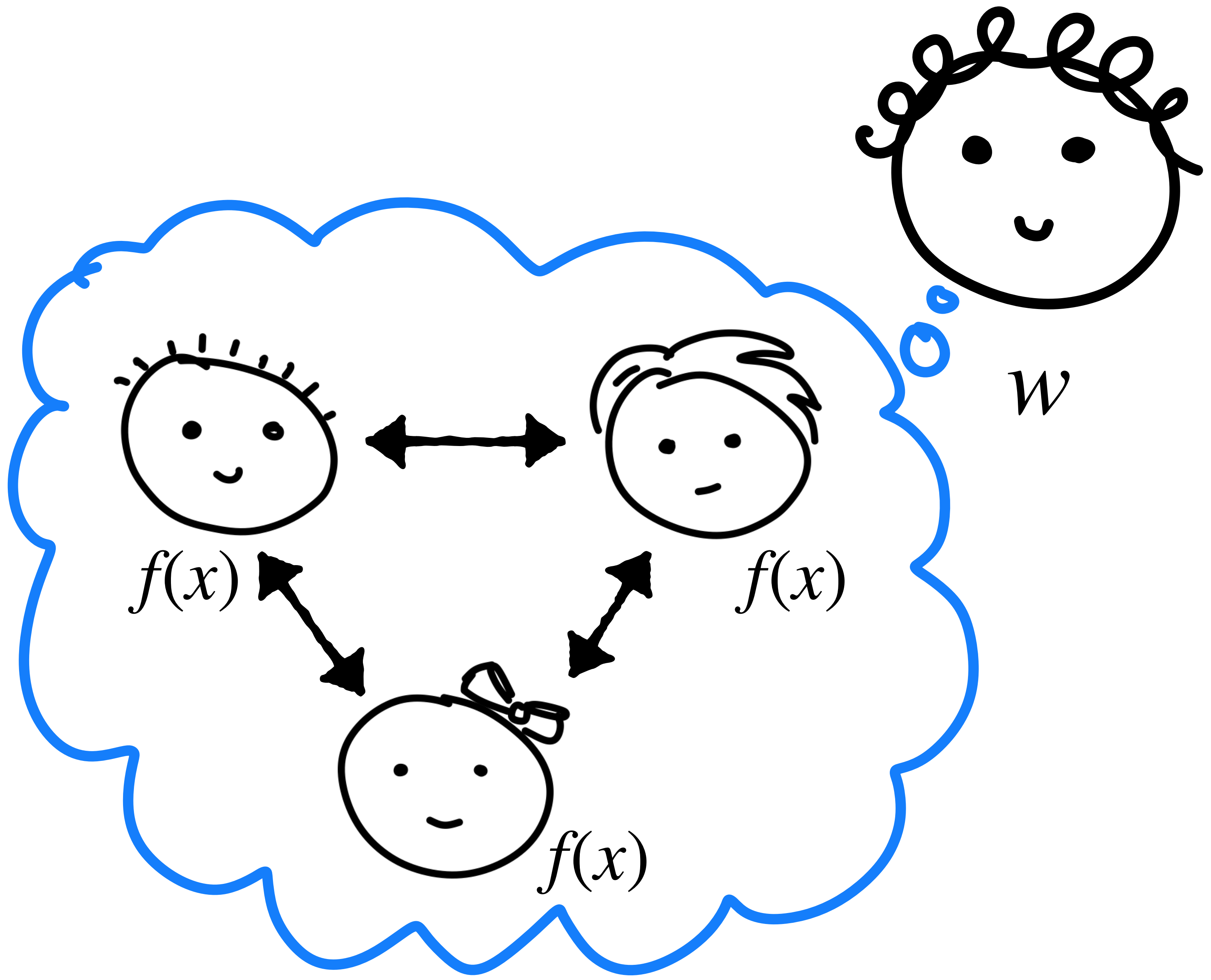
Open x: $\xrightarrow{x_B}$ $\xleftarrow{x_C}$

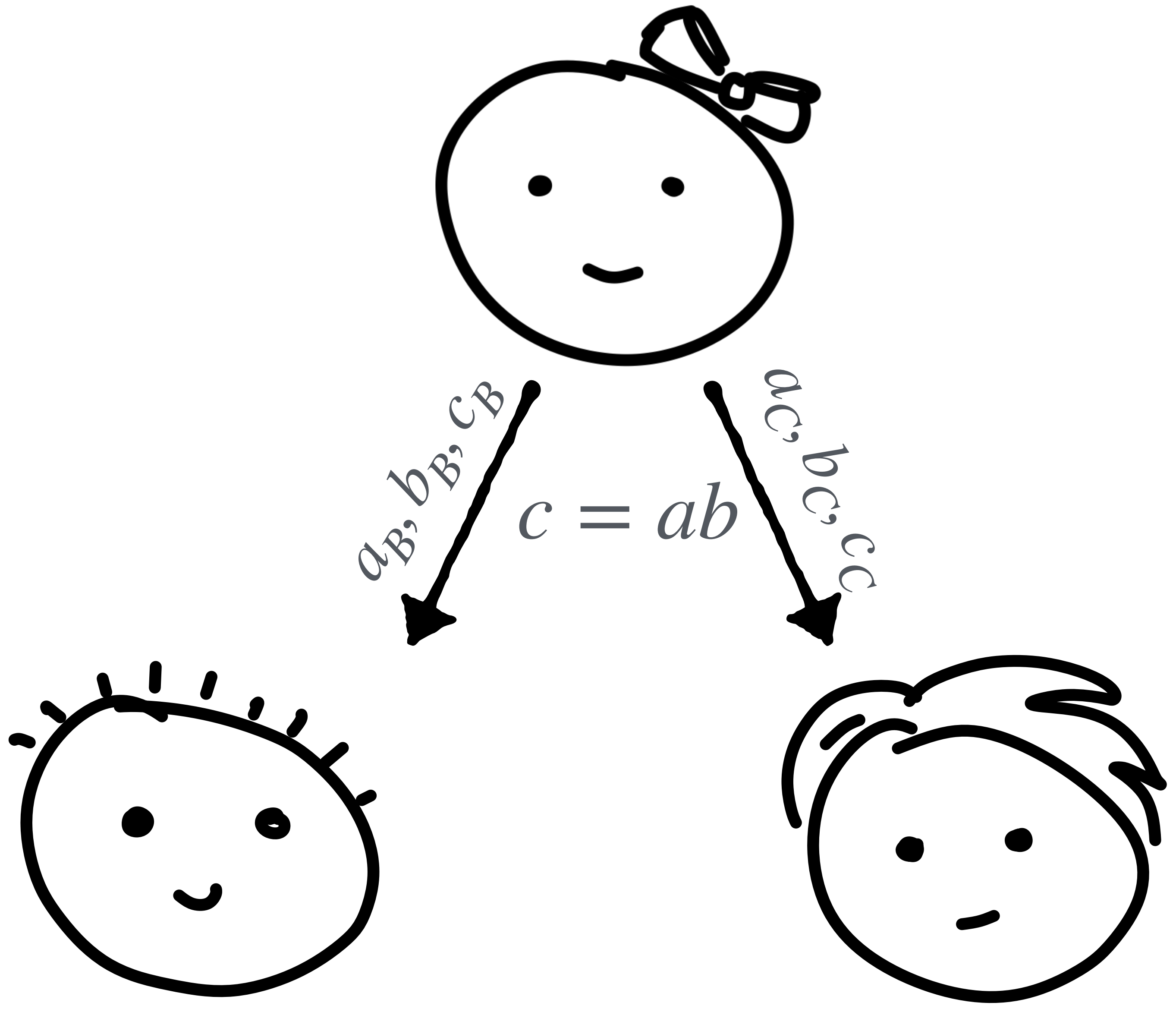
Add x and y: $z_B = x_B + y_B$ $z_C = x_C + y_C$

Mult x and y: some openings and additions

Done!

MPC from Correlated Randomness





Invariant: for wire value x, we have $x =$ x_B + x_C (mod m)

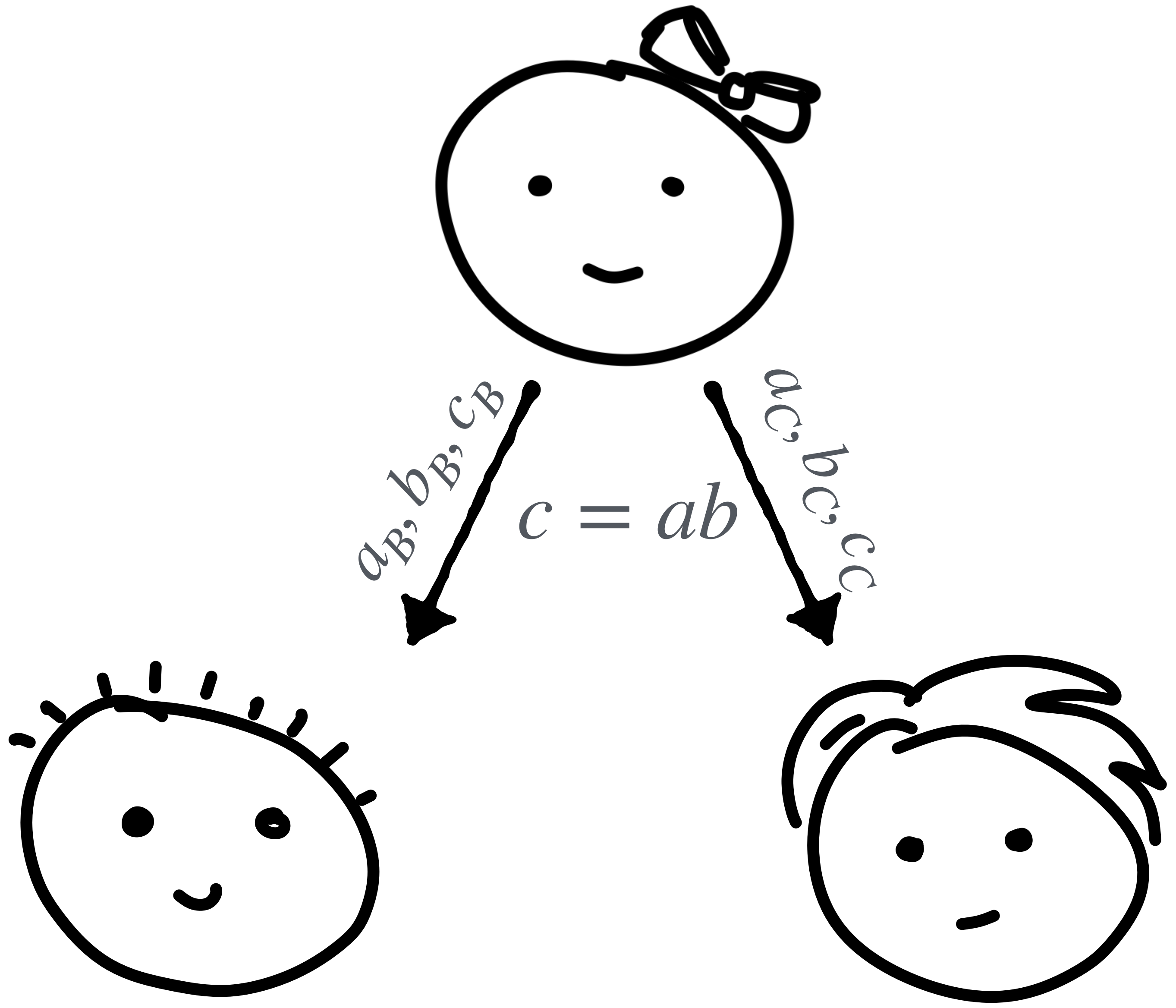
Input x:	secret share x	
Open x:	$\xrightarrow{x_B}$ $\xleftarrow[x_C]{}$	
Add x and y:	$z_B = x_B + y_B$	$z_C = x_C + y_C$
Mult x and y:	some openings and additions	
Output y:	Open y, send it to Eve	

Q: what is missing?

ZK Simulator for Eve

$S_{MPC,E}(\perp, y)$:

- run Eve honestly
- send y on behalf of Alice and Bob



Invariant: for wire value x, we have $x = x_B + x_C$

Input x: secret share x

Open x: $\xrightarrow{x_B}$ $\xleftarrow[x_C]{}$

Add x and y: $z_B = x_B + y_B$ $z_C = x_C + y_C$

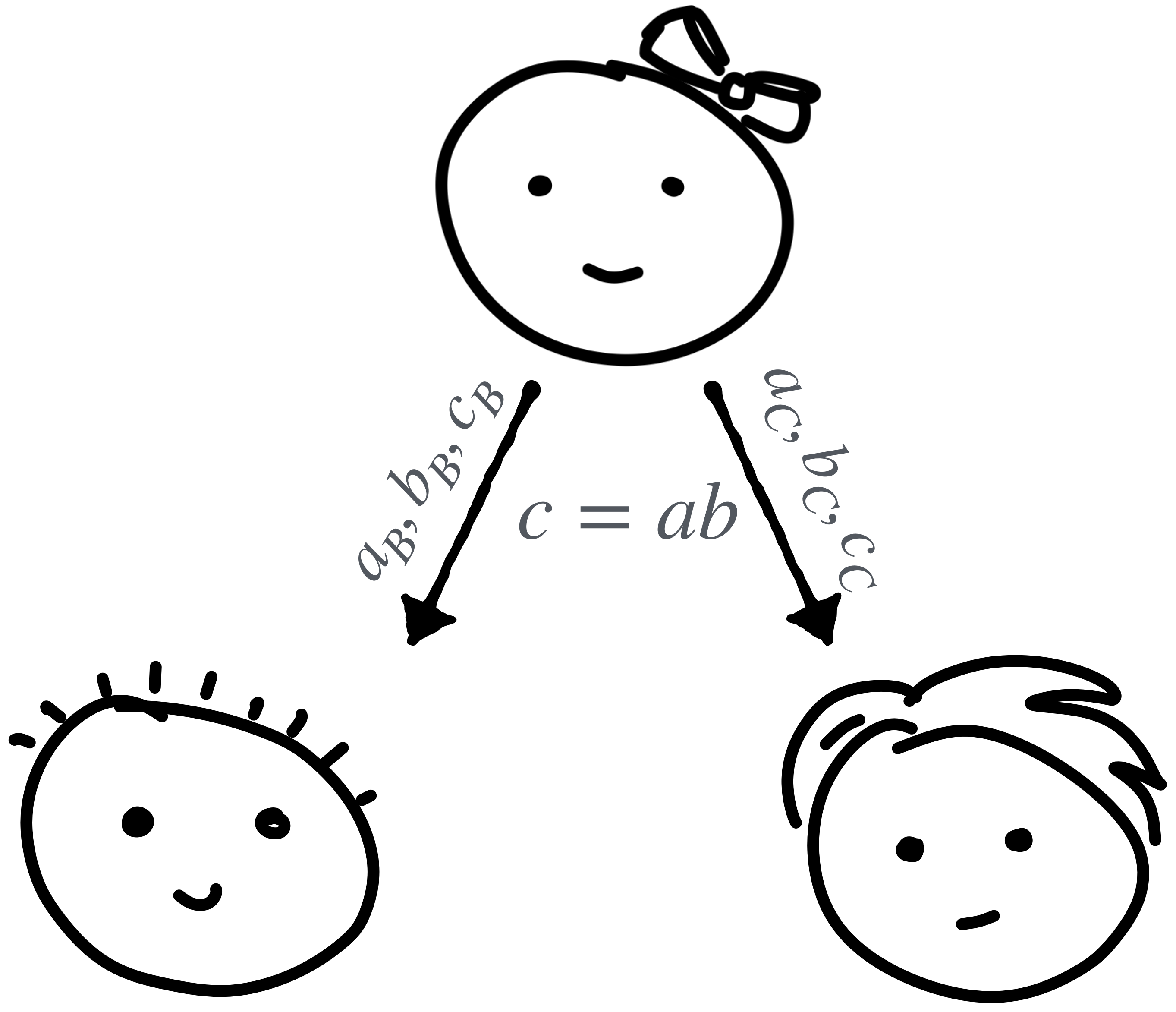
Mult x and y: some openings and additions

Output y: Open y, send it to Eve

ZK Simulator for Bob (/Charlie)

$S_{MPC,B}(\text{input}_B, y)$:

- Run Bob honestly
- Send random values on Eve's behalf
- Send random values on Charlie's behalf
- When opening the output, set y_C s.t. $y_B + y_C = y$



Invariant: for wire value x, we have $x = x_B + x_C$

Input x: secret share x

Open x: $\xrightarrow{x_B}$ $\xleftarrow{x_C}$

Add x and y: $z_B = x_B + y_B$ $z_C = x_C + y_C$

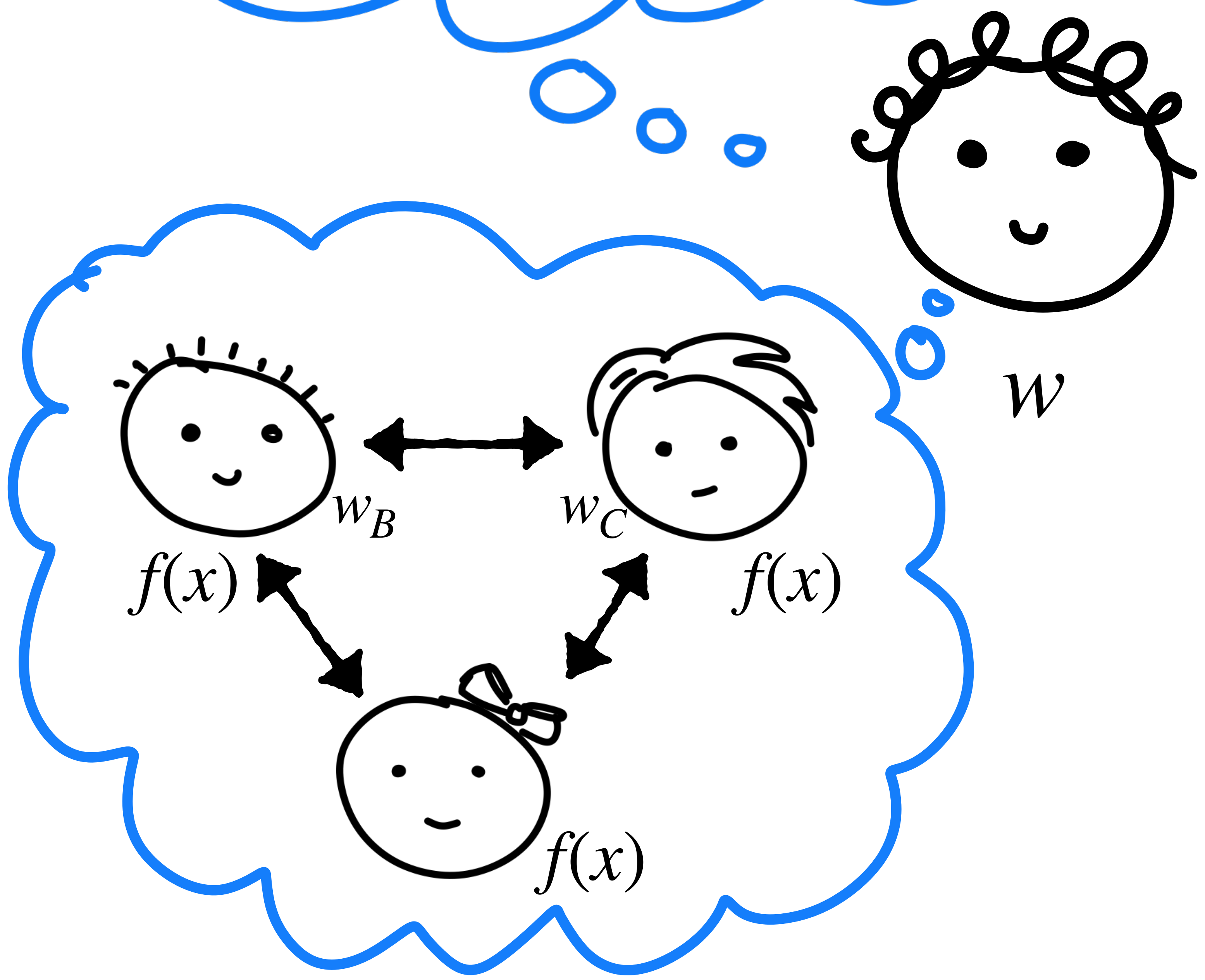
Mult x and y: some openings and additions

Output y: Open y, send it to Eve

ZKP from MPC

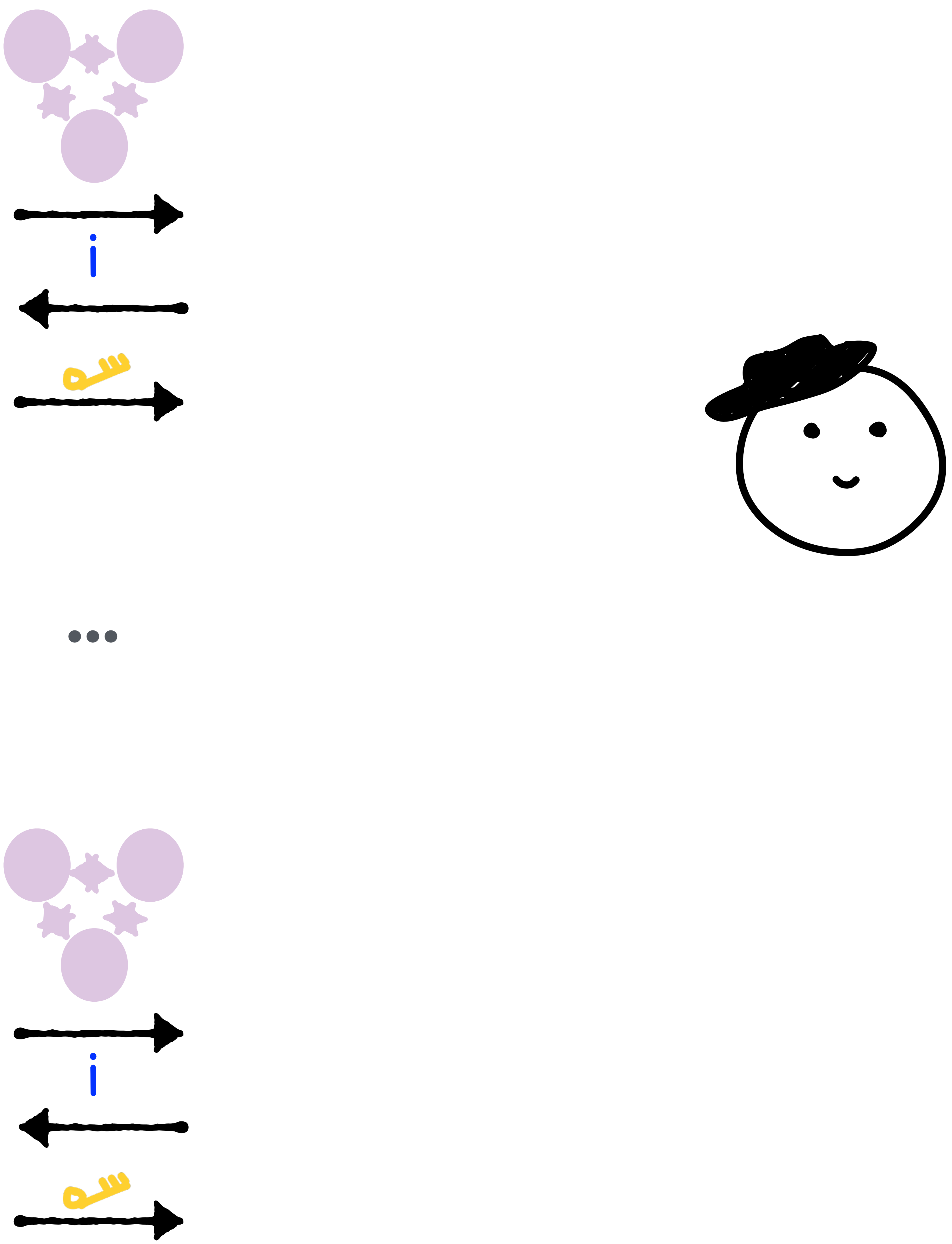
Goals:

- ✓ completeness
- ✓ soundness
- ✓ ZK



MPC for $f(w_B, w_C, \perp\ ) = R(x, w_B + w_C)$ with:

- 1-privacy
- perfect correctness

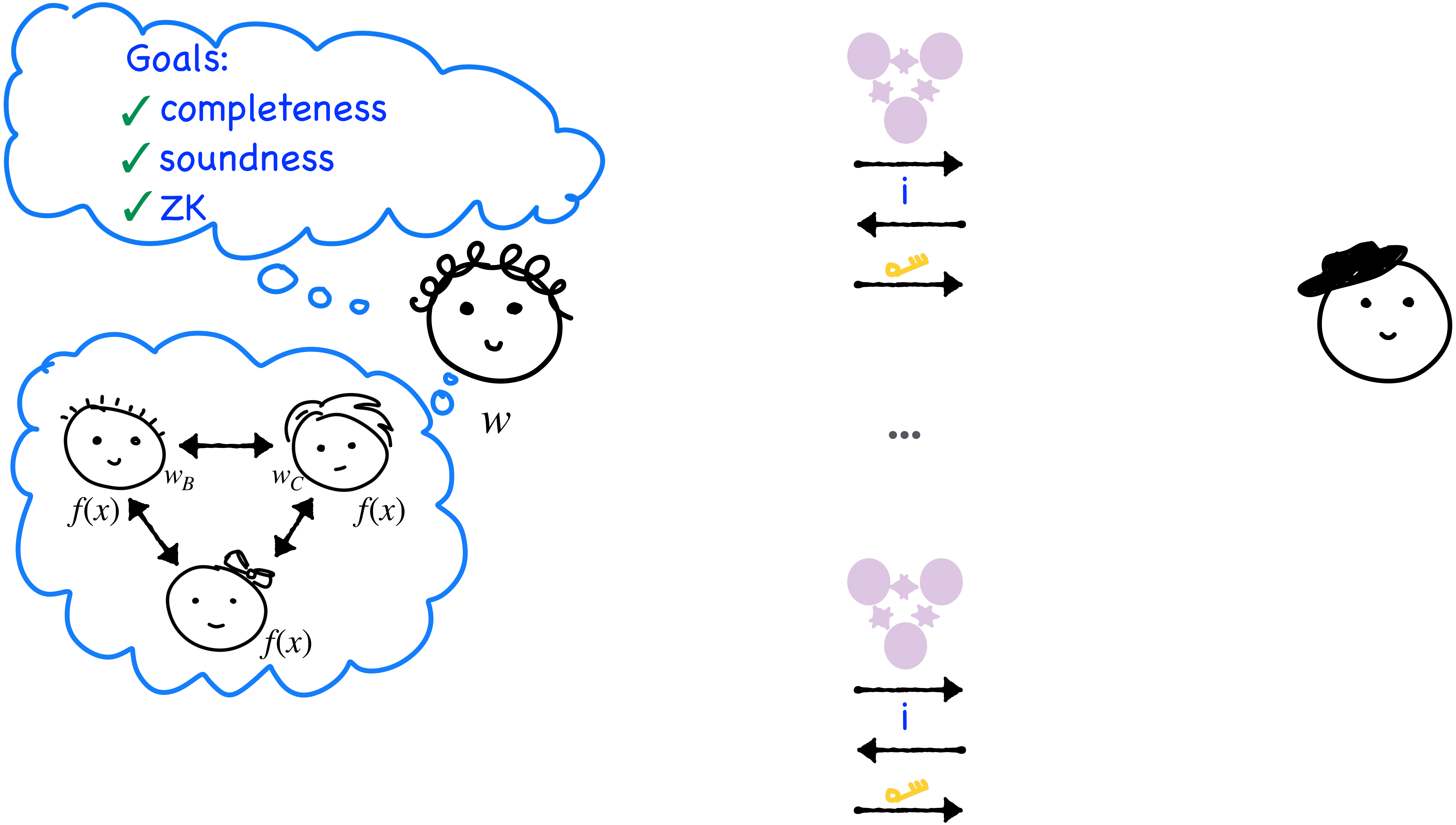


ZKP and MPC: Day 2

- Recap
- A Concrete Lightweight MPC Scheme
- **Reducing Rounds**
- Better Communication Efficiency
- MPC from ZK

Sophia Yakoubov

ZKP from MPC



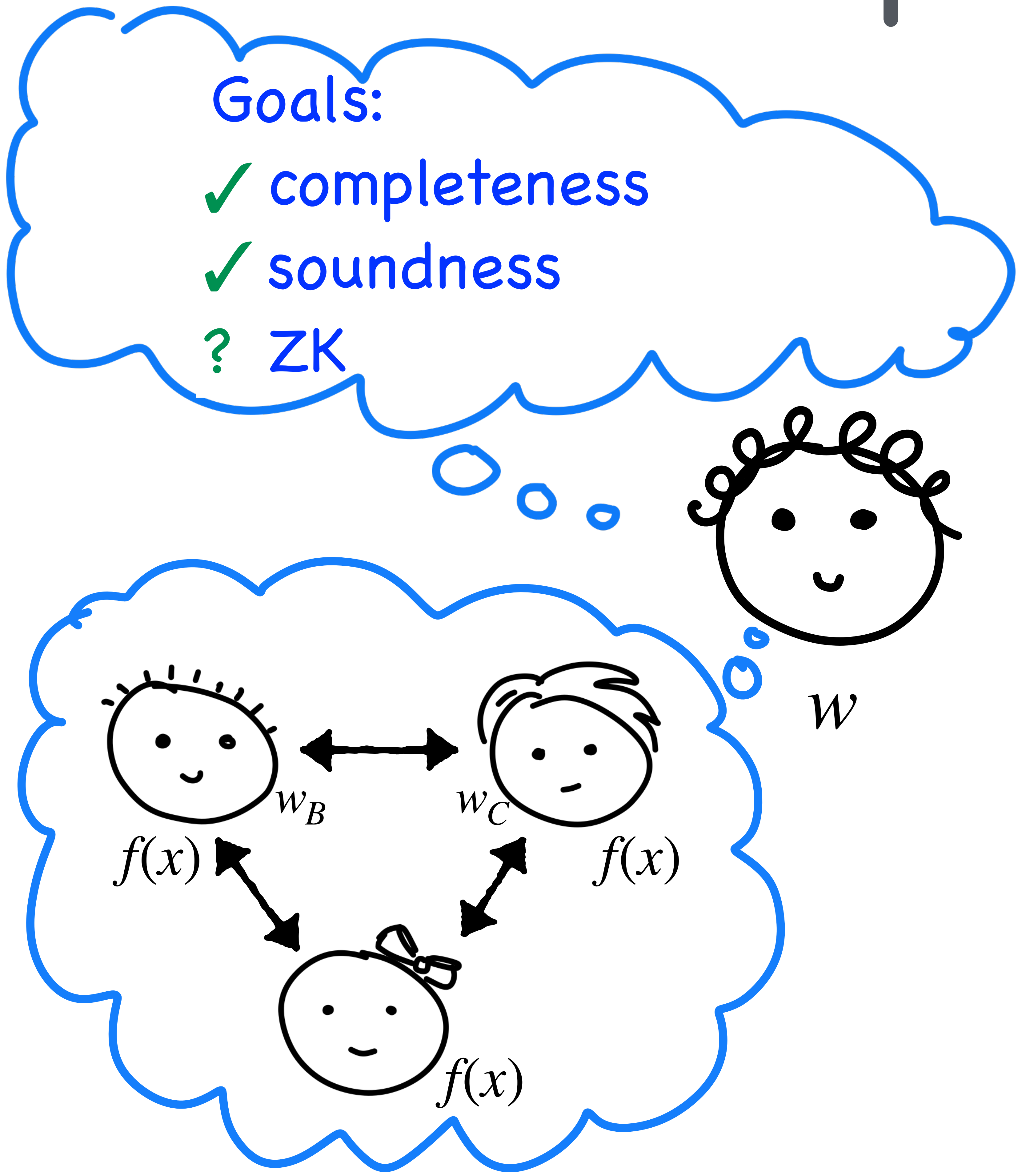
Goals:

✓ completeness

✓ soundness

✓ ZK

Can we Squish This?

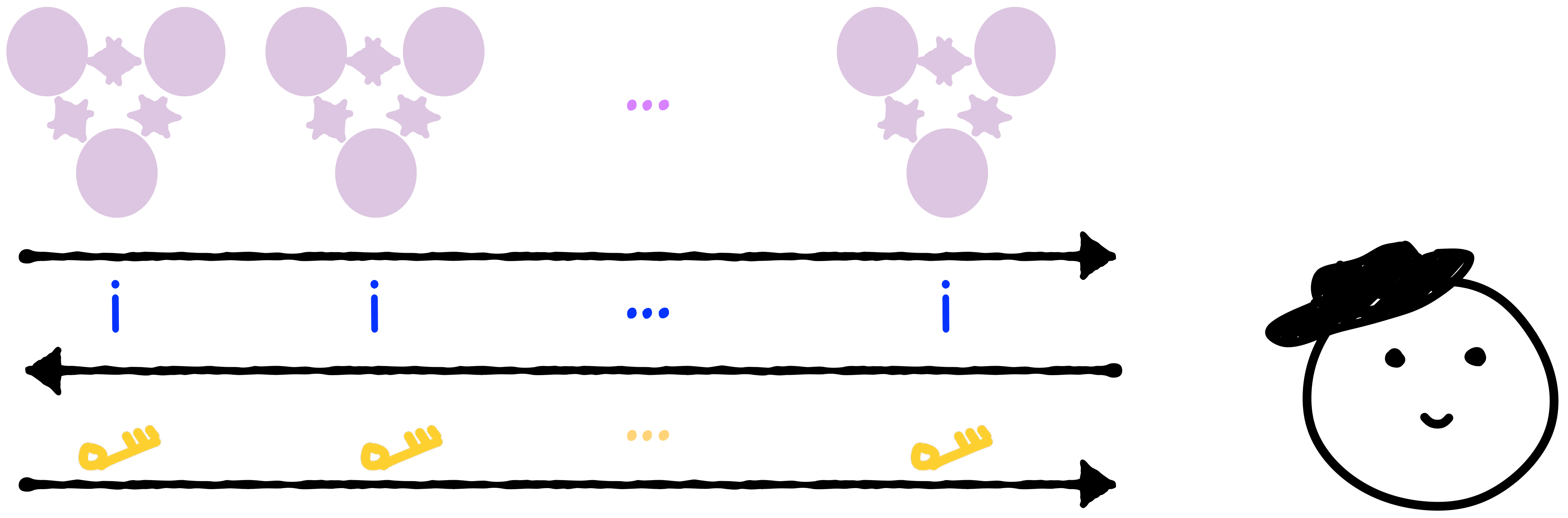


Goals:

✓ completeness

✓ soundness

? ZK

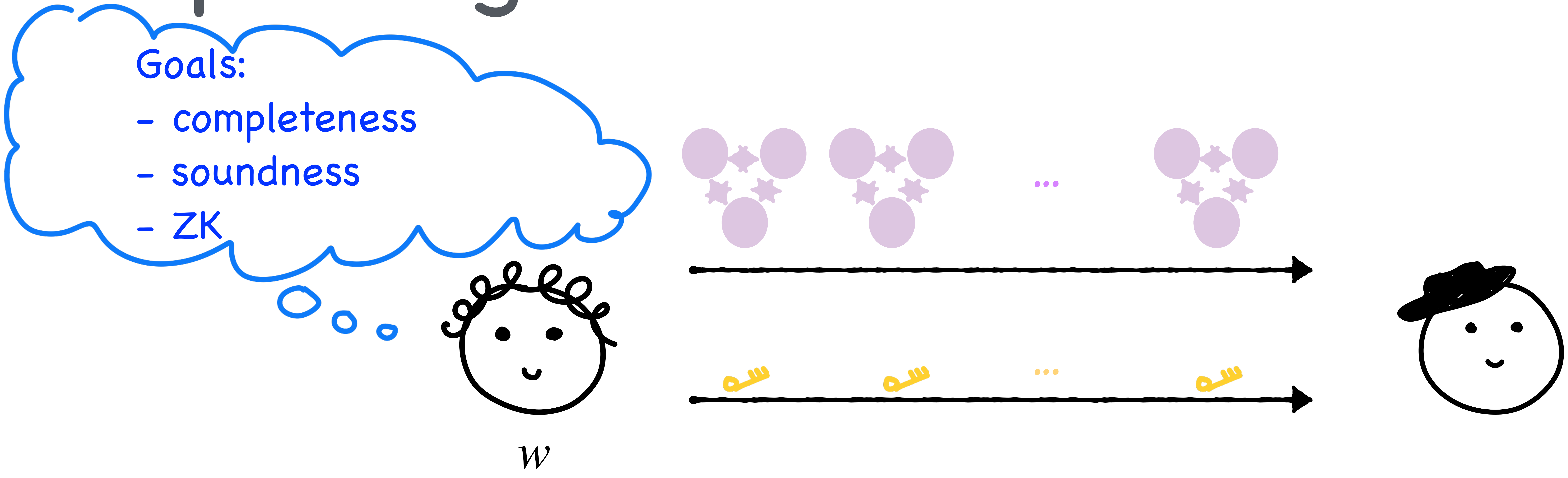


What if Dani is honest?
✓ ZK

What can we do if Dani is not honest?

- Let Dani prove knowledge of their choices first!
- Don't let Dani pick!

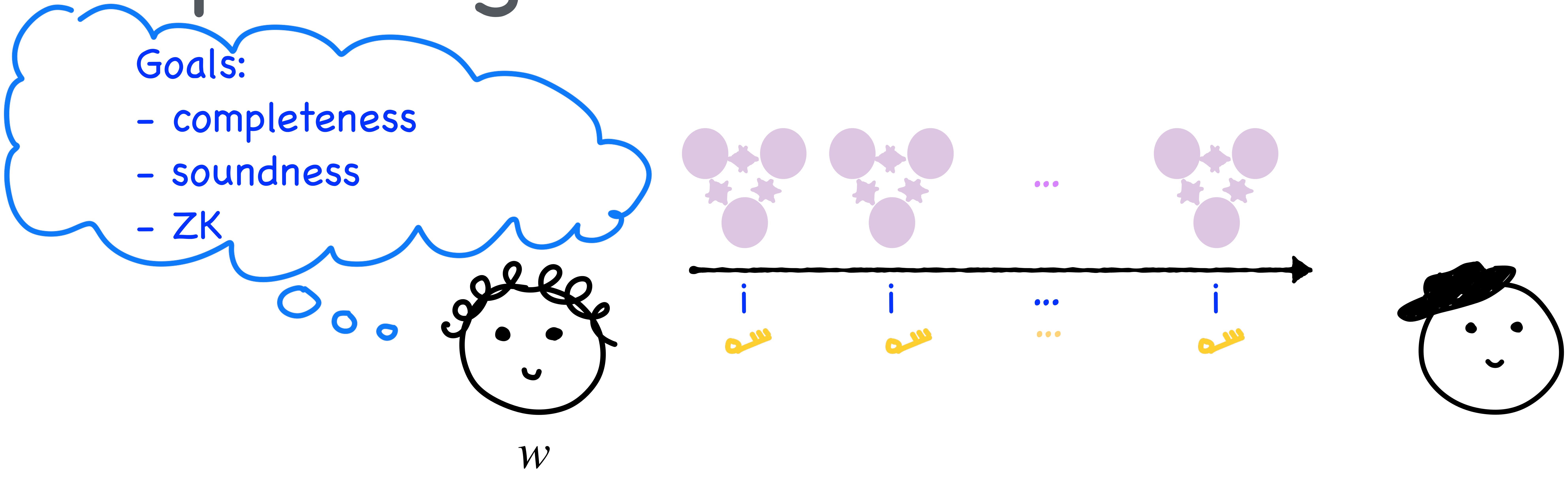
Squishing Rounds



Goals:
- completeness
- soundness
- ZK

i, i, ..., i random

Squishing Rounds

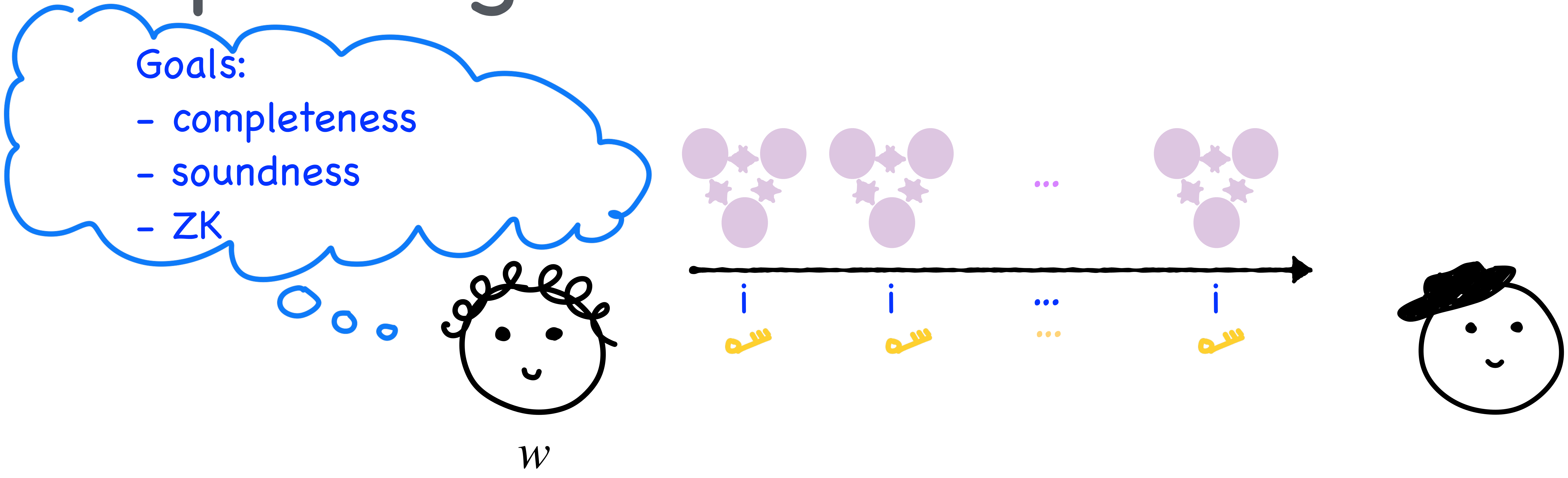


Goals:
- completeness
- soundness
- ZK

i, i, ..., i random

Q: what property dies?

Squishing Rounds: Fiat-Shamir Heuristic



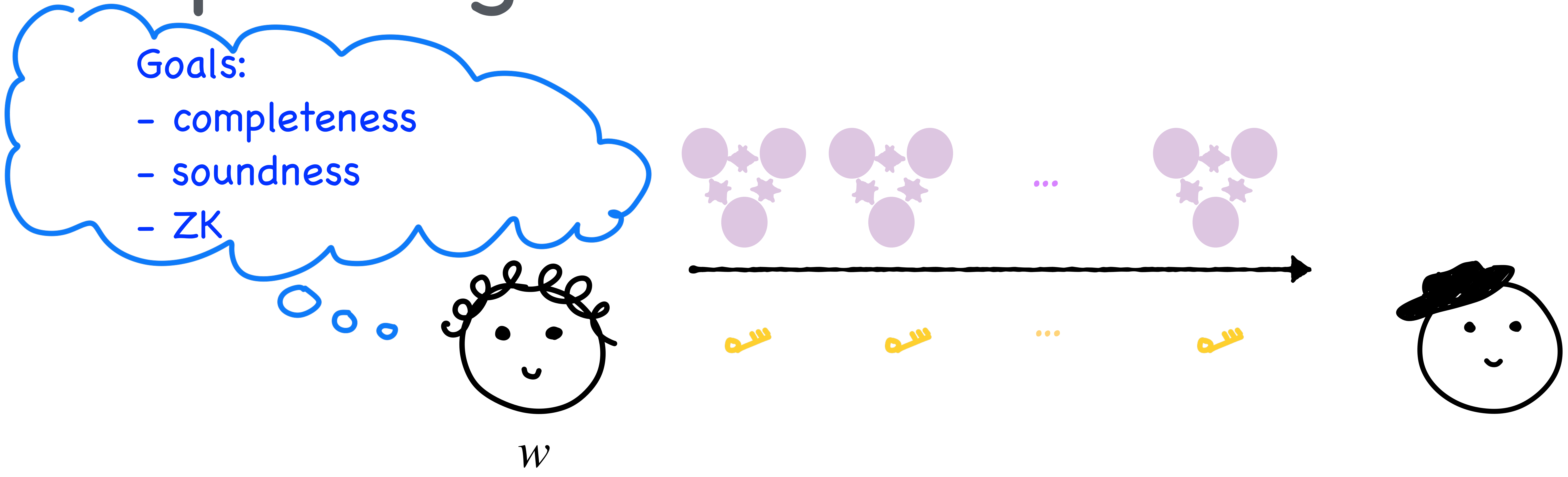
Goals:

- completeness
- soundness
- ZK

i, i, …, i = H( )

H is a random oracle

Squishing Rounds: Fiat-Shamir Heuristic


Goals:
- completeness
- soundness
- ZK

i, i, ..., i = H(✿✿ ✿)

H is a random oracle

i, i, ..., i = H(✿✿ ✿)

For each i:

Open(✿, 🔑) → party i's view

Check that:

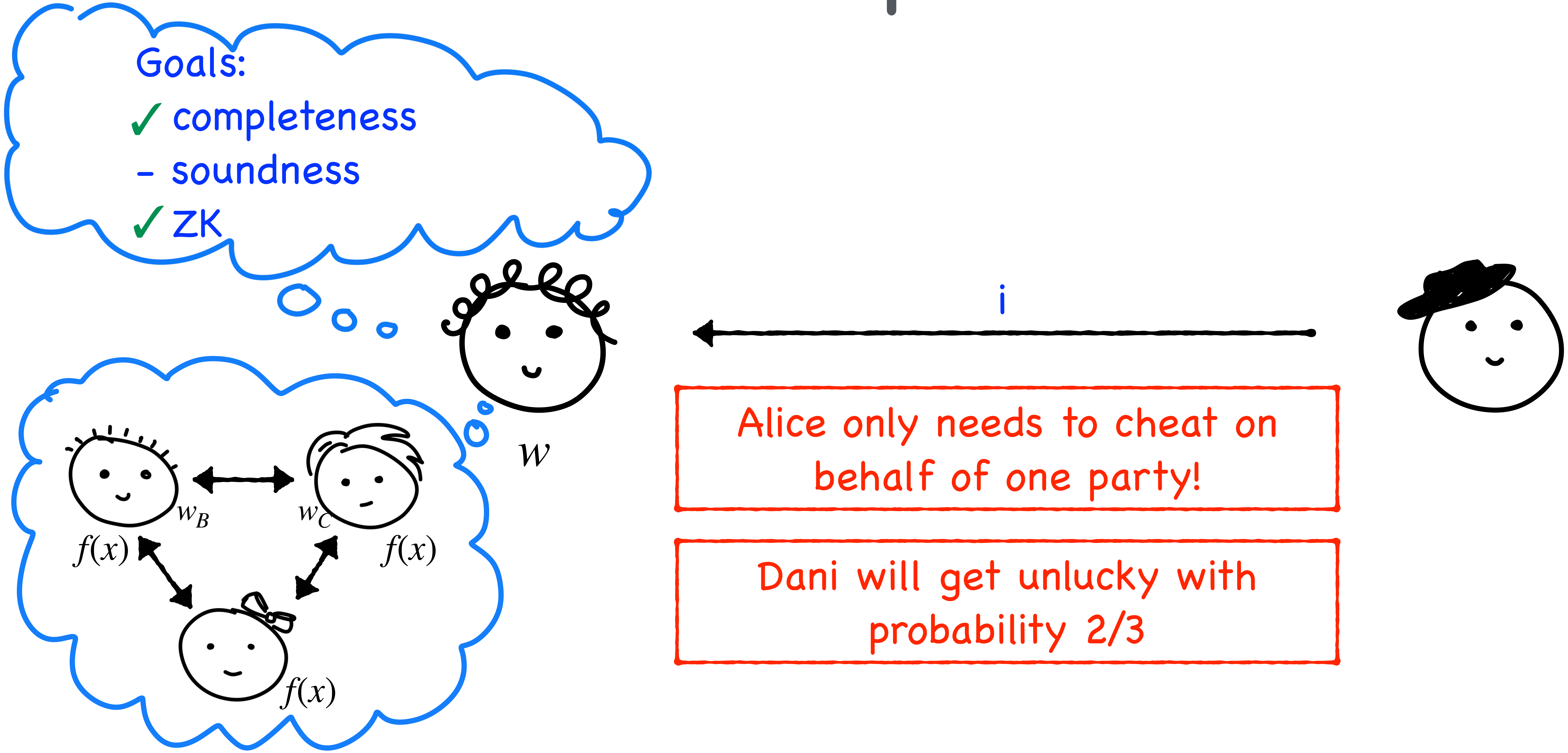
- party i did not cheat, and
- output is 1

ZKP and MPC: Day 2

- Recap
- A Concrete Lightweight MPC Scheme
- Reducing Rounds
- **Better Communication Efficiency**
- MPC from ZK

Sophia Yakoubov

Can We Avoid Repetition?



Goals:

✓ completeness

- soundness

✓ ZK

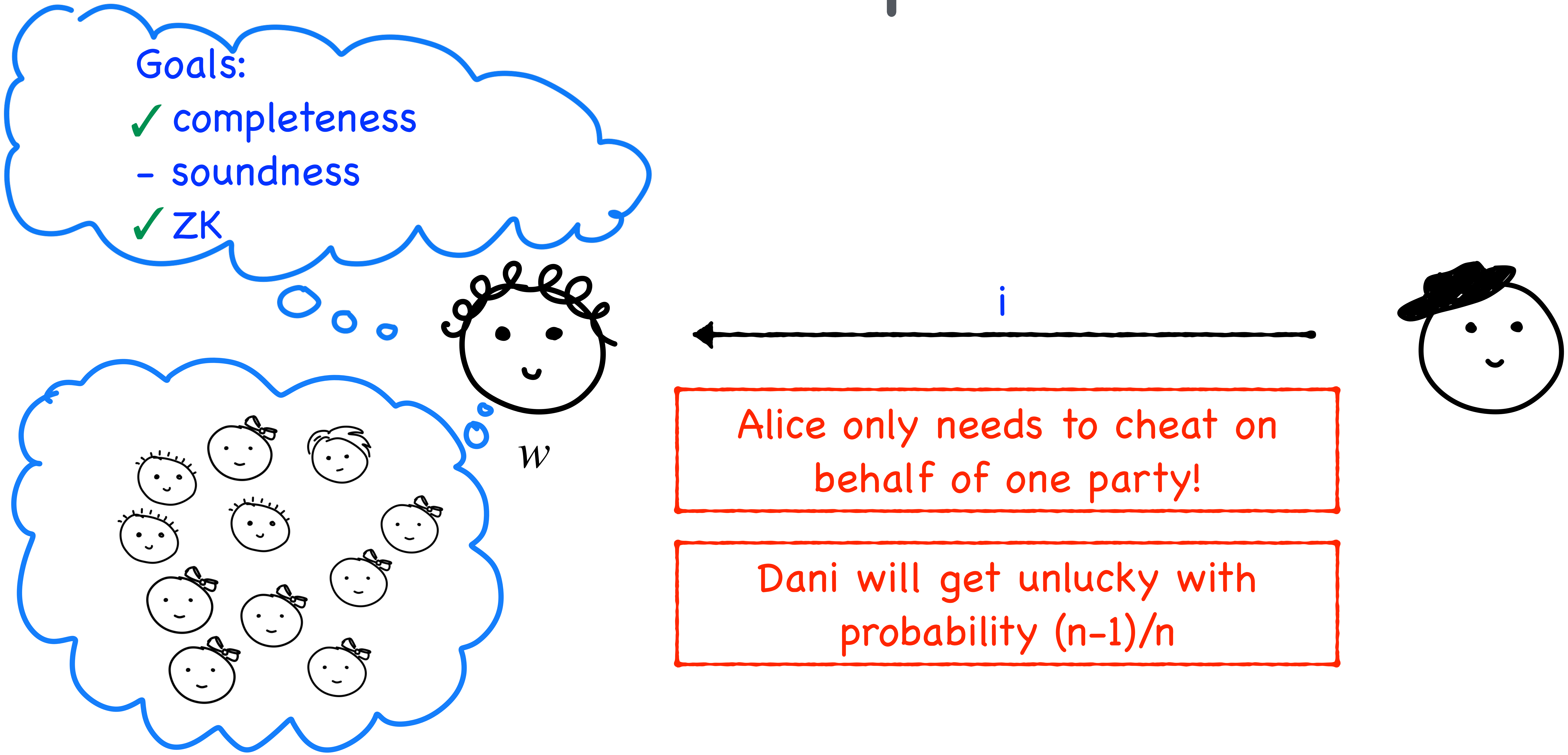
Alice only needs to cheat on behalf of one party!

Dani will get unlucky with probability 2/3

MPC for $R(x, w_B + w_C)$ with:

- 1-privacy
- perfect correctness

Can We Avoid Repetition?



Goals:

✓ completeness

- soundness

✓ ZK

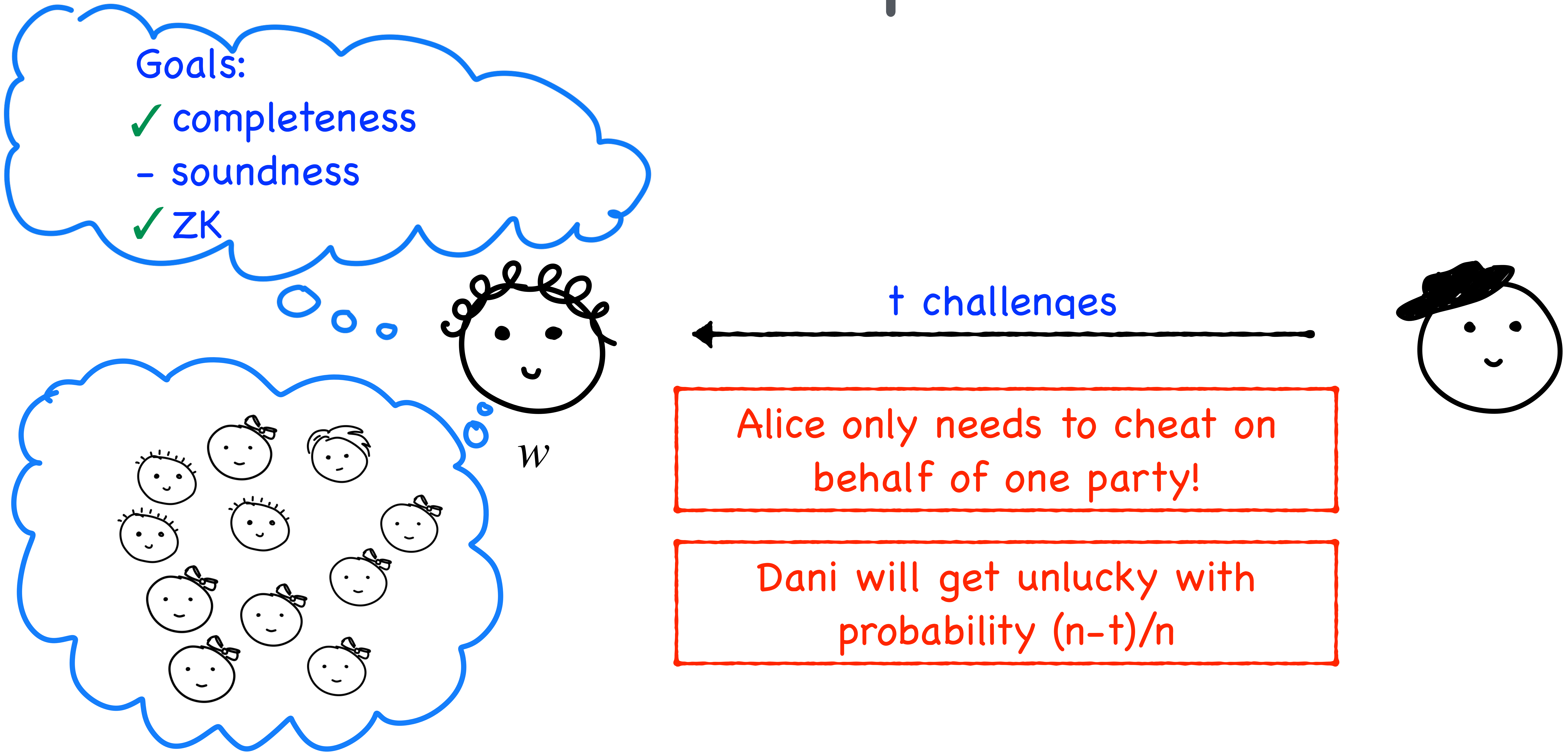
Alice only needs to cheat on behalf of one party!

Dani will get unlucky with probability (n-1)/n

MPC for $R(x, w_B + w_C)$ with:

- 1-privacy
- perfect correctness

Can We Avoid Repetition?



Goals:

✓ completeness

- soundness

✓ ZK

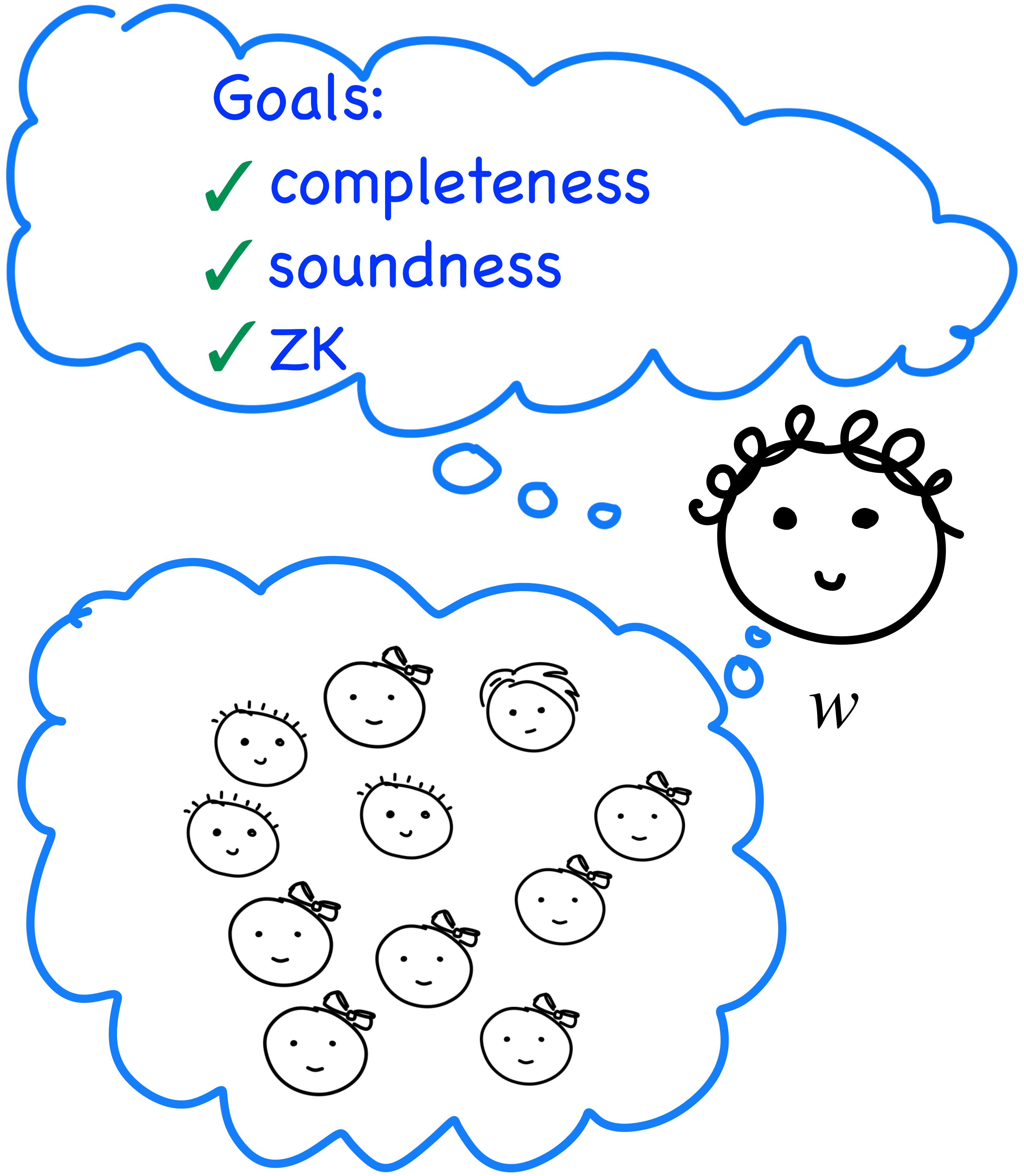
Alice only needs to cheat on behalf of one party!

Dani will get unlucky with probability (n-t)/n

MPC for $R(x, w_B + w_C)$ with:

- t-privacy
- perfect correctness

Can We Avoid Repetition?



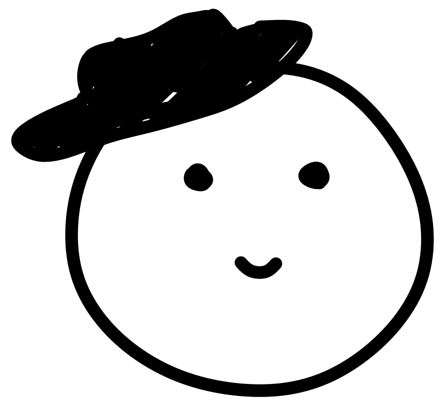
Goals:

✓ completeness

✓ soundness

✓ ZK

t challenges



Alice needs to cheat on behalf of t+1 parties!

Dani will get unlucky with probability $\binom{n-(t+1)}{t} / \binom{n}{t}$ = negl

MPC for $R(x, w_B + w_C)$ with:

- t-privacy Q: Does privacy need to hold if anyone cheats?
- perfect correctness **even if up to t parties cheat** → "malicious security"

Can We Avoid Repetition?

- Yes! But what's the point?

	Communication Complexity	Tools
Reduce to Sudoku (or something…)	$poly(k, \|R\|)$	lightweight
Run MPC	$O(k\|R\|)$	heavyweight
Run MPC in the Head	$O(k\|R\|)$	lightweight

Avoiding Repetition in MPC in the Head	$O(t\|VIEW\|) = O(k\|R\|)$	lightweight

Can We Avoid Repetition?

- Yes! But what's the point?

	Communication Complexity	Tools
Reduce to Sudoku (or something…)	$poly(k, \|R\|)$	lightweight
Run MPC	$O(k\|R\|)$	heavyweight
Run MPC in the Head	$O(k\|R\|)$	lightweight

- Using a very special MPC, we can do better!

Avoiding Repetition in MPC in the Head	$O(\|R\|) + poly(k, \log(\|R\|))$	lightweight

Back to Reality!

- Repetition performs better [ZKBoo, GMO]
- Asymptotically loses to zk-STARKs / zk-SNARKs, but wins for small computations!
- Gives us efficient post-quantum digital signatures!

Up til now…

Zero Knowledge Proofs (ZKP)

⇑

Secure Multiparty Computation (MPC)

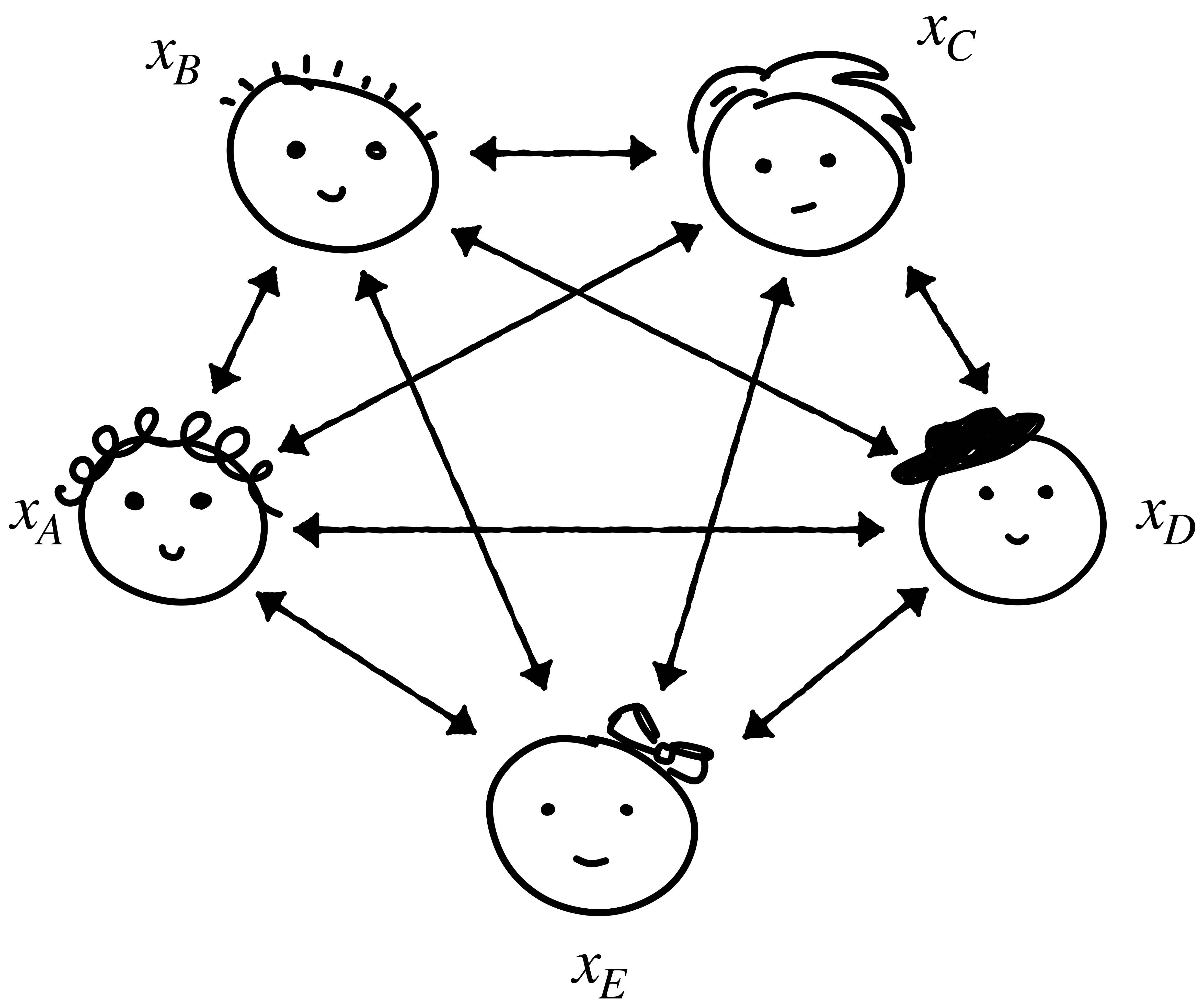
Briefly:

Zero Knowledge Proofs (ZKP)

$$\Downarrow$$

Secure Multiparty Computation (MPC)

Back to MPC



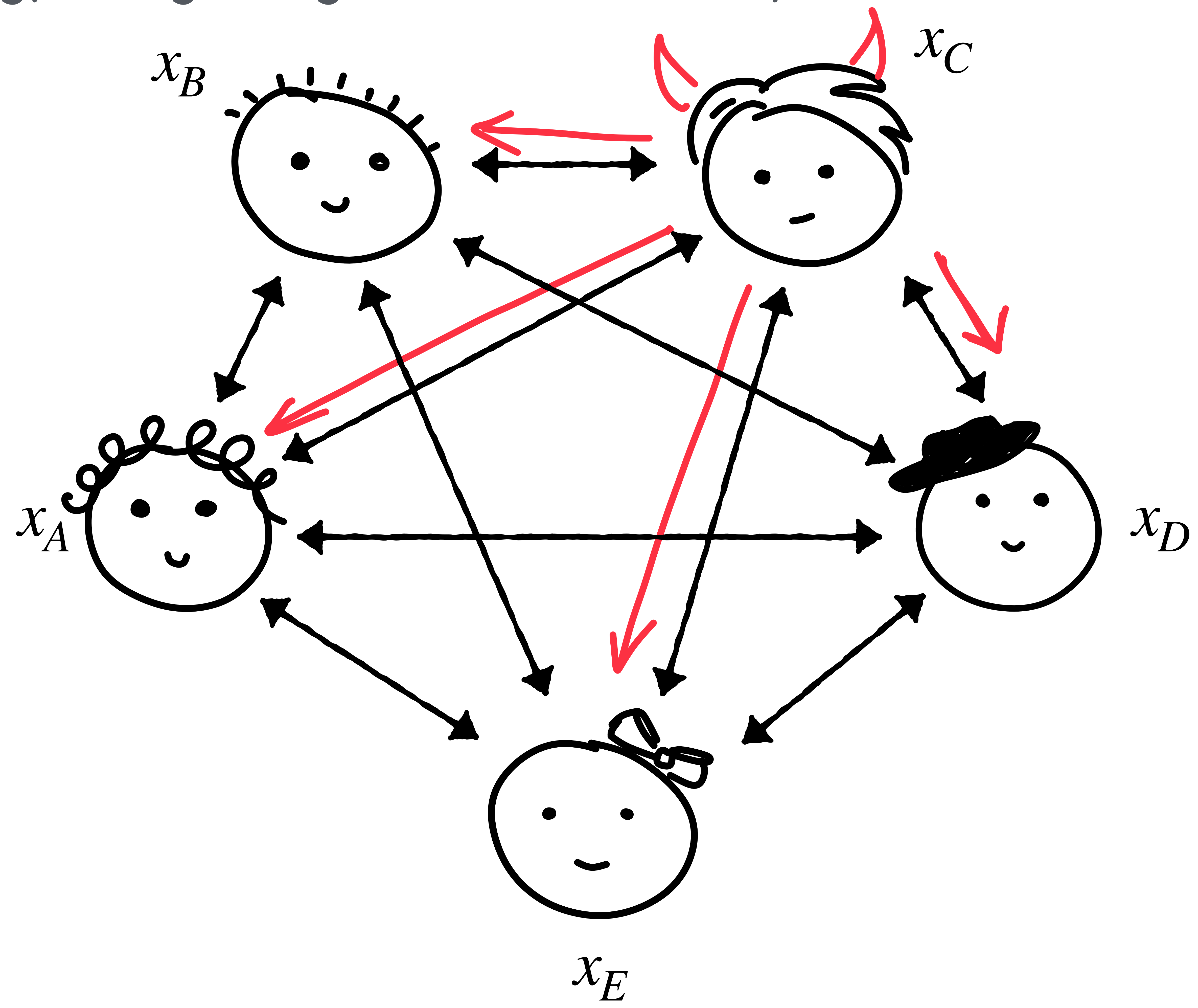
We have:

- correctness
- privacy

as long as everyone follows instructions.

Back to MPC

Strategy for getting malicious security?



We want:

- correctness
- privacy

even if up to t participants cheat!

take a protocol secure against "passive" corruptions, and have each participant zero-knowledge-prove their correct behavior!

Questions?

Zero Knowledge Proofs (ZKP)

$\Updownarrow$

Secure Multiparty Computation (MPC)