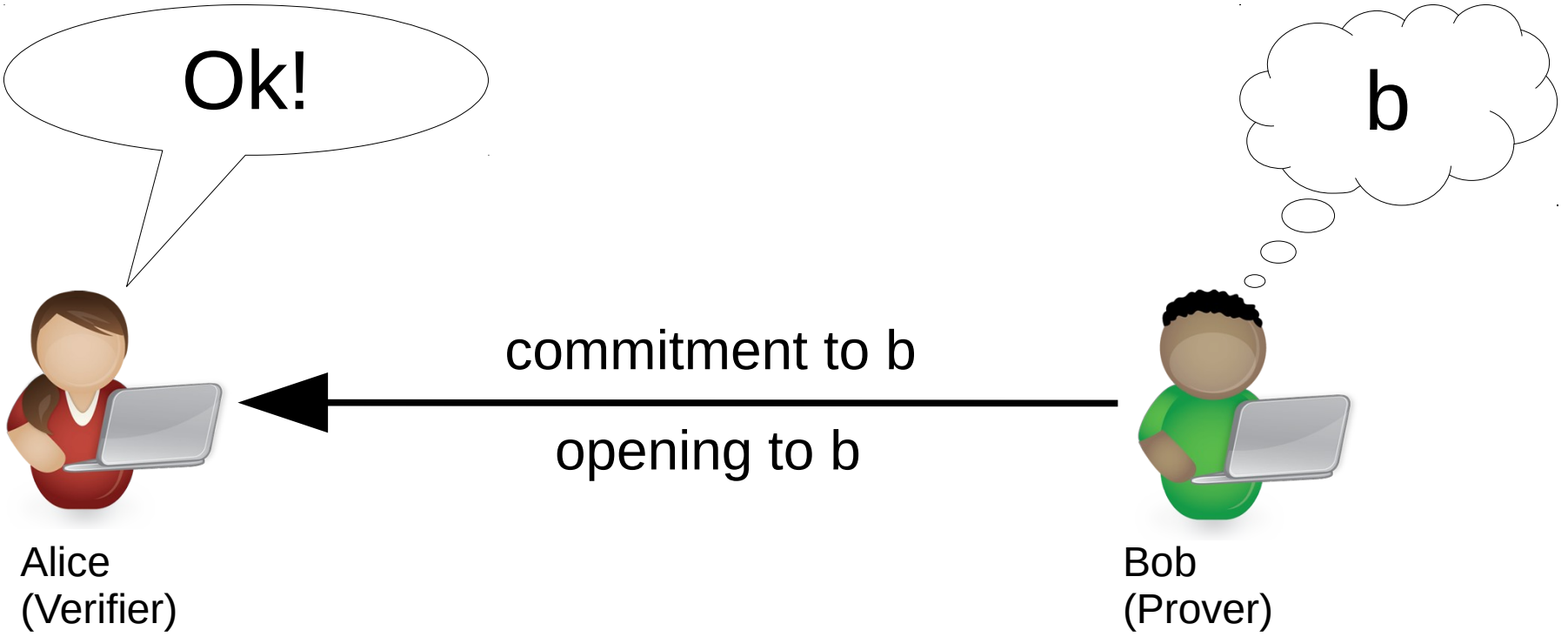
Multi-Prover Commitments Against Non-Signaling Attacks

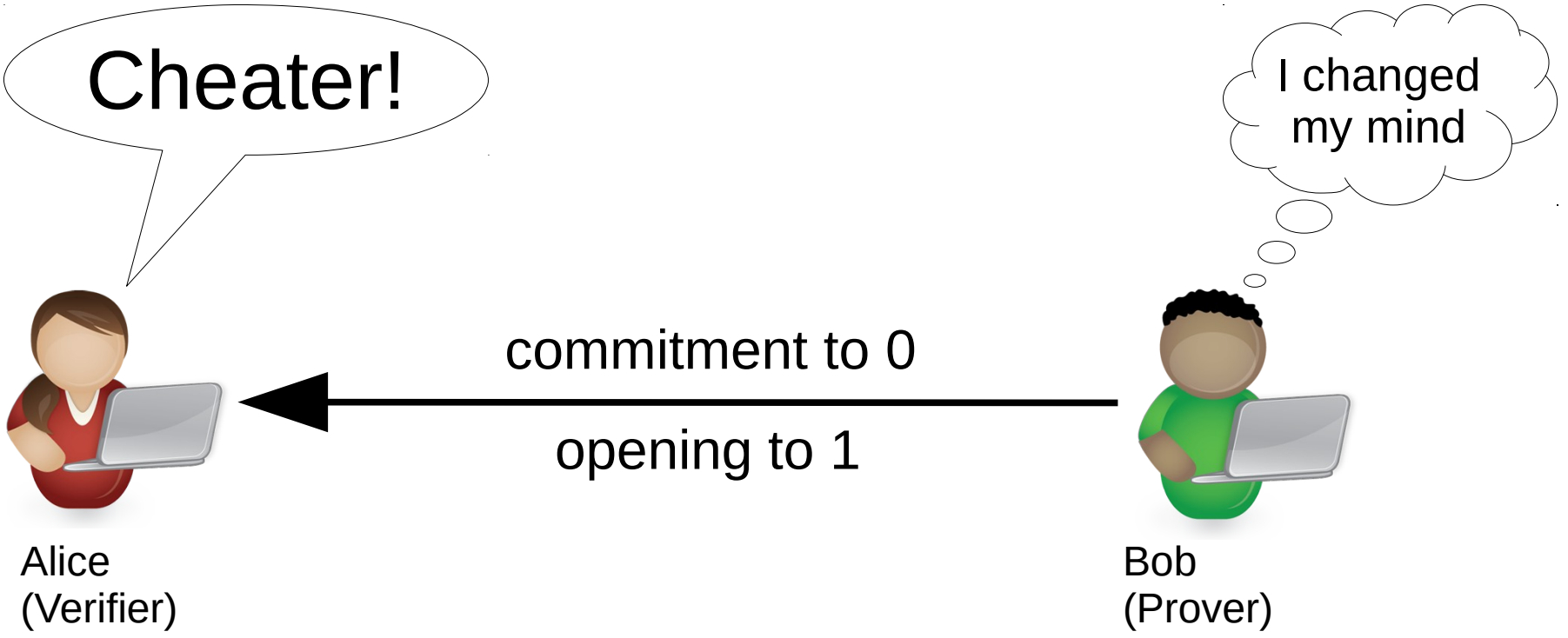
Max Fillinger (CWI)

Joint work with Serge Fehr (CWI)

Bit-commitment



Bit-commitment

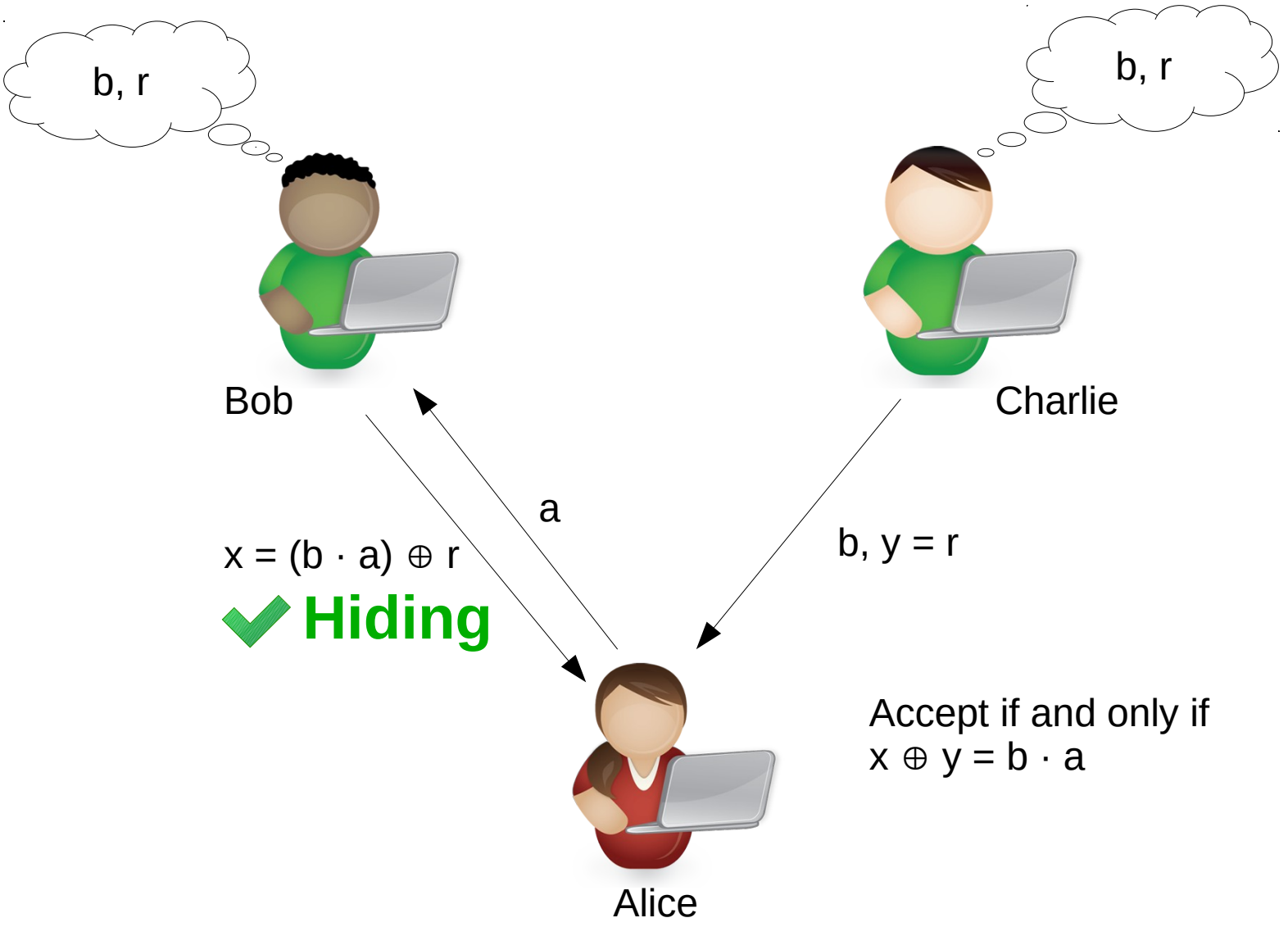


Bit-commitment

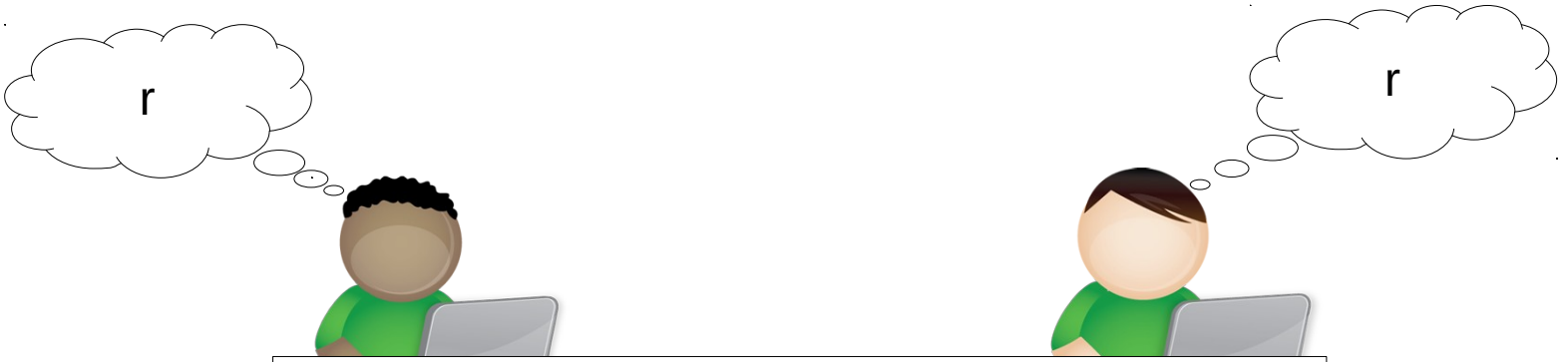
Information-theoretic security is impossible, even with quantum communication

- computational hardness assumptions
- bounded (quantum) memory
- multiple non-communicating provers (Ben-Or, Goldwasser, Kilian, Wigderson 1988)

A Two-prover Scheme



A Two-prover Scheme



Security based ONLY on non-communication...

Or not?

ie

= x opens to 0

= x ⊕ a opens to 1

⊕ y_1 = a

Alice

Accept if and only if
$x \oplus y = b \cdot a$

✔ **Binding**

Resources

[CSST11] Hidden assumption:

Provers only have classical shared randomness

But security depends on provers' resources

- Shared randomness 
- Quantum entanglement 
- General non-signaling system 

Resources

- There are schemes that are

✔ **Binding**

✔ **Binding**

✘ **Non-binding**

- There are schemes that are

✔ **Binding**

✘ **Non-binding**

NO known scheme is

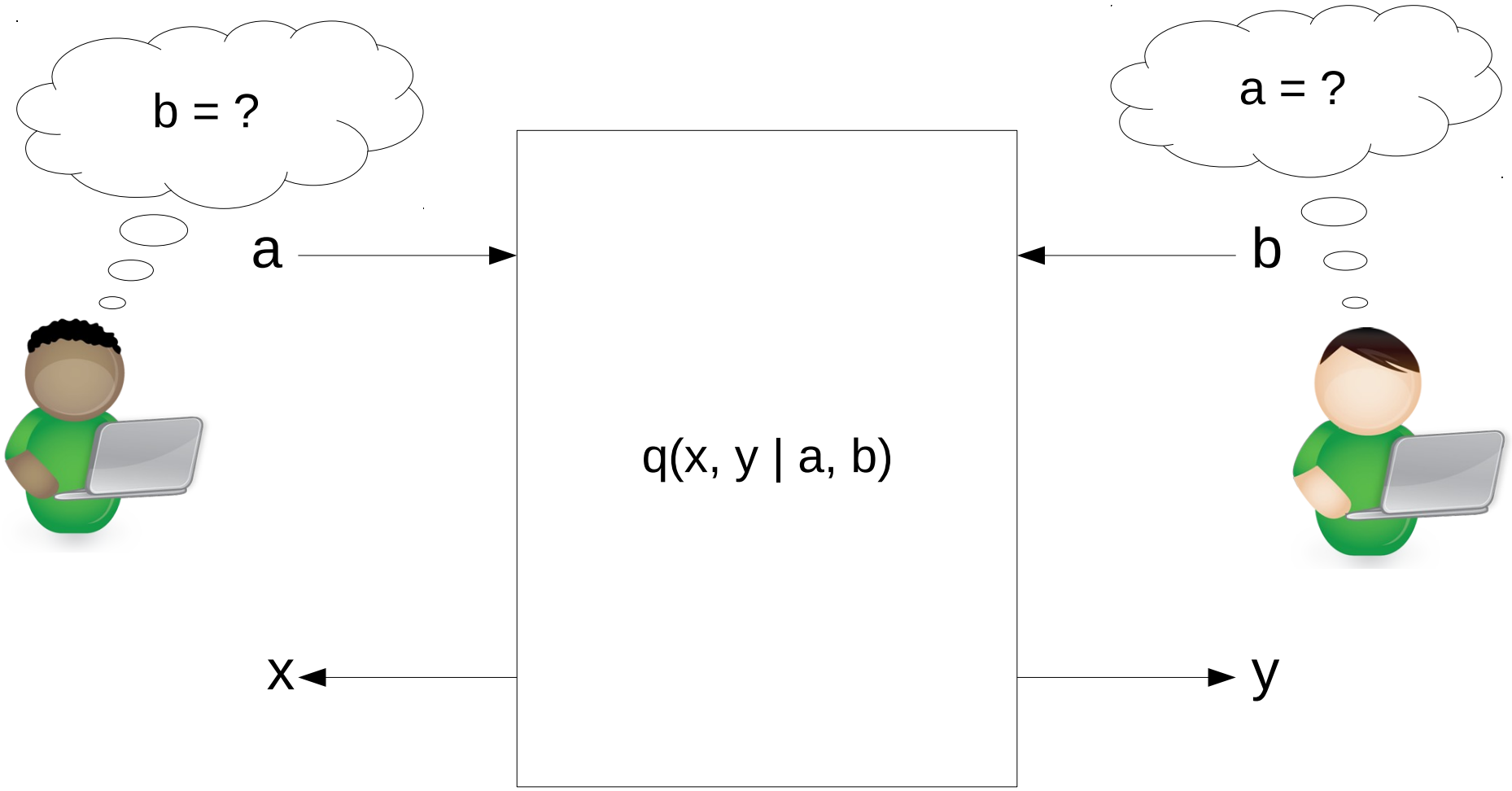
✔ **Binding**

Can we base security only on non-communication?

Impossibility result for 2 provers

Positive result for 3 provers

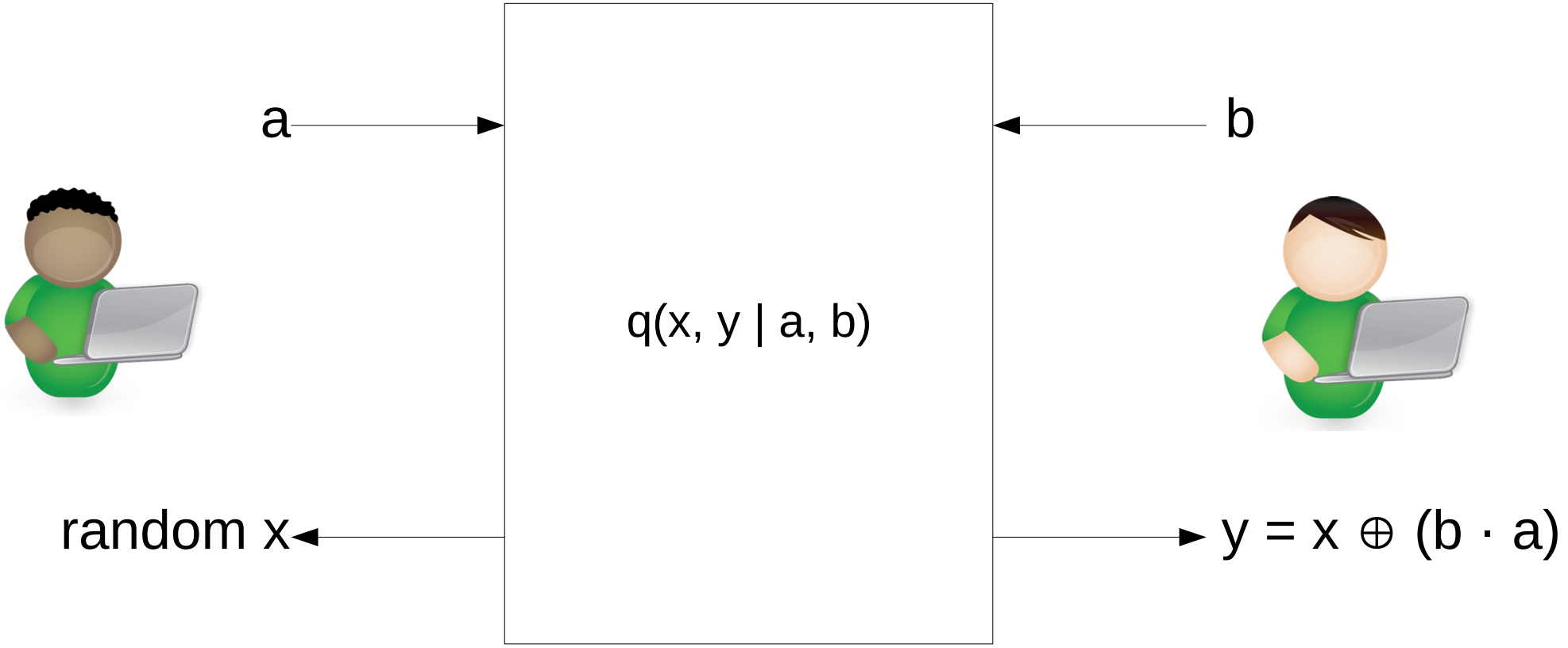
Defining Non-signaling



$q(x \mid a, b) = q(x \mid a, b')$

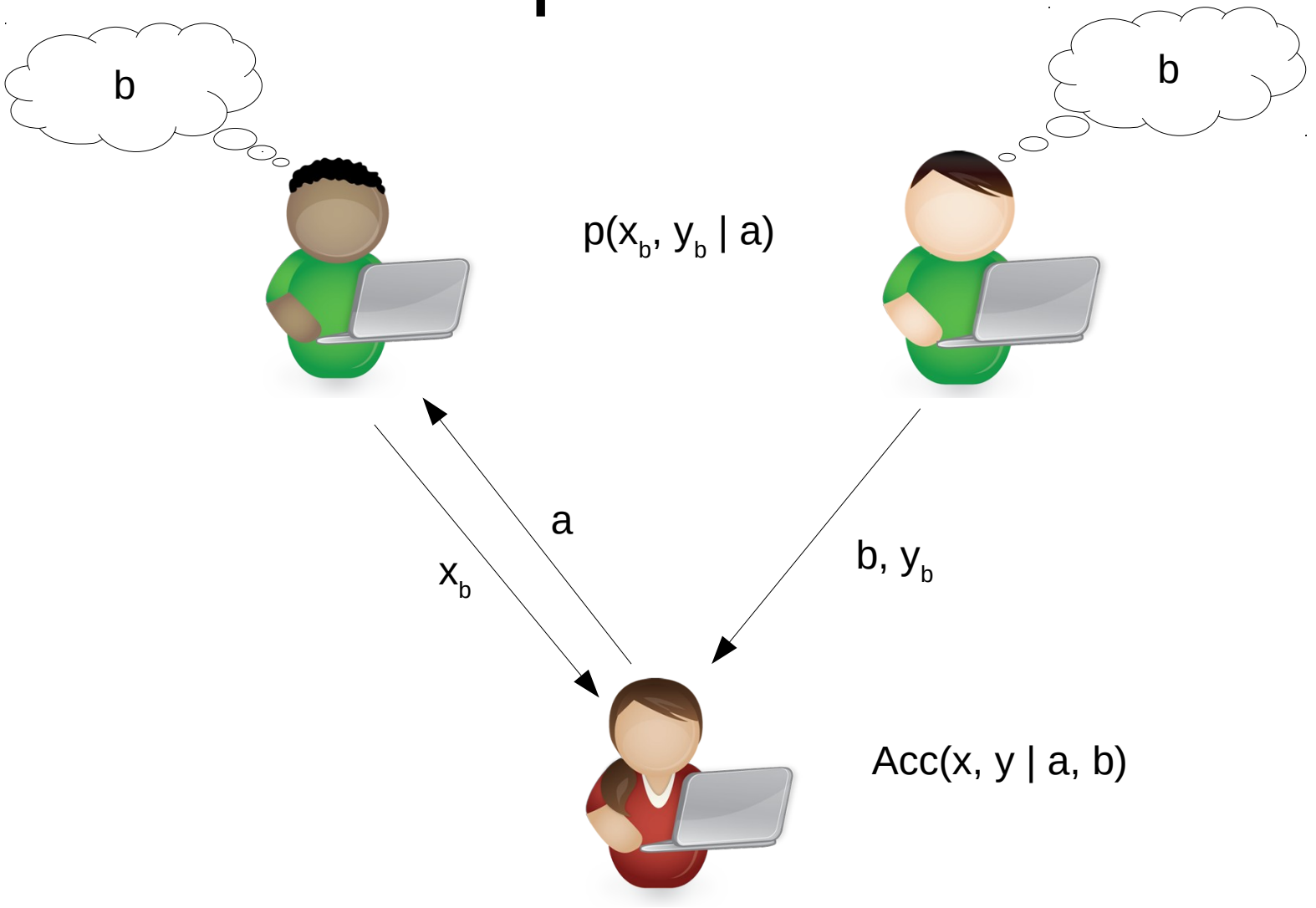
$q(y \mid a, b) = q(y \mid a', b)$

Example Non-signaling System



$$x \oplus y = b \cdot a$$

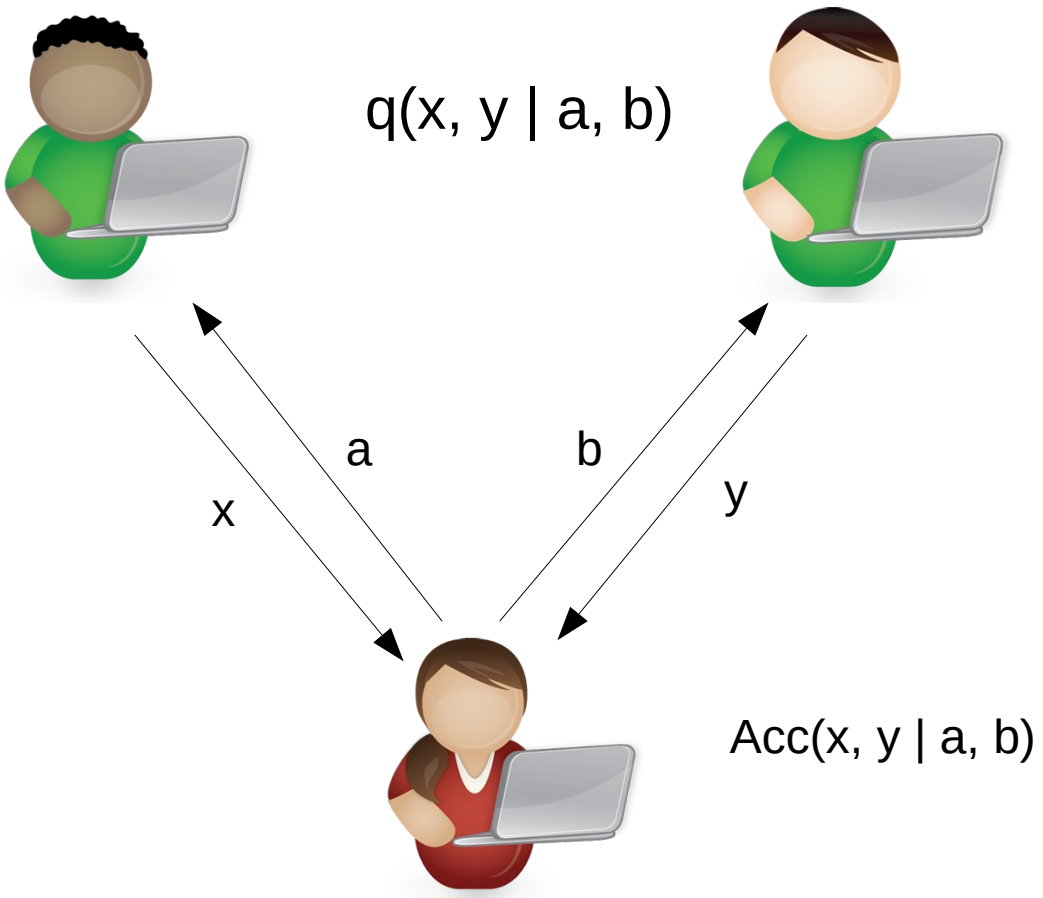
Simple Schemes



Properties of Simple Schemes

- soundness
- ε-hiding: $p(x_0 \mid a) \approx p(x_1 \mid a)$
- δ-binding: See next slide

The Binding Game



$P_b(q)$: Probability that Alice accepts opening for b

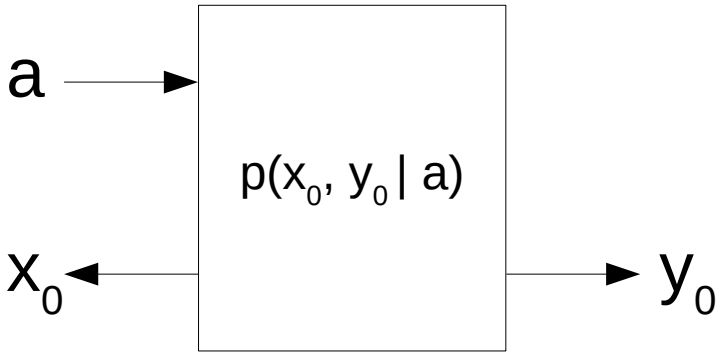
δ-binding: For all q, $P_0(q) + P_1(q) \leq 1 + \delta$

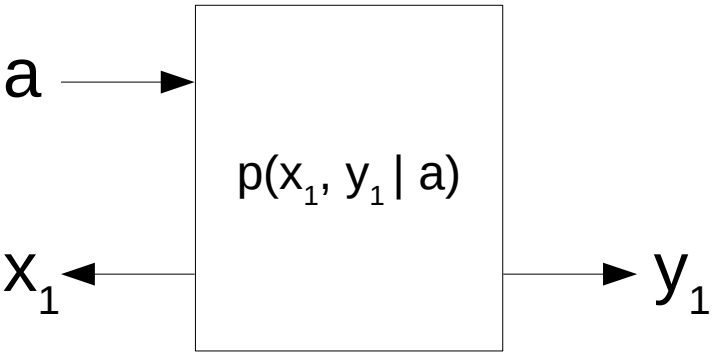
Impossibility Result 1

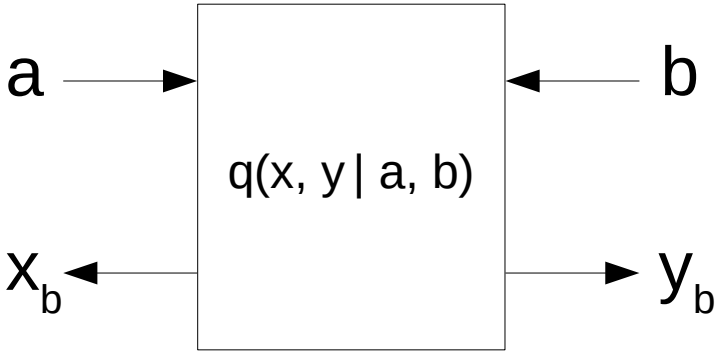
If a simple bit-commitment scheme is perfectly hiding, it is completely non-binding.

(the dishonest provers can always win)

Proof







$q(y \mid a, b) = p(y_b \mid a)$ independent of a

$q(x \mid a, 0) = p(x_0 \mid a) = p(x_1 \mid a) = q(x \mid a, 1)$

hiding

What about non-perfect schemes?

Can't use previous strategy, only almost non-signaling

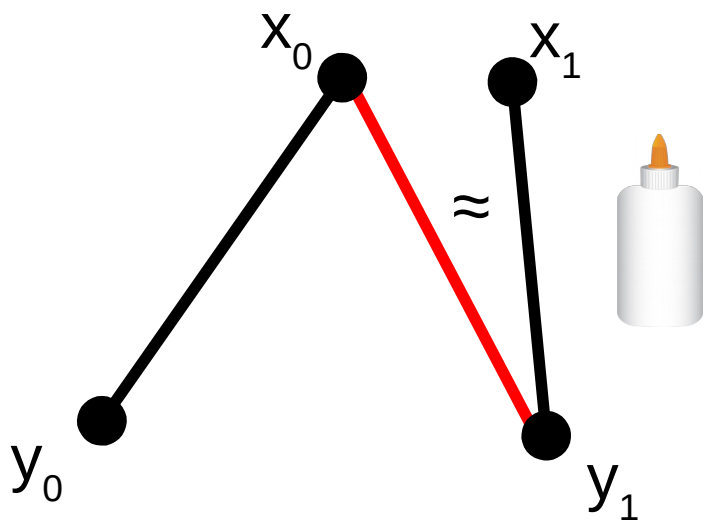
Impossibility Result 2

If a scheme is ε-hiding, it is at best (1-ε)-binding

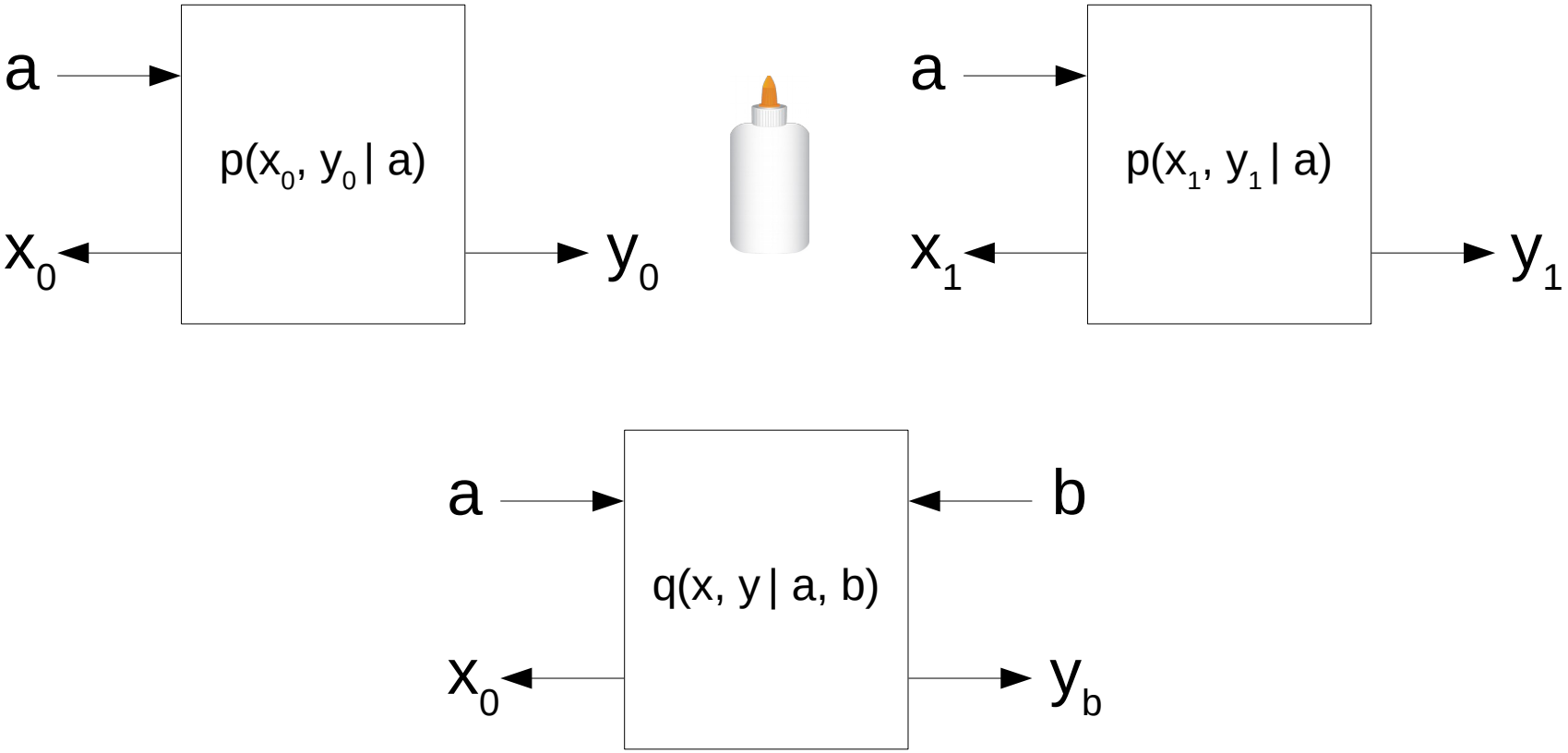
A Tool: The Gluing Lemma

$p(x_0, y_0)$, $p(x_1, y_1)$ s.t. $p(x_0) \approx p(x_1)$

$\Rightarrow \exists\ p(x_0, x_1, y_0, y_1)$ s.t. $p(x_0, y_1) \approx p(x_1, y_1)$



Proof



$q(x, y \mid a, 0) = p(x_0, y_0 \mid a)$

$q(x, y \mid a, 1) = p(x_0, y_1 \mid a) \approx p(x_1, y_1 \mid a)$

Results for General Schemes

Perfectly hiding $\Rightarrow$ completely non-binding

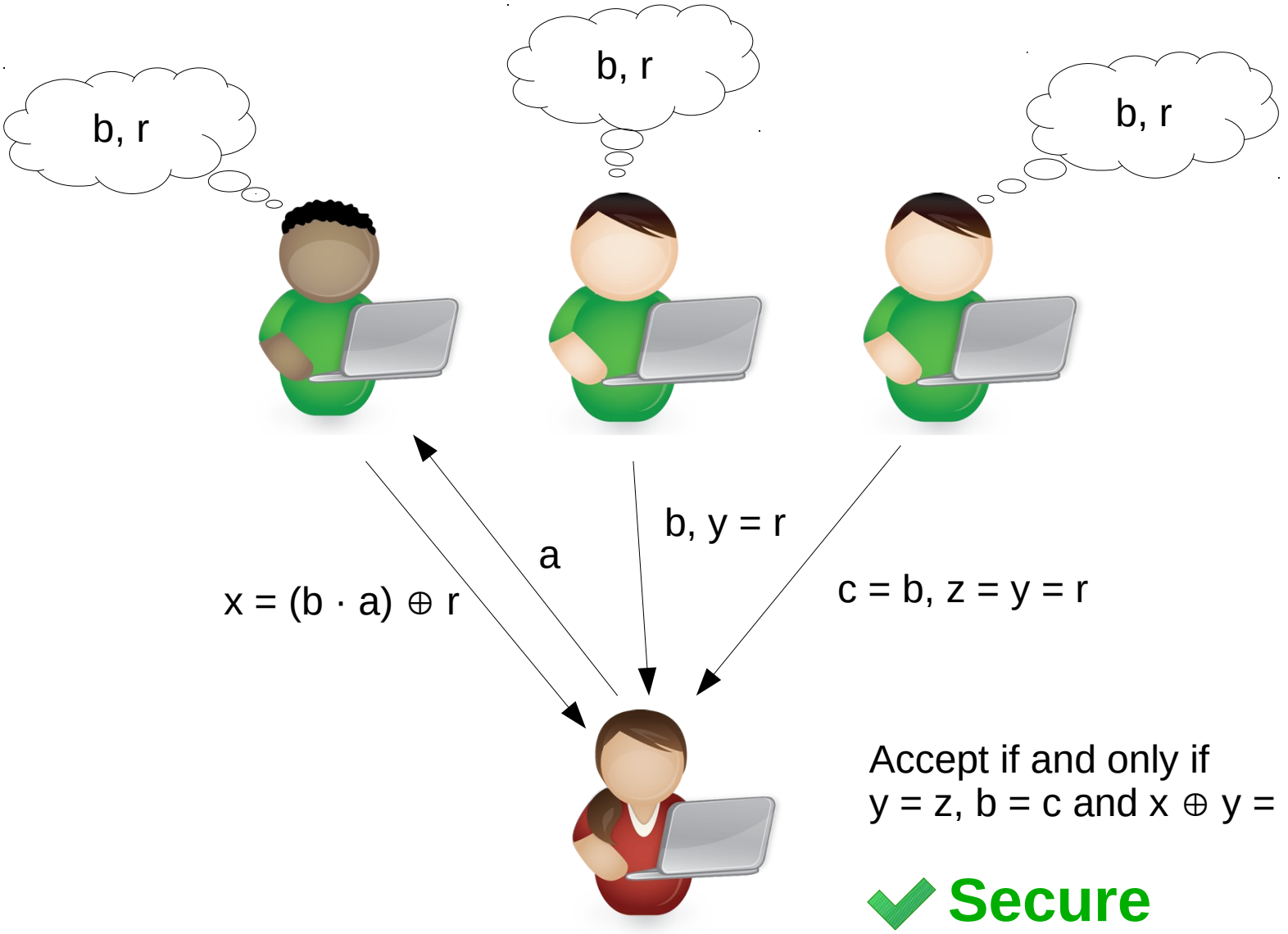
ε-hiding $\Rightarrow$ at best $(1-5\varepsilon)$-binding

Results for Multi-round Schemes

Perfectly hiding $\Rightarrow$ completely non-binding

ε-hiding $\Rightarrow$?

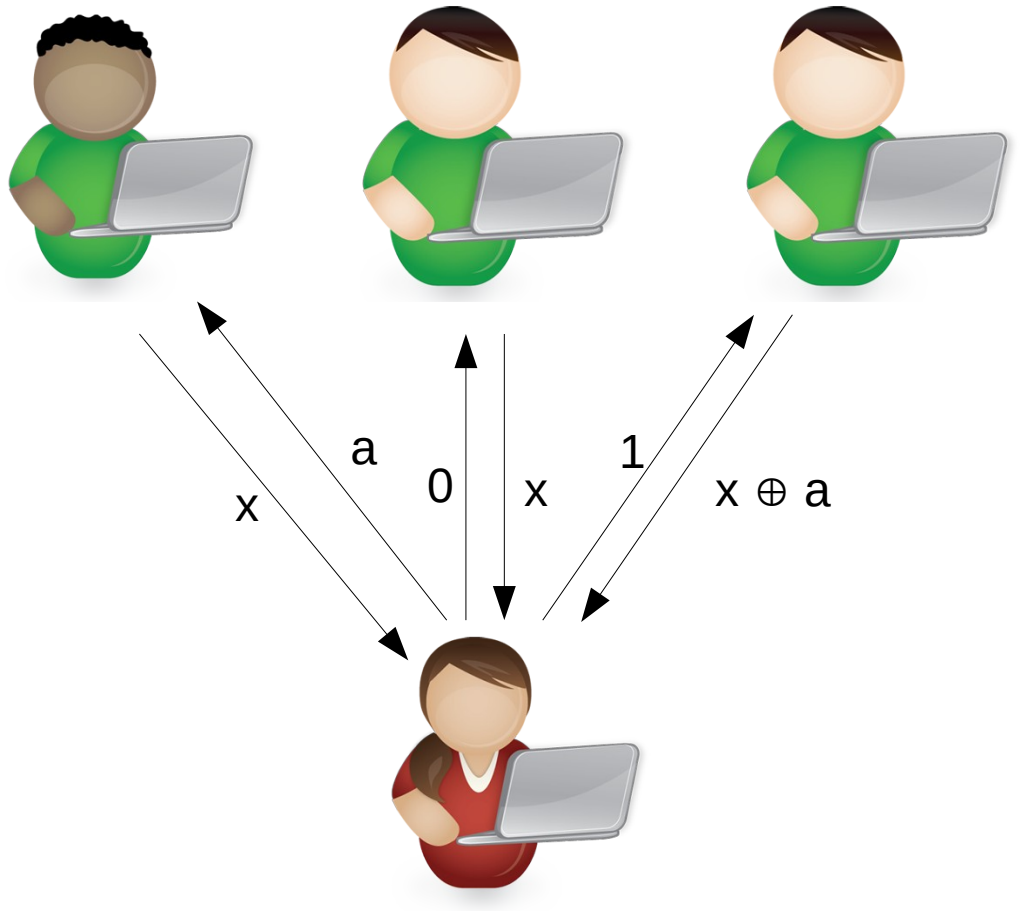
A Three-prover Scheme



Accept if and only if
$y = z$, $b = c$ and $x \oplus y = b \cdot a$

Secure
against non-signaling provers

A Three-prover Scheme



Results

ALL schemes: Perfectly hiding $\Rightarrow$ non-binding

One-round: Extends to non-perfect case

Simple schemes: Tight bound

Security by adding a third prover

Open questions

Improved/tight bound for general schemes

Multi-round: Non-perfect case

Thank you!