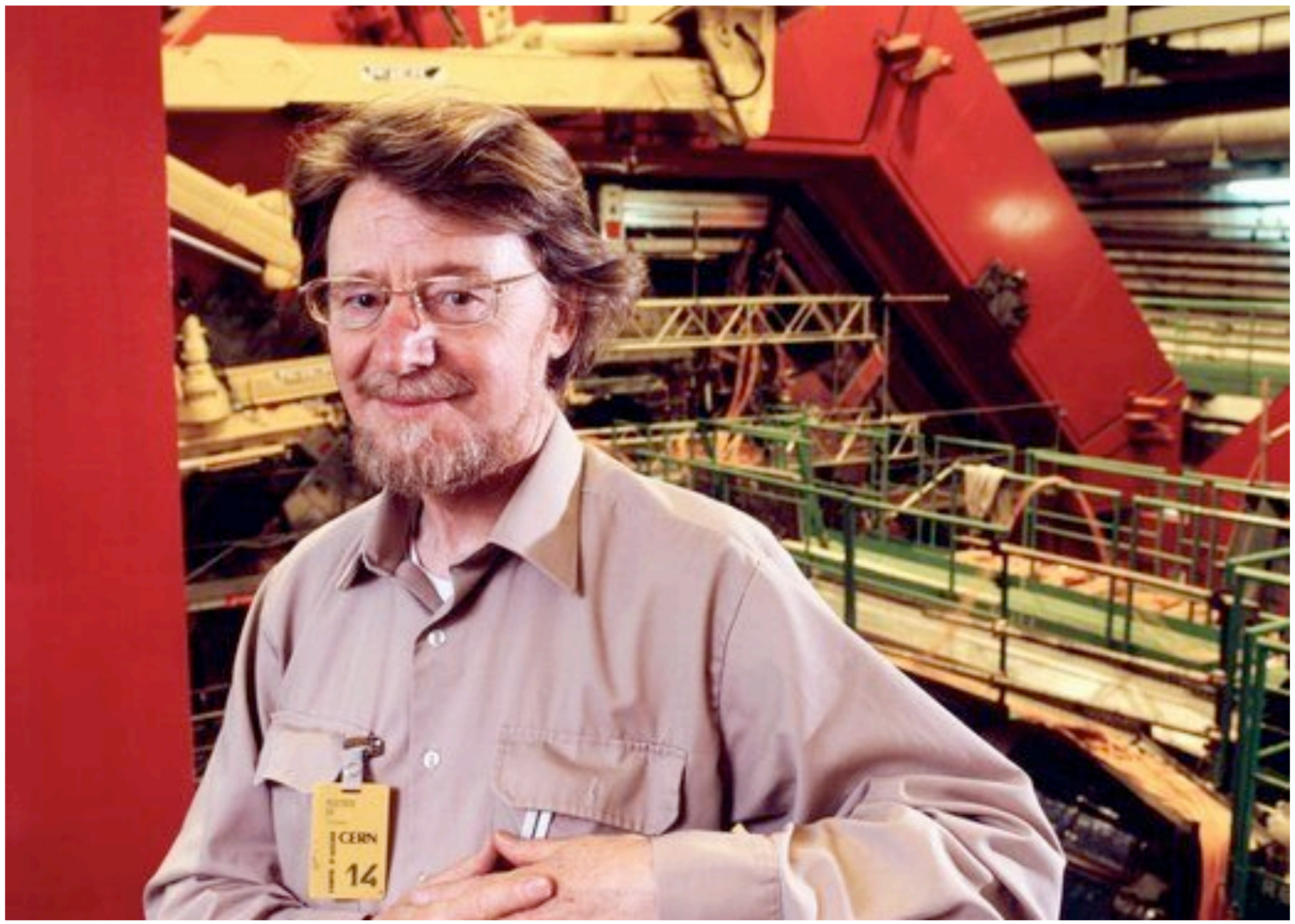
Putting Bell inequalities to work

Dan Browne - AMOPP Group, UCL

joint work with: **Janet Anders**, **Earl Campbell** (former post-docs) and **Matty Hoban** (former PhD student)

Talk Outline

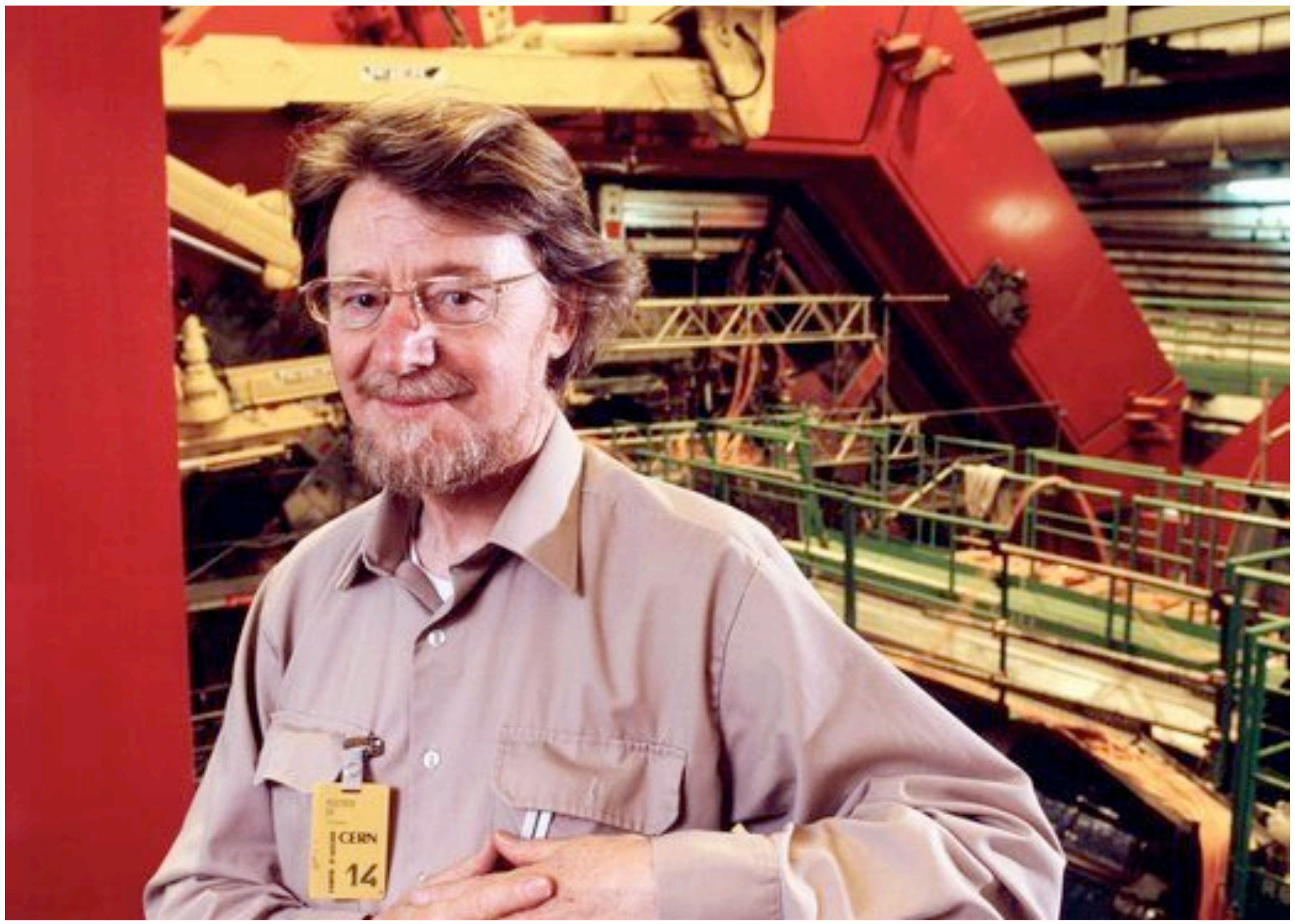


- Understanding **Bell inequalities** from the point of view of **computation**.

Talk Outline

- Understanding **Bell inequalities** from the point of view of **computation**.

Talk Outline



- Understanding **Bell inequalities** from the point of view of **computation**.

Talk Outline

Correlations

↓

Correlations and Computation

↓

From Classical Correlations

↓

To Quantum Correlations

Talk Outline

Correlations

↓

Correlations and Computation

↓

From Classical Correlations

↓

To Quantum Correlations

Correlations

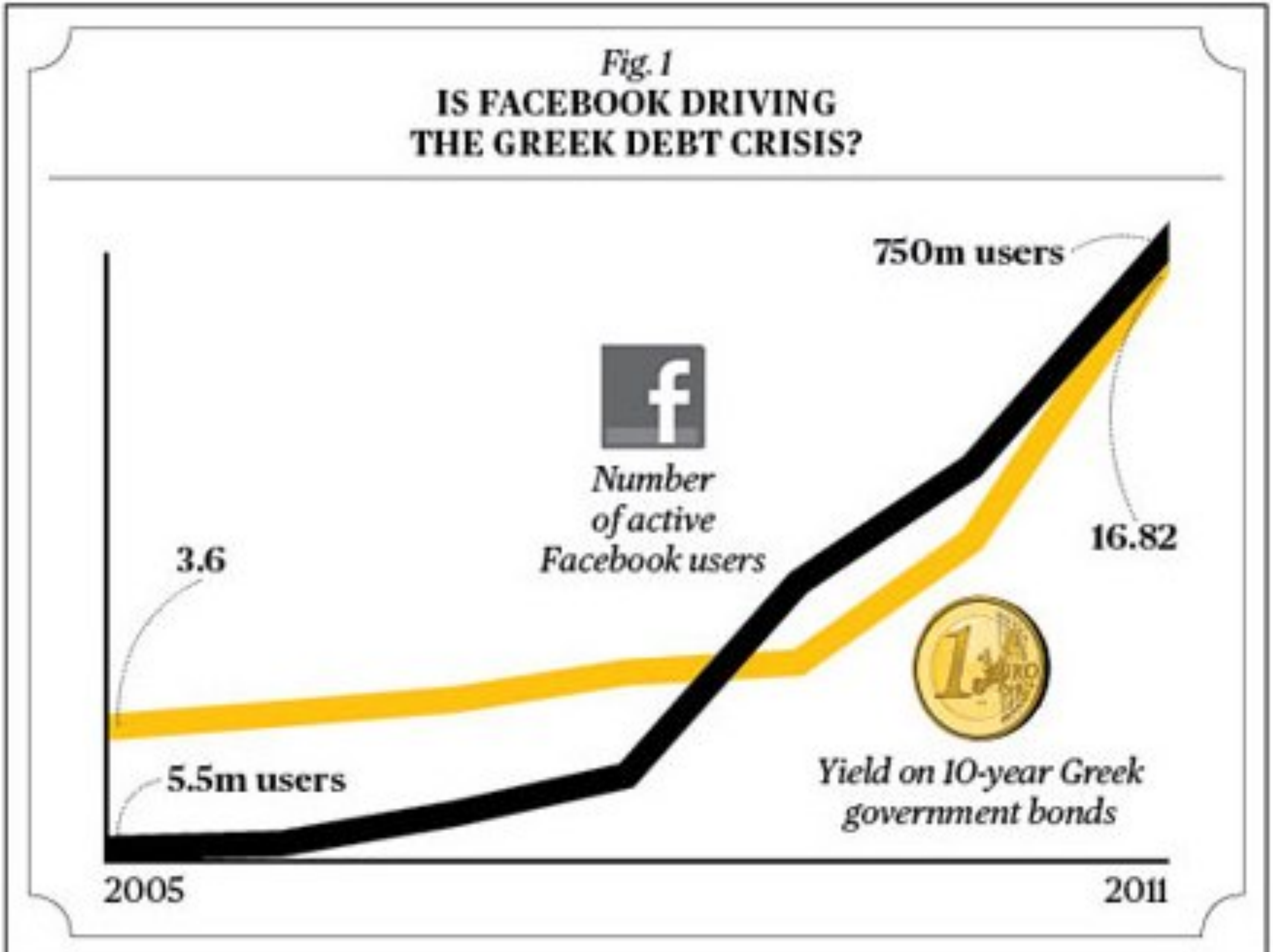


Image taken from www.businessweek.com

Correlations

Correlations

Alice

Bob

Correlations

Alice

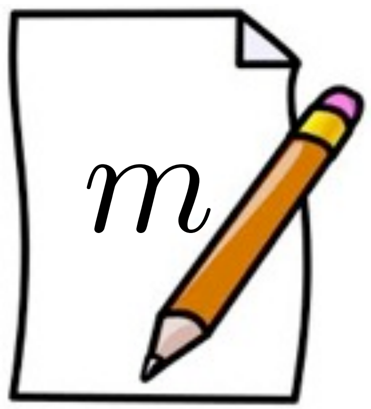
Bob

Correlated

Correlations as a resource

Alice | **Bob**

Message bit



The Vernam cypher (or one-time pad)

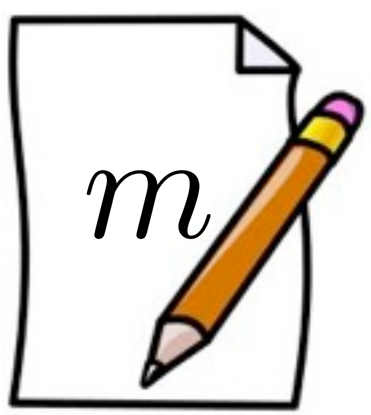
The **only** provably unbreakable crypto-system.

Correlations as a resource

Alice

Bob

Message bit



Secret random correlated bit

Secret random correlated bit

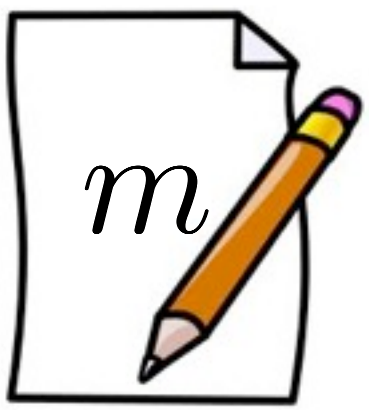
The Vernam cypher (or one-time pad)

The **only** provably unbreakable crypto-system.

Correlations as a resource

Alice | **Bob**

Message bit



Secret random correlated bit

Secret random correlated bit

$$m \oplus r \longrightarrow$$

The Vernam cypher (or one-time pad)

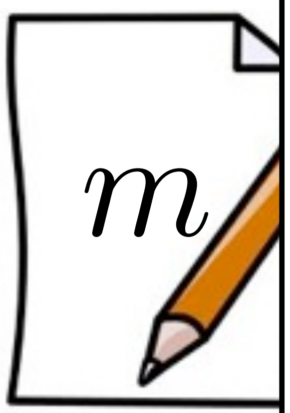
The **only** provably unbreakable crypto-system.

Correlations as a resource

Alice

Bob

Message b



Notation: Addition Modulo 2

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 1 = 0$$

ret random
rrelated bit

$$m \oplus r$$

$$\longrightarrow$$

The Vernam cypher (or one-time pad)

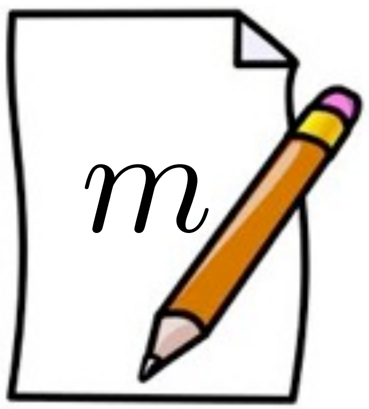
The **only** provably unbreakable crypto-system.

Correlations as a resource

Alice

Bob

Message bit



Secret random correlated bit

Secret random correlated bit

$$m \oplus r$$

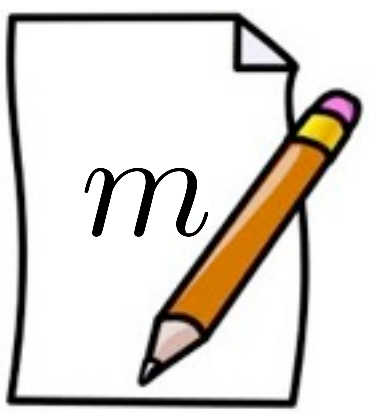
The Vernam cypher (or one-time pad)

The **only** provably unbreakable crypto-system.

Correlations as a resource

Alice | **Bob**

Message bit

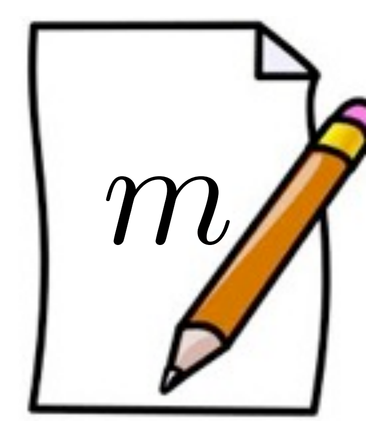


Secret random correlated bit

Secret random correlated bit

$$m \oplus r \longrightarrow$$

$$m \oplus r \oplus r = m$$



The Vernam cypher (or one-time pad)

The **only** provably unbreakable crypto-system.

Talk Outline

Correlations

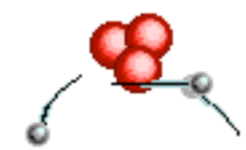
Bell's Theorem

Correlations and Computation

From Classical Correlations

To Quantum Correlations

Bell's theorem



- **John Bell (1960s) (**paraphrased):
  - Measurements on **space-like separated quantum** systems can exhibit **correlations impossible** to achieve in classical physics (or **any local realistic** theory).

Bell’s theorem

Local realistic theories (Local hidden variable models)

Local

An observed **event** (e.g. the outcome of a measurement) can only be **influenced** by events in its **past light cone**.

Bell’s theorem

Local realistic theories (Local hidden variable models)

Local

An observed **event** (e.g. the outcome of a measurement) can only be **influenced** by events in its **past light cone**.

Realistic

Measurements reveal **pre-existing** properties - i.e. any apparent **randomness** is due to our **ignorance** only.

Bell’s theorem

Local realistic theories (Local hidden variable models)

Local

An observed **event** (e.g. the outcome of a measurement) can only be **influenced** by events in its **past light cone**.

Realistic

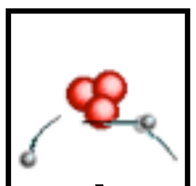
Measurements reveal **pre-existing** properties - i.e. any apparent **randomness** is due to our **ignorance** only.

Relativistic **classical physics** is **local realistic.**

The CHSH Inequality

The "Textbook" Bell Inequality

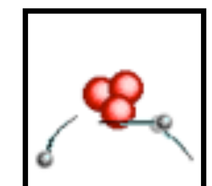
2 settings (0 or 1)



+1 or -1

space-like separated measurements

2 settings (0 or1)



+1 or -1

E_{jk} Expectation value of product of outcomes

Local realistic theories satisfy the **CHSH Bell Inequality**

$$|E_{00} + E_{10} + E_{01} - E_{11}| \leq 2$$

Violated by QM

Two readings of Bell's theorem

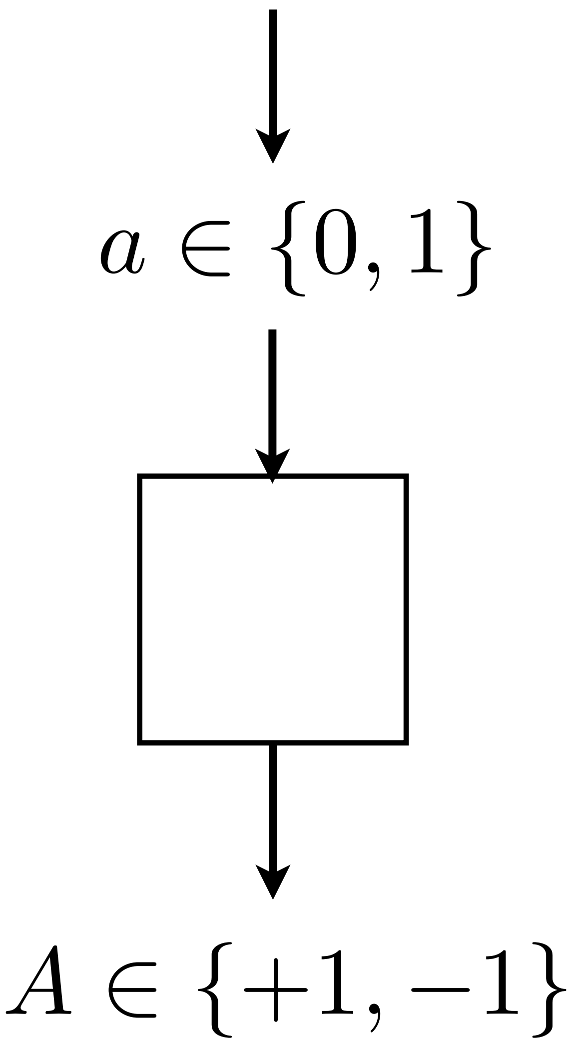
- **Standard interpretation**
  - Quantum Mechanics is not a local realistic theory.

Two readings of Bell's theorem

- **Standard interpretation**
  - Quantum Mechanics is not a local realistic theory.
- **Quantum Information interpretation**
  - Correlations in Quantum Mechanics achieve something **impossible** in classical physics.
  - What can we **use** this for?

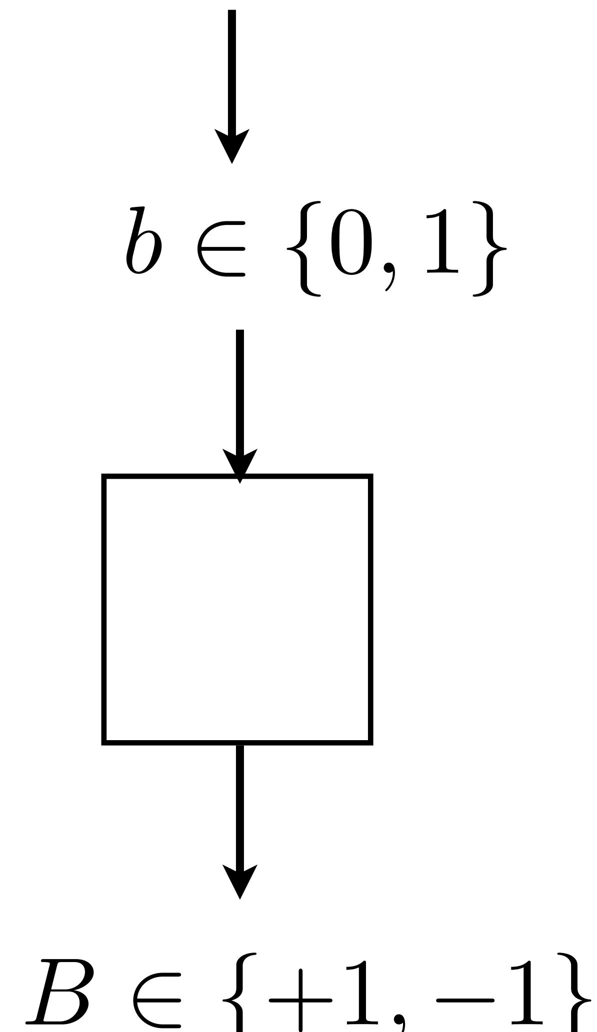
From correlations to computations

Alice

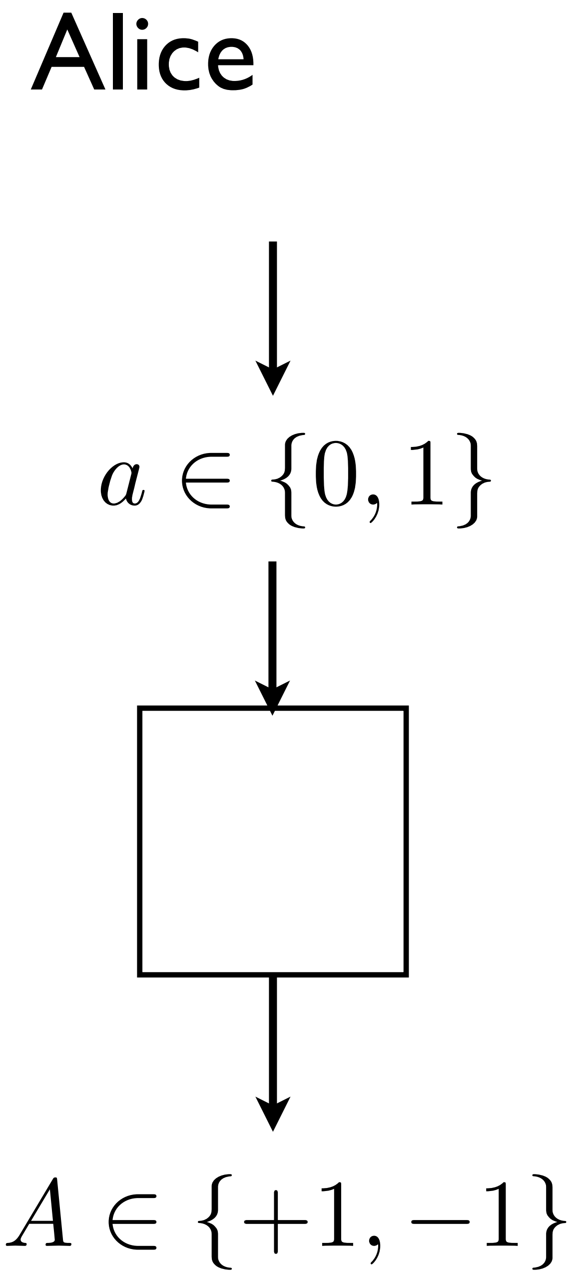


In the setting of Bell's theorem, we are asking:

Bob



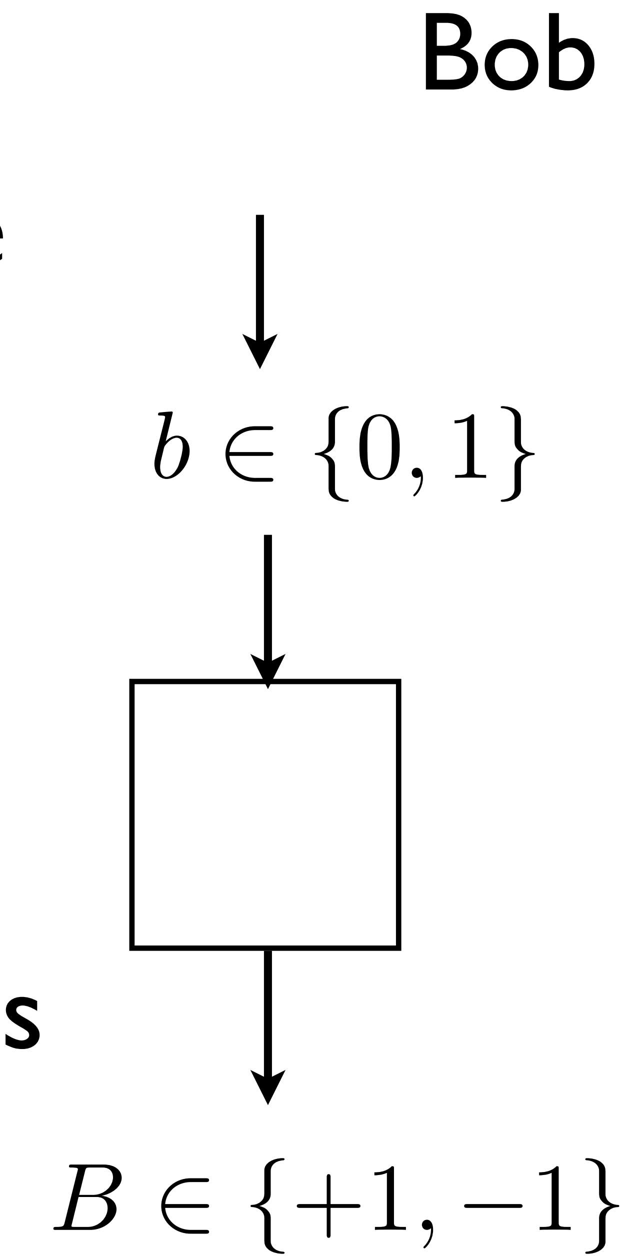
From correlations to computations



In the setting of Bell's theorem, we are asking:

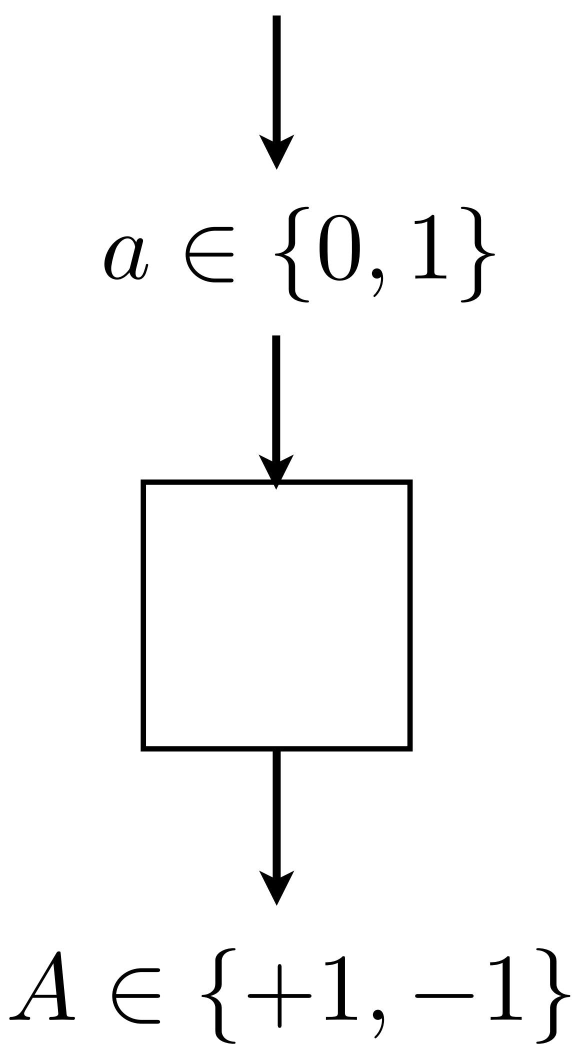
What **correlations** are **possible** in principle in:

Classical (local realistic) **Physics**
Quantum Physics

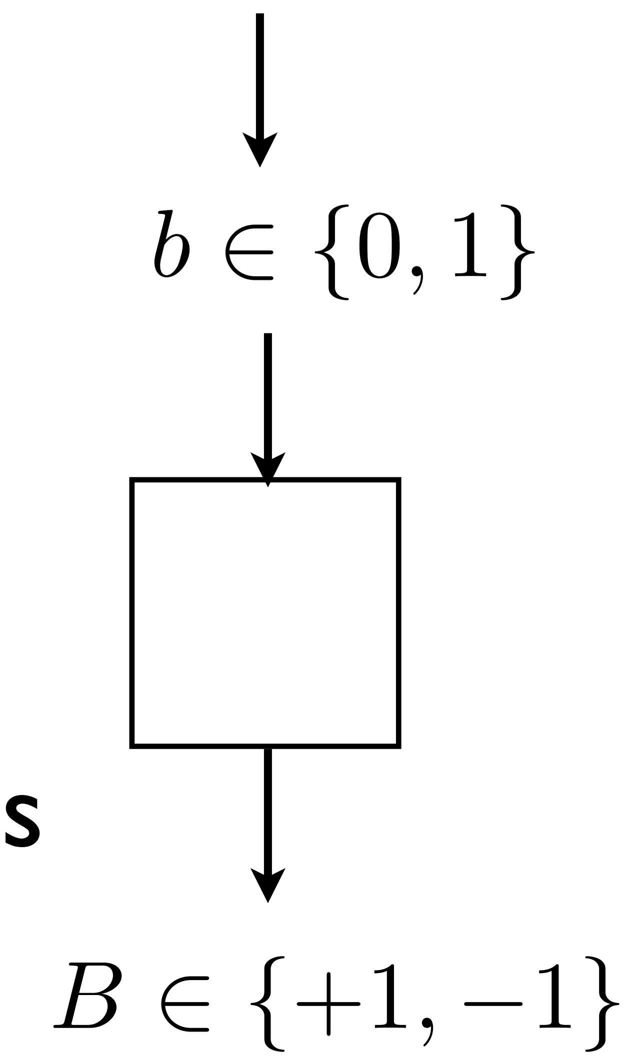


From correlations to computations

Alice



Bob



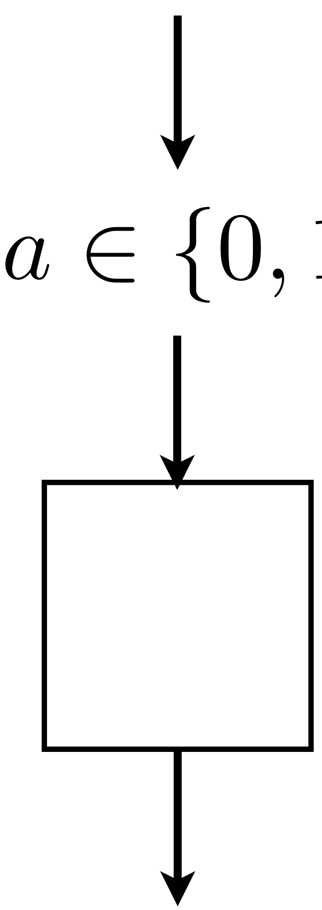
Our approach...

What **correlations** are **possible** in principle in:

- **Classical** (local realistic) **Physics**
- **Quantum Physics**

From correlations to computations

Alice

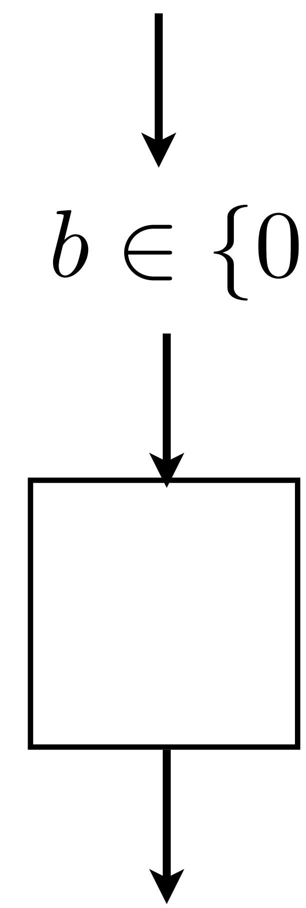


$a \in \{0,1\}$

$\cancel{A \in \{+1,-1\}}$

$A \in \{0,1\}$

Bob



$b \in \{0,1\}$

$\cancel{B \in \{+1,-1\}}$

$B \in \{0,1\}$

Our approach...

computations

What ~~**correlations**~~ are **possible** in principle in:

Classical (local realistic) **Physics**

Quantum Physics

Talk Outline

Correlations

↓

Correlations and Computation

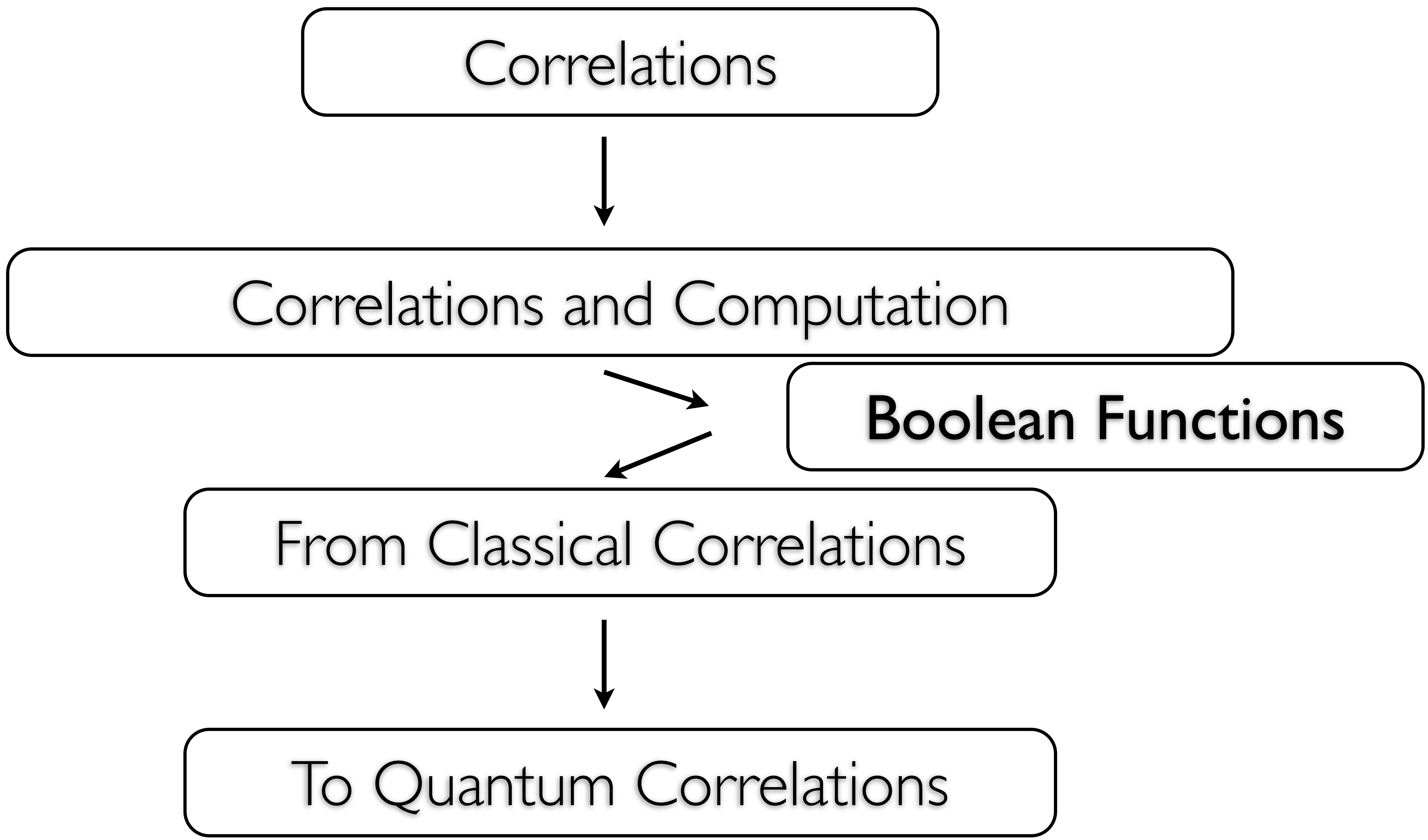
↓

From Classical Correlations

↓

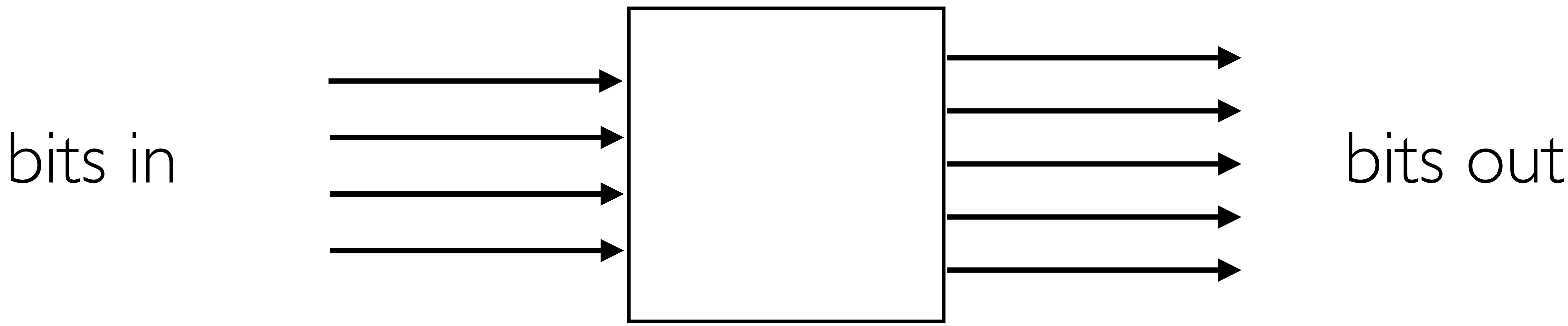
To Quantum Correlations

Talk Outline



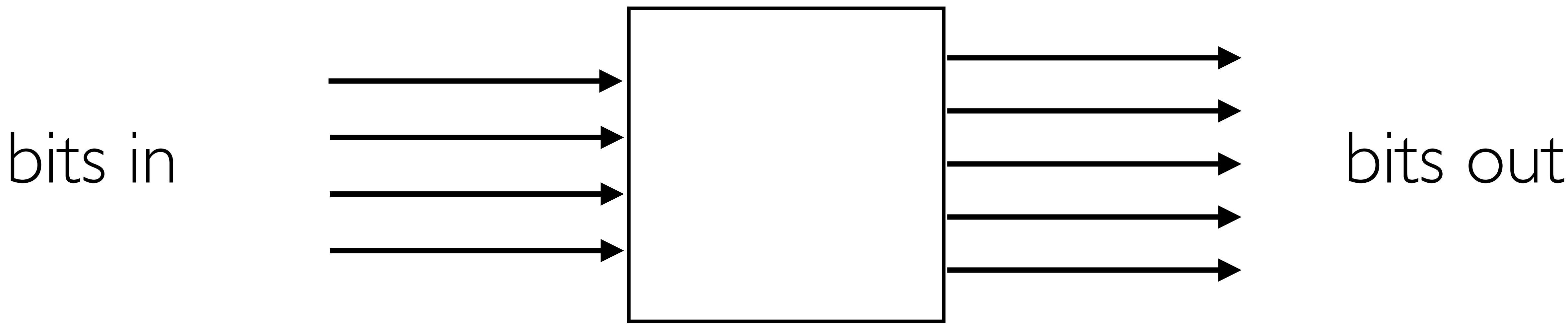
Boolean functions

A computation

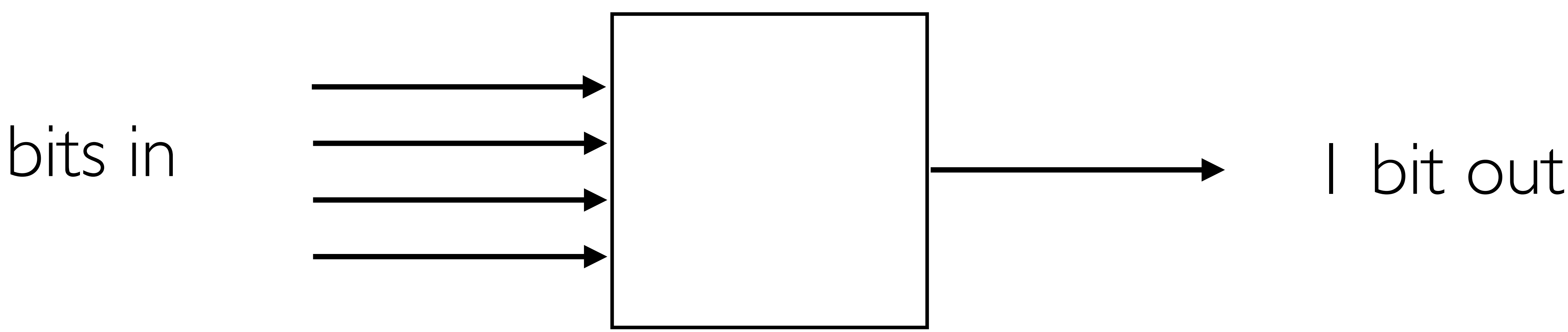


Boolean functions

A computation

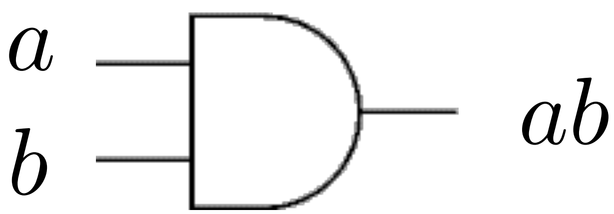


A Boolean function



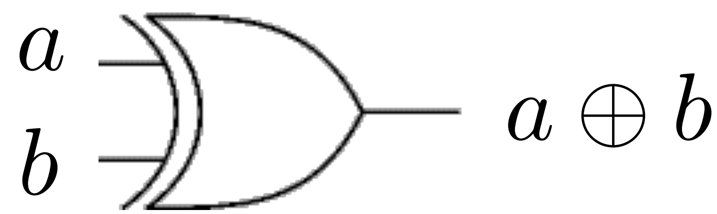
Boolean Functions

AND



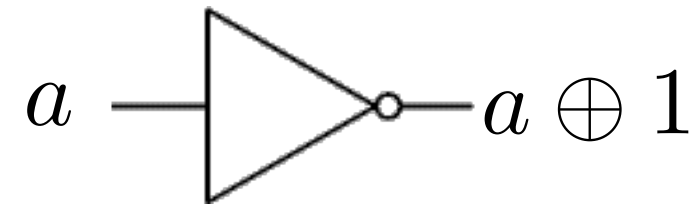
a	b	a b
0	0	0
0	1	0
1	0	0
1	1	1

XOR



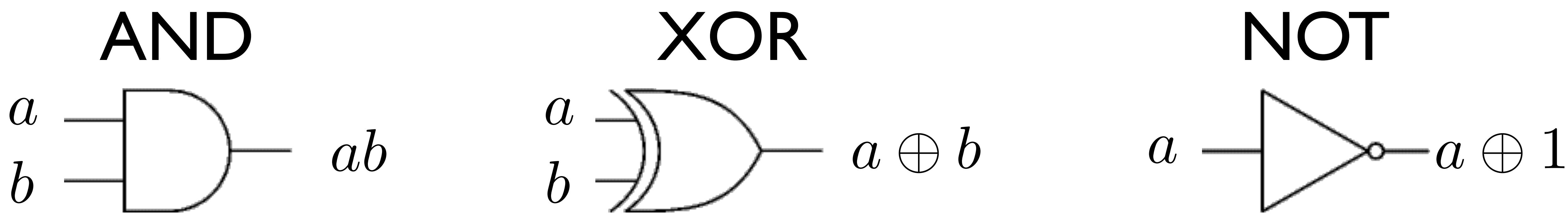
a	b	a⊕b
0	0	0
0	1	1
1	0	1
1	1	0

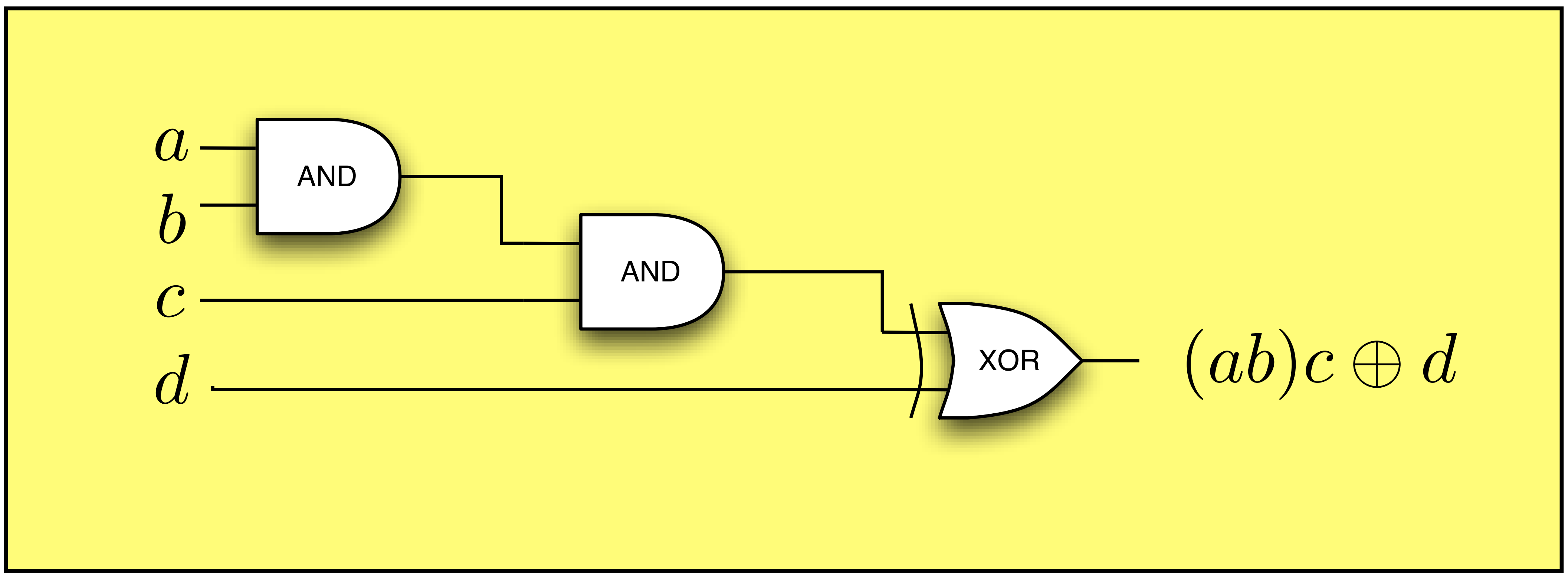
NOT



a	a⊕1
0	1
1	0

Boolean Functions



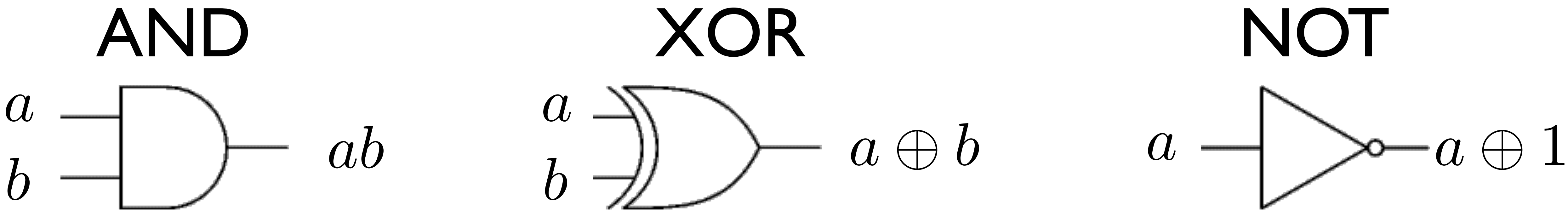


Any Boolean function can:

be composed as a network of **AND**, **XOR**, and **NOT**.

be written as a **polynomial** (mod 2).

Boolean Functions

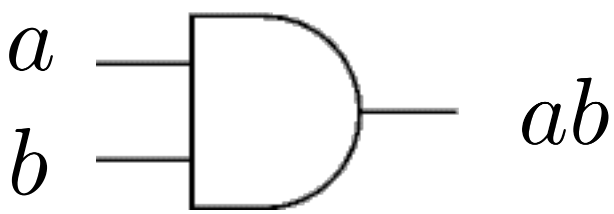


AND, **XOR**, and **NOT** are a **universal** set of logic gates.

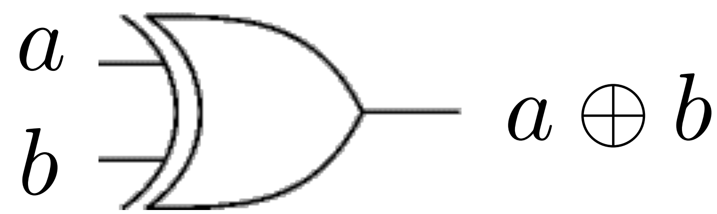
XOR, and **NOT** alone do not form a **universal** set.

Boolean Functions

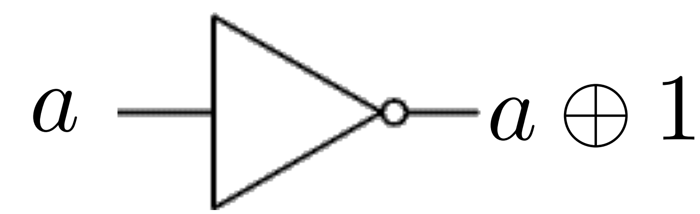
AND



XOR



NOT



AND, **XOR**, and **NOT** are a **universal** set of logic gates.

XOR, and **NOT** alone do not form a **universal** set.

Circuits of **XOR** and **NOT** alone can **only** express **linear functions.**

E.g.

$$f(a,b,c,d) = a \oplus b \oplus c \oplus 1$$

↑ very important for the rest of this talk!

Talk Outline

Correlations

↓

Correlations and Computation

↓

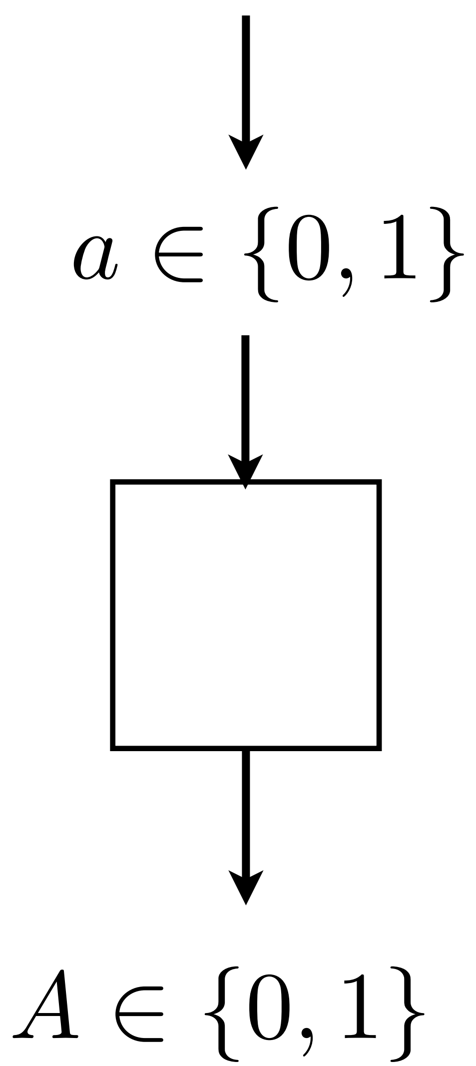
From Classical Correlations

↓

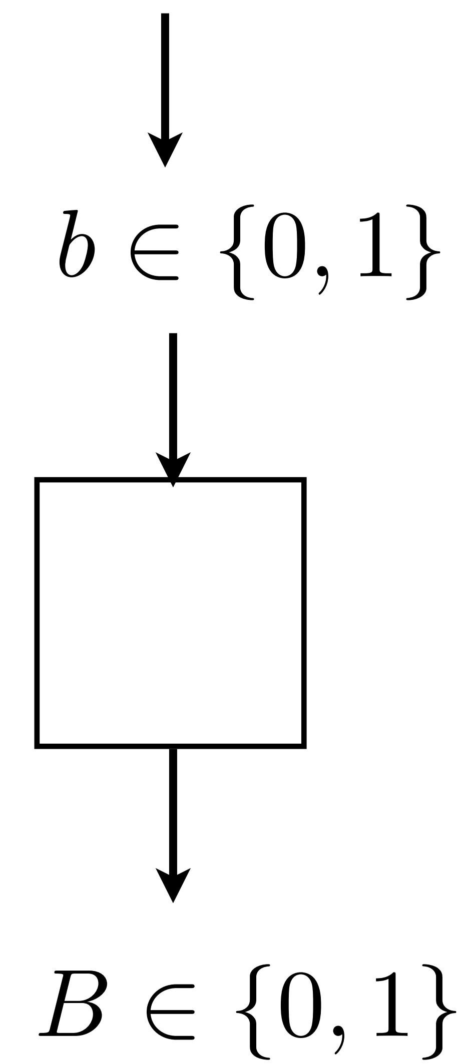
To Quantum Correlations

From correlations to computations

Alice



Bob



In this setup,
what set of **computations** are
possible in principle in:

Classical (local realistic) **Physics**

Quantum Physics

From correlations to computations

Alice

$a \in \{0,1\}$

$A \in \{0,1\}$

Bob

$b \in \{0,1\}$

$B \in \{0,1\}$

In this setup,
what set of **computations** are
possible in principle in:

Classical (local realistic) **Physics**

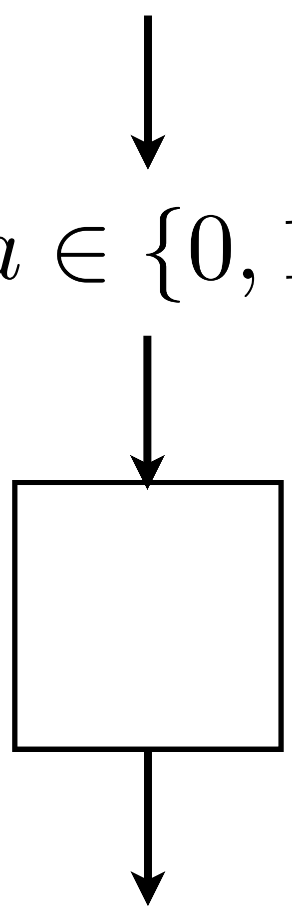
First task

Quantum Physics

From correlations to computations

Alice

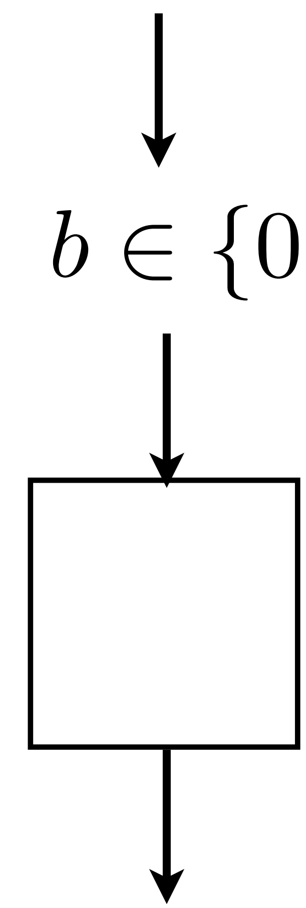
$a \in \{0,1\}$



$A \in \{0,1\}$

Bob

$b \in \{0,1\}$



$B \in \{0,1\}$

In this setup, Boolean Functions
what set of ~~**computations**~~ are
possible in principle in:

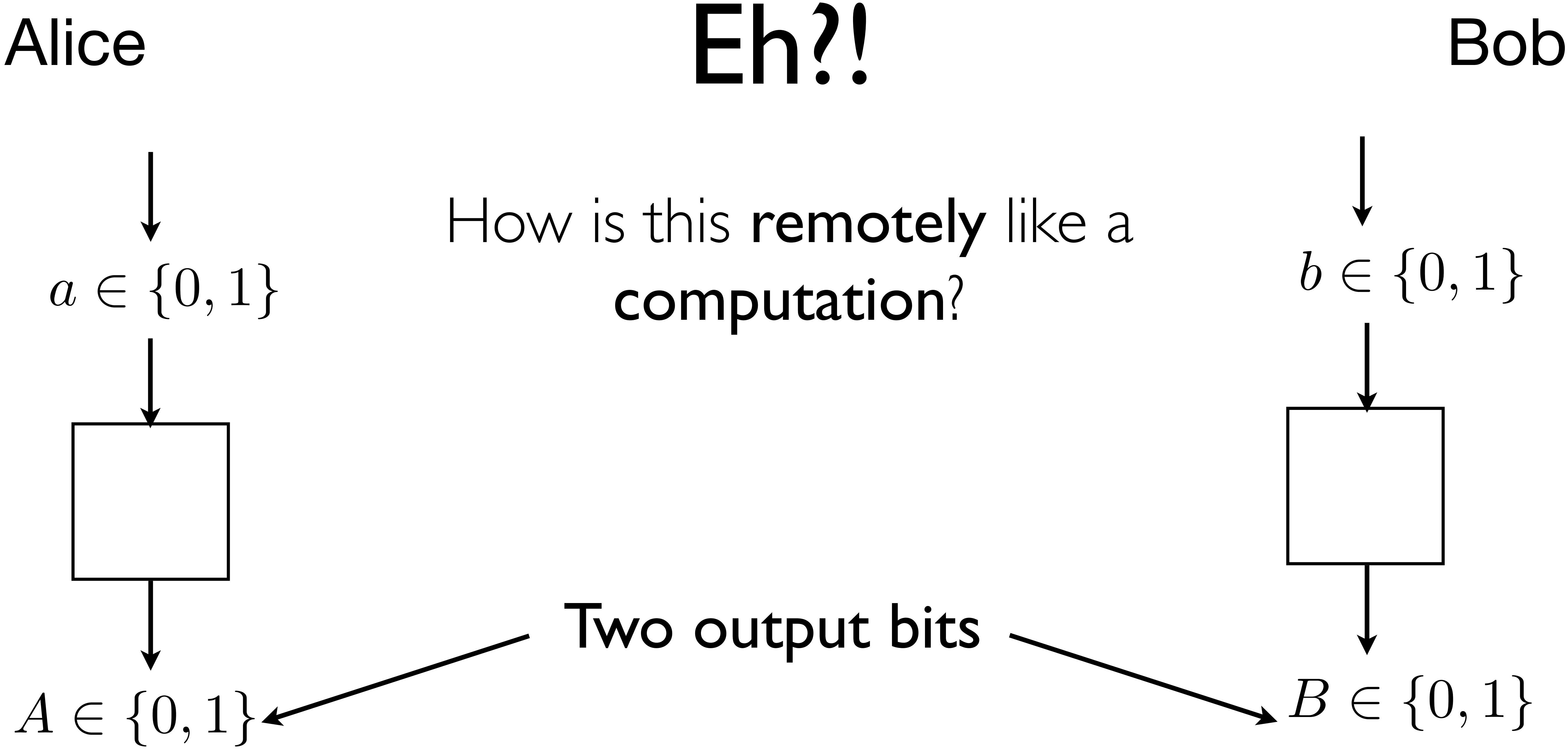
Classical (local realistic) **Physics**

First task

Quantum Physics

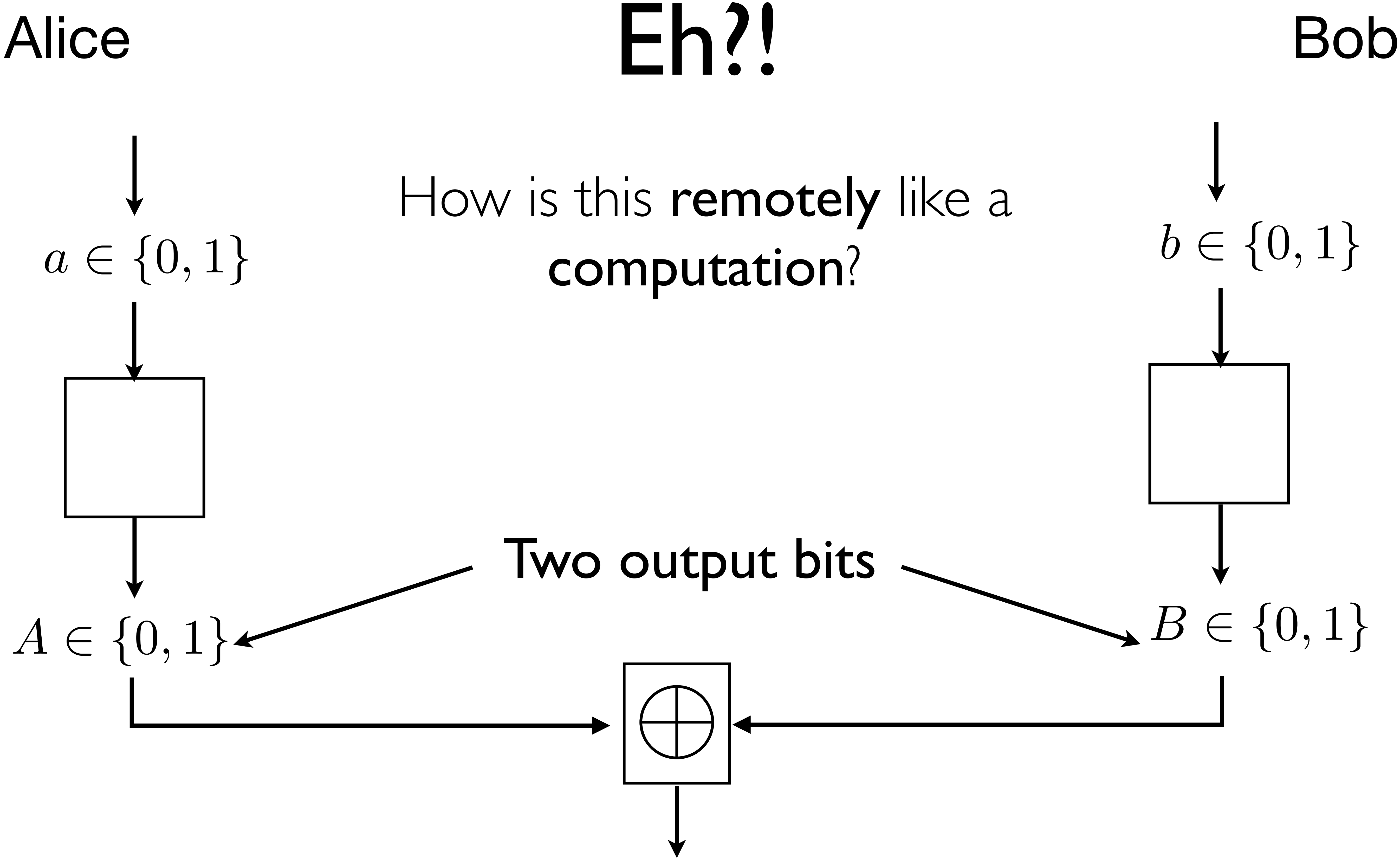
Eh?!

How is this **remotely** like a **computation**?



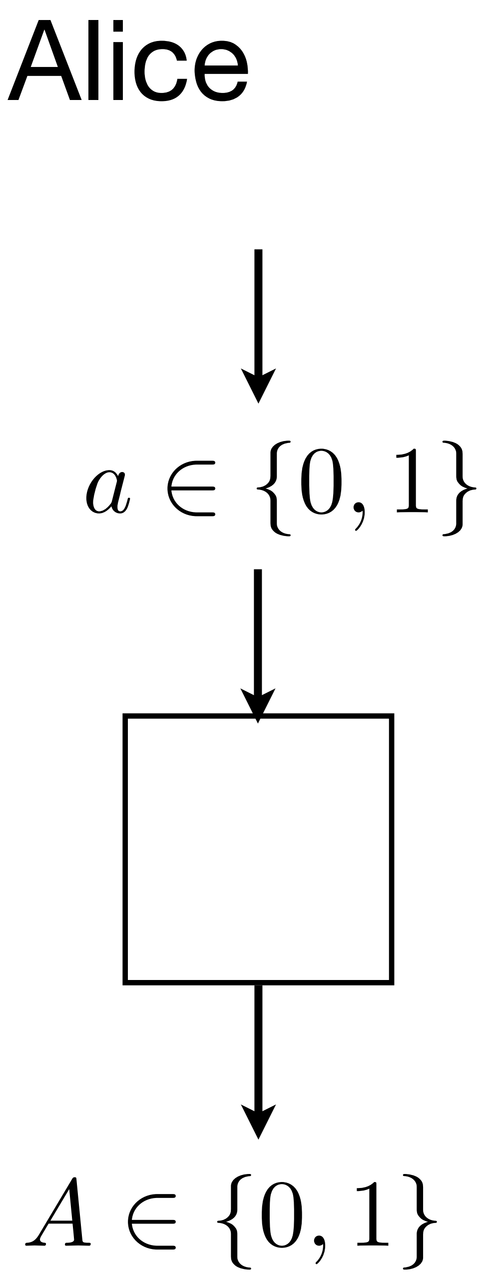
Eh?!

How is this **remotely** like a **computation**?



Add an **XOR** gate, and consider A⊕B to be the **output** of the computation.

The setup: recap

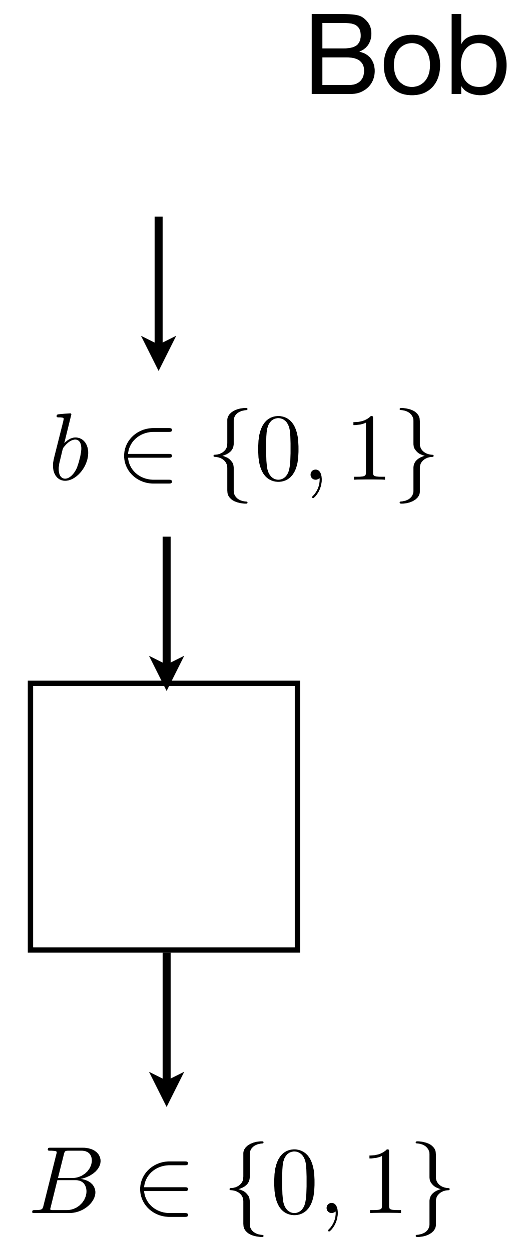


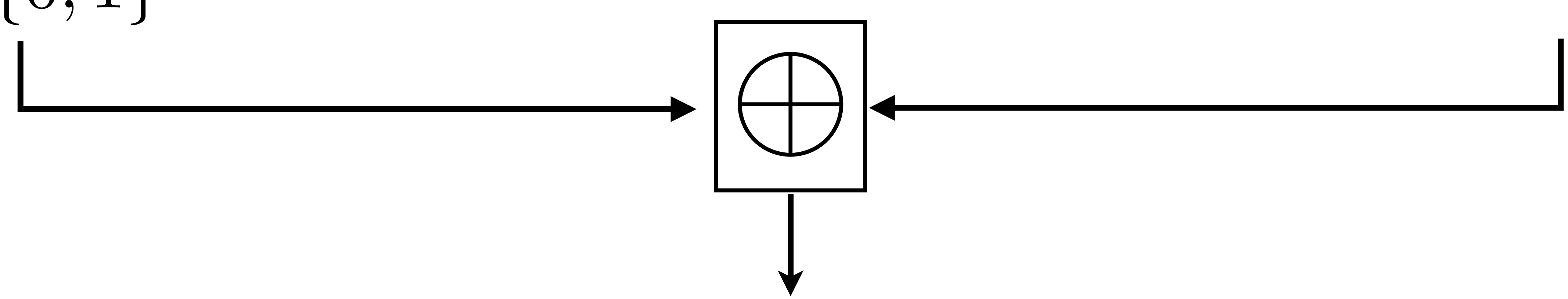
Space-like separated parties.

No advance warning of input.

Output is A⊕B.

Alice and Bob may share correlated bits, pre-agree an "algorithm".





Alice

The setup: recap

Bob

$a \in \{0,1\}$

$b \in \{0,1\}$

Space-like separated parties.

No advance warning of input.

Output is A⊕B.

Alice and Bob may share correlated bits, pre-agree an "algorithm".

$A \in \{0,1\}$

$B \in \{0,1\}$

$\oplus$

What Boolean functions are achievable **in principle** in classical physics?

Alice

What Boolean functions are achievable **in principle** given classical physics?

Bob

$a \in \{0, 1\}$

Space-like separated parties.

No advance warning of input.

Output is A⊕B.

Alice and Bob may share correlated bits, pre-agree an “algorithm”.

$b \in \{0, 1\}$

$A \in \{0, 1\}$

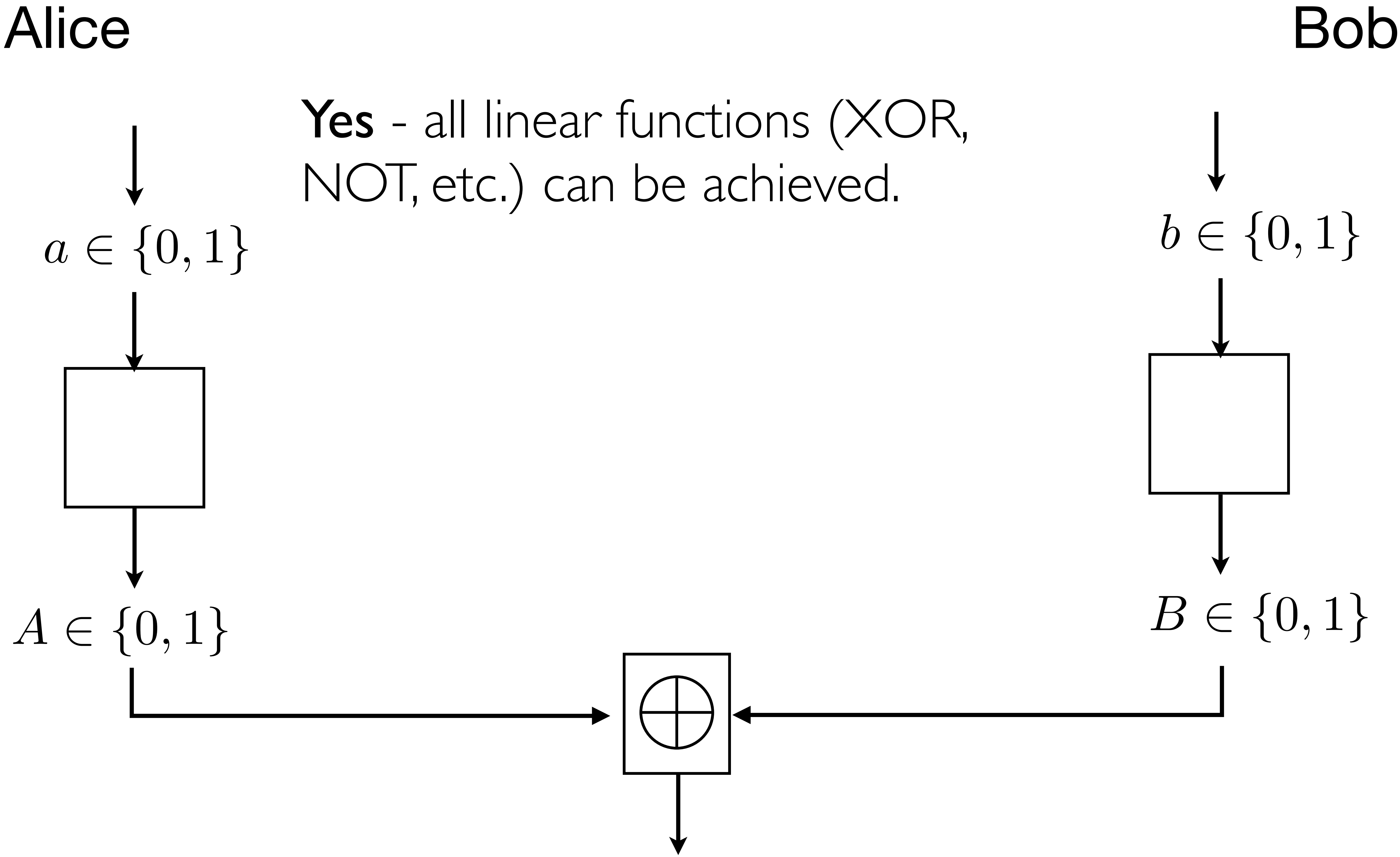
$B \in \{0, 1\}$

$\oplus$

Ideas?

From correlation to computation

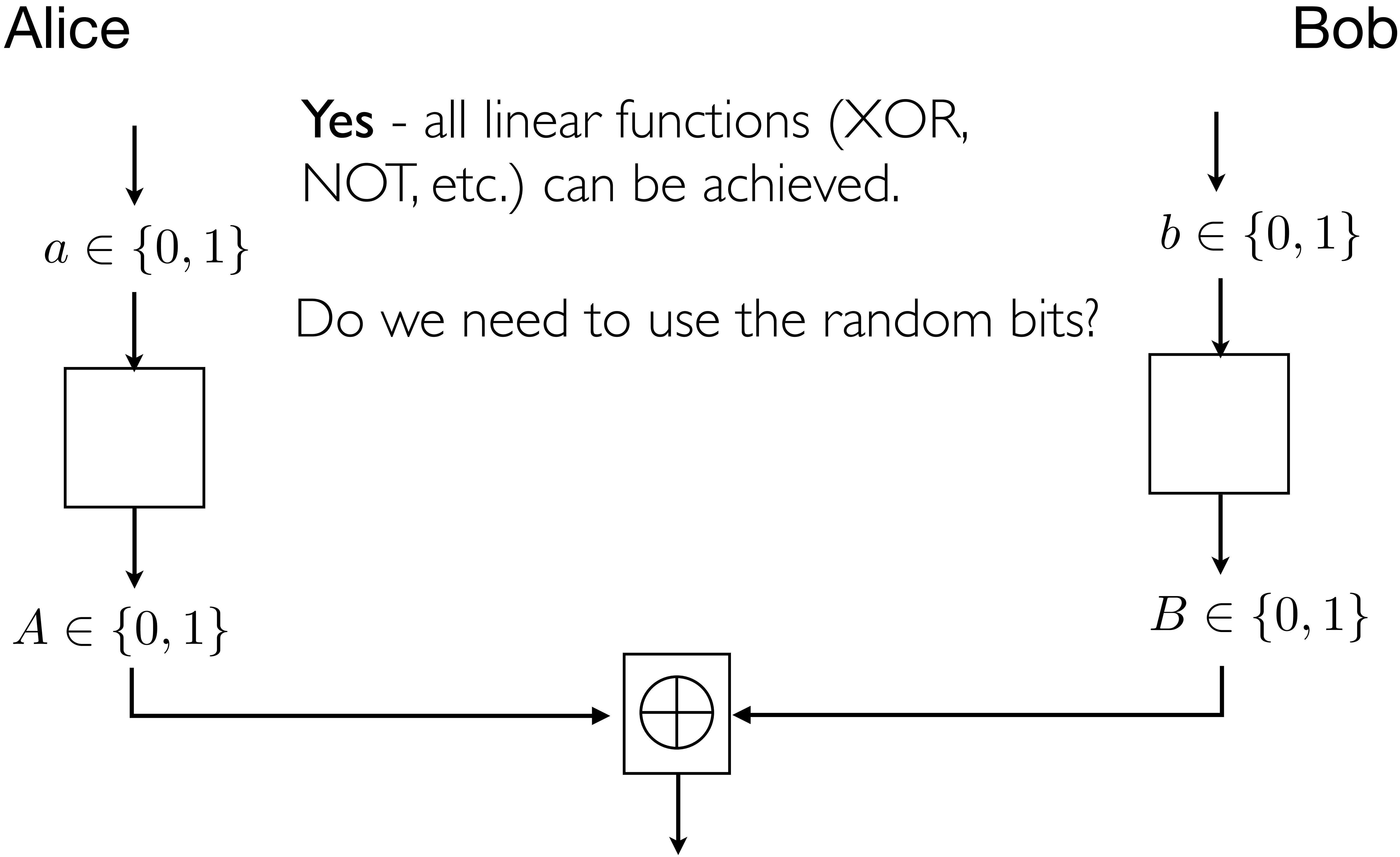
Yes - all linear functions (XOR, NOT, etc.) can be achieved.



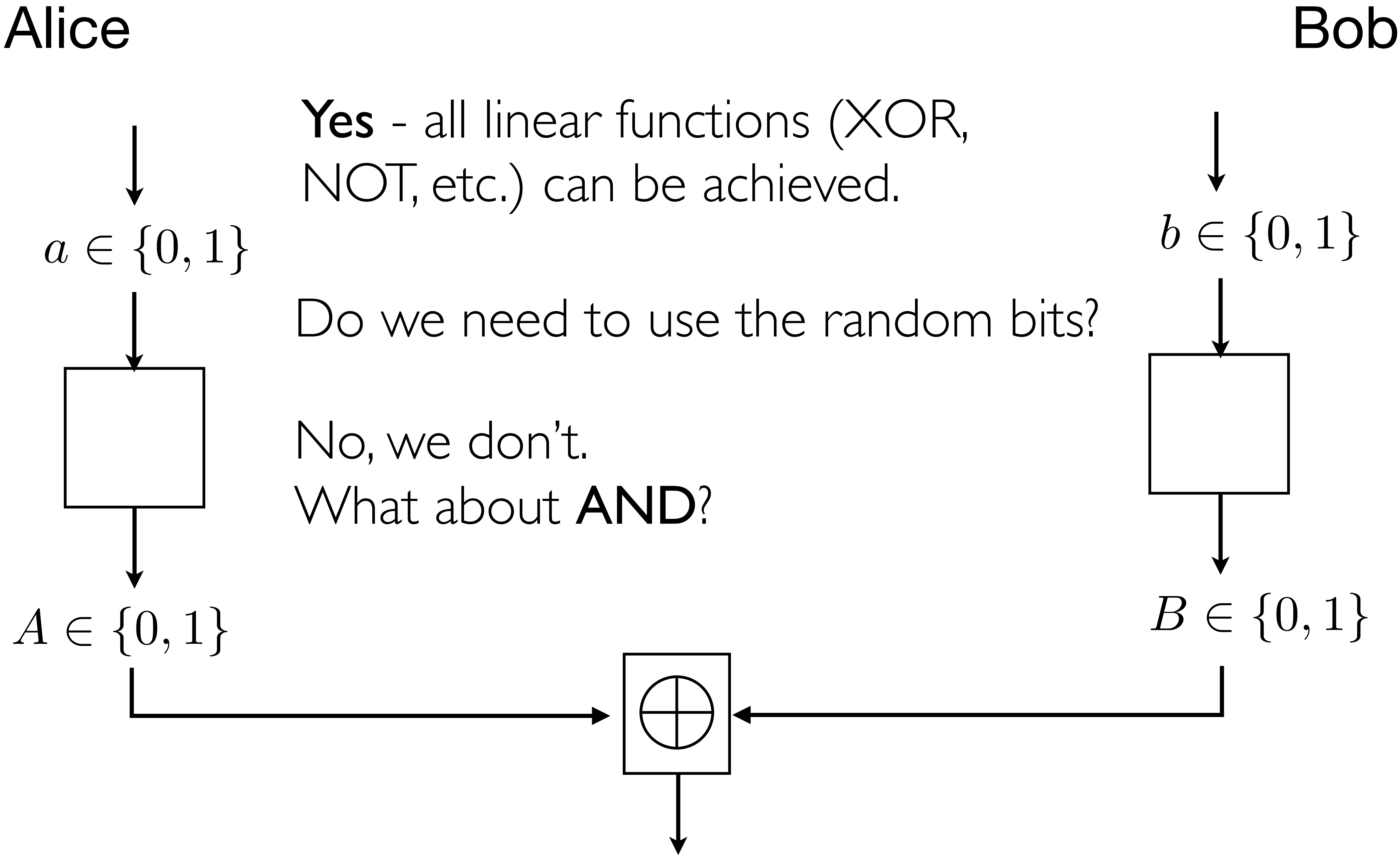
From correlation to computation

Yes - all linear functions (XOR, NOT, etc.) can be achieved.

Do we need to use the random bits?



From correlation to computation



Yes - all linear functions (XOR, NOT, etc.) can be achieved.

Do we need to use the random bits?

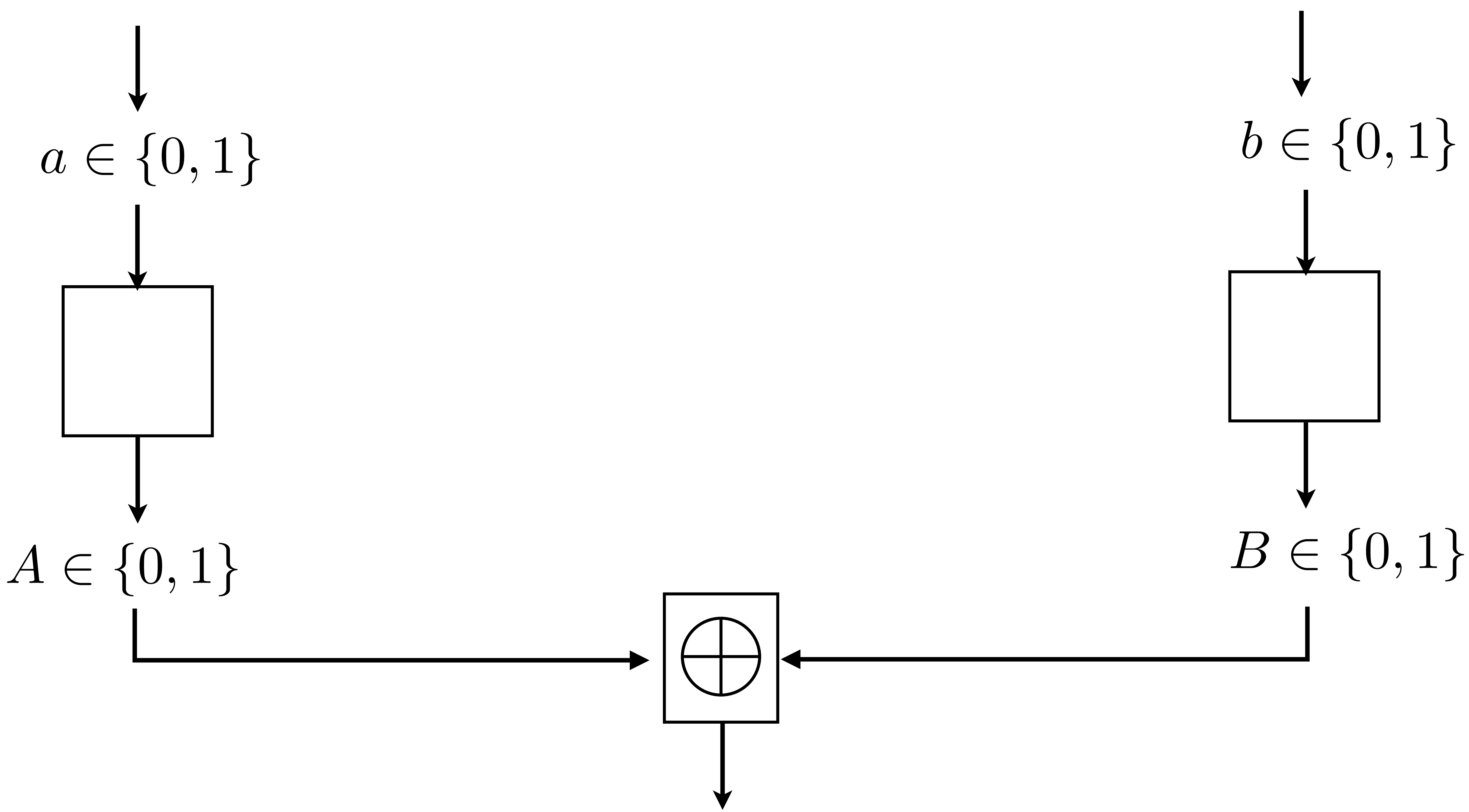
No, we don't.
What about **AND**?

From correlation to computation

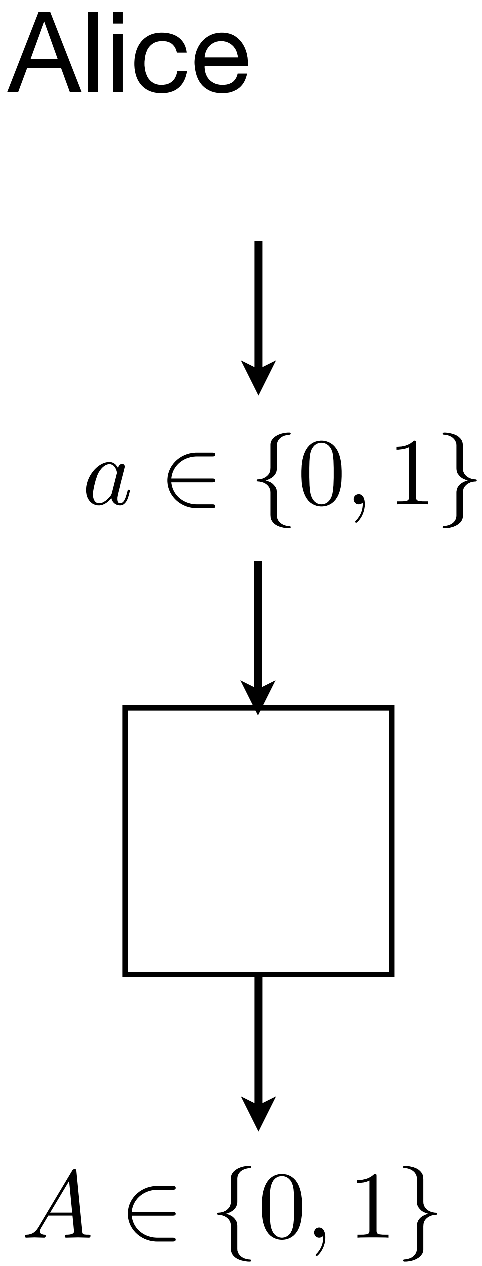
Alice

Bob

AND is **impossible** to achieve.



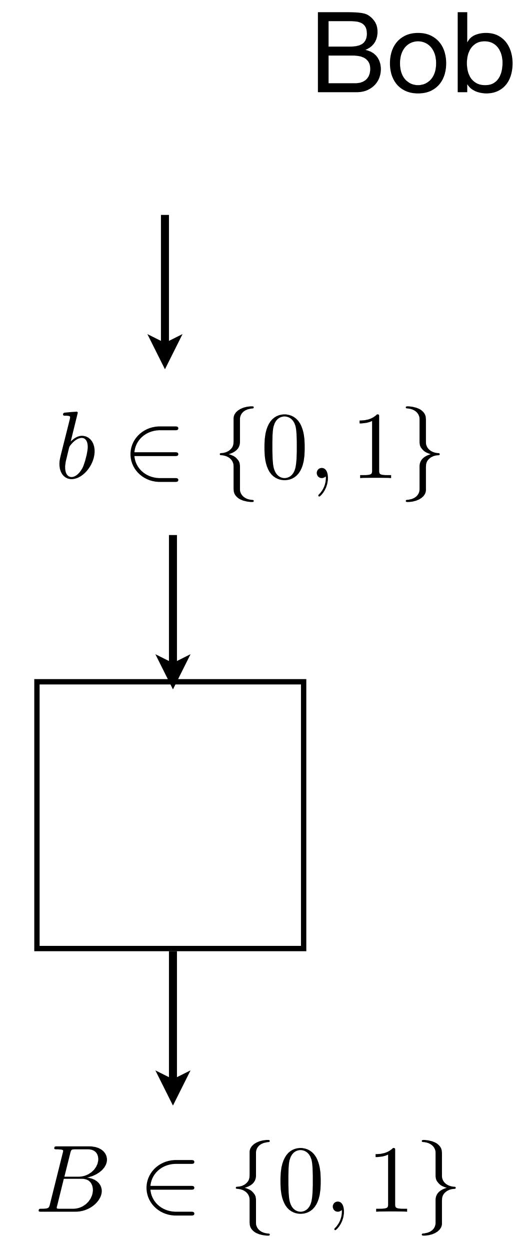
From correlation to computation

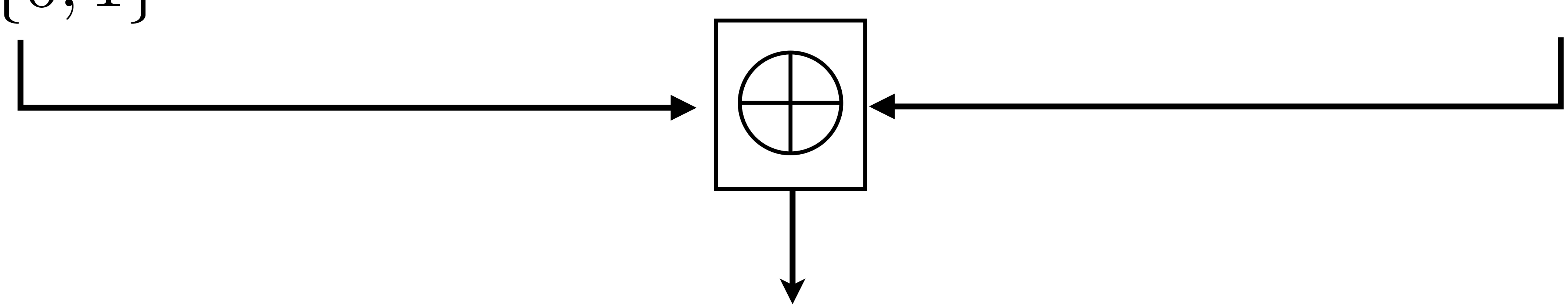


AND is **impossible** to achieve.

We can prove that:

With this set up, in **any** locally realistic theory, the **linear functions** are the only Boolean functions deterministically achievable.





From correlation to computation

Alice

Bob

$a \in \{0, 1\}$

$b \in \{0, 1\}$

$A \in \{0, 1\}$

$B \in \{0, 1\}$

$\oplus$

AND is **impossible** to achieve.

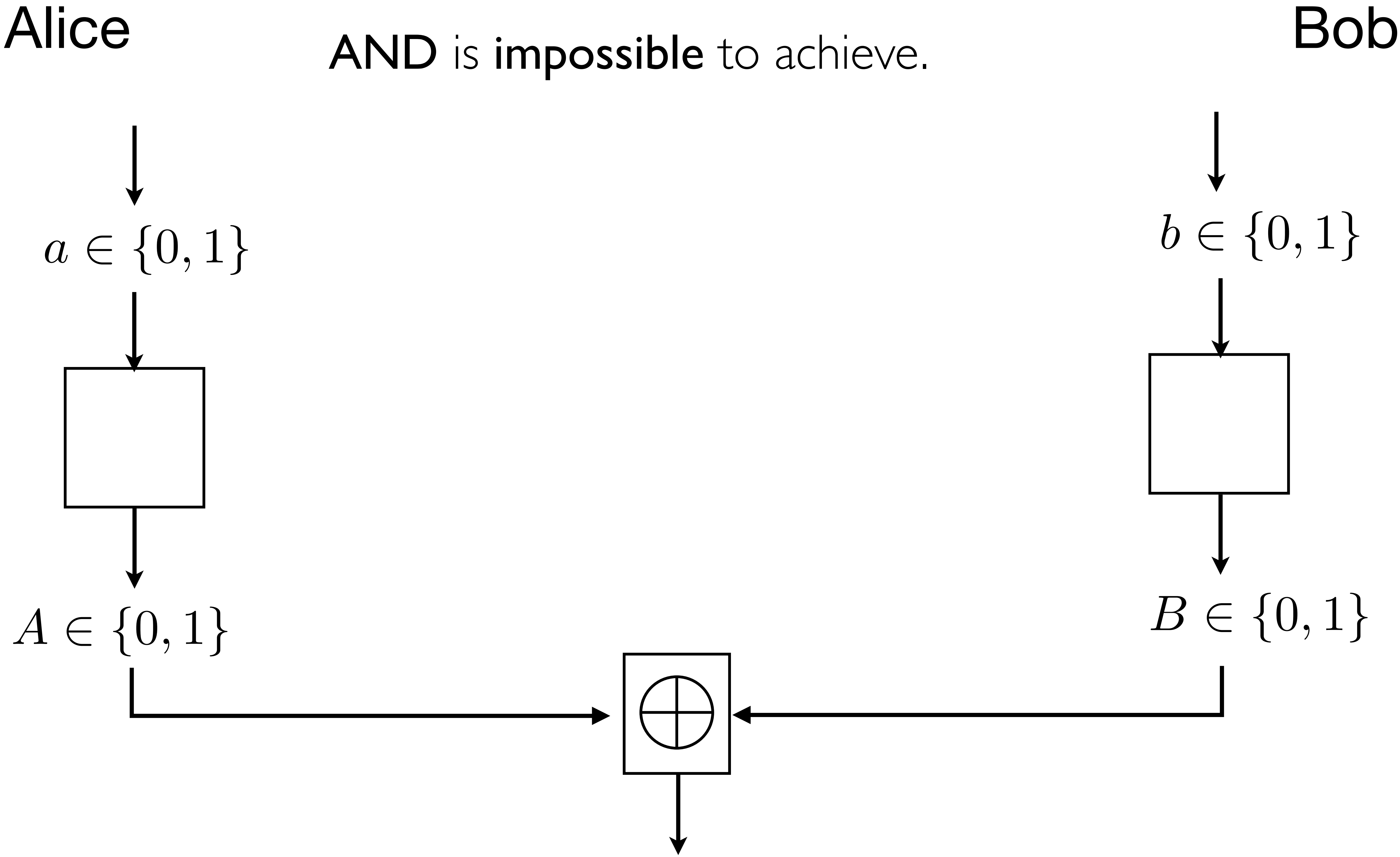
We can prove that:

With this set up, in **any** locally realistic theory, the **linear functions** are the only Boolean functions deterministically achievable.

contains the Bell inequalities

From correlation to computation

AND is **impossible** to achieve.

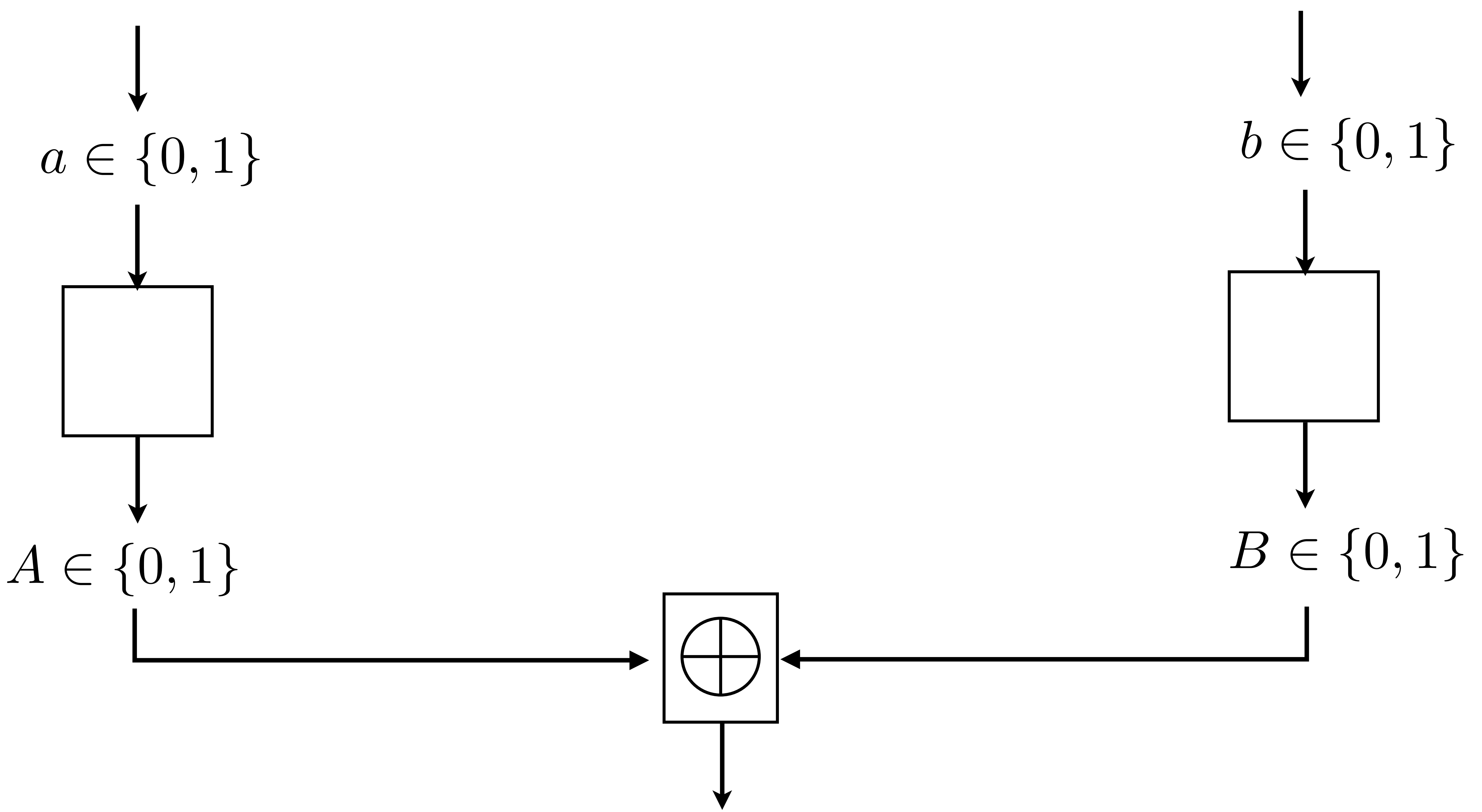


From correlation to computation

Alice

AND is **impossible** to achieve **deterministically**.

Bob



From correlation to computation

Alice

Bob

AND is **impossible** to achieve **deterministically**.

Let's allow it to sometimes fail.

$a \in \{0,1\}$

$b \in \{0,1\}$

Assume **a** and **b** are **fair coins**.
i.e. 50% chance 0 or 1.

New task:

Find the **highest probability** (on average) to achieve **AND**, i.e. that **A⊕B=ab**.

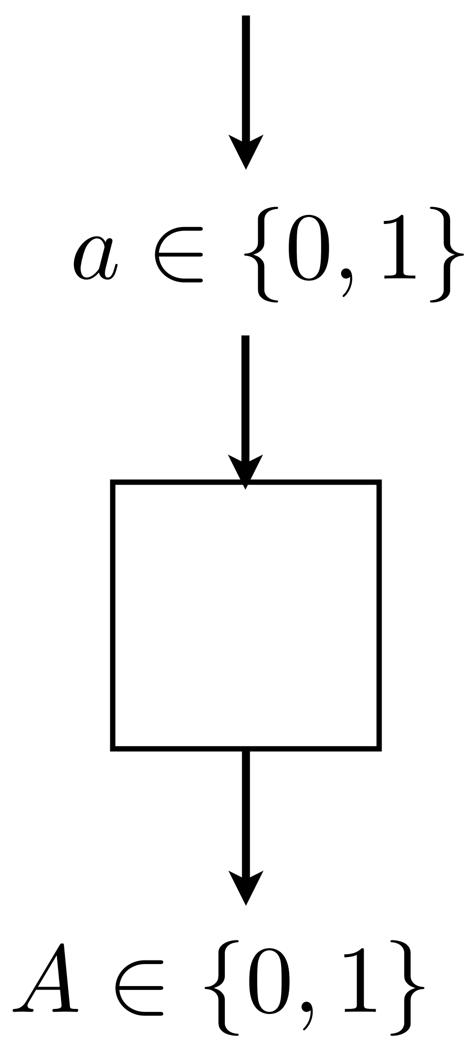
$A \in \{0,1\}$

$B \in \{0,1\}$

$\oplus$

From correlation to computation

Alice



Example

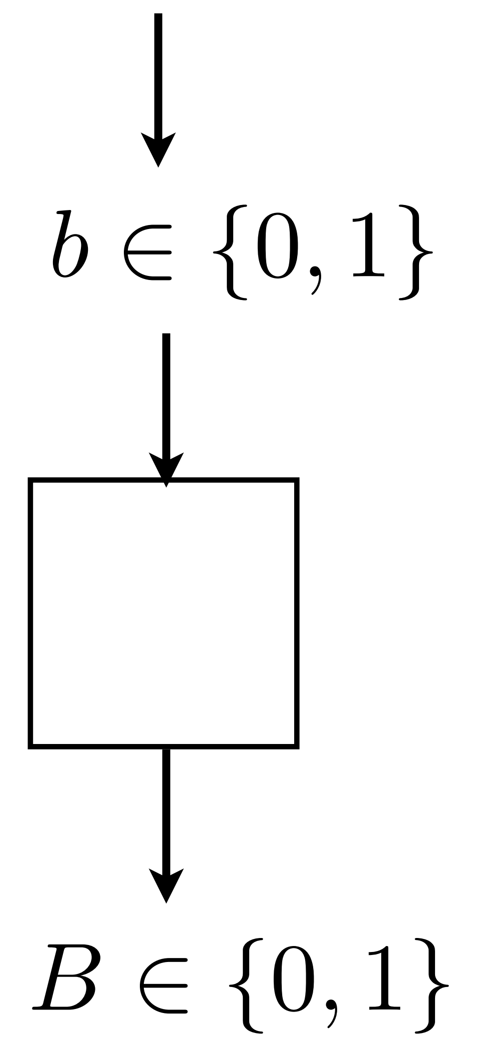
The simplest strategy - "always output 0" will be correct on average **75%** of the time.

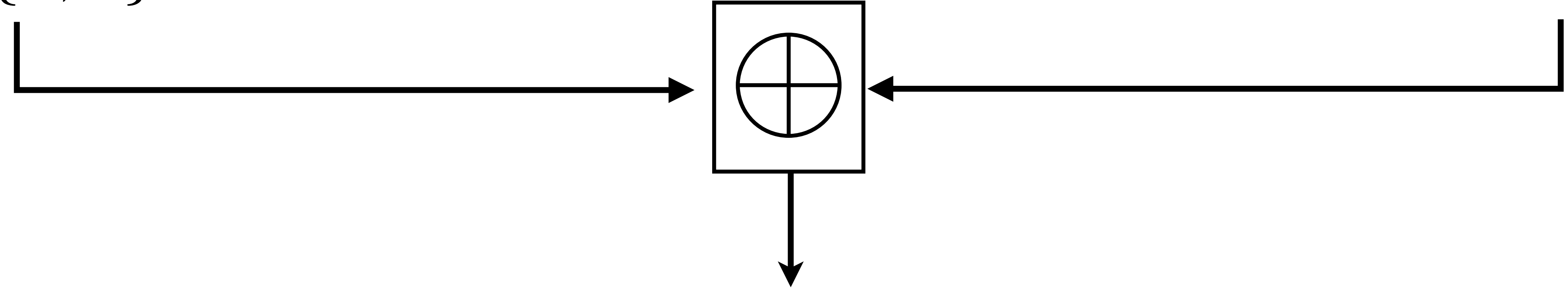
a	b	a b	0
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	0

AND

0

Bob





From correlation to computation

Alice

Bob

Can **75**% be beaten?

$a \in \{0,1\}$

$b \in \{0,1\}$

No - we can show that **every possible strategy** (with or without correlations) based on **local realistic** physics satisfies:

$$Prob(A \oplus B = ab) \leq 0.75$$

A Bell inequality

$A \in \{0,1\}$

$B \in \{0,1\}$

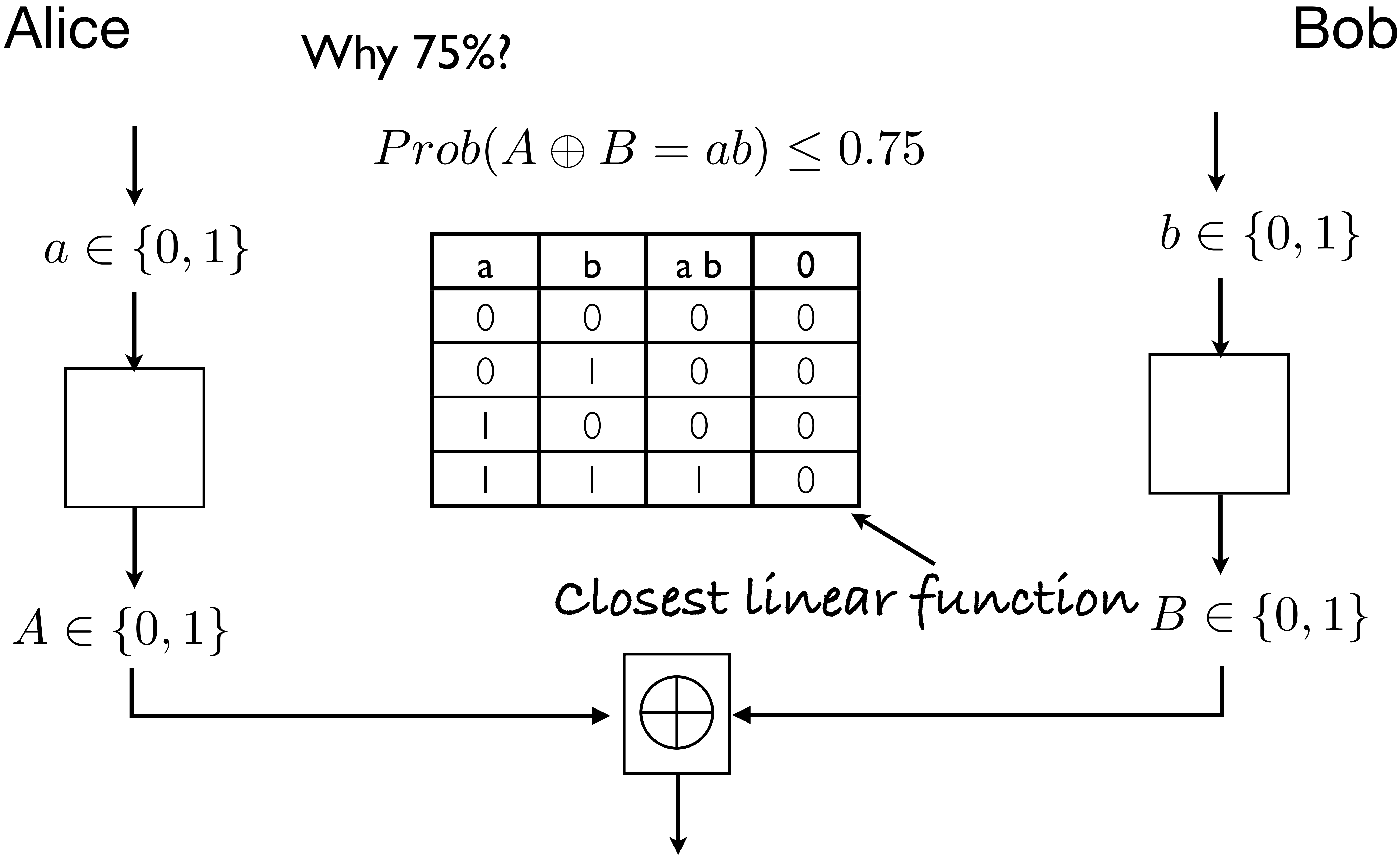
From correlation to computation

Why 75%?

$$Prob(A \oplus B = ab) \leq 0.75$$

a	b	a b	0
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	0

Closest linear function



Talk Outline

Correlations

↓

Correlations and Computation

↓

From Classical Correlations

↓

To Quantum Correlations

Qubits

bits $\longrightarrow$ **qubits**

$101101\ldots$ $\quad\quad$ $\alpha|101101\ldots\rangle + \beta|001001\ldots\rangle + \cdots$

Complex weighted superposition

The prototypical qubit **- the spin 1/2**

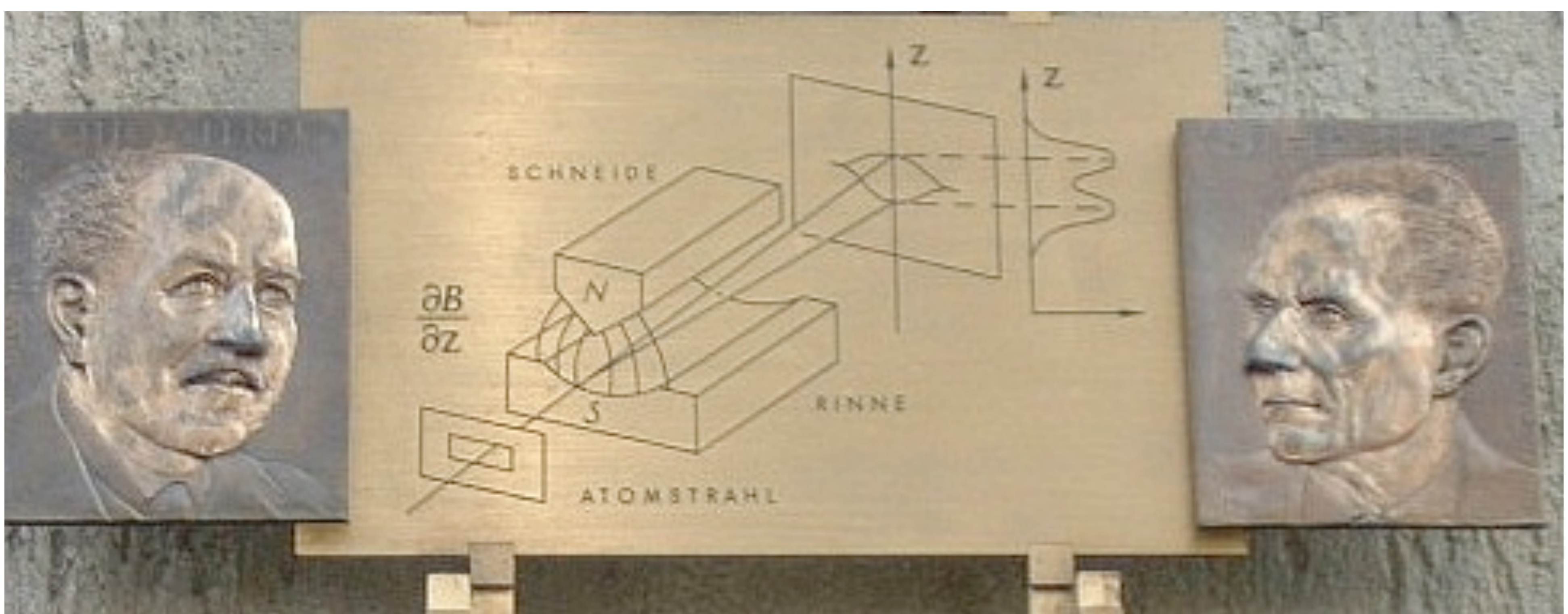
$$|0\rangle = |\uparrow\rangle \qquad |1\rangle = |\downarrow\rangle$$

Qubit measurements

- Key observables: **Pauli operators** (σx, σy, σz)

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- E.g. Stern-Gerlach measurements



Many qubits

- Superposition principle + multiple systems
  $\rightarrow$ **entangled states**:

$$|\psi\rangle = \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$$ Not entangled

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$ Entangled

Many qubits

- Superposition principle + multiple systems
  $\rightarrow$ **entangled states**:

$$|\psi\rangle = \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$$ Not entangled

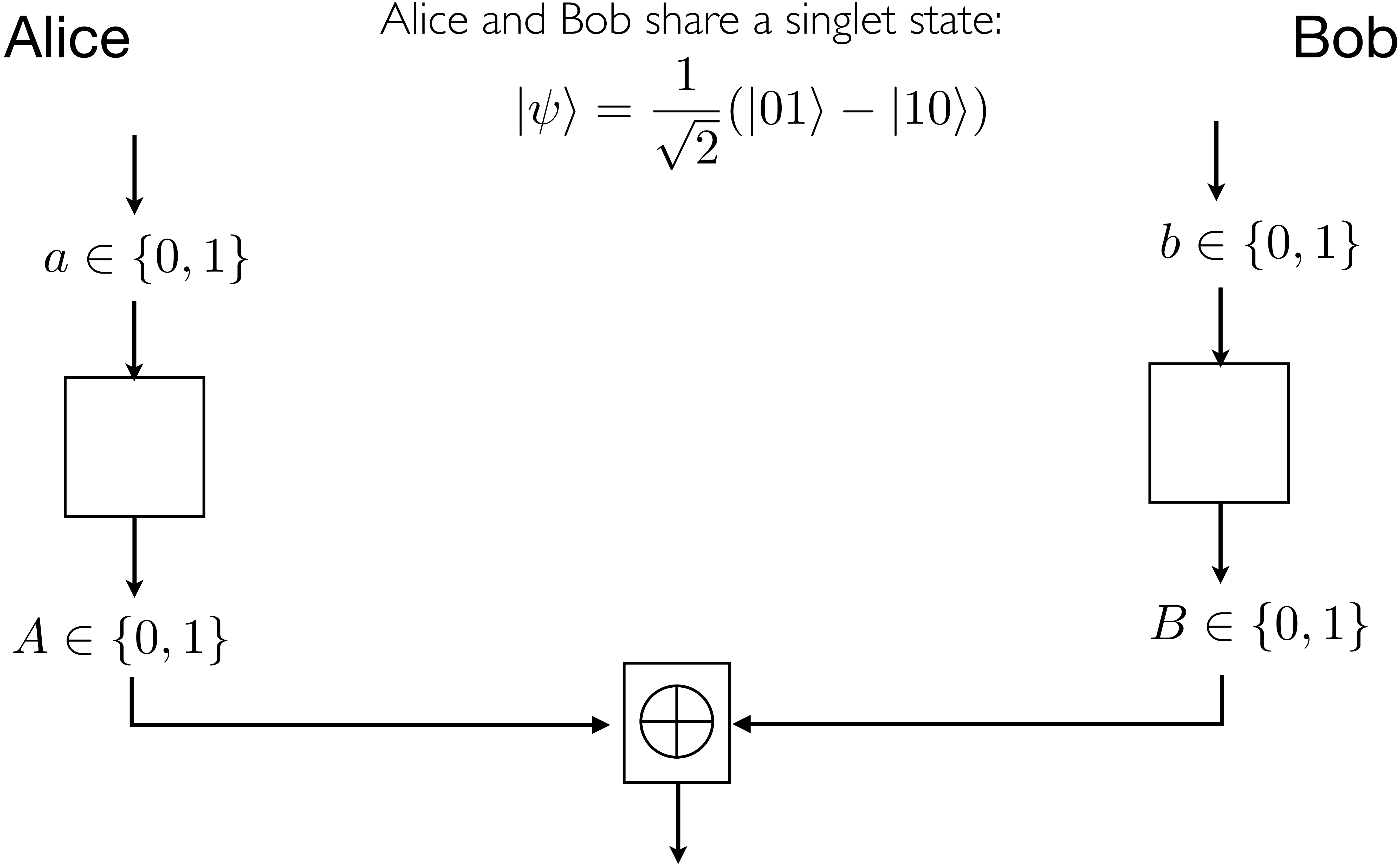
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$ Entangled

Can violate Bell inequalities...

How to violate a Bell Inequality

Alice and Bob share a singlet state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

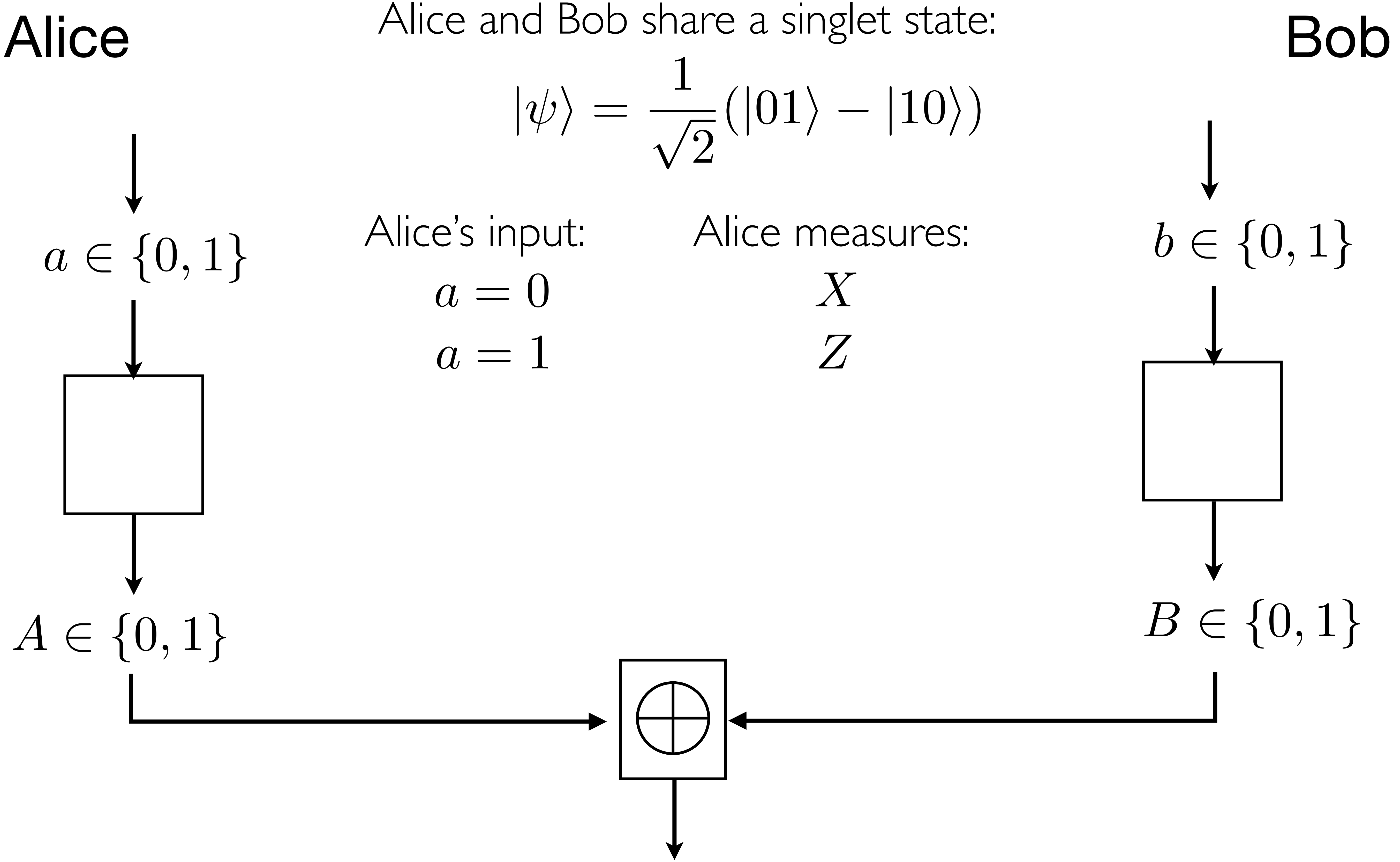


How to violate a Bell Inequality

Alice and Bob share a singlet state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Alice's input:	Alice measures:
$a = 0$	X
$a = 1$	Z



How to violate a Bell Inequality

Alice

Bob

Alice and Bob share a singlet state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$a \in \{0, 1\}$

$b \in \{0, 1\}$

Alice's input:	Alice measures:
$a = 0$	X
$a = 1$	Z

Bob's input:	Bob measures:
$b = 0$	$(-X - Z)/\sqrt{2}$
$b = 1$	$(Z - X)/\sqrt{2}$

$A \in \{0, 1\}$

$B \in \{0, 1\}$

$\oplus$

How to violate a Bell Inequality

Alice

Bob

Alice and Bob share a singlet state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$a \in \{0,1\}$

$b \in \{0,1\}$

Alice's input:	Alice measures:
$a = 0$	X
$a = 1$	Z

Bob's input:	Bob measures:
$b = 0$	$(-X - Z)/\sqrt{2}$
$b = 1$	$(Z - X)/\sqrt{2}$

$A \in \{0,1\}$

$B \in \{0,1\}$

Convert +1/-1 to 0/1.

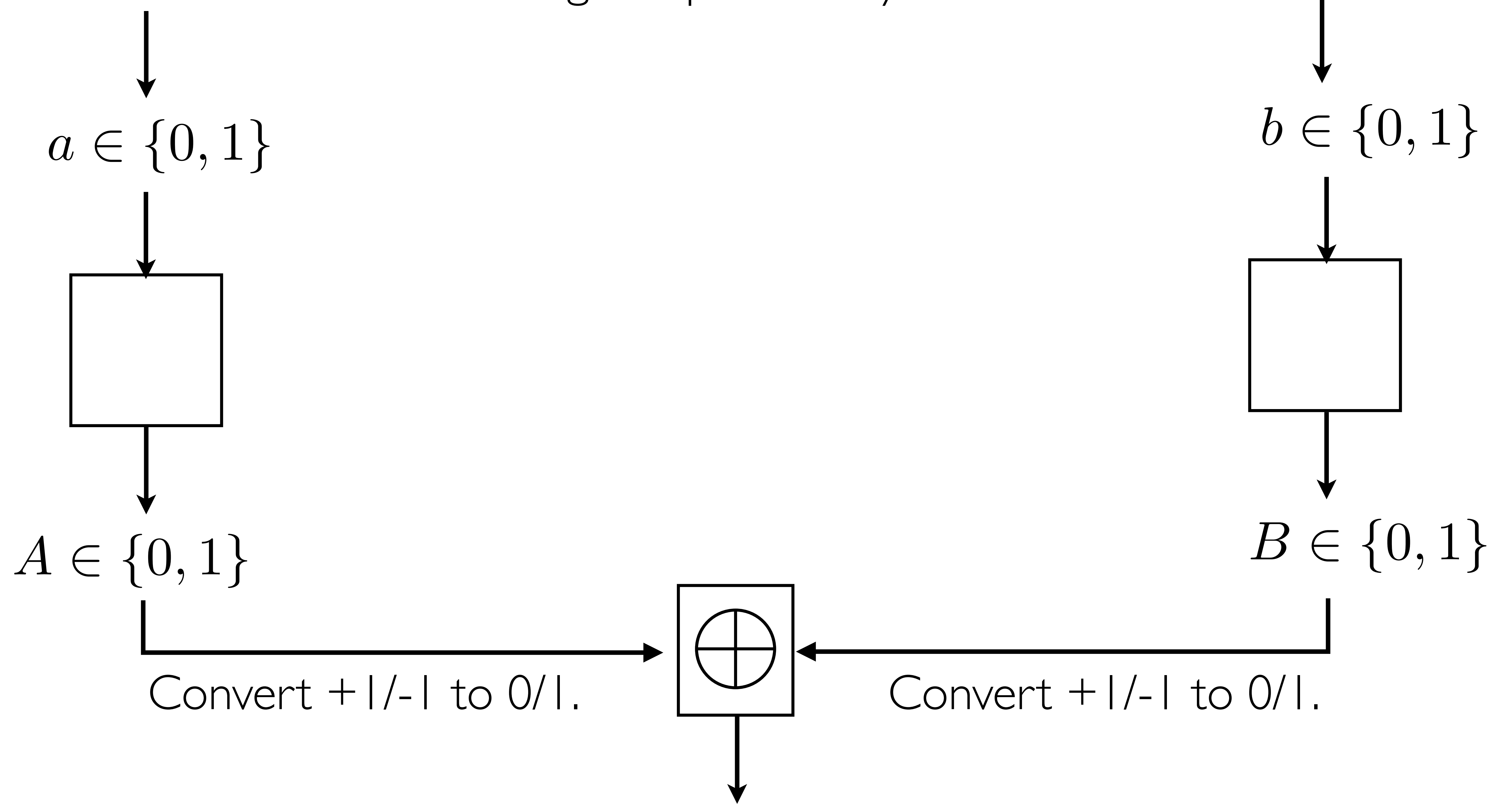
$\oplus$

Convert +1/-1 to 0/1.

Violating the Bell Inequality

Alice Bob

Calculating the probability, we find..

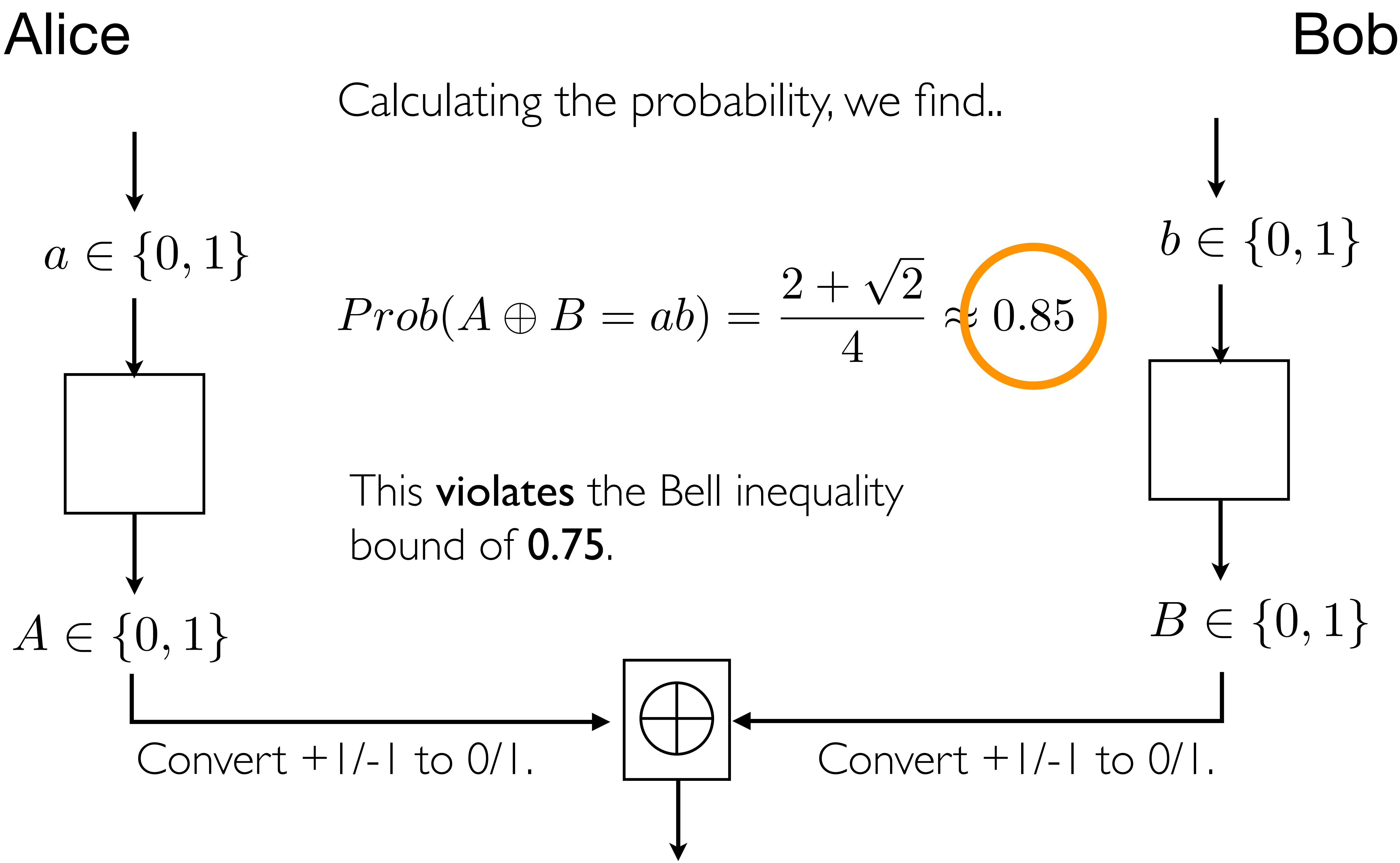


Violating the Bell Inequality

Calculating the probability, we find..

$$Prob(A \oplus B = ab) = \frac{2+\sqrt{2}}{4} \approx 0.85$$

This **violates** the Bell inequality bound of **0.75**.



Are quantum correlations useful for computation?

The results so far...

- For all local realistic theories:

$$Prob(A \oplus B = ab) \leq 0.75$$

equivalent to orig. Bell ineq.

- For quantum mechanics, we demonstrated

$$Prob(A \oplus B = ab) = \frac{2+\sqrt{2}}{4} \approx 0.85$$

provable upper bound

Talk Outline

Correlations

↓

Correlations and Computation

↓

From Classical Correlations

↓

To Quantum Correlations

Talk Outline

Correlations

↓

Correlations and Computation

↓

From Classical Correlations

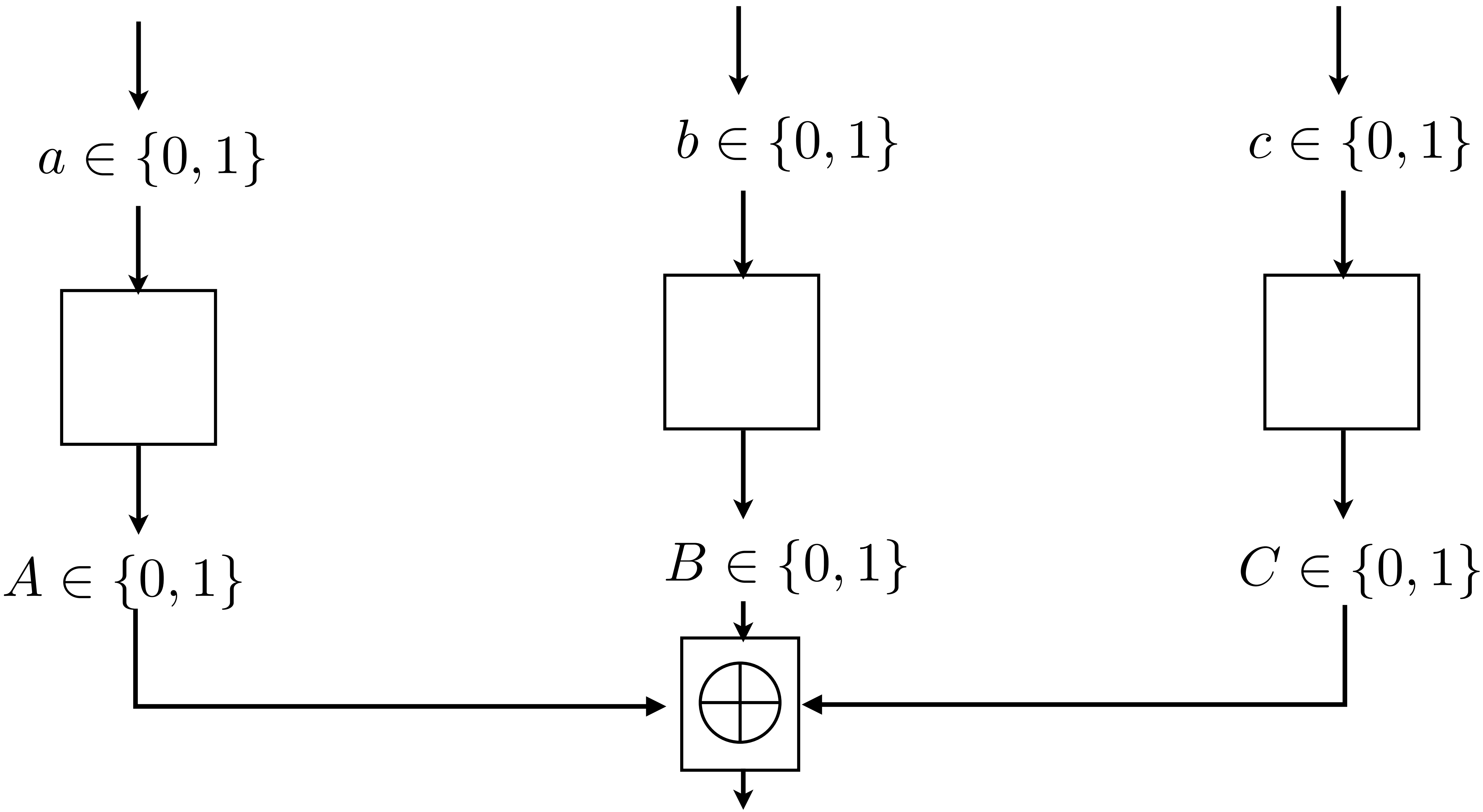
↓

To Quantum Correlations

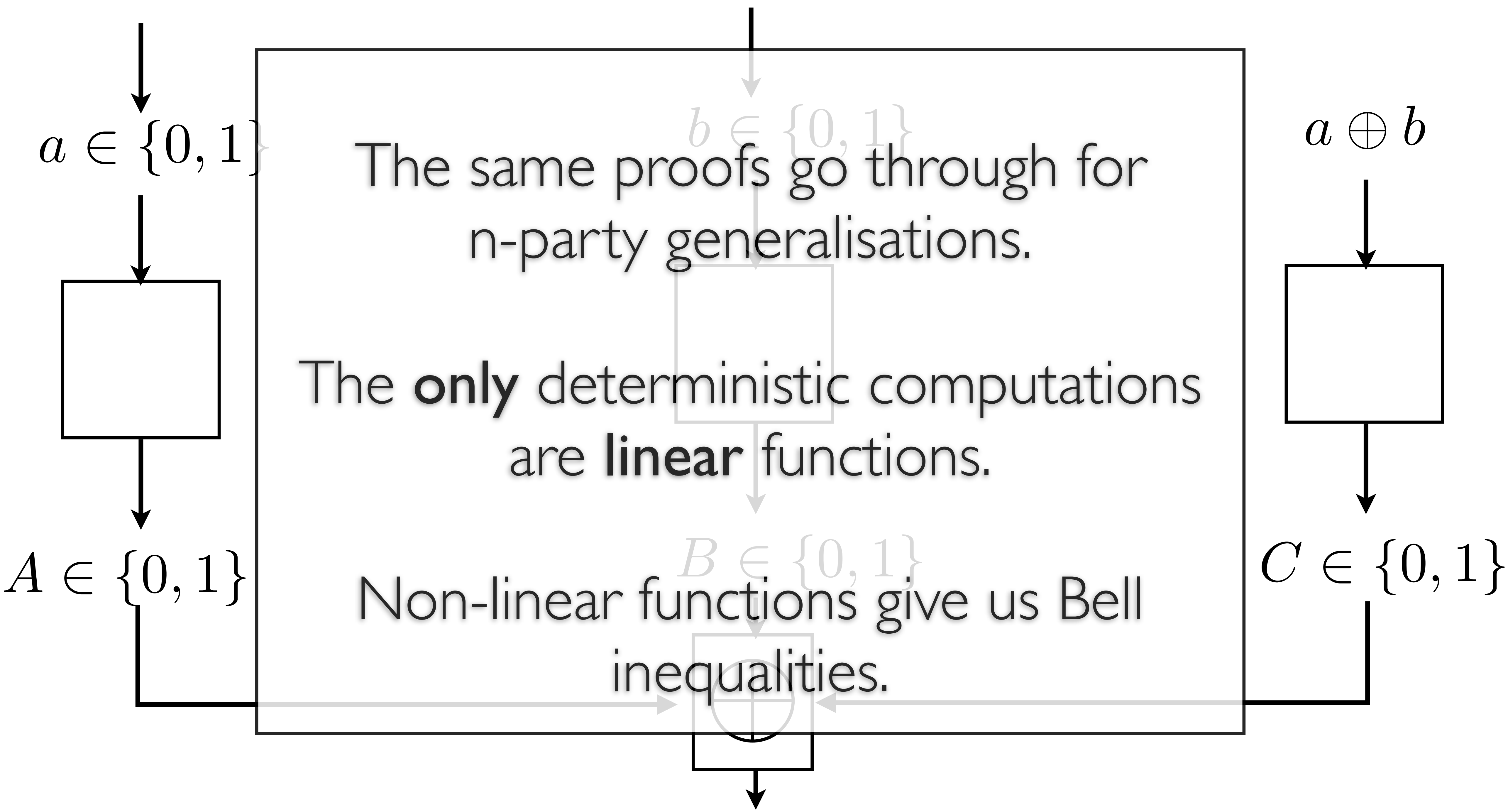
↓

From two to many...

Two to Three



Two to Three

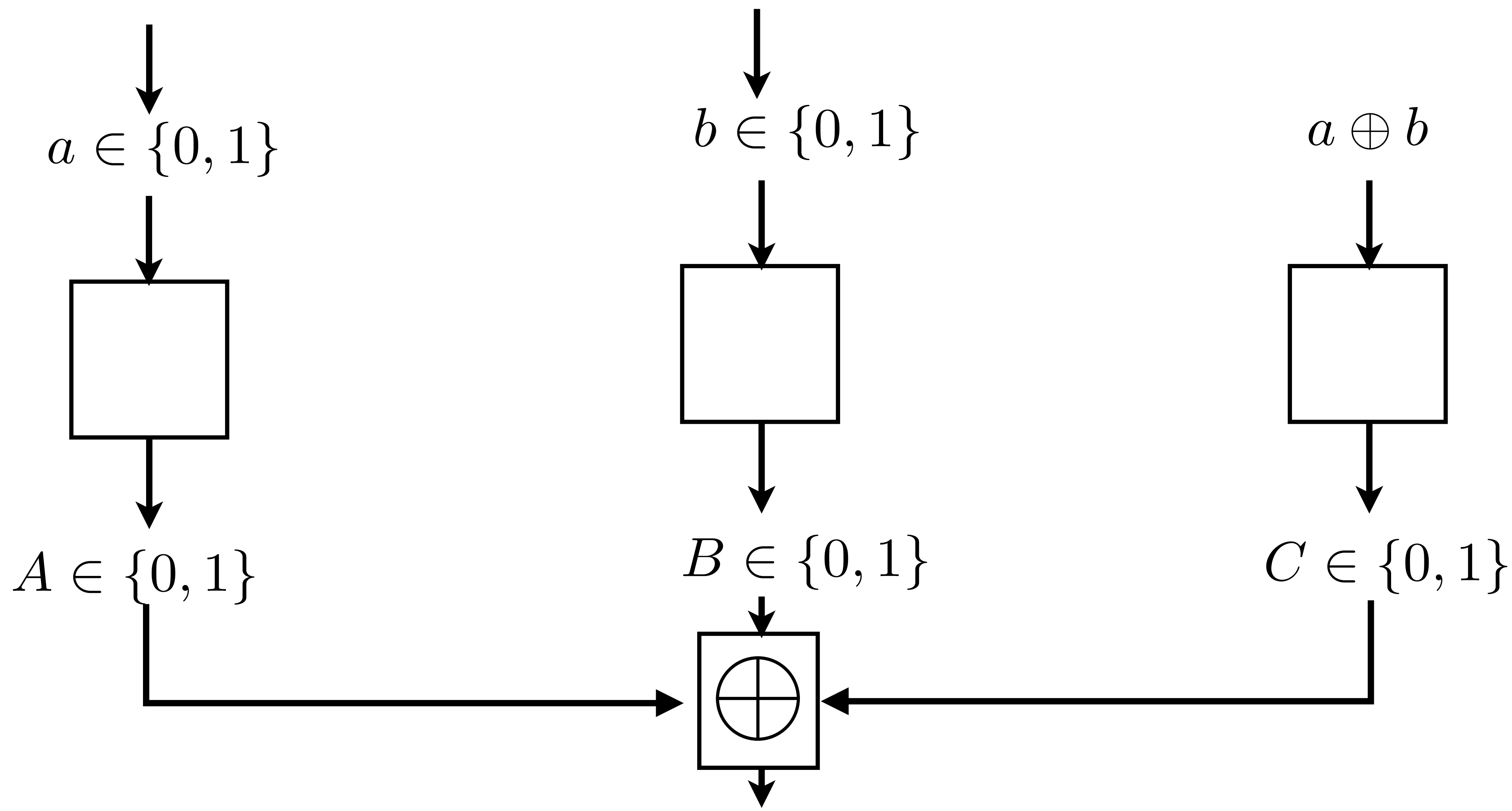


The same proofs go through for n-party generalisations.

The **only** deterministic computations are **linear** functions.

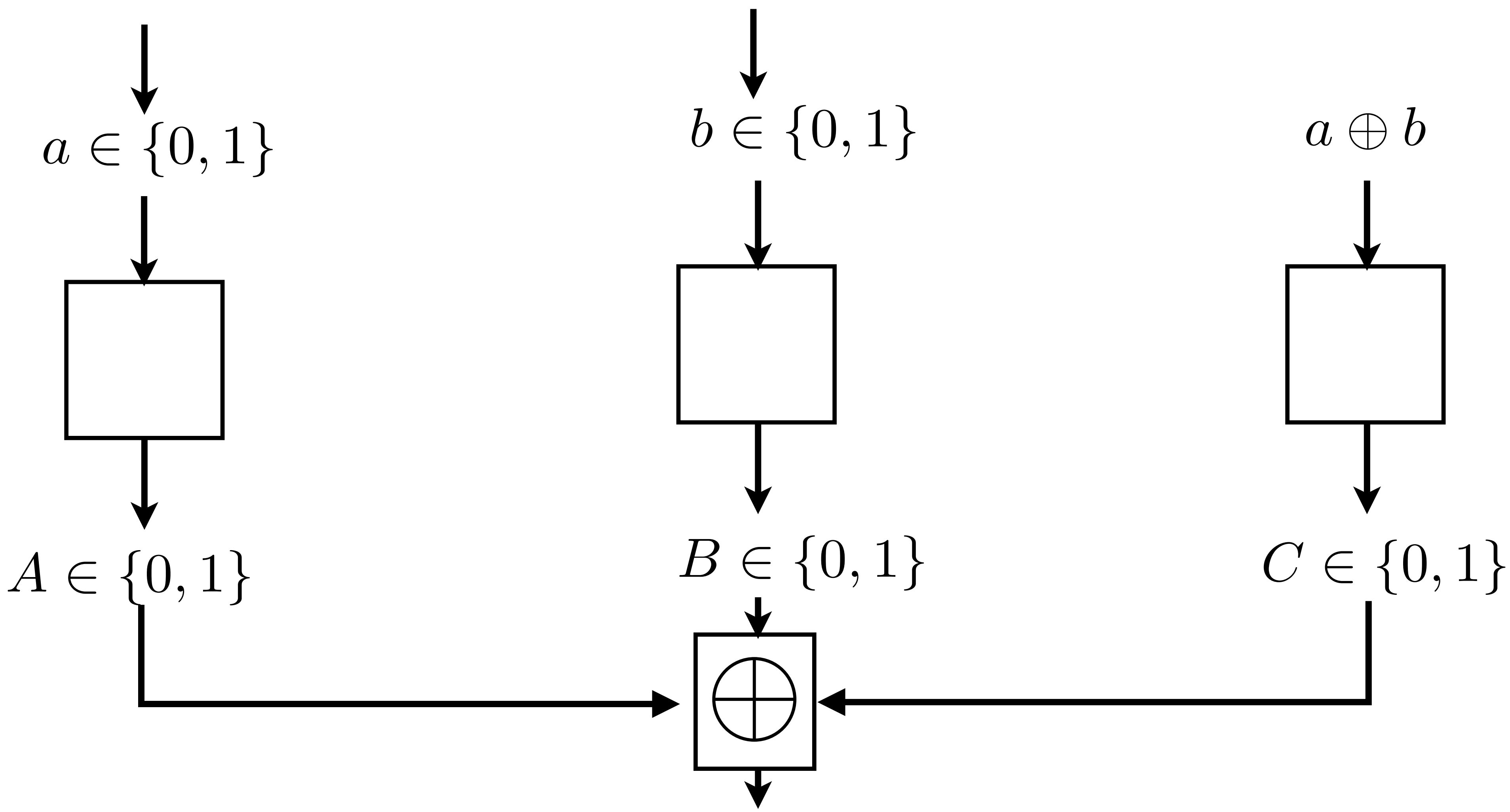
Non-linear functions give us Bell inequalities.

Two to Three



GHZ State: $(1/\sqrt{2})(|000\rangle + |111\rangle)$

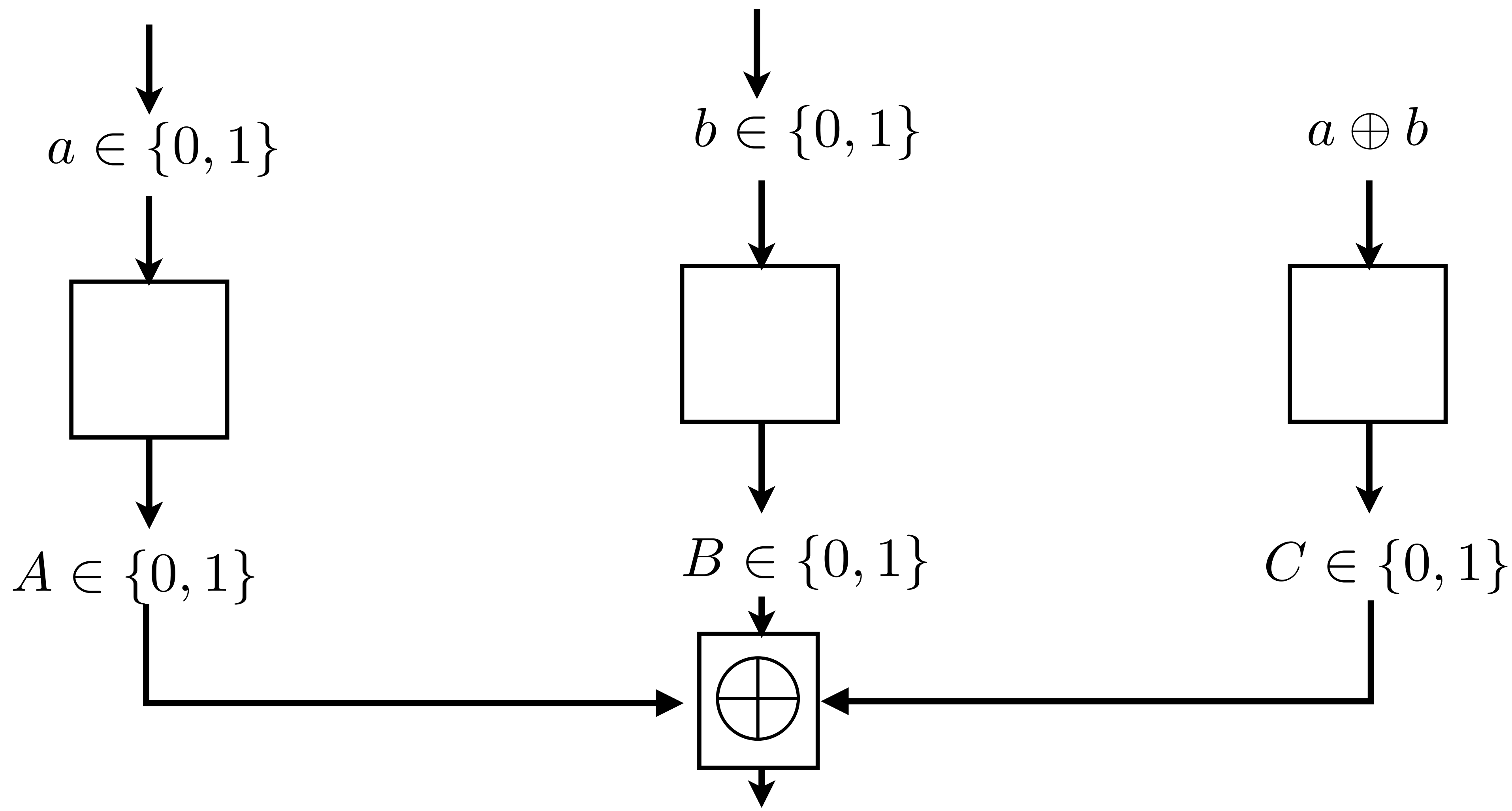
Two to Three



GHZ State: $(1/\sqrt{2})(|000\rangle + |111\rangle)$

Measurements: 0: X 1: Y

Two to Three

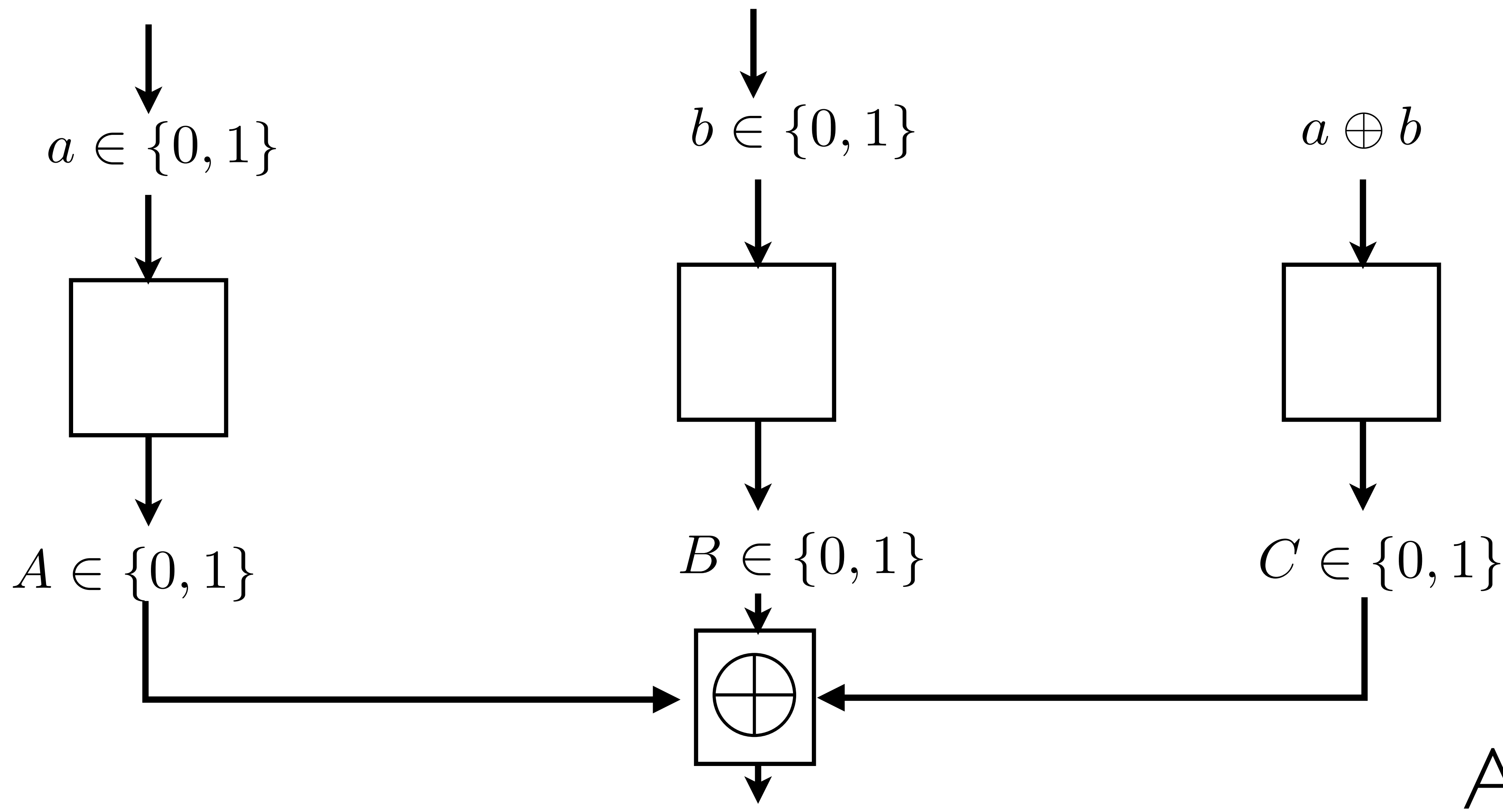


GHZ State: $(1/\sqrt{2})(|000\rangle + |111\rangle)$

Measurements: **0**: X **1**: Y

Output **always** satisfies: $A \oplus B \oplus C = ab$

Two to Three



An **AND** with **100%** probability!

GHZ State: $(1/\sqrt{2})(|000\rangle + |111\rangle)$

Measurements: **0**: X **1**: Y

Output **always** satisfies: $A \oplus B \oplus C = ab$

Two to Three

- In this three party case, we achieve a clear separation.

Classical correlations: **Linear functions**

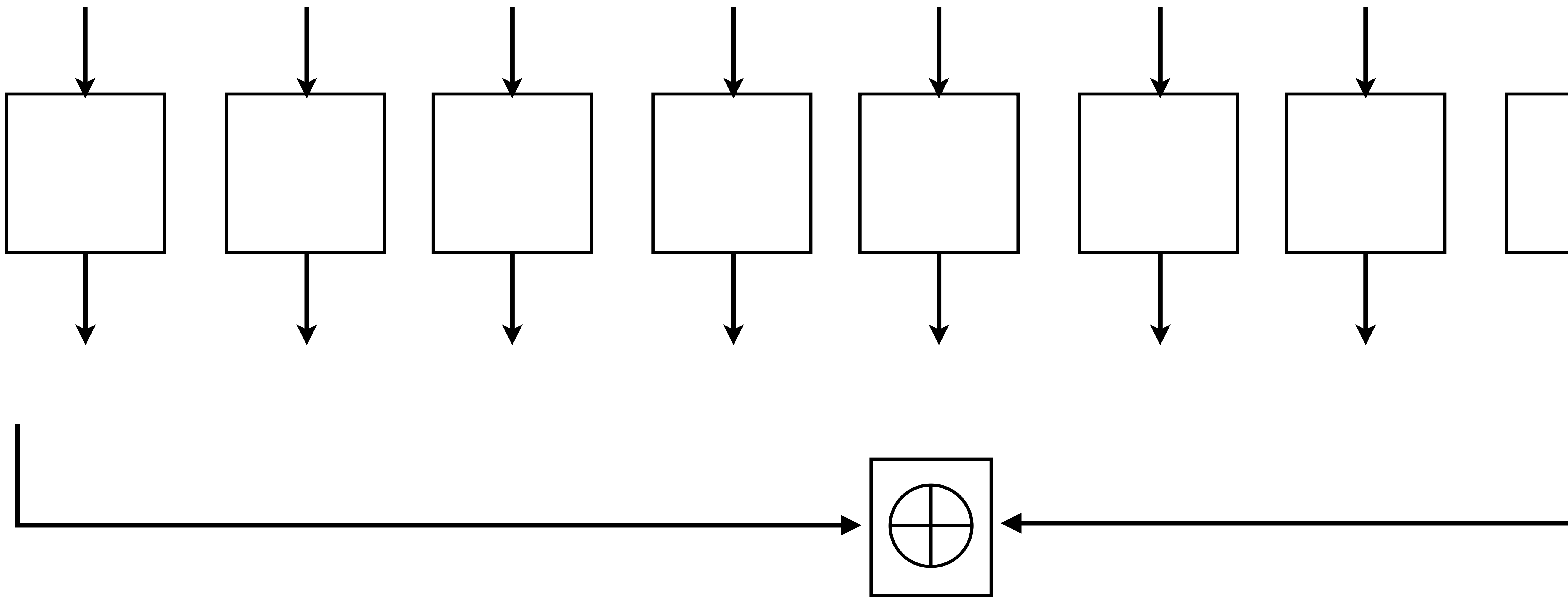
Correlations provide no advantage at all.

Quantum correlations: **All functions deterministically**

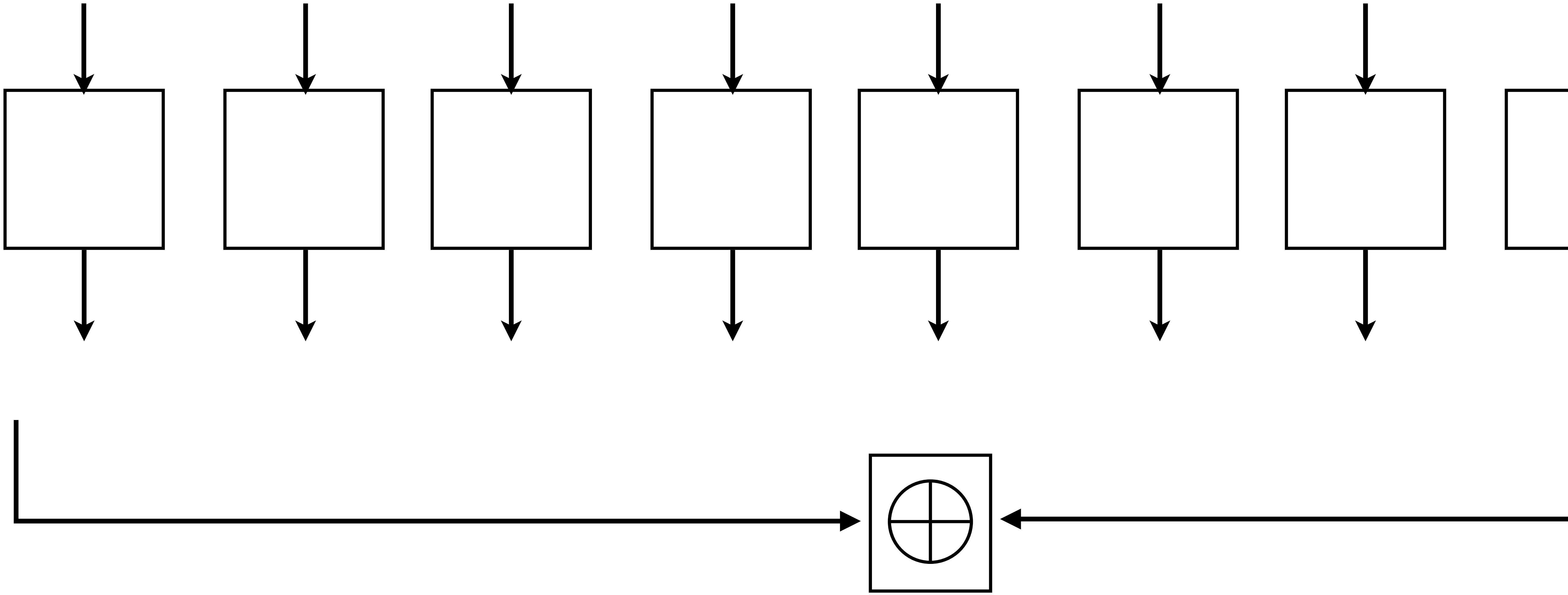
Since AND, XOR, NOT form a universal set.

- In quantum mechanics, **correlations** are a **computational resource**.

Three to Many?



Three to Many?



Classical correlations: **Linear functions**

Same arguments apply.

Quantum correlations?

Three to Many?

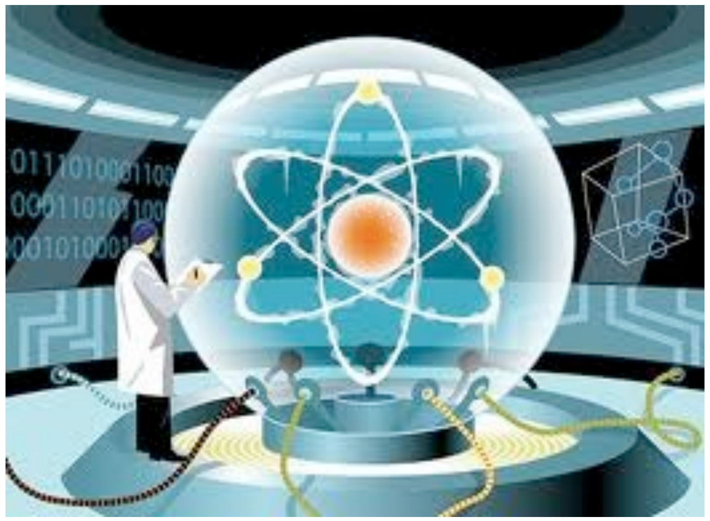
Is there anything beyond all Boolean functions?

Three to Many?

Is there anything beyond all Boolean functions?

Universal quantum computing.

Quantum computing in a nut-shell



In a quantum computer, **coherent unitary** logic gates act on **quantum bits**.

Quantum computing in a nut-shell

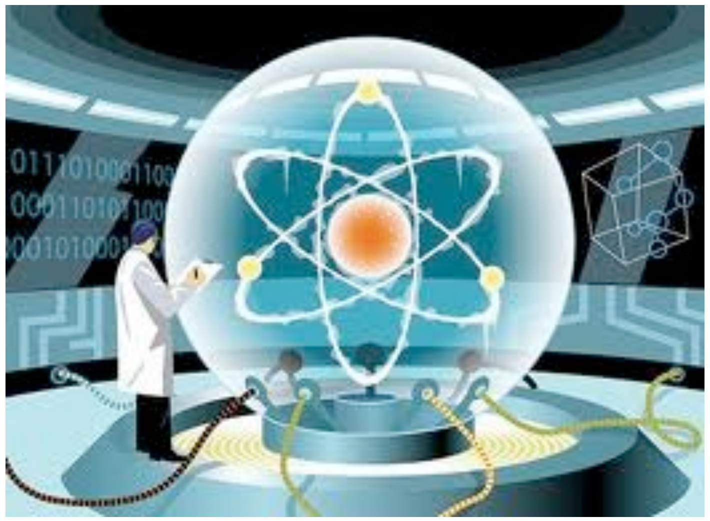
Superposition

Entanglement

Quantum measurement

In a quantum computer, **coherent unitary** logic gates act on **quantum bits**.

Quantum computing in a nut-shell



Superposition

Entanglement

Quantum measurement

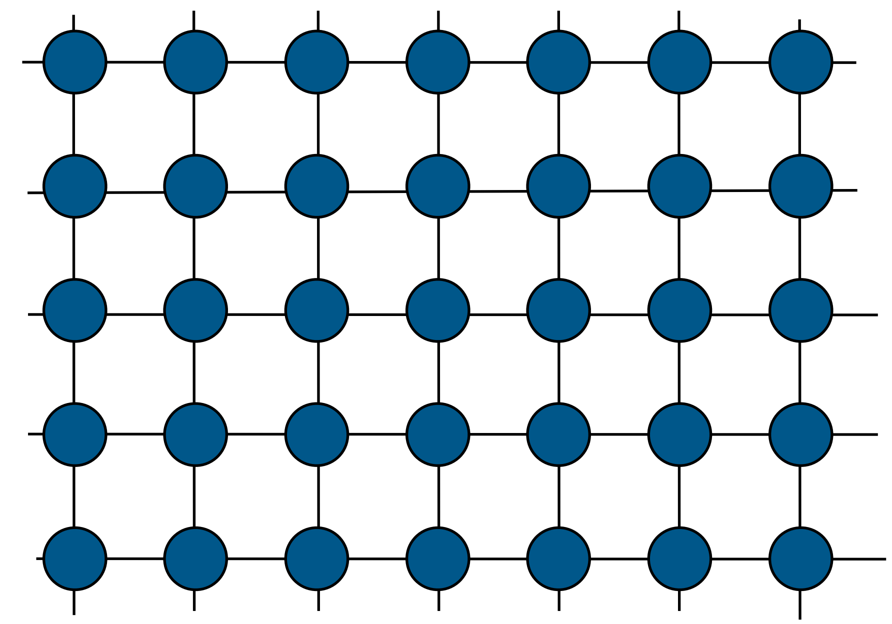
In a quantum computer, **coherent unitary** logic gates act on **quantum bits**.

For certain problems (e.g. factoring, simulating quantum physics) an **exponential speedup** over best classical algorithms.

A very special quantum state

“Cluster state”

Lattice of qubits



“Recipe” for the state

- Qubits prepared in state

$$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$$

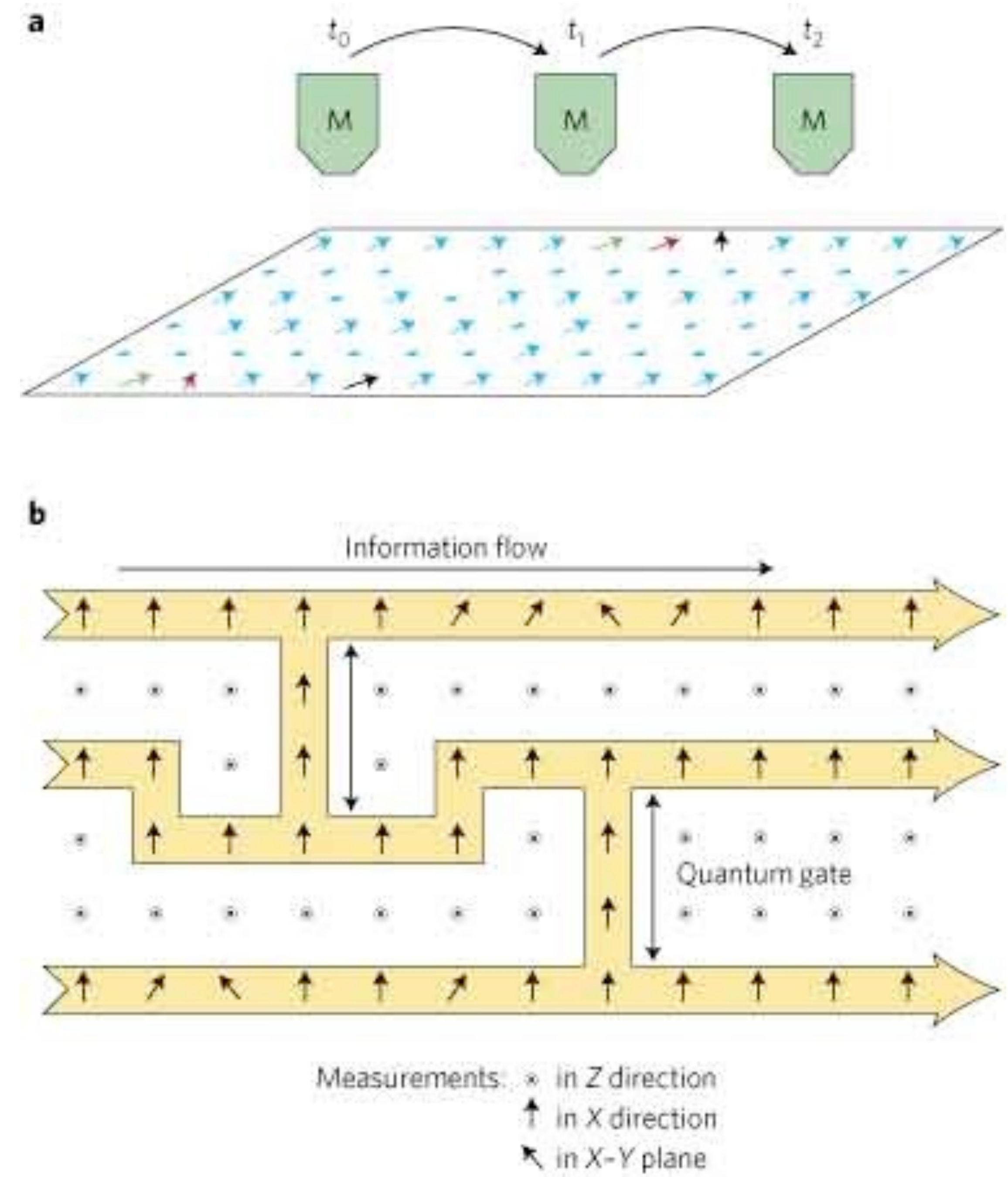
A “many-body singlet”

Application of an entangling two-qubit controlled-Z gate

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Measurement-based quantum computing

- With single-qubit measurements
  - on a (large enough) cluster state
  - (assisted with XOR gates)
- one can implement **any** quantum computation.



Quantum correlations are a resource for **quantum computation.**

Bell inequalities tell us **no** classical analogue of this effect exists.

Summary

Classical correlations: **No computational utility**

Quantum correlations: **A rich computational resource**

Summary

Classical correlations: **No computational utility**

Quantum correlations: **A rich computational resource**

- At the **heart** of Bell's theorem is **Computation.**

References

- **Bell’s Theorem and generalisations**
  - J.S Bell, Physics 1, 195 (1964).
  - D. M. Greenberger, M. Horne, A. Zeilinger, 'Bell's Theorem, Quantum Theory, and Conceptions of the Universe', 69-72 (1989).
- **Measurement-based quantum computation**
  - R. Raussendorf, and H. J. Briegel, Phys. Rev. Lett. 86, 5188- 5191 (2001)
  - H. J. Briegel, D. E. Browne, W. Dur, R. Raussendorf, M. Van den Nest, Nature Physics 5 1, 19-26 (2009).
- **Correlations and Computation**
  - J.Anders, D.E.Browne, Phys.Rev.Lett.102,050502(2009).
  - M.J. Hoban and D.E. Browne, Phys. Rev. Lett. 107, 120402 (2011)
  - M.J. Hoban, J. J. Wallman and D.E. Browne, Phys. Rev. A 84, 062107 (2011)