

Lecture 7

Intrinsic randomness
and its practical uses

Plan of the Lecture

The violation of Bell inequalities, proof of intrinsic randomness

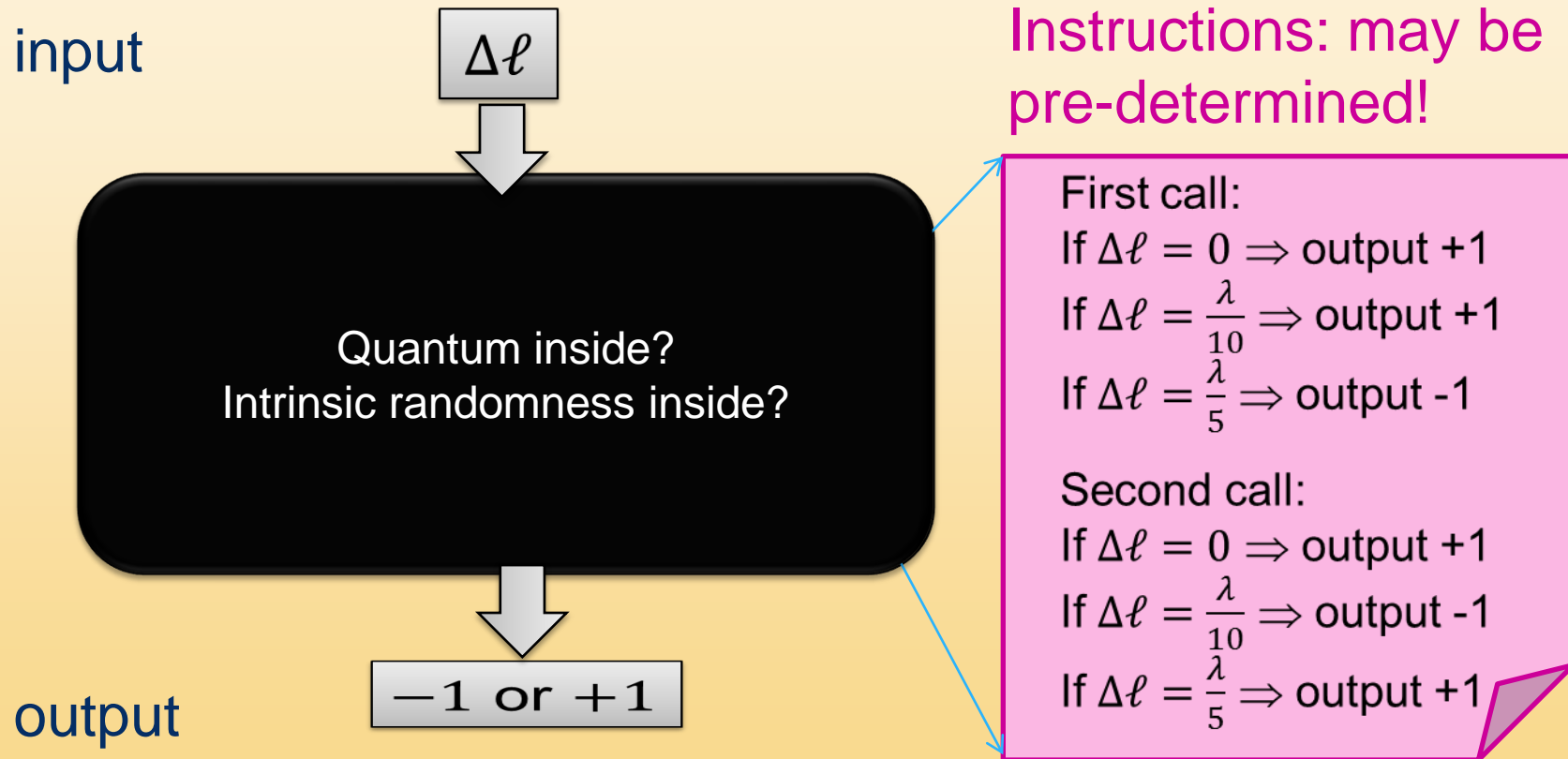
1 Pre-established agreement

2-3 Bell's theorem and its implications

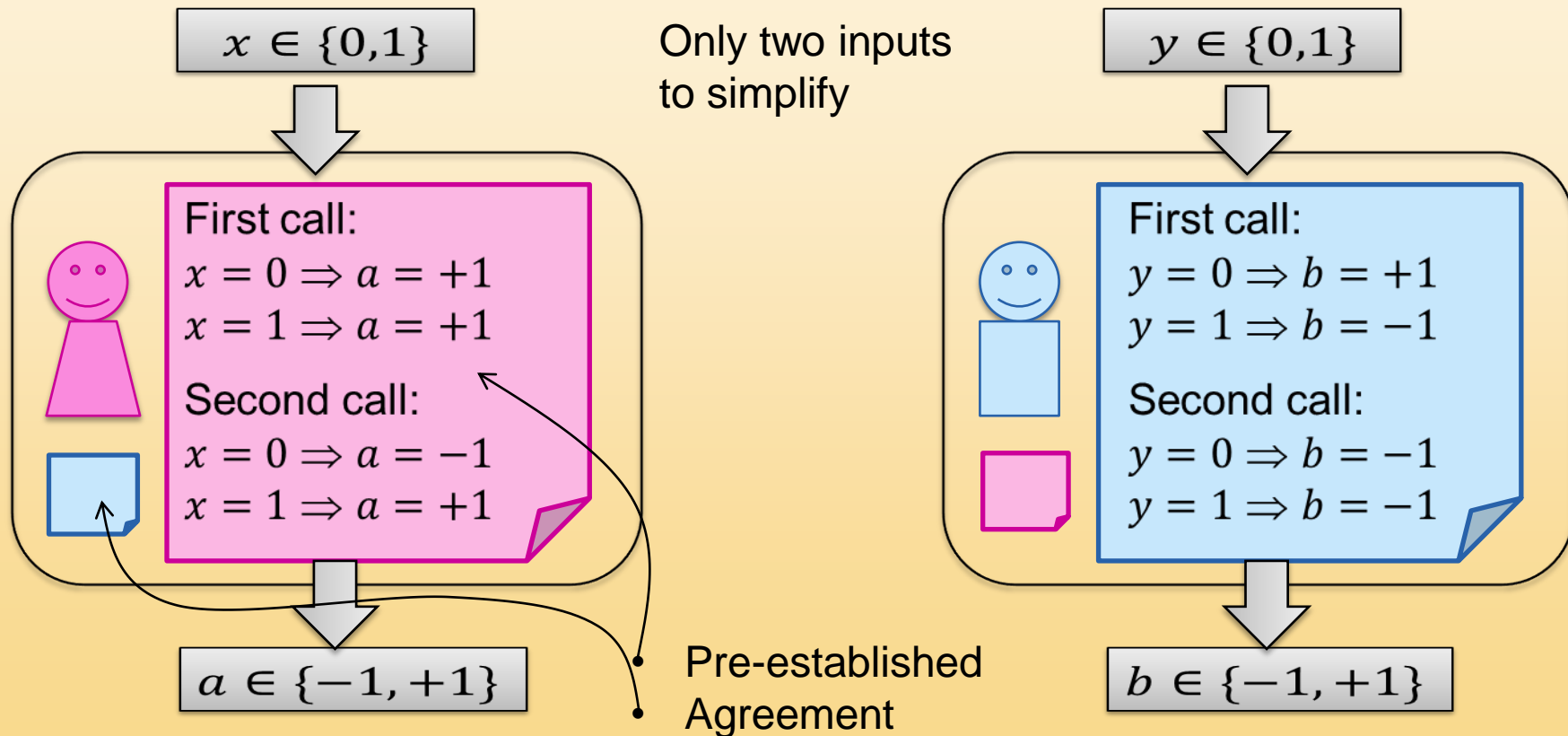
4 Quantum information

PRE-ESTABLISHED AGREEMENT

Black-boxes reloaded



Two parties



What A&B can do...

Example: same input \Rightarrow same output



First call:

$x = 0 \Rightarrow a = +1$

$x = 1 \Rightarrow a = +1$

Second call:

$x = 0 \Rightarrow a = -1$

$x = 1 \Rightarrow a = +1$



First call:

$y = 0 \Rightarrow b = +1$

$y = 1 \Rightarrow b = +1$

Second call:


$y = 0 \Rightarrow b = -1$

$y = 1 \Rightarrow b = +1$

- Obvious: just share the same list of instructions
- Real life example: agents of the same company bidding in different stock exchanges upon knowing if Party A or Party B has won the elections

... and what they can't do


Example: same output unless $x = y = 1$



Alice is represented by a pink stick figure. To her right is a pink rectangular box with a folded bottom-right corner, containing her view of the world.

First call:
 $x = 0 \Rightarrow a = +1$
 $x = 1 \Rightarrow a = +1$

Second call:
 $x = 0 \Rightarrow a = -1$
 $x = 1 \Rightarrow a = -1$



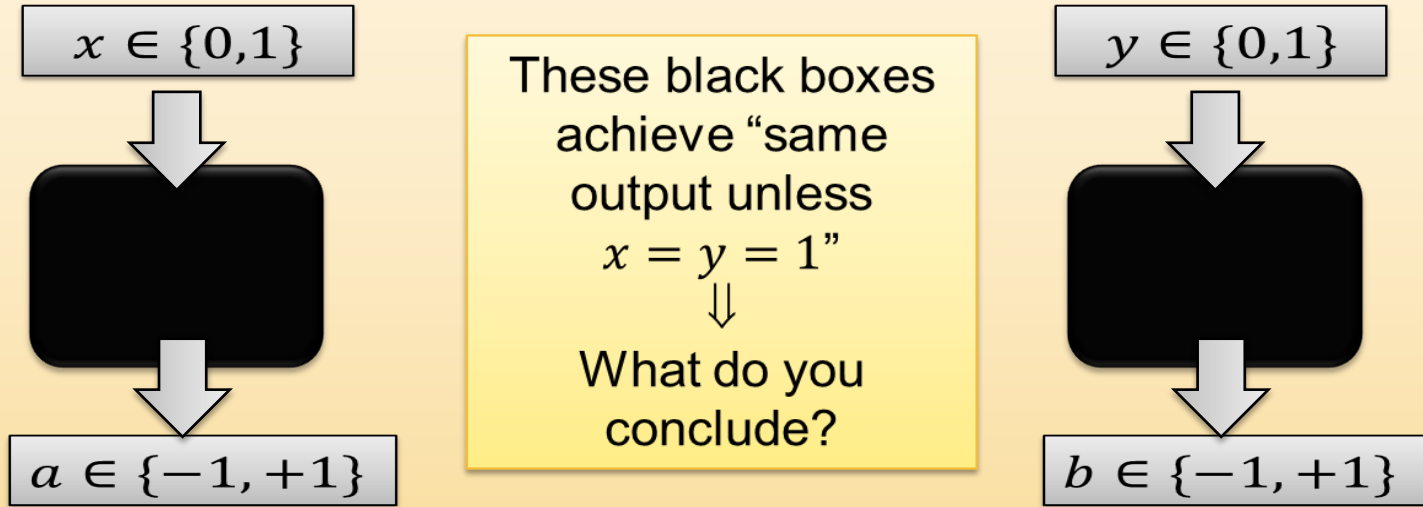
Bob is represented by a blue stick figure. To his right is a blue rectangular box with a folded bottom-right corner, containing his view of the world.

First call:
 $y = 0 \Rightarrow b = +1$
 $y = 1 \Rightarrow$ **depends on x**

Second call:
 $y = 0 \Rightarrow b = -1$
 $y = 1 \Rightarrow$ **depends on x**

- Bob should know the actual input of Alice, not only how she may react to any input.
- Classically, it can only be solved by Alice signaling to Bob (i.e. sending x)

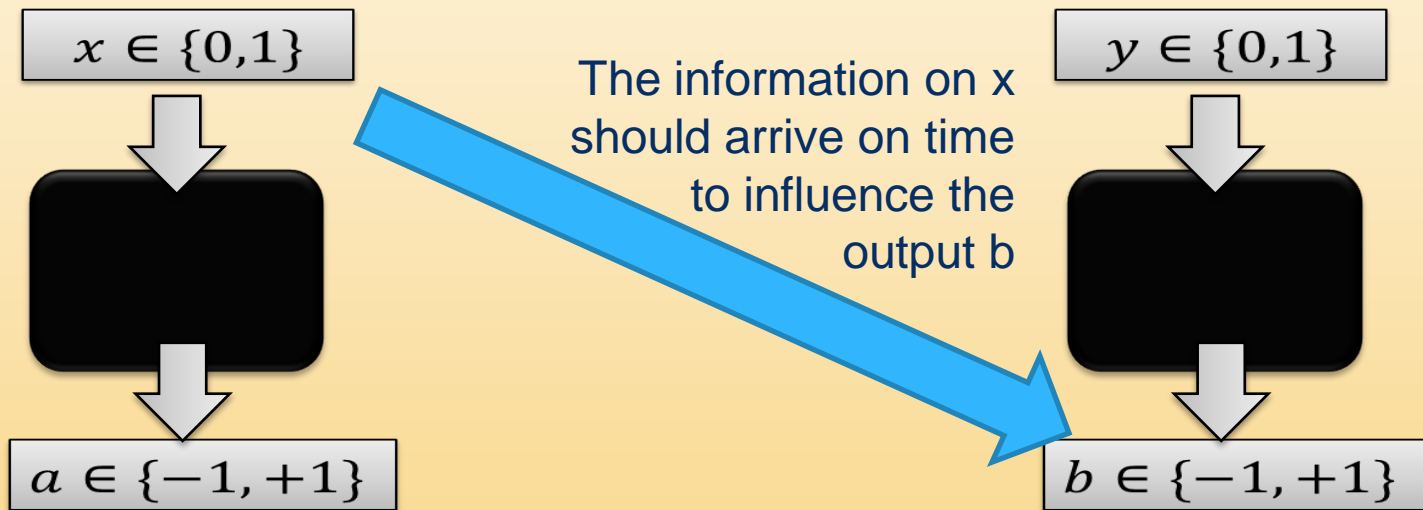
Suppose now...



- *Necessary* conclusion: **at least one of the outcomes was not pre-established**
- Inference of classical mechanism: one boxes is sending a signal to the other
- ... but what if no signal can have been sent?

No signal faster than light

Concretely, what if the boxes are so far apart, that a signal from one should propagate faster than light to reach the other?



This is what two quantum “particles” separated by a large distance can do!

BELL'S THEOREM (1)

Derivation

The assumption



This call:

$$x = 0 \Rightarrow a_0$$

$$x = 1 \Rightarrow a_1$$

$$a_0, a_1, b_0, b_1 \in \{-1, +1\}$$



This call:

$$y = 0 \Rightarrow b_0$$

$$y = 1 \Rightarrow b_1$$

Pre-established agreement: for each call, the four outcomes (a_0, a_1, b_0, b_1) are pre-determined

Simple algebra

For each call, the four outcomes (a_0, a_1, b_0, b_1) are pre-determined



For each call, it would be possible to compute the number

$$S = a_0b_0 + a_0b_1 + a_1b_0 - a_1b_1$$

Observation: either $S = +2$ or $S = -2$.

Proof: notice that $S = a_0(b_0 + b_1) + a_1(b_0 - b_1)$

\Rightarrow If $b_0 = b_1$, the first term is $\pm 1 \times \pm 2$ and the second term is zero


\Rightarrow If $b_0 = -b_1$, the first term is zero and the second term is $\pm 1 \times \pm 2$.

Simple averages

In each call, Alice gets either a_0 or a_1 , Bob gets either b_0 or b_1
 \Rightarrow it is impossible to measure S on each call...

... but it is possible to measure the average of S over many calls:

$$\langle S \rangle = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle$$

 Average of $a \times b$ over all the calls where $x = 0$ and $y = 0$.

Observation: $\langle S \rangle \leq 2$ for pre-established agreement.

Proof: under pre-established agreement, S is either $+2$ or -2 , so the average cannot exceed 2.

Bell's theorem

Pre-established agreement $\Rightarrow \langle S \rangle \leq 2$

A measurable number



- The first such inequality was derived by John Bell in 1964
- The one presented here is by Clauser-Horne-Shimony-Holt (CHSH) 1969

If one observes $\langle S \rangle > 2$ (“violation” of the Bell inequality), pre-established agreement cannot be the explanation

- Quantum theory predicts a violation for suitable experiments
- The experiments confirm the violation.

An example

Same output unless $x = y = 1$

x	y	ab
0	0	+1
0	1	+1
1	0	+1
1	1	-1

Quantum systems
can't win this
game perfectly, but
can reach

$$\langle S \rangle = 2\sqrt{2} \\ \approx 2.8284$$

$$\langle S \rangle = +1 + +1 + +1 - -1 = 4 > 2$$

Suggested Readings

Wikipedia pages:

- http://en.wikipedia.org/wiki/Bell_theorem

BELL'S THEOREM (2)

Implications

Short history of Bell's theorem (1)

- “The outcomes of measurements are not pre-established” was an early dogma of quantum theory
- Most physicists accepted it; Einstein and some others did not and hoped to save determinism with “local hidden variables” [LHV = pre-established agreement]
- Until Bell, the debate remained purely conceptual.
- Bell tried to write down an explicit LHV model that reproduces all predictions of quantum theory... and ended up proving that it is impossible.

Short history of Bell's theorem (2)

- No available data matched those needed for a Bell test: need for dedicated experiments.
- 1970's: some attempts, not conclusive
- First conclusive test: Aspect & coworkers, Orsay 1981-2, with two photons.
- Many experiments since, all confirming violation
 - 1998 Gisin's group (Geneva): detectors 10km apart
 - 1998 Zeilinger's group (Innsbruck): random choice of x, y in each run
 - 21st century: more photons, two ions, two atoms, one atom and one photon...

In our universe

Bell inequality violated

⇒ No pre-established agreement

⇒ The outcome of at least one box did not pre-exist



There is a signal

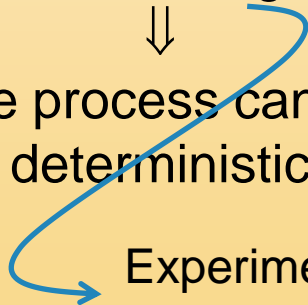


The process can be
deterministic

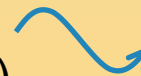
There is no signal



The process cannot be deterministic



Experiments: such a signal should propagate
faster than light (and in fact, at infinite speed!)



(not sure this is
our universe...)

Intrinsic randomness


With signal

Without signal

Disclaimer: the overwhelming majority of physicists accept that **no signal** is involved in quantum violations of Bell inequalities.

- Recall that Bohm's wave ("ether") is postulated to be unobservable

determinism for an observer who can see all the parallel universes



Even if one is willing to invoke infinite speeds or parallel universes to save determinism, violation of Bell inequalities implies **intrinsic randomness for users in our universe.**

Bell is “device-independent”

- Notice that I did not describe the devices inside the boxes, the physical systems under study etc.
- Of course, to *set up* such an experiment, one needs to know how to create **entanglement**, which beam-splitters and detectors to use...
- But the violation of a Bell inequality can be *assessed* without any of this knowledge: black-box, or “device-independent”, scenario.

QUANTUM INFORMATION

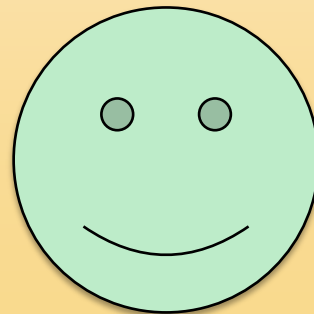
Attitudes

You cannot know both
position and momentum

You cannot predict the
outcome of a measurement,
only the statistics



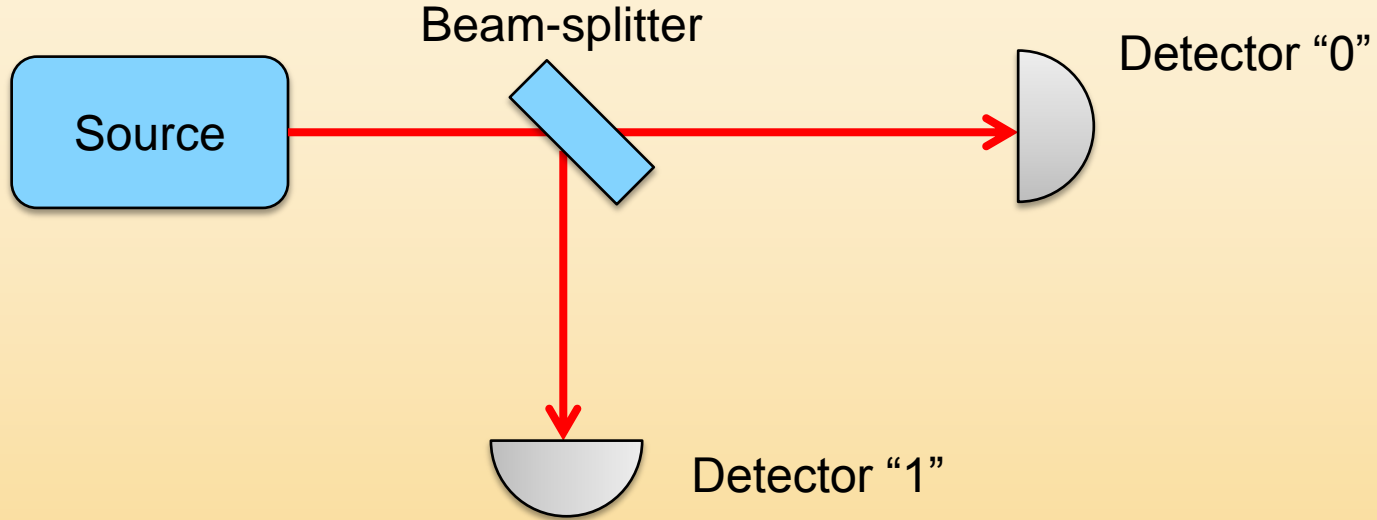
There is a source of real
randomness out there,
let's use it!



Brief overview of Q-info

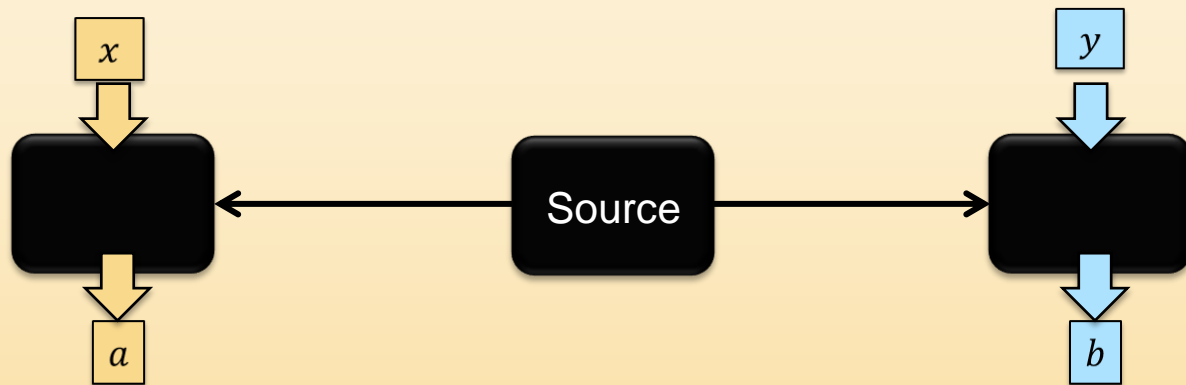
- Quantum cryptography
 - Main tasks: key distribution for use in OTP; secure RNG
 - Bennett & Brassard 1984 (BB84); Ekert 1991
 - Present status: commercial product
- Quantum computing
 - Main task: factoring integers (a threat for RSA)
 - Shor 1994
 - Present status: still far away, working on simpler relevant applications

Trusted RNG



- Recall that single “particle” does not withstand the “black-box” test.
- Need to characterize source and beam-splitter in order to certify randomness (similar to the resistor of Lecture 4)

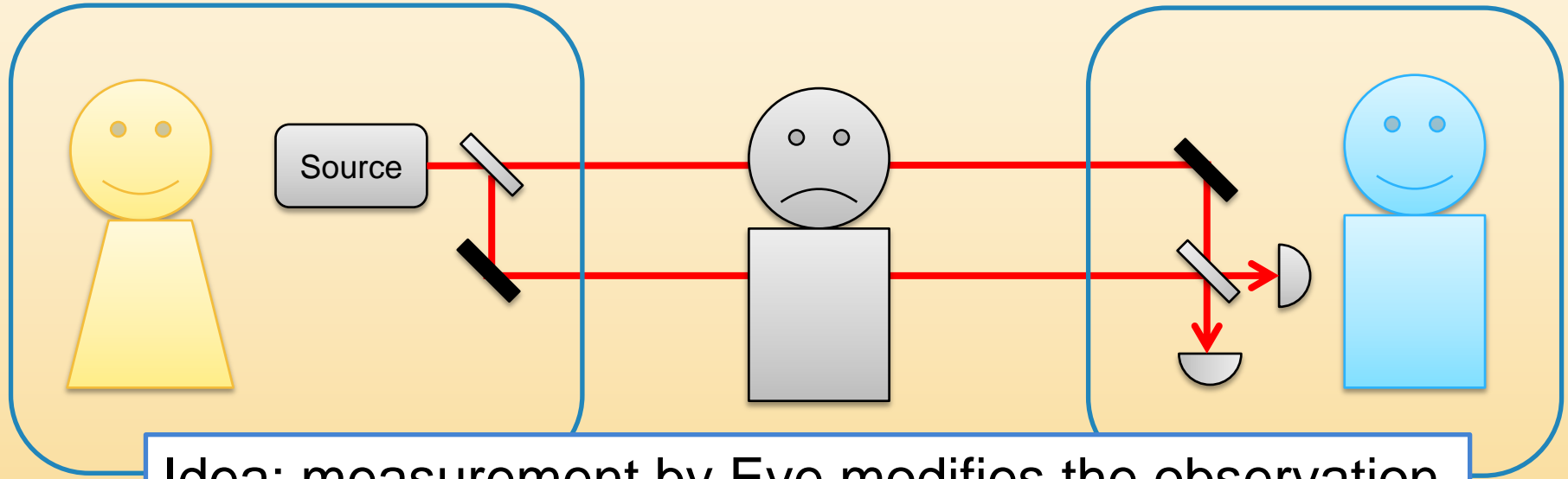
Untrusted RNG



(a, b) is random even for the producer if $\left\{ \begin{array}{l} \text{Bell inequality violated} \\ \text{No-signaling between the boxes} \end{array} \right.$

- The users don't need to characterize the devices ("device-independent")
- The min-entropy of intrinsic randomness is a function of $\langle S \rangle$
 - For $\langle S \rangle = 2\sqrt{2}$, both a and b are perfect fair coins.

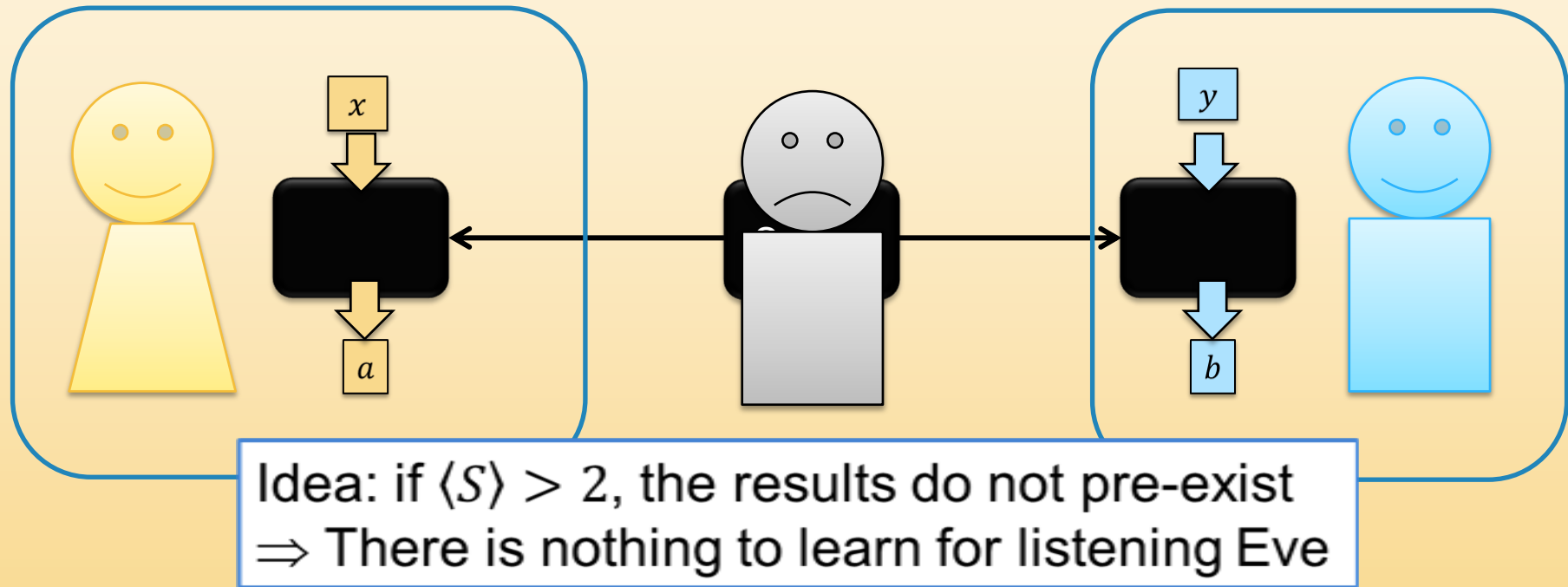
Key-distribution à la BB84



Idea: measurement by Eve modifies the observation
⇒ If Eve is listening, Alice and Bob will notice it

Trust: Alice and Bob need to characterize their devices (source, beam-splitters...)

Key-distribution à la Ekert



Trust: Alice and Bob need to ensure no-signaling (no radio inside the black box) but do not need to characterize their devices ("device-independent")

Suggested Readings

Check "Quantum Random" in <http://www.didaktik.physik.uni-erlangen.de/quantumlab/english/index.html>

Wikipedia pages:

- http://en.wikipedia.org/wiki/Quantum_information_science
- http://en.wikipedia.org/wiki/Quantum_key_distribution

Summary of Lecture 7

The violation of Bell inequalities, proof of intrinsic randomness

- Contrary to one black box, two black boxes cannot always be simulated with pre-established data
- Violation of Bell inequalities \Rightarrow the outcomes are not pre-established \Rightarrow cannot be predicted
- Violation observed in many experiments
- Quantum information: making it useful