Quantum Key Distribution

BIU Winter School on Quantum Cryptography | February 15, 2021

Rotem Arnon-Friedman | Weizmann Institute of Science

Quantum Cryptography

Quantum cryptography

Post-quantum cryptography

Quantum Key Distribution (QKD)

Post-quantum cryptography

Quantum Key Distribution (QKD)

- Quantum protocol
- Quantum adversary (information theoretic)
- Composable quantum security definition
- Security proofs based on the laws of quantum physics

We have a lot to learn.... :)

Outline

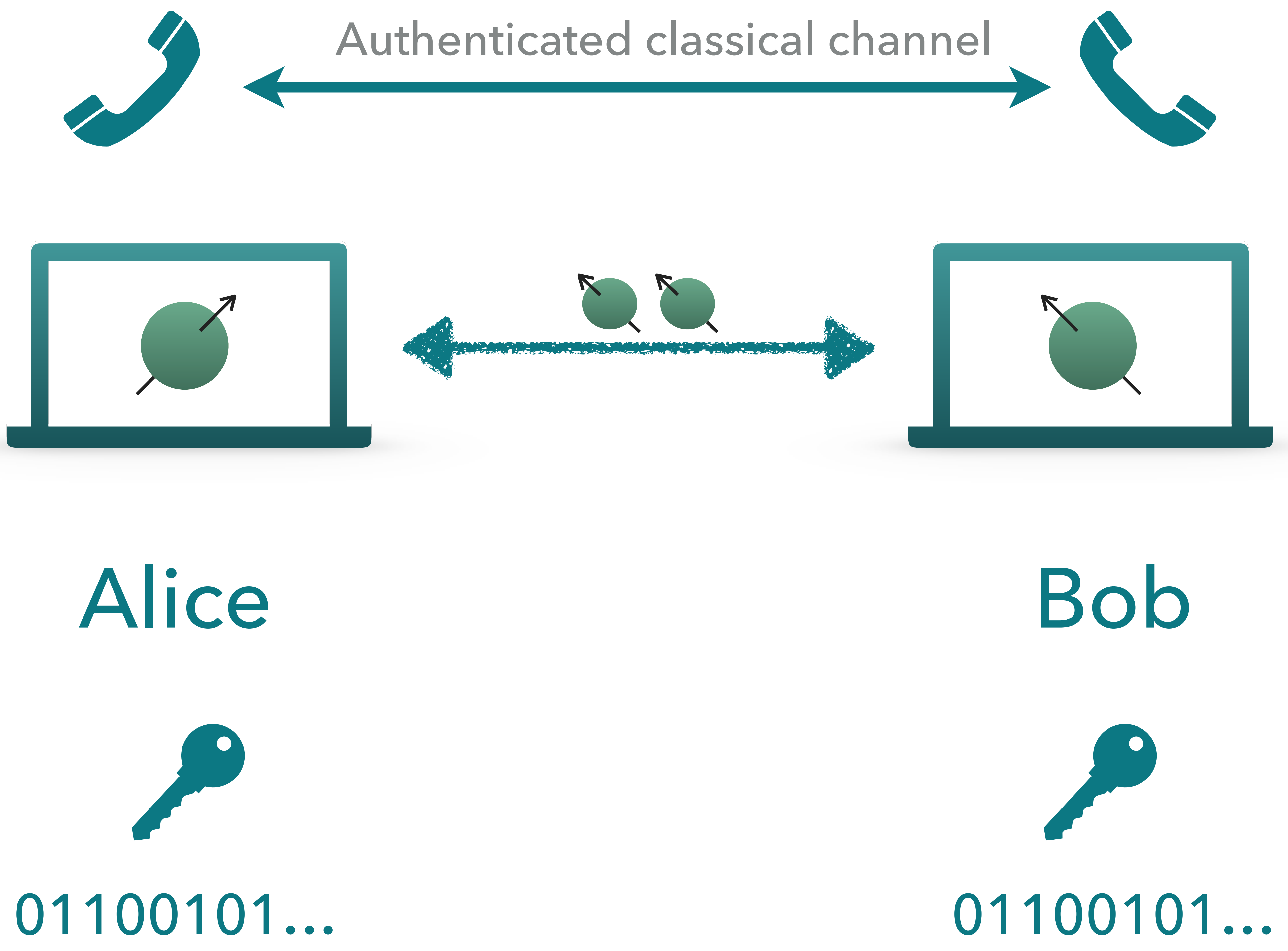
- Lecture 1:
  - Introduction
  - BB84 and Ekert91 protocols
- Lecture 2:
  - QKD security definition
  - Quantum-proof randomness extractors
- Lecture 3:
  - Security proof (the main parts)
  - Device-independent quantum key distribution

1. The task
2. It’s alive

Introduction

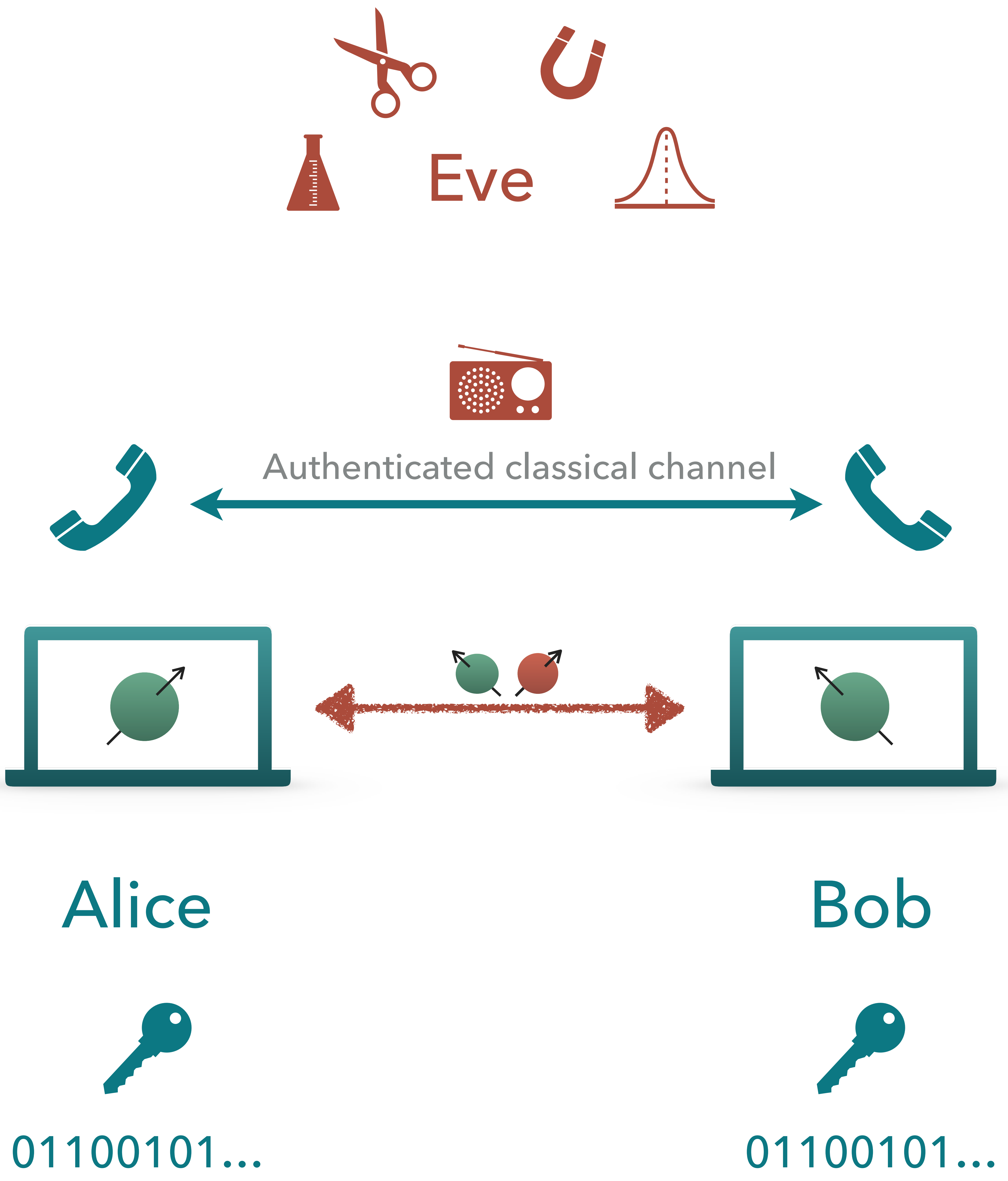
The Task

- Two honest parties: Alice and Bob
  - Goal: Create a secret key
- Resources:
  - Local quantum devices (Not a quantum computer)
  - Public quantum communication channel
  - Public authenticated classical communication channel



The Task

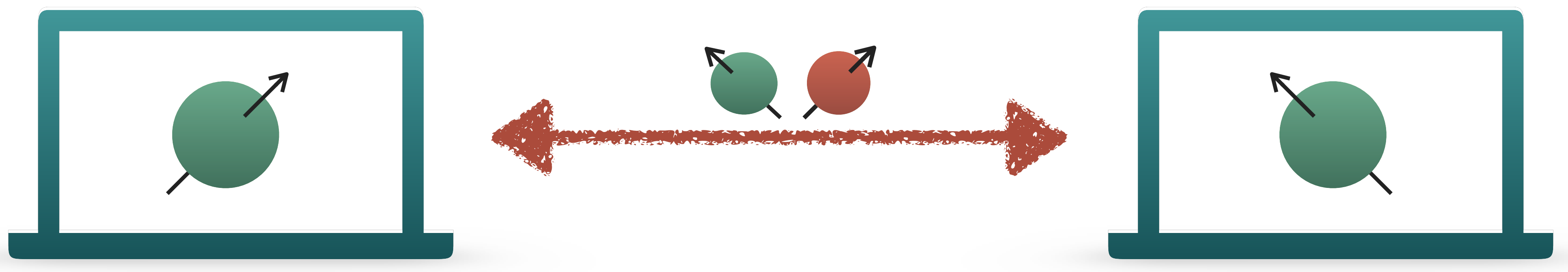
- Two honest parties: Alice and Bob
  - Goal: Create a secret key
- One dishonest party: Eve
  - Eve's goal: gain as much information as possible about the key
- **Information theoretic security**
- High key rate
- Expansion rather than distribution
  - "Everlasting security"



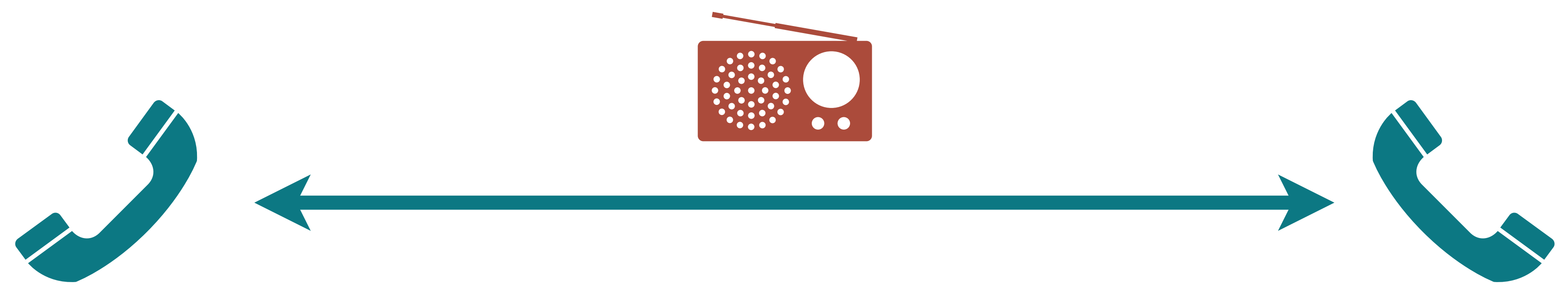
The Task

- Structure of a general QKD protocol:

1. Generation of the classical raw data using the quantum devices



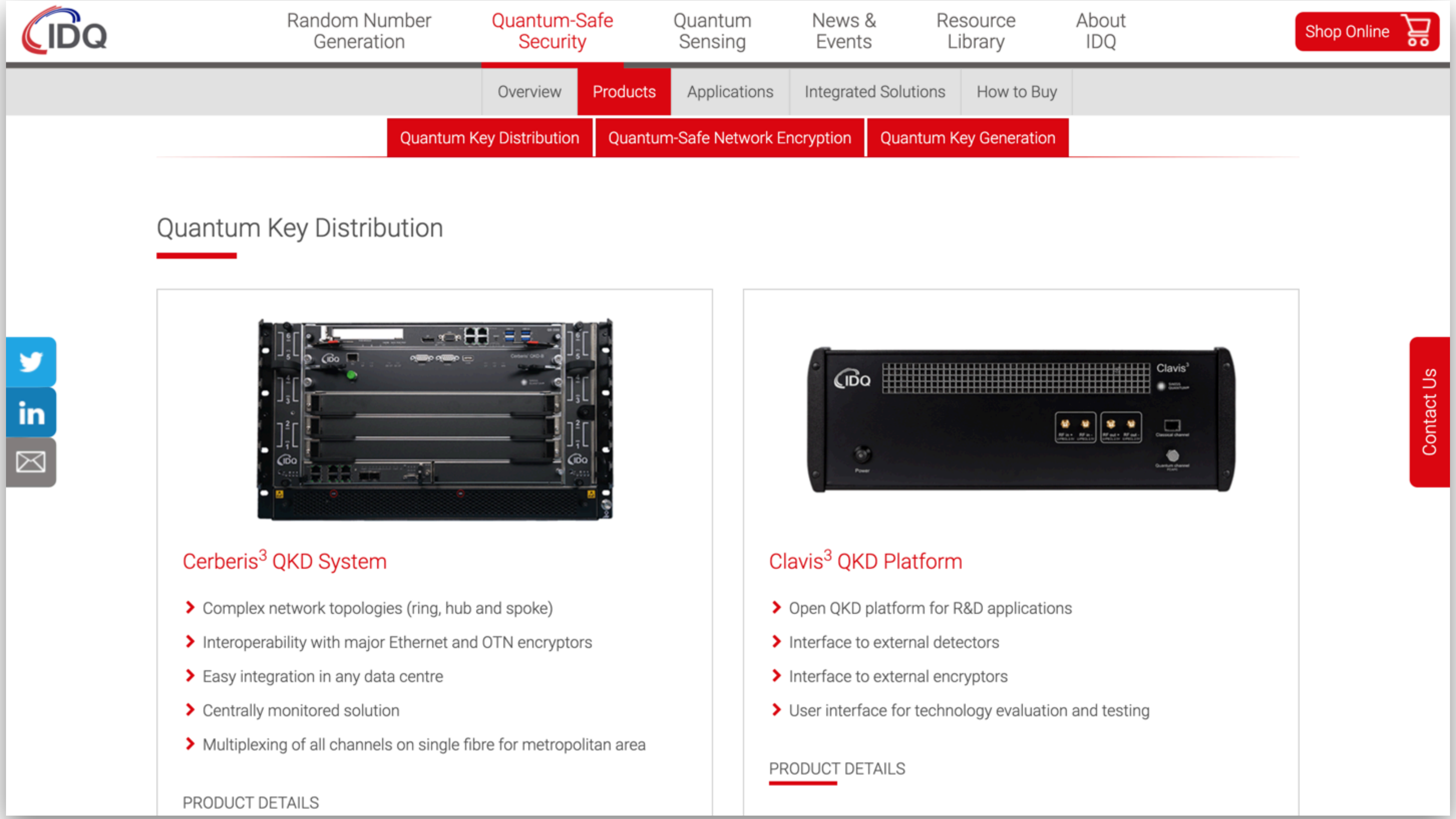
2. Classical processing of the data (**post-quantum cryptography**)



It's Alive

- Types of protocols:
  - Prepare and measure protocols
  - Entanglement based protocols
  - Discrete-variable protocols
  - Continues-variable protocols
  - Device-independent protocols
  - Semi-device-independent
  - One-way classical processing
  - Two-way classical processing
  - …
- Some examples:
  - BB84 protocol
  - Six-state protocol
  - Ekert 91 protocol
  - COW protocol
  - Satellite-based protocols
  - Ping-pong protocol
  - Twin-field protocol
  - …
- Quantum hacking 

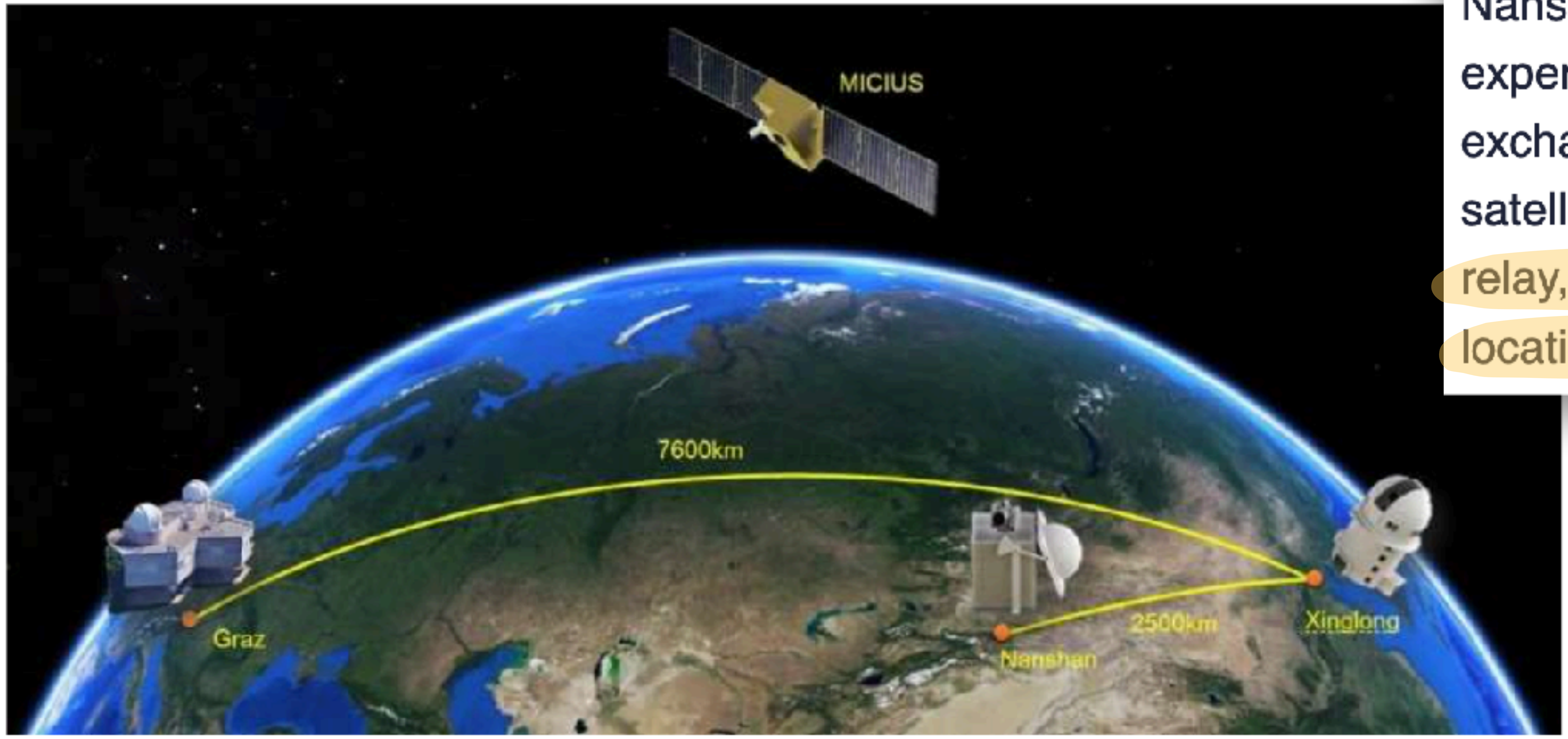
It's Alive


IDQ
Random Number Generation
Quantum-Safe Security
Quantum Sensing
News & Events
Resource Library
About IDQ
Shop Online
Overview
Products
Applications
Integrated Solutions
How to Buy
Quantum Key Distribution
Quantum-Safe Network Encryption
Quantum Key Generation
Quantum Key Distribution
Cerberis3 QKD System
Complex network topologies (ring, hub and spoke)
Interoperability with major Ethernet and OTN encryptors
Easy integration in any data centre
Centrally monitored solution
Multiplexing of all channels on single fibre for metropolitan area
PRODUCT DETAILS
Clavis3 QKD Platform
Open QKD platform for R&D applications
Interface to external detectors
Interface to external encryptors
User interface for technology evaluation and testing
PRODUCT DETAILS
Contact Us

It's Alive

Real-world intercontinental quantum communications enabled by the Micius satellite

by University of Science and Technology of China



A joint China-Austria team has performed quantum key distribution between the quantum-science satellite Micius and multiple ground stations located in Xinglong (near Beijing), Nanshan (near Urumqi), and Graz (near Vienna). Such experiments demonstrate the secure satellite-to-ground exchange of cryptographic keys during the passage of the satellite Micius over a ground station. Using Micius as a trusted relay, a secret key was created between China and Europe at locations separated up to 7,600 km on the Earth.

1. BB84 protocol
2. Intuition
3. Ekert 91 protocol
4. Intuition

Security reduction

Getting Started

BB84: Prepare and Measure

1. Alice prepares one of the 4 states

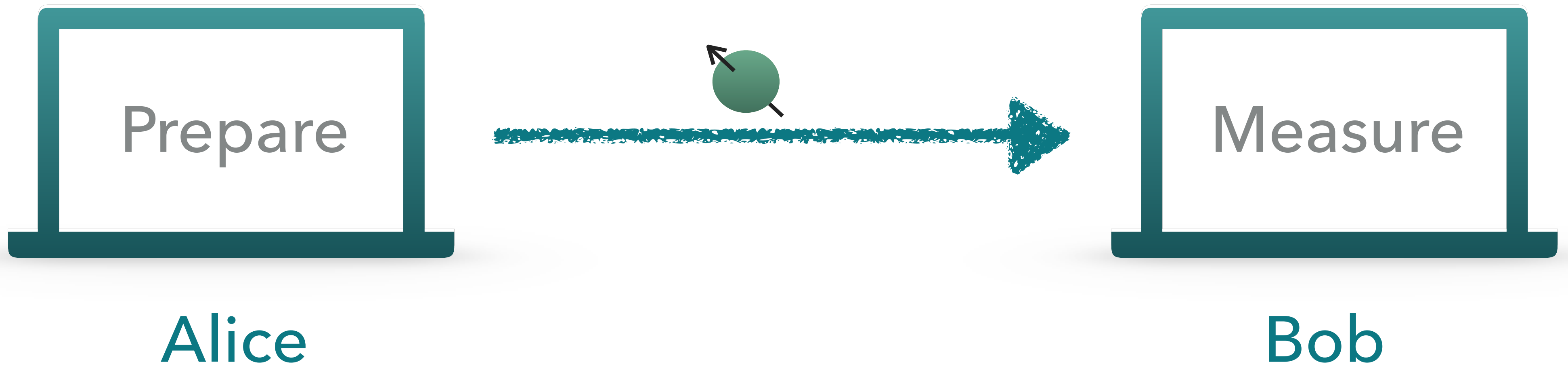
$$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$$

at random and sends to Bob.

Same as choosing a basis Z/X
and an eigenstate in that basis

Z : standard basis $\{|0\rangle, |1\rangle\}$
X : diagonal basis $\{|+\rangle, |-\rangle\}$

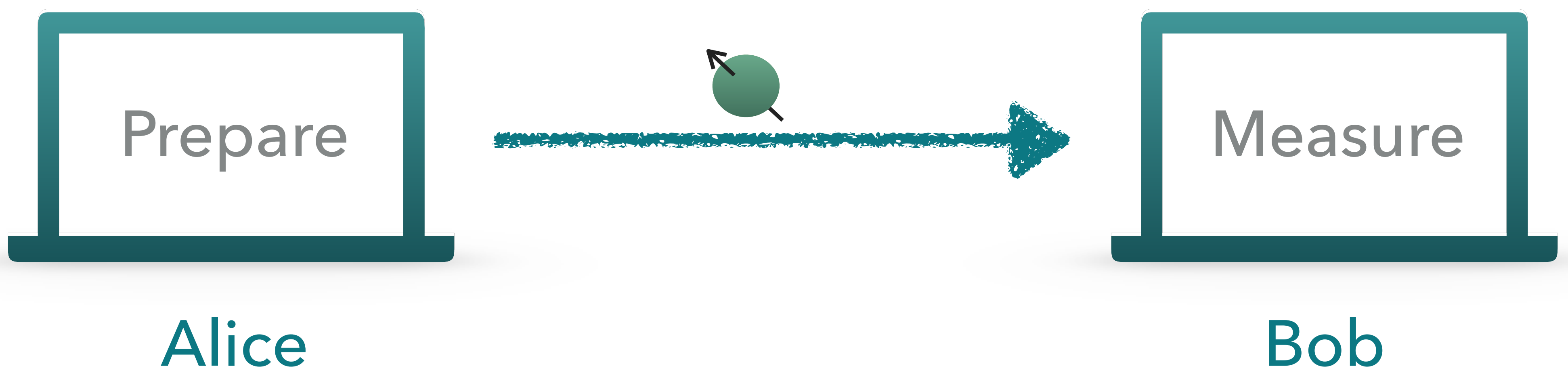
(Honest and noiseless case)



$Z \quad |0\rangle$

BB84: Prepare and Measure

(Honest and noiseless case)



1. Alice prepares one of the 4 states

$$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$$

at random and sends to Bob.

2. Bob chooses at random whether to measure the received qubit at the Z or X basis.
    - He measures and records the outcome.

Alice		Bob	
Z	$\|0\rangle$	Z	$\|0\rangle$
X	$\|-\rangle$	X	$\|-\rangle$
X	$\|+\rangle$	Z	$\|1\rangle$

(w.p. 1/2)

Reminder: $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

BB84: Prepare and Measure

1. Alice prepares one of the 4 states

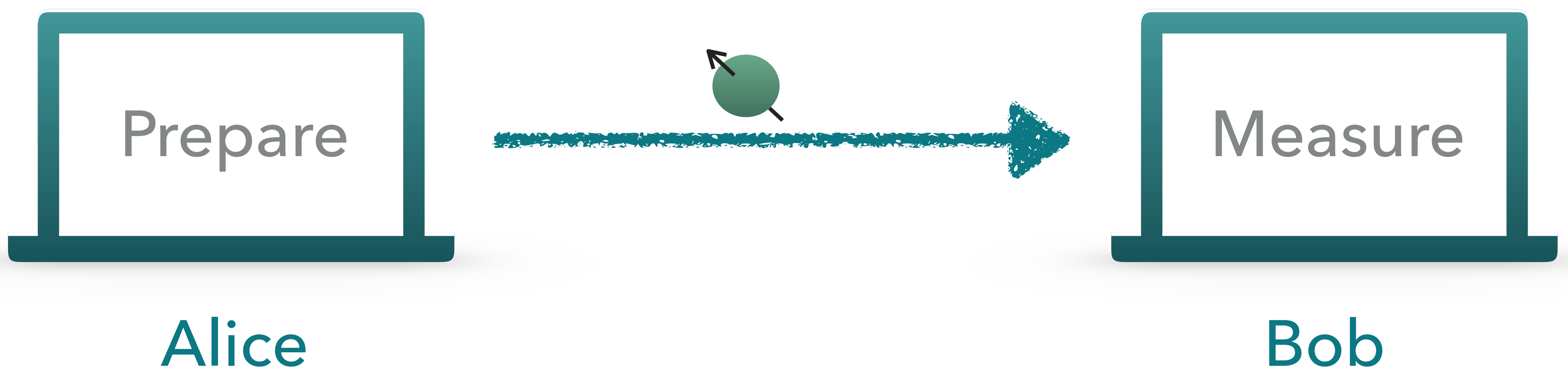
$$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$$

   at random and sends to Bob.

2. Bob chooses at random whether to measure the received qubit at the Z or X basis.

3. Alice and Bob publicly announce their chosen bases.

(Honest and noiseless case)

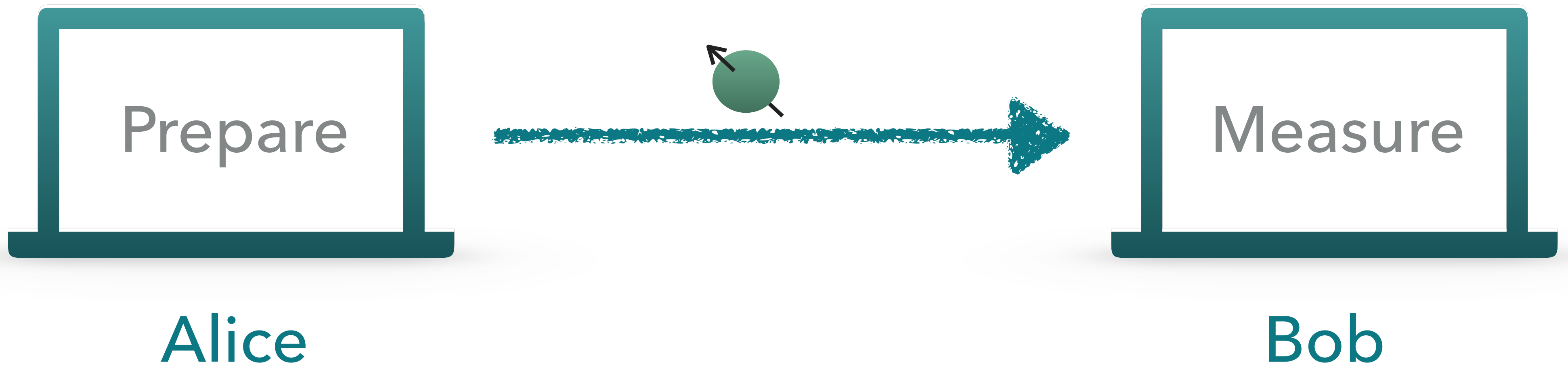


Z	$\|0\rangle$	Z	$\|0\rangle$
X	$\|-\rangle$	X	$\|-\rangle$
~~X~~	~~$\|+\rangle$~~	~~Z~~	~~$\|1\rangle$~~
Z	$\|1\rangle$	Z	$\|1\rangle$
~~Z~~	~~$\|0\rangle$~~	~~X~~	~~$\|+\rangle$~~
Z	$\|0\rangle$	Z	$\|0\rangle$
X	$\|+\rangle$	X	$\|+\rangle$

BB84: Prepare and Measure

1. Alice prepares one of the 4 states
$$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$$
at random and sends to Bob.
2. Bob chooses at random whether to measure the received qubit at the Z or X basis.
3. Alice and Bob publicly announce their chosen bases.
4. The "Z-outputs" construct the key.

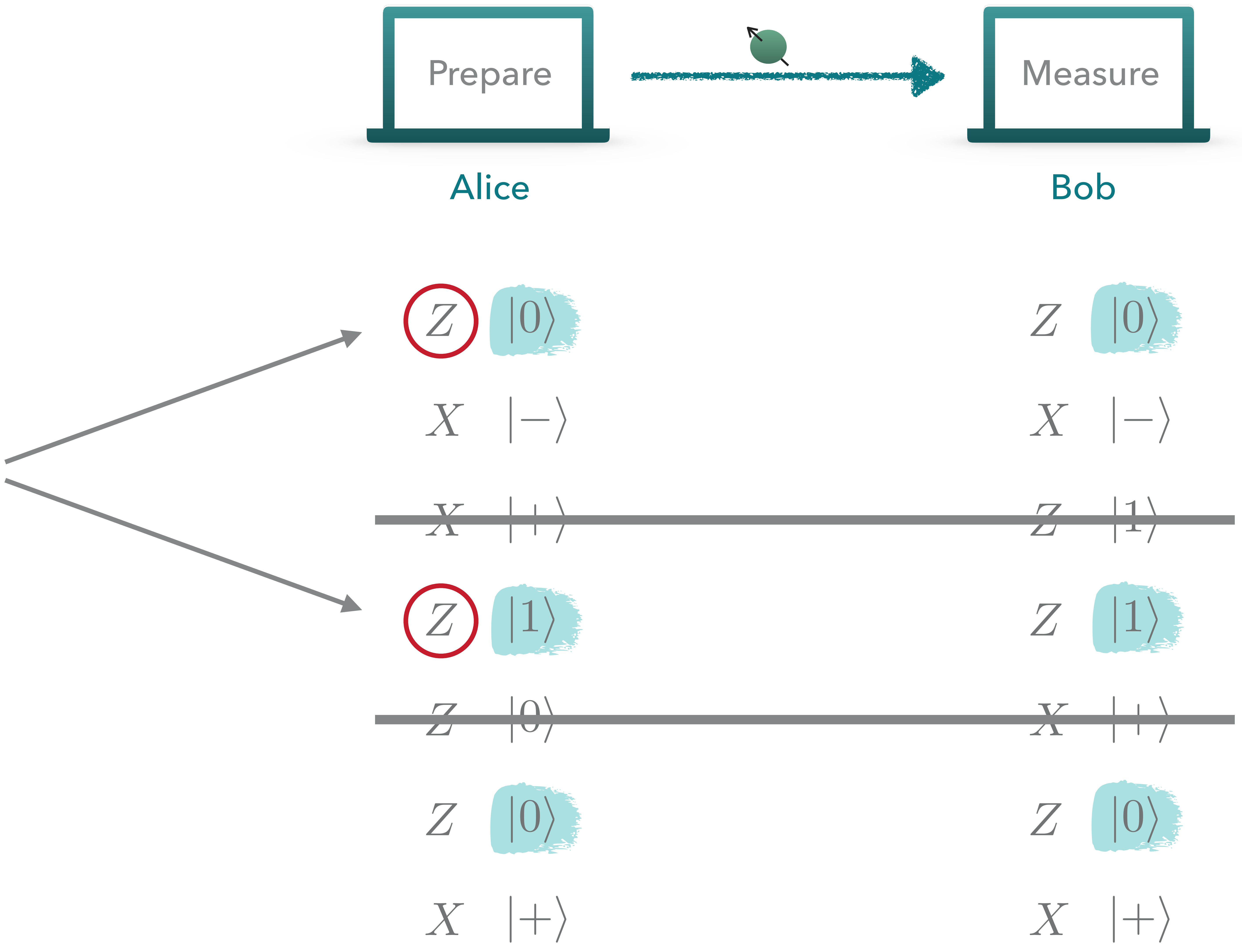
(Honest and noiseless case)



Alice		Bob	
Z	$\|0\rangle$	Z	$\|0\rangle$
X	$\|-\rangle$	X	$\|-\rangle$
~~X~~	~~$\|+\rangle$~~	~~Z~~	~~$\|1\rangle$~~
Z	$\|1\rangle$	Z	$\|1\rangle$
~~Z~~	~~$\|0\rangle$~~	~~X~~	~~$\|+\rangle$~~
Z	$\|0\rangle$	Z	$\|0\rangle$
X	$\|+\rangle$	X	$\|+\rangle$

BB84: Prepare and Measure

(Honest and noiseless case)



Notice:

The measurement **basis** does not reveal any information about the **key bit!**

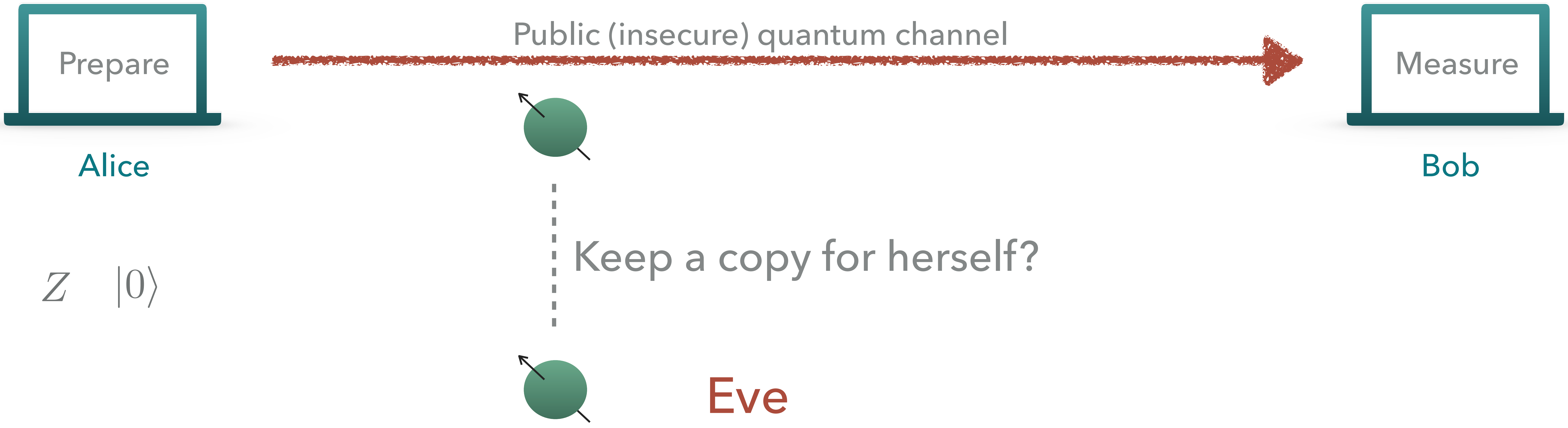
Questions?

BB84: Prepare and Measure

Let's add the adversary (and/or noise) into the picture!

- Eve's goal: gain as much information as possible about the key
  - … without being detected
- The protocol should **abort** when detecting too much interference/noise

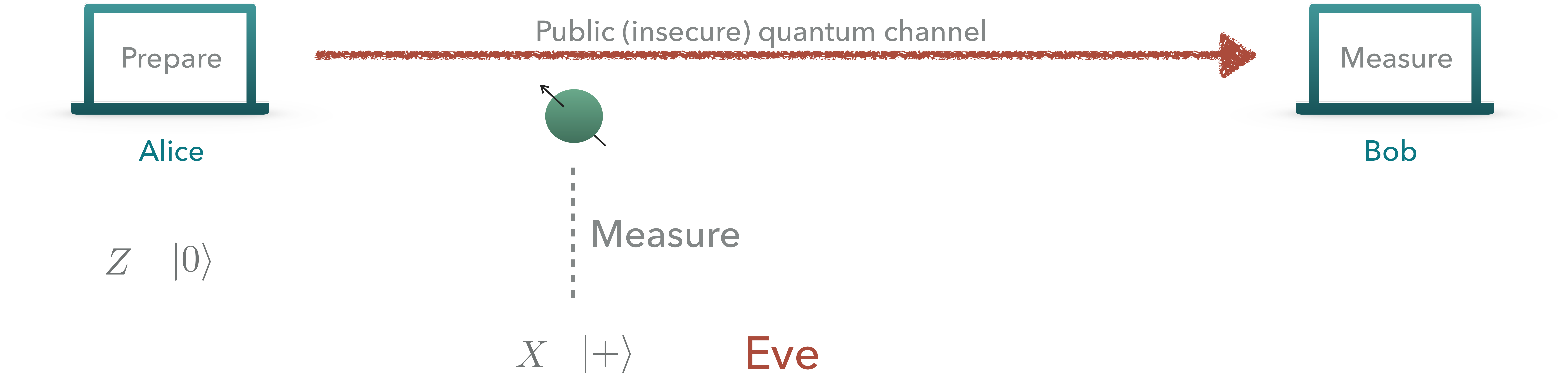
BB84: Intuition



$Z \quad |0\rangle$

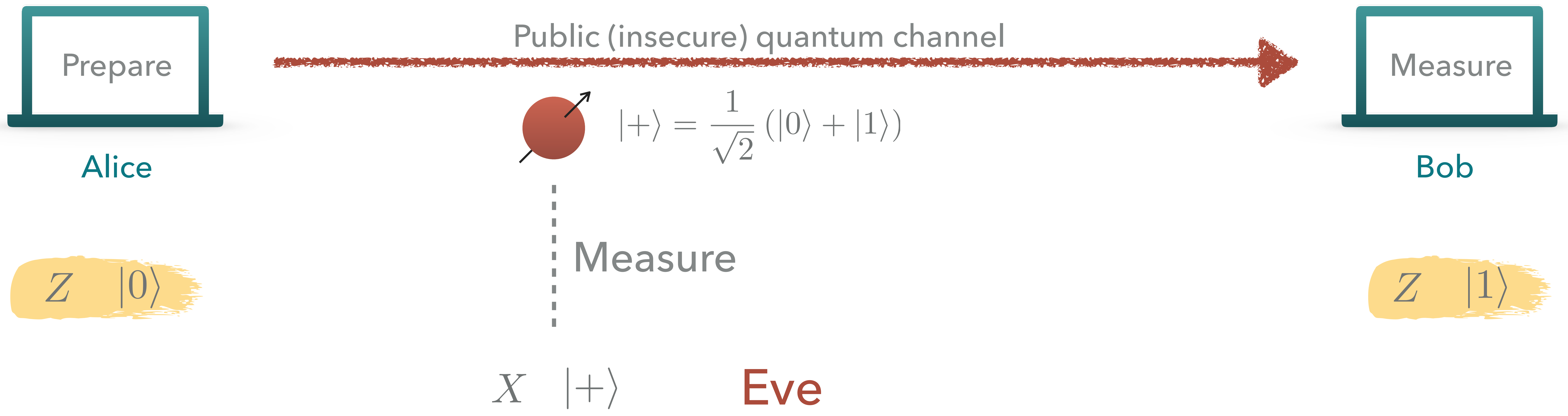
- There are **many** ways for Eve to interact with the state on the channel but…
  - No-cloning

BB84: Intuition



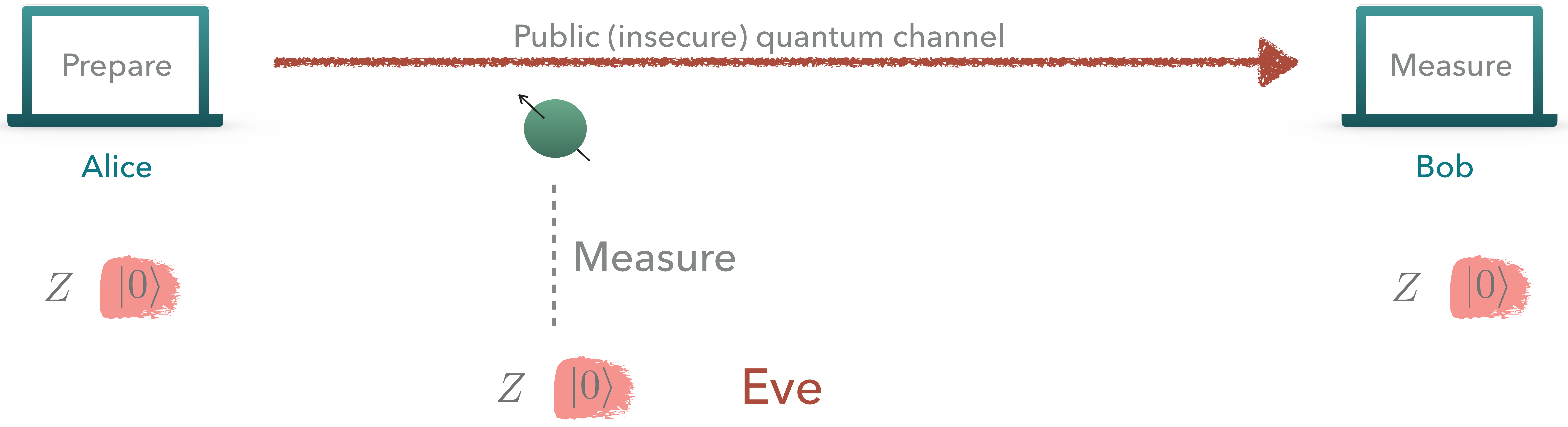
- There are **many** ways for Eve to interact with the state on the channel but…

BB84: Intuition



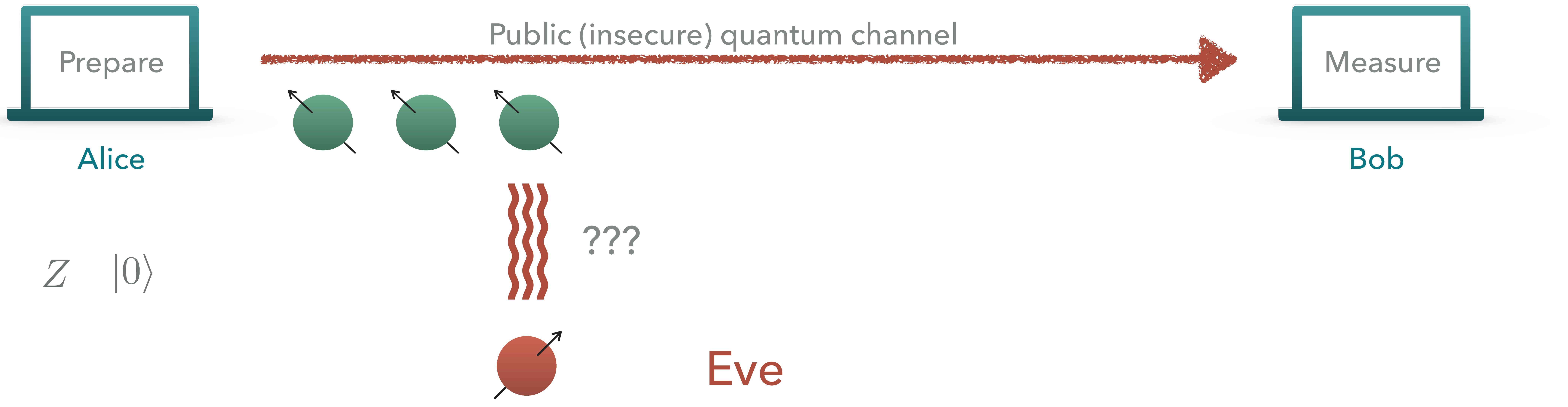
- There are **many** ways for Eve to interact with the state on the channel but…
  - Measurement disturbance $\implies$ Introduction of errors
  - The protocol needs to include a **test** for errors and **abort** if too many are observed (and otherwise correct them)

BB84: Intuition



- There are **many** ways for Eve to interact with the state on the channel but…
  - The protocol needs to include a privacy amplification step

BB84: Intuition

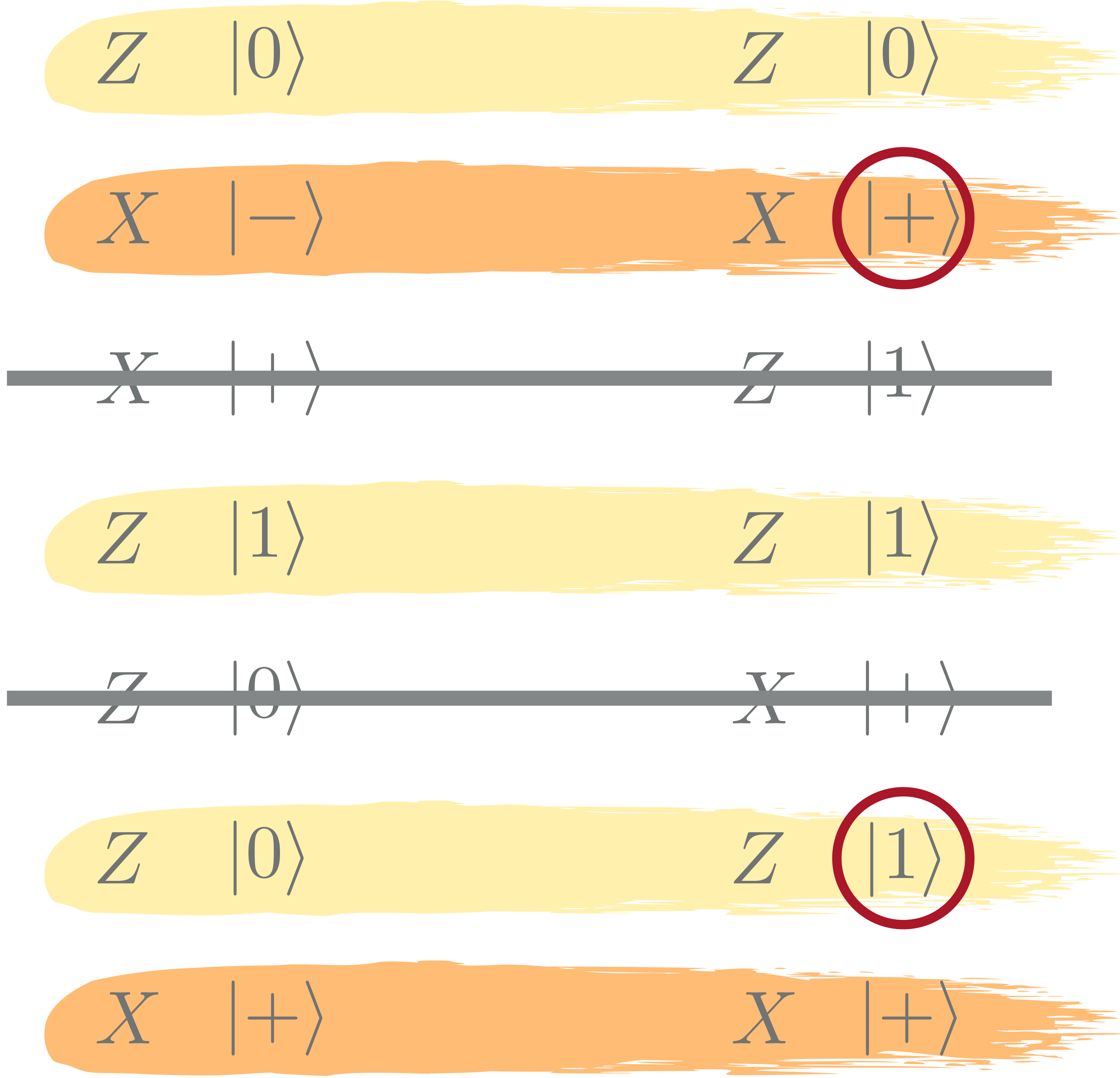


- Eve can do a lot more, e.g., entangle the qubit to her qubits…
- Think many rounds :o
- We'll need to deal with all of this

Questions?

BB84: Prepare and Measure

1. Alice prepares one of the 4 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ at random and sends to Bob.
2. Bob chooses at random a basis to measure and records the outcome.
3. **Sifting:** Alice and Bob publicly announce their chosen bases and keep only the rounds in which they chose the same basis.
4. **Testing for errors:** Alice and Bob check on how many of the rounds in which they both chose the X-basis their outcomes are not identical.
   If the error rate is too high they **abort**.
5. **Classical post-processing:** Alice and Bob apply error correction and privacy amplification on the remaining bits.



Questions?

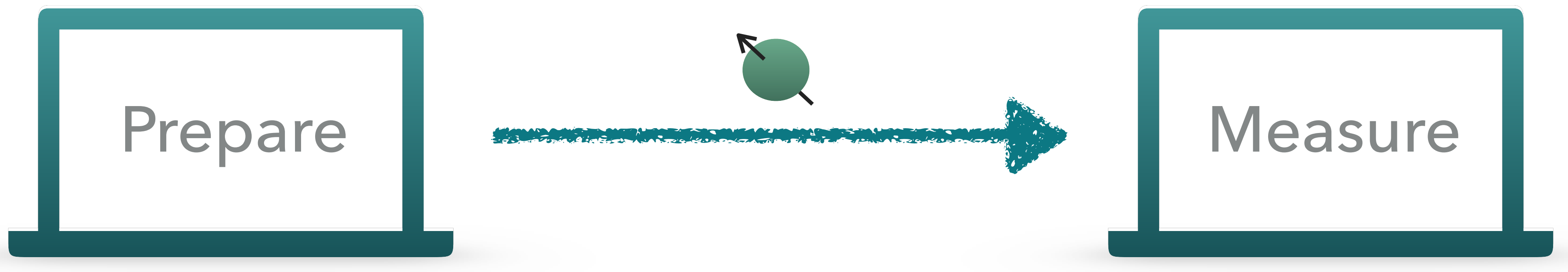
1. BB84 protocol
2. Intuition
3. Ekert 91 protocol
4. Intuition

Security reduction

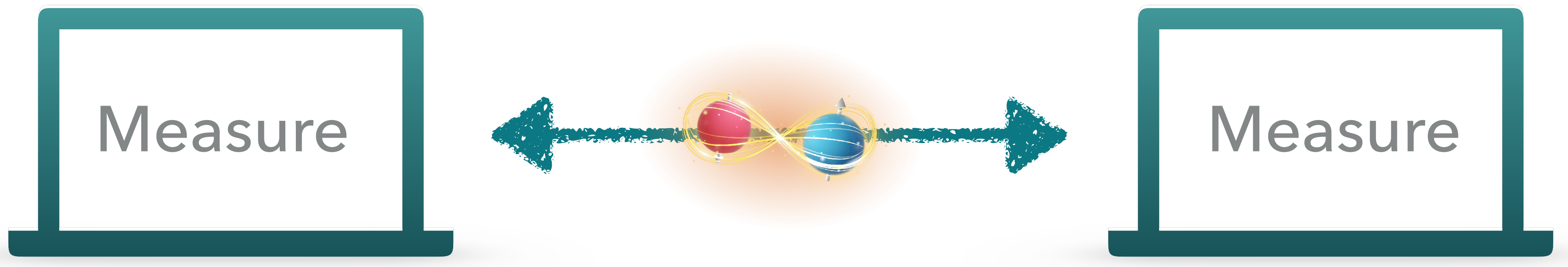
Getting Started

Entanglement-Based Protocols

- The BB84 protocol is a “prepare and measure protocol”

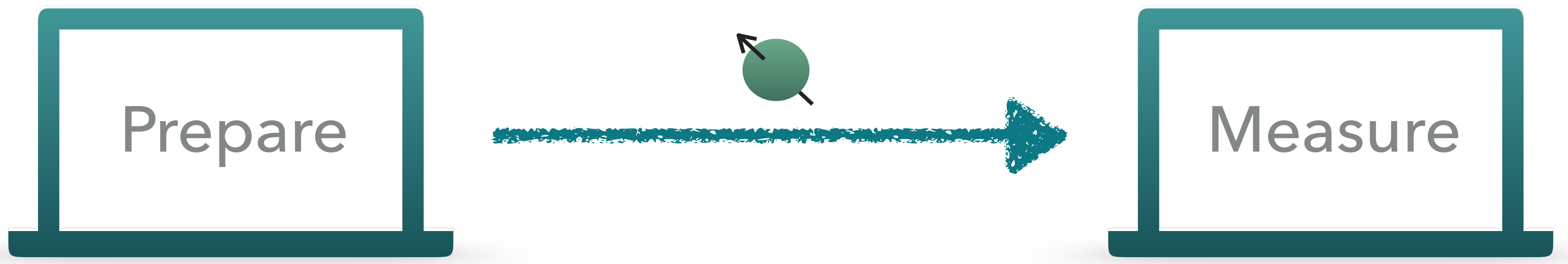


- Entanglement based protocols:
  - Instead of sending quits over a channel Alice and Bob use entangled states

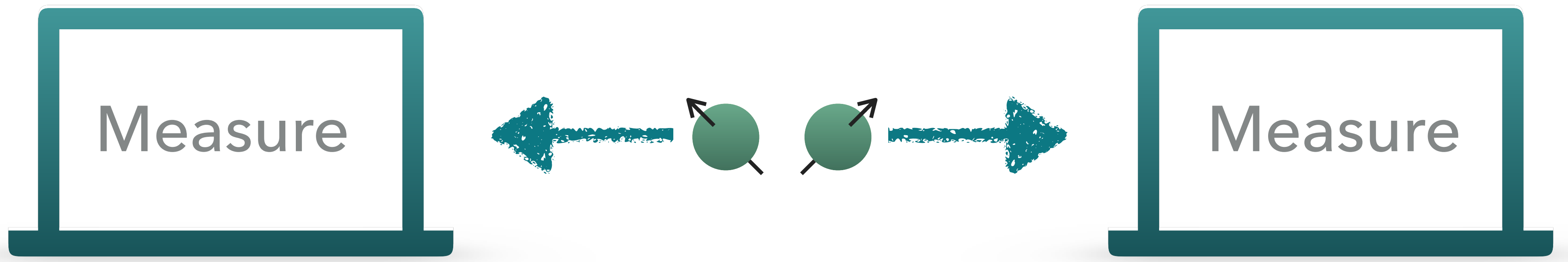


Entanglement-Based Protocols

- The BB84 protocol is a “prepare and measure protocol”



- Entanglement based protocols:
  - Instead of sending quits over a channel Alice and Bob use entangled states



  - Gives us a different point of view

Entanglement-Based Protocols

- Maximally entangled state (EPR state) shared between Alice and Bob

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|--\rangle + |++\rangle)$$

- When measuring in the same basis, Alice and Bob get the same outcomes

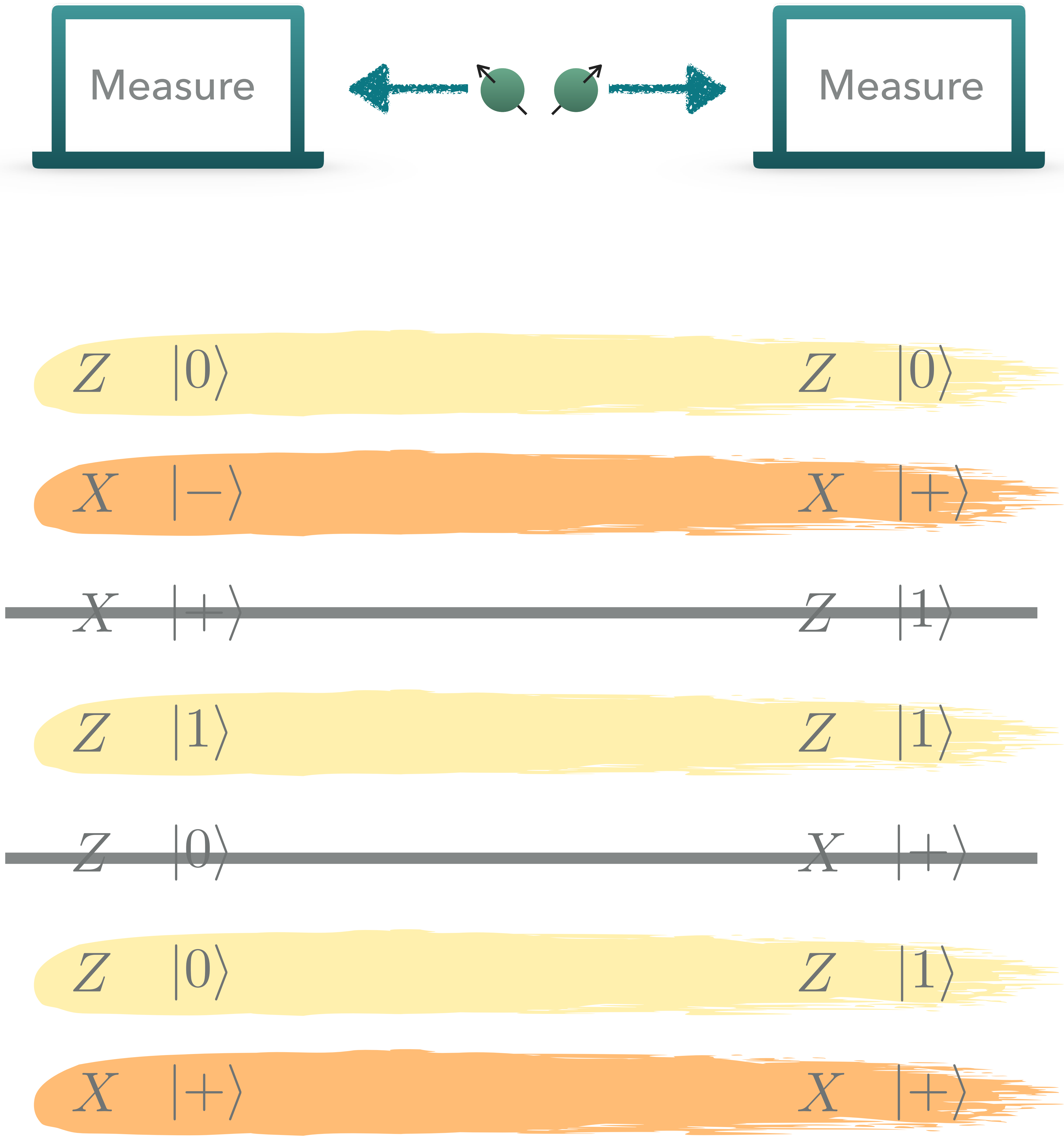
Z	$|0\rangle$	Z	$|0\rangle$
X	$|-\rangle$	X	$|-\rangle$
X	$|+\rangle$	Z	$|1\rangle$
Z	$|1\rangle$	Z	$|1\rangle$
Z	$|0\rangle$	X	$|+\rangle$

Same statistics as in the BB84 protocol!

Can't be done without entanglement

Ekert 91 Protocol

- Ekert 91 protocol: same as BB84 but using **distribution of entanglement**
  1. Alice and Bob get their share of the entangled state
  2. They each choose a basis to measure at random
  3. Sifting
  4. Testing for errors
  5. Classical post-processing

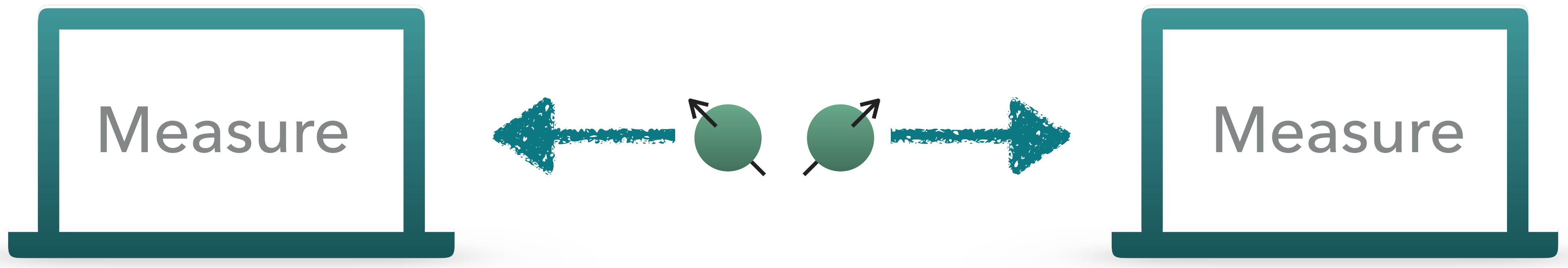


Ekert 91: Intuition

- Honest noiseless case:
  - Distribution of the maximally entangled state $|\Phi^+\rangle_{AB}$
  - Each outcomes achieved w.p. 0.5
  - Pure state
    - $\Rightarrow$ Any purification takes the form

$$|\Phi^+\rangle_{AB} \otimes |\psi\rangle_E$$

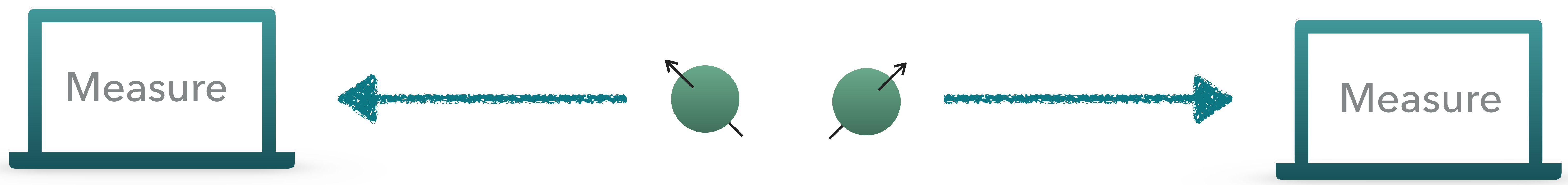
    - $\Rightarrow$ Completely independent of the rest of the world (including Eve)



Z	$\|0\rangle$	Z	$\|0\rangle$
X	$\|-\rangle$	X	$\|+\rangle$
~~X~~	~~$\|+\rangle$~~	~~Z~~	~~$\|1\rangle$~~
Z	$\|1\rangle$	Z	$\|1\rangle$
~~Z~~	~~$\|0\rangle$~~	~~X~~	~~$\|+\rangle$~~
Z	$\|0\rangle$	Z	$\|1\rangle$
X	$\|+\rangle$	X	$\|+\rangle$

Ekert 91: Intuition

- Let’s bring Eve into the picture

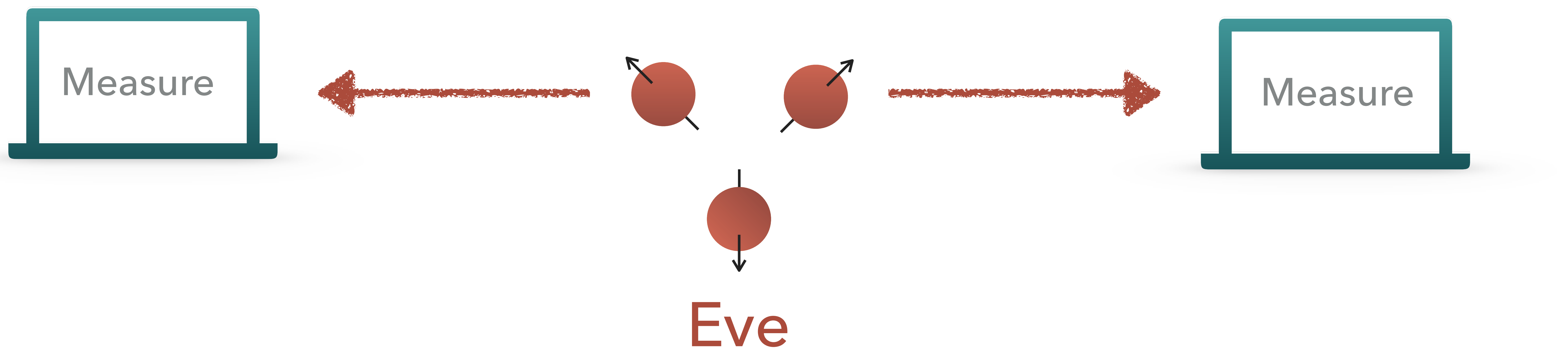


Eve

Ekert 91: Intuition

Questions?

- Let's bring Eve into the picture

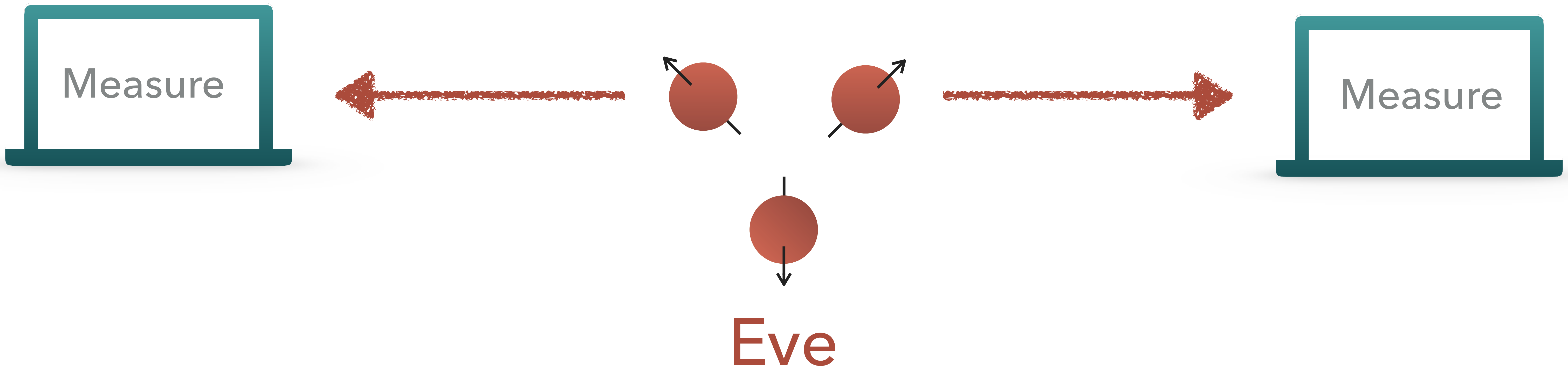


- Alice, Bob and Eve share a tripartite state $|\psi\rangle_{ABE}$
    - Alice and Bob's state $\rho_{AB} = \mathrm{Tr}_E \left(|\psi\rangle_{ABE} \right)$ (density matrix; partial trace)
    - Eve is holding the purification = most powerful adversary

Compare to:
$|\Phi^+\rangle_{AB} \otimes |\psi\rangle_E$

Ekert 91: Intuition

- Alice, Bob and Eve share a tripartite state $|\psi\rangle_{ABE}$
- Ideally $|\Phi^+\rangle_{AB} \otimes |\psi\rangle_E$
- Quantum "features" of entanglement:
  - Monogamy of entanglement
  - Uncertainty relations (third lecture)



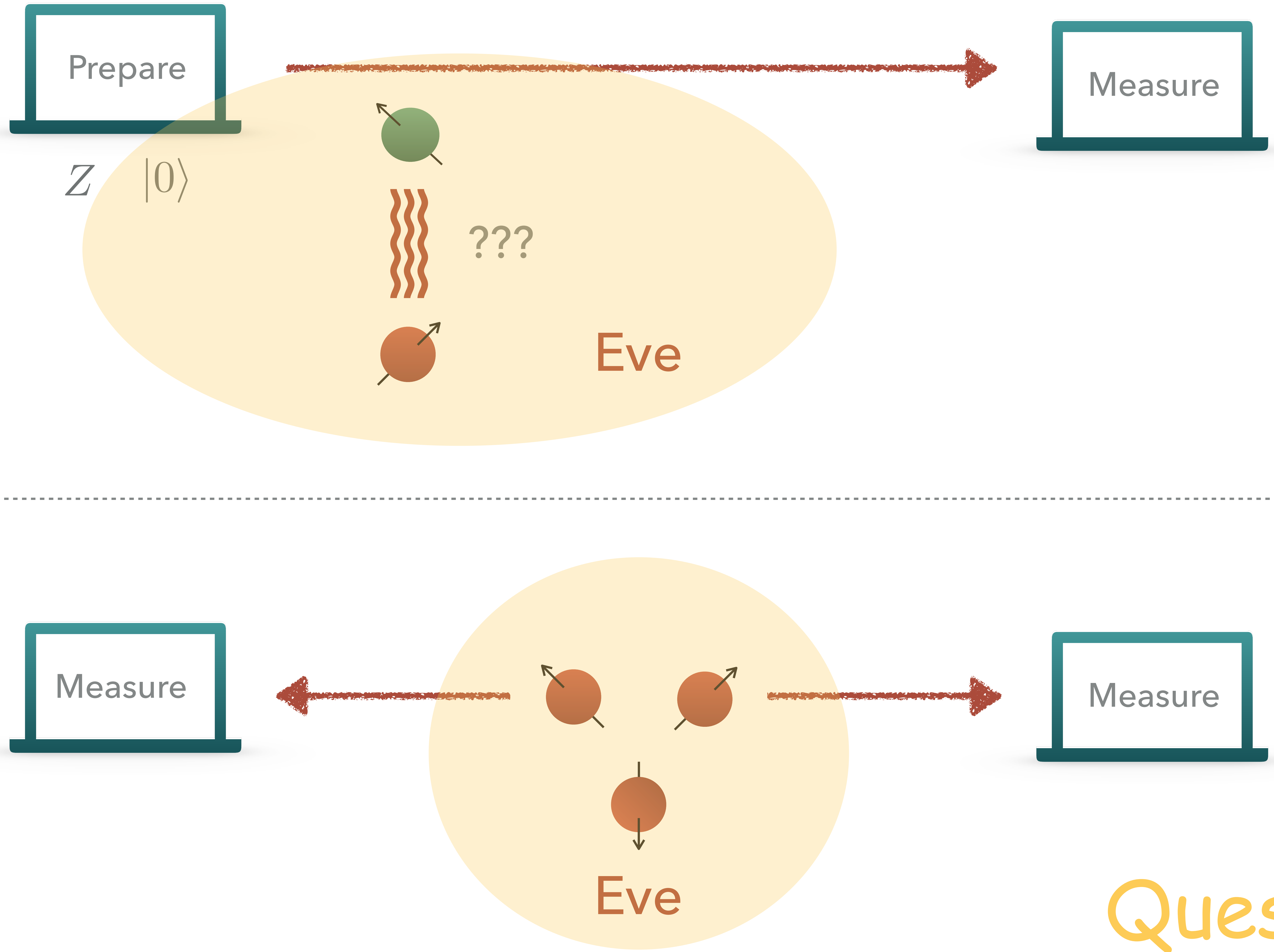
Security Reduction

BB84

Security reduction

Ekert 91

- Adversary is stronger
- Mathematically cleaner



Questions?

In the Following Lectures

- QKD security definition
  - What does it mean to prove security?
  - Quantum abstract cryptography framework
- Security proof
  - Quantum-proof extractors
  - Where the laws of quantum physics help us
- A different model for QKD– device-independent QKD (stronger adversary)

Quantum Key Distribution

BIU Winter School on Quantum Cryptography | February 15, 2021

Rotem Arnon-Friedman | Weizmann Institute of Science

Outline

- Lecture 1:
  - Introduction
  - BB84 and Ekert91 protocols
- Lecture 2:
  - QKD security definition
  - Quantum-proof randomness extractors
- Lecture 3:
  - Security proof (the main parts)
  - Device-independent quantum key distribution

Security Definition (Informal)

- What does it mean to prove security?
  - If "things go sufficiently well"– we would like to produce a key:
    - Identical keys for Alice and Bob
    - Unknown to Eve
  - If "things don't go well" (too much noise / too active adversary)– we would like to detect it and abort
  - The protocol can be **implemented**

Correctness

Secrecy

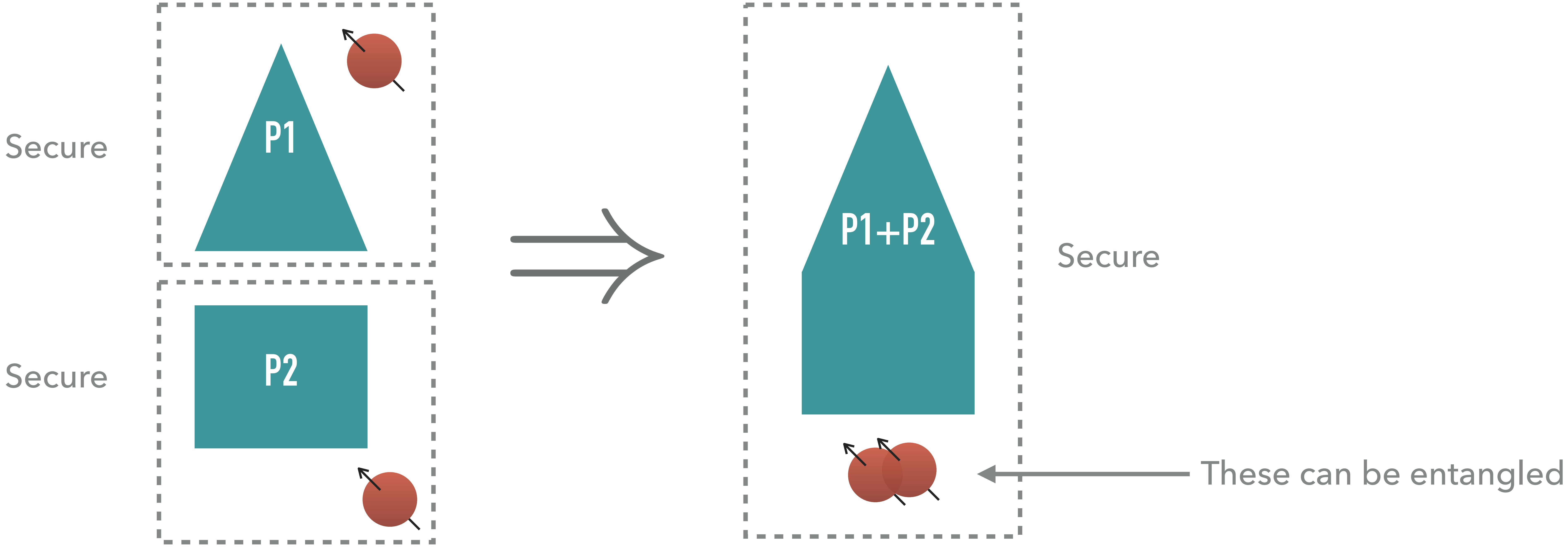
Soundness

Completeness (noise-tolerance)

Security Definition (Informal)

How do we make this **formal**?

Quantum compassable security



1. Composable security
2. Equivalence to trace distance definition

Security Definition

Composable Security

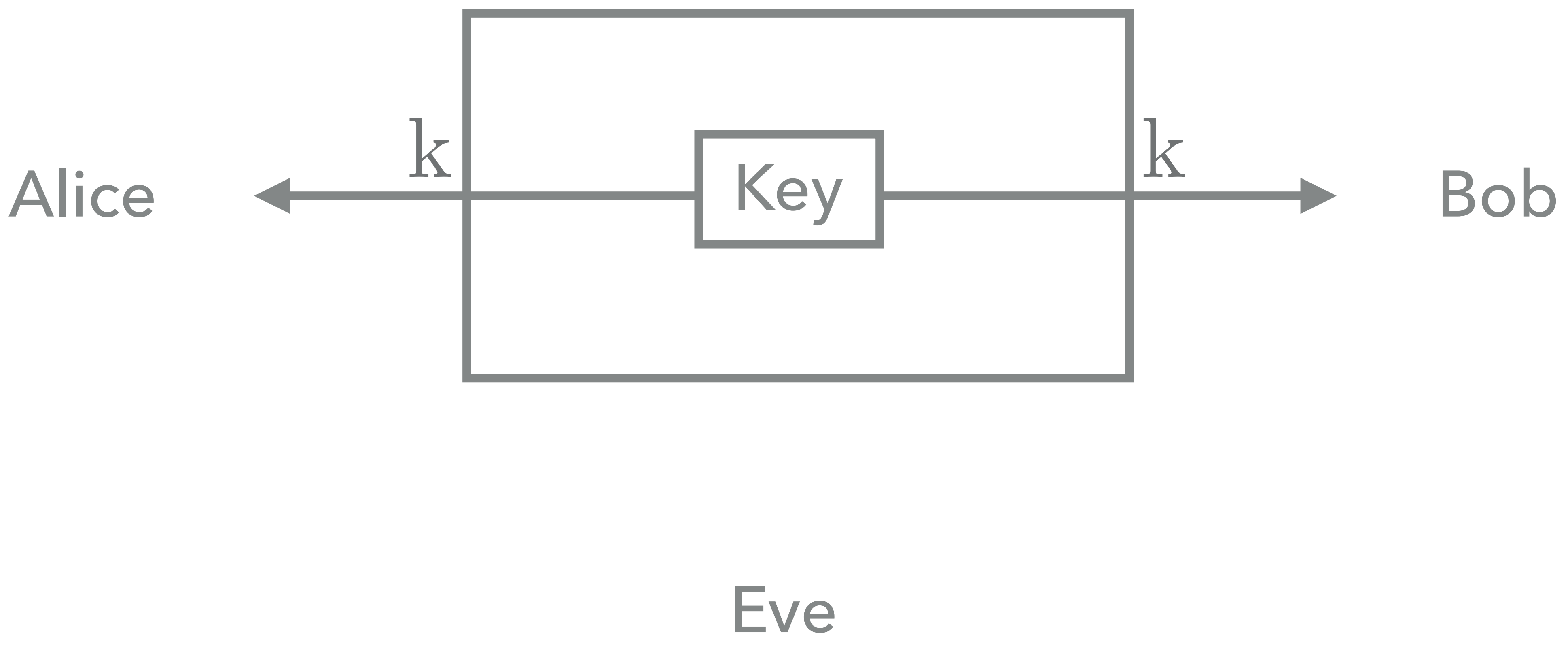
- Abstract cryptography framework
- Complete mathematical framework
- Important “steps”:
  1. Model the ideal system
  2. Identify the resources and model the real system
  3. Quantum distinguisher– try to distinguish the real from ideal
- Gives a precise description of what we achieve
- (In the past a weaker security definition was used without anyone noticing!)

Ideal System

Ideal key distribution resource

$$|K| = \ell$$

$$K \sim U_\ell$$

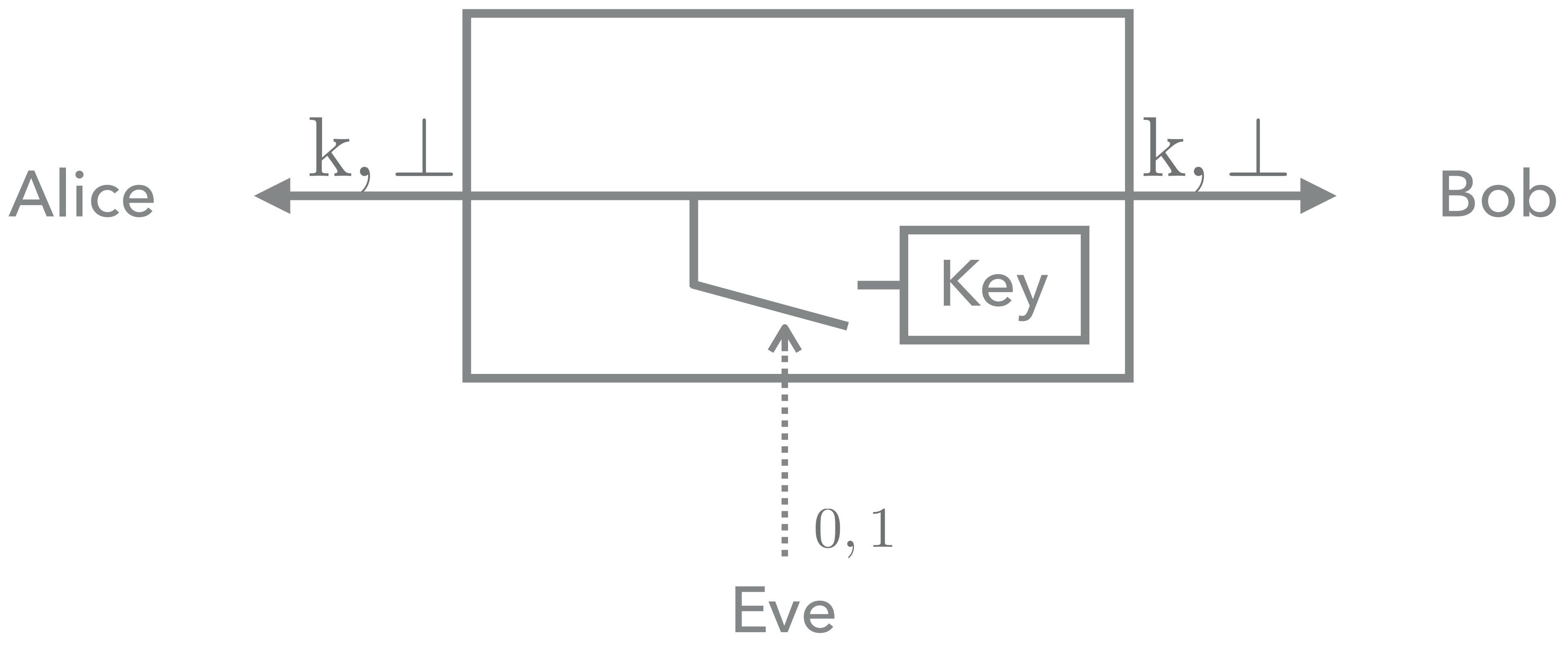


Ideal System

Ideal key distribution resource

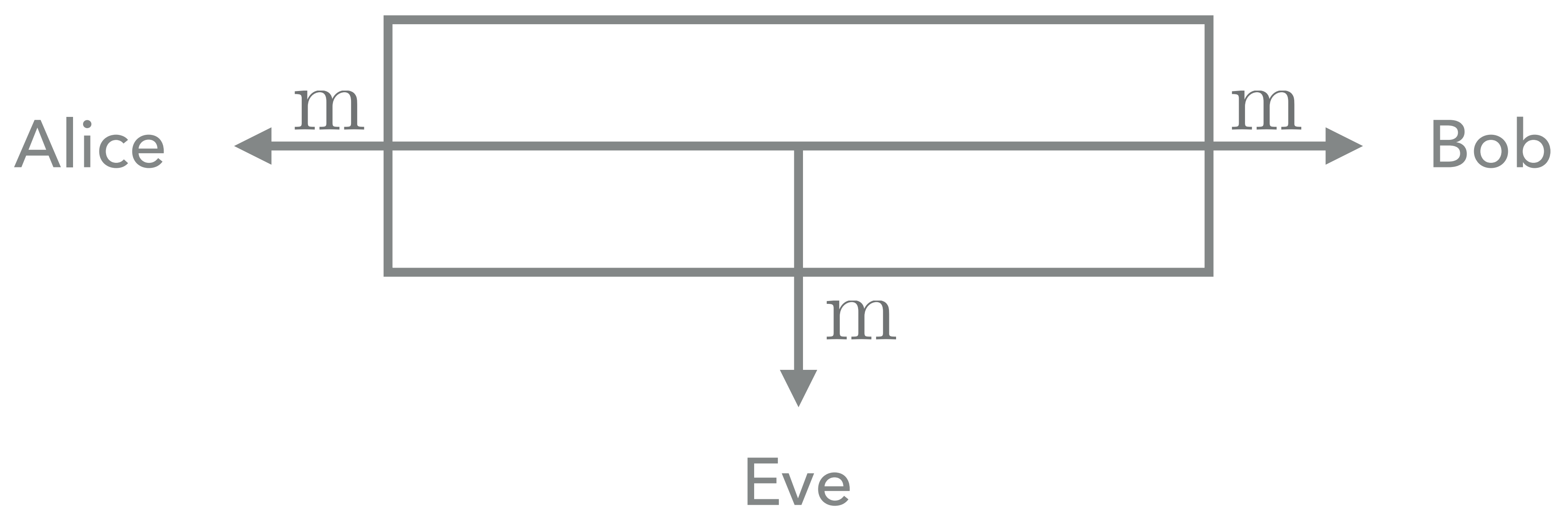
$$|K| = \ell$$

$$K \sim U_\ell$$

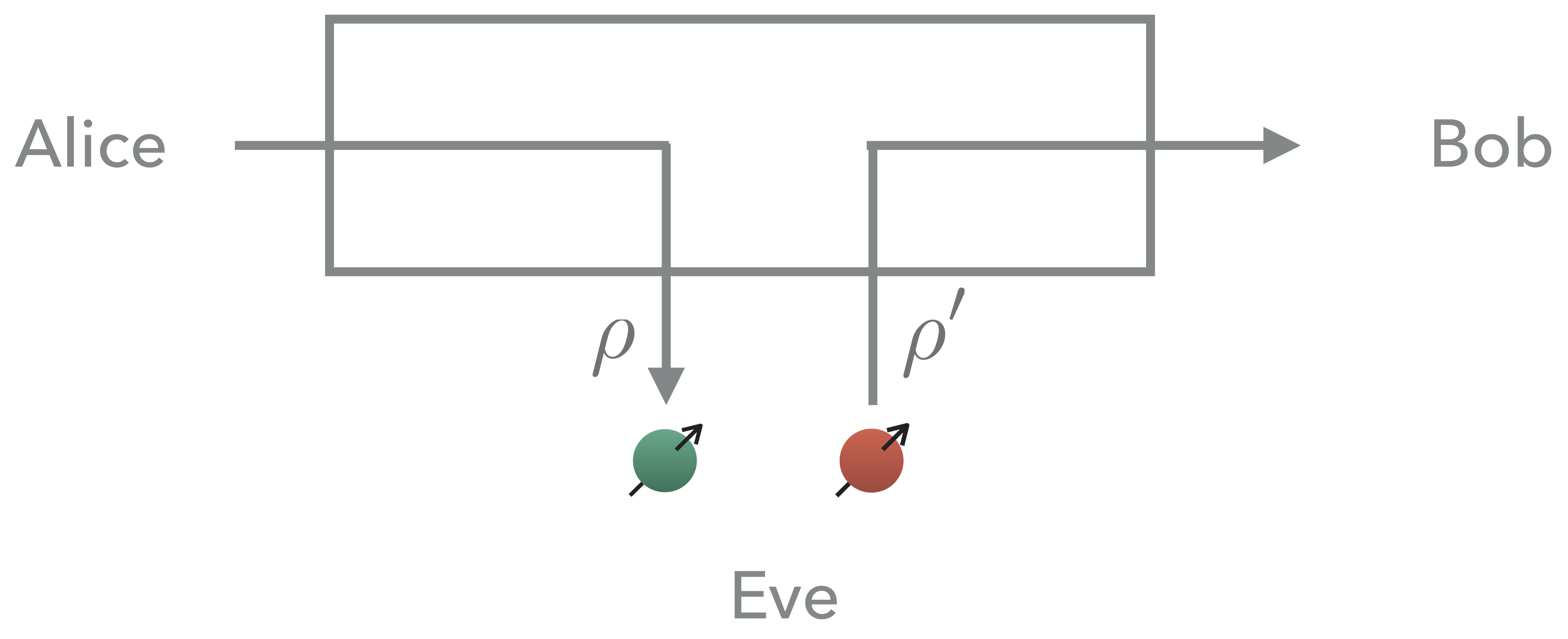


Real System

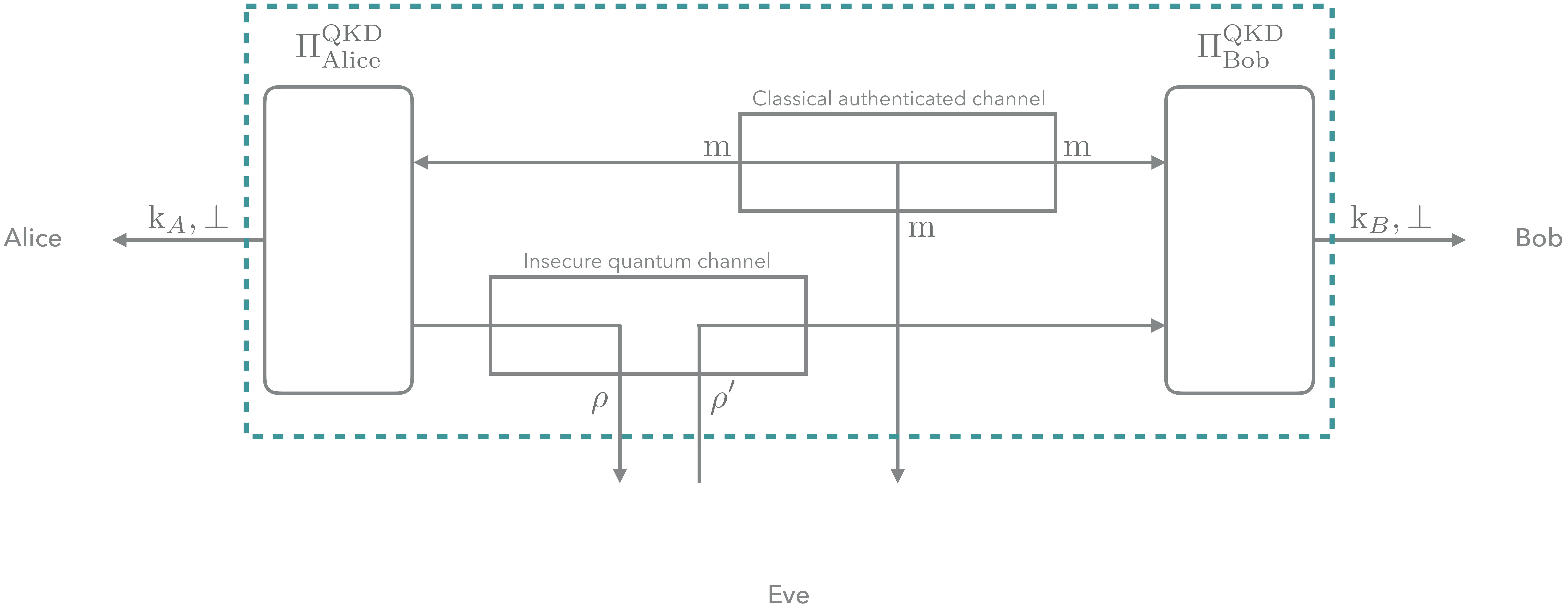
- Resources (our building blocks):
  - Authenticated classical channel



  - Insecure quantum channel



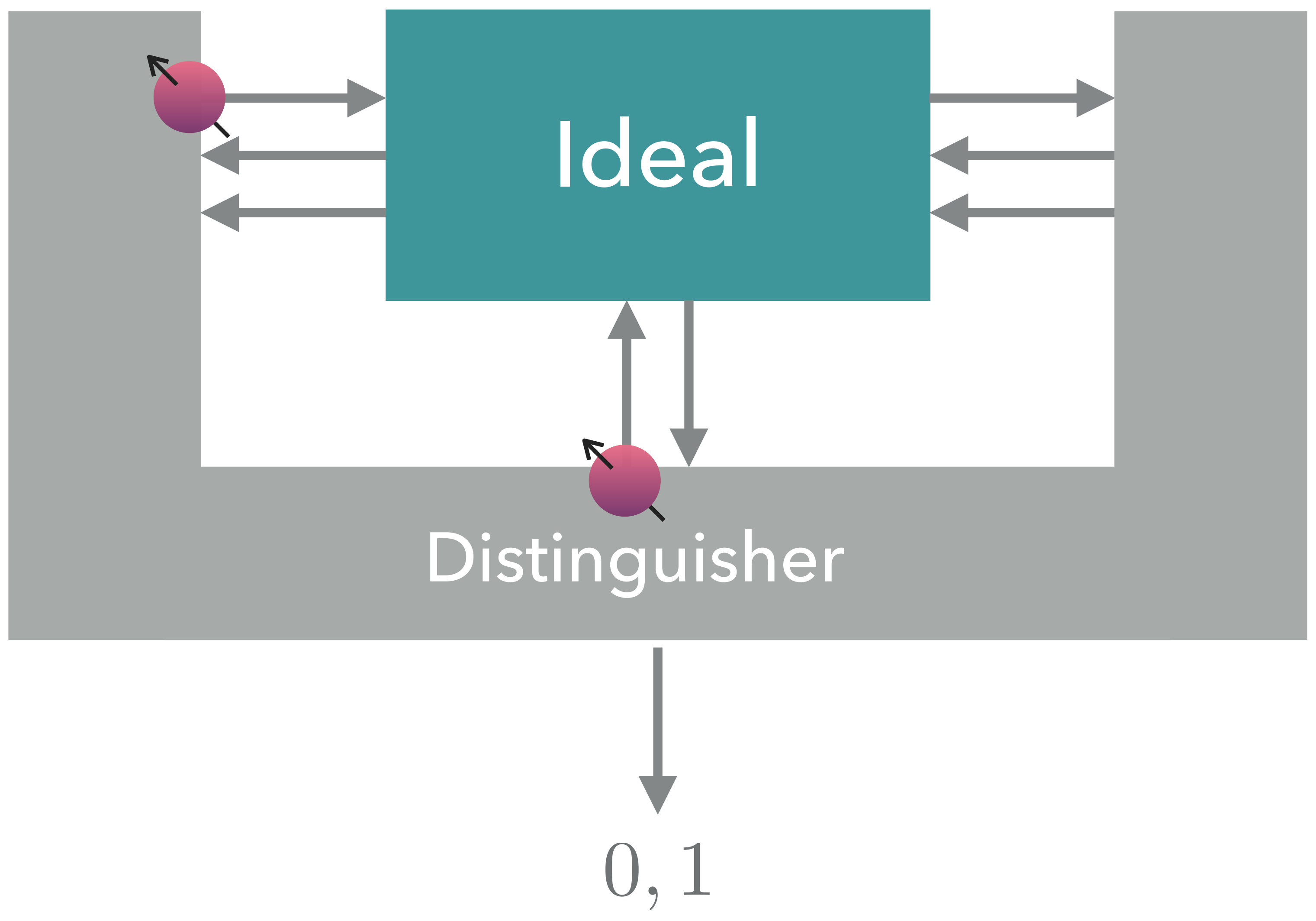
Real System

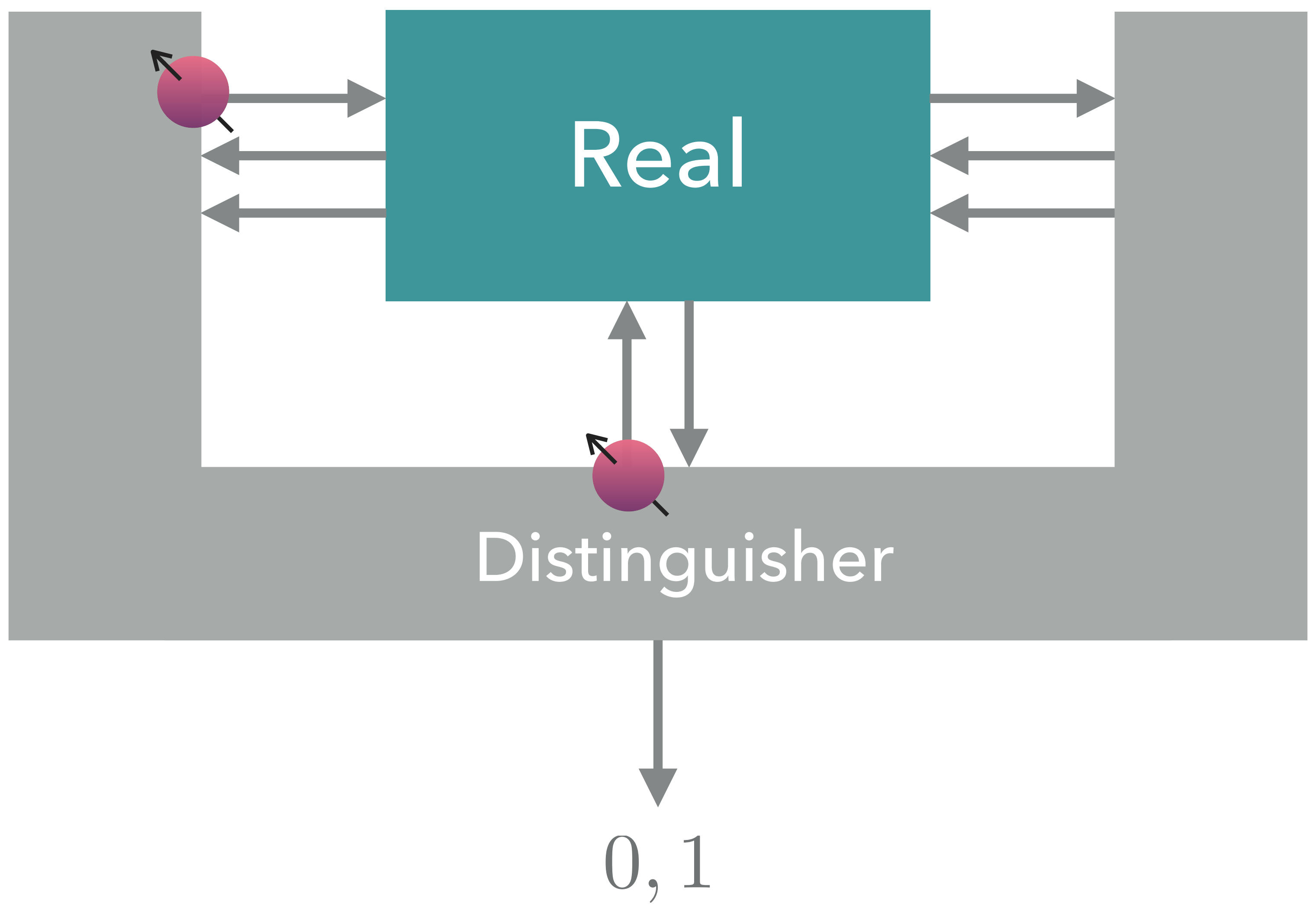


Π^{QKD}_{Alice}
Π^{QKD}_{Bob}
Classical authenticated channel
m
m
m
Alice
$k_A, \perp$
$k_B, \perp$
Bob
Insecure quantum channel
ρ
ρ'
Eve

Distinguisher

- The real system is secure if it's indistinguishable from the ideal system



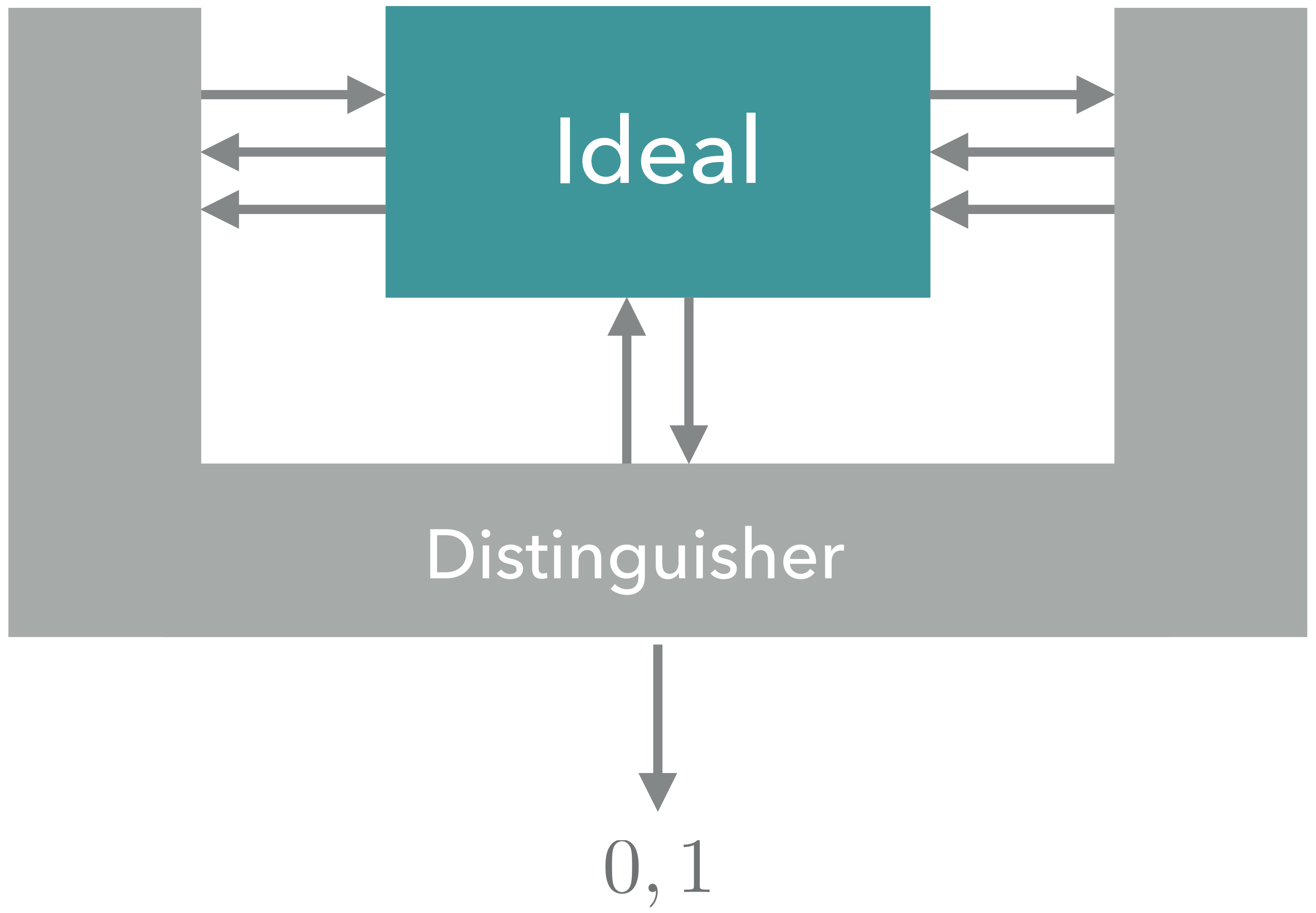


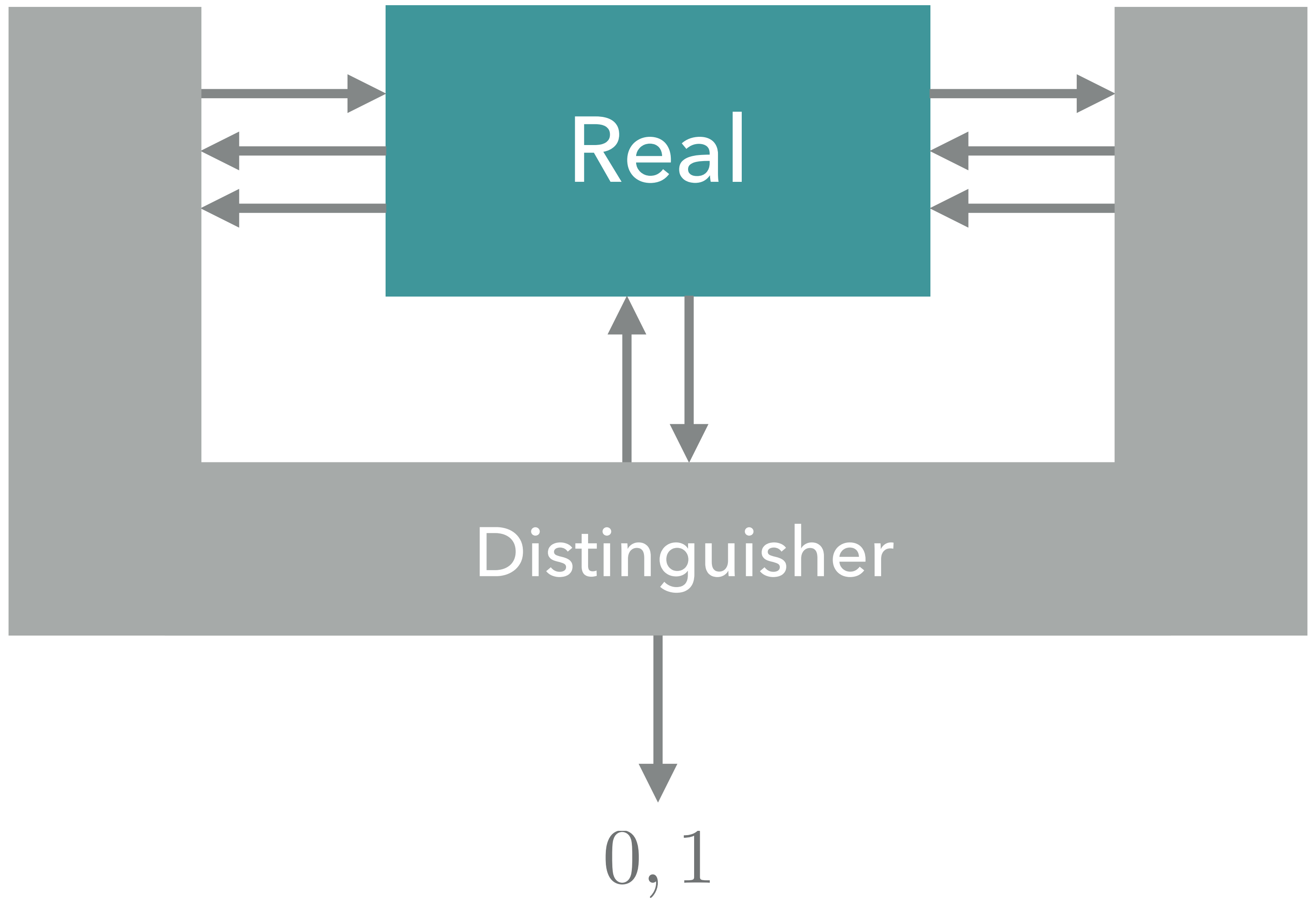
- Distinguishing advantage $d(\mathcal{I}, \mathcal{R}) = \sup_D |\Pr[D(\mathcal{I}) = 1] - \Pr[D(\mathcal{R}) = 1]|$

1. Quantum distinguisher ("quantum combs")
2. No "division" to parties (crucial for composability)
3. Everything is finite (no "poly", "neg"...)

Distinguisher

- The real system is secure if it's indistinguishable from the ideal system

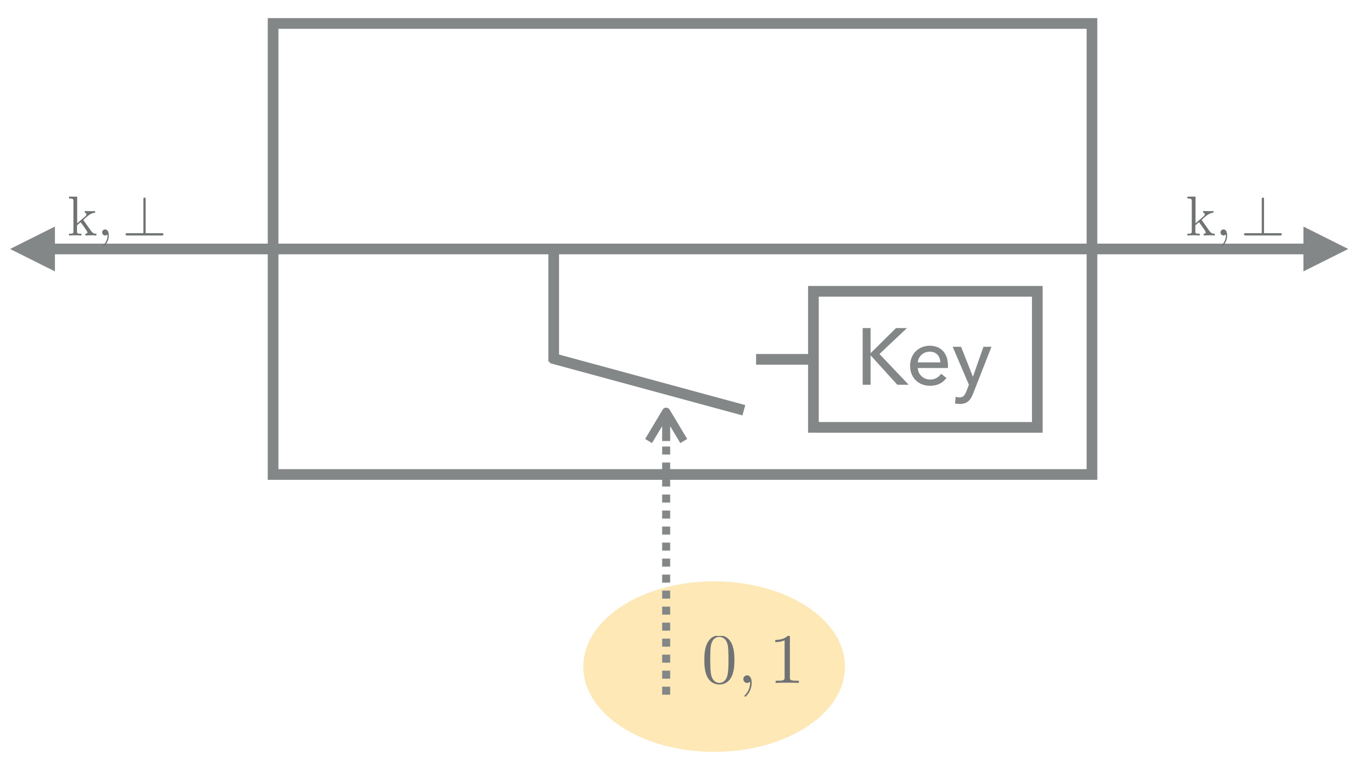




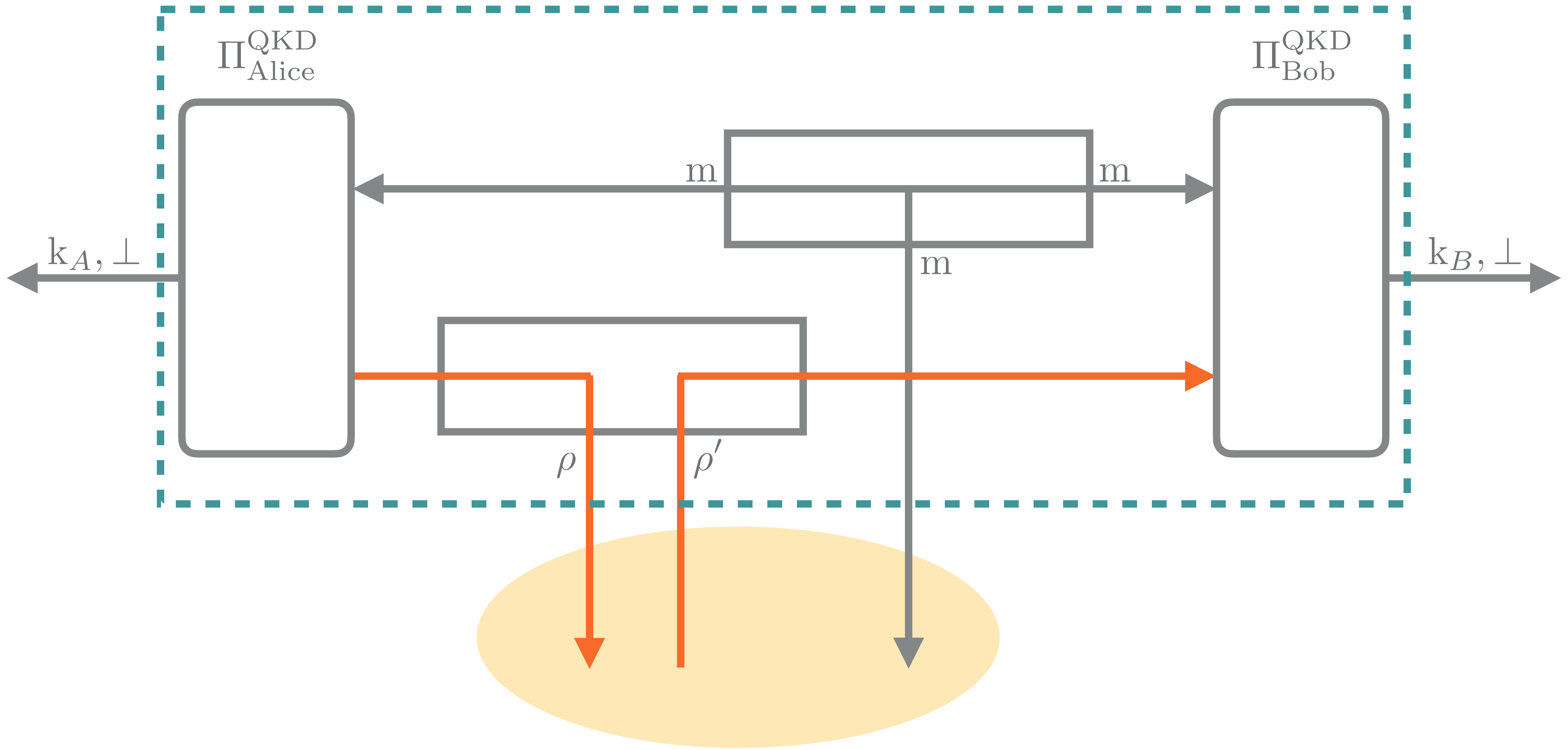
- Distinguishing advantage $d(\mathcal{I}, \mathcal{R}) = \sup_D |\Pr[D(\mathcal{I}) = 1] - \Pr[D(\mathcal{R}) = 1]|$
- Security: $d(\mathcal{I}, \mathcal{R}) \leq \varepsilon$
  - (Sort of...)

Distinguisher

Ideal system

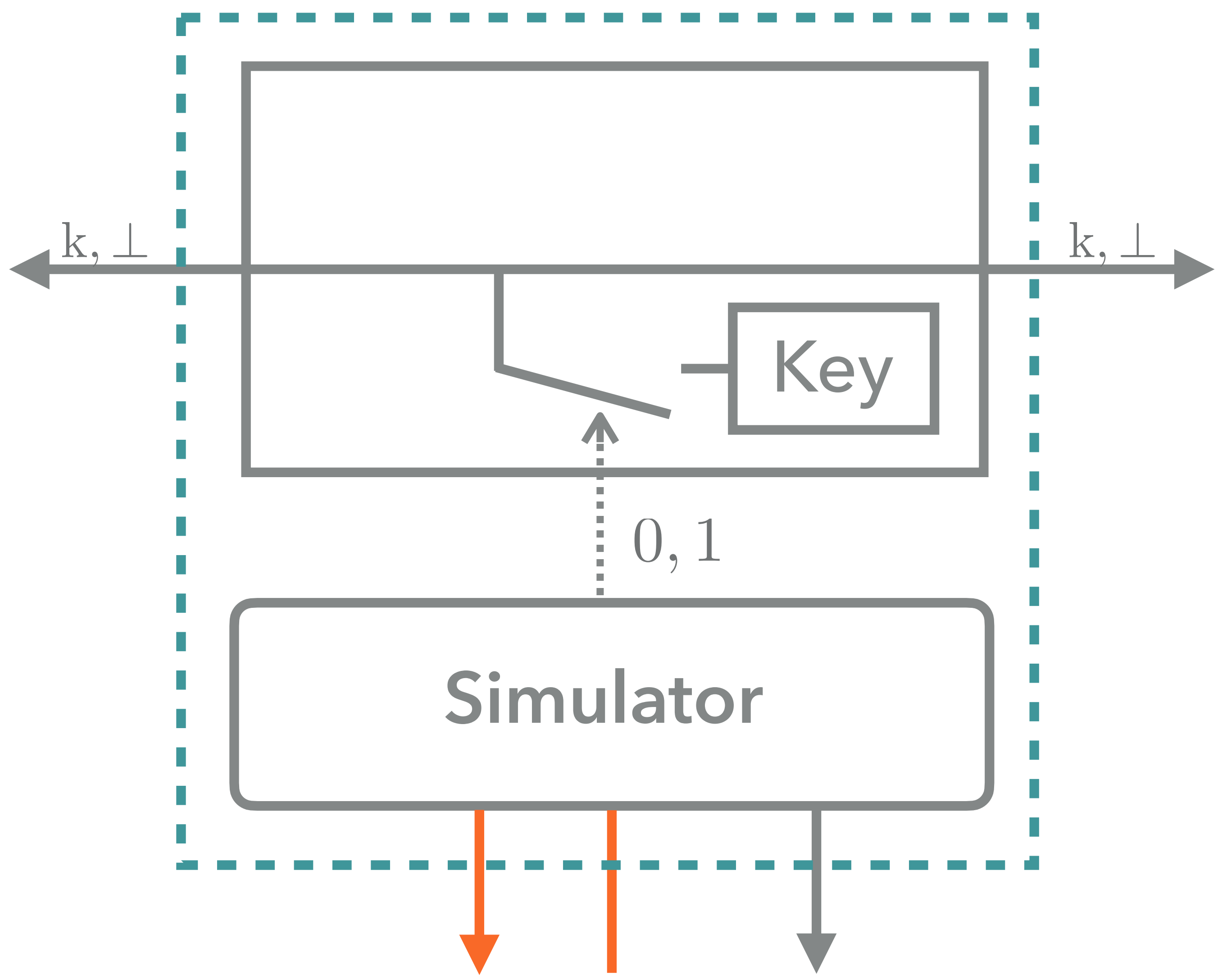


Real system

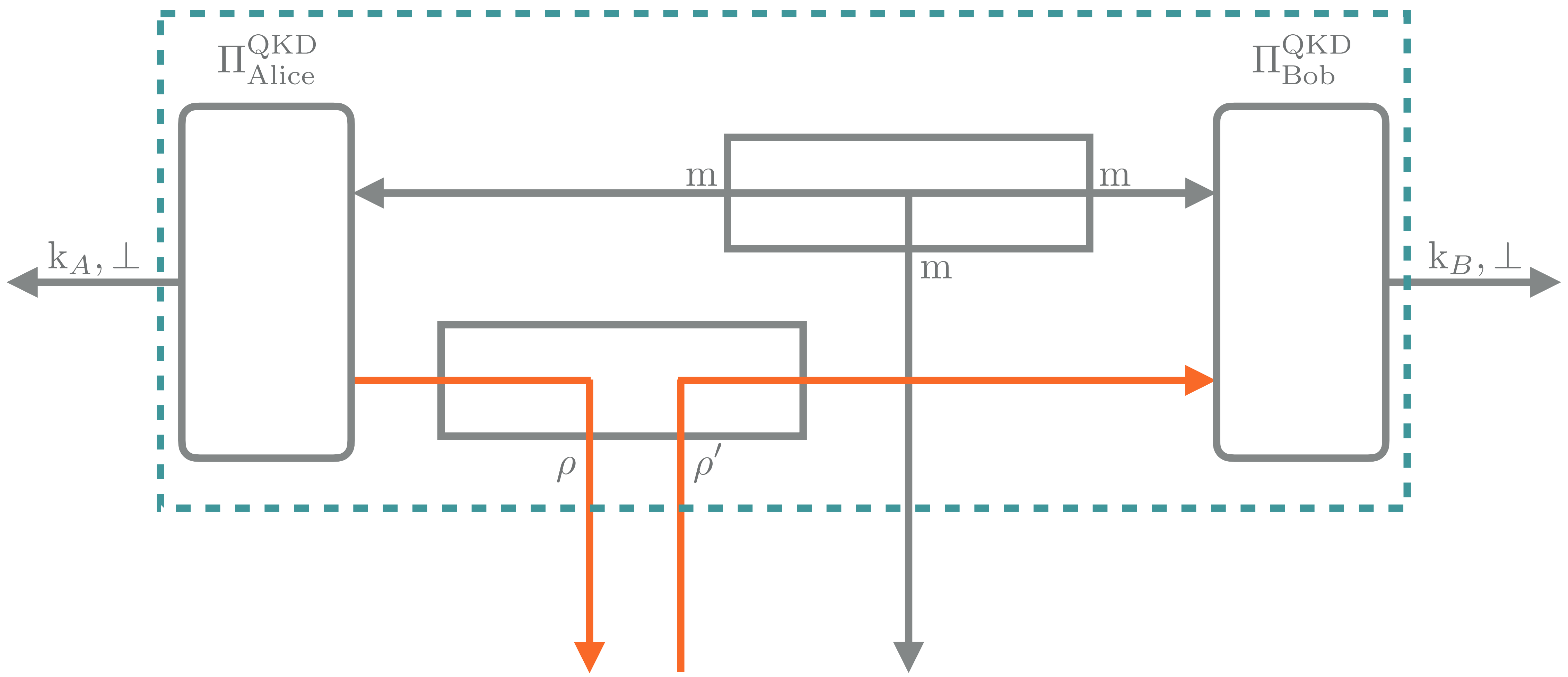


Distinguisher

Ideal system



Real system



- The protocol is secure if there exists a simulator such that $d(\mathcal{I}, \mathcal{R}) \leq \varepsilon$
- It's clear what we're proving
- As it turns out, it's equivalent to another statement

Questions?

Security Definition

- The definitions that arise from the composable security framework were shown to be equivalent to another widely-used definition
- Recall our informal definition:
  - If "things go sufficiently well"– we would like to produce a key:
    - Identical keys for Alice and Bob
    - Unknown to Eve
  - If "things don't go well" we would like to detect it and abort
  - The protocol can be **implemented**

Correctness

Secrecy

Soundness

Completeness (noise-tolerance)

Security Definition

- Def. [Correctness]: A protocol is $\varepsilon_{\text{corr}}$-correct, if $\Pr\left(K_A \neq K_B\right) \leq \varepsilon_{\text{corr}}$
- Def. [Secrecy]: A protocol is ε_{sec}-secret if

$$\underbrace{(1 - \Pr(\text{abort}))}_{\text{If we almost always abort, the key is trivially secret}} \|\rho_{K_A E} - \rho_{U_\ell} \otimes \rho_E\| \leq \varepsilon_{\text{sec}} \qquad |\mathrm{K}| = \ell$$

If we almost always abort, the key is trivially secret

Security Definition

- Def. [Correctness]: A protocol is $\varepsilon_{\text{corr}}$-correct, if $\Pr\left(K_A \neq K_B\right) \leq \varepsilon_{\text{corr}}$
- Def. [Secrecy]: A protocol is ε_{sec}-secret if

$$(1 - \Pr(\text{abort})) \, \underbrace{\left\|\rho_{K_A E} - \rho_{U_\ell} \otimes \rho_E\right\|}_{} \leq \varepsilon_{\text{sec}} \qquad |\mathrm{K}| = \ell$$

Trace distance between two states: the real and ideal (want this to be small)

Security Definition

- Def. [Correctness]: A protocol is $\varepsilon_{\mathrm{corr}}$-correct, if $\Pr(K_A \neq K_B) \leq \varepsilon_{\mathrm{corr}}$
- Def. [Secrecy]: A protocol is $\varepsilon_{\mathrm{sec}}$-secret if

$$(1 - \Pr(\mathrm{abort})) \, \|\rho_{K_A E} - \rho_{U_\ell} \otimes \rho_E\| \leq \varepsilon_{\mathrm{sec}}$$

$|\mathrm{K}| = \ell$

Real state of Alice and Eve at the end of the protocol (when not aborting)

Uniform key

Eve's quantum state

Security Definition

- Def. [Correctness]: A protocol is $\varepsilon_{\text{corr}}$-correct, if $\Pr\left(K_A \neq K_B\right) \leq \varepsilon_{\text{corr}}$
- Def. [Secrecy]: A protocol is ε_{sec}-secret if

$$(1 - \Pr(\text{abort}))\, \|\rho_{K_A E} - \rho_{U_\ell} \otimes \rho_E\| \leq \varepsilon_{\text{sec}}$$

$|\mathrm{K}| = \ell$

- If a protocol is $\varepsilon_{\text{corr}}$-correct and ε_{sec}-secret, then it is $(\varepsilon_{\text{corr}} + \varepsilon_{\text{sec}})$**-correct-and-secret**
- Def. [Security]: A protocol is $\left(\varepsilon^s_{\text{QKD}}, \varepsilon^c_{\text{QKD}}, \ell\right)$**-secure** if:
  1. (Soundness) The protocols is $\varepsilon^s_{\text{QKD}}$-correct-and-secret
  2. (Completeness) There exists a quantum apparatus that implements the protocol such that the probability of aborting is at most $\varepsilon^c_{\text{QKD}}$

Security Definition

- Def. [Correctness]: A protocol is $\varepsilon_{\text{corr}}$-correct, if $\Pr(K_A \neq K_B) \leq \varepsilon_{\text{corr}}$
- Def. [S

$|\mathrm{K}| = \ell$

- If a pr ct-
  and-s
- Def. [S
  1. (S
  2. (C the
     protocol such that the probability of aborting is at most $\varepsilon^{c}_{\text{QKD}}$

- This security definition of QKD was proven to be **equivalent** to the composable security definition we've seen before
- Justifies using this definition
- Things can go wrong otherwise…

Security Definition

- Def. [Secrecy]: A protocol is ε_{sec}-secret if

$$(1 - \Pr(\text{abort})) \left\| \rho_{K_A E} - \rho_{U_\ell} \otimes \rho_E \right\| \leq \varepsilon_{\text{sec}} \qquad |\mathrm{K}| = \ell$$

Trace distance between two states: the real and ideal (want this to be small)

- To make this small we use a privacy amplification step in the protocols

Questions?

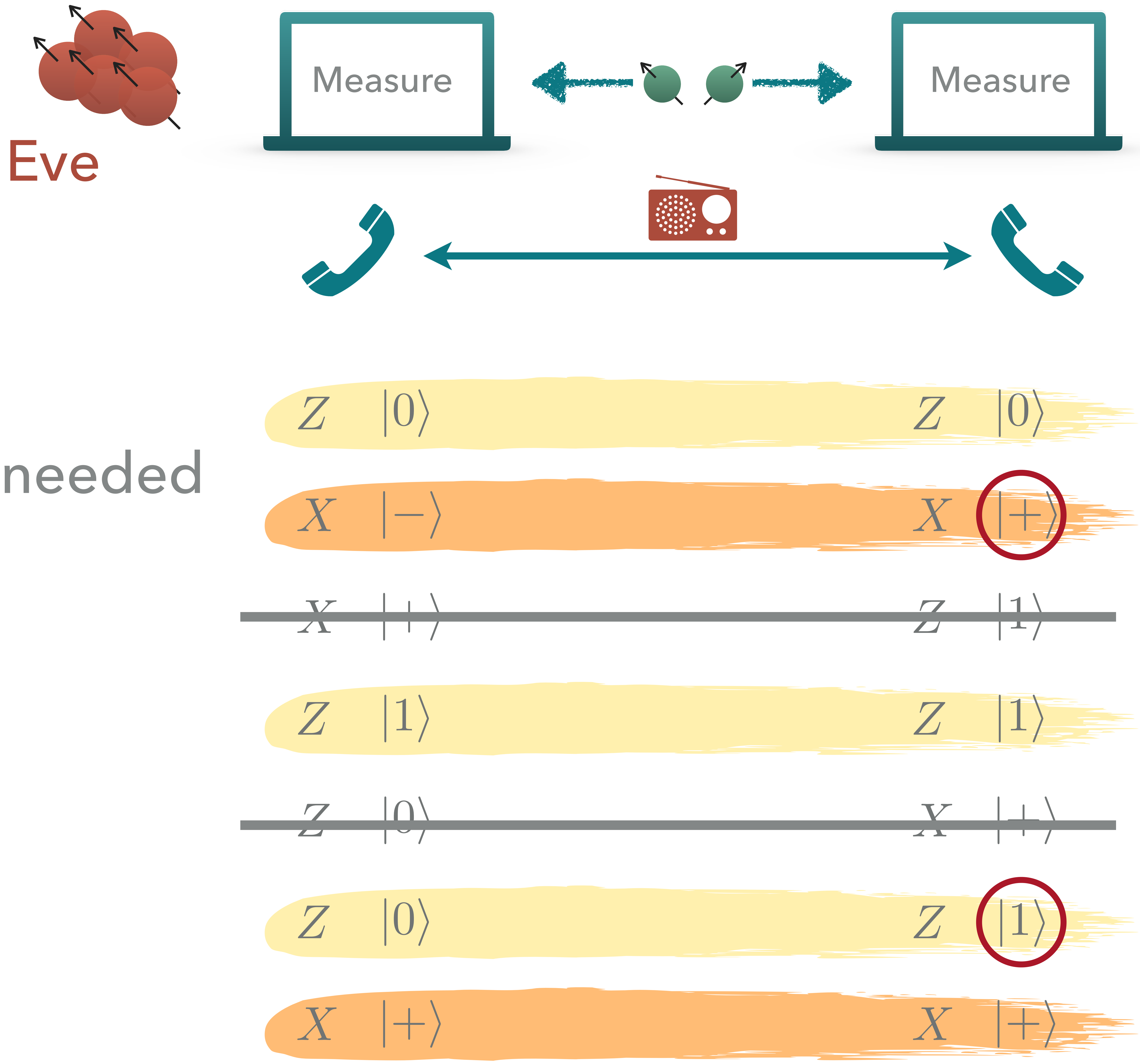
Post-quantum cryptography
Information-theoretic

Privacy Amplification

Quantum-Proof Randomness Extractors

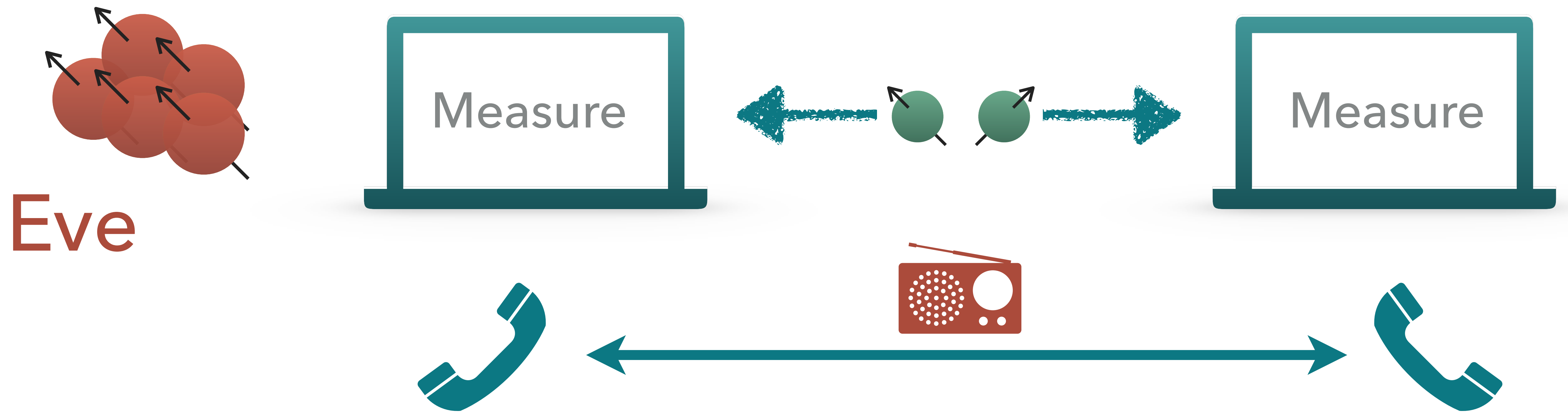
QKD

- Data generation
  - Measuring the quantum states
  - Sifting
  - Test (check for errors) and abort if needed
- Classical post-processing
  - Classical error correction
  - Privacy amplification



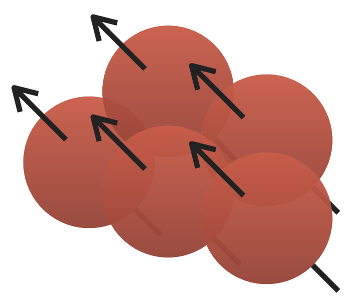
QKD

- Data generation
  - Measuring the quantum states
  - Sifting
  - Test (check for errors) and abort if needed
- Classical post-processing
  - Classical error correction
  - Privacy amplification



Alice and Bob are exchanging **classical** information in the presence of a **quantum** adversary

Privacy Amplification



Eve

Alice's raw key: 0 1 0 1 0 0 0 1 0 0 1 1 0 0 1 1 1 0 1 1 0 ...

Classical-quantum state: $$\rho_{\mathrm{A}E} = \sum_{\mathrm{a}} p(\mathrm{a})|\mathrm{a}\rangle\langle\mathrm{a}|_{\mathrm{A}} \otimes \rho_E^{\mathrm{a}}$$

- We have some correlations between Alice's raw key A and Eve's quantum system E
- Privacy amplification: get rid of these correlations!

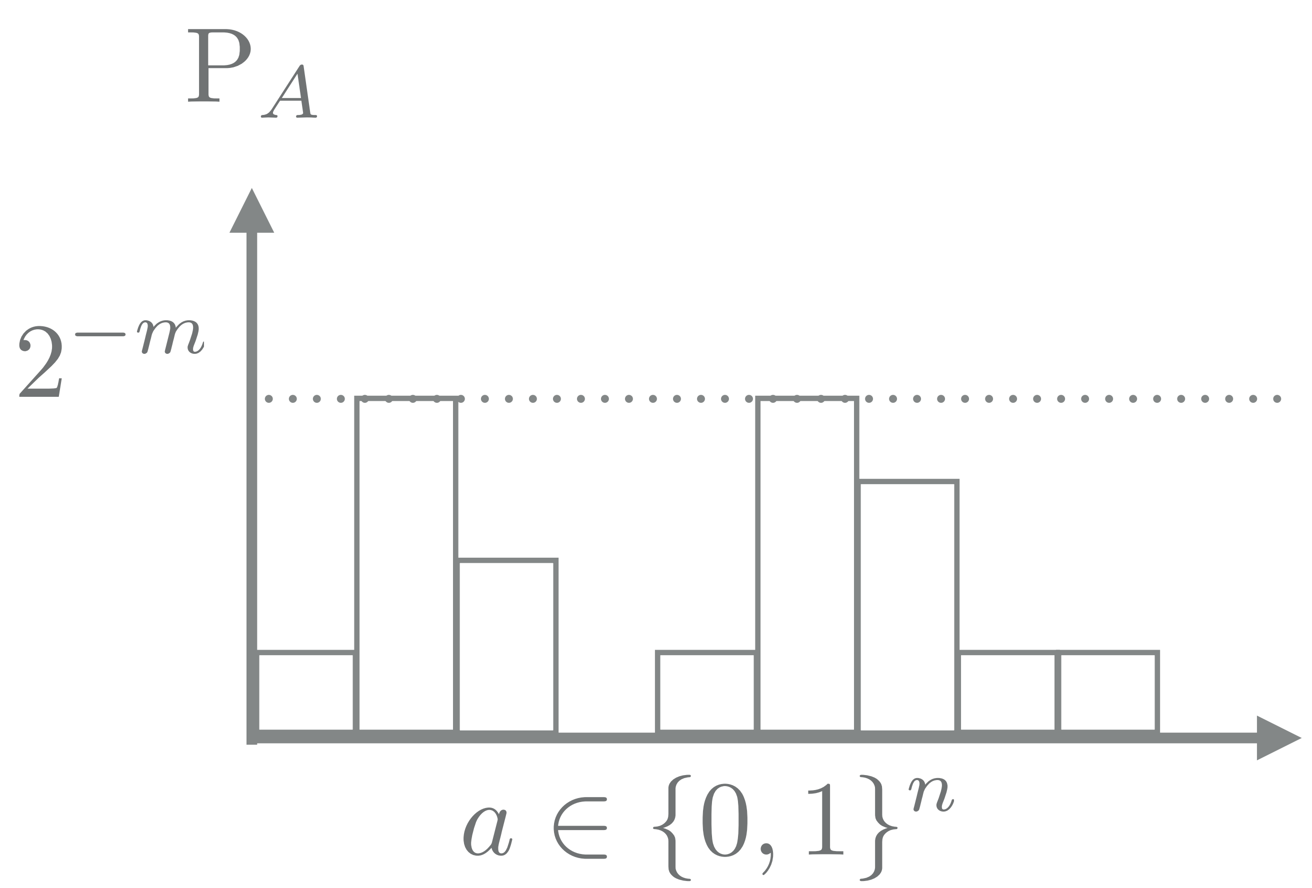
Want to get: $$\rho_{U_\ell} \otimes \rho_E = \sum_k 2^{-\ell}|k\rangle\langle k|_{K_A} \otimes \rho_E$$ ← Perfect (ideal) key

- Tool: **Quantum-proof** randomness extractors

Randomness Extractors

- Want to transform a large but weak source of randomness into a shorter uniform distribution
- Cryptography; Pseudo-randomness; Combinatorics

Weak source of randomness



Min-entropy:

$p_{\text{guess}}(A)$

$$H_{\min}(A) = -\log\left(\max_a \Pr[a]\right)$$

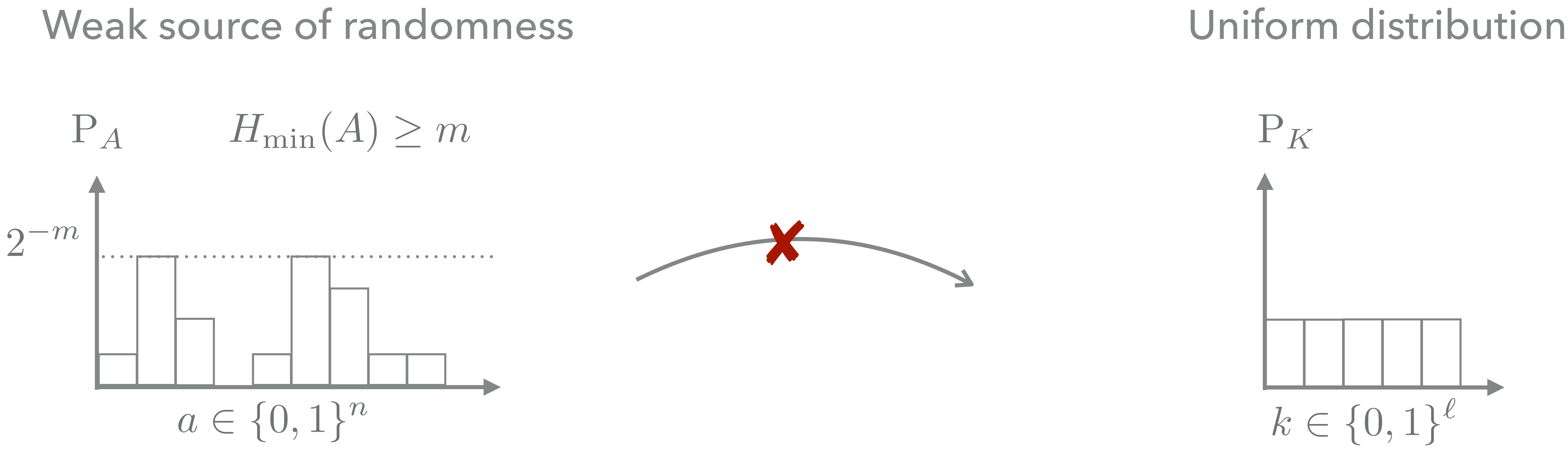
$$H_{\min}(A) \geq m :$$

$$\forall a \in \{0,1\}^n, \quad \Pr[a] \leq 2^{-m}$$

Randomness Extractors

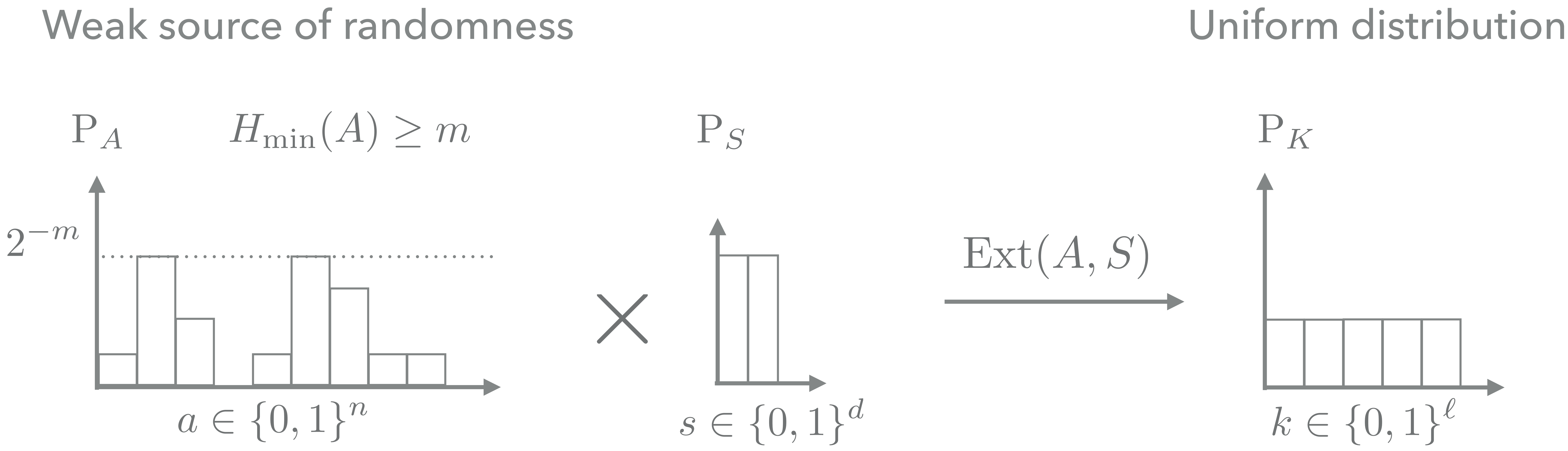
- Want to transform a large but weak source of randomness into a shorter uniform distribution

- Impossible to achieve deterministically



Randomness Extractors

- Want to transform a large but weak source of randomness into a shorter uniform distribution
- Impossible to achieve deterministically
- Possible with an additional short random seed



Randomness Extractors

- Def. [Randomness extractor]: A function $\mathrm{Ext}(A,S) : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^\ell$ is called a **strong** (m,ε)-randomness extractor if for

  1. $S = U_d$
  2. any P_A with $H_{\min}(A) \geq m$

  we have

$$\|\mathrm{Ext}(A,S)S - U_\ell \times S\| \leq \varepsilon$$

Output of the extractor

Uniform key

Eve?

(Strong extractor: the seed is made public during the QKD protocol)

"Classical-Proof" Randomness Extractors

- Def. [Randomness extractor]: A function $\mathrm{Ext}(A,S):\{0,1\}^n\times\{0,1\}^d\to\{0,1\}^\ell$ is called a classical-proof strong (m,ε)-randomness extractor if for

1. $S=U_d$
2. any P_{AE} with $H_{\min}(A|E)\geq m$

$$H_{\min}(A|E)=-\log p_{\text{guess}}(A|E)$$

$$p_{\text{guess}}(A|E)=\mathbb{E}_e p_{\text{guess}}(A_{|E=e})=\mathbb{E}_e\max_a \Pr[a|e]$$

we have

$$\|\mathrm{Ext}(A,S)SE-U_\ell\times SE\|\leq\varepsilon$$

Eve?

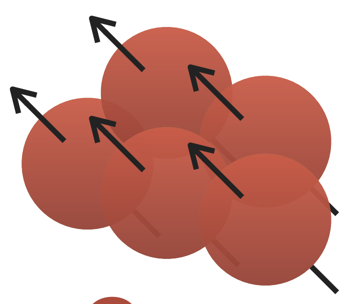
$$=\mathbb{E}_e\|\mathrm{Ext}(A_{|E=e},S)S-U_\ell\times S\|$$

Classical side information (E) is kind of trivial when considering extractors…

Quantum-Proof Randomness Extractors

- Def. [Randomness extractor]: A function $\mathrm{Ext}(A,S):\{0,1\}^n\times\{0,1\}^d\rightarrow\{0,1\}^\ell$ is called a **quantum-proof** strong (m,ε)-randomness extractor if for

1. $S=U_d$
2. any $\rho_{\mathrm{A}E}=\sum_{\mathrm{a}}p(\mathrm{a})|\mathrm{a}\rangle\langle\mathrm{a}|_{\mathrm{A}}\otimes\rho_E^{\mathrm{a}}$ with $H_{\min}(A|E)\geq m$



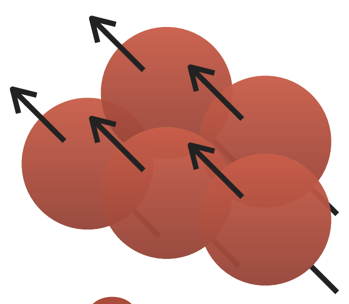
Eve?

$$H_{\min}(A|E)=-\log p_{\mathrm{guess}}(A|E)$$

Quantum-Proof Randomness Extractors

- Def. [Randomness extractor]: A function $\mathrm{Ext}(A,S):\{0,1\}^n\times\{0,1\}^d\rightarrow\{0,1\}^\ell$ is called a **quantum-proof** strong (m,ε)-randomness extractor if for

1. $S=U_d$
2. any $\rho_{\mathrm{A}E}=\sum_{\mathrm{a}} p(\mathrm{a})|\mathrm{a}\rangle\langle\mathrm{a}|_{\mathrm{A}}\otimes\rho_E^{\mathrm{a}}$ with $H_{\min}(A|E)\geq m$



$$H_{\min}(A|E)=-\log p_{\mathrm{guess}}(A|E)$$

$$p_{\mathrm{guess}}(A|E)=\max_{\{M_E^a\}_a}\sum_a p(a)\mathrm{Tr}(M_E^a\rho_E^a)$$

Guessing prob. with access to a quantum system

Quantum-Proof Randomness Extractors

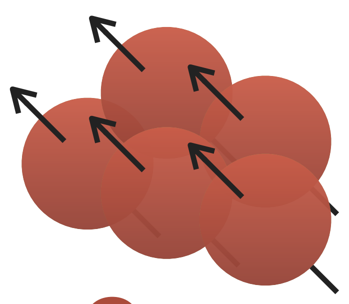
- Def. [Randomness extractor]: A function $\mathrm{Ext}(A,S):\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^\ell$ is called a **quantum-proof** strong (m,ε)-randomness extractor if for

1. $S = U_d$
2. any $\rho_{\mathrm{A}E} = \sum_{\mathrm{a}} p(\mathrm{a})|\mathrm{a}\rangle\langle\mathrm{a}|_{\mathrm{A}} \otimes \rho_E^{\mathrm{a}}$ with $H_{\min}(A|E) \geq m$

we have

$$\|\rho_{\mathrm{Ext}(A,S)SE} - \rho_{U_\ell} \otimes \rho_{SE}\| \leq \varepsilon$$

Questions?



Eve?

Eve's system is kept quantum!
Crucial for composability!

- The quantum case doesn't follow from the classical one… :(/ :)

$$H_{\min}(A|E) = -\log p_{\mathrm{guess}}(A|E)$$

$$p_{\mathrm{guess}}(A|E) = \max_{\{M_E^a\}_a} \sum_a p(a)\mathrm{Tr}(M_E^a \rho_E^a)$$

Guessing prob. with an access to a quantum system

Why did I tell you all of that…?

Security Definition

- Def. [Secrecy]: A protocol is ε_{sec}-secret if

$$(1 - \Pr(\text{abort})) \, \| \rho_{K_A E} - \rho_{U_\ell} \otimes \rho_E \| \leq \varepsilon_{\text{sec}}$$

Trace distance between two states: the real and ideal (want this to be small)

QKD

- Data generation
  - Measuring the quantum states
  - Sifting
  - Test (check for errors) and abort if needed
- Classical post-processing
  - Classical error correction
  - Privacy amplification ← Using an extractor

Quantum-Proof Randomness Extractors

- Def. [Randomness extractor]: A function $\text{Ext}(A,S) : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^\ell$ is called a **quantum-proof** strong (m,ε)-randomness extractor if for

1. $S = U_d$
2. any $\rho_{\text{AE}} = \sum_{\text{a}} p(\text{a}) |\text{a}\rangle\langle\text{a}|_{\text{A}} \otimes \rho_{\text{E}}^{\text{a}}$ with $H_{\min}(A|E) \geq m$

we have

$$\| \rho_{\text{Ext}(A,S)SE} - \rho_{U_\ell} \otimes \rho_{SE} \| \leq \varepsilon$$

- For the extractor to work we need to have a sufficiently high min-entropy in Alice's outputs
- The main challenge in proving the security of QKD protocols is to lower-bound the min-entropy
- This is what we're going to look at next

Quantum Key Distribution

BIU Winter School on Quantum Cryptography | February 15, 2021

Rotem Arnon-Friedman | Weizmann Institute of Science

Outline

- Lecture 1:
  - Introduction
  - BB84 and Ekert91 protocols
- Lecture 2:
  - QKD security definition
  - Quantum-proof randomness extractors
- Lecture 3:
  - Security proof (the main parts)
  - Device-independent quantum key distribution

Security Definition

- Def. [Secrecy]: A protocol is ε_{sec}-secret if

$$(1 - \Pr(\text{abort}))\,\|\rho_{K_A E} - \rho_{U_\ell} \otimes \rho_E\| \leq \varepsilon_{\text{sec}}$$

Trace distance between two states: the real and ideal (want this to be small)

QKD

- Data generation
  - Measuring the quantum states
  - Sifting
  - Test (check for errors) and abort if needed
- Classical post-processing
  - Classical error correction
  - Privacy amplification

Quantum-Proof Randomness Extractors

- Def. [Randomness extractor]: A function $\text{Ext}(A,S) : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^\ell$ is called a **quantum-proof** strong (m, ε)-randomness extractor if for

1. $S = U_d$
2. any $\rho_{\text{AE}} = \sum_{\text{a}} p(\text{a})|\text{a}\rangle\langle\text{a}|_{\text{A}} \otimes \rho_{\text{E}}^{\text{a}}$ with $H_{\min}(A|E) \geq m$

we have

$$\|\rho_{\text{Ext}(A,S)SE} - \rho_{U_\ell} \otimes \rho_{SE}\| \leq \varepsilon$$

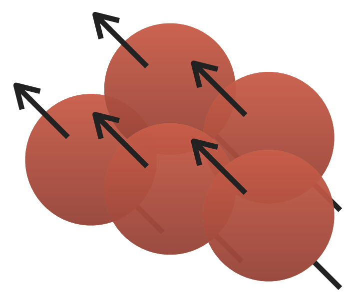
- For the extractor to work we need to have a sufficiently high min-entropy in Alice's outputs
- The main challenge in proving the security of QKD protocols is to lower-bound the min-entropy
- This is what we're going to look at next

Recap

- We need to lower-bound $H_{\min}(A|E) \geq m$ of the state in the end of the execution of the protocol:

$$\rho_{AE} = \sum_{a} p(a)|a\rangle\langle a|_A \otimes \rho_E^a$$

Alice's raw key : 0 1 0 1 0 0 0 1 0 ...



Eve

- After that, a quantum-proof extractor does the work

Alice		Bob	
Z	$\|0\rangle$	Z	$\|0\rangle$
X	$\|-\rangle$	X	$\|+\rangle$
~~X~~	~~$\|+\rangle$~~	~~Z~~	~~$\|1\rangle$~~
Z	$\|1\rangle$	Z	$\|1\rangle$
~~Z~~	~~$\|0\rangle$~~	~~X~~	~~$\|+\rangle$~~
Z	$\|0\rangle$	Z	$\|1\rangle$
X	$\|+\rangle$	X	$\|+\rangle$
⋮		⋮	

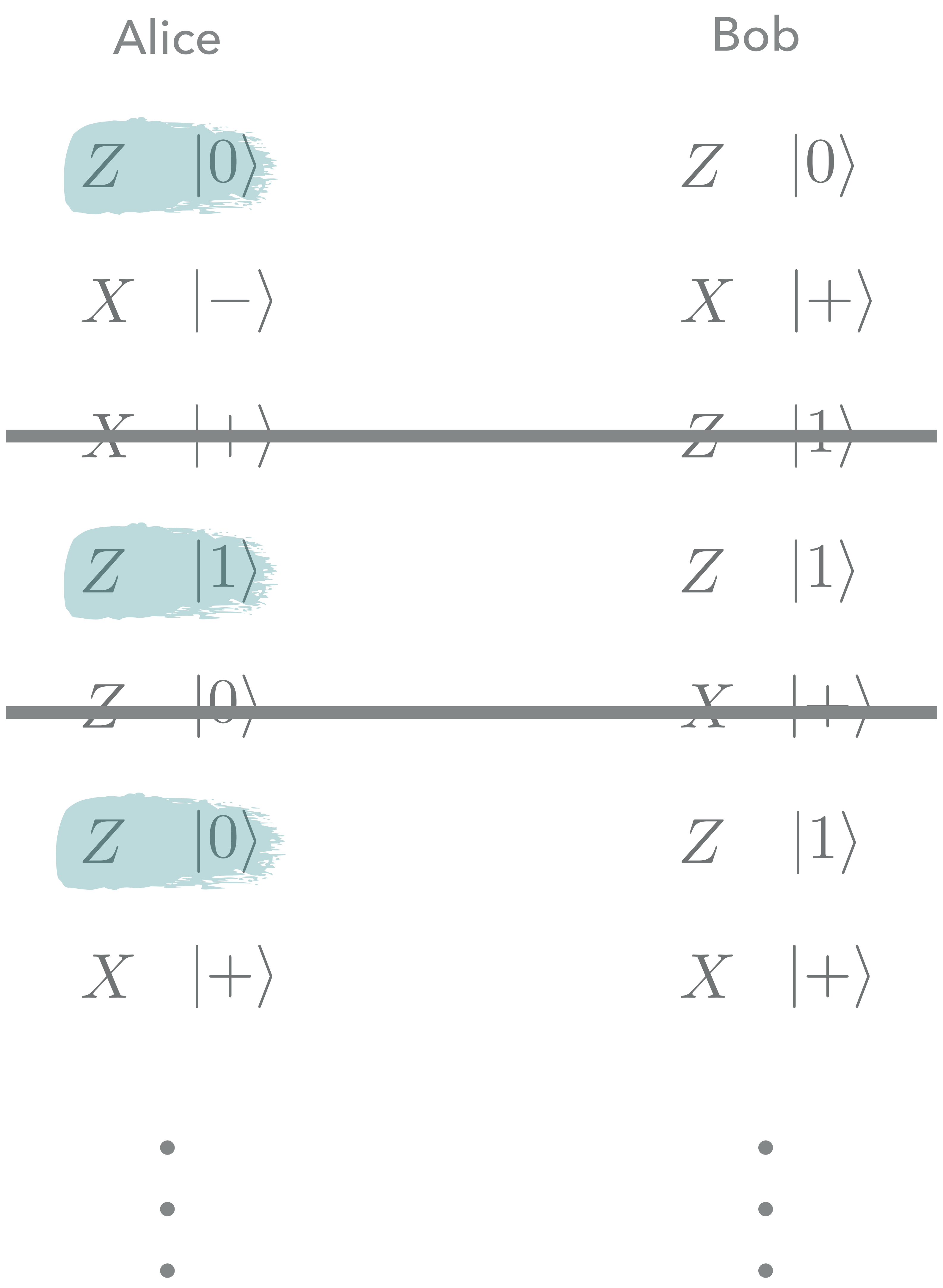
1. Quantum-proof extractors ✓ (Computer science)
2. Reduction to IID (Information theory)
3. Uncertainty relation (Quantum physics)

Security Proof

(Somewhat informal, just presenting the main statements)

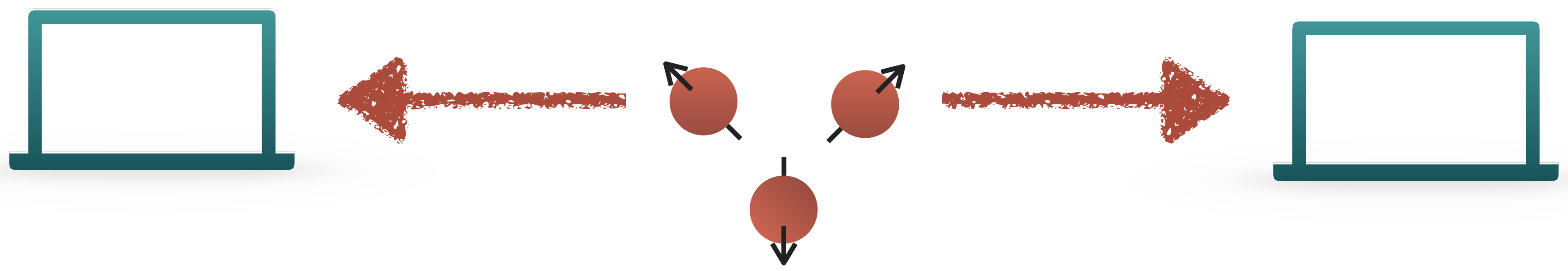
Entropy Accumulation

- We need to lower-bound $H_{\min}(\mathbf{A}|E) \geq m$ of the state in the end of the execution of the protocol
- $\mathbf{a} \in \{0,1\}^n$, for n the number of rounds in the protocol
- How do we analyze Eve's actions over n rounds?
  - Adaptive strategies, global operation :(
  - Entropy doesn't need to be produced in every round



Reduction to IID

- Wishful thinking: Eve uses the same strategy in each round, independently of all other rounds



σ_{ABE}

- The initial state is an "independently and identically distributed" (IID) state

$$\rho_{\mathbf{ABE}} = \sigma_{ABE}^{\otimes n}$$

- Intuitively: we only need to understand what happens in **one** round

	Alice		Bob	
σ_{ABE}	Z	$\|0\rangle$	Z	$\|0\rangle$
σ_{ABE}	X	$\|-\rangle$	X	$\|+\rangle$
σ_{ABE}	~~X~~	~~$\|+\rangle$~~	~~Z~~	~~$\|1\rangle$~~
σ_{ABE}	Z	$\|1\rangle$	Z	$\|1\rangle$
σ_{ABE}	~~Z~~	~~$\|0\rangle$~~	~~X~~	~~$\|+\rangle$~~
σ_{ABE}	Z	$\|0\rangle$	Z	$\|1\rangle$
σ_{ABE}	X	$\|+\rangle$	X	$\|+\rangle$
	$\vdots$		$\vdots$	

(Quantum) Asymptotic Equipartition Property

- A property of entropy of IID states $\rho_{\mathbf{ABE}} = \sigma_{ABE}^{\otimes n}$:

$$H_{\min}^{\varepsilon}(\mathbf{A}|\mathbf{E})_\rho \geq nH(A|E)_\sigma - c_\varepsilon\sqrt{n}$$

Many different entropies…
All describe some form of uncertainty, lack of knowledge

(Quantum) Asymptotic Equipartition Property

- A property of entropy of IID states $\rho_{\mathbf{ABE}} = \sigma_{ABE}^{\otimes n}$:

$$H_{\min}^{\varepsilon}(\mathbf{A}|\mathbf{E})_{\rho} \geq nH(A|E)_{\sigma} - c_{\varepsilon}\sqrt{n}$$

Smooth min-entropy

- Closely related to the min-entropy
- Good for the extractors
- (Crucial and better)

von Neumann entropy

- Quantum version of the Shannon entropy
- (Always larger than the min-entropy)

$$H(A)_{\sigma} = -\mathrm{Tr}(\sigma \log \sigma)$$

$$H(A|E) = H(AE) - H(E)$$

- Tells us that for IID states we now need to find a single-round quantity $H(A|E)_{\sigma}$

Reduction to IID

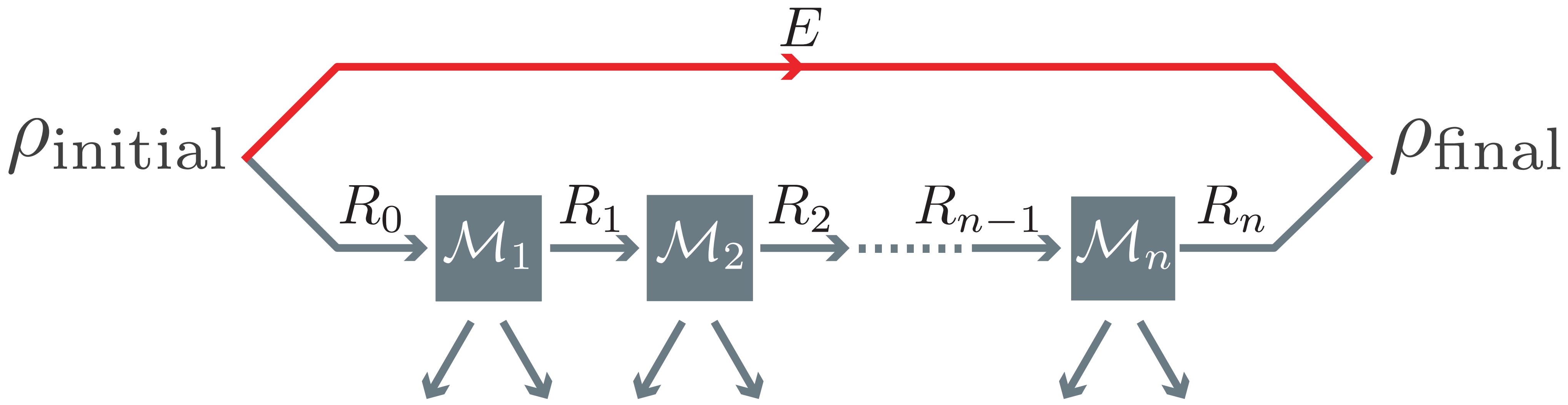
- Of course, that was only a wishful thinking. But…
- A theorem called “**the entropy accumulation theorem**” tells us that under certain conditions

$$H^{\varepsilon}_{\min}(\mathbf{A}|\mathbf{E})_{\rho} \geq nH(A|E)_{\sigma} - c_{\varepsilon}\sqrt{n}$$

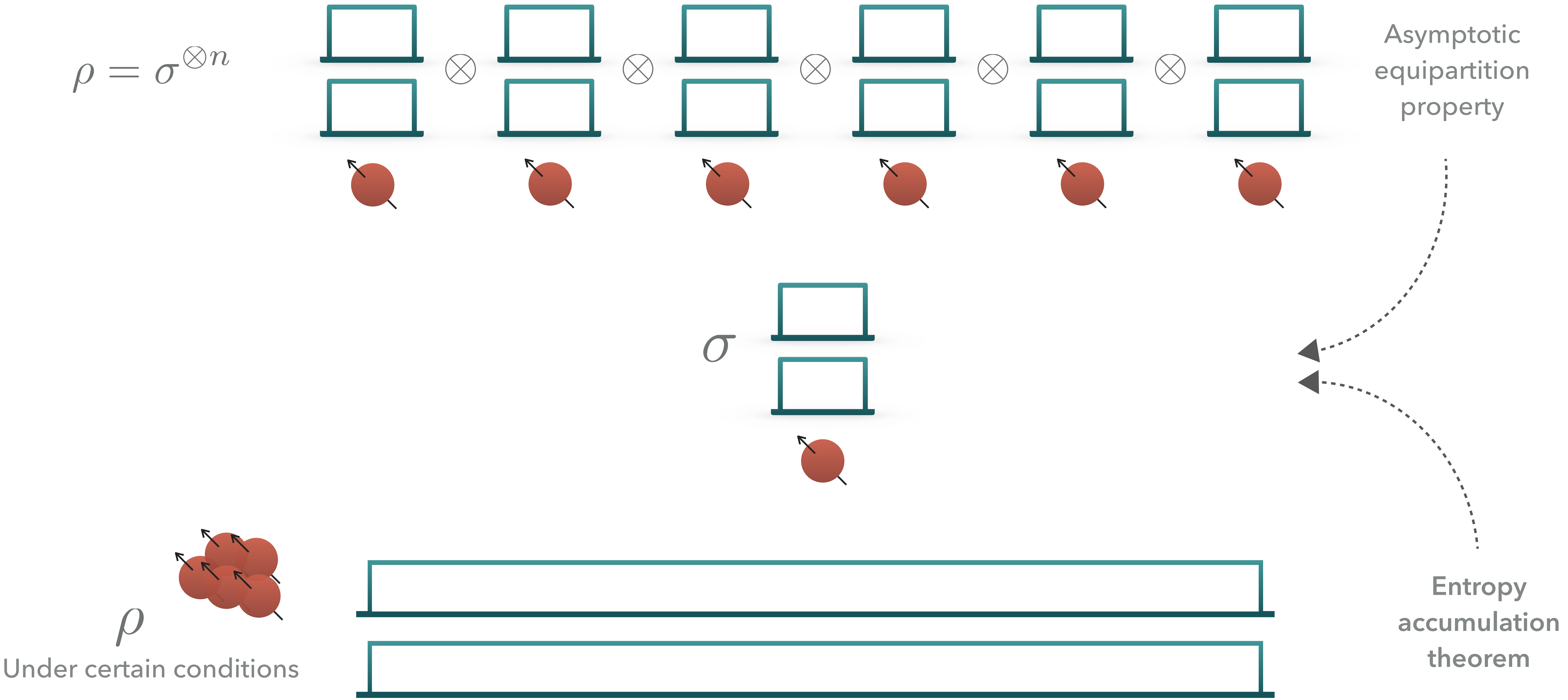
still holds, with σ defined via some optimization problem

  - (Roughly, σ is the state that minimizes $H(A|E)_{\sigma}$ over all states that are compatible with the data that Alice and Bob observe throughout the execution of the protocol)

- Reduction to IID (not black box)

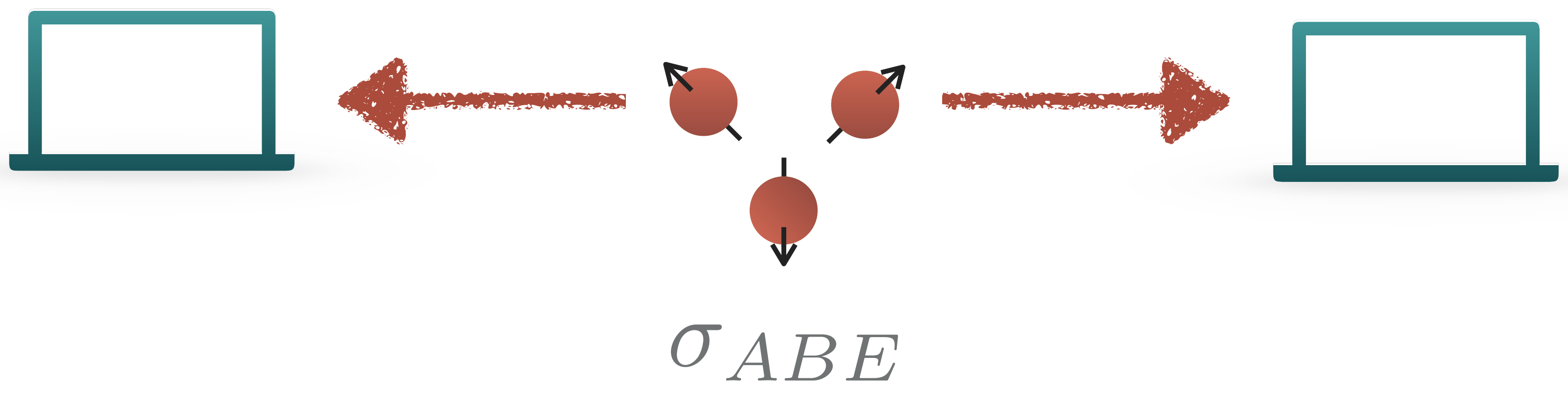


Reduction to IID



Reduction to IID

- Eve uses the same strategy in each round, independently of all other rounds



- $$H^{\varepsilon}_{\min}(\mathbf{A}|\mathbf{E})_{\rho} \geq nH(A|E)_{\sigma} - c_{\varepsilon}\sqrt{n}$$

- Our goal is now to lower-bound the amount of von Neumann entropy produced in one round

Questions?

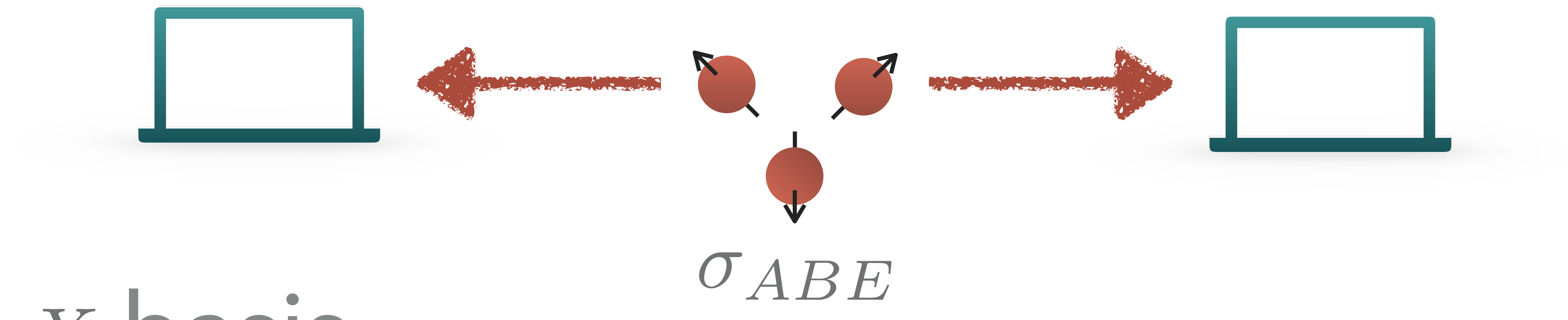
	Alice		Bob	
σ_{ABE}	Z	$\|0\rangle$	Z	$\|0\rangle$
σ_{ABE}	X	$\|-\rangle$	X	$\|+\rangle$
σ_{ABE}	~~X~~	~~$\|+\rangle$~~	~~Z~~	~~$\|1\rangle$~~
σ_{ABE}	Z	$\|1\rangle$	Z	$\|1\rangle$
σ_{ABE}	~~Z~~	~~$\|0\rangle$~~	~~X~~	~~$\|+\rangle$~~
σ_{ABE}	Z	$\|0\rangle$	Z	$\|1\rangle$
σ_{ABE}	X	$\|+\rangle$	X	$\|+\rangle$
	$\vdots$		$\vdots$	

1. Quantum-proof extractors ✓ (Computer science)
2. Reduction to IID ✓ (Information theory)
3. Uncertainty relation (Quantum physics)

Security Proof

(Somewhat informal, just presenting the main statements)

Uncertainty Relation

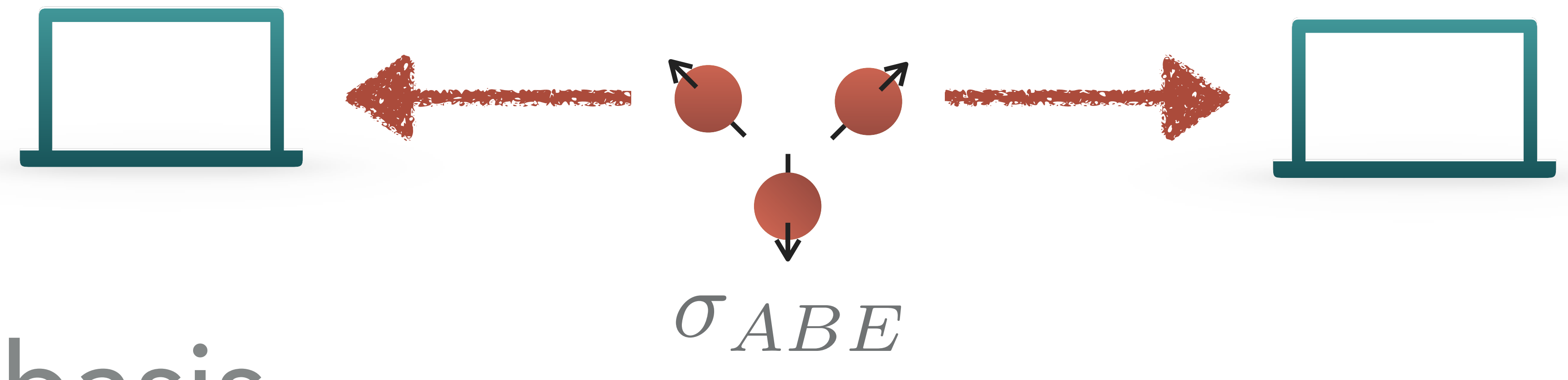


- Tripartite quantum state σ_{ABE}
- Alice is measuring either in the Z basis or the X basis
    - Incompatible bases– can't guess both outcomes with certainty

$$H(\mathrm{A}_Z) + H(\mathrm{A}_X) \geq 1$$

Notation: the outcome of measuring the system in the given basis

Uncertainty Relation

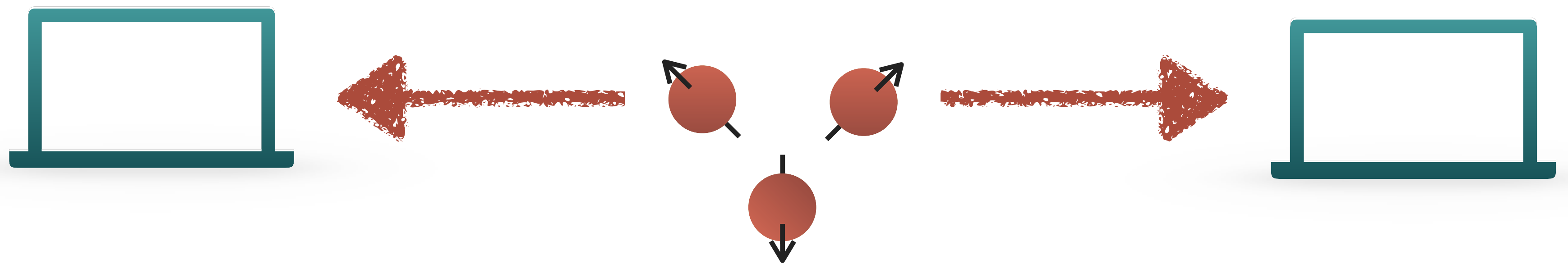


- Tripartite quantum state σ_{ABE}
- Alice is measuring either in the Z basis or the X basis
  - Incompatible bases– can't guess both outcomes with certainty

$$H(\mathrm{A}_Z) + H(\mathrm{A}_X) \geq 1$$

Z	$\|0\rangle$	Z	$\|0\rangle$
X	$\|-\rangle$	X	$\|+\rangle$
~~X~~	~~$\|+\rangle$~~	~~Z~~	~~$\|1\rangle$~~
Z	$\|1\rangle$	Z	$\|1\rangle$
~~Z~~	~~$\|0\rangle$~~	~~X~~	~~$\|+\rangle$~~
Z	$\|0\rangle$	Z	$\|1\rangle$
X	$\|+\rangle$	X	$\|+\rangle$

Uncertainty Relation



- Tripartite quantum state σ_{ABE}
- Alice is measuring either in the Z basis or the X basis
  - Incompatible bases– can't guess both outcomes with certainty

$$H(\mathrm{A}_Z) + H(\mathrm{A}_X) \geq 1$$

- Given access to Bob's state one can do better

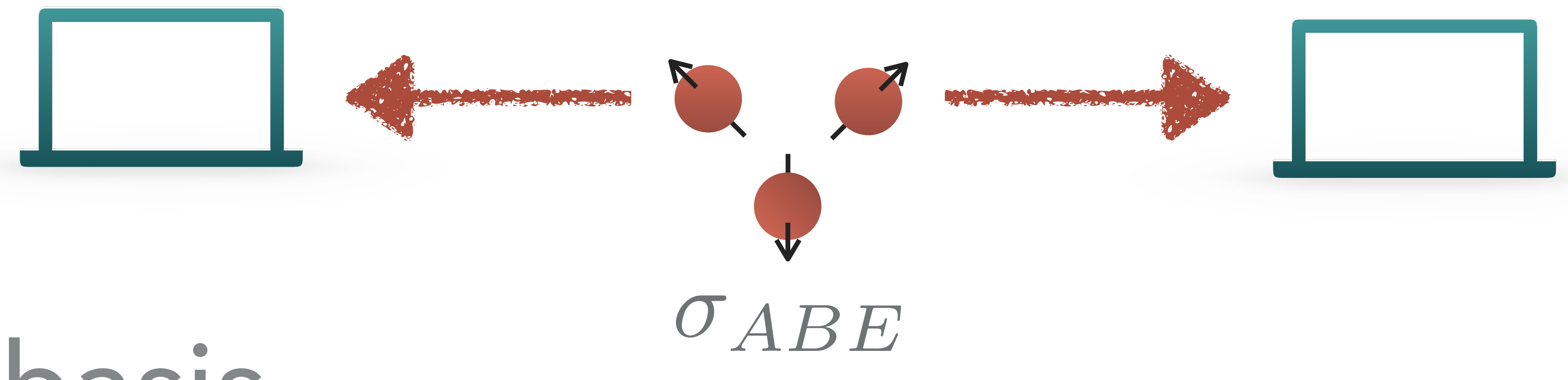
$$H(\mathrm{A}_Z|B) + H(\mathrm{A}_X|B) \geq 1 + H(A|B)$$

Negative when Alice and Bob are entangled!

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|--\rangle + |++\rangle)$$

Uncertainty Relation

- Tripartite quantum state σ_{ABE}



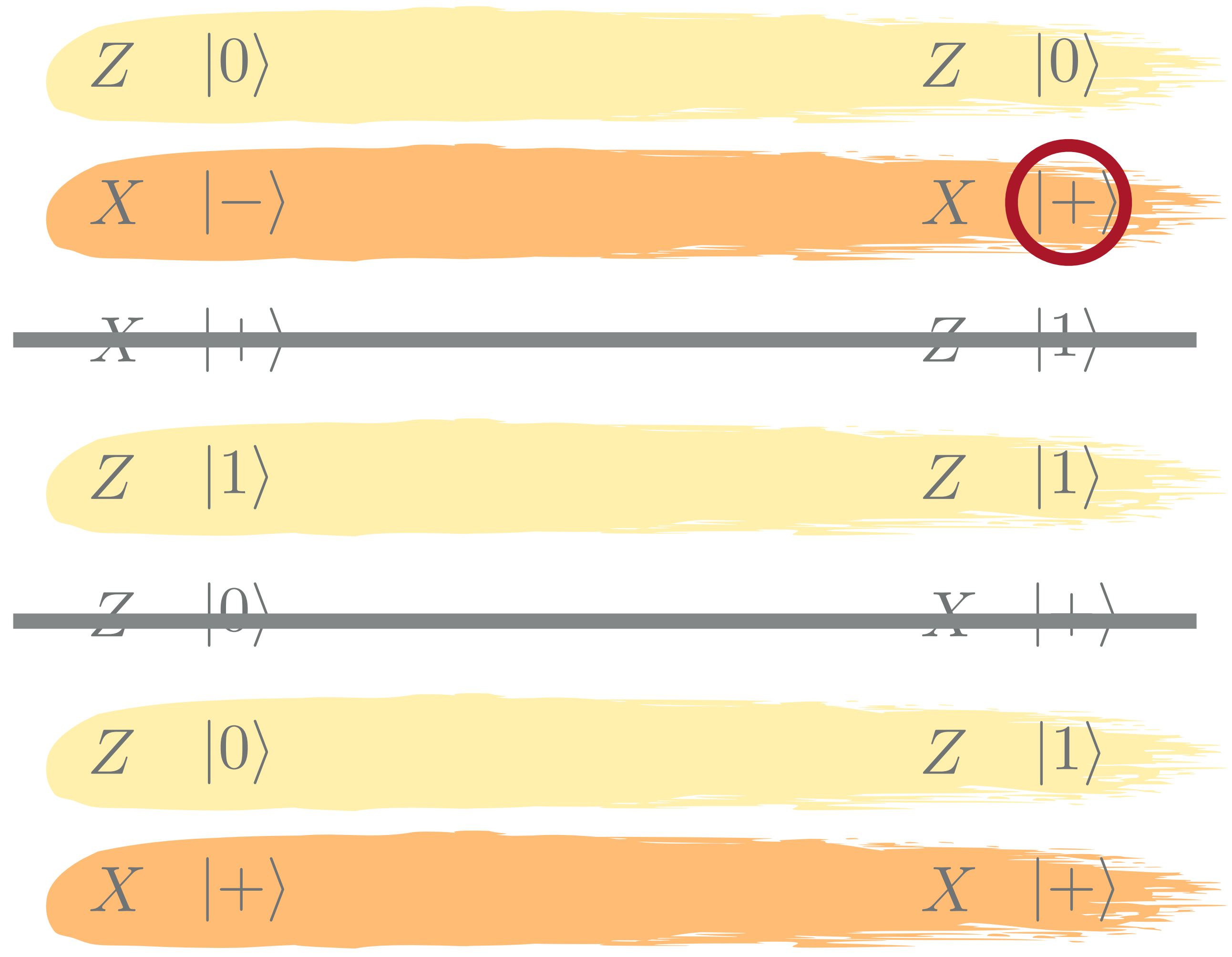
- Alice is measuring either in the Z basis or the X basis
- Using some entropic relations, $H(\mathrm{A}_Z|B) + H(\mathrm{A}_X|B) \geq 1 + H(A|B)$ can be rewritten as

$$\underbrace{H(\mathrm{A}_Z|E)} \geq 1 - H(\mathrm{A}_X|\mathrm{B}_X)$$

Eve's uncertainty regarding the raw key bit

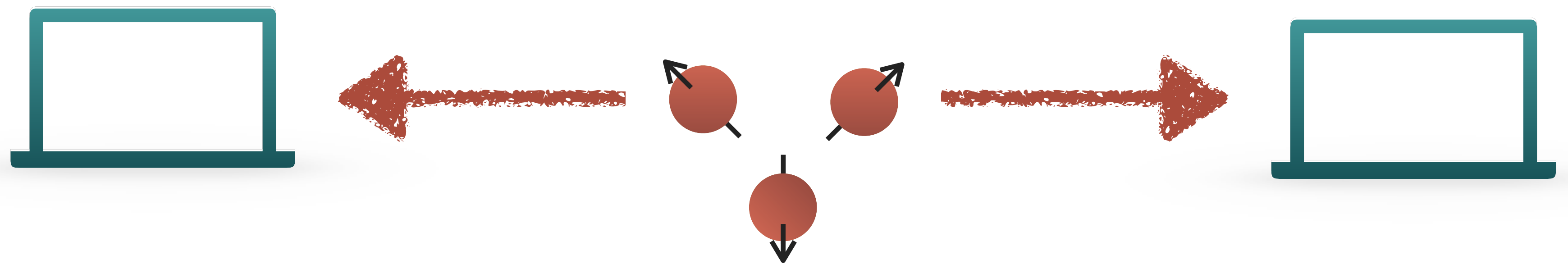
↑

What we need in order to lower-bound the total amount of entropy $H^{\varepsilon}_{\min}(\mathbf{A}_Z|E)$



Uncertainty Relation

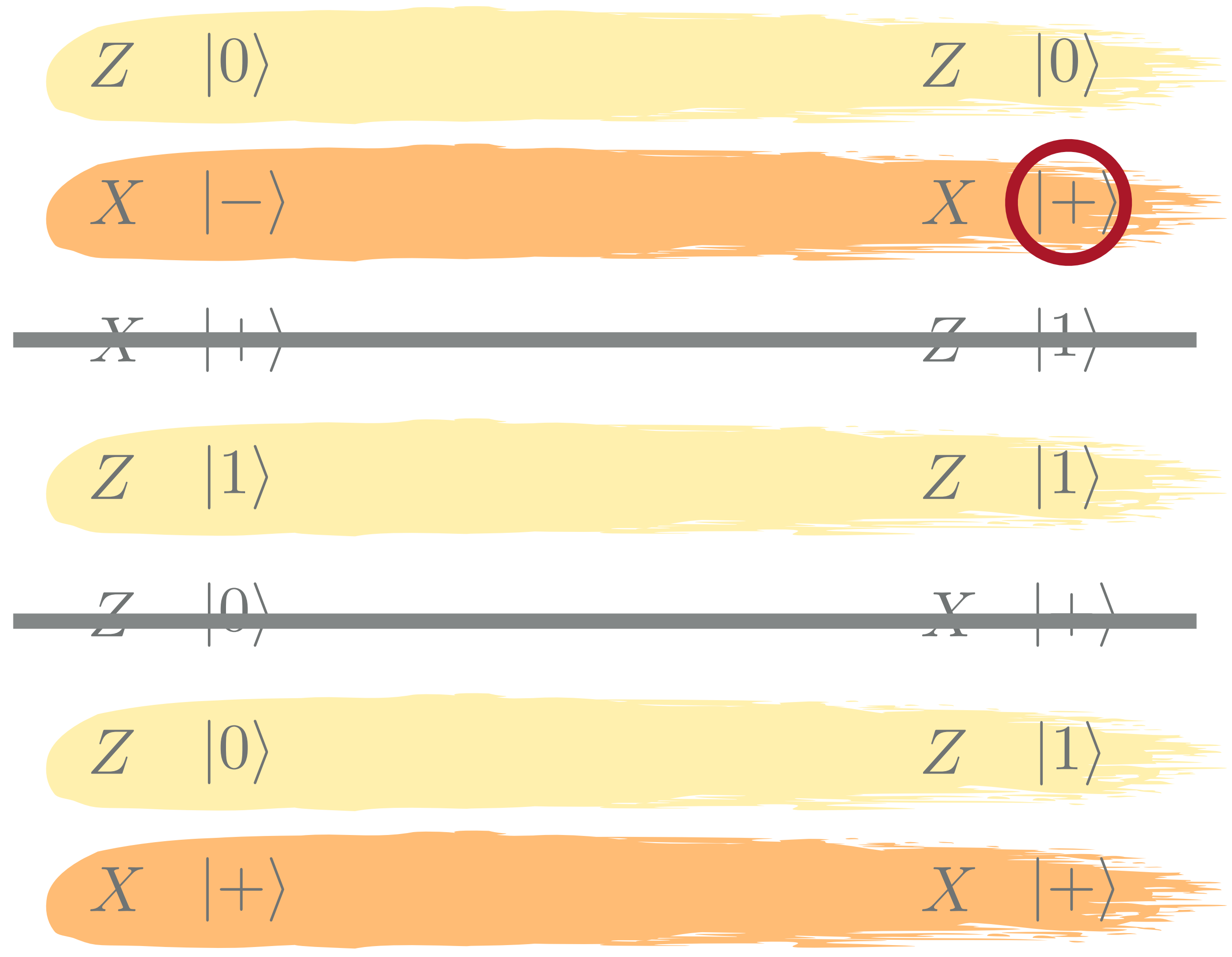
- Tripartite quantum state σ_{ABE}



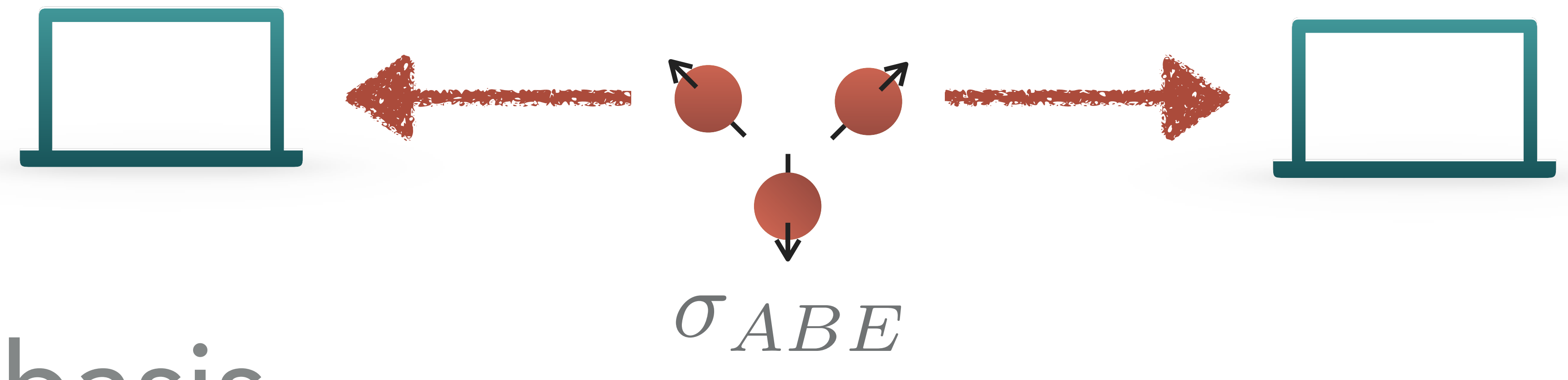
- Alice is measuring either in the Z basis or the X basis
- Using some entropic relations, $H(\mathrm{A}_Z|B) + H(\mathrm{A}_X|B) \geq 1 + H(A|B)$ can be rewritten as

$$H(\mathrm{A}_Z|E) \geq 1 - \underbrace{H(\mathrm{A}_X|\mathrm{B}_X)}_{\text{"Error rate"}}$$

Can be **estimated** from the **observed data** during the execution of the protocol



Uncertainty Relation



- Tripartite quantum state σ_{ABE}
- Alice is measuring either in the Z basis or the X basis
- Using some entropic relations, $H(\mathrm{A}_Z|B) + H(\mathrm{A}_X|B) \geq 1 + H(A|B)$ can be rewritten as

$$H(\mathrm{A}_Z|E) \geq 1 - H(\mathrm{A}_X|\mathrm{B}_X)$$

Questions?

- Example: perfect correlations (no errors) imply 1 bit of entropy per round

- Take-home message: quantum physics allows us to bound **Eve's knowledge** using **Alice and Bob's observed data** (replaces computational assumptions)

Security Proof

1. Uncertainty relation

$$H(\mathrm{A}_Z|E) \geq 1 - H(\mathrm{A}_X|\mathrm{B}_X)$$

$$\downarrow$$

2. Entropy accumulation
   (Reduction to IID)

$$H^{\varepsilon}_{\min}(\mathbf{A}|\mathbf{E})_\rho \geq nH(A|E)_\sigma - c_\varepsilon\sqrt{n}$$

$$\downarrow$$

3. Quantum-proof extractors

$$\|\rho_{\mathrm{Ext}(A,S)SE} - \rho_{U_\ell} \otimes \rho_{SE}\| \leq \varepsilon$$

$$\downarrow$$

4. Secrecy

$$(1 - \Pr(\mathrm{abort}))\, \|\rho_{K_A E} - \rho_{U_\ell} \otimes \rho_E\| \leq \varepsilon_{\mathrm{sec}}$$

$$\downarrow$$

5. Security

(Secrecy + correctness + completeness)

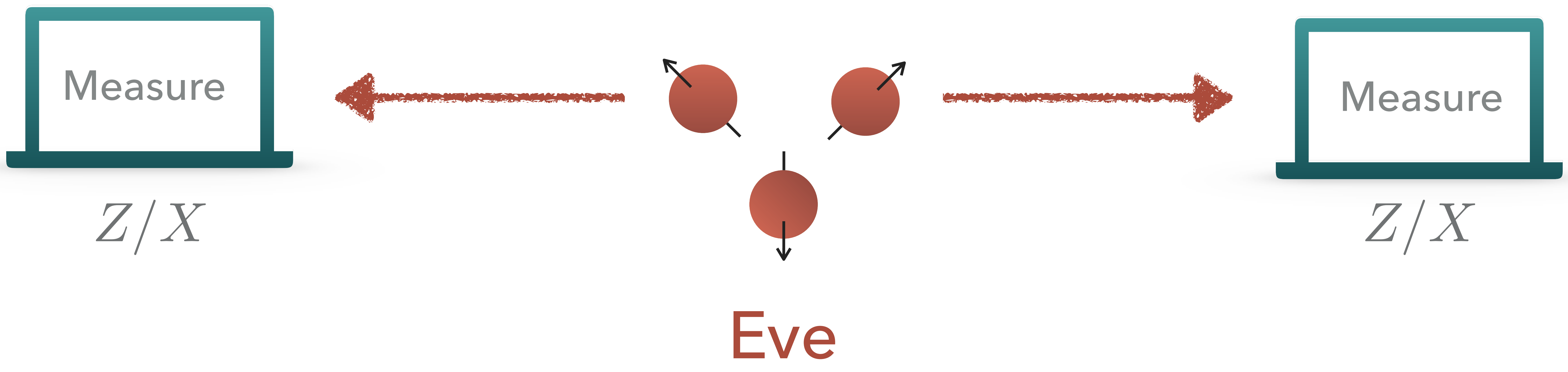
Questions?

1. Motivation
2. Non-local games
3. Security

Device-Independent QKD

Motivation

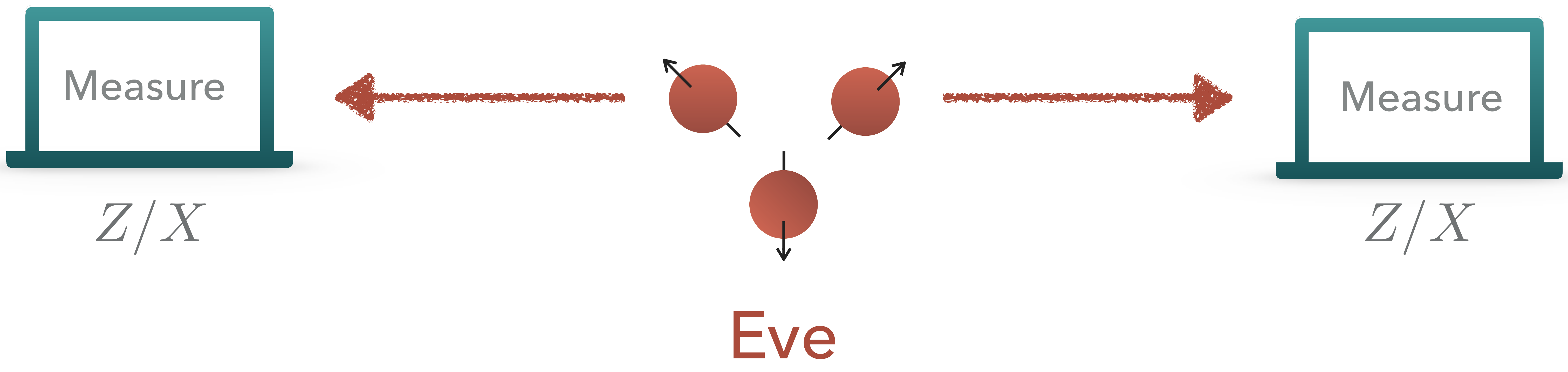
- Ekert 91



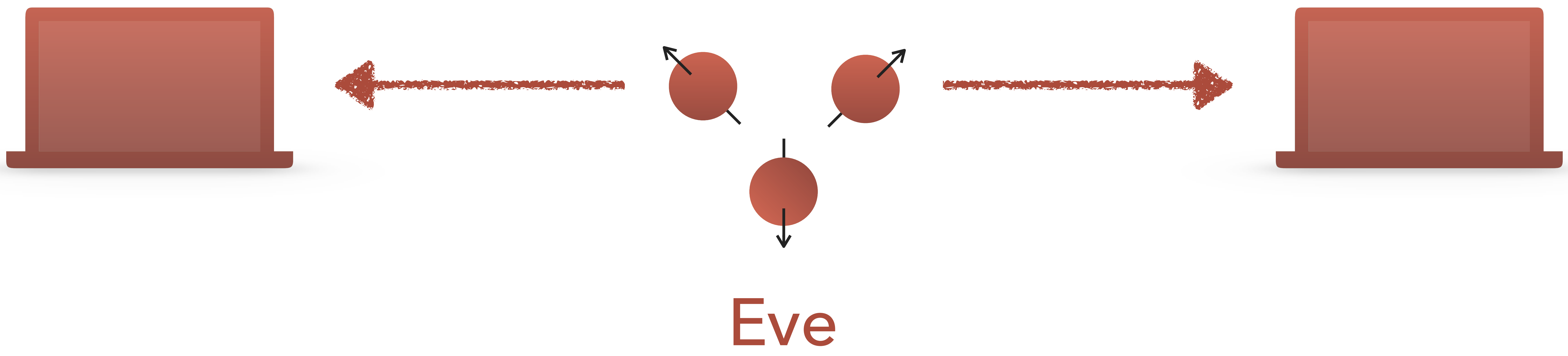
- Uncertainty relation $H(\mathrm{A}_Z|E) \geq 1 - H(\mathrm{A}_X|\mathrm{B}_X)$
  - What if the measurements are not exact…?
  - What if we don't know the dimension…? (Side channels)
  - What if…

Motivation

- Ekert 91



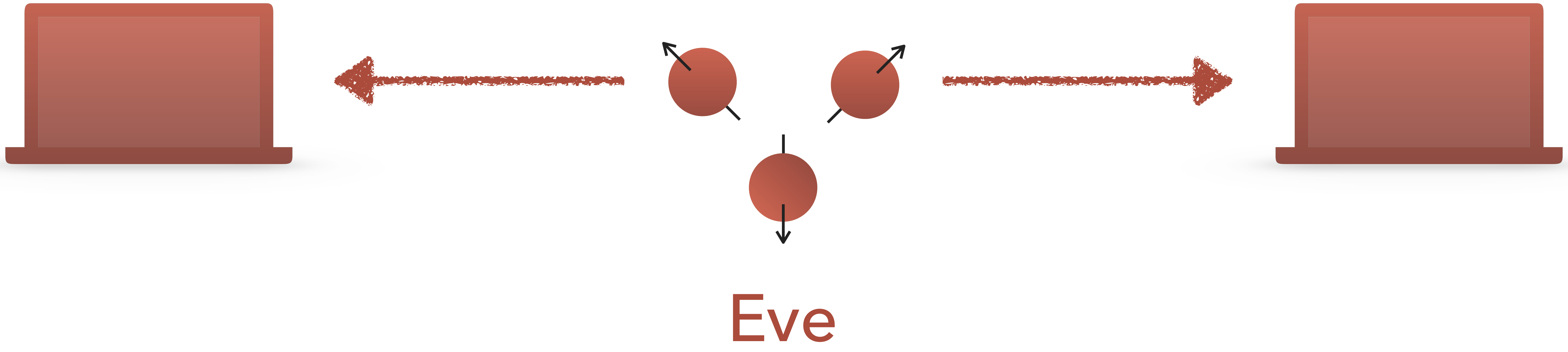
- Device-independent



- Paranoid cryptographers; **Realistic physicists;** Fundamental physics

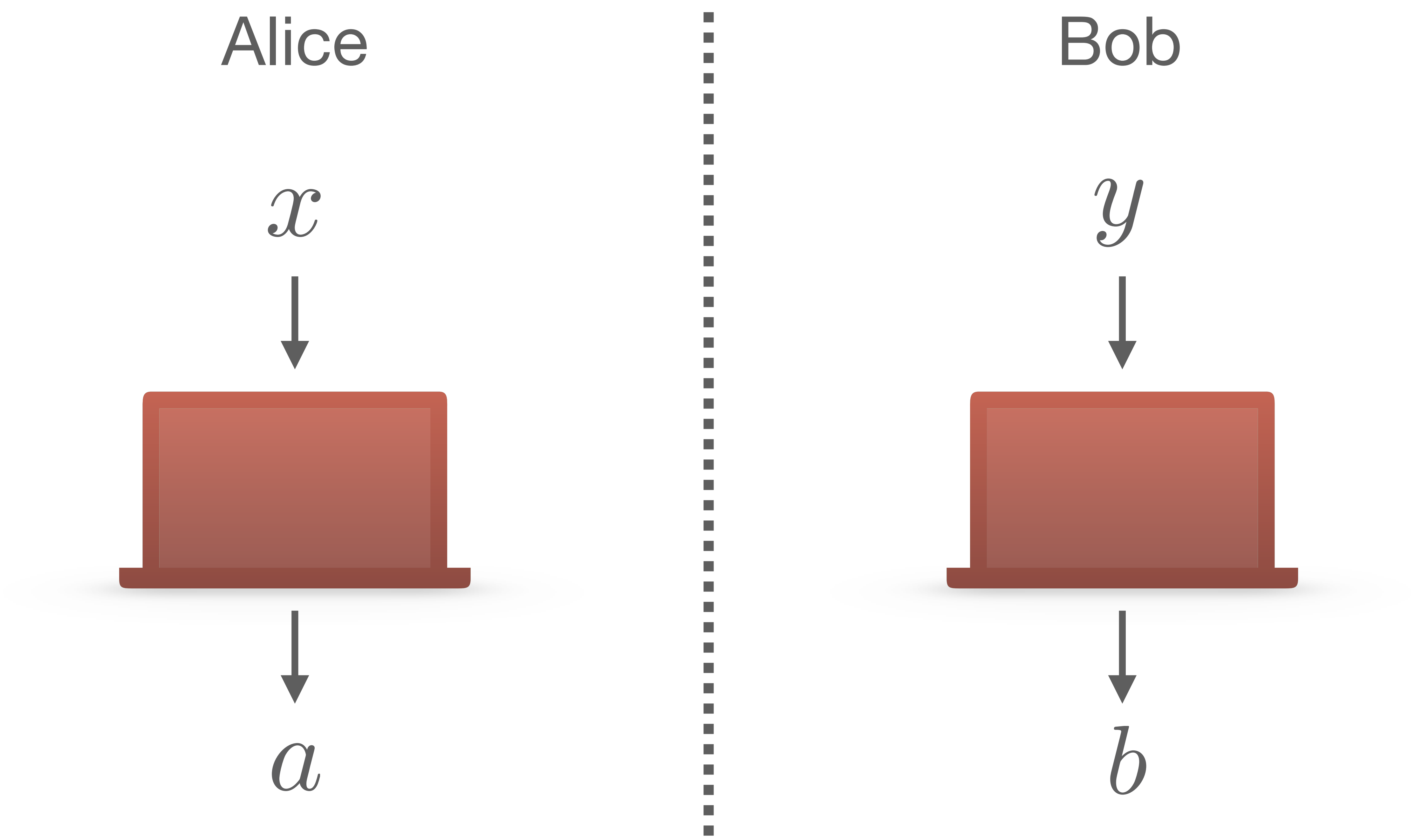
How Can That Be?

- How can we create keys this way?



- There's one thing we do know (can enforce)– the partition to Alice and Bob
- Similar to a multi-prover setting

Non-Local Games

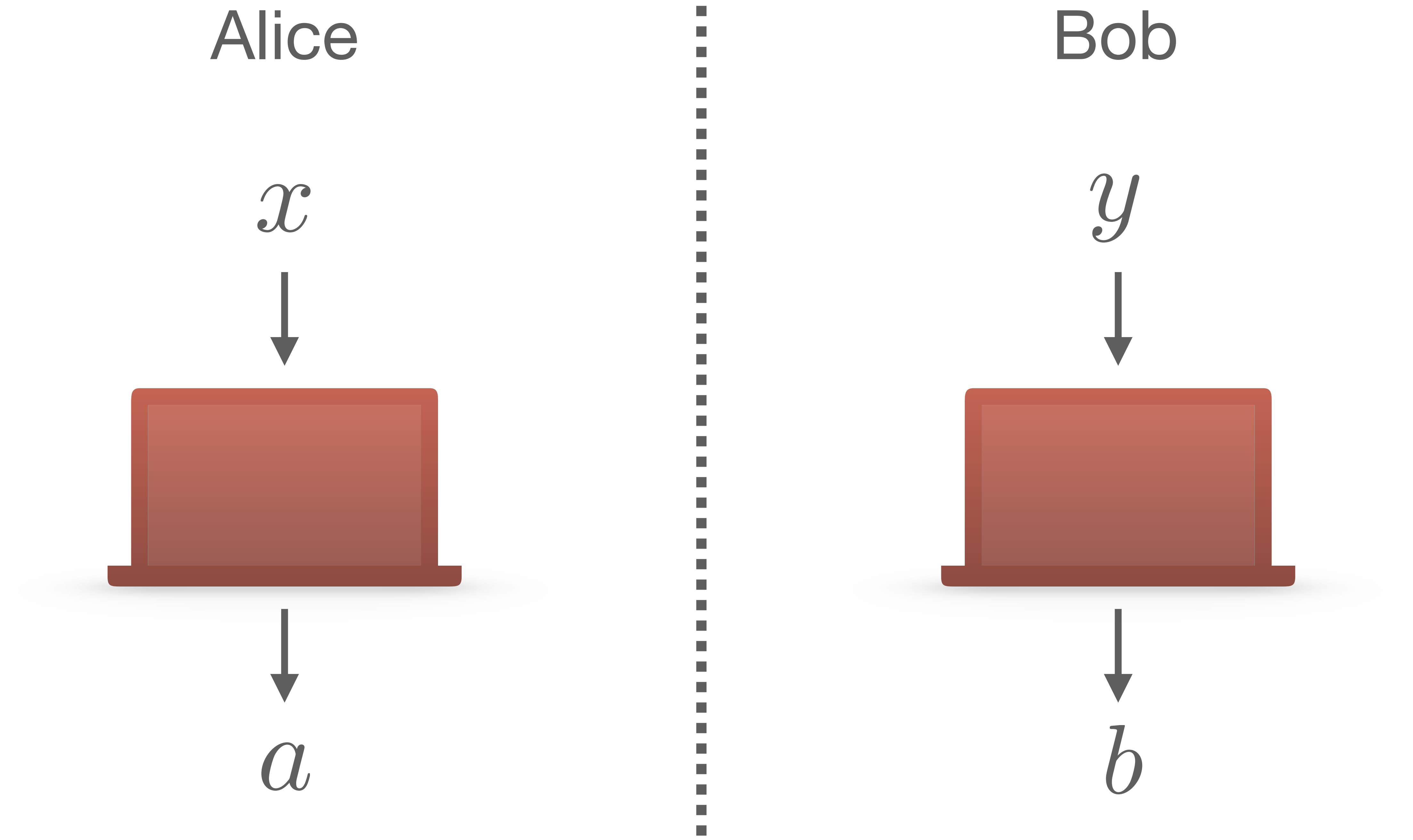


(Multi-prover proof system)

CHSH Game:

Alice:	Input	$x \in \{0,1\}$
	Output	$a \in \{0,1\}$
Bob:	Input	$y \in \{0,1\}$
	Output	$b \in \{0,1\}$
Win:	$a \oplus b = x \cdot y$	

Non-Local Games



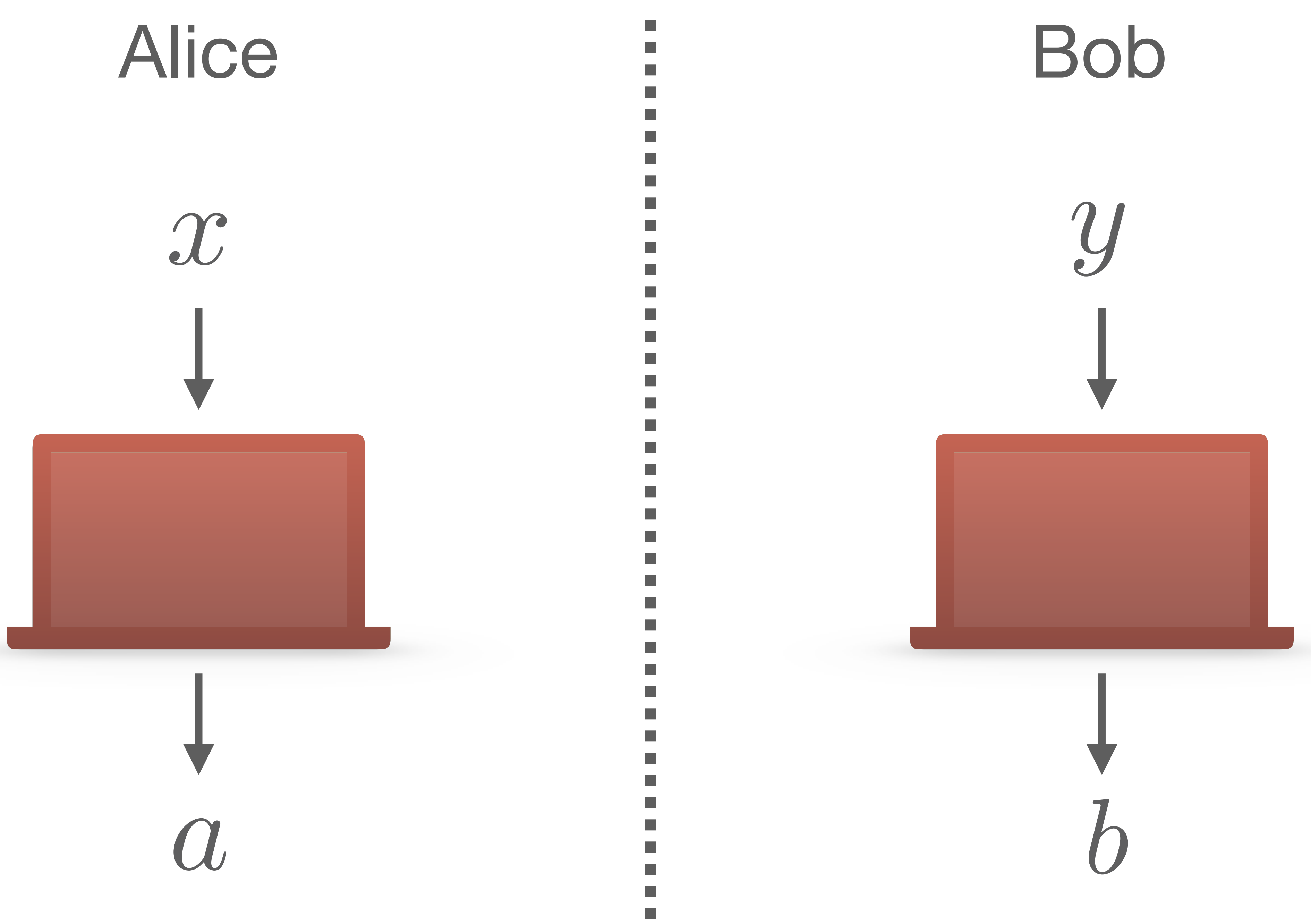
CHSH Game:

Alice:	Input	$x \in \{0,1\}$
	Output	$a \in \{0,1\}$
Bob:	Input	$y \in \{0,1\}$
	Output	$b \in \{0,1\}$
Win:	$a \oplus b = x \cdot y$	

Shared randomness

- Best classical strategy: 75% winning probability $p(ab|xy) = \sum_\lambda p(\lambda)p(a|x\lambda)p(b|y\lambda)$
- Best quantum strategy: ~85% winning probability $|\Phi^+\rangle_{AB}$

Non-Local Games



CHSH Game:

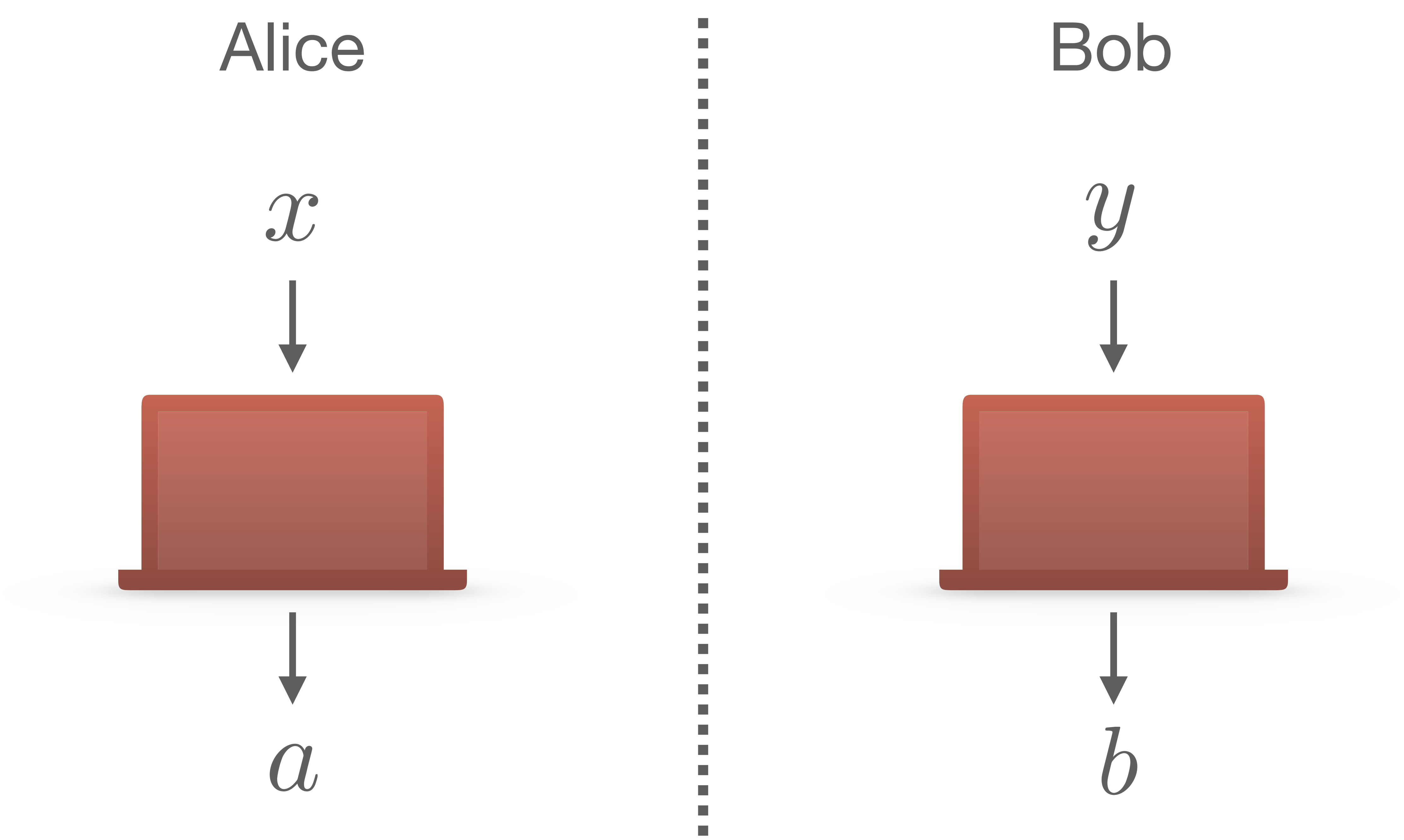
Alice:	Input	$x \in \{0,1\}$
	Output	$a \in \{0,1\}$
Bob:	Input	$y \in \{0,1\}$
	Output	$b \in \{0,1\}$
Win:	$a \oplus b = x \cdot y$	

- Best classical strategy: 75% winning probability
- Best quantum strategy: ~85% winning probability

} Quantum advantage

Cannot be simulated classically!

Non-Local Games

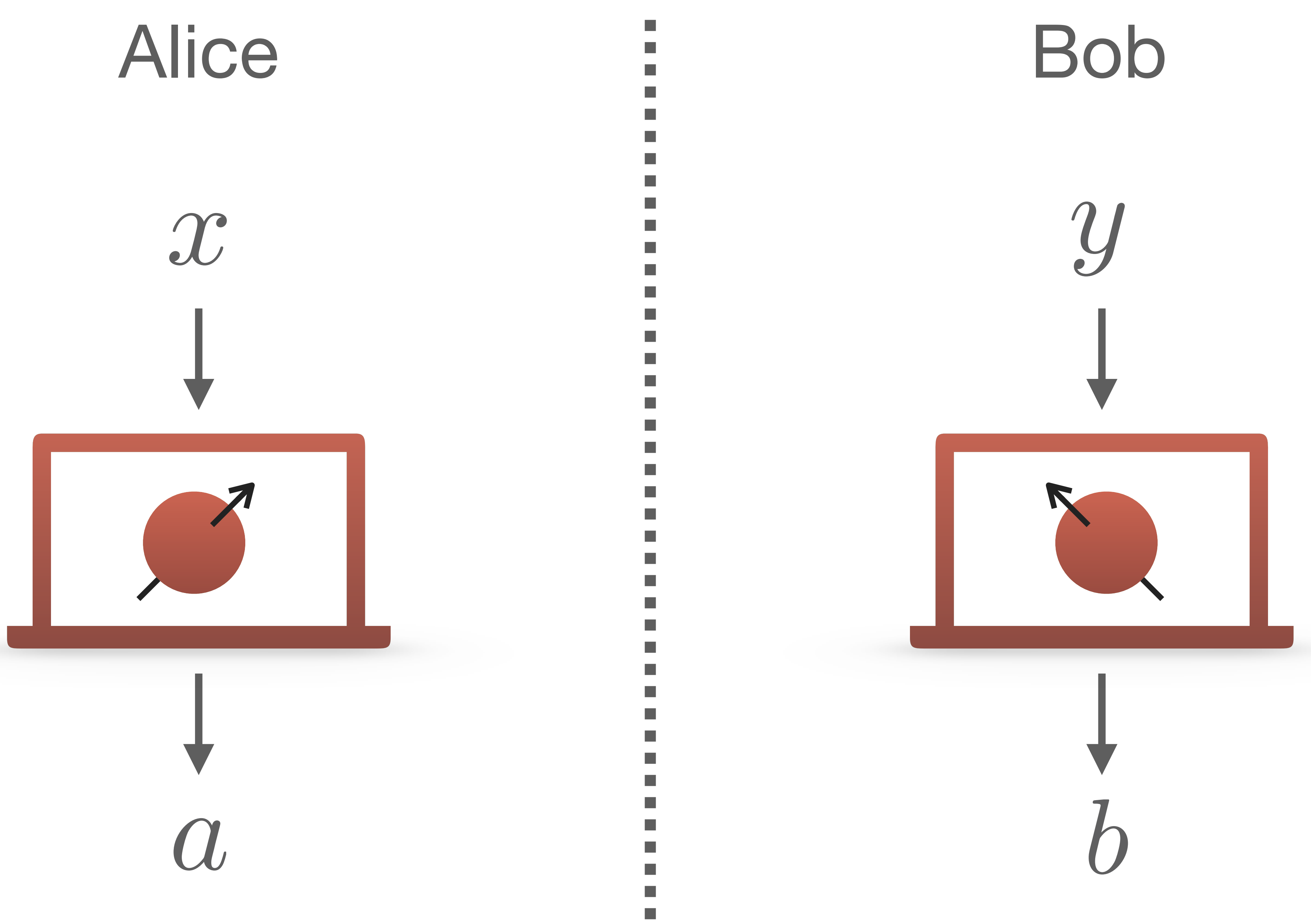


- Standard proof system: check if $w \in L$

- Best classical strategy: 75% winning probability
- Best quantum strategy: ~85% winning probability

} Quantum advantage

Non-Local Games



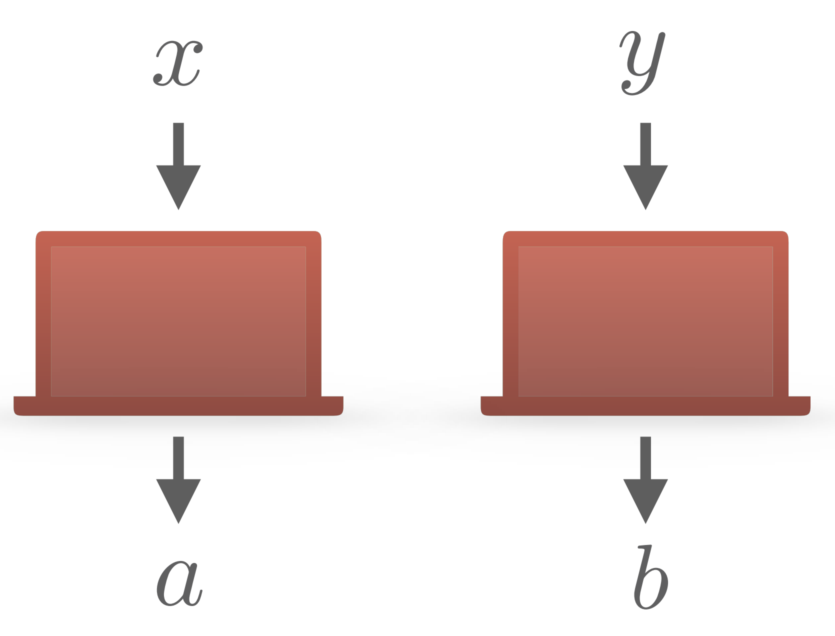
- Standard proof system: check if $w \in L$
- Non-local game: check if the device is **quantum**
- In fact– a certification of the production of **entropy**

- Best classical strategy: 75% winning probability
- Best quantum strategy: ~85% winning probability

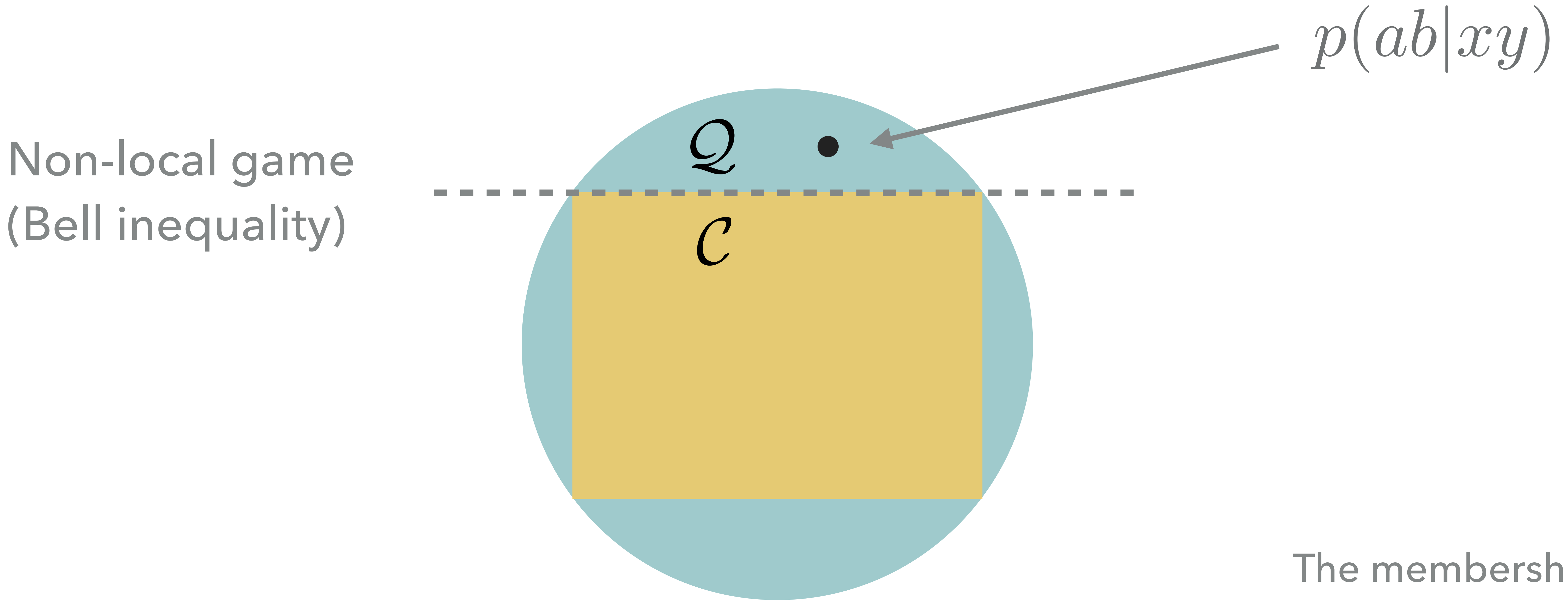
} Quantum advantage

Correlation Space

- The devices are described by a correlation $p(ab|xy)$
  - No assumption regarding the measurements/state/dimension



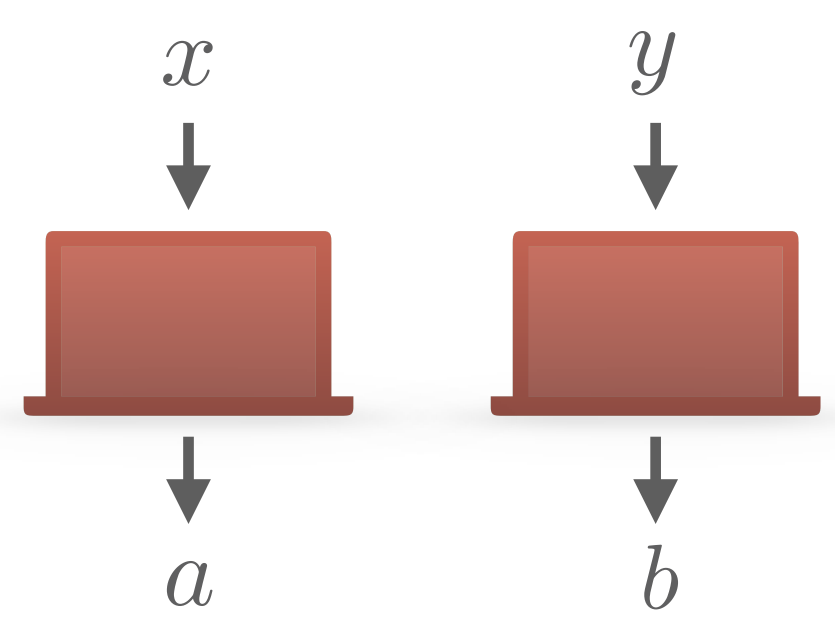
- Correlation space:



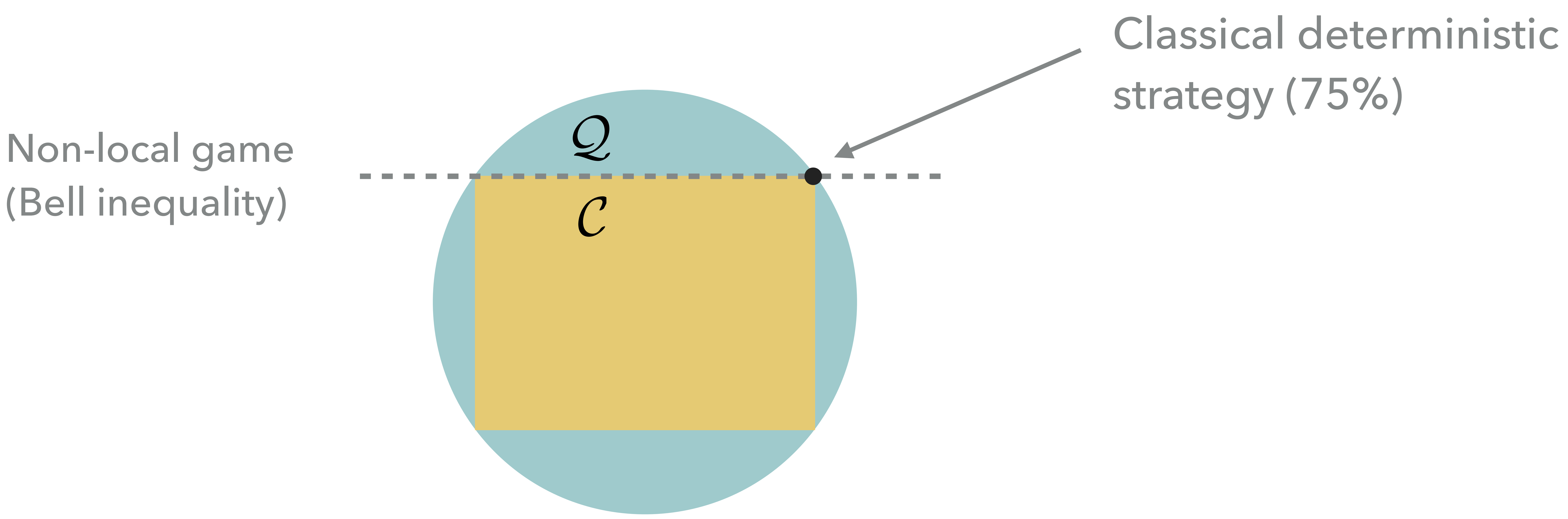
The membership in the quantum set problem is undecidable!

Correlation Space

- The devices are described by a correlation $p(ab|xy)$
  - No assumption regarding the measurements/state/dimension

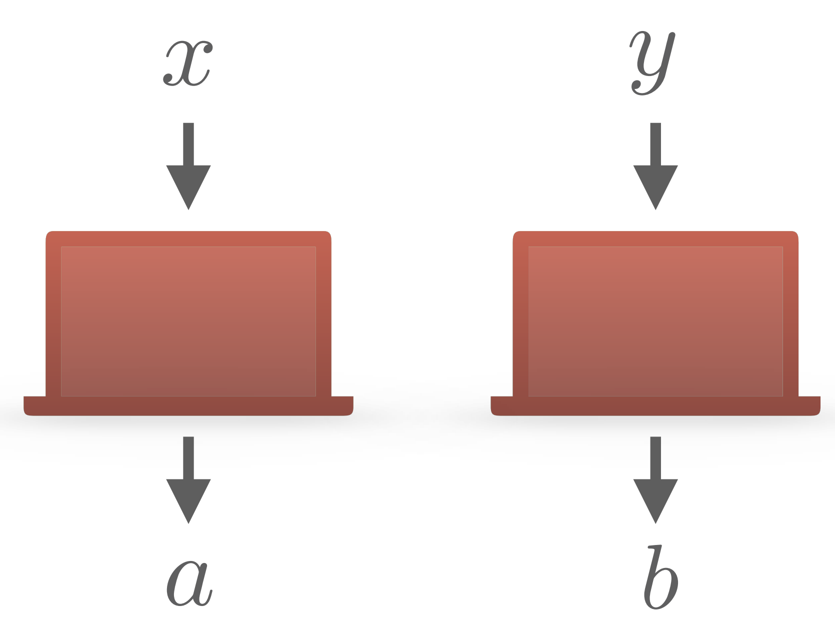


- Correlation space:

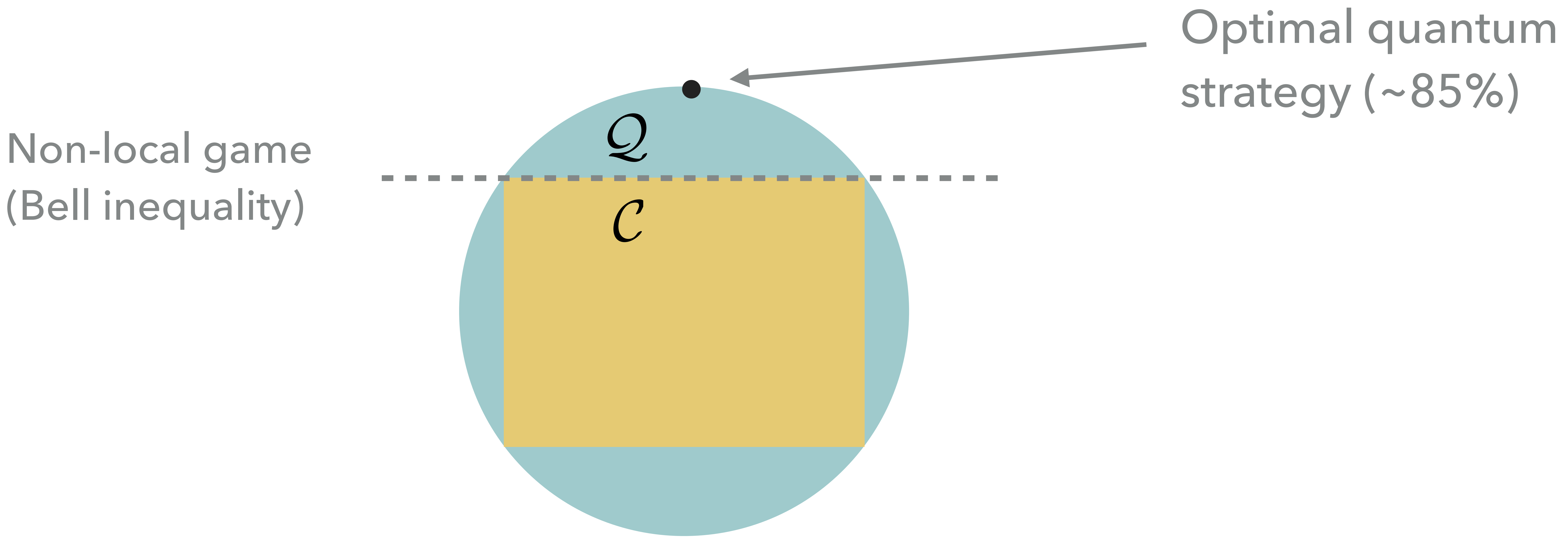


Correlation Space

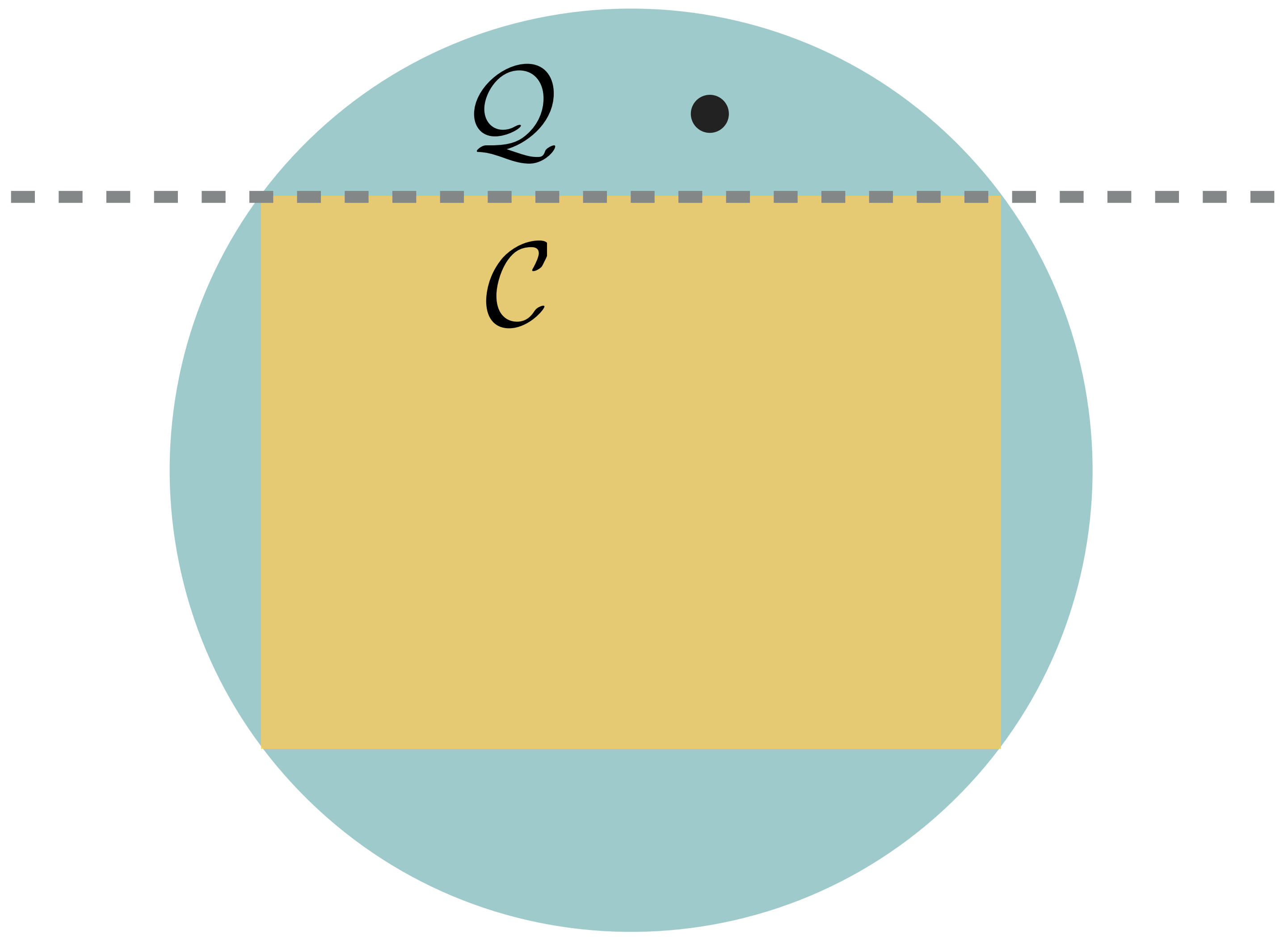
- The devices are described by a correlation $p(ab|xy)$
  - No assumption regarding the measurements/state/dimension

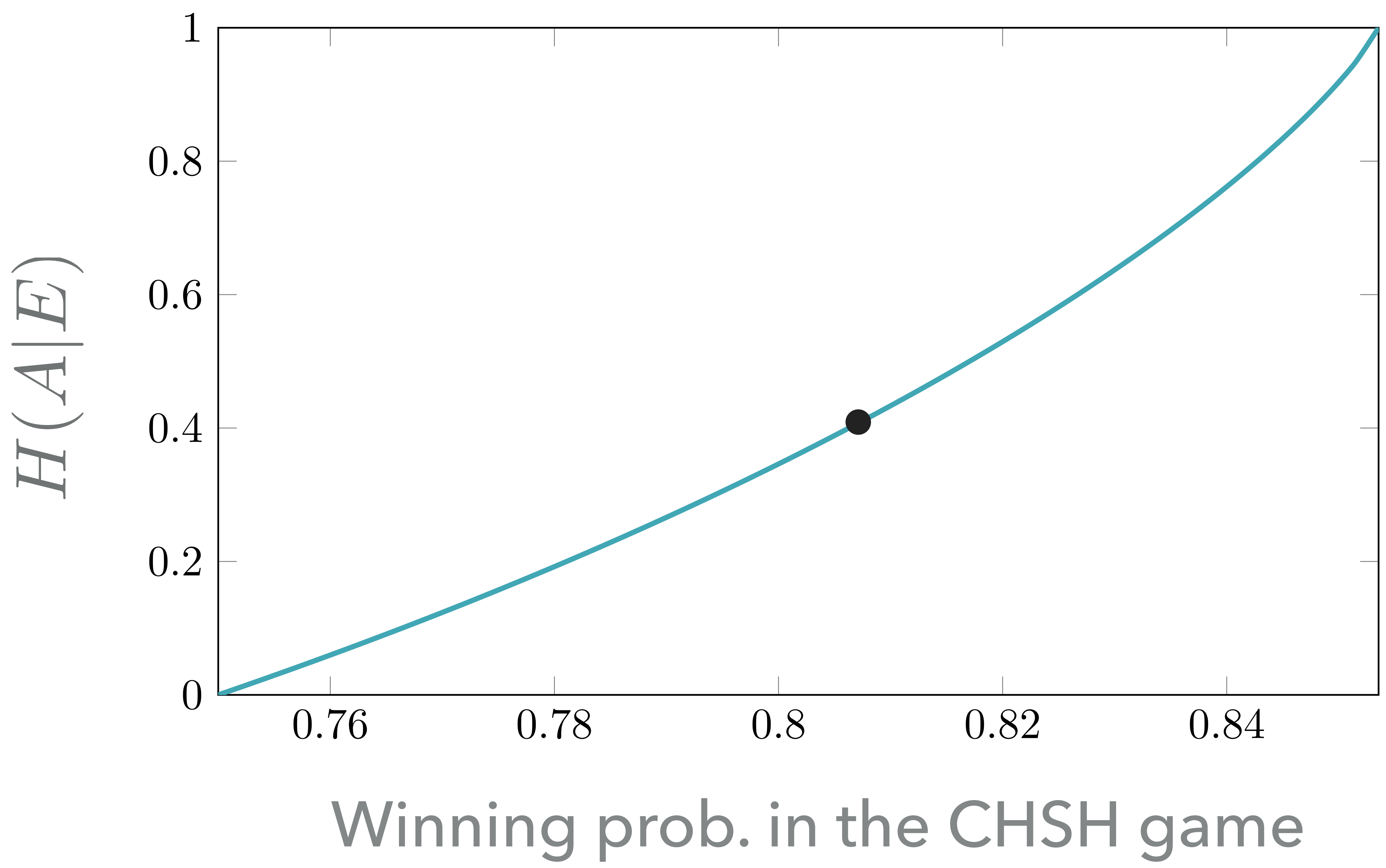


- Correlation space:



Certification of Entropy





Questions?

- Take-home message: quantum physics allows us to bound **Eve's knowledge** using **Alice and Bob's observed data**

DI Security Proof

1. **Winning a non-local game** $$H(A|E) \geq f(\text{win prob.})$$
   $$\downarrow$$
2. Entropy accumulation (Reduction to IID) $$H_{\min}^{\varepsilon}(\mathbf{A}|\mathbf{E})_{\rho} \geq nH(A|E)_{\sigma} - c_{\varepsilon}\sqrt{n}$$
   $$\downarrow$$
3. Quantum-proof extractors $$\|\rho_{\mathrm{Ext}(A,S)SE} - \rho_{U_\ell} \otimes \rho_{SE}\| \leq \varepsilon$$
   $$\downarrow$$
4. Secrecy $$(1 - \Pr(\text{abort}))\, \|\rho_{K_A E} - \rho_{U_\ell} \otimes \rho_E\| \leq \varepsilon_{\text{sec}}$$
   $$\downarrow$$
5. Security* (Secrecy + correctness + completeness)

“Disclaimers”

- This sequence of steps doesn’t always work
- There are QKD protocols whose security we don’t know how to prove
  - Among them protocols that are of high relevance in practice
- Looking for new protocols
  - **Two-way classical** post-processing (“advantage distillation”)
- Many “intermediate” models that we need to learn to analyze

QKD Take-Home Messages

- In QKD everything goes quantum
  - Composable security definitions (delicate!)
  - Entropies (delicate!)
  - Quantum-proof extractors (delicate!)
- The laws of quantum physics allow us to bound Eve's knowledge from the data that Alice and Bob observe during the execution of the protocol
- Quantitative bounds matter!

Thank you!