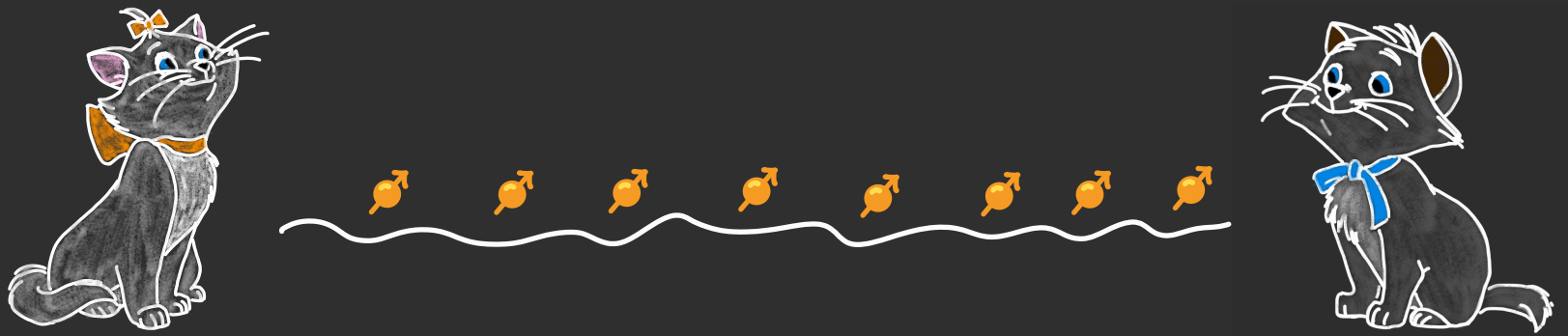
Composition of (quantum) communication protocols

Ramona Wolf
Universität Siegen



ATI Friday seminar

November 21, 2025

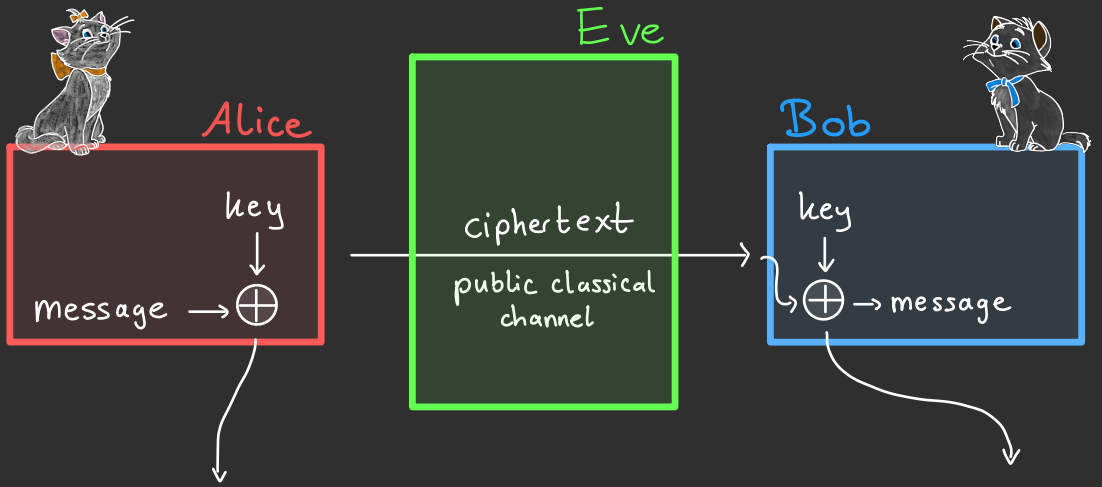
Goal: Secure communication

→ Messages cannot be tampered with

→ Messages cannot be overheard

Information-theoretic security

Unbreakable encryption scheme: The one-time pad

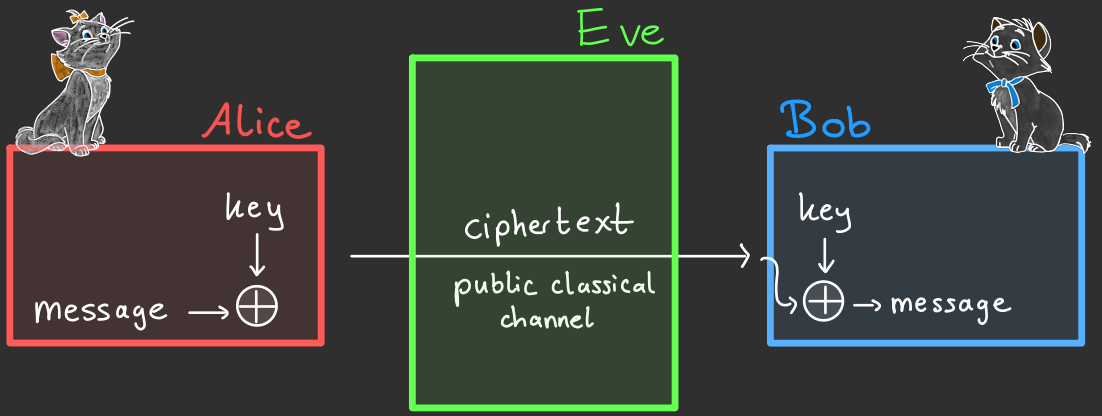


message 0 1 0 1 1 0 0 1 ...
random → key 1 0 0 1 0 1 0 0 ...
random → ciphertext 1 1 0 0 1 1 0 1 ...

ciphertext 1 1 0 0 1 1 0 1 ...
key 1 0 0 1 0 1 0 0 ...
message 0 1 0 1 1 0 0 1 ...

Information-theoretic security

Unbreakable encryption scheme: The one-time pad

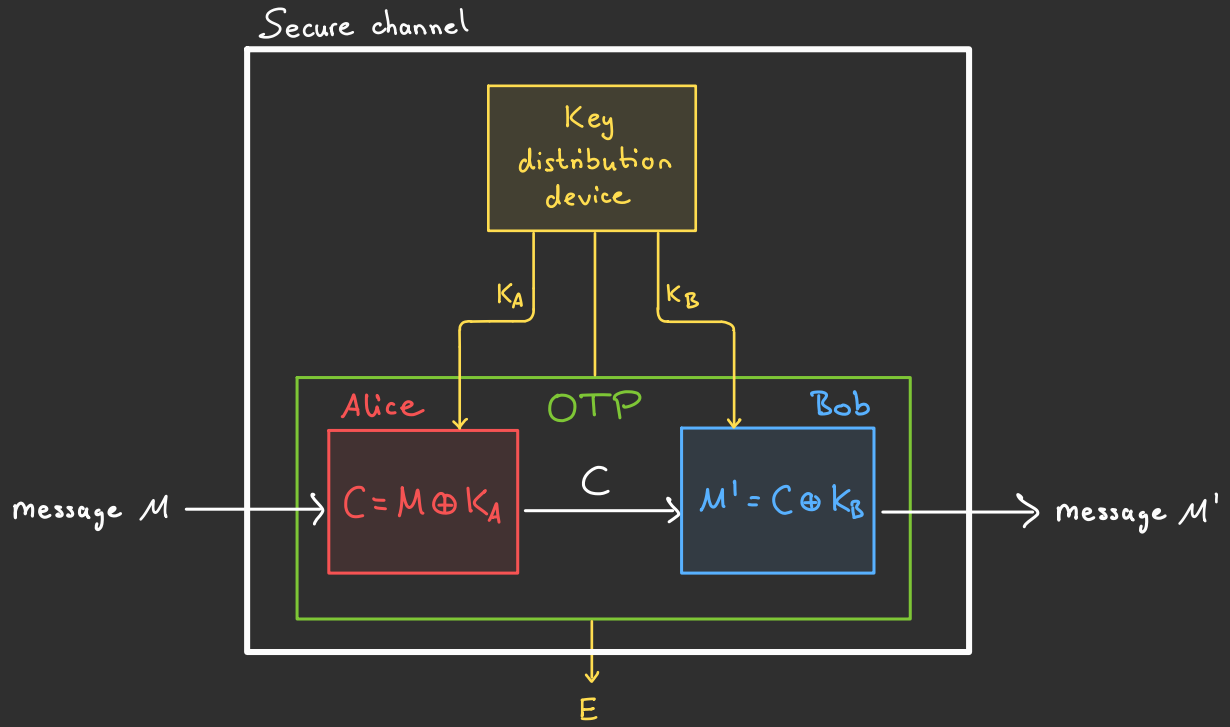


Cryptographic key:

1. Uniformly random
2. Identical for Alice and Bob
3. Unknown to Eve

} Allows for unbreakable encryption (Shannon, 1949)

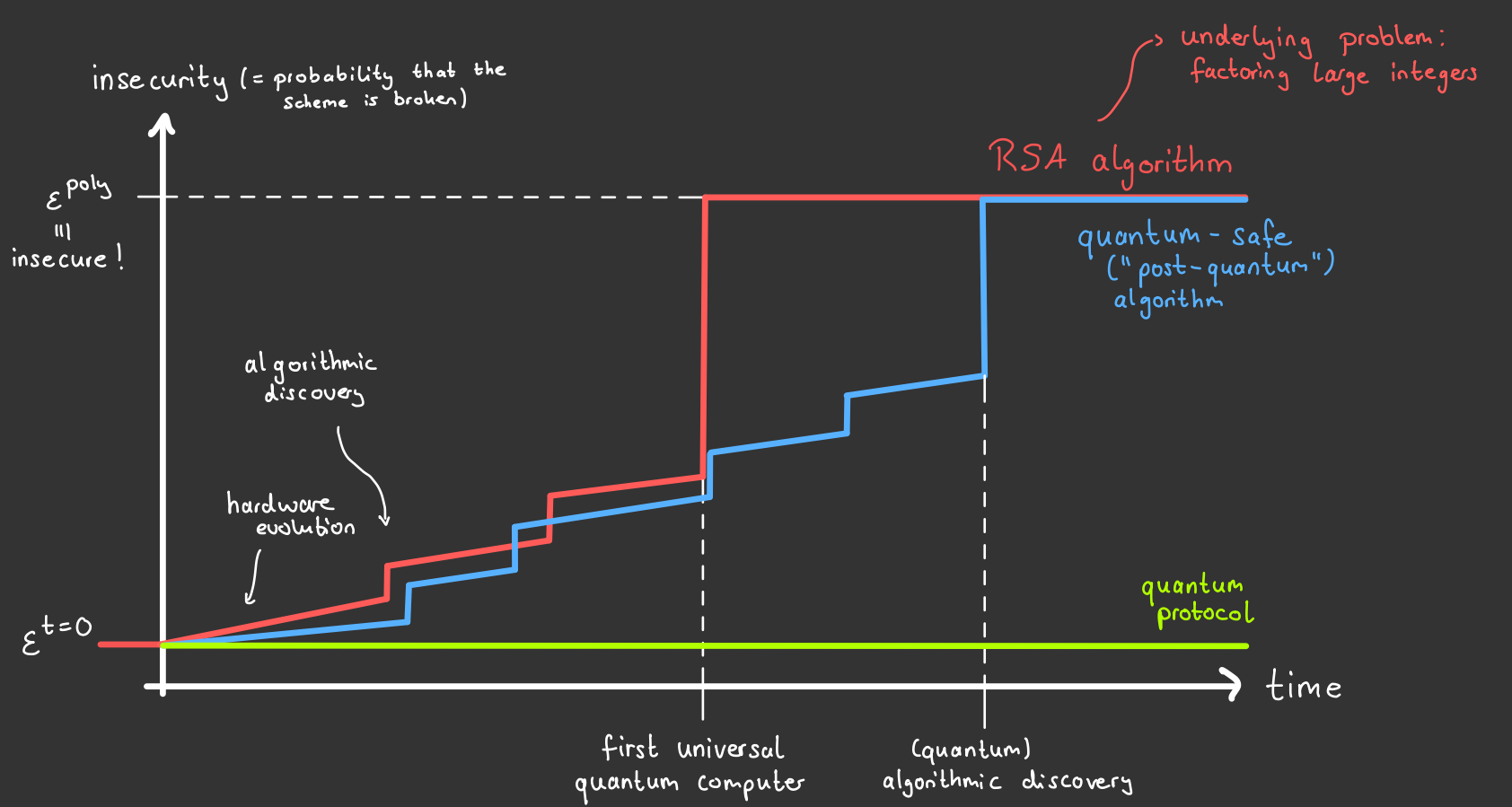
Composing protocols



Idea: Security of the whole system follows from security of its parts

(Security guarantee for OTP) + (Security guarante of key generation) $\Rightarrow$ Security guarantee for the channel

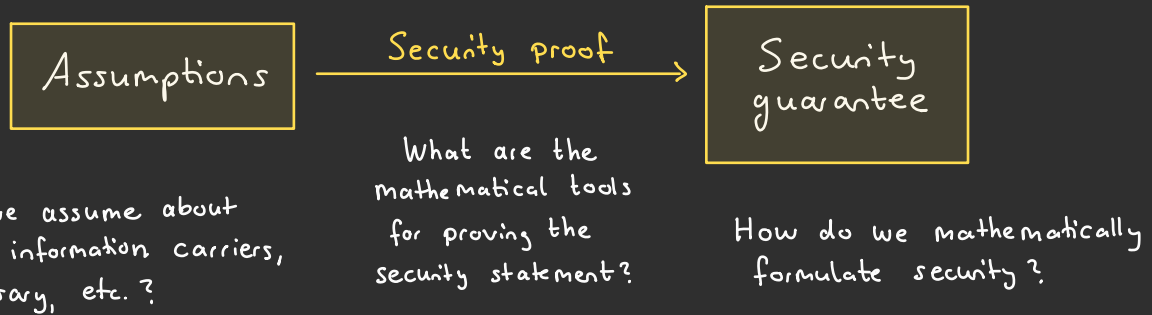
Why Quantum Cryptography?



Unbreakable security: Quantum key distribution

How is this achieved? → Security proof

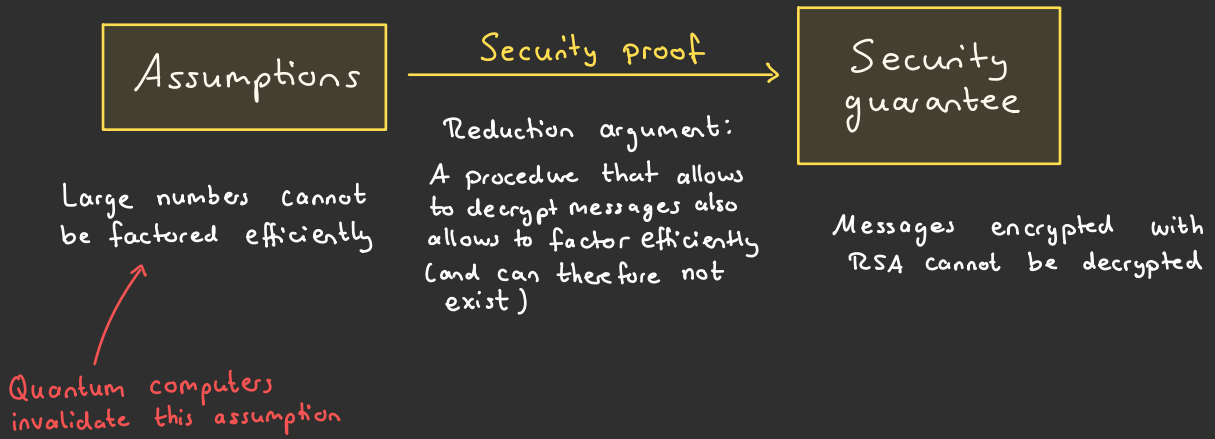
General structure:



Mathematical theorem → Should match physical reality!

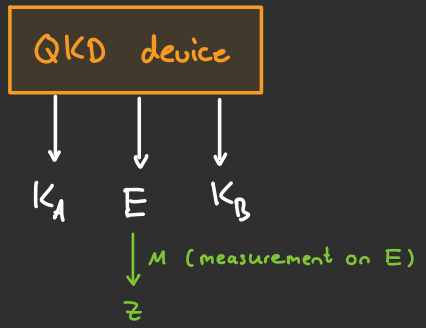
Unbreakable security: Quantum key distribution

Example: RSA encryption



Cautionary tale I:
Watch your definitions

How to define security?



Recall: Properties of a cryptographic key

1. Uniformly random
2. Identical for Alice and Bob
3. Unknown to Eve

Used in the early days of QKD security proofs

Proposal for security definition:

(i) $\Pr[K_A \neq K_B] \leq \varepsilon_1$ (captures 2.)

(ii) $\sup_M \frac{1}{2} \| P_{K_A Z} - P_U \times P_Z \| \leq \varepsilon_2$ (captures 1. + 3.)

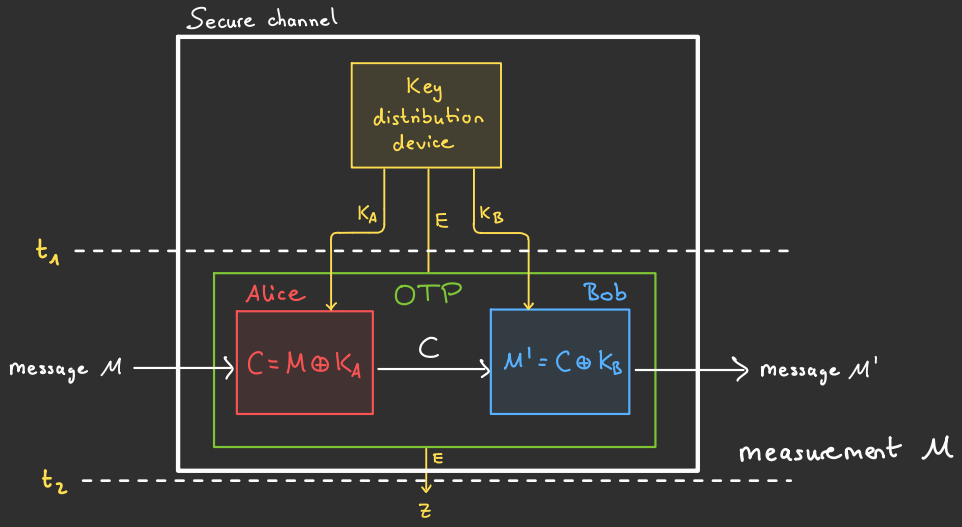
(P_U: uniform distribution)

$\Leftrightarrow I^{acc}(K_A:E) = \max_M I(K_A:Z) \leq \varepsilon_2'$

(I^{acc}: accessible information; I: mutual information)

Is this secure?
I.e., secure in any application?

Composability issue: Information locking



Security guarantee:

* $\Pr[K_A \neq K_B] \leq \varepsilon_1$
* $\max_M I(K_A : Z) \leq \varepsilon_2$

More natural: Put measurement M at the end of the whole protocol

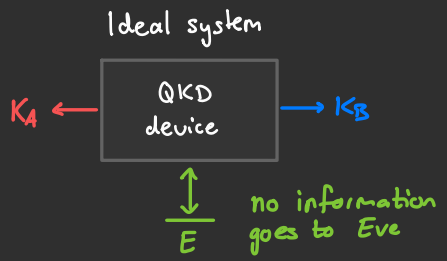
(keep quantum information as long as possible)

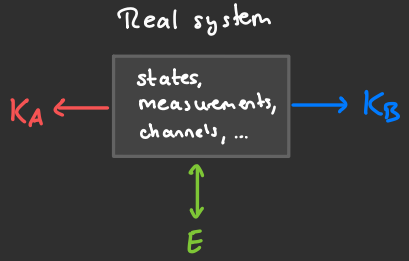
Composability issue: Optimal measurement at time t_2 might not be the same as at time t_1

→ There exist explicit attacks that exploit this fact
[König, Renner, Barnum, Maurer, 2006]

⇒ Paradigm shift in QKD due to composability issues

Solution: Composable security definition





Quantum state describing this system:

$$\rho^{ideal}_{K_A K_B E} = \frac{1}{|2^k|} \sum_k |k\times k|_{K_A} \otimes |k\times k|_{K_B} \otimes \rho_E$$

- $= Pr[key = k]$; $|2^k| =$ # keys of length k → each possible key is equally likely
- k = whole key, i.e., 0100101111... → Alice & Bob share the same key
- Eve has no information about the key

described by $\rho^{real}_{K_A K_B E}$

Security definition:

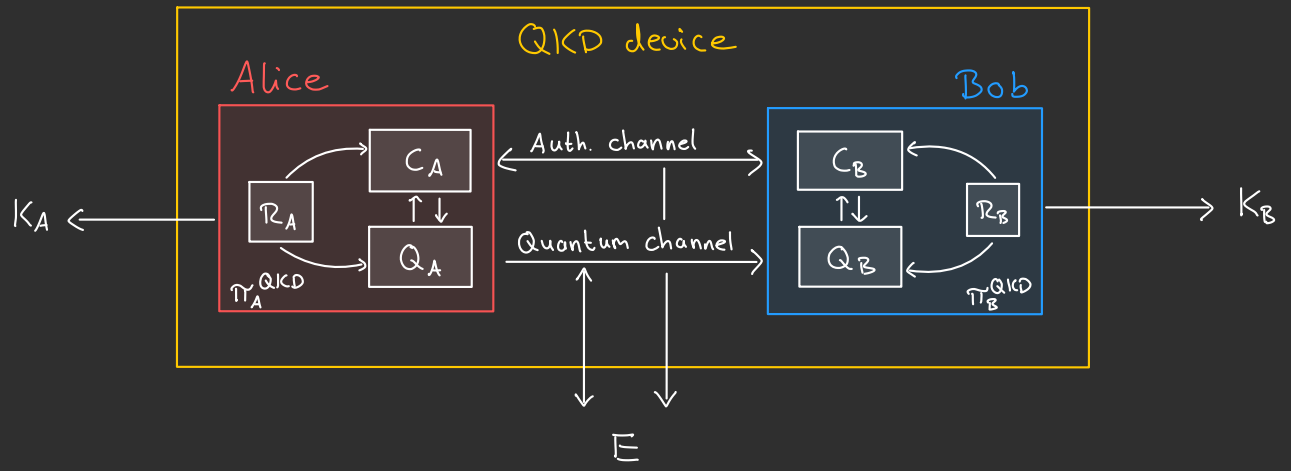
A QKD protocol is ε-secure if

$$\| \rho^{real}_{K_A K_B E} - \rho^{ideal}_{K_A K_B E} \|_1 \leq \varepsilon.$$

↳ has been derived within a composable framework, so it guarantees security in any application

Cautionary tale Ⅱ:
Watch your assumptions

Composability & Device-independent QKD



Device-independence: Treat Q_A and Q_B as black boxes

→ no assumption about their inner workings

We have security proofs for DIQKD for the composable security definition

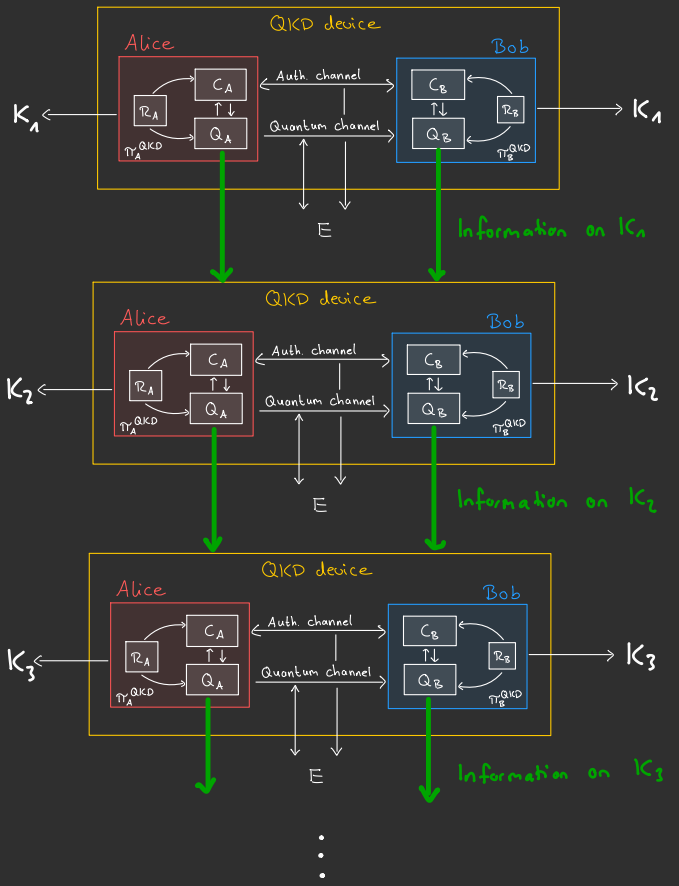
What can go wrong?

Composability & Device-independent QKD

Round 1:

Round 2:

Round 3:



Problem:
Behaviour of Q_A, Q_B in round 2 can reveal information about K_1

Example:
K_1 is a bit string, i.e., a number. Q_A, Q_B could force the protocol to abort starting from the round that corresponds to K_1.

Composability & Device-independent QKD

Issue: The composability framework used to derive the security definition does not allow us to reuse the devices

→ another composability issue!

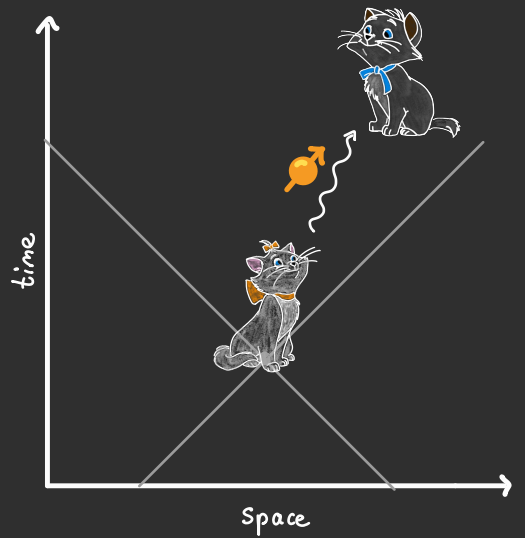
⇒ DIQKD is only secure if we assume that the devices are memoryless

→ goes against the fundamental idea of device-independence

How to solve this?

We need to extend the framework to allow for reusing devices

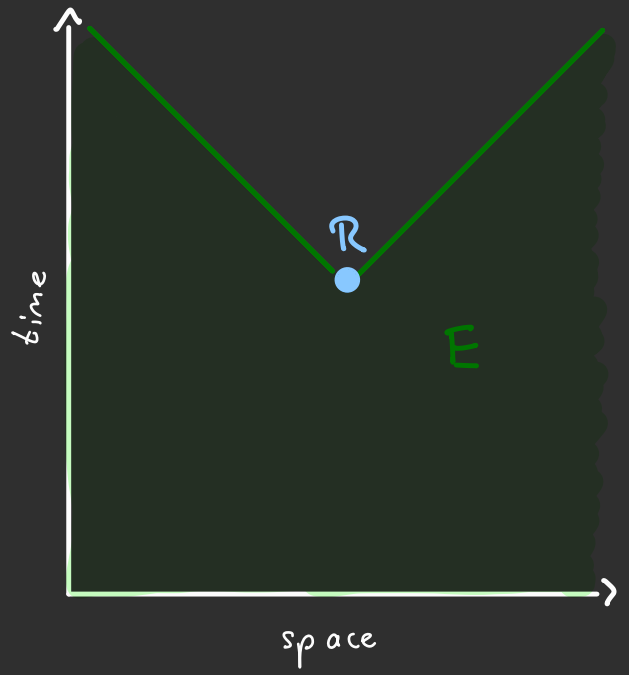
A framework for (quantum) communication protocols in spacetime



based on joint work with Renato Renner (in preparation)

Challenge: How to define randomness?

What is randomness?



Intuitively:

Someone who has access to all the knowledge in region E should not be able to predict R.

How to formalise this mathematically?

Classical: $P_{RE} = P_U \times P_E$

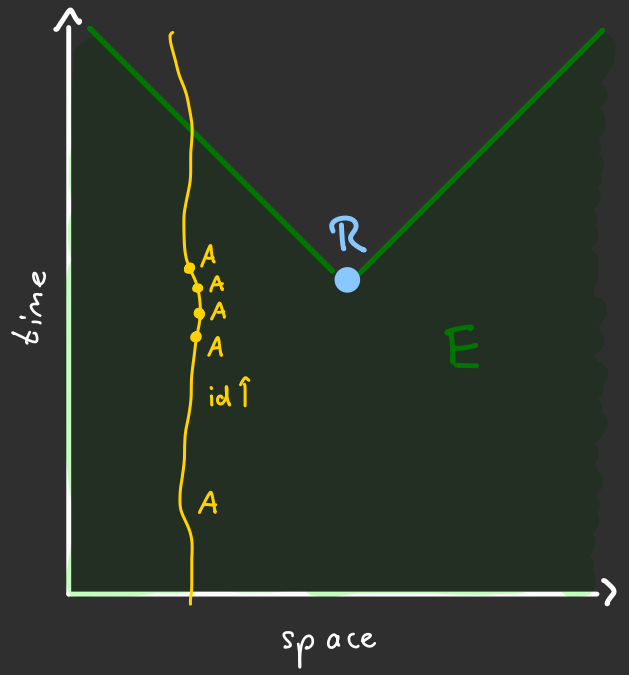
↑ uniform distribution

Quantum: $\rho_{RE} = \rho_R \otimes \rho_E$?

Does not exist!

Challenge: How to define randomness?

What is randomness?



The issue with ρ_E:

$$\rho_E = \rho_A \otimes \rho_A \otimes \rho_A \otimes \rho_A \otimes \dots$$

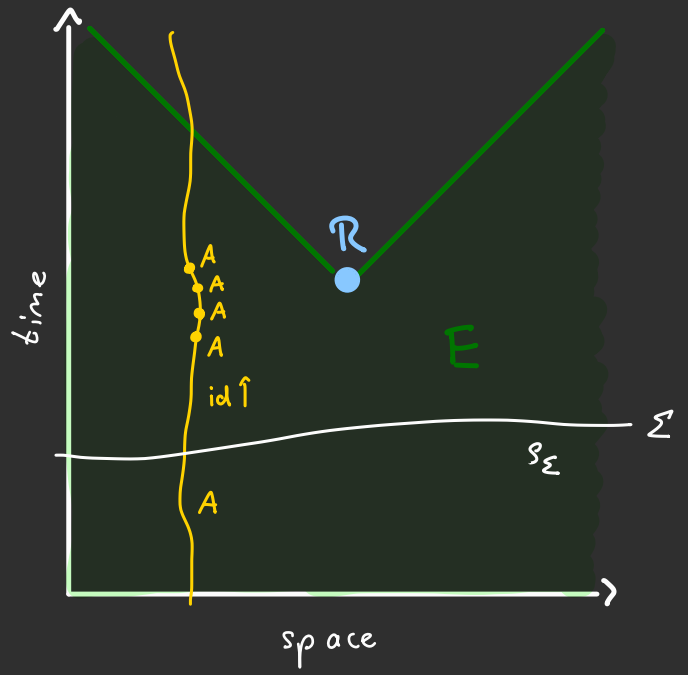
⇒ Many copies of the same quantum state!

⇒ Can build maps between spacetime regions that can clone arbitrary quantum systems

Violates the no-cloning theorem!

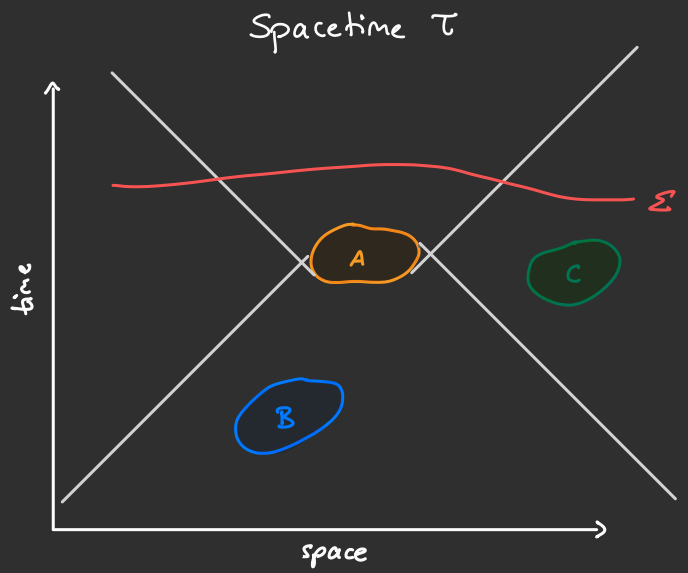
Challenge: How to define randomness?

What is randomness?

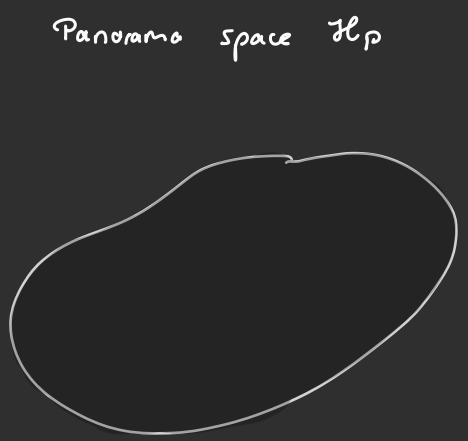


Quantum states are - a priori - only defined on time slices Σ

The framework: General idea



Indicates which regions / objects we are interested in

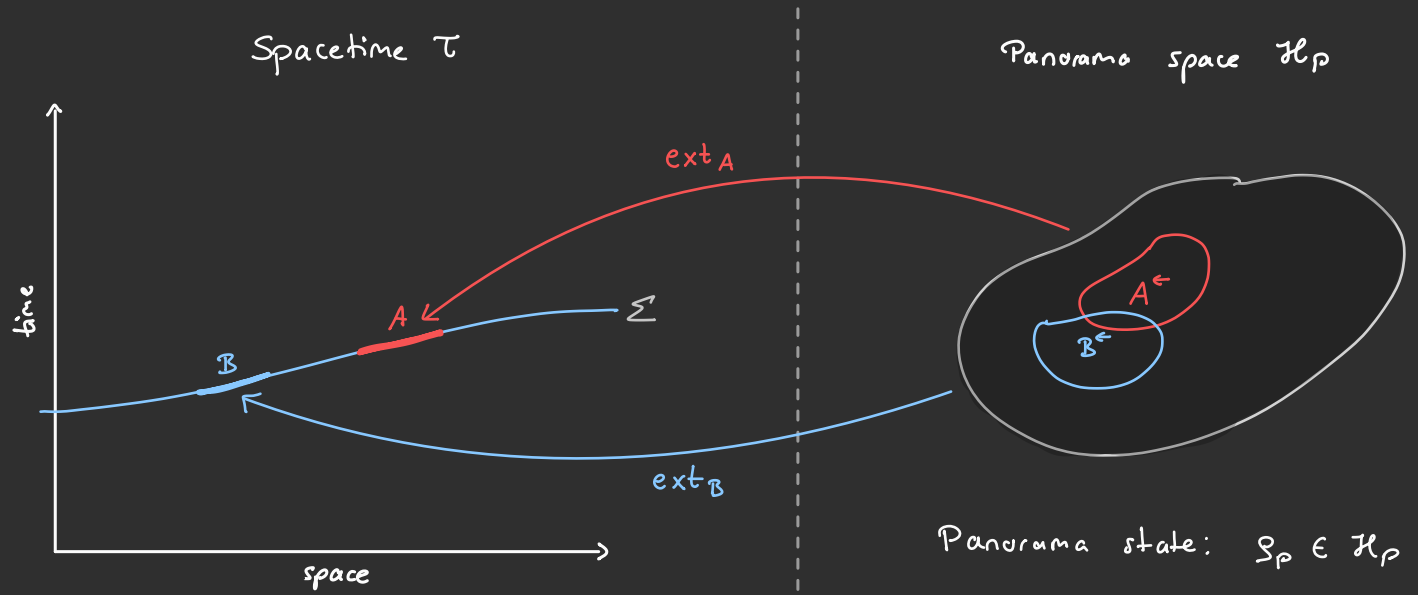


Panorama state: $\mathcal{S}_P \in \mathcal{H}_P$

Contains <u>all</u> information about the world at any time (past / future)

The framework: General idea

Most important part: Connection between the two spaces via "extraction maps"



Panorama state: $\mathcal{S}_P \in \mathcal{H}_P$

$A^\blacktriangleleft, B^\blacktriangleleft$: representations of A, B contain all information about the spacetime regions

can overlap!

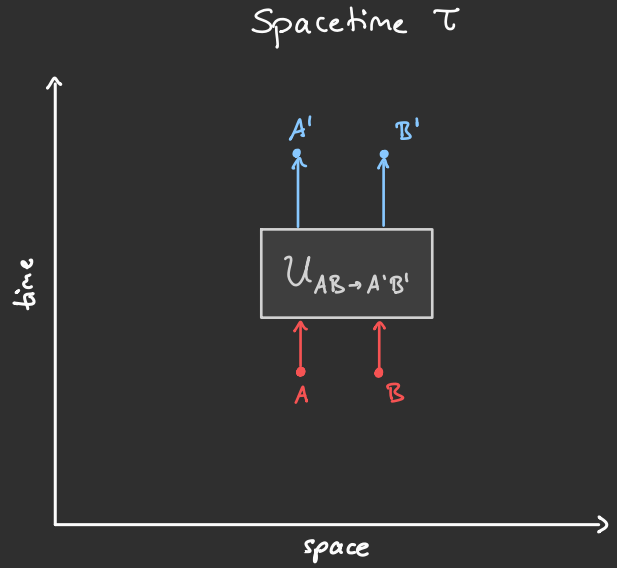
Definition: Representation

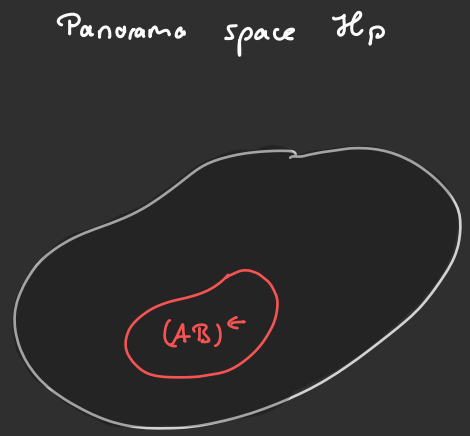
$A^\blacktriangleleft$ is a representation of A if ext_A is independent of $(A^\blacktriangleleft)^c$:

$$ext_A = \mathcal{M}_{A^\blacktriangleleft \to A} \circ tr_{(A^\blacktriangleleft)^c}.$$

The framework: General idea

Example: Unitary map

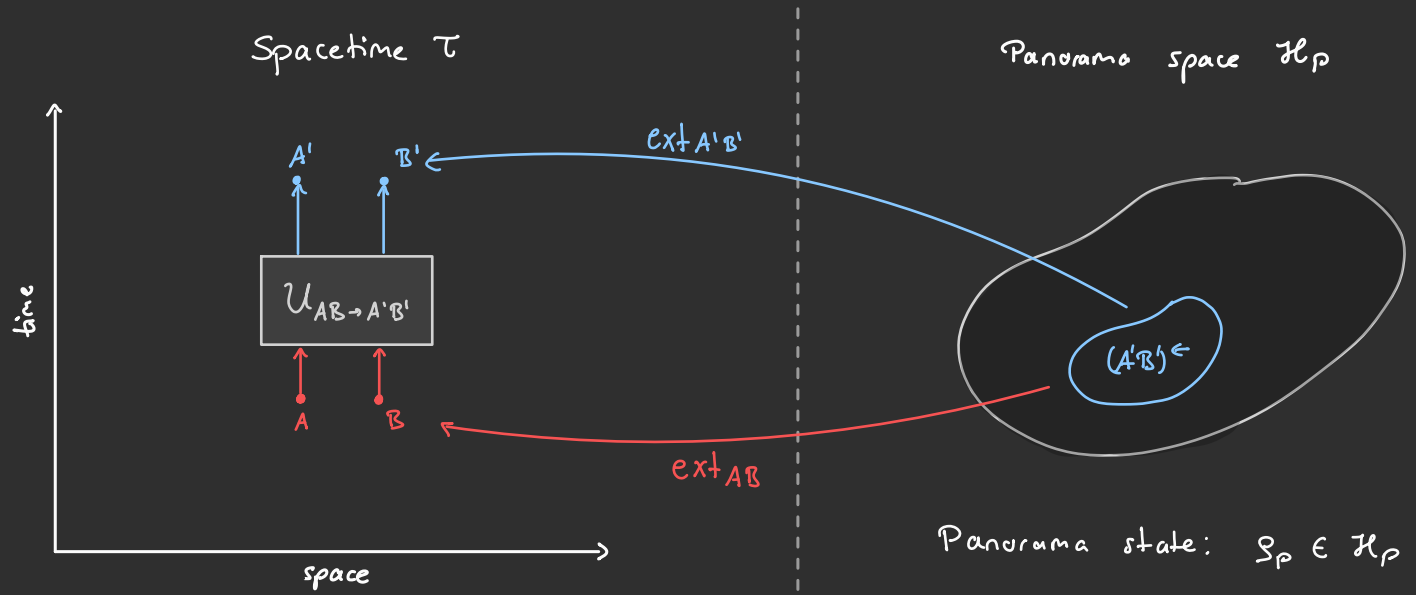




Panorama state: $\mathcal{S}_P \in \mathcal{H}_P$

The framework: General idea

Example: Unitary map



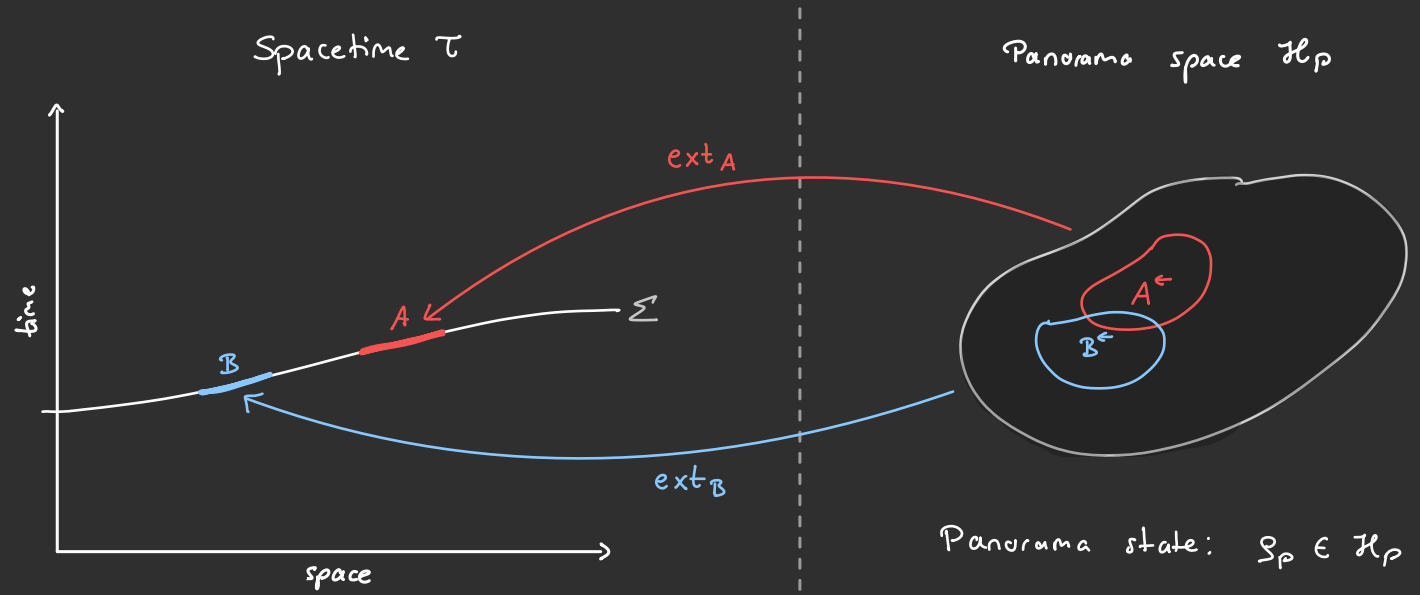
Panorama state: $\varsigma_P \in \mathcal{H}_P$

All information that is in $A'B'$ was already in AB.

$$ext_{A'B'} = U_{AB \to A'B'} \circ ext_{AB}$$

The framework: General idea

Most important part: Connection between the two spaces via "extraction maps"



Panorama state: $\mathcal{S}_P \in \mathcal{H}_P$

$A^\leftarrow, B^\leftarrow$: representations of A, B contain all information about the spacetime regions

can overlap!

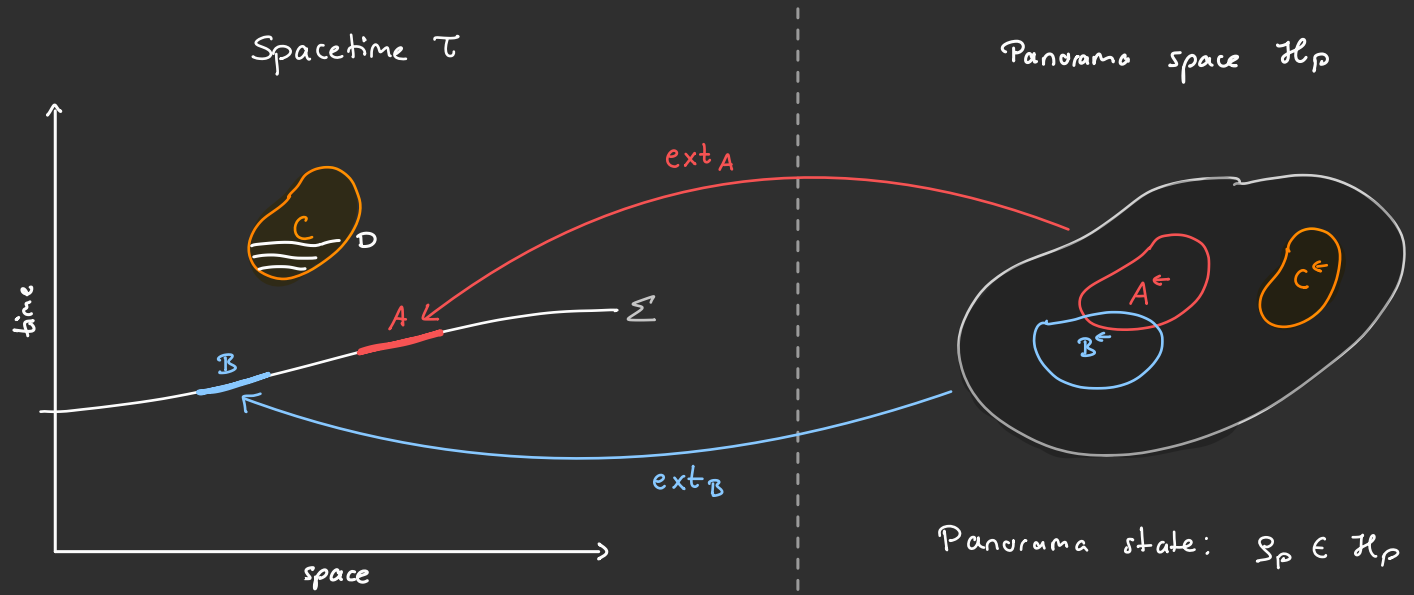
Definition: Representation

$A^\leftarrow$ is a representation of A if ext_A is independent of $(A^\leftarrow)^c$:

$$ext_A = \mathcal{M}_{A^\leftarrow \to A} \circ tr_{(A^\leftarrow)^c}.$$

The framework: General idea

Most important part: Connection between the two spaces via "extraction maps"



Panorama state: $\mathcal{S}_P \in \mathcal{H}_P$

Also works for spacetime regions!

→ Can assign a state $\mathcal{S}_{C^{\leftarrow}}$ to a spacetime region

Definition: Representation

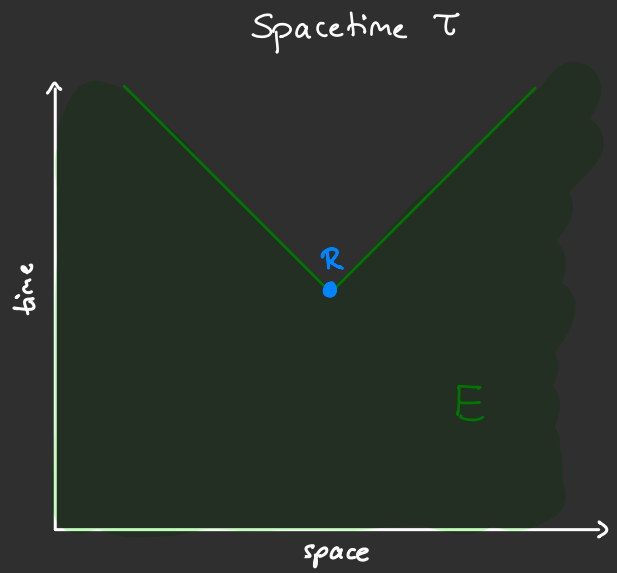
$C^{\leftarrow}$ is a representation of C if ext_D is independent of $(C^{\leftarrow})^c$

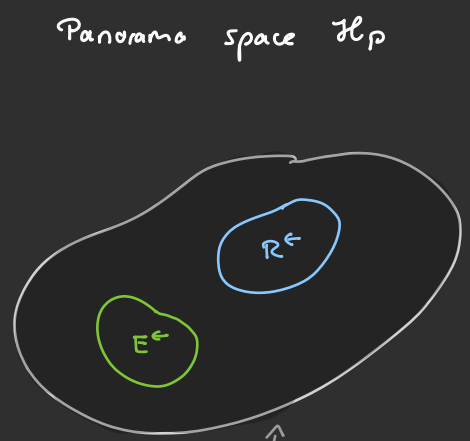
$\forall D \subset A$:

$$ext_D = \mathcal{M}_{C^{\leftarrow} \to D} \circ tr_{(C^{\leftarrow})^c}.$$

The framework: General idea

Application: Randomness





Definition: A system R is called random if it is independent of E, i.e., there exist representations R^{ϵ} and E^{ϵ} such that

$$\rho_{R^{\epsilon}E^{\epsilon}} = \rho_{R^{\epsilon}} \otimes \rho_{E^{\epsilon}}$$

and $\rho_R = \pi_R$ (maximally mixed).

The framework: General idea

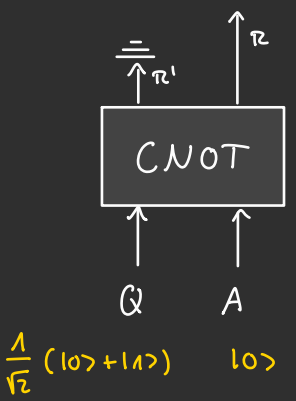
Application: Randomness

Definition: A system R is called random if it is independent of E, i.e., there exist representations R^{ϵ} and E^{ϵ} such that

$$\rho_{R^{\epsilon}E^{\epsilon}} = \rho_{R^{\epsilon}} \otimes \rho_{E^{\epsilon}} \quad (*)$$

and $\rho_R = \pi_R$ (maximally mixed).

Important: There exists a protocol that can achieve this!



$$\rho_R = \mathrm{tr}_{R'}\left(|\Psi\rangle\langle\Psi|_{RR'}\right) = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) = \pi_R$$

$$|\Psi\rangle_{R'R} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

AND one can show $(*)$!

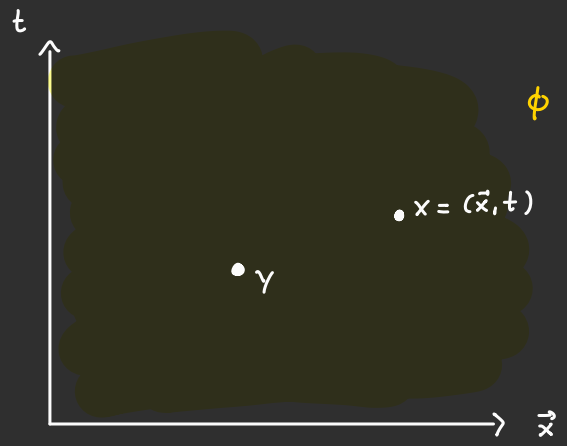
Why not Quantum Field Theory?

- Quantum field: $\phi(x) \quad \forall x \in T$
- Correlation functions:

$$\langle \Omega \mid \phi(x)\, \phi(y) \mid \Omega \rangle$$

- Scattering amplitudes

$$\langle \phi_F \mid e^{-iHT} \mid \phi_I \rangle, \qquad \phi(0) = \phi_I \quad \phi(T) = \phi_F$$



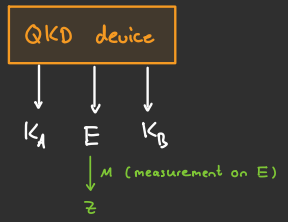
⇒ QFT expresses everything in term of the predicted statistics ($\hat{=}$ classical information)

Not sufficient for QKD!

Recall: 1st security definition was based on classical information

- $\Pr[K_A \neq K_B] \leq \varepsilon_1$
- $\sup_M \frac{1}{2} \left| P_{K_A Z} - P_U \times P_Z \right| \leq \varepsilon_2$

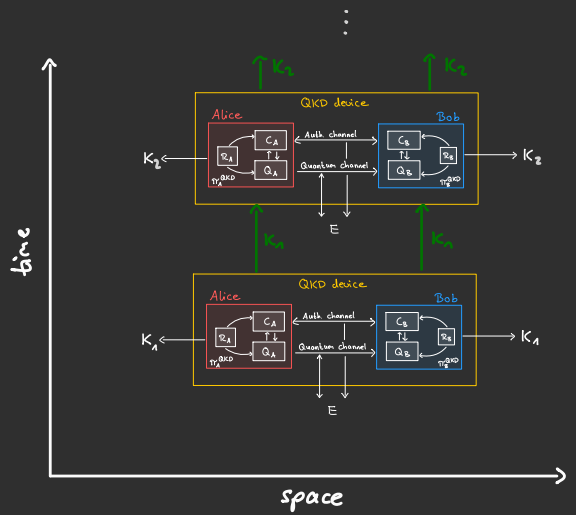
→ Composability issues



We need to be able to talk about quantum information!

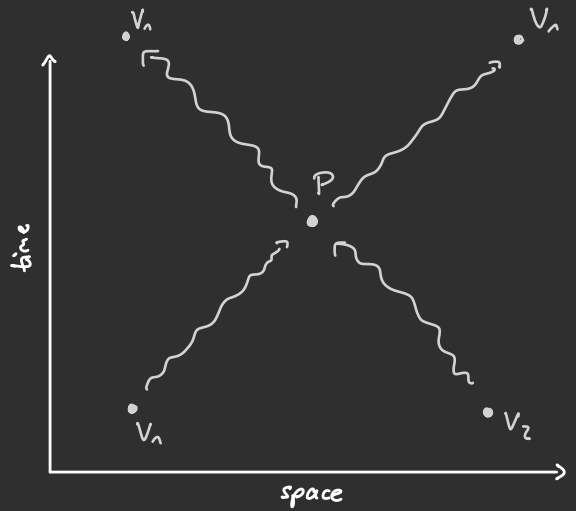
Outlook: Application to more protocols

DI QKD: Reusability of devices



→ Find a way to represent this in the abstract Hilbert space $\mathcal{H}_P$

Quantum position verification



Position of the party is a cryptographic credential