Why modelling randomness requires going beyond standard quantum information theory

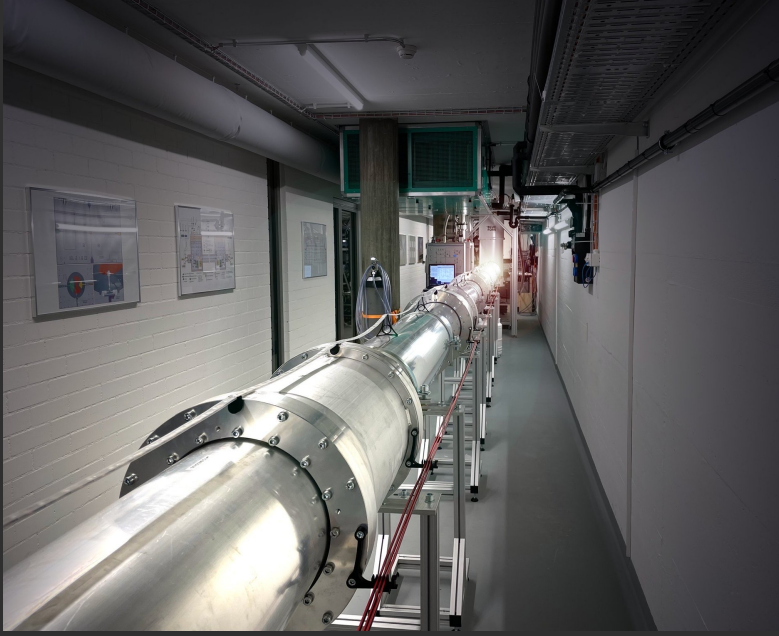
A panoramic model of quantum information in spacetime

Ramona Wolf
Universität Innsbruck

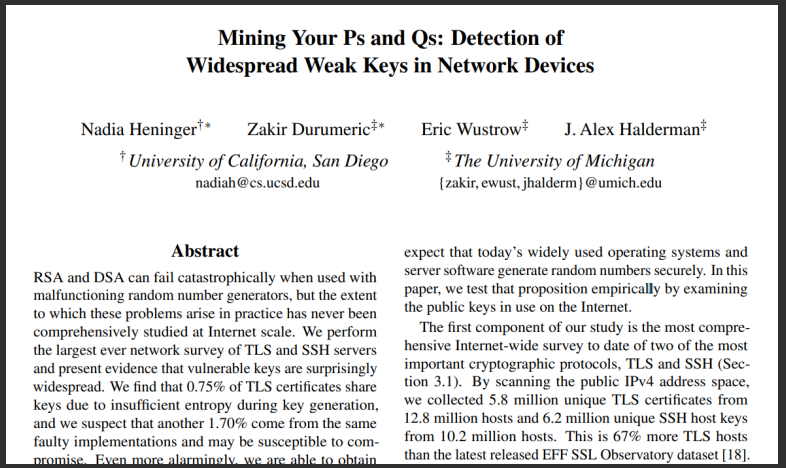
22.06.2026

7th Seefeld Workshop on Quantum Information

What is randomness ?



What is randomness ?



Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices

Nadia Heninger[†*] Zakir Durumeric[‡*] Eric Wustrow[‡] J. Alex Halderman[‡]

[†] *University of California, San Diego*
nadiah@cs.ucsd.edu

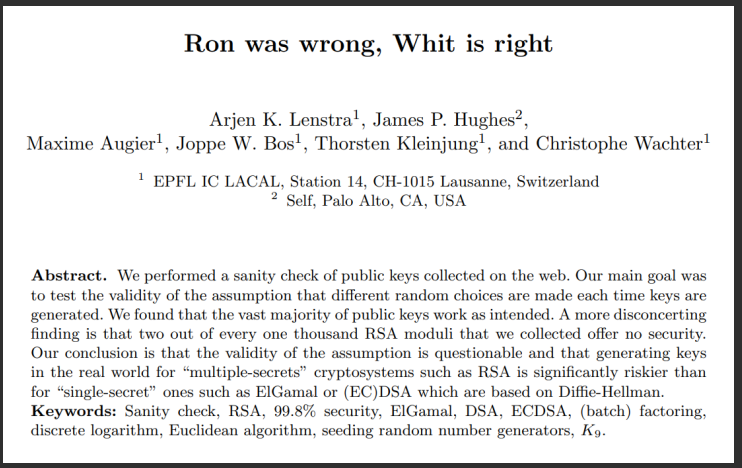
[‡] *The University of Michigan*
{zakir, ewust, jhalderm}@umich.edu

Abstract

RSA and DSA can fail catastrophically when used with malfunctioning random number generators, but the extent to which these problems arise in practice has never been comprehensively studied at Internet scale. We perform the largest ever network survey of TLS and SSH servers and present evidence that vulnerable keys are surprisingly widespread. We find that 0.75% of TLS certificates share keys due to insufficient entropy during key generation, and we suspect that another 1.70% come from the same faulty implementations and may be susceptible to compromise. Even more alarmingly, we are able to obtain

expect that today's widely used operating systems and server software generate random numbers securely. In this paper, we test that proposition empirically by examining the public keys in use on the Internet.

The first component of our study is the most comprehensive Internet-wide survey to date of two of the most important cryptographic protocols, TLS and SSH (Section 3.1). By scanning the public IPv4 address space, we collected 5.8 million unique TLS certificates from 12.8 million hosts and 6.2 million unique SSH host keys from 10.2 million hosts. This is 67% more TLS hosts than the latest released EFF SSL Observatory dataset [18].



Ron was wrong, Whit is right

Arjen K. Lenstra[1], James P. Hughes[2],
Maxime Augier[1], Joppe W. Bos[1], Thorsten Kleinjung[1], and Christophe Wachter[1]

[1] EPFL IC LACAL, Station 14, CH-1015 Lausanne, Switzerland
[2] Self, Palo Alto, CA, USA

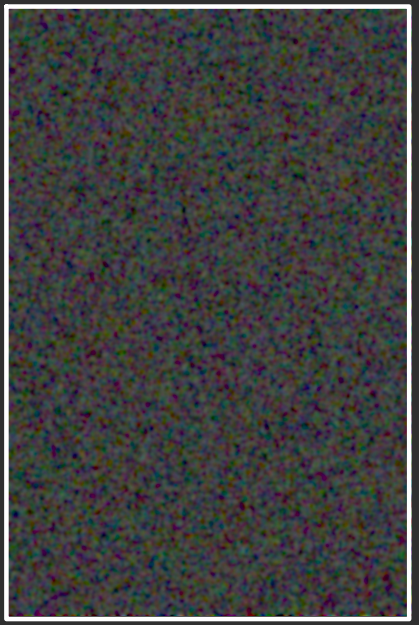
Abstract. We performed a sanity check of public keys collected on the web. Our main goal was to test the validity of the assumption that different random choices are made each time keys are generated. We found that the vast majority of public keys work as intended. A more disconcerting finding is that two out of every one thousand RSA moduli that we collected offer no security. Our conclusion is that the validity of the assumption is questionable and that generating keys in the real world for "multiple-secrets" cryptosystems such as RSA is significantly riskier than for "single-secret" ones such as ElGamal or (EC)DSA which are based on Diffie-Hellman.
Keywords: Sanity check, RSA, 99.8% security, ElGamal, DSA, ECDSA, (batch) factoring, discrete logarithm, Euclidean algorithm, seeding random number generators, K_9.

"RSA [...] can fail catastrophically when used with malfunctioning random number generators ..."

What is randomness ?

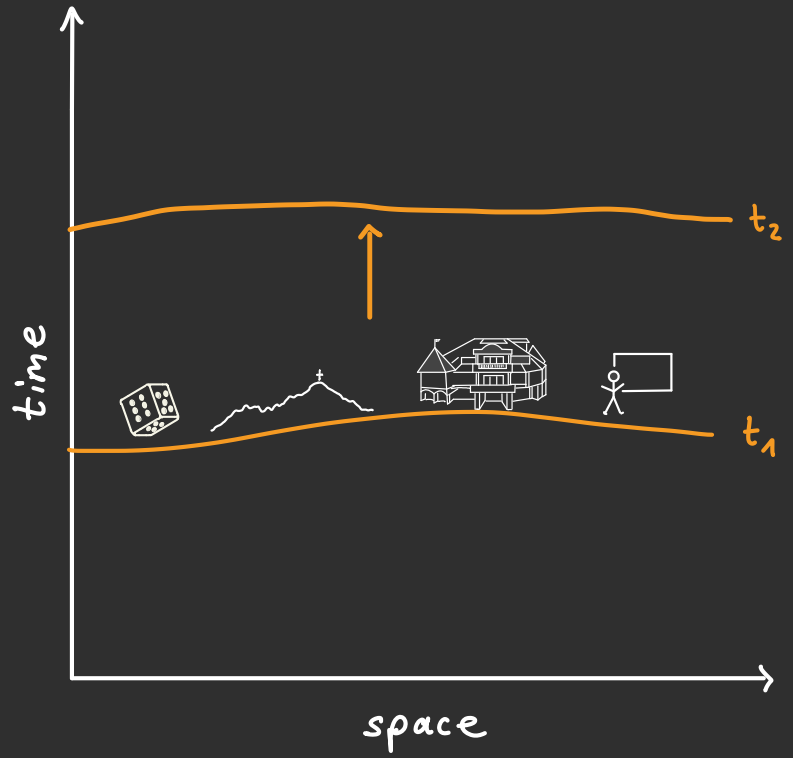
imperfect randomness

perfect randomness



How can randomness even exist?

random $\hat{=}$ unpredictable



Quantum mechanics:

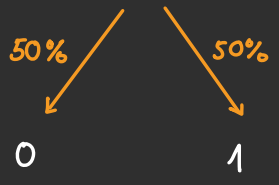
Everything evolves unitarily!

⇒ From an information theory perspective, there can never be anything new

no randomness ☹

How can randomness even exist ?

A quantum experiment: $\frac{1}{\sqrt{2}}\left(|0\rangle_Q + |1\rangle_Q\right)$



Measurement in computational basis

random bit

Unitary evolution: Model the measurement device $|\Psi\rangle_M$

$$\frac{1}{\sqrt{2}}\left(|0\rangle_Q + |1\rangle_Q\right)|\Psi\rangle_M \xmapsto{\text{measurement}} \frac{1}{\sqrt{2}}\left(|0\rangle_Q|0\rangle_M + |1\rangle_Q|1\rangle_M\right)$$

random bit ?

How can randomness even exist?

A quantum experiment:

requires a pure input state

$$\frac{1}{\sqrt{2}}\left(|0\rangle_Q + |1\rangle_Q\right)$$

50% → 0

50% → 1

Measurement in computational basis

random bit

$|\Psi\rangle_{universe}$ pure

ρ_Q - highly entangled with the rest

⇒ An all-powerful adversary can guess and/or influence the bit

Randomness is only possible

if we restrict the availability of information!

What does it take?

Defining randomness

If this was true, randomness would be impossible

- Random system R (e.g., bit string of length l)
- Knowledge of the adversary E (quantum system)

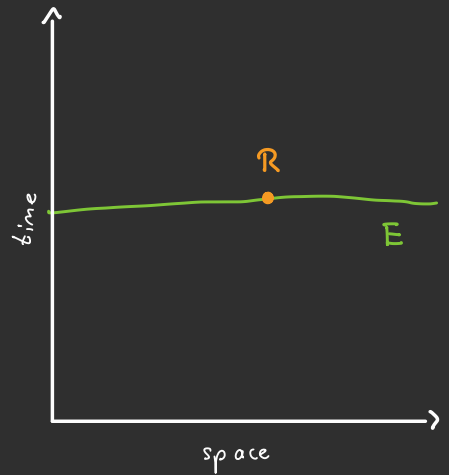
"Everything else"

Two properties:

1. Uniform distribution: $\rho_R = \frac{1}{2^l} \sum_{r \in \{0,1\}^l} |r\rangle\langle r|_R$

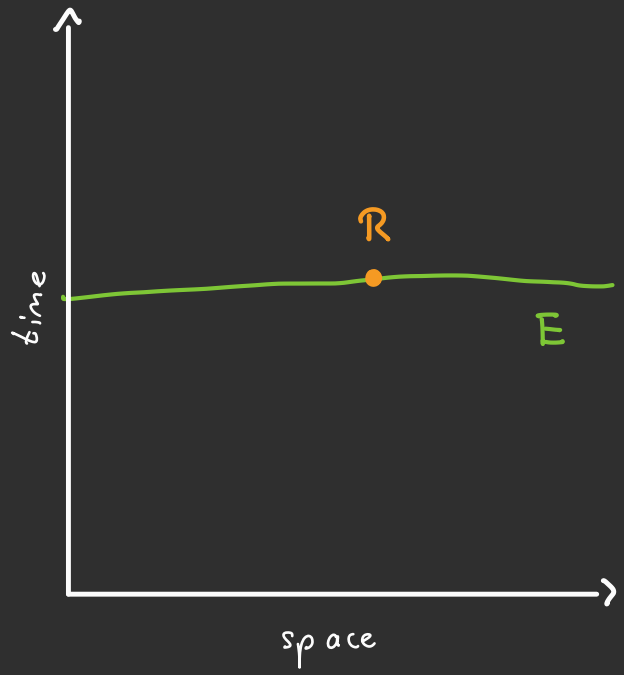
2. Independence: $\rho_{RE} = \rho_R \otimes \rho_E$

(State-of-the-art definition of randomness)

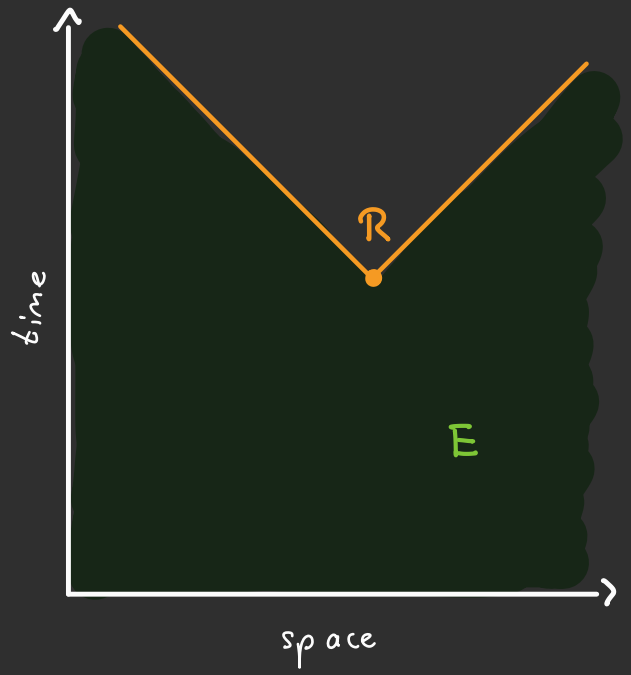


What does E contain?

Defining randomness



Defining 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?

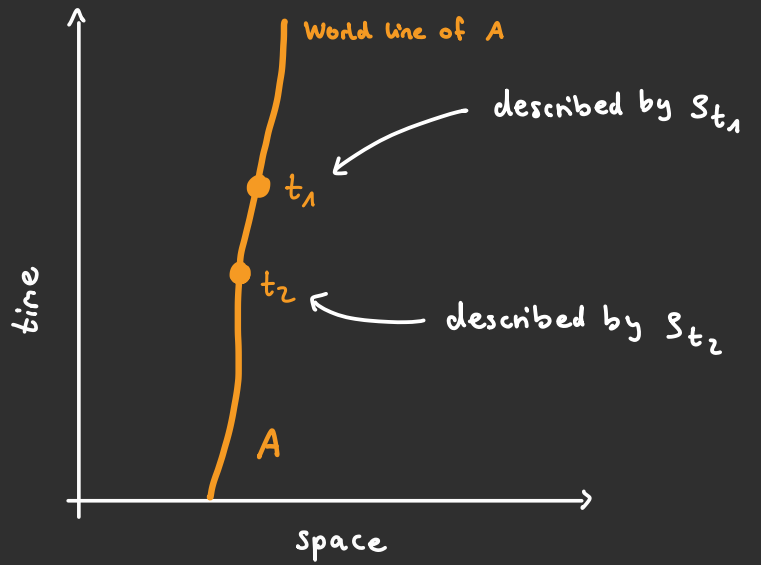
Classical: $P_{RE} = P_U \times P_E$

↑ uniform distribution

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

↑ The joint state does not exist!

General correlations ?



Can we describe correlations between A at time t_1 and t_2?

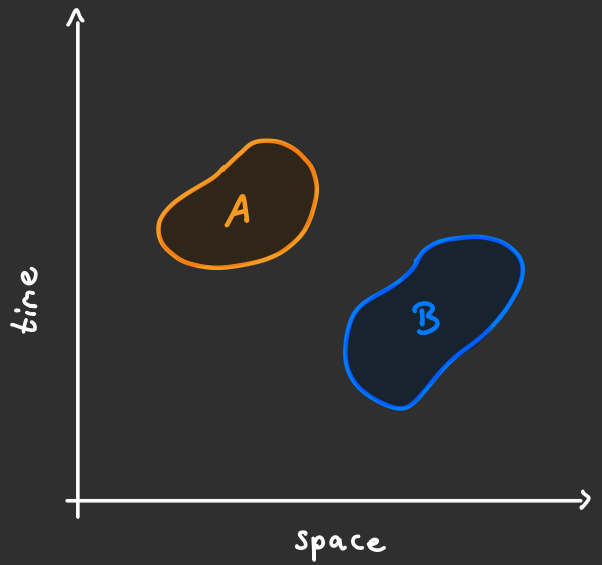
Issue: The joint state $\varrho_{t_1 t_2}$ does not exist!

Approaches for temporal correlations:

- Pseudo density matrices
- quantum combs
- ...

What about general spacetime regions?

What about more general correlations ?



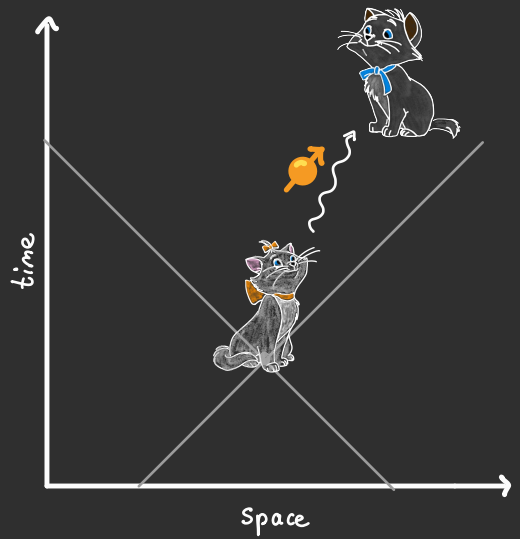
We would like to write, e.g.

$$\rho_{AB} = \rho_A \otimes \rho_B$$

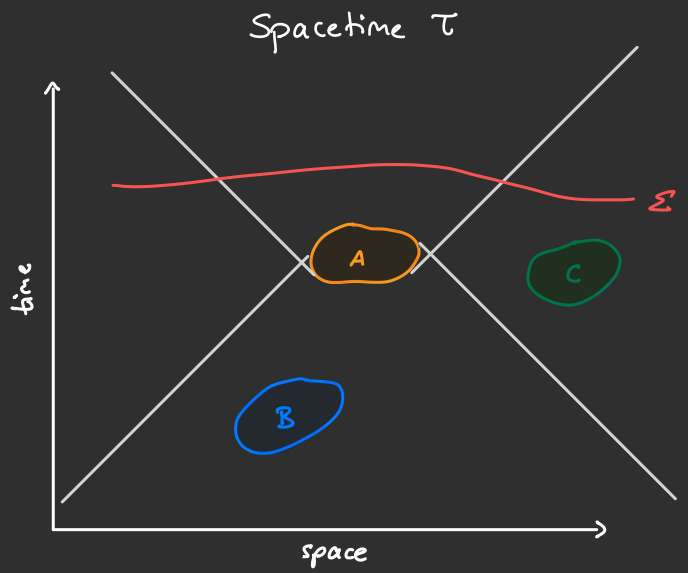
but these states do not necessarily exist

A panoramic model of quantum information in spacetime

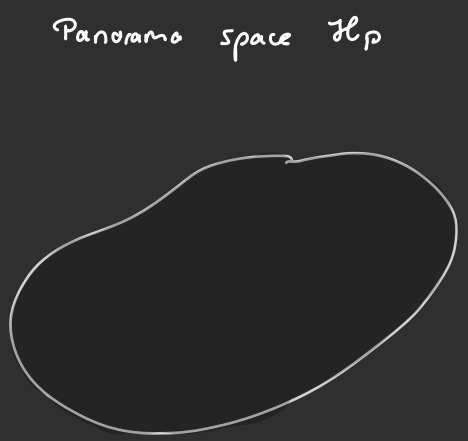
joint work with Renato Renner (in preparation)



The framework: General idea



Indicates which regions / objects we are interested in

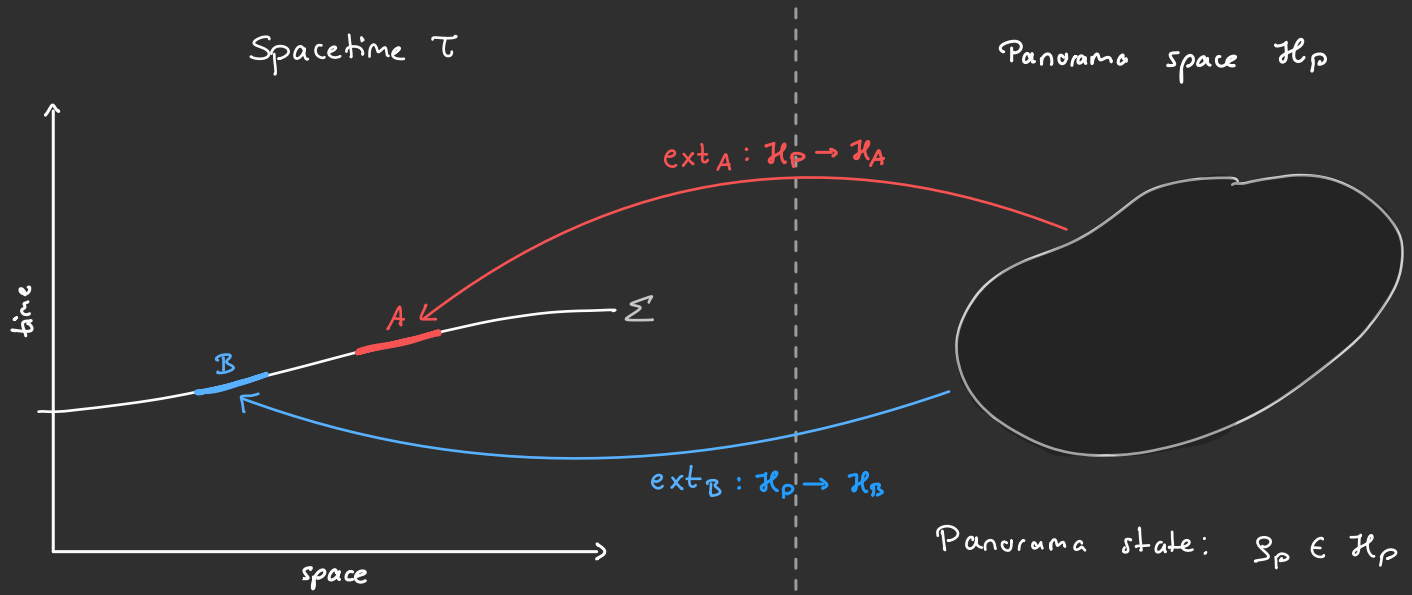


Panorama state: $\mathcal{S}_P \in \mathcal{H}_P$

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

The framework: General idea

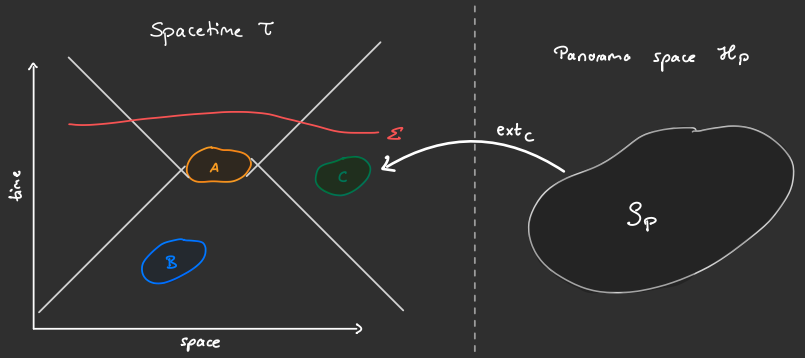
Most important part: Connection between the two spaces via "extraction maps"



$\rho_A = ext_A(\rho_P)$

$\rho_B = ext_B(\rho_P)$

The framework: General idea



World model:

$$\mathbb{W} = \{\tau,\ \mathcal{H}_P,\ \mathcal{S}_P,\ \{ext_D\}_{D\in\Delta}\}$$

- τ – spacetime: partially ordered set
- $\mathcal{H}_P$ – panorama space: Hilbert space that captures all possible states of the world
- $\mathcal{S}_P \in \mathcal{H}_P$ – panorama state: captures our knowledge about all systems in spacetime
- $\{ext_D\}_{D\in\Delta}$ – extraction maps: connect spacetime regions with abstract knowledge
  Δ: "admissible regions" = spacetime regions that admit a quantum state description

= Basic information about the situation we want to describe

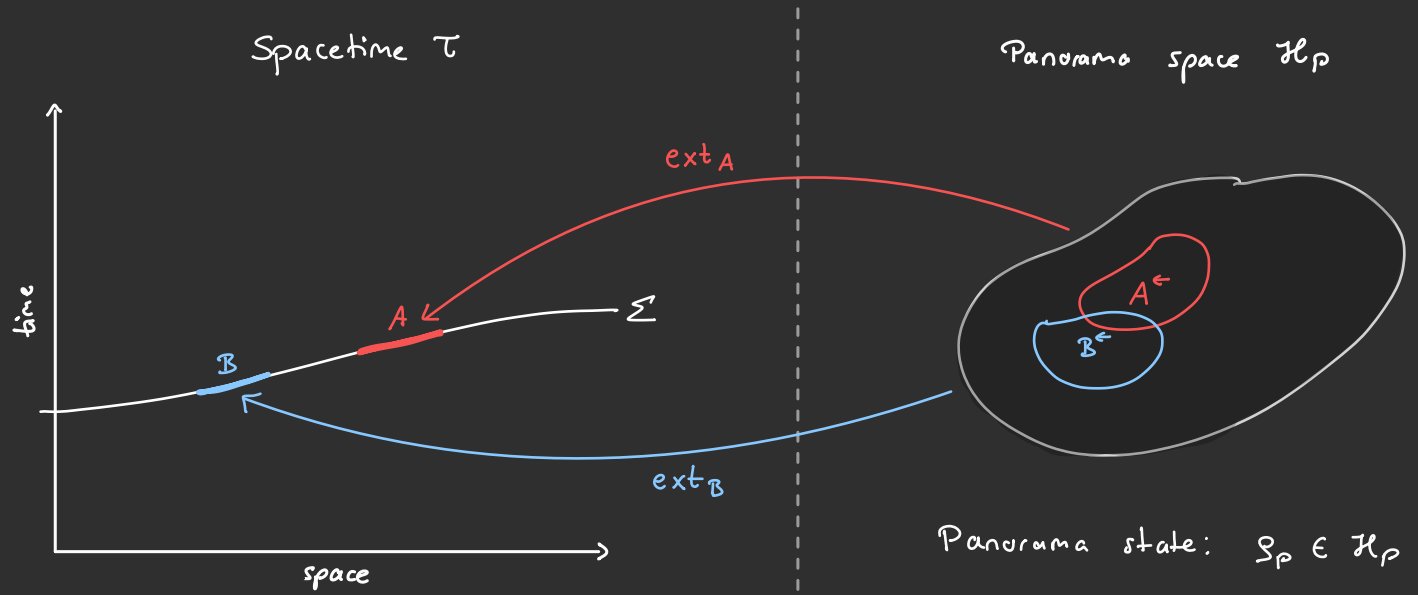
Some consistency conditions have to be fulfilled, for example:

If $B \subseteq A$, then there exists a CPTP map $\mathcal{M}_{A\to B}$ such that

$$ext_B = \mathcal{M}_{A\to B} \circ ext_A$$

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!

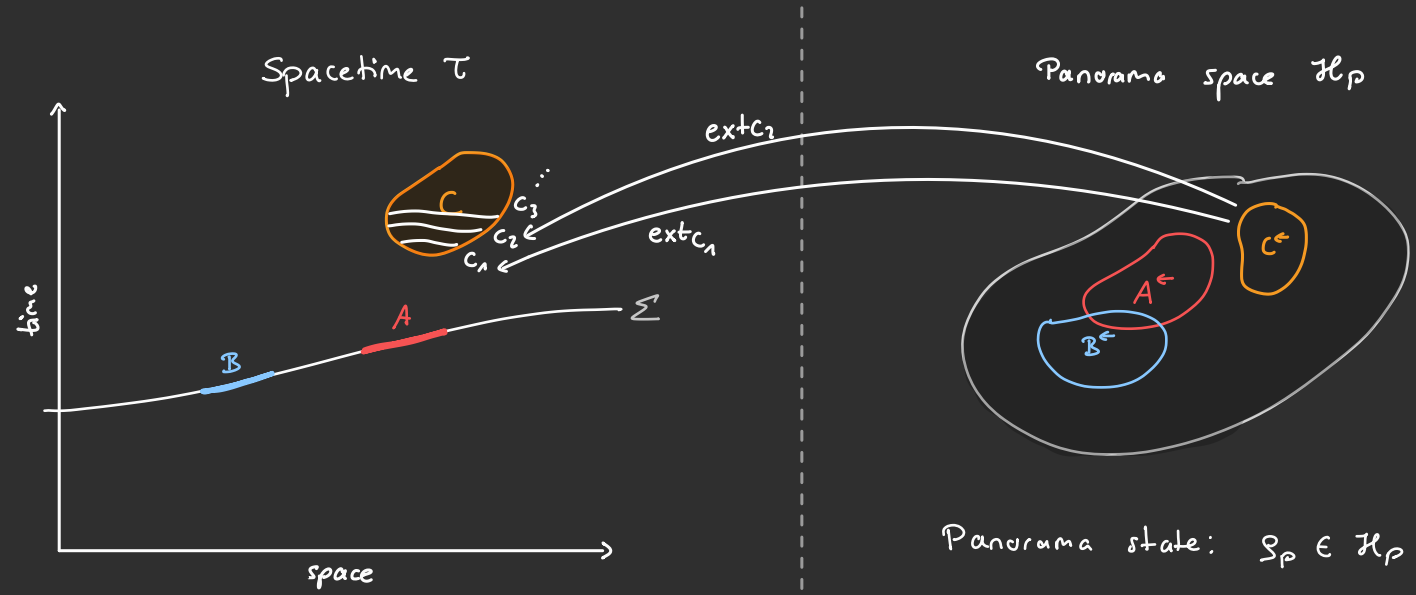
Definition: Representation

$A^\blacktriangleleft$ 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

But what about general spacetime regions?



Definition: Representation

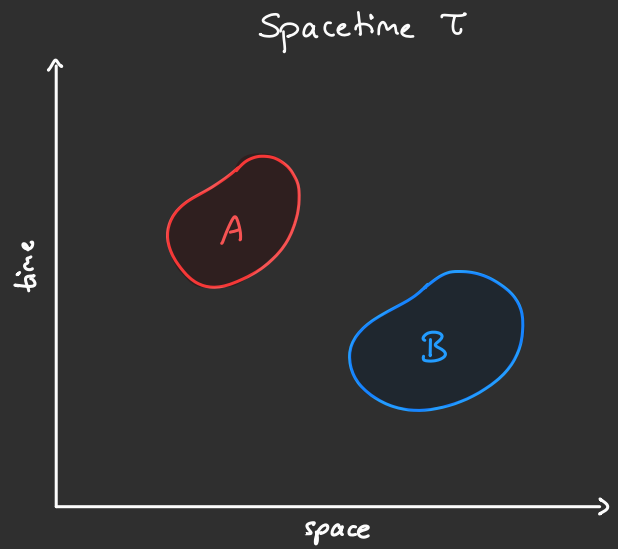
$C^{\blacktriangleleft}$ is a representation of C if ext_{c_i} is independent of $(C^{\blacktriangleleft})^c$ for all $c_i \in \Delta$ with $c_i \subseteq C$:

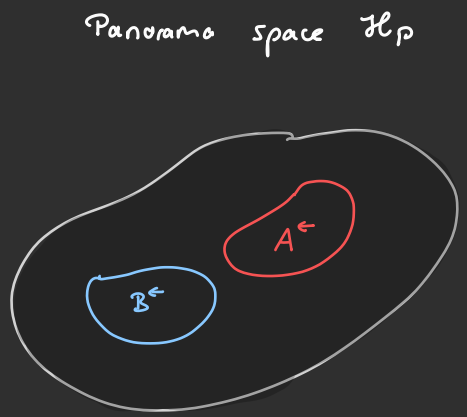
(Δ: admissible regions)

$$\text{ext}_{c_i} = \mathcal{M}_{C^{\blacktriangleleft} \to c_i} \circ \text{tr}_{(C^{\blacktriangleleft})^c}$$

Representations exist for <u>all</u> spacetime regions!

The framework: General idea



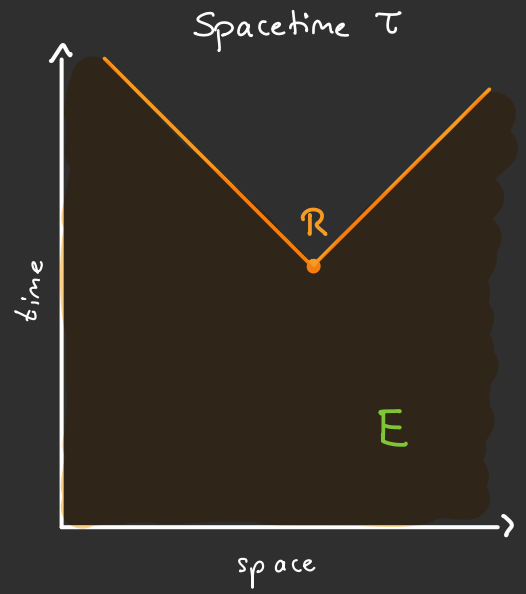


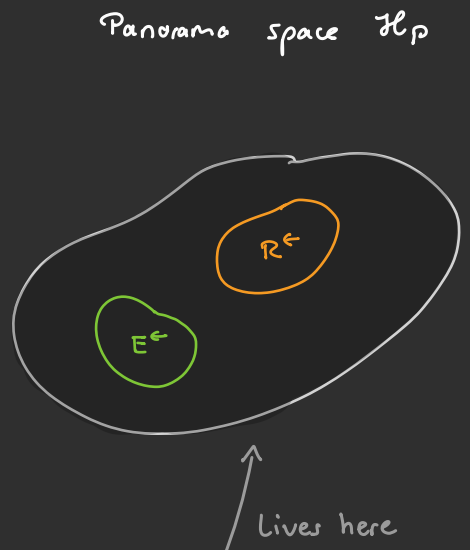
Why is this useful?

S_A, S_B, S_{AB} might all not exist – but $A^{\leftarrow}$ and $B^{\leftarrow}$ are subsystems of $\mathcal{H}_P$

$\Rightarrow$ $S_{A^{\leftarrow}B^{\leftarrow}}$ exists

Application: Randomness





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

$$\rho_{\mathcal{R}^{\in} E^{\in}} = \rho_{\mathcal{R}^{\in}} \otimes \rho_{E^{\in}}$$

and $\rho_{\mathcal{R}} = \pi_{\mathcal{R}}$ (maximally mixed).

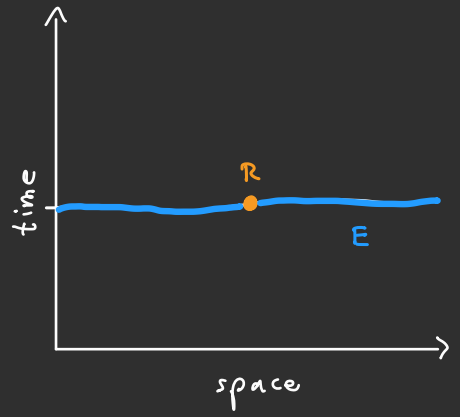
Application: Randomness

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

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

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

Sanity check: If ρ_{RE} exists, does it coincide with the current definition?



We can show:

If $R^{\leftarrow}$ and $E^{\leftarrow}$ are representations of R and E such that

$$\rho_{R^{\leftarrow}E^{\leftarrow}} = \rho_{R^{\leftarrow}} \otimes \rho_{E^{\leftarrow}},$$

then

$$\rho_{RE} = \mathrm{ext}_{RE}(\rho_{R^{\leftarrow}E^{\leftarrow}}) = \rho_R \otimes \rho_E.$$

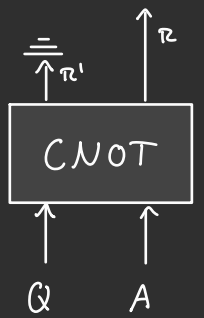
Application: Randomness

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

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

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

Important: There exists a protocol that can achieve this!



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

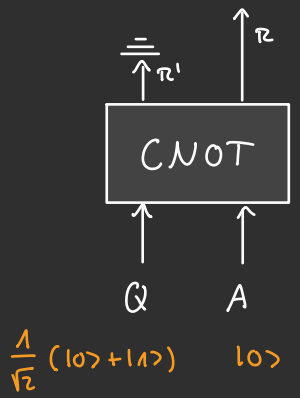
$$|\Psi\rangle_{R'R} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ $\quad$ $|0\rangle$

AND one can show $(*)$!

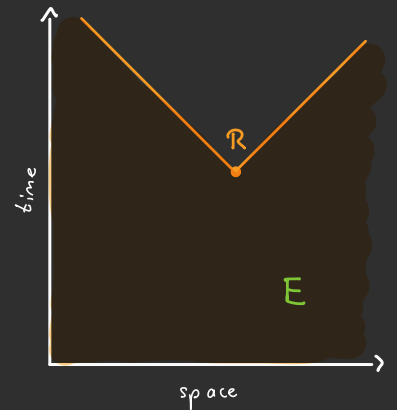
(I will spare you the proof)

Randomness : Lessons learned



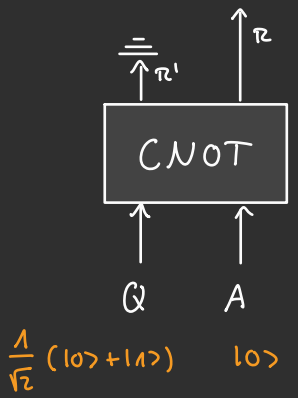
$$\rho_R = tr_{R'}\left(|\Psi\rangle\langle\Psi|_{RR'}\right) = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) = \pi_R$$

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



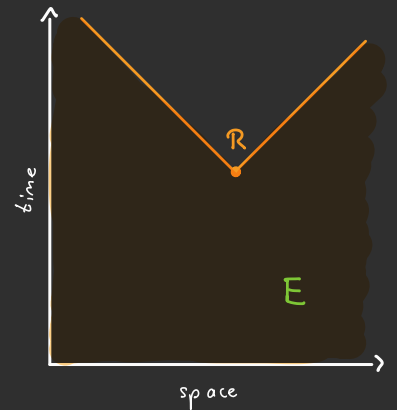
What does E contain?

Randomness : Lessons learned



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

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



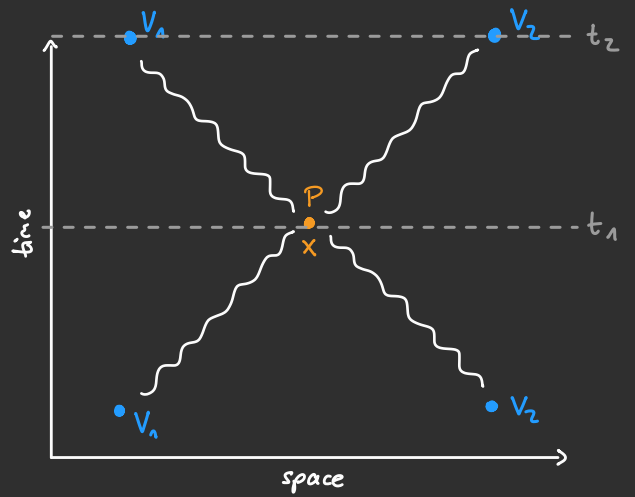
What does E <u>not</u> contain?

- We assume that we can prepare a system in a <u>pure state</u>
- E does <u>not</u> have access to the traced out system R'

More applications

Example: Quantum position verification (QPV)

Position of the party is a cryptographic credential



P – Prover: Has to prove that he is at position X

V_1, V_2 – Verifiers: Check that P is actually at position X

Missing: A composable security proof

Challenges: Events happen at different times

Points in spacetime are a cryptographic credential

Security statement: If the check at spacetime points (V_1, t_2) and (V_2, t_2) was successful, then the prover P was at position (X, t_1)

→ Needs a framework that takes into account spacetime


Questions ?