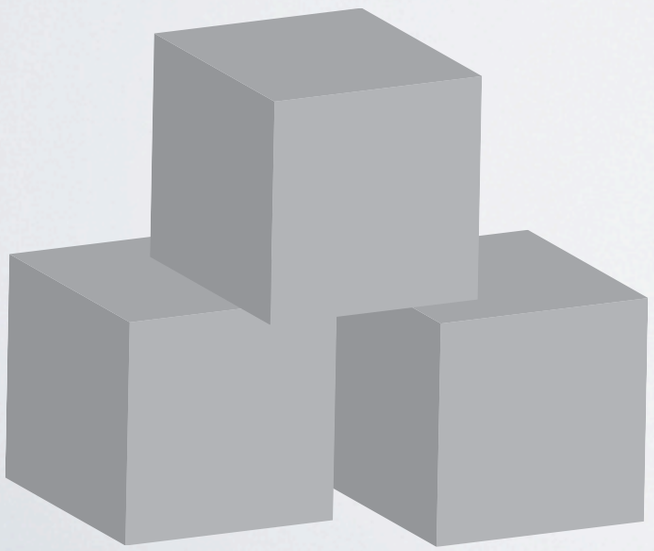
Limits of

Privacy Amplification *Against* Non-Signaling Memory Attacks

Rotem Arnon-Friedman & Amnon Ta-Shma

ETH Zurich Tel-Aviv University



QCrypt 2013

Outline

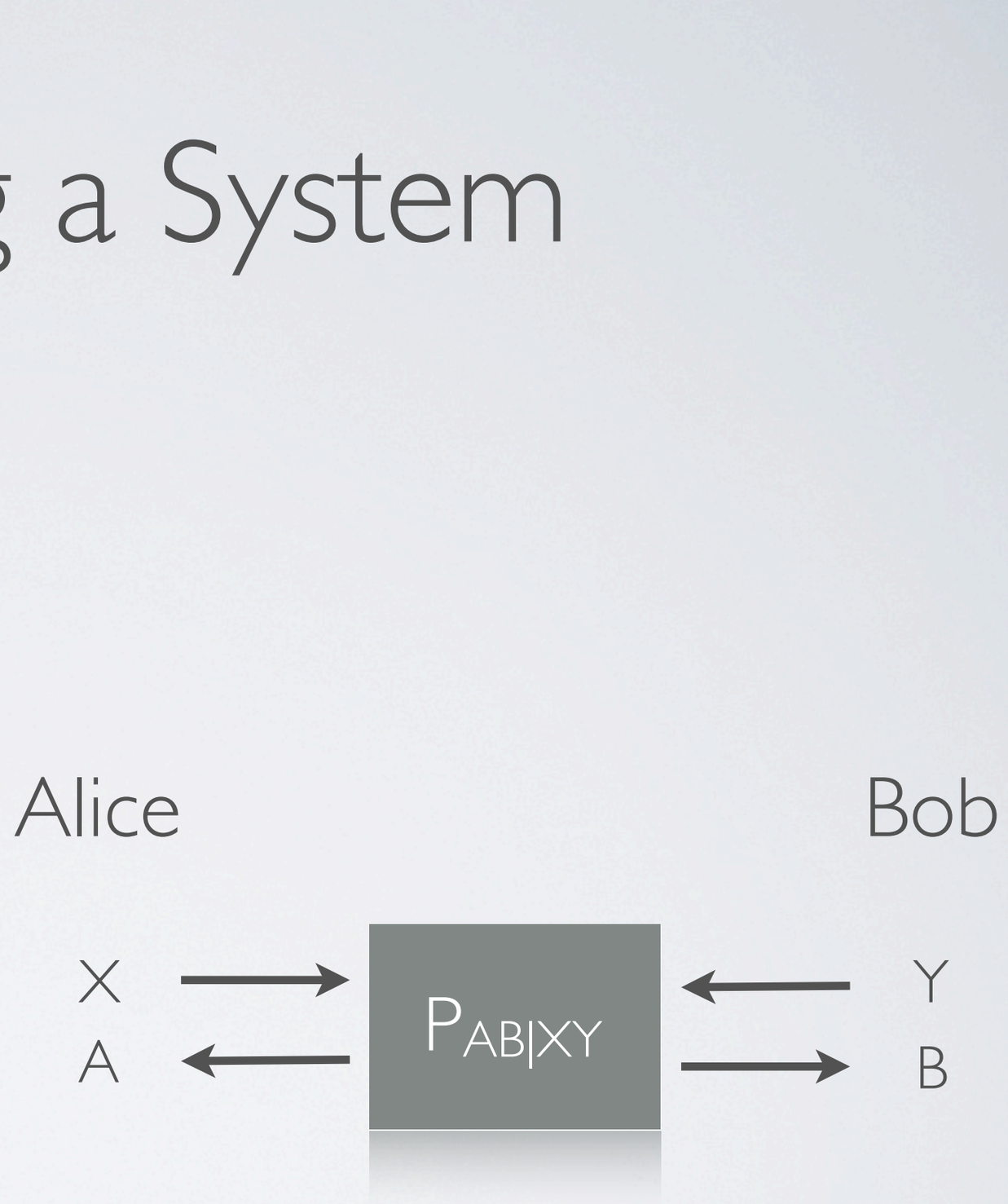
- Motivation
    - Device independent cryptography
    - Privacy Amplification
- Different non-signaling conditions
- Result
- Summary

Device Independent Cryptography

- Bridge the gap between theory and experiment { Noise, Imperfections
- Assume **less** about the physical systems and measurements
- Extreme case - use only the observed statistics
- Chained Bell inequalities [Braunstein et al., 1990]

Modeling a System

- System $P_{AB|XY}$
- X,Y - measurements
- A,B - outcomes
- $P_{AB|XY}(ab|xy)$



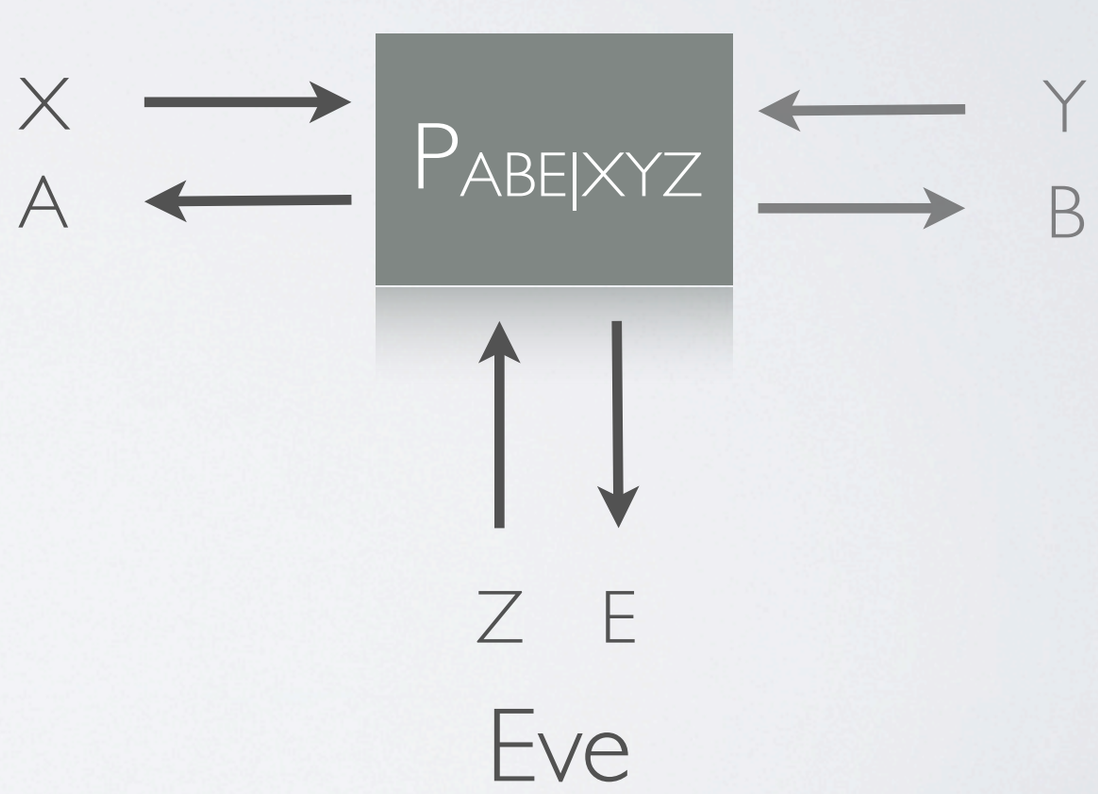
Privacy Amplification

- Alice's goal: secrecy with respect to Eve
- Secrecy measure - distance from uniform

$$d\left(A|E(Z),X\right) \leq \varepsilon$$

operational meaning - distinguishing advantage

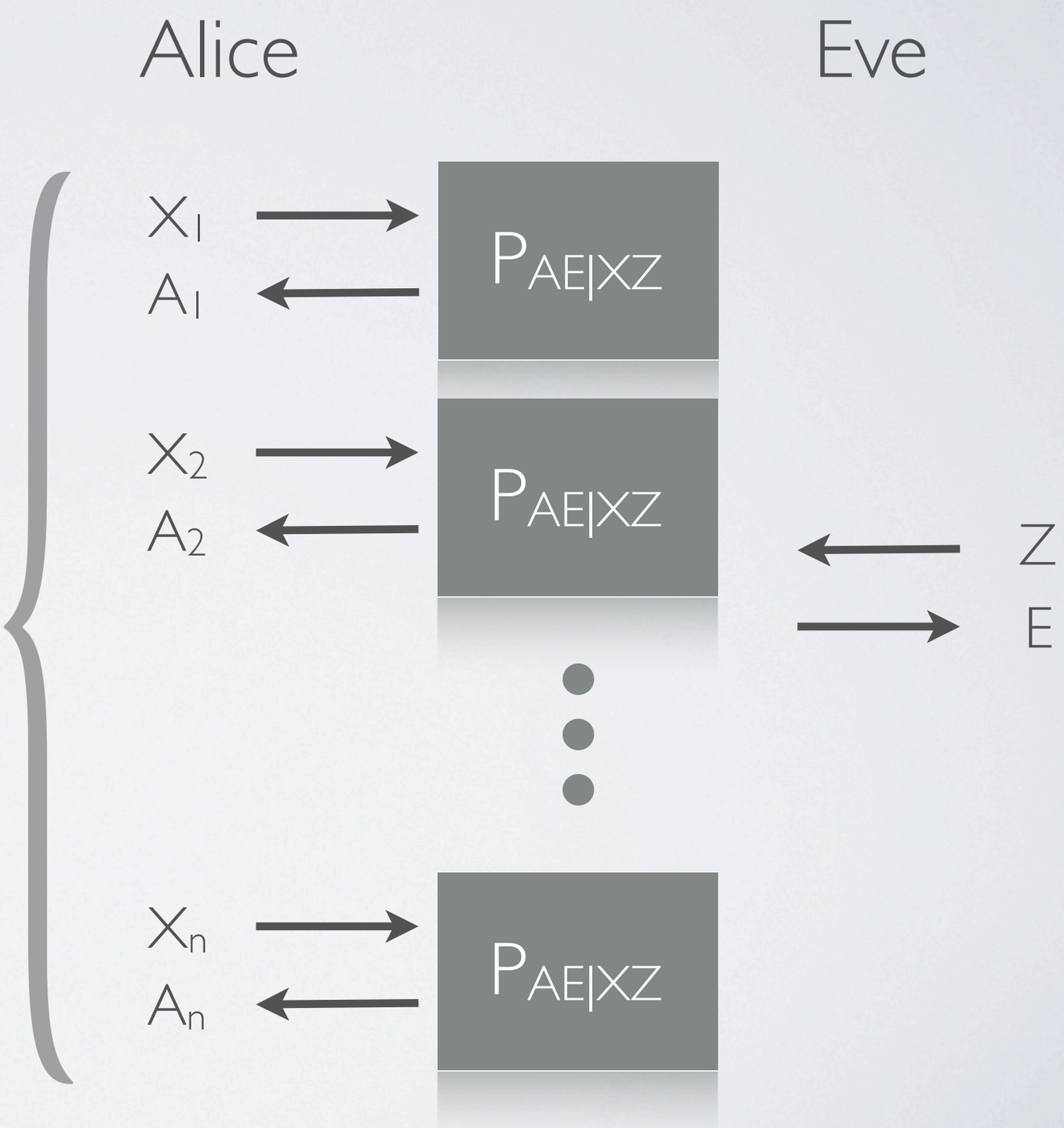
- Bob is there just for non-locality



Privacy Amplification

$$f(A) = K$$

$$d\left(K|E(Z), X, f\right) \leq \varepsilon^n$$



Possible / Impossible

- PA is said to be **possible**:

$$\exists f \quad d\left(K|E(Z), X, f\right) \leq \varepsilon^n$$

- **Exponential** PA is said to be **impossible**:

$$\forall f \quad d\left(K|E(Z), X, f\right) \geq \frac{\varepsilon}{n}$$

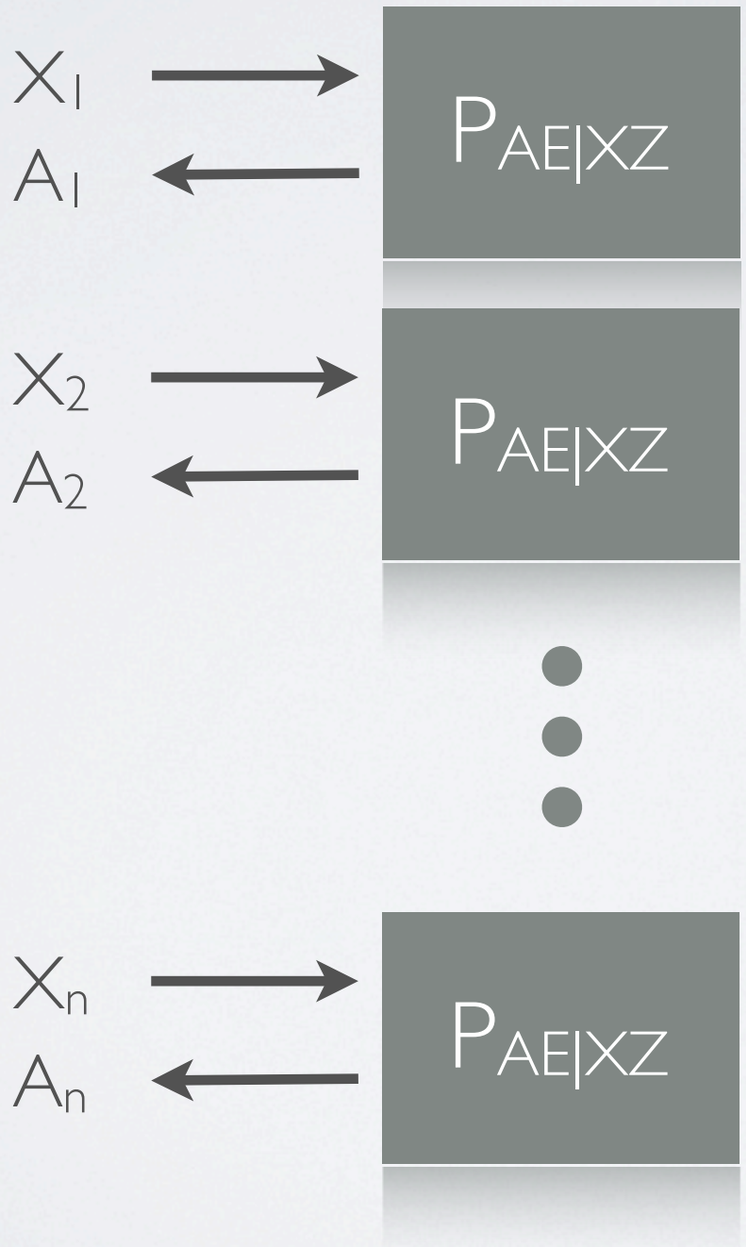
- PA is said to be **impossible**:

$$\forall f \quad d\left(K|E(Z), X, f\right) \geq \varepsilon$$

Under Which Assumptions?

Alice

Eve



assumptions regarding the **system**

non-signaling conditions?

assumptions regarding the power of the **adversary**

classical?

quantum?

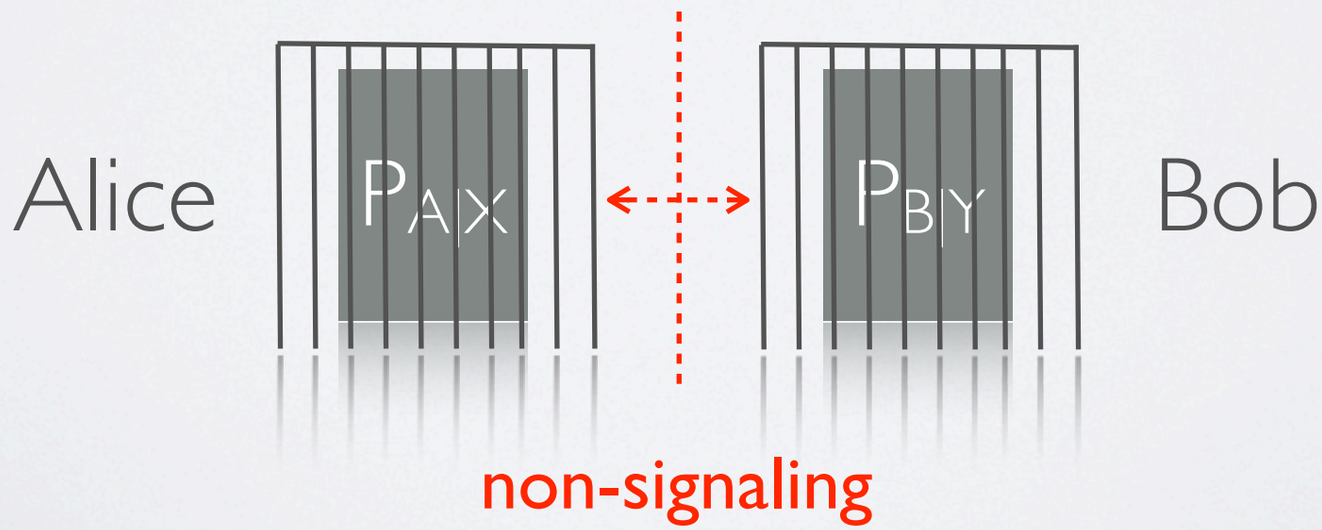
super-quantum

Different Non-Signaling Conditions

- Alice and Bob can enforce local non-signaling conditions between the subsystems

- Shielding the systems / placing them far away

- The non-signaling conditions restrict the adversary



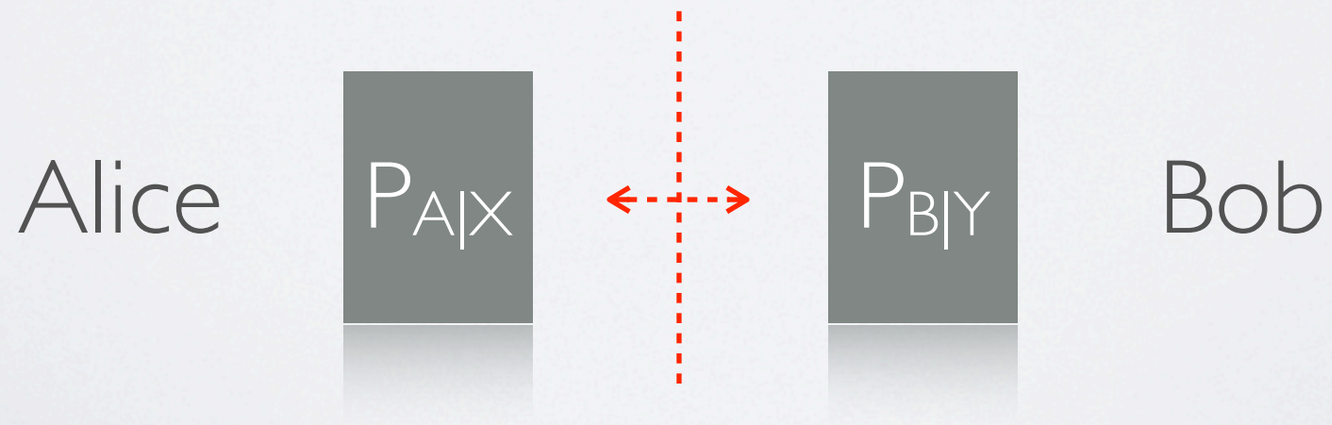
Alice-Bob Non-Signaling Cond.

- Alice and Bob cannot signal each other using the system
- Mathematically:

$$\forall x, x', y, b \quad \sum_a \mathrm{P}_{AB|XY}(a, b, x, y) = \sum_a \mathrm{P}_{AB|XY}(a, b, x', y)$$

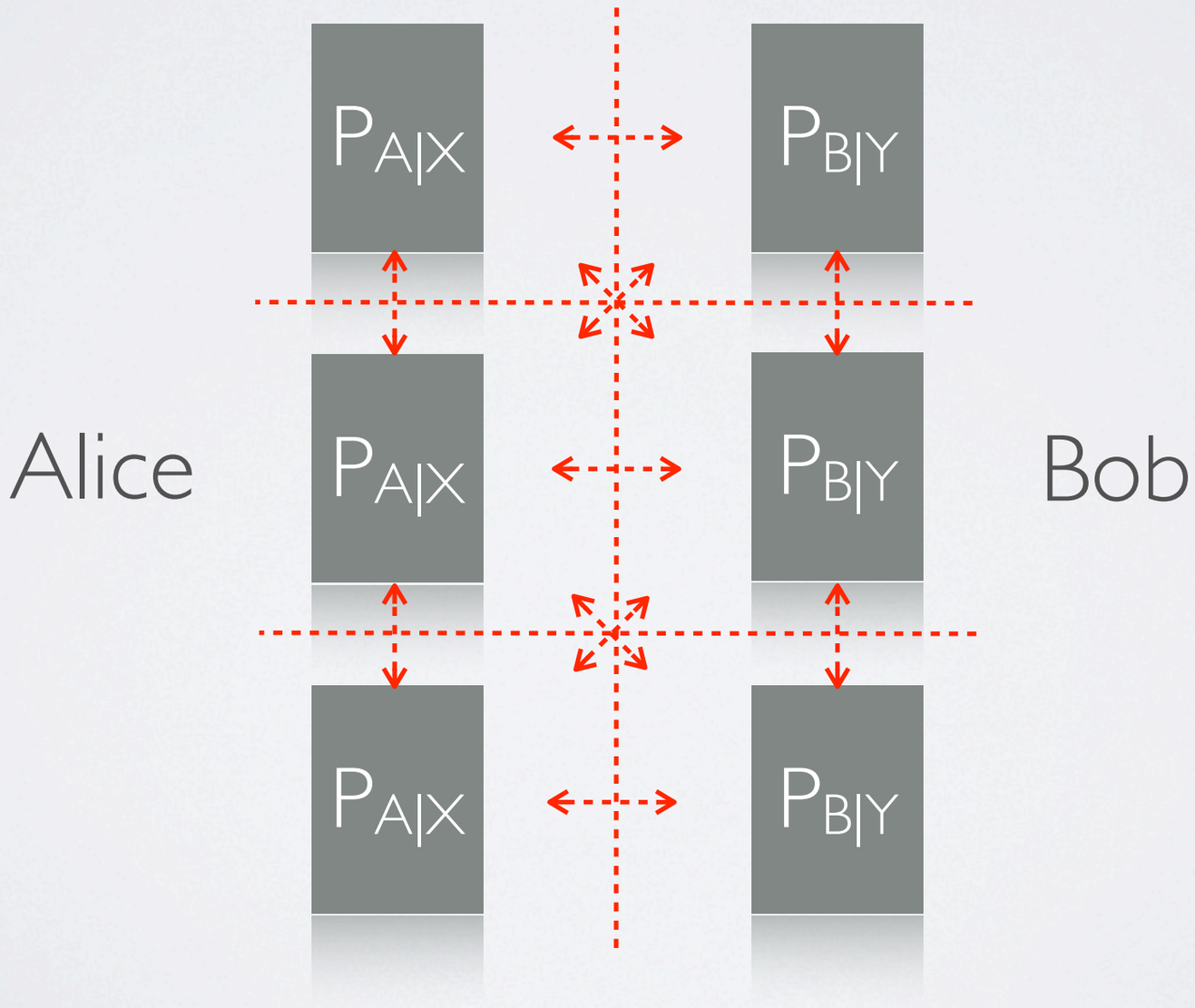
$$\forall y, y', x, a \quad \sum_b \mathrm{P}_{AB|XY}(a, b, x, y) = \sum_b \mathrm{P}_{AB|XY}(a, b, x, y')$$

- PA against non-signaling adv. is **impossible** [Hänggi et al., 2010]



Full Non-Signaling Cond.

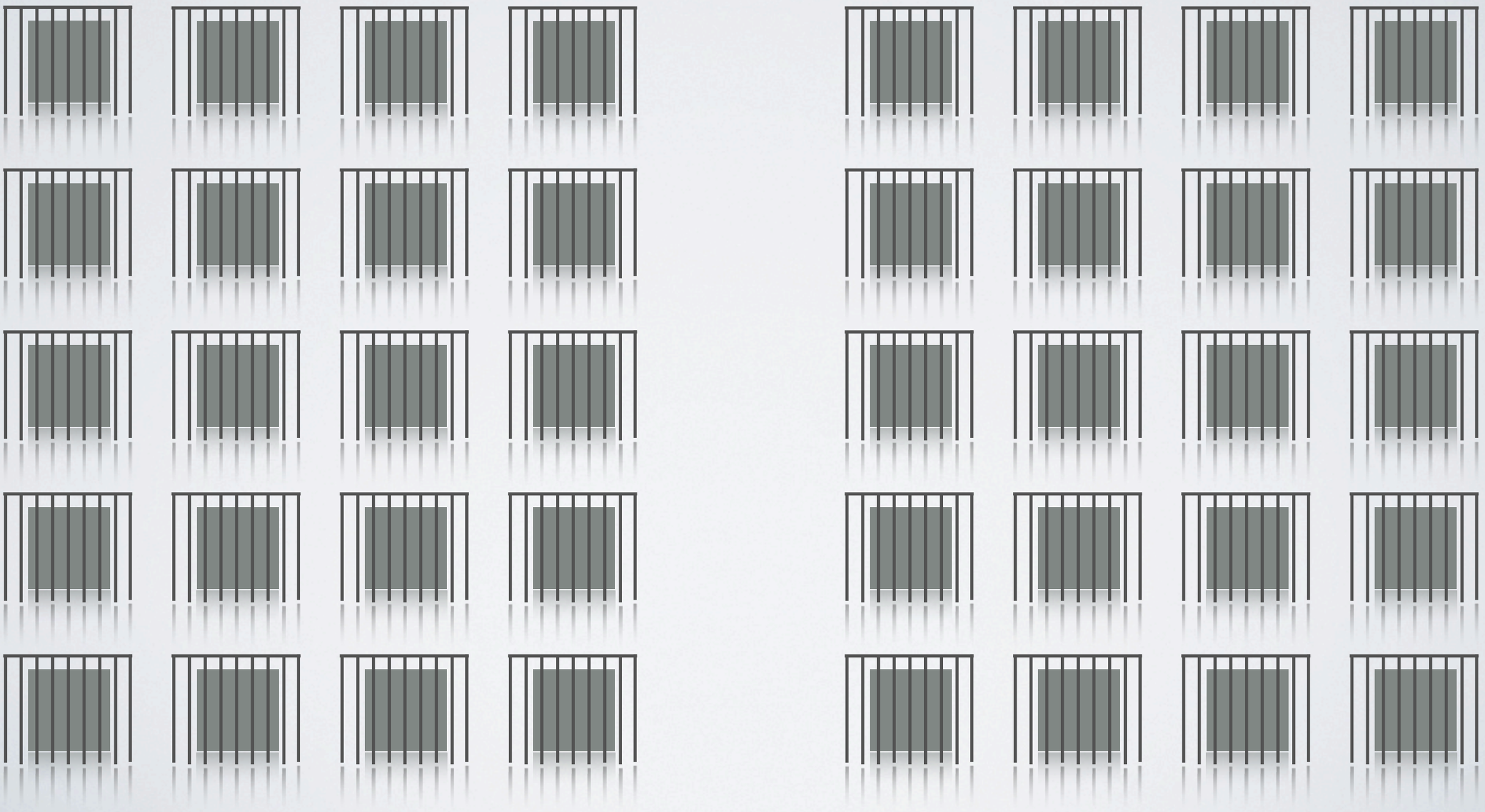
- Non-signaling between all the subsystems



Full Non-Signaling Cond.

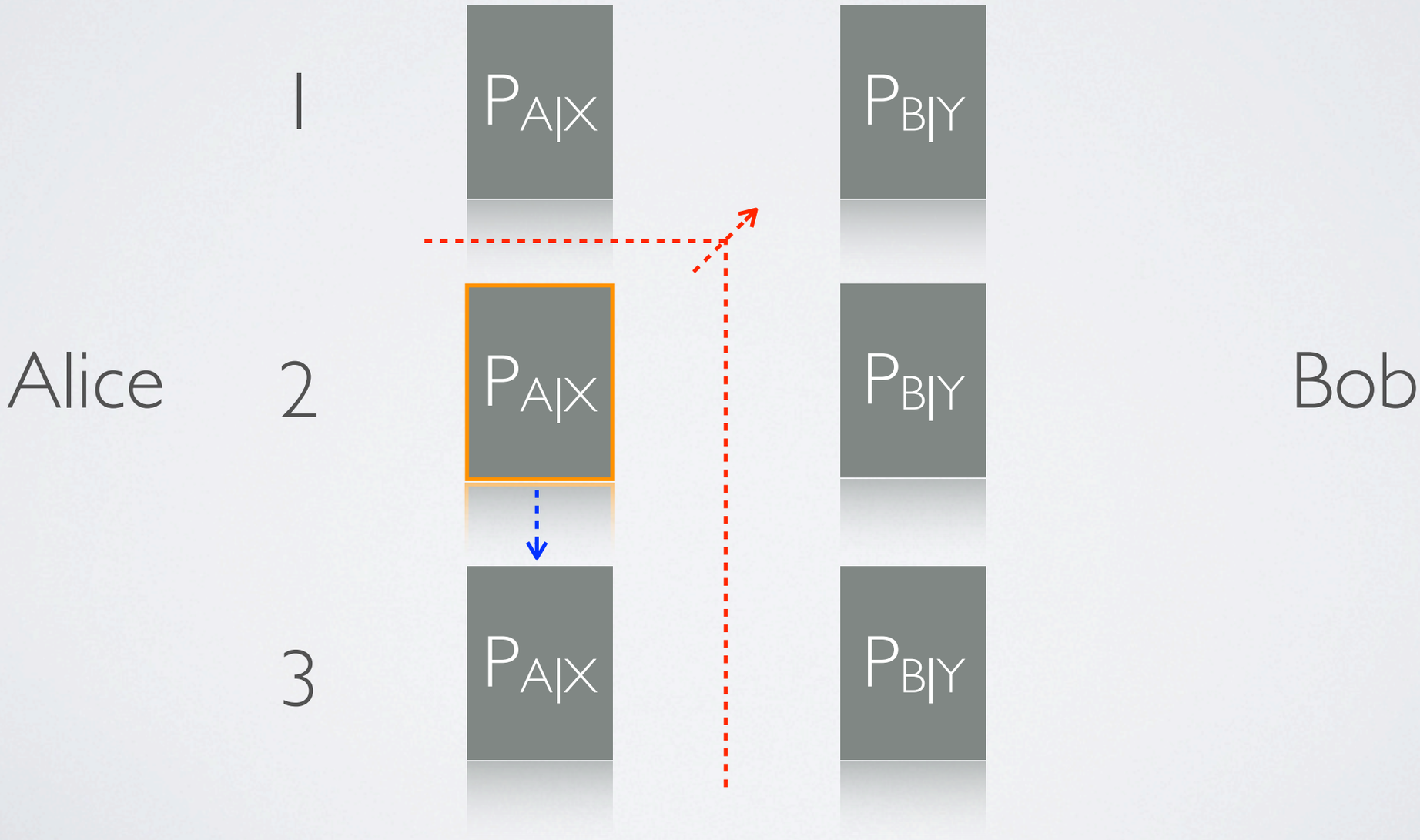
Alice

Bob



Time-Ordered N.S. Cond.

- The "future" cannot signal the "past"
- Models device with memory - relevant for implementations



Time-Ordered N.S. Cond.

- These are the non-signaling conditions we get "for free"
- Allow for memory in the devices
- Easy to implement
- **Is PA possible under these conditions?**

Result

- Non-signaling adversary
- **Exponential** PA is **impossible**: $\forall f \quad d(K|E(Z), X, f) \geq \frac{\varepsilon}{n}$
- No-go theorem
- Is linear PA possible?

open question

Proof Idea

- Alice and Bob share systems which violate the chained Bell inequality

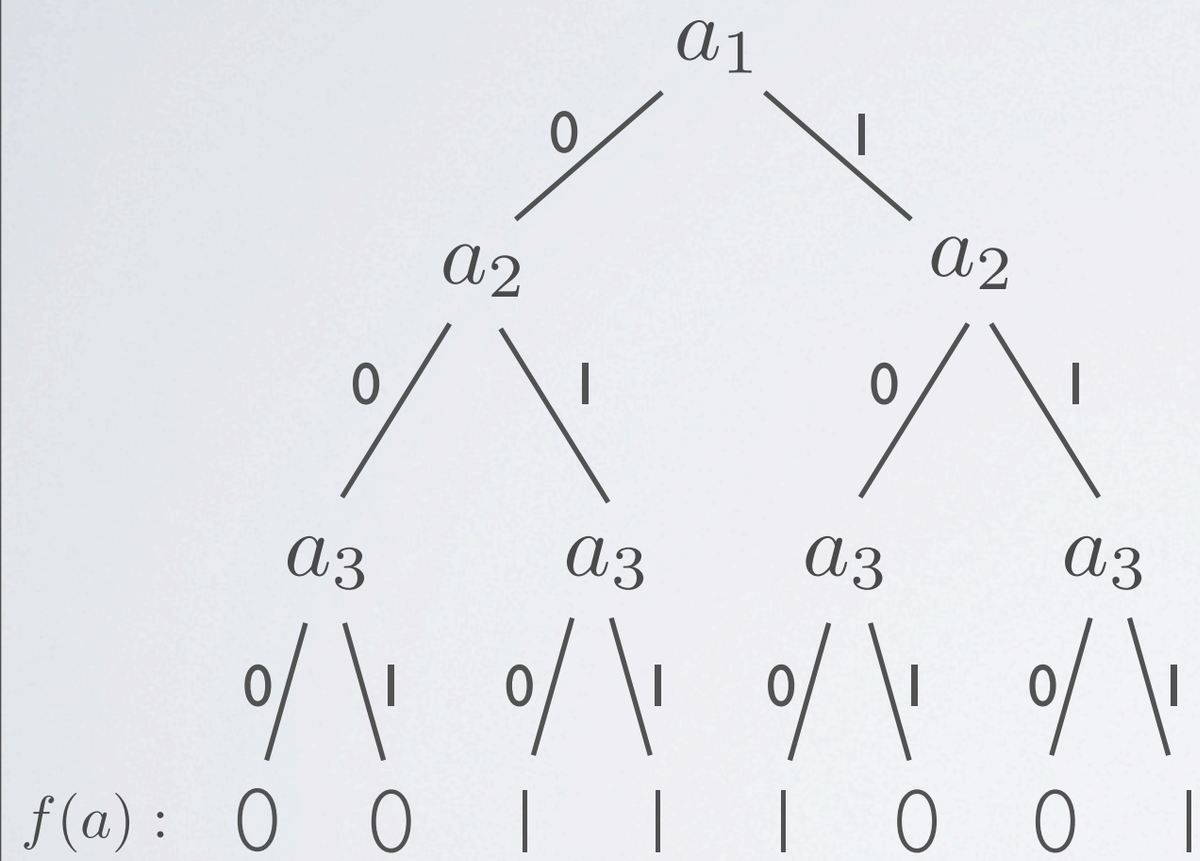
- For any hash function - adversarial strategy

- Eve gains at least a linear amount of information

$$\forall f \quad d\left(K|E(Z), X, f\right) \geq \frac{\varepsilon}{n}$$

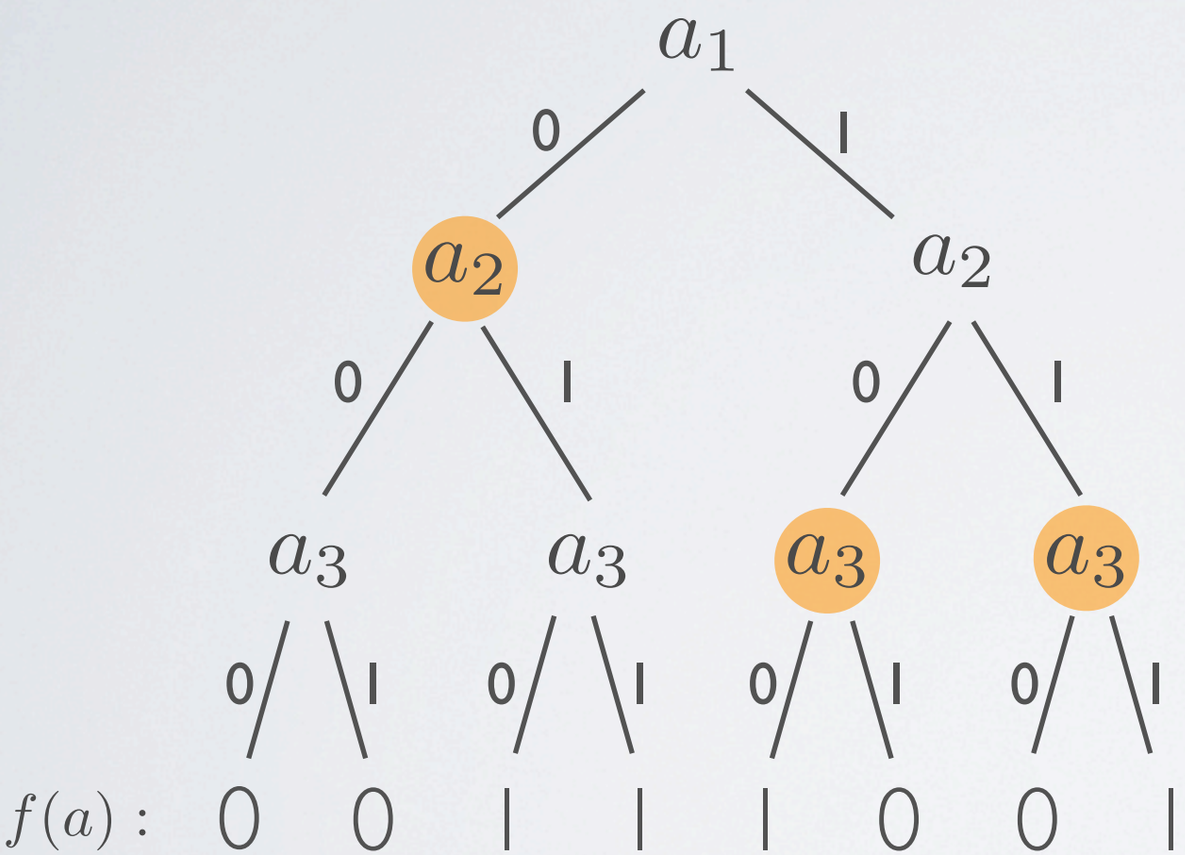
Proof Idea

Binary tree for $f : \{a_1, a_2, a_3\} \to \{0, 1\}$



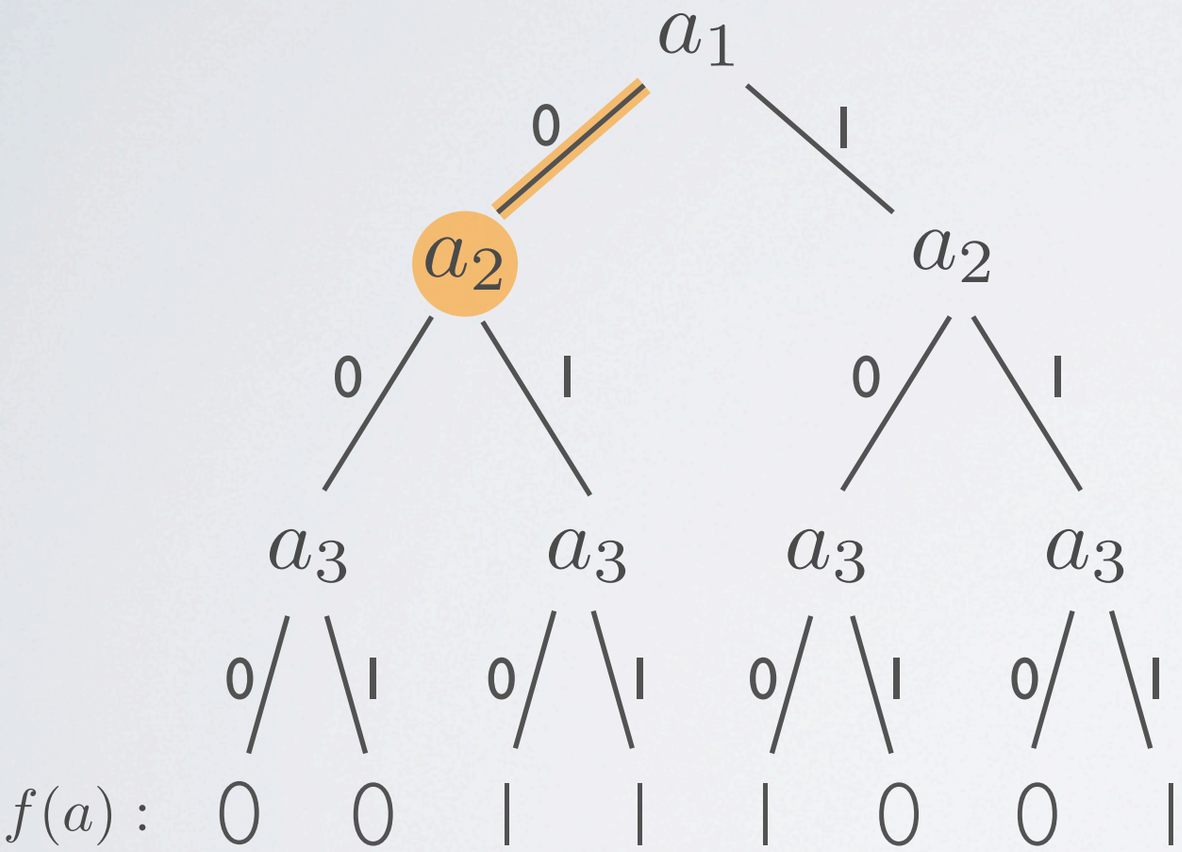
Proof Idea

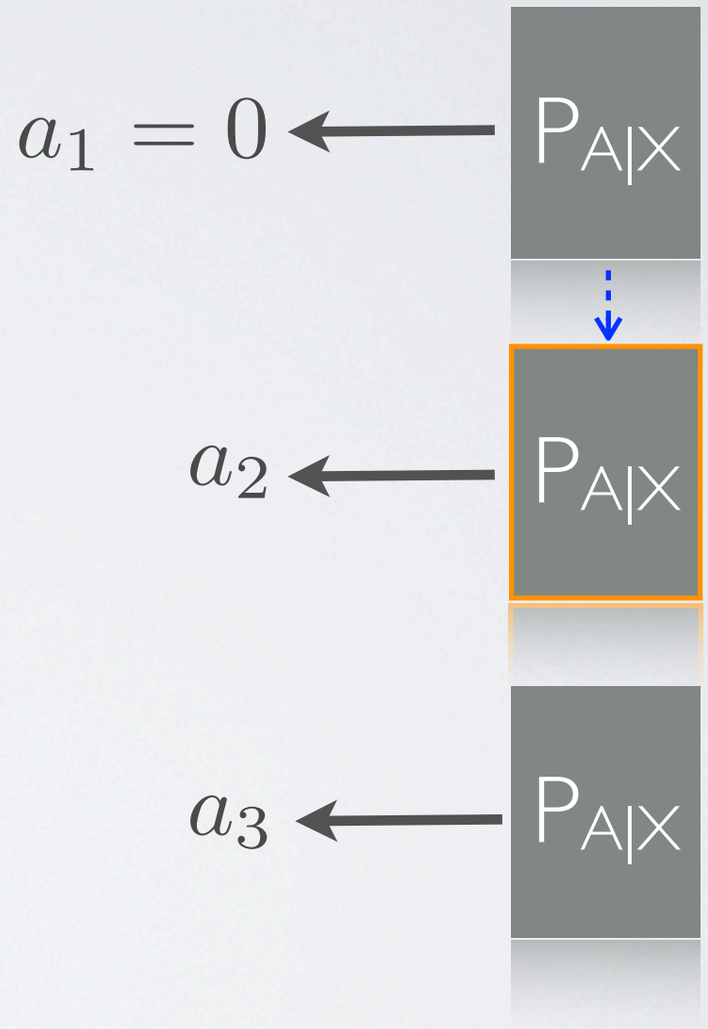
Binary tree for f



Proof Idea

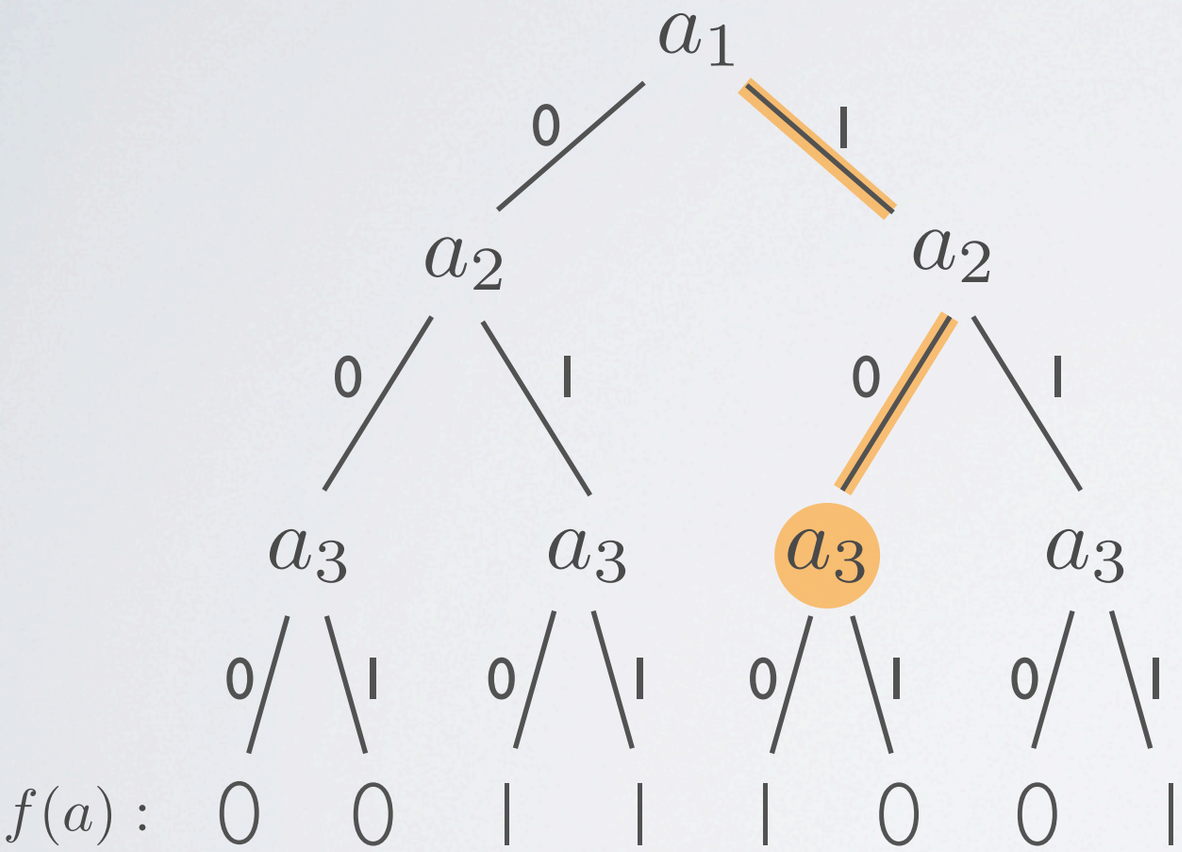
Binary tree for f

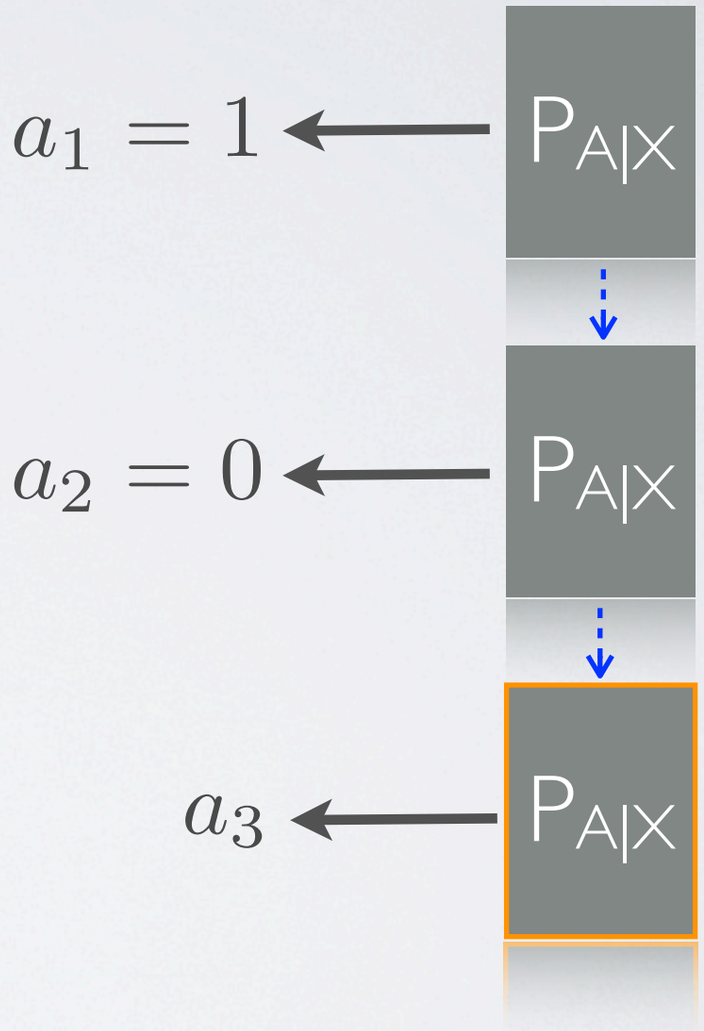




Proof Idea

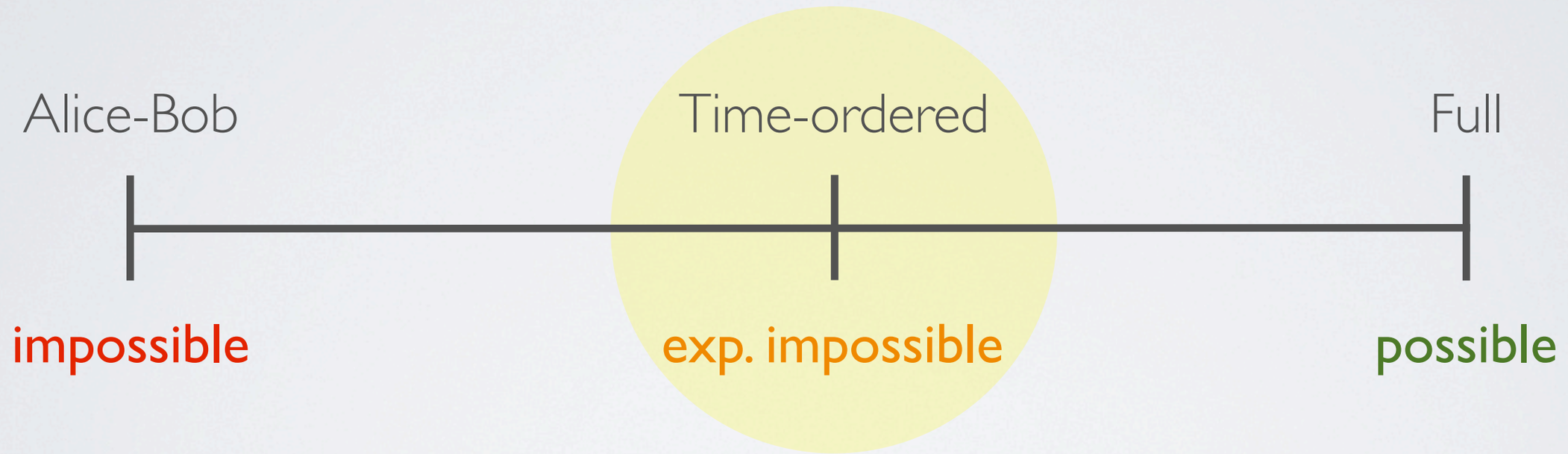
Binary tree for f





Summary

- Exponential PA is impossible when considering non-signaling adversaries and allowing memory



- In contrast to the quantum case - where PA is possible [Vazirani et al., 2012]

- Gap between quantum and super-quantum adversaries

Thank You!

arXiv: 1211.1125

Physical Review A, Vol. 86, No. 6, DOI:10.1103