Device-independent Quantum Cryptography

QSIT general meeting

Arosa | February 2, 2017

Rotem Arnon-Friedman (ETH)

QSIT Quantum Science and Technology
National Centre of Competence in Research

FNSNF
Swiss National Science Foundation

AIR FORCE OFFICE OF SCIENTIFIC RESEARCH
UNITED STATES AIR FORCE

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Outline

1. Cryptography
2. Quantum cryptography
3. Device-Independent quantum cryptography
4. A taste of our work

Cryptography:

(from Greek: **κρυπτός** kryptós, "hidden, secret"; and **γράφειν** graphein, "writing") is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

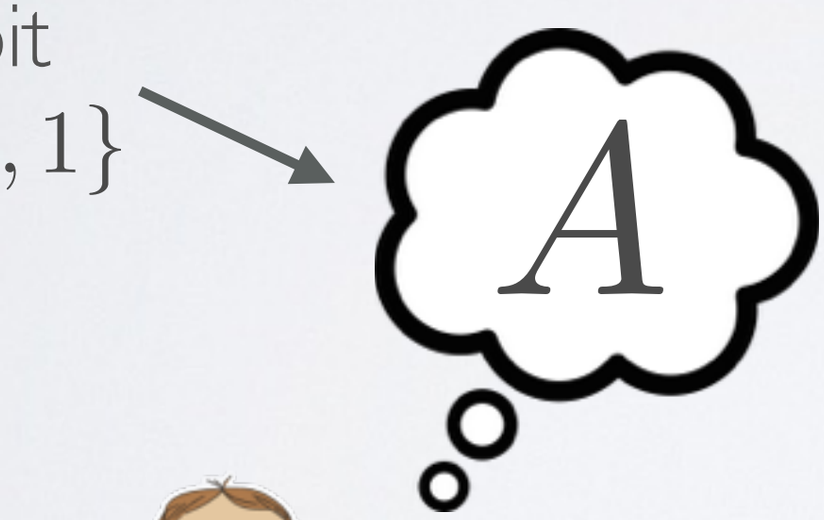
- Wikipedia

Baby example

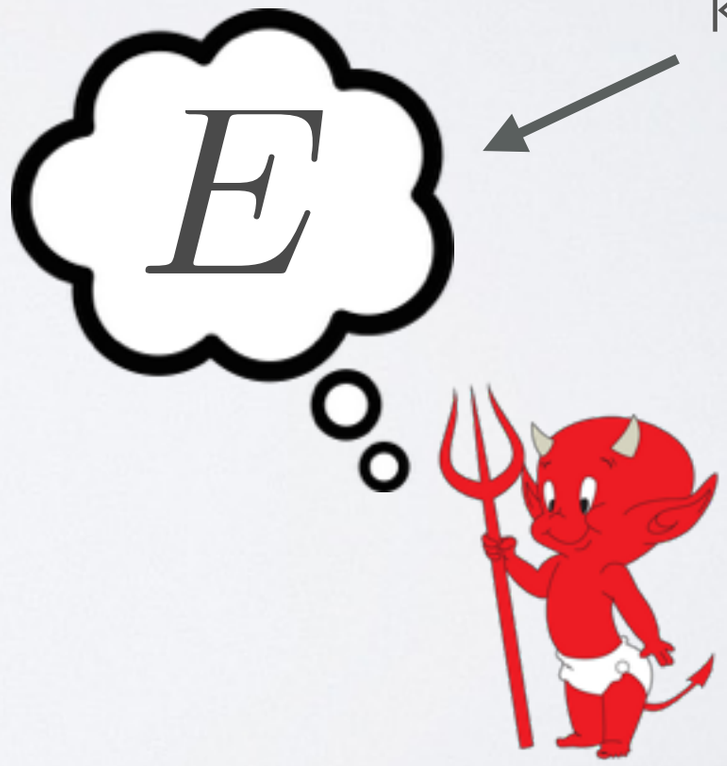
Cryptography:

(from Greek: **κρυπτός** kryptós, "hidden, secret"; and **γράφειν** graphein, "writing") is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

one bit
$A \in \{0,1\}$



knowledge about A



Baby example

- A should look **random** from **adversary's point of view**

Baby example: the **classical** way

Baby example: the **classical** way

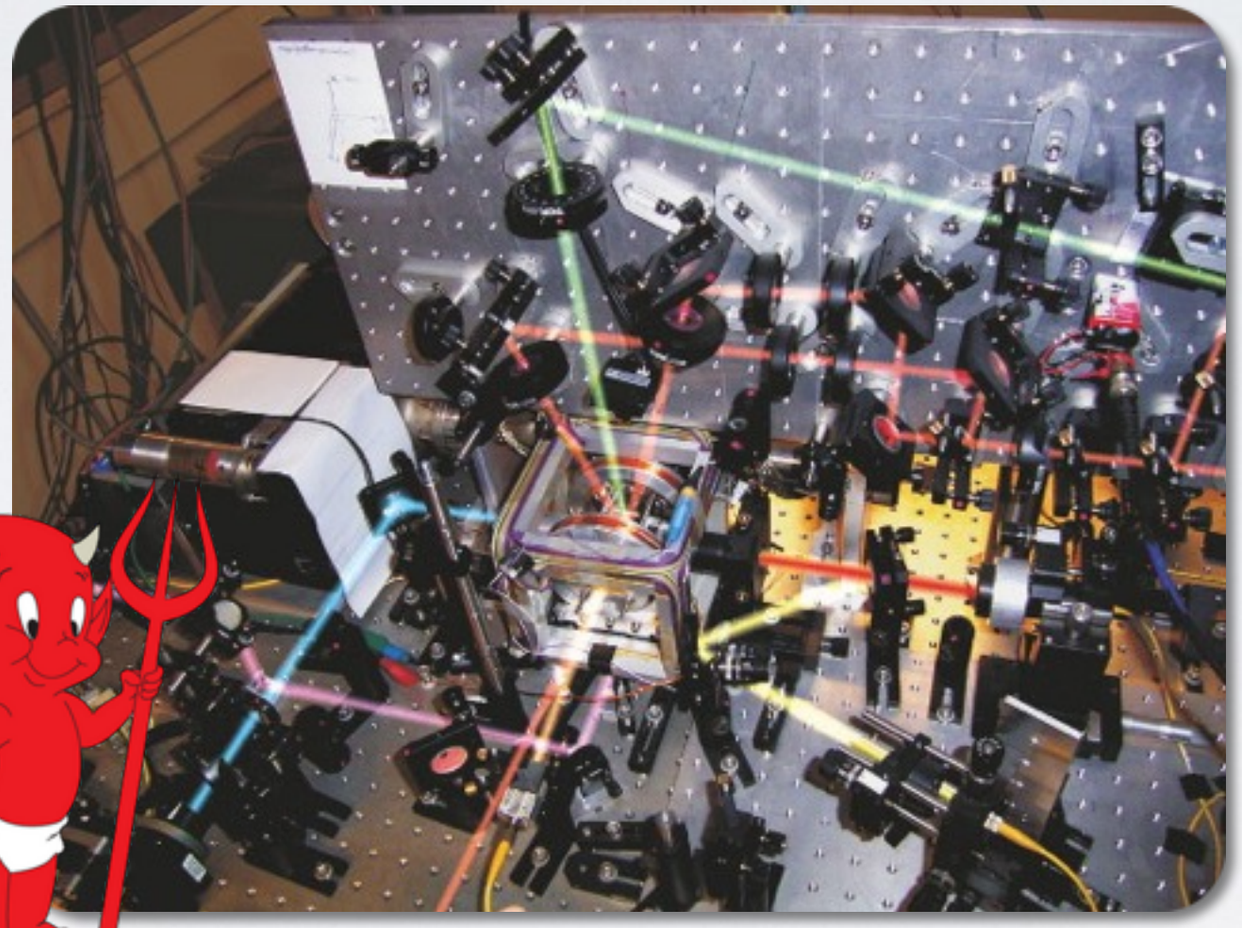
Baby example: the **quantum** way

- According to QM the result is unknown before the photon is emitted
- Problem arise due to imperfections in the experiment

Device-independent cryptography

- Hacking of QKD — due to imperfections in the implementation
- Bridge the gap between theory and experiment { Noise, Imperfections }
- Assume **less** about the physical systems and measurements

The black box approach

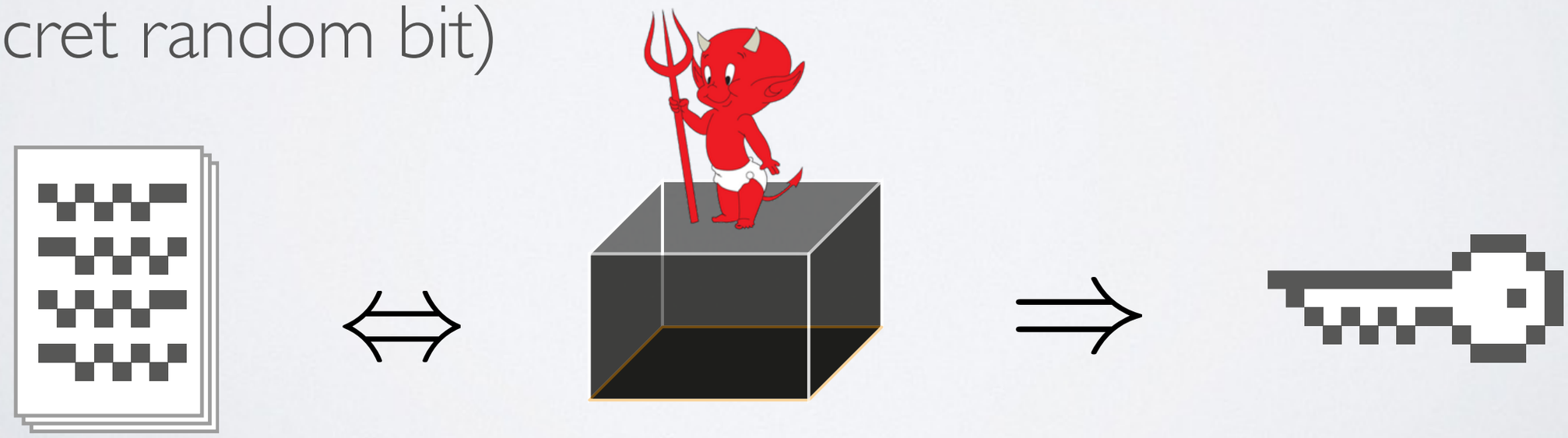


The black box approach

classical interaction

Device-independent cryptography

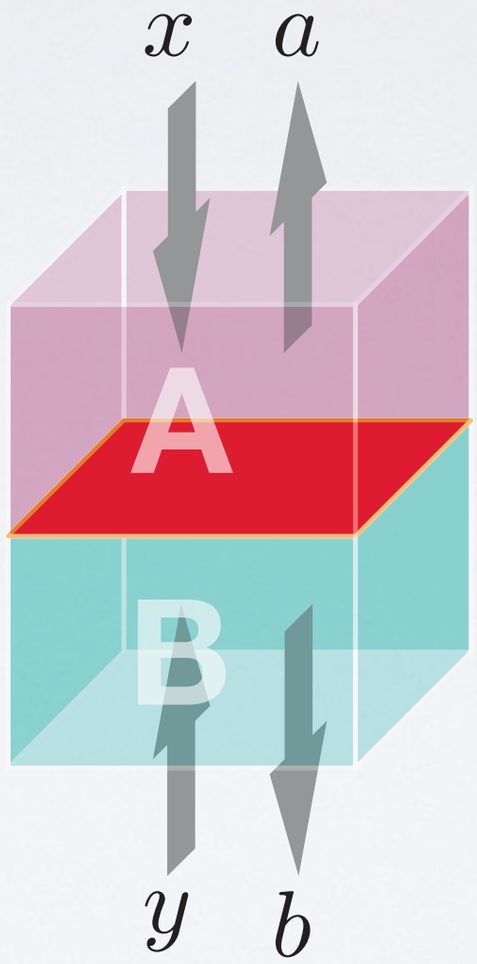
- Honest parties share an uncharacterised device
- They interact with it according to some known protocol (e.g., DI randomness generation protocol)
- They either abort or accomplish their task (e.g., output a secret random bit)



Bell inequality / game

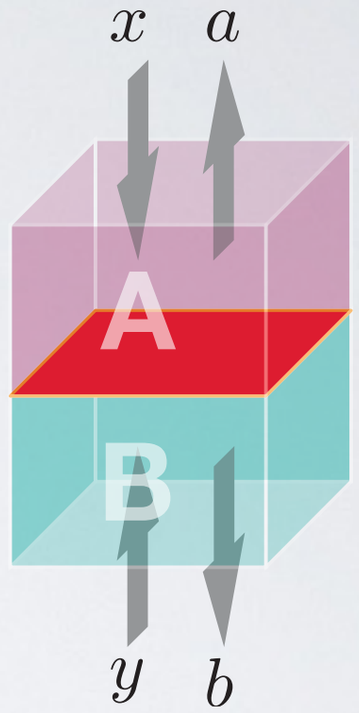
Alice

Bob



Example: the CHSH game

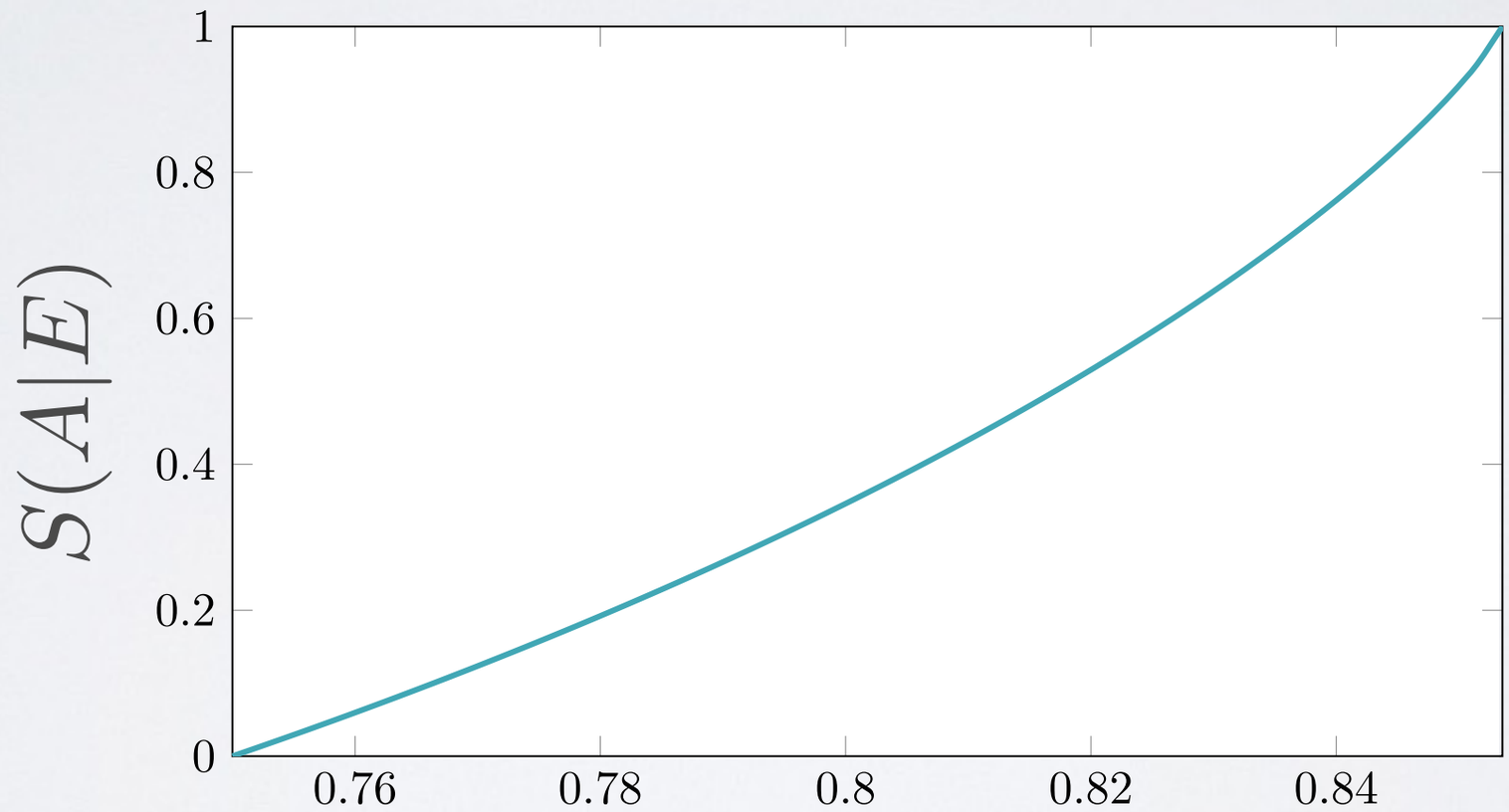
Alice:	Input	$x \in \{0, 1\}$
	Output	$a \in \{0, 1\}$
Bob:	Input	$y \in \{0, 1\}$
	Output	$b \in \{0, 1\}$
Win:		$a \oplus b = x \cdot y$



- Best classical strategy: 75% winning
- Best quantum strategy: ~85% winning
- Quantum advantage

Example: the CHSH game

- Quantum advantage implies secret randomness:



how **random** A is from the **adversary's** point of view

[Pironio, Acìn, Brunner *et al.*, 09]

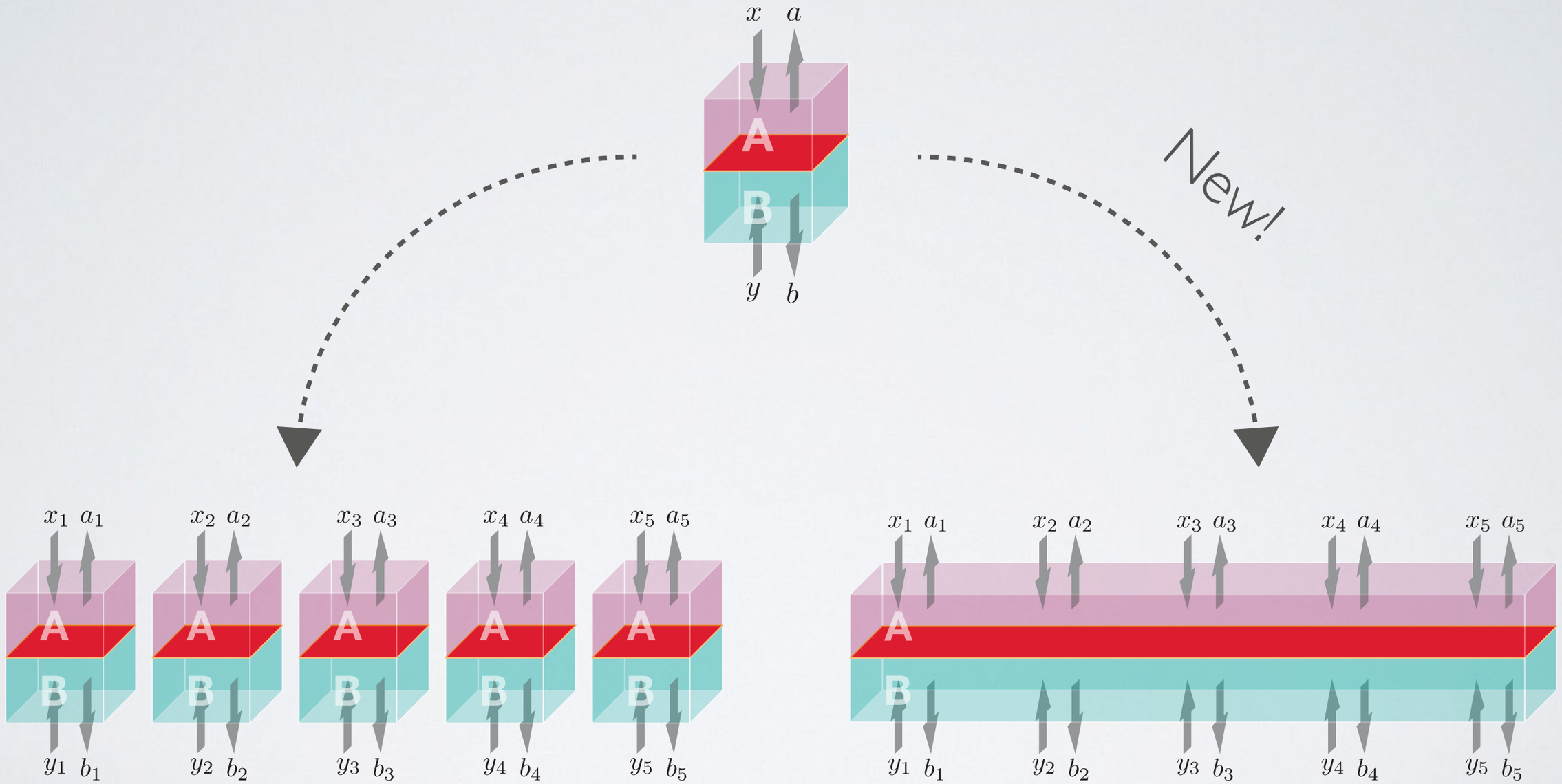
A taste of our work:

Simple and Tight Device-independent Security Proofs

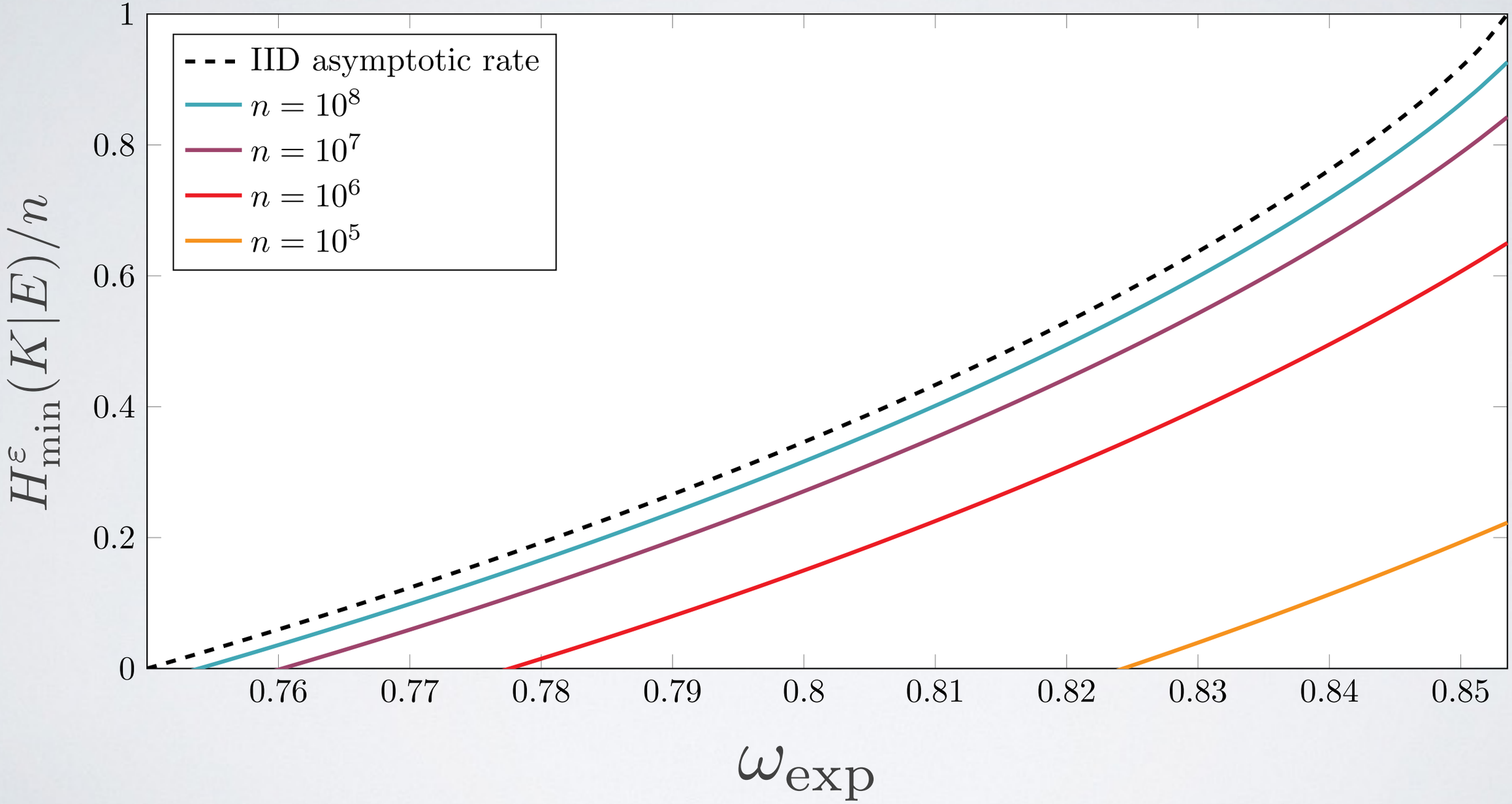
arXiv:1607.01797

Joint work with Renato Renner (ETH) and Thomas Vidick (Caltech)

A taste of our work



Entropy rate (CHSH)



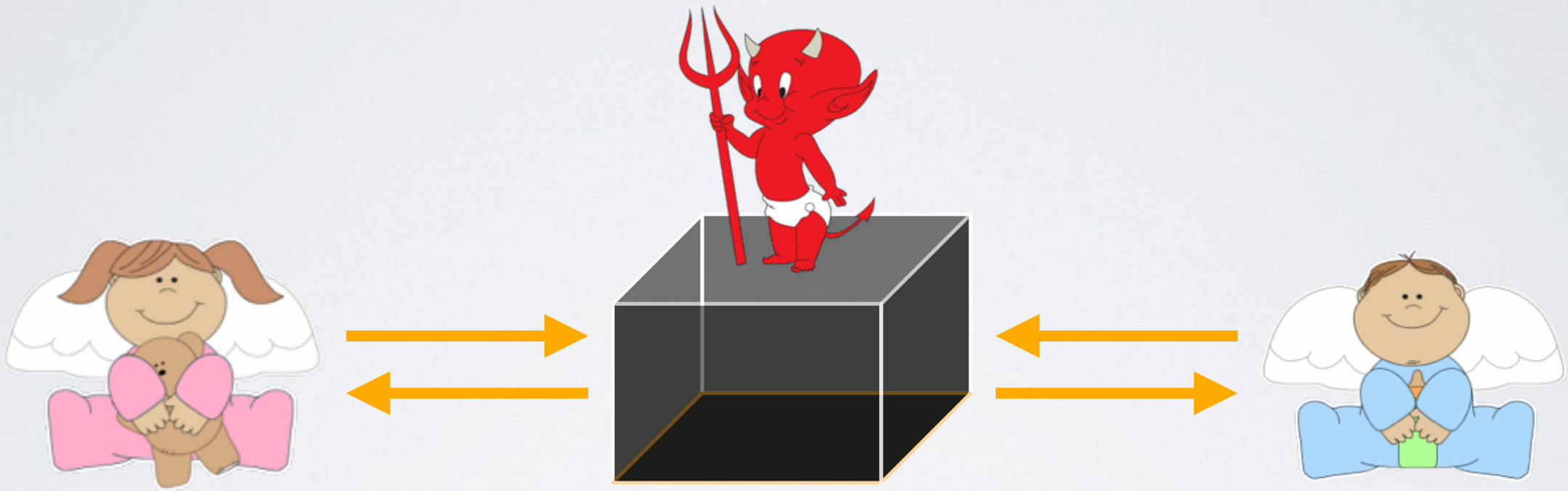
The next step: experiment!

- Loophole-free Bell tests
  - Delft university of technology, NIST, University of Vienna…
  - Necessary **first step** for device-independent cryptography

The next step: experiment!

- The next big challenge: an experiment that implements device-independent QKD
- Harder than the loophole-free Bell test
- The theory is now ready

Thank you!



Device-independent Quantum Cryptography

Rotem Arnon-Friedman (ETH)