Entropy Accumulation in Device-independent Protocols

QIP17

Seattle | January 19, 2017

arXiv: 1607.01796 & 1607.01797

Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, & Thomas Vidick

Outline

1. Introduction to device-independence

2. The difficulty of proving security

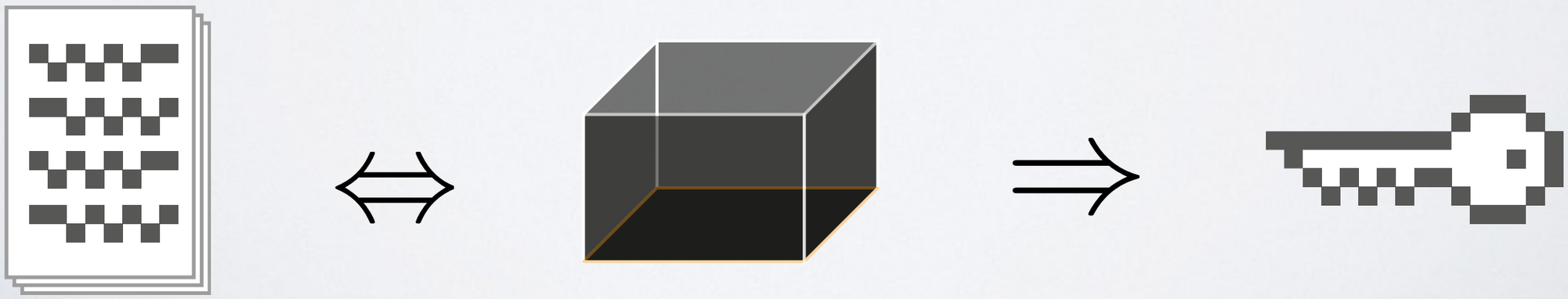
3. Overview …

Brief introduction to

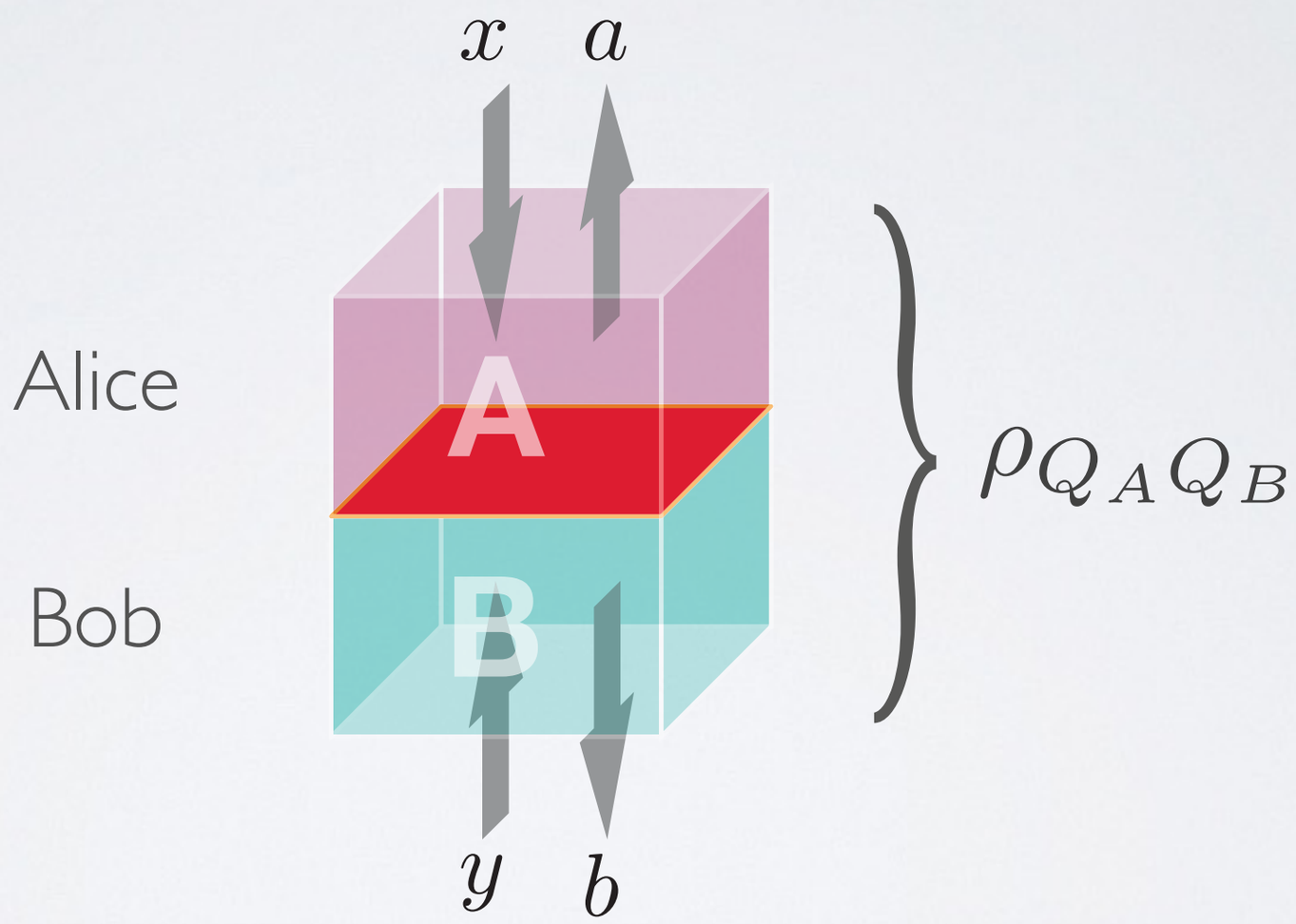
Device-independent Cryptography

The concept of DI

- Alice and Bob share an uncharacterised device
- They interact with it according to some known protocol (e.g., DI quantum key distribution protocol)
- They either abort or accomplish their task (e.g., output a good key)

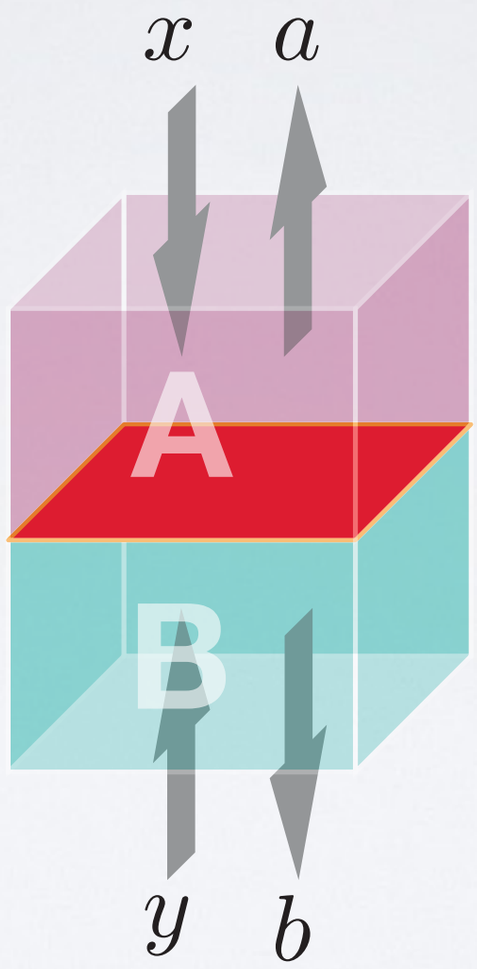


Bell inequality / game



Bell inequality / game

No communication



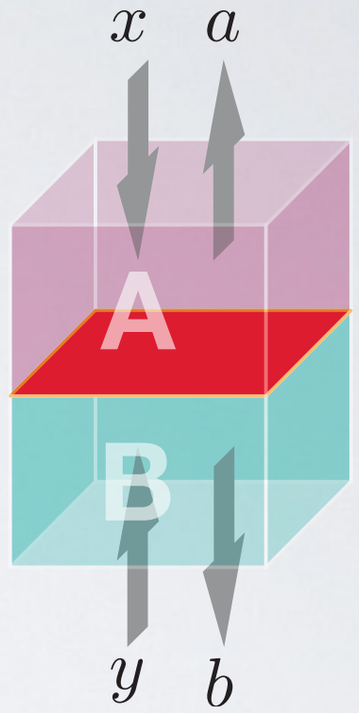
Winning condition: $\omega(a, b, x, y) \in \{0, 1\}$

Bell inequality / game

- Winning prob. of the device: $\omega \in [0, 1]$
- Bell inequality: $\forall \omega_c \quad \omega_c \leq I$
- Quantum advantage (violation): $\exists \omega_q \quad \omega_q > I$
- $\Rightarrow$ some secret randomness in the outputs with respect to an adversary holding a purification of $\rho_{Q_A Q_B}$

Example: the CHSH game

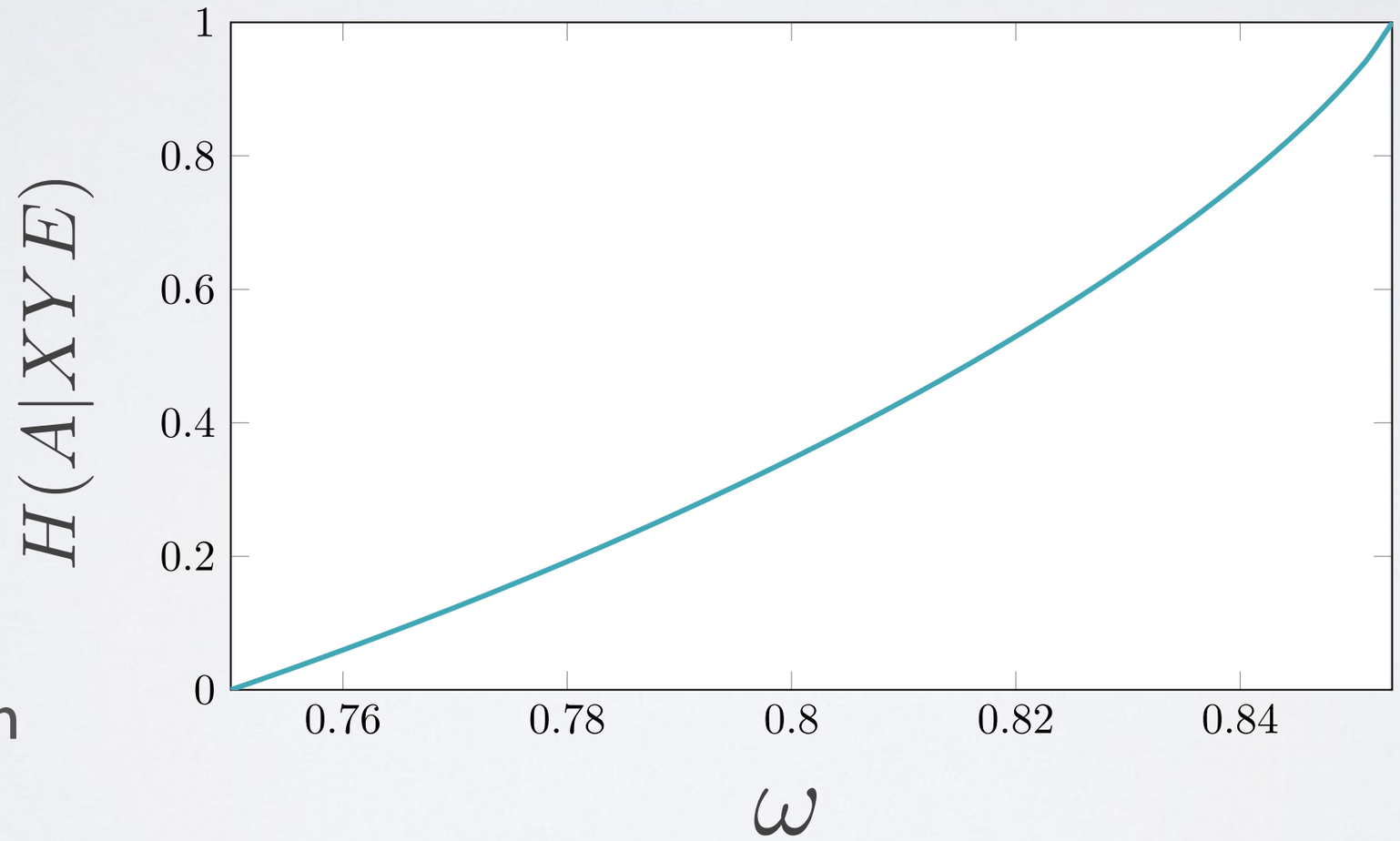
Alice:	Input	$x \in \{0, 1\}$
	Output	$a \in \{0, 1\}$
Bob:	Input	$y \in \{0, 1\}$
	Output	$b \in \{0, 1\}$
Win:		$a \oplus b = x \cdot y$



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

Example: the CHSH game

- Quantum advantage implies secret randomness:

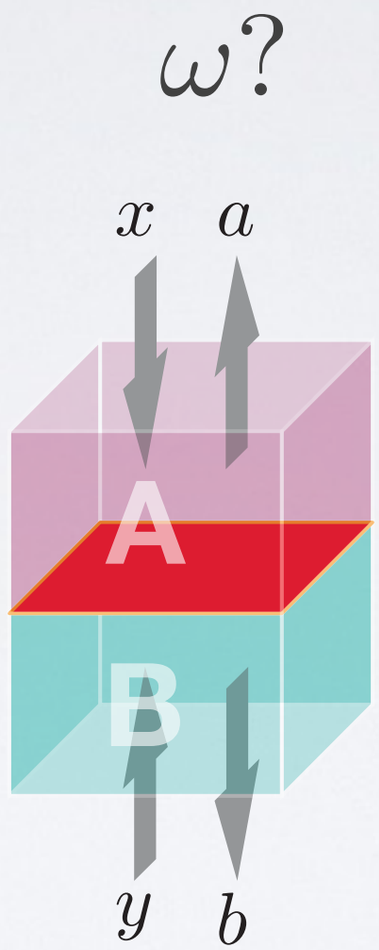


How **random** A is from **Eve**'s point of view

[Pironio, Acìn, Brunner *et al.*, 09]

The Difficulty of Proving Security

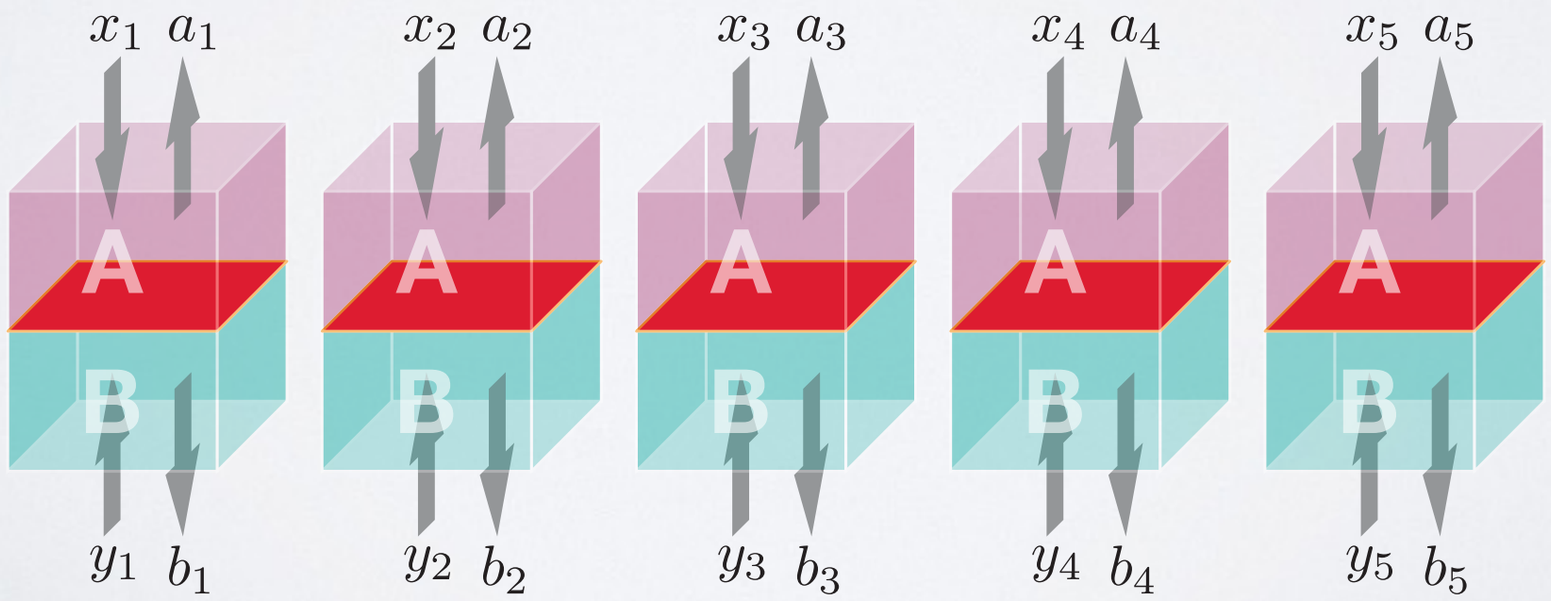
The difficulty of proving security



The IID assumption

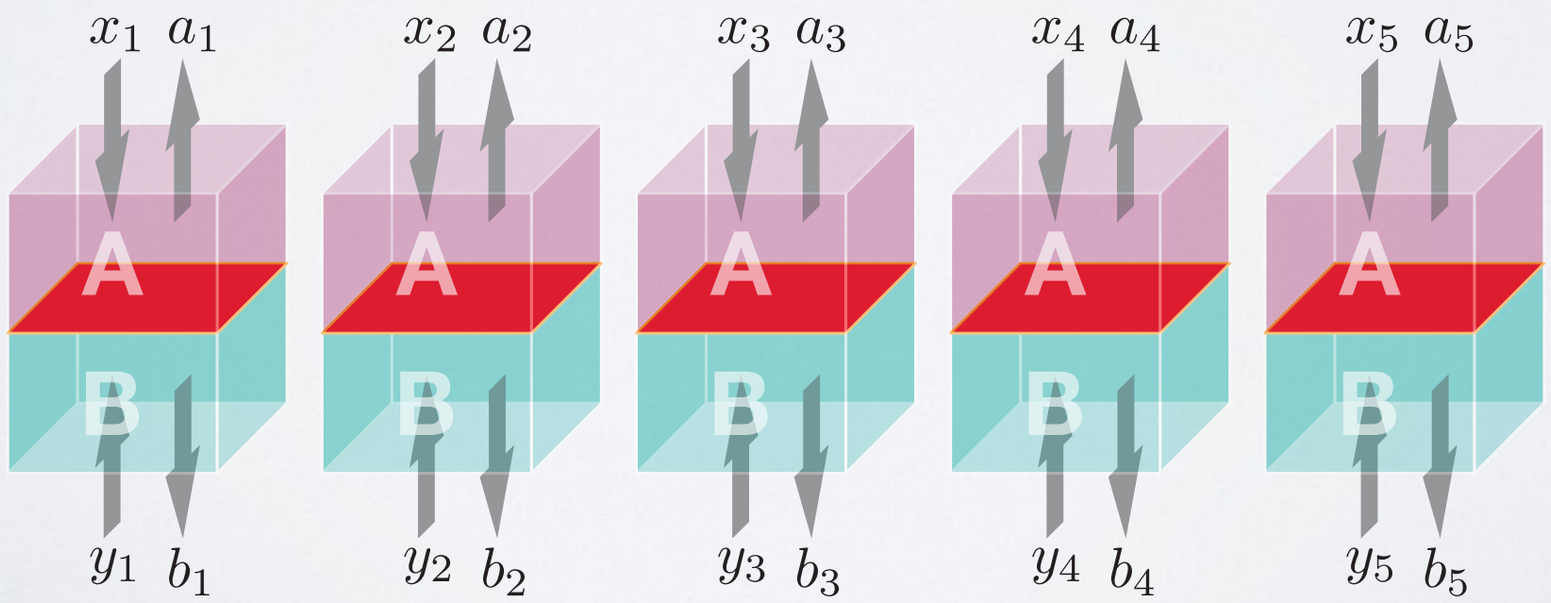
- Play the game many times independently and identically
- Estimate the winning probability in one device
- The total amount of entropy is *roughly* the number of games × entropy in one game

Simple! ✔



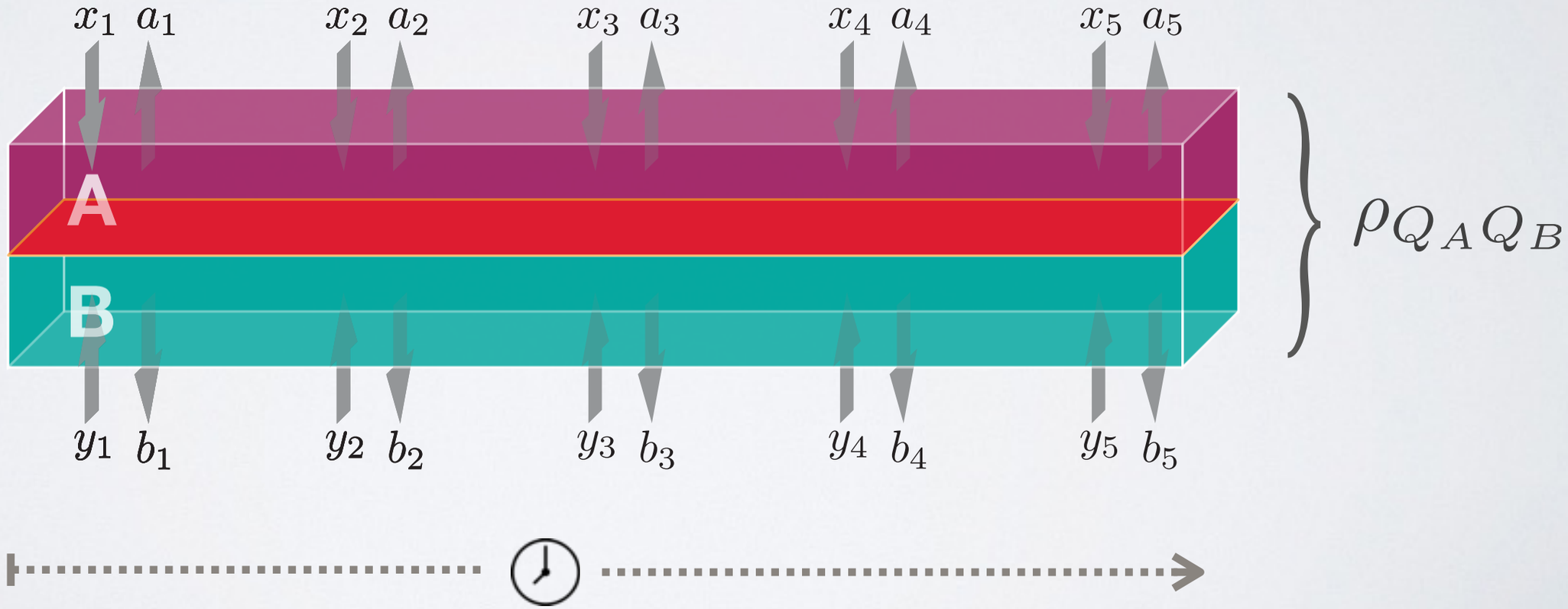
The IID assumption

- IID is a strong assumption! (e.g., no memory at all)
- Cannot use de Finetti theorems (in contrast to standard QKD for example)



The general case

- One component to each party
- Sequential interaction with Alice and Bob's components



Previous DIQKD works

[Ekert, 91]
[Mayers and Yao, 98]

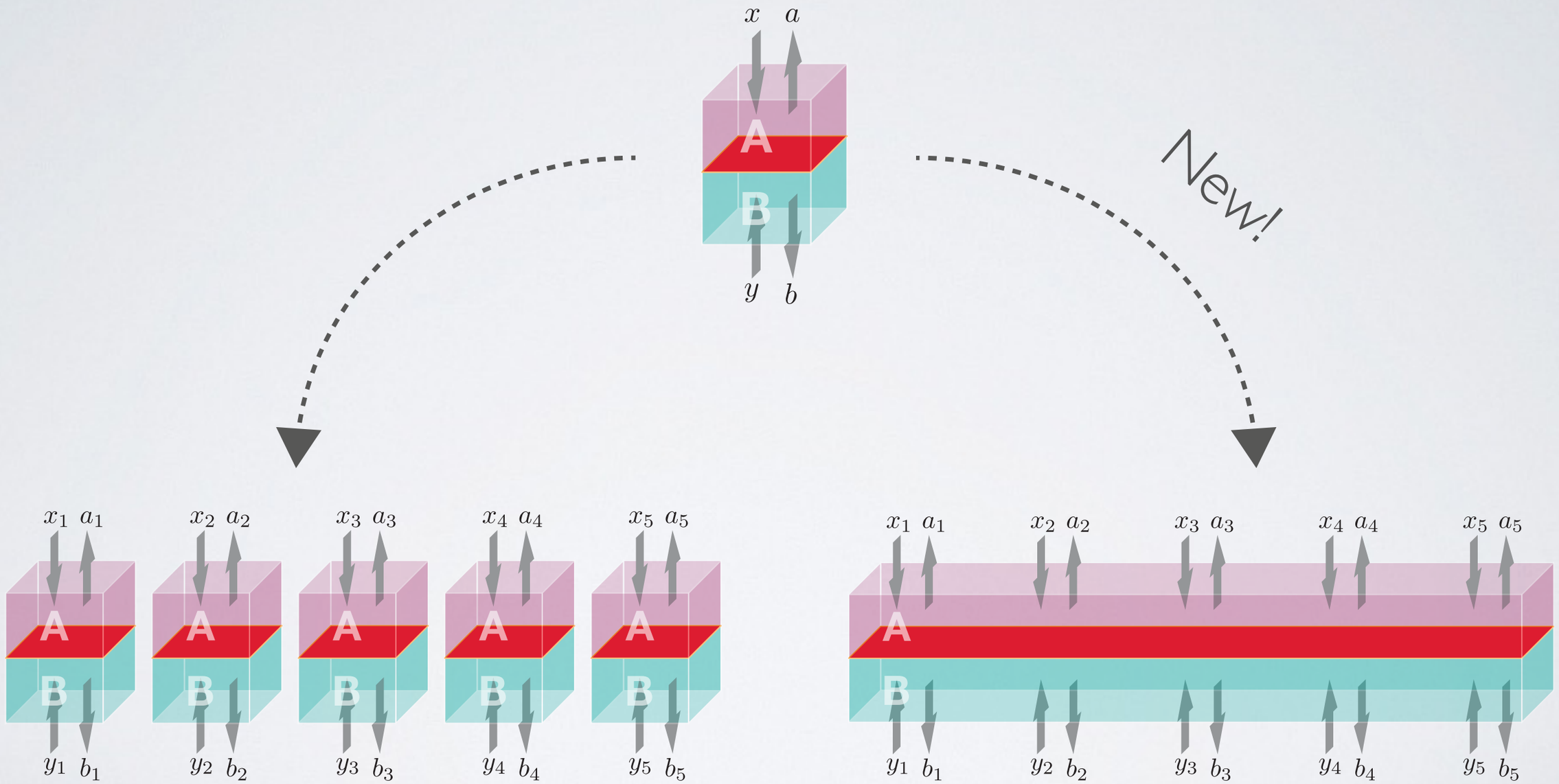
[Barrett, Hardy, and Kent, 05]
Proof of concept

[Pironio, Acìn, Brunner *et al.*, 09]
IID + asymptotic
Optimal rates! ✔

General security
[Reichardt, Unger, and Vazirani, 13]
[Vazirani and Vidick, 14]
[Miller and Shi, 14]

Overview

Overview


x a
A
B
y b
New!
x_1 a_1 x_2 a_2 x_3 a_3 x_4 a_4 x_5 a_5
A
B
y_1 b_1 y_2 b_2 y_3 b_3 y_4 b_4 y_5 b_5
IID
x_1 a_1 x_2 a_2 x_3 a_3 x_4 a_4 x_5 a_5
A
B
y_1 b_1 y_2 b_2 y_3 b_3 y_4 b_4 y_5 b_5
Sequential

Outline of the rest of talk

4. Security under the IID assumption

5. General security proof

   - New tool: the Entropy Accumulation Theorem
   - Application: new results for DI cryptography

6. Summary and open questions

Security Proof under the IID Assumption

Proving security

- Main task: lower-bounding the smooth min-entropy

$$H_{\min}^{\varepsilon}(K|E)$$

where K is the raw data, E the quantum side-information belonging to the adversary, and ε a security parameter

- Tightly determines the maximal length of an extractable secret key

Security — IID

- $K = K_1 \dots K_n$ IID random variables
- $E = E_1 \dots E_n$ IID quantum side-information

- For the **von-Neumann entropy**:

$$\begin{aligned} H(K_1 \dots K_n | E_1 \dots E_n) &= \sum_i H(K_i | E_1 \dots E_n K_1 \dots K_{i-1}) \\ &= \sum_i H(K_i | E_i) \\ &= n H(K_1 | E_1) \end{aligned}$$

Security — IID

- $K = K_1 \dots K_n$ IID random variables
- $E = E_1 \dots E_n$ IID quantum side-information
- For the **smooth min-entropy**:

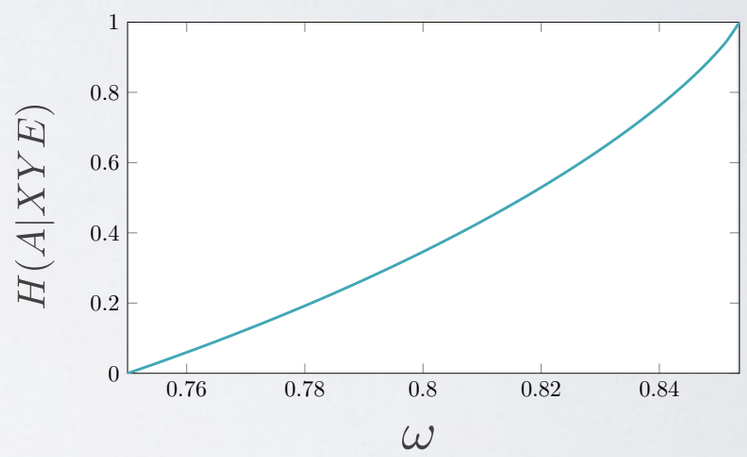
$$H_{\min}^{\varepsilon}(K|E) \geq nH(K_1|E_1) - c_\varepsilon \sqrt{n}$$

Quantum Asymptotic Equipartition Property
[Tomamichel, Colbeck, and Renner, 09]

Security — IID

1. Play the game many times and calculate the average winning probability

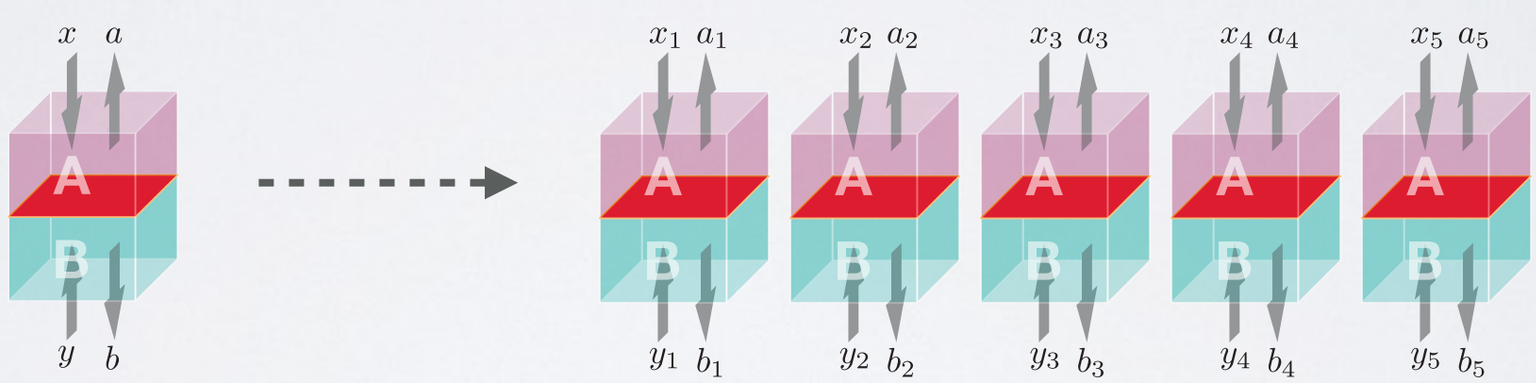
2. Use the single-round relation between the winning probability and the von-Neumann entropy



3. Plug into the quantum AEP: total smooth min-entropy is $nH(K_1|E_1)$ in first order

Security — IID (remarks)

- Need to understand only the physics of a single-round Simple! ✔

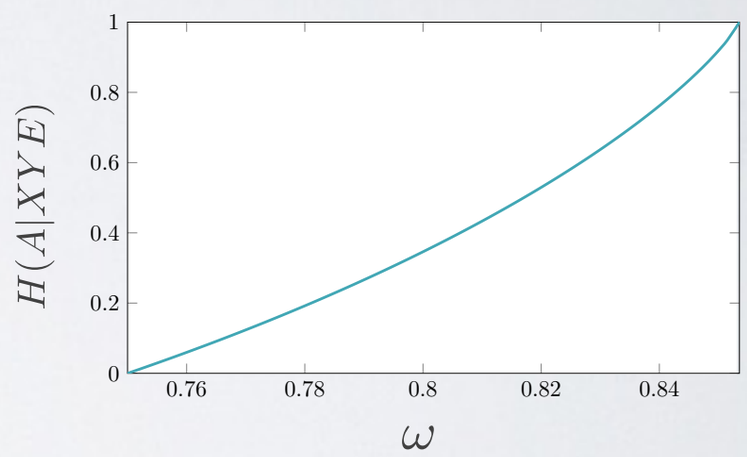


- The von-Neumann entropy is the relevant single-round quantity Tight! ✔

Security — IID

1. Play the game many times and calculate the average winning probability

2. Use the single-round relation between the winning probability and the von-Neumann entropy



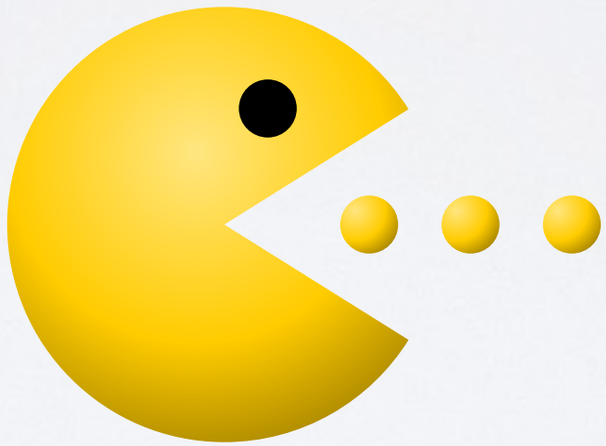
3. Plug into the quantum AEP: total smooth min-entropy is $nH(K_1|E_1)$ in first order

General Security Proof

General security

- Still need to lower-bound $H_{\min}^{\varepsilon}(K|E)$
- Instead of IID behaviour of the device, consider more general sequential processes
- "Extend" the quantum AEP to the sequential scenario $\Rightarrow$ The Entropy Accumulation Theorem

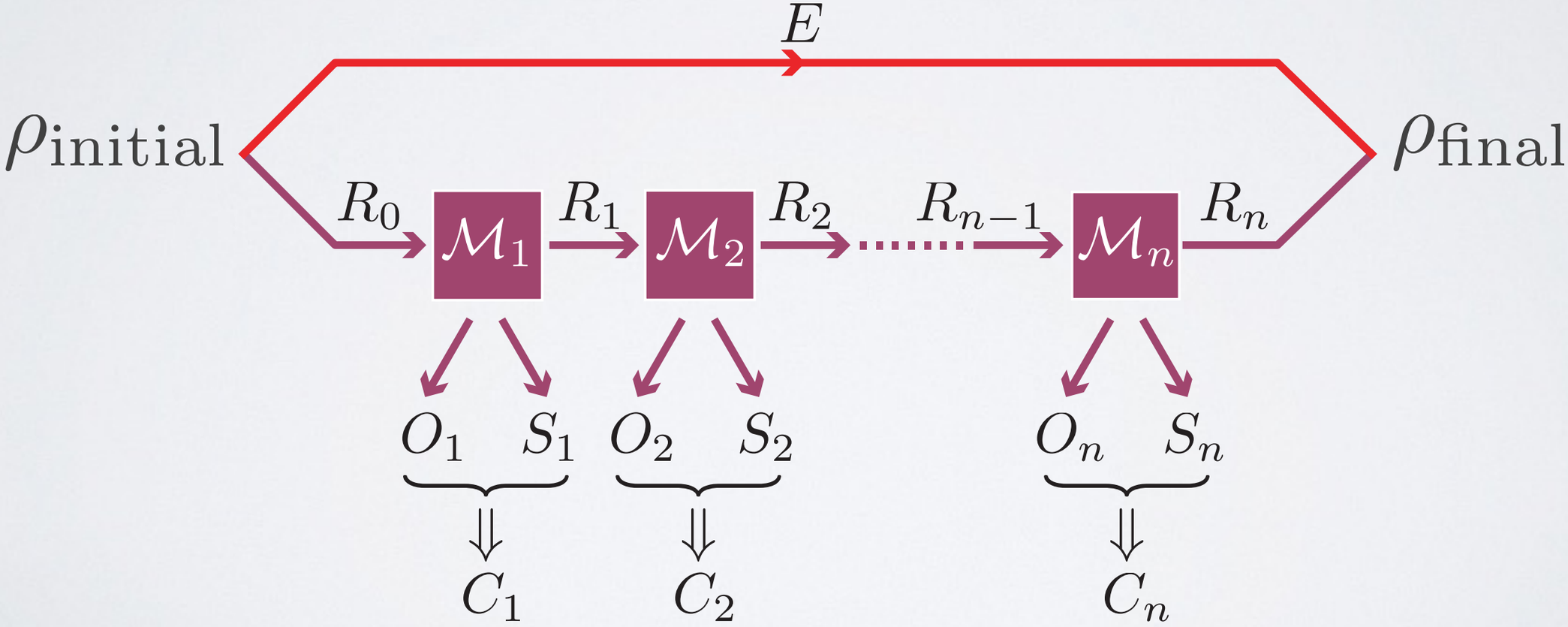
The EAT



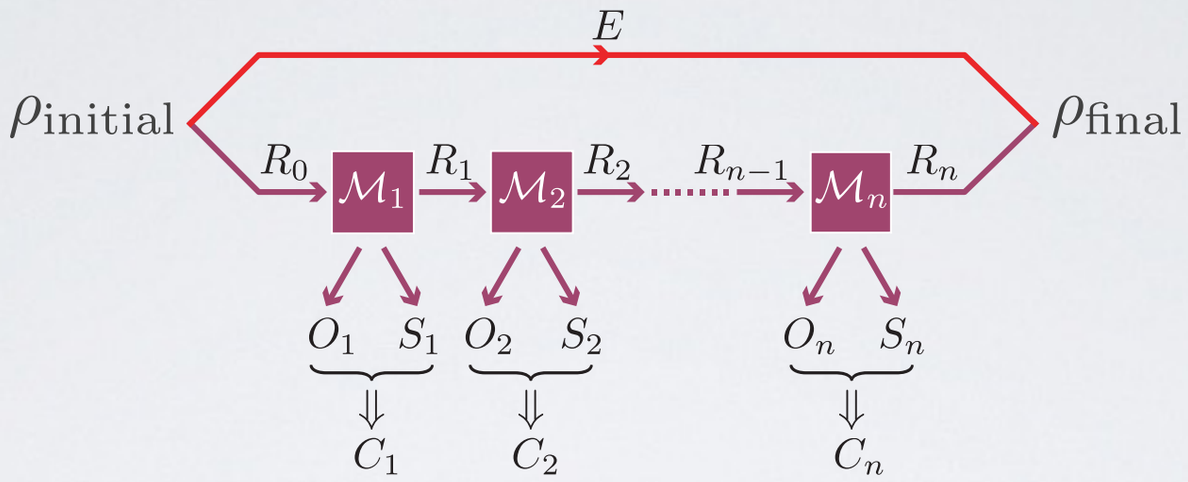
Sequential process

- Model of a sequential process:

$H^{\varepsilon}_{\min}(O|SE)?$



EAT channels



- Assumptions on the channels: $\forall i$

1. O_i finite dimensional with dimension d_{O_i}

2. C_i is a classical register that can be measured from $\rho_{O_i S_i}$ without changing the state

3. For any initial state, the final state fulfils the Markov-chain condition: $O_{1\ldots i-1} \leftrightarrow S_{1\ldots i-1} E \leftrightarrow S_i$

Empirical statistics

$$c_1 \dots c_n = 0100110000000010$$

- Frequencies from the observed data:

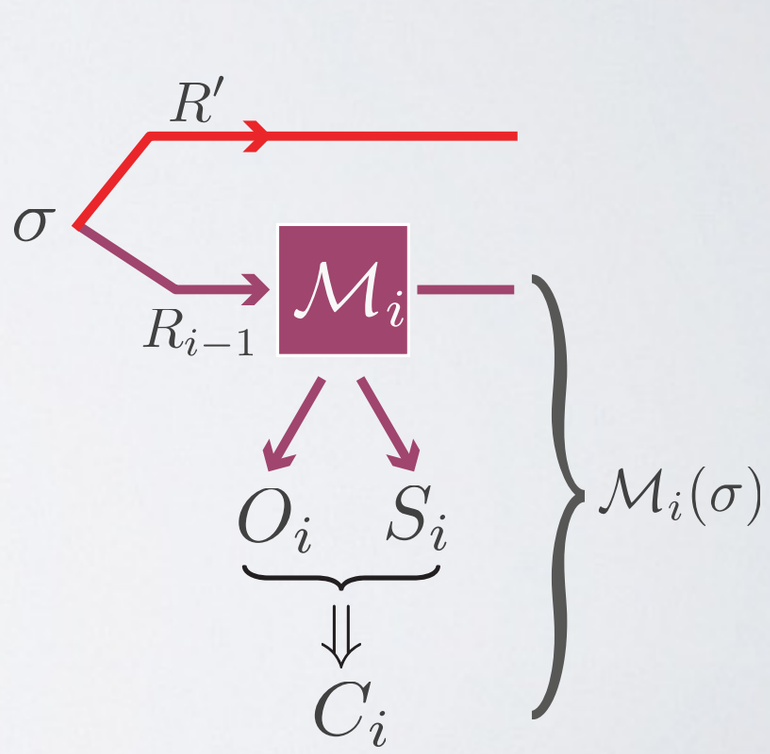
$$\mathsf{freq}(c_1 \dots c_n)(0) = \frac{3}{4} \qquad \mathsf{freq}(c_1 \dots c_n)(1) = \frac{1}{4}$$

- $\mathsf{freq}(c_1 \dots c_n)$ is a probability distribution over $\mathcal{C}$

Min-tradeoff function

- Min-tradeoff function $f_{\min}$ — worst-case von-Neumann entropy in a single-round

$$f_{\min}(\mathsf{freq}(c_1 \dots c_n)) \leq \inf H\left(O_i | S_i R'\right)_{\mathcal{M}_i(\sigma)}$$



- The infimum is over states $\sigma_{R_{i-1}R'}$ such that

$$\mathcal{M}_i(\sigma)_{C_i} = \mathsf{freq}(c_1 \dots c_n)$$

Entropy accumulation theorem

- Event depending on the frequencies $\Omega \subseteq \mathcal{C}^{\otimes n}$
- $\rho_{|\Omega}$ the final state conditioned on Ω
- $t \in \mathbb{R}$ such that $f_{min}(\mathsf{freq}(c_1 \dots c_n)) \geq t$ for all $c_1 \dots c_n \in \Omega$

Entropy accumulation theorem

- $f_{min}(\mathsf{freq}(c_1 \dots c_n)) \geq t$ for all $c_1 \dots c_n \in \Omega$
- EAT:

$$H^{\varepsilon}_{\min}(O|SE)_{\rho_{|\Omega}} > nt - v\sqrt{n}$$

where v depends on $\|\nabla f_{\min}\|_{\infty},\ \varepsilon,\ p_{\Omega},\ d_{O_i}$

- Similar statement for the smooth max-entropy

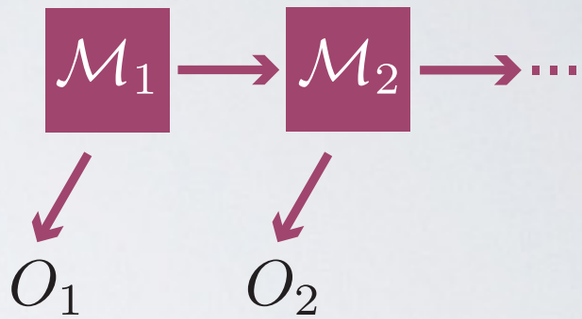
Main ingredients in the proof

- Heavily relies on the sandwiched relative Rényi entropies introduced in [Wilde, Winter, and Yang, 14] and [Müller-Lennert, Dupuis, Szehr, *et al.*, 13]

- A new chain rule for the sandwiched relative Rényi entropies was developed to prove the EAT

Main ingredients in the proof

- "Classical version of the min-tradeoff function":
  Seq. proc. creates $O_1, O_2, \ldots$
  How much can we extract from O_2 after we use O_1?



$$H(O_2|O_1) = \mathbb{E}_{o_1,o_2}\left[-\log \Pr(o_2|o_1)\right]$$

Too optimistic

$$H^{w.c.}_{\min}(O_2|O_1) = \min_{o_1,o_2}\left[-\log \Pr(o_2|o_1)\right]$$

Too pessimistic

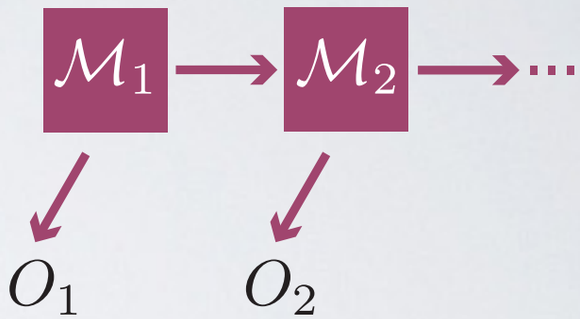
$O_1 = 0 \Rightarrow O_2 = 0$

$O_1 = 1 \Rightarrow O_2$ uniform

O_1 & O_2 independent

Main ingredients in the proof

- "Classical version of the min-tradeoff function":
  Seq. proc. creates $O_1, O_2, \ldots$
  How much can we extract from O_2 after we use O_1?



$$H(O_2|O_1) = \mathbb{E}_{o_1,o_2}\left[-\log \Pr(o_2|o_1)\right]$$

Too optimistic

$$H^{w.c.}_{\min}(O_2|O_1) = \min_{o_1,o_2}\left[-\log \Pr(o_2|o_1)\right]$$

Too pessimistic

Intermediate:

$$\min_{o_1} \mathbb{E}_{o_2} - \log \Pr[o_2|o_1]$$

the min-tradeoff function is the "quantum version" of this

Finally, we are ready!

Applying the EAT to DI Cryptography

DI entropy accumulation pro.

- Main building block in DI cryptographic protocols

DI Entropy Accumulation Protocol

Arguments:

G – two-player non-local game
$\mathcal{X}, \mathcal{Y}$ – possible inputs for Alice Bob
D – untrusted device of two components that can play G repeatedly
$n \in \mathbb{N}_+$ – number of rounds
ω_{exp} – expected winning prob. for an honest (noisy) implementation
$\delta_{\text{est}} \in (0, 1)$ – width of the statistical confidence interval

1: For every round $i \in [n]$ do Steps 2-4:
2: Alice and Bob choose inputs $X_i \in \mathcal{X}$ and $Y_i \in \mathcal{Y}$ respectively.
3: They use D with X_i, Y_i and record the outputs A_i and B_i respectively.
4: They set $C_i = w(A_i, B_i, X_i, Y_i)$.
5: Alice and Bob abort if $\sum_j C_j < (\omega_{\text{exp}} - \delta_{\text{est}}) \cdot n$.

DI entropy accumulation pro.

- Channels — the behaviour of Alice and Bob + uncharacterised device in each round

- C_i — win or lose in game i

- Event Ω — the protocol not aborting

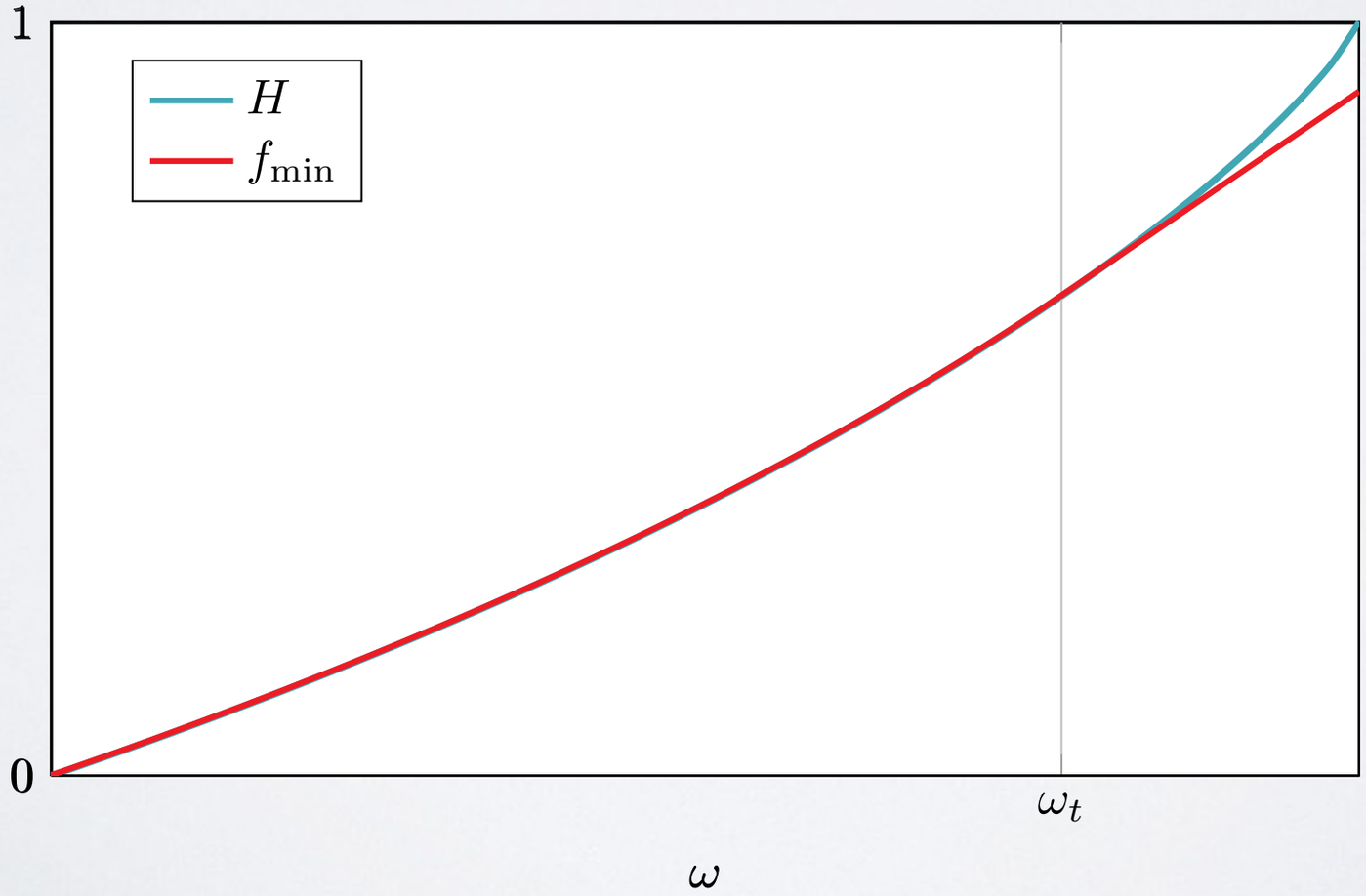
$$\Omega = \{c | \sum_i c_i \geq (\omega_{\text{exp}} - \delta_{\text{est}}) \cdot n\}$$

- $\rho_{|\Omega}$ — final state conditioned on not aborting

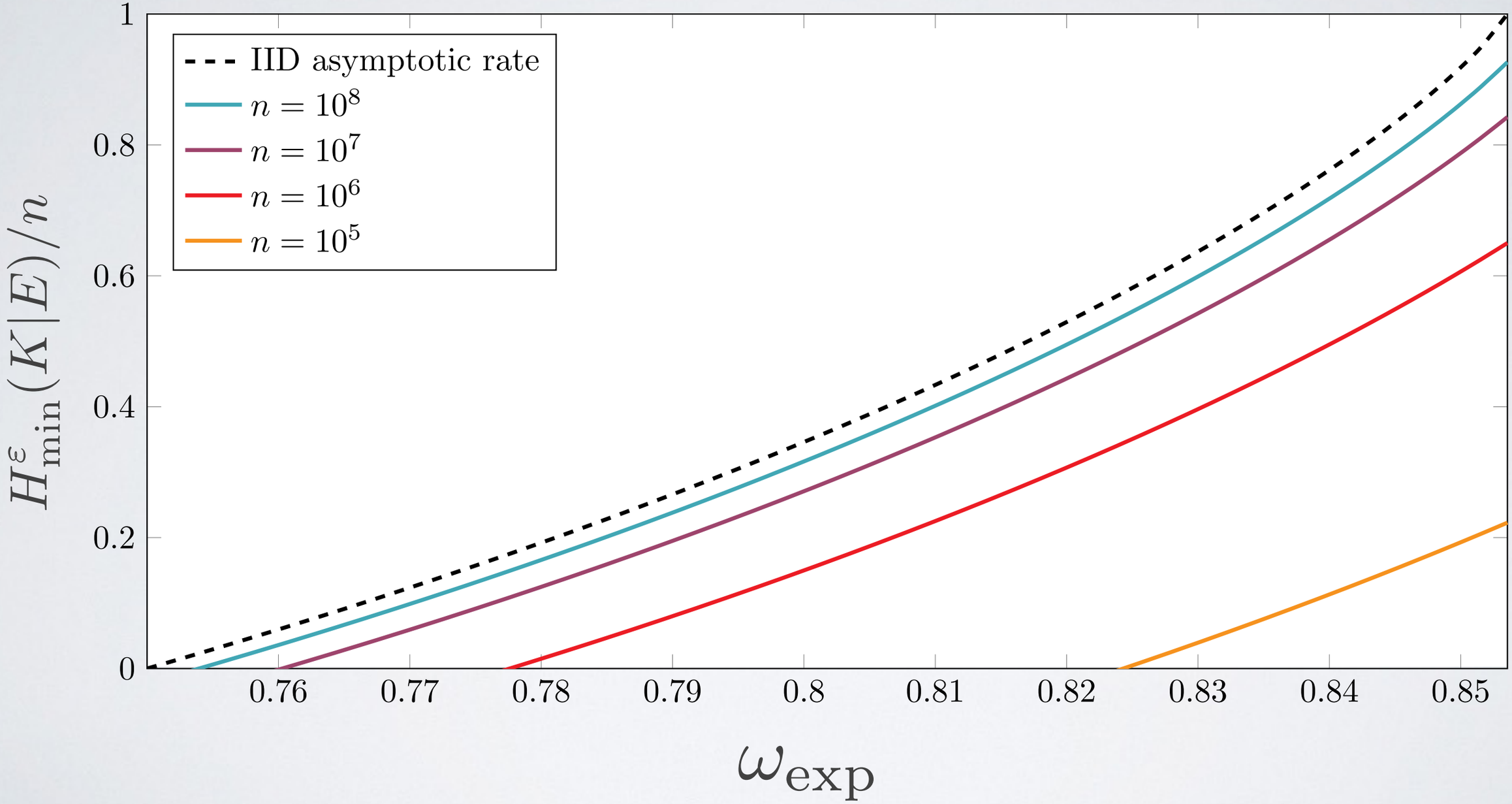
- We lower-bound $H^{\varepsilon}_{\min}(A|XYE)_{\rho_{|\Omega}}$

Min-tradeoff function

$$f_{\min}(\omega) \leq \inf_{\substack{\sigma \text{ with winning} \\ \text{prob.} \geq \omega_{\exp} - \delta_{\text{est}}}} H(A_1|X_1 Y_1 E)_{\mathcal{M}_i(\sigma)}$$



Entropy rate (CHSH)



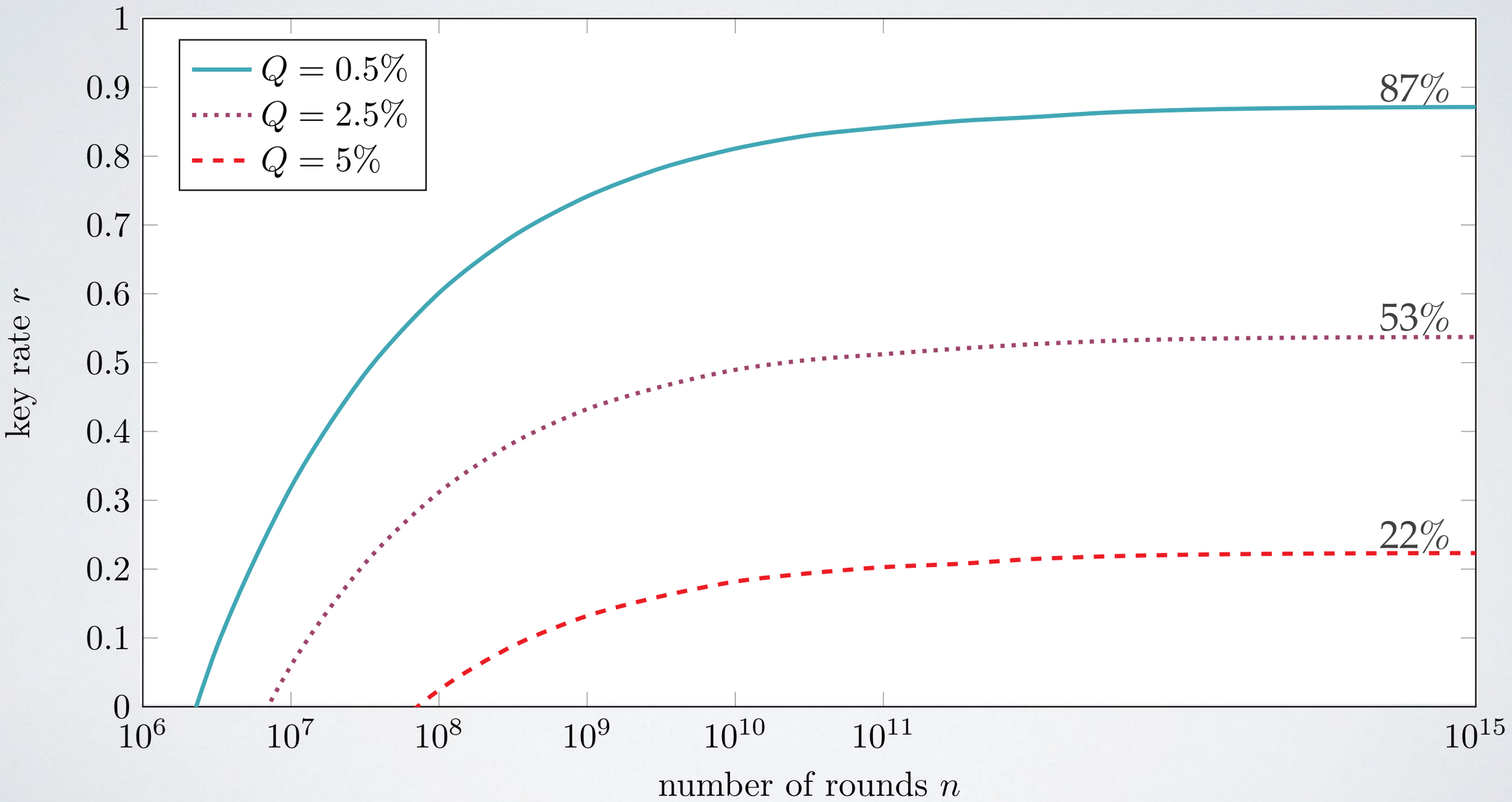
DIQKD

- Based on the Entropy Accumulation protocol
- Classical-post processing on top:
  - Error correction
  - Privacy amplification

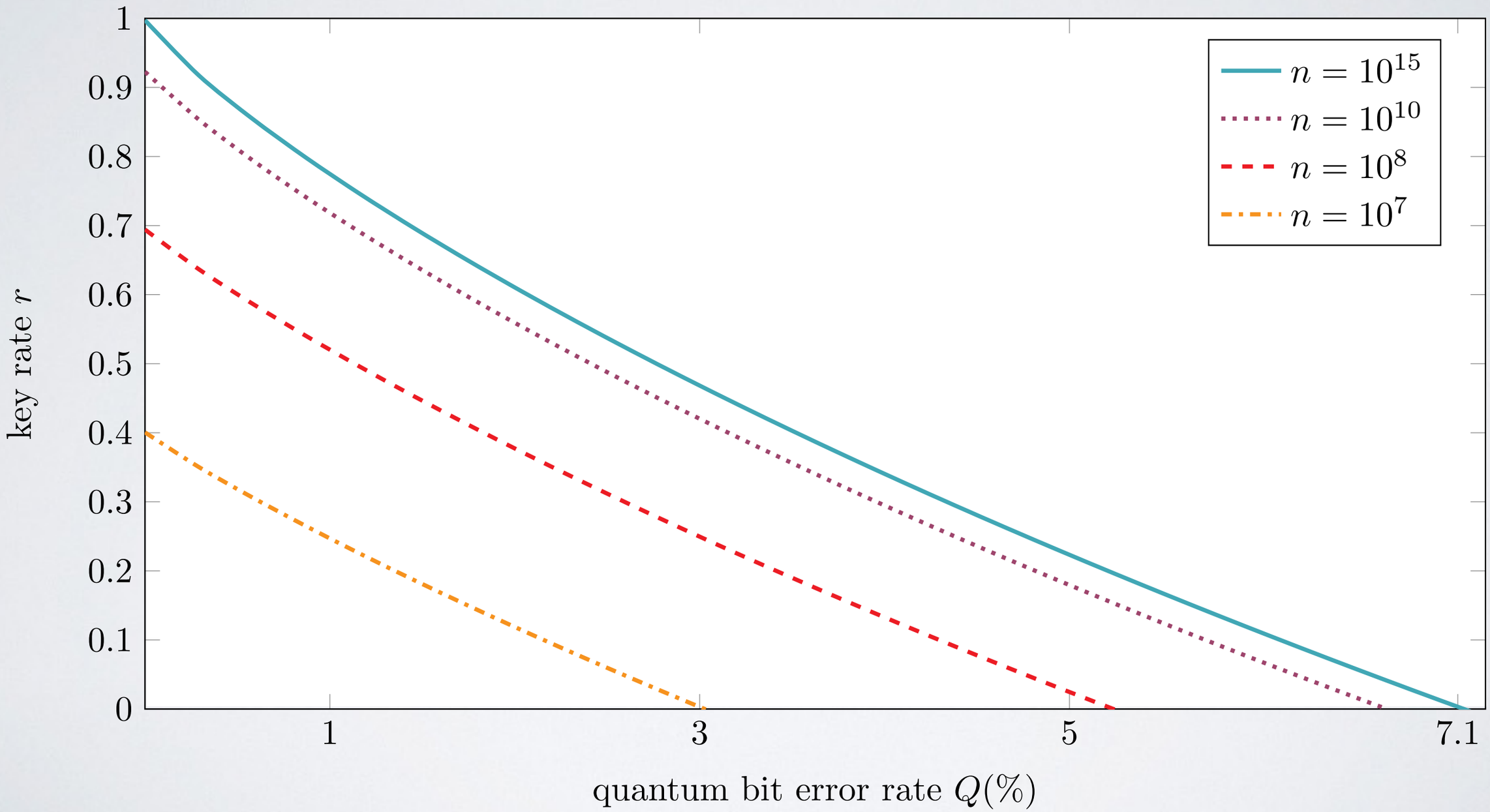
DIQKD — The setting

- Standard assumptions:
  - Alice and Bob's physical locations are secure (unwanted information cannot leak outside to Eve or between their devices)
  - Trusted random number generator
  - Trusted classical post-processing units
  - Authenticated, but public, classical channel
  - Quantum physics is correct (and complete)
- Communication is allowed between Alice and Bob, and from Eve to Alice and Bob, between the rounds of the game (can create "entanglement on the fly")

DIQKD

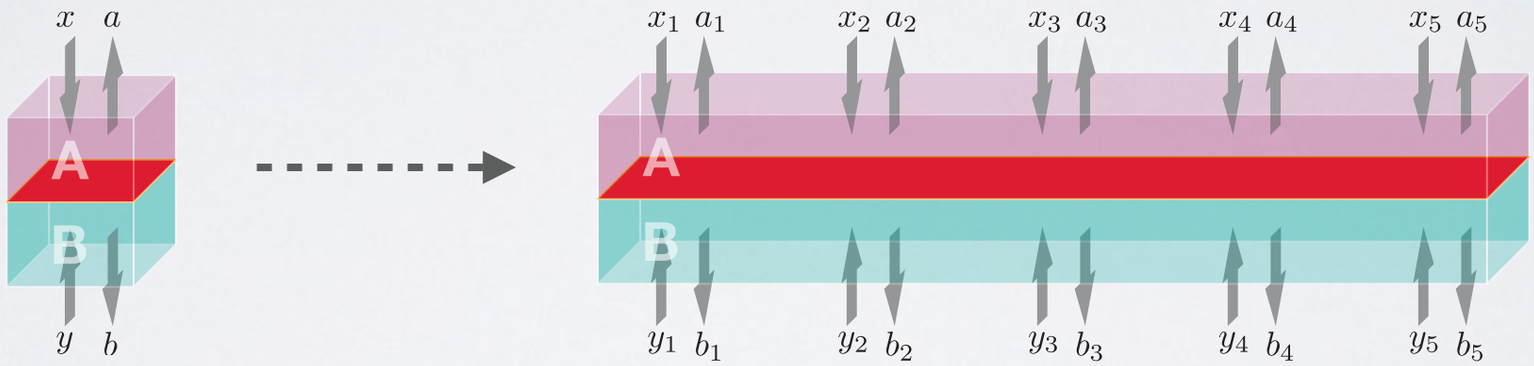

$Q = 0.5\%$
$Q = 2.5\%$
$Q = 5\%$
87%
53%
22%
key rate r
number of rounds n
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
10^6
10^7
10^8
10^9
10^{10}
10^{11}
10^{15}

DIQKD


key rate r
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
1
3
5
7.1
quantum bit error rate $Q(\%)$
$n = 10^{15}$
$n = 10^{10}$
$n = 10^{8}$
$n = 10^{7}$

General security (remarks)

- Need to understand only the physics of a single-round Simple! ✔



- The von-Neumann entropy is the relevant single-round quantity Tight! ✔

- The optimal attack is the IID attack in first order

Summary

Summary

1. New information-theoretic tool: the EAT

- Describes how entropy accumulates in sequential quantum processes
- The von-Neumann entropy is the relevant single-round quantity

2. New framework to prove security of DI protocols

- Modular, simple, and tight security proof
- Concrete examples: DIQKD and randomness expansion based on CHSH
- In essence, the best adversarial attack is the IID attack also in the DI scenario

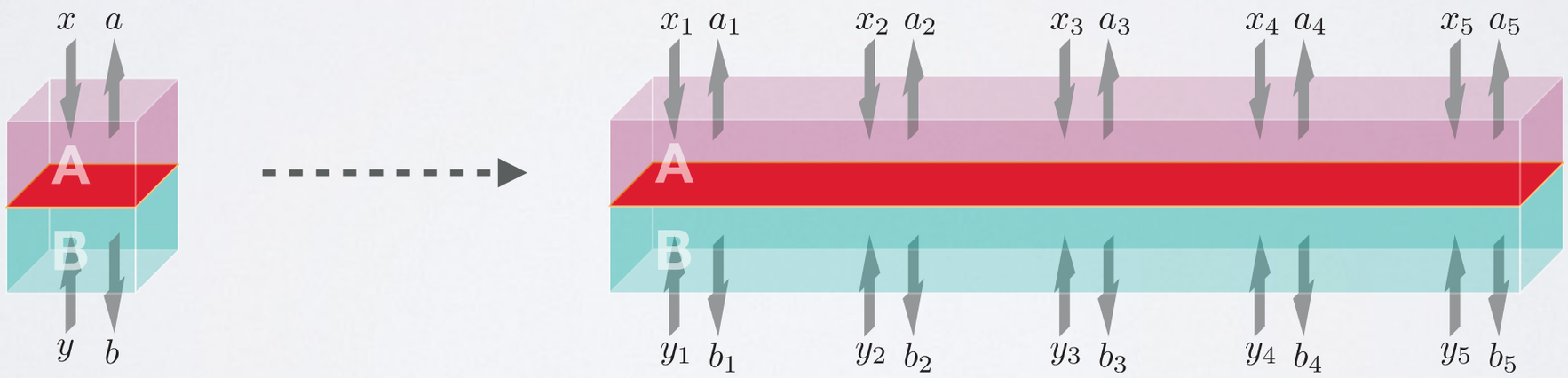
What's next?

1. Apply the EAT and our framework to other protocols and scenarios
   - Example: two-party DI crypto [Ribeiro, Murta, and Wehner, 16]
   - Also relevant for device dependent cryptography, instead of de Finetti thm.
2. DIQKD:
   - Apply with different Bell inequalities & classical post-processing
   - Experiment: detection efficiencies should be relatively high for a positive key rate with the current protocol
3. Is there a general technique to bound the conditional von-Neumann entropy $H(K_1|E_1)$ given the Bell violation?

Thank you!

Entropy Accumulation in Device-independent Protocols

arXiv: 1607.01796 & 1607.01797



Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, & Thomas Vidick

References

- [BHK05] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. Physical Review Letters, 95(1):010503, 2005.
- [Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. Physical review letters, 67(6):661, 1991.
- [MS14] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In Proceedings of the 46th Annual ACM Symposium on Theory of Computing, pages 417–426. ACM, 2014.
- [MLDS+13] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel. On quantum Rényi entropies: A new generalization and some properties. J. Math. Phys., 54(12):122203, 2013.
- [MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on, pages 503–509. IEEE, 1998.
- [PAB+09] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. New Journal of Physics, 11(4):045021, 2009.
- [RUV13] B. W. Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systems. Nature, 496(7446):456–460, 2013.
- [RMW16] J. Ribeiro, G. Murta, S. Wehner. Fully general device-independence for two-party cryptography and position verification. arXiv:1609.08487.
- [TCR09] M. Tomamichel, R. Colbeck, and R. Renner. A fully quantum asymptotic equipartition property. IEEE Trans. Inform. Theory, 55:5840-5847, 2009.
- [VV14] U. Vazirani and T. Vidick. Fully device-independent quantum key distribution. Physical review letters, 113(14):140501, 2014.
- [WWY14] M. Wilde, A. Winter, and D. Yang. Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy. Comm. Math. Phys., 331(2):593–622, 2014.