Simple and Tight Device-independent Security Proofs

QCrypt 16

Washington DC | September 12, 2016

arXiv:1607.01797

Rotem Arnon-Friedman (ETH), Renato Renner (ETH), and Thomas Vidick (Caltech)

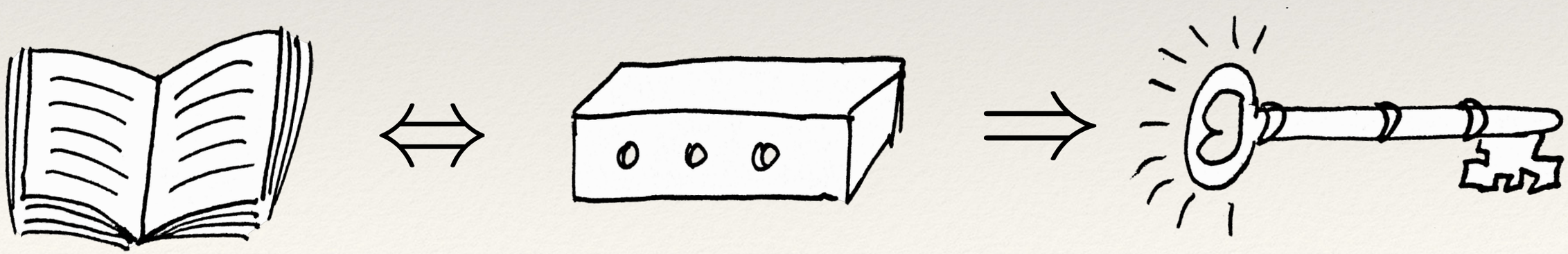
Outline

1. Introduction
2. The difficulty of proving security
3. Contribution and results
4. Proof technique
5. Outlook

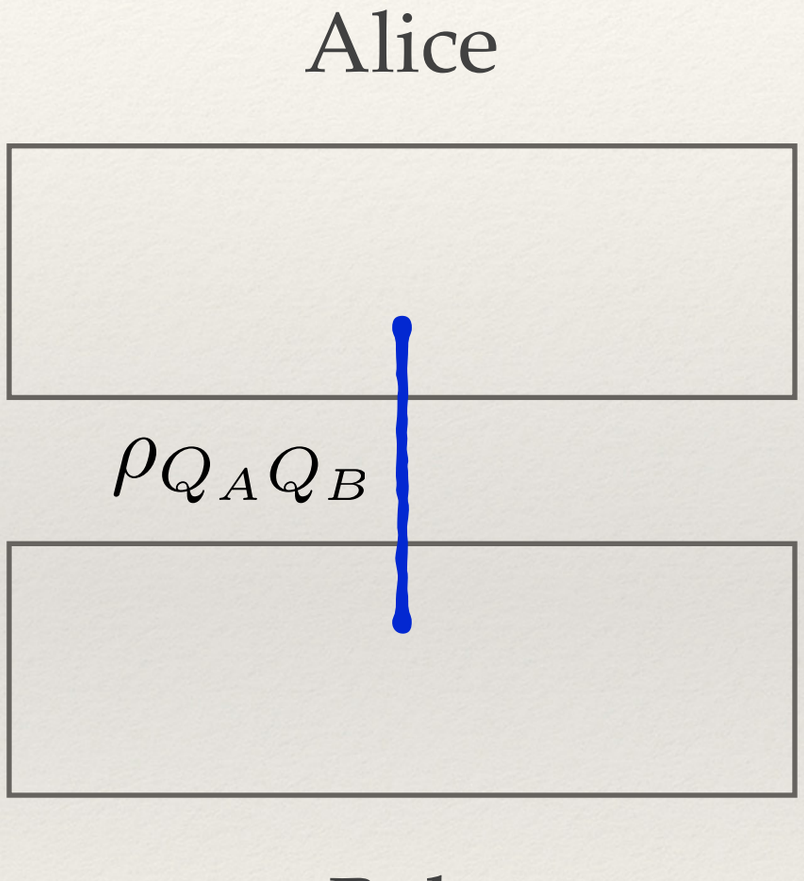
The concept of device independence

The concept of DI

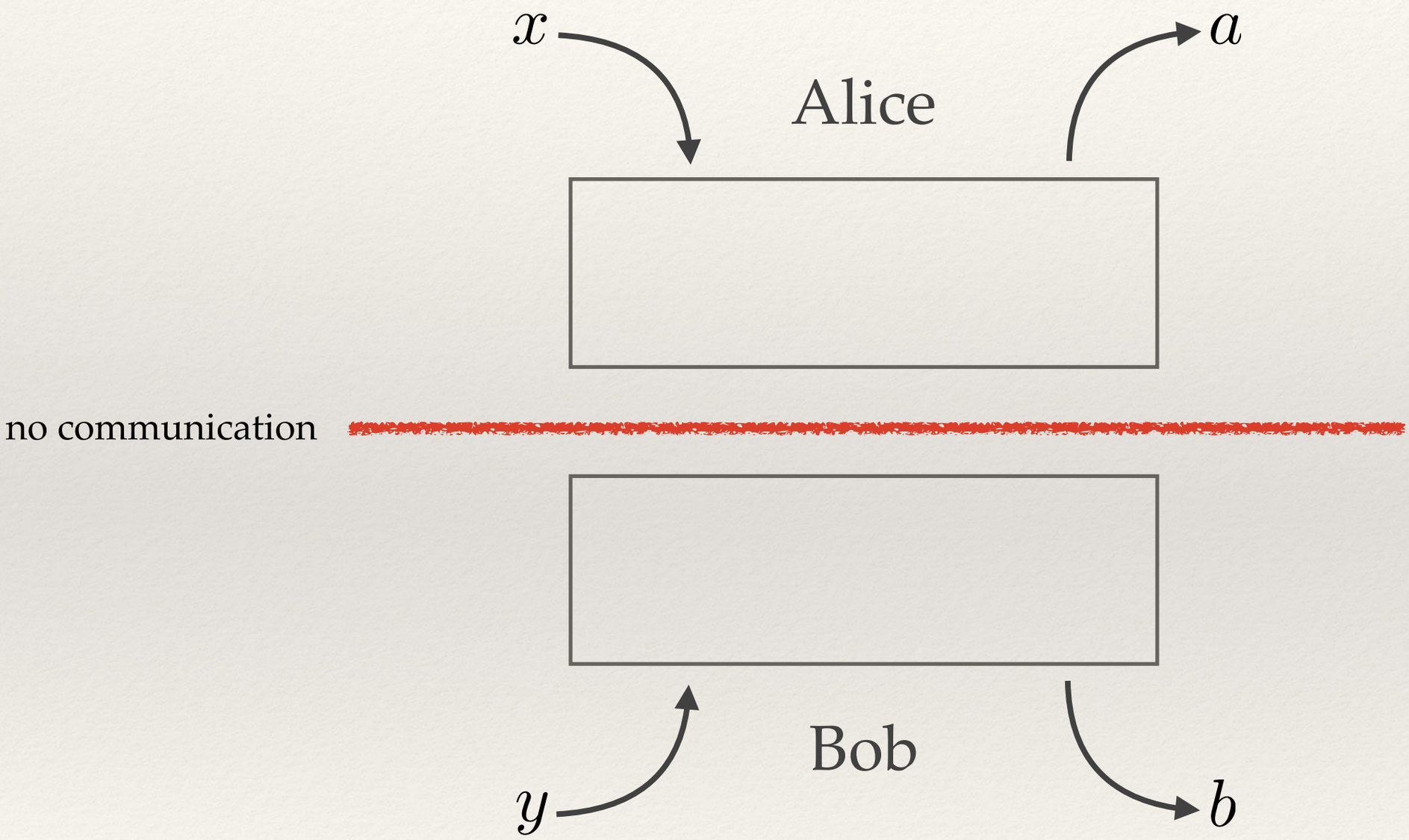
- Alice and Bob share an uncharacterised device
- They interact with it according to some known protocol (e.g., DI quantum key distribution protocol)
- They either abort or accomplish their task (e.g., output a good key)



Bell inequality / game



Bell inequality / game



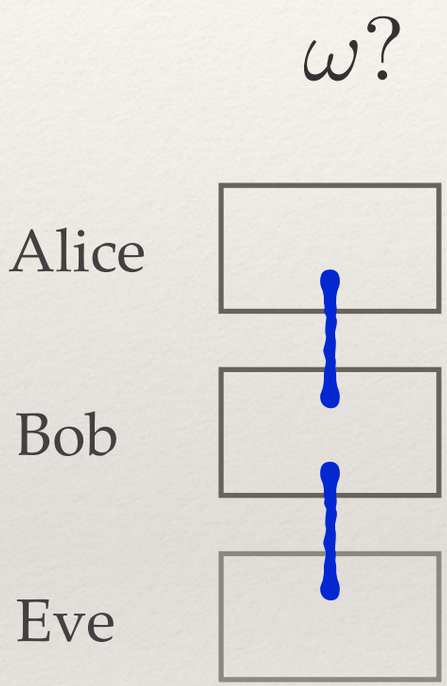
Winning condition: $w(a, b, x, y) \in \{0, 1\}$

Bell inequality / game

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

The difficulty of proving security

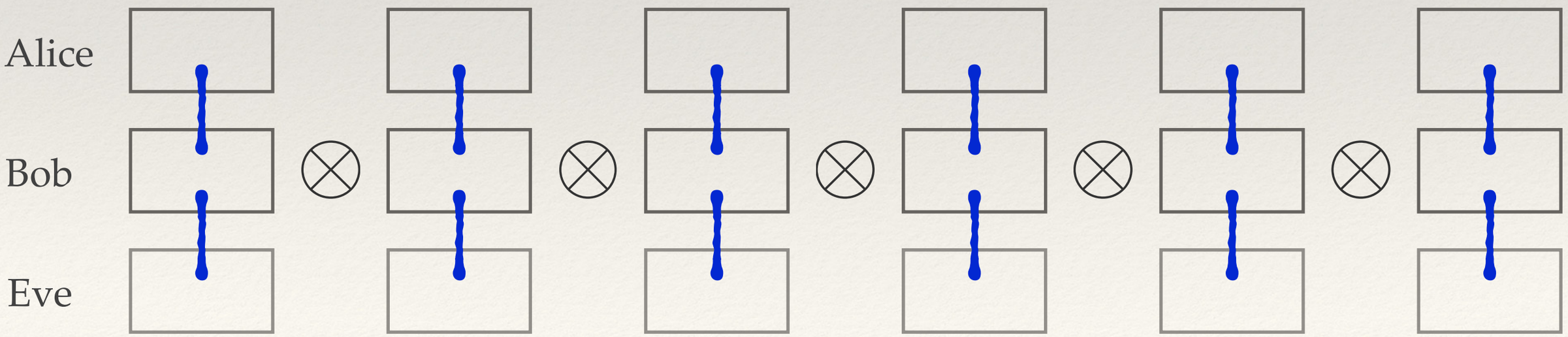
The difficulty of proving security



The IID assumption

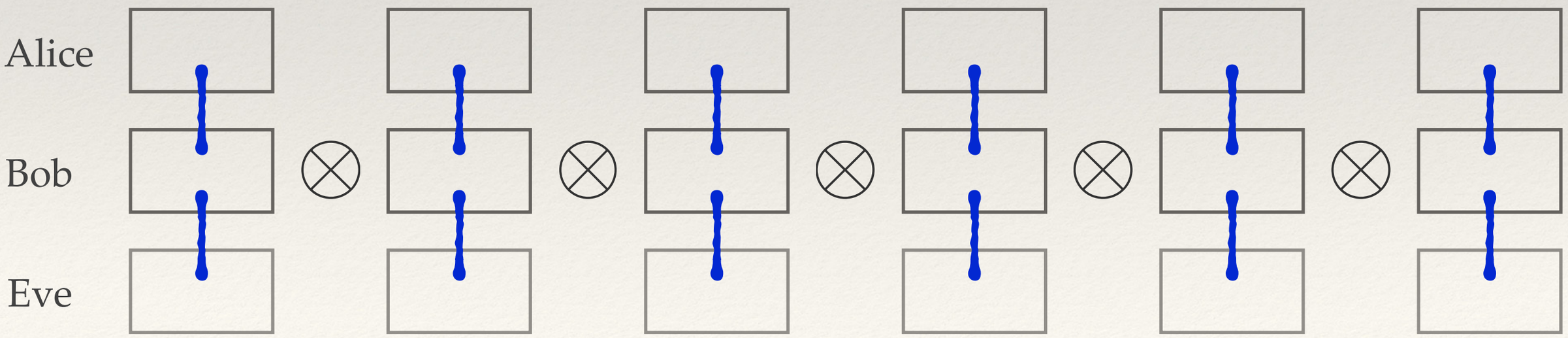
- Play the game many times in an independent and identical way
- Estimate the winning probability in one device
- The total amount of entropy is *roughly* the number of games $\times$ entropy in one game

Simple! ✔



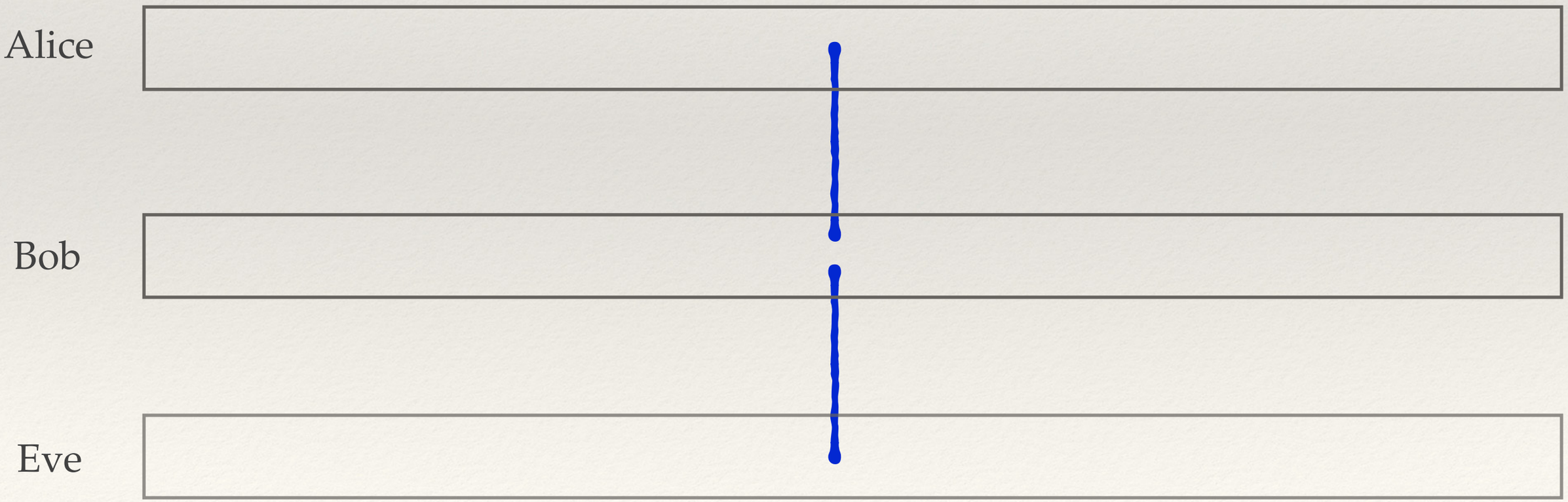
The IID assumption

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



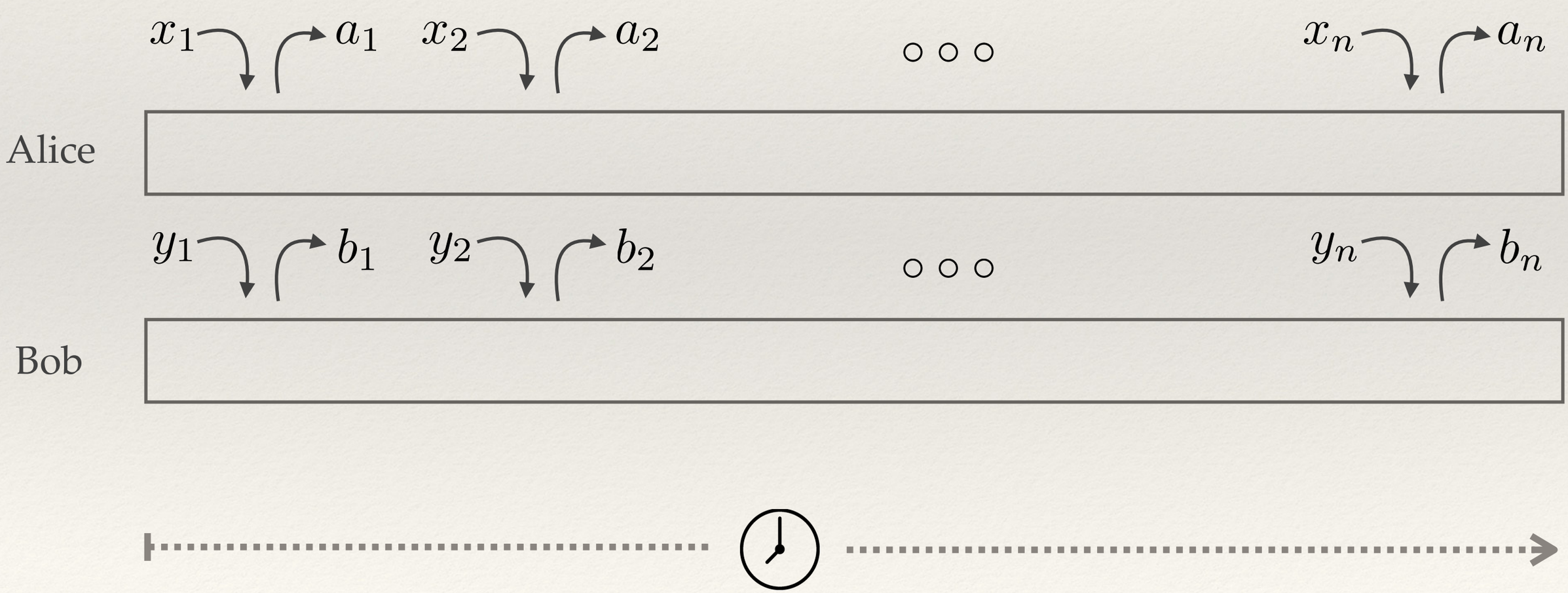
The general case

- One component to each party



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]
[Vidick and Vazirani, 14]
[Miller and Shi, 14]

Contribution and Results

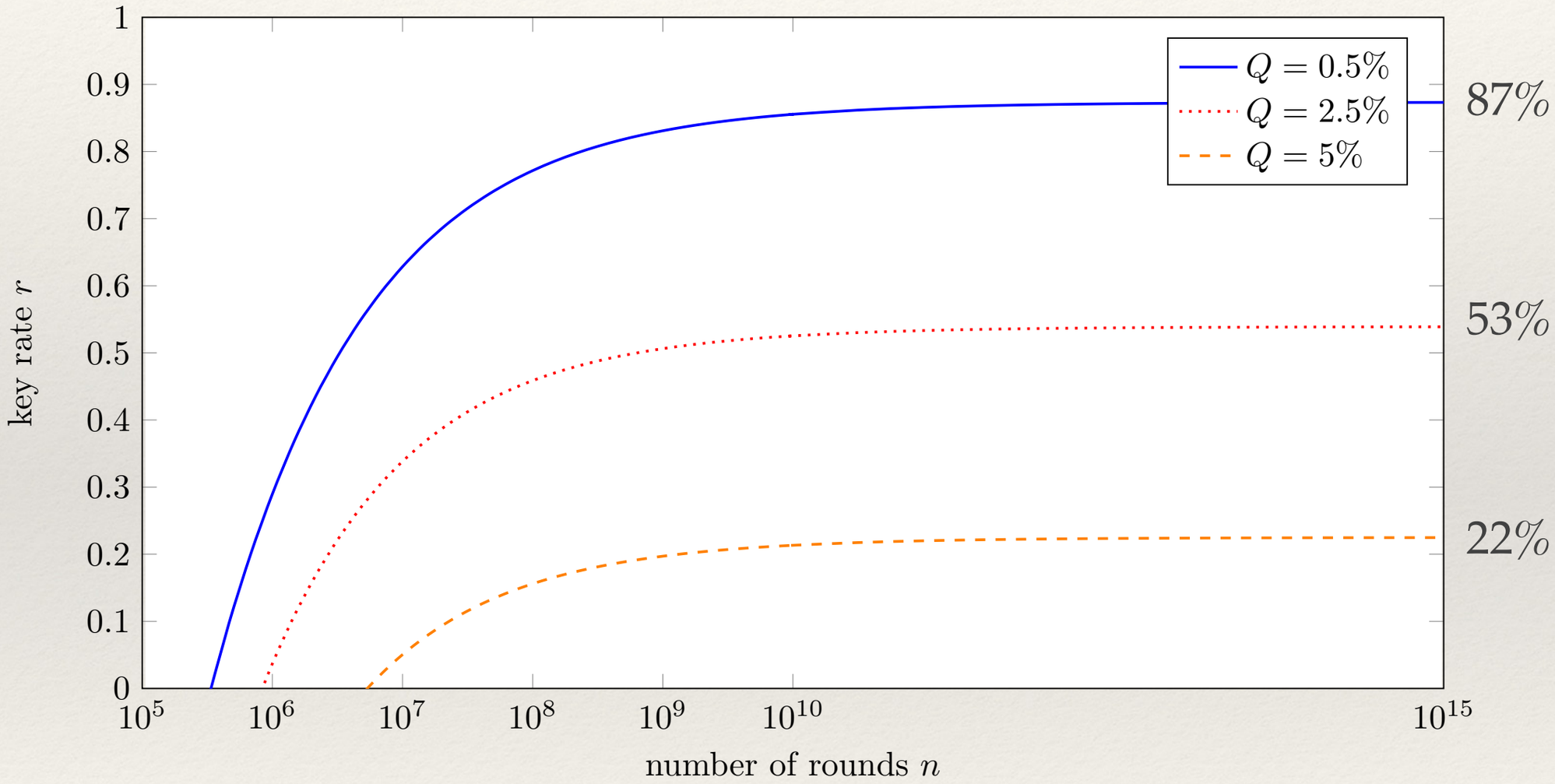
The setting

- 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")

Contribution

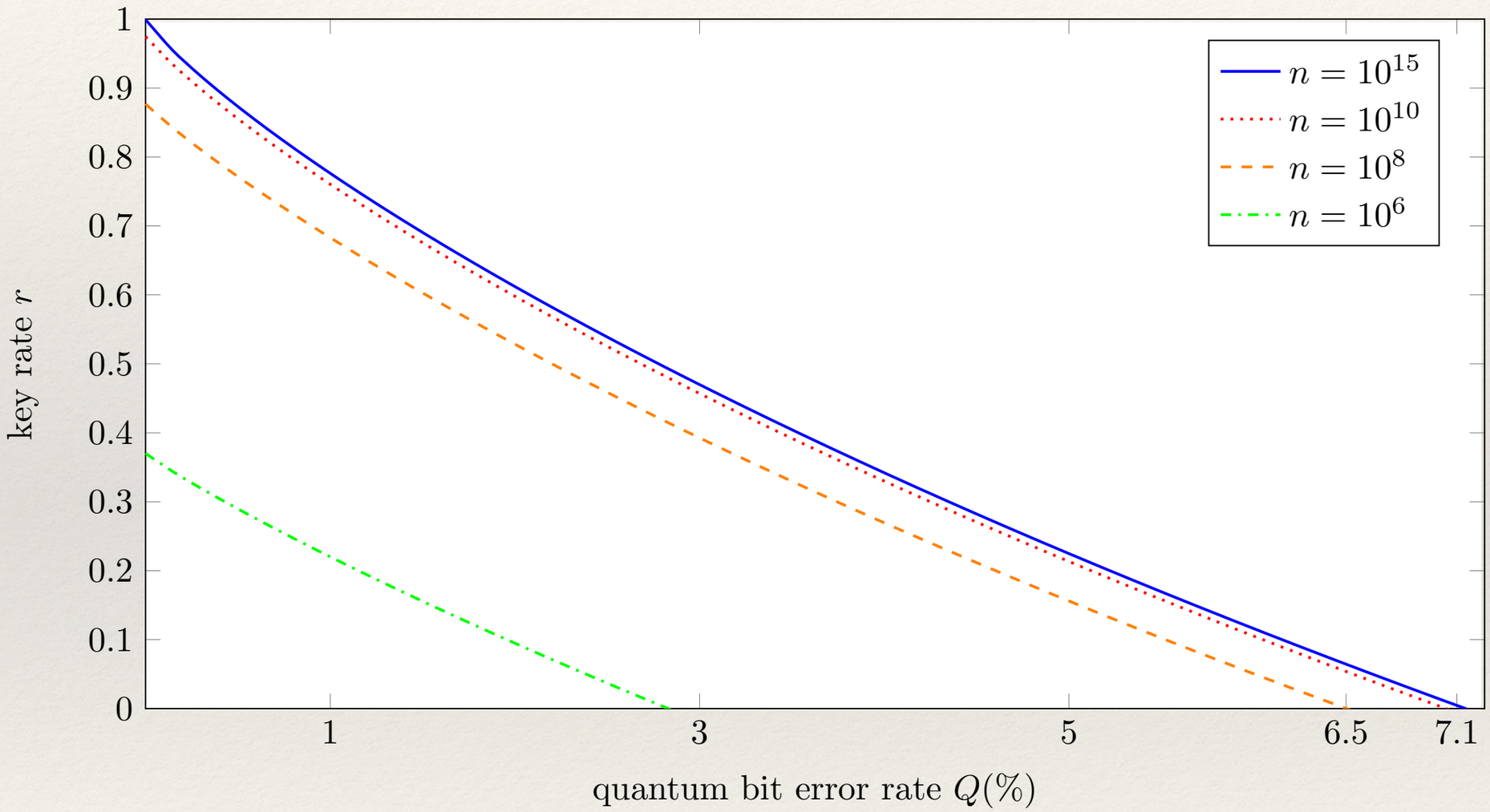
- General framework (flexible protocol + analysis) to prove security of a broad range of DI protocols
- In essence, the proof technique is a reduction to the IID case — sufficient to understand the case of just one game Simple! ✔
- This reduction is virtually lossless in terms of parameters (e.g., key rate vs. noise tradeoff) Tight! ✔

DIQKD key rates



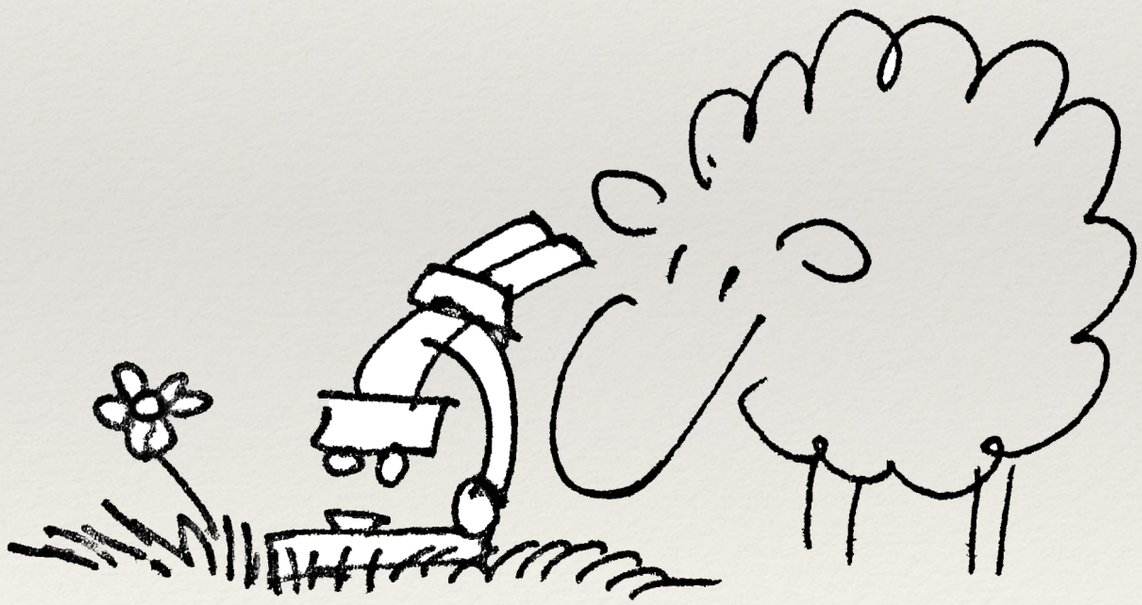
Comparable to the rates achieved in QKD [Scarani and Renner, 08] ✔

DIQKD key rates



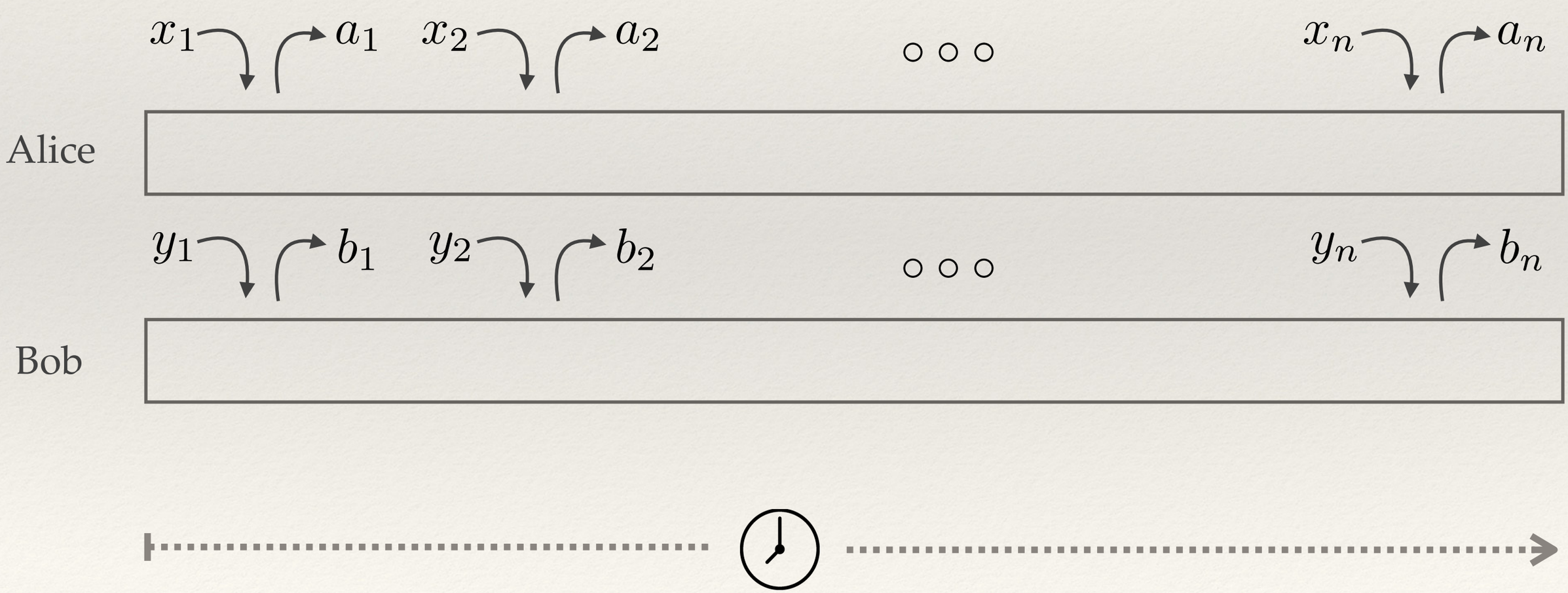
Essentially coincides with the tight bounds achieved in the IID and asymptotic case [PAB+09] for large number of rounds ✔

Proof technique



Proof technique

- Use the sequential structure of the protocol to bound the total conditional smooth min-entropy $H_{\min}^{\varepsilon}(A|E)$



Proof technique

- Use the sequential structure of the protocol to bound the total conditional smooth min-entropy $H_{\min}^{\varepsilon}(A|E)$
- This is done using a new chain rule for entropies — Entropy Accumulation [Dupuis, Fawzi, and Renner, 16]
- The total amount of entropy is *roughly* the number of rounds $\times$ entropy in one game

Simple! ✔

- The relevant one game quantity: $H(A_i|E)$ for all states with a given Bell violation
  - For CHSH a tight bound was shown in [PAB+09]

Outlook

Summary

- General framework to prove security of DI protocols
  - Simple and tight security proofs
    - Concrete examples: DIQKD and randomness expansion based on CHSH
    - (Almost) feasible with today's technology
- In essence, the best adversarial attack is the IID attack also in the DI scenario

What's next?

- Key rates are optimal only with respect to the structure of the considered protocol. Are there better protocols?
  - Different Bell inequalities?
  - Two-way classical post-processing?
- Experiment: detection efficiencies should be relatively high to get a positive key rate
- Is there a general technique to bound the conditional von Neumann entropy $H(A_i|E)$ given the Bell violation?

Thank you!

arXiv:1607.01797 | Simple and tight device-independent security proofs

References

- [BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. Physical Review Letters, 95(1):010503, 2005.
- [DFR16] Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. arXiv: 1607.01796, 2016.
- [Eke91] Artur K Ekert. Quantum cryptography based on Bell's theorem. Physical review letters, 67(6):661, 1991.
- [MS14] Carl A Miller and Yaoyun 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.
- [MY98] Dominic Mayers and Angela Yao. Quantum cryptography with imperfect apparatus. In Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on, pages 503–509. IEEE, 1998.
- [PAB+09] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. New Journal of Physics, 11(4):045021, 2009.
- [RUV13] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. Nature, 496(7446):456–460, 2013.
- [SR08] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. Physical review letters, 100(20):200501, 2008.
- [VV14] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. Physical review letters, 113(14):140501, 2014.