Device-Independent Certification of One-Shot Distillable Entanglement

NJP 2019 | arXiv:1712.09369 | Joint work with Jean-Daniel Bancal

QCrypt | August 2019 | Montreal, Canada

Rotem Arnon-Friedman | UC Berkeley

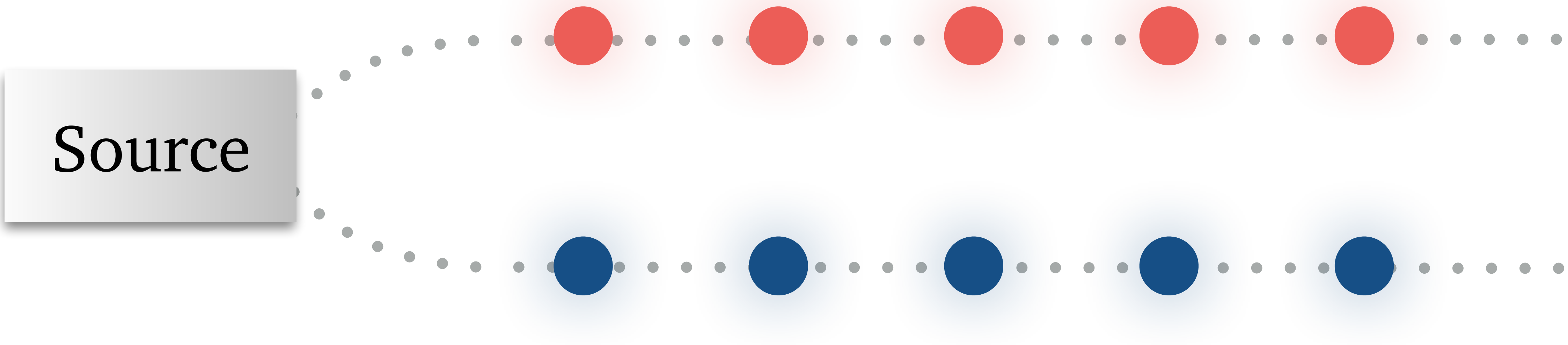
Outlook

- Motivation
- The setting
- Results
    - What is a DI entanglement certification protocol?
    - Protocol and entanglement rates
- Proof technique
- **Open questions**

Motivation

Uncharacterized Entanglement Sources

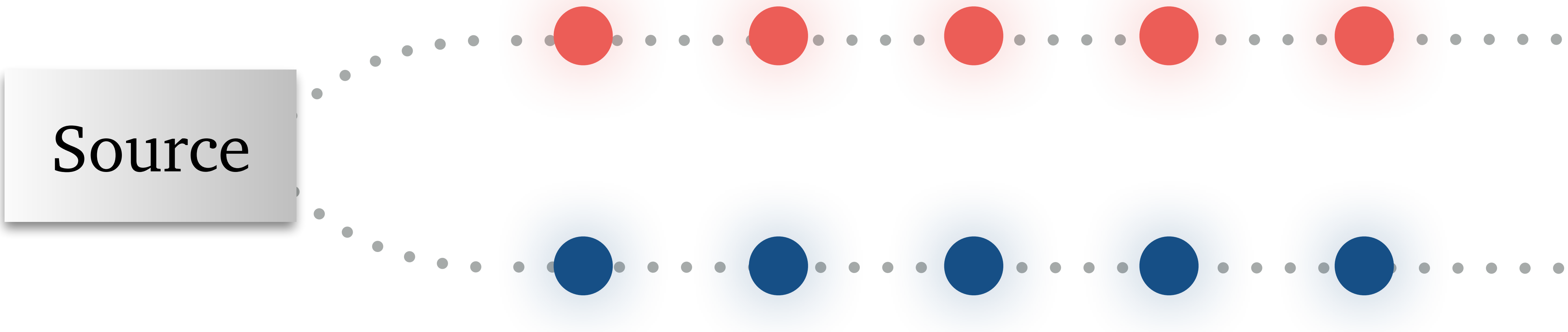
- Physical source distributing entanglement:



- Is the source good?
  - Does it create a lot of "useful entanglement"?
  - Is it better than another source?
- Uncharacterized; malicious manufacturer

Uncharacterized Entanglement Sources

- Physical source distributing entanglement:



- **Goal**: Certify that the source produces high amounts of entanglement
  - Operational certification: Entanglement left for further applications after the certification
  - Realistic completeness: Relevant for experiments

Uncharacterized Entanglement Sources

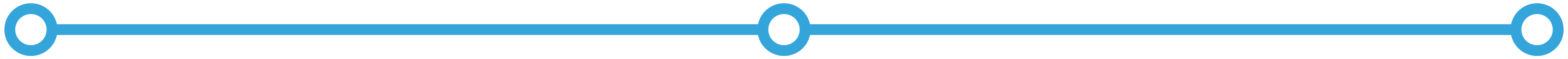
How is this related to QKD?

It’s not (directly) related!

Uncharacterized Entanglement Sources

How is this related to quantum cryptography?

- Manufacturer of the quantum devices may be malicious
- Proof technique may be useful for other cryptographic tasks
- Natural task in the device-independent framework



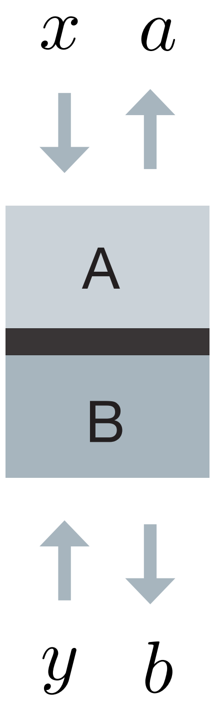
Certification of
classical randomness
DIQKD

Certification of
quantum entanglement

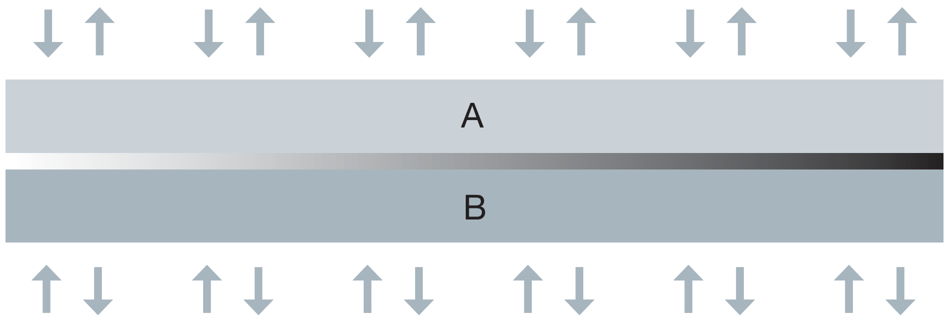
Certification of
quantum states
(self-testing)

The Setting

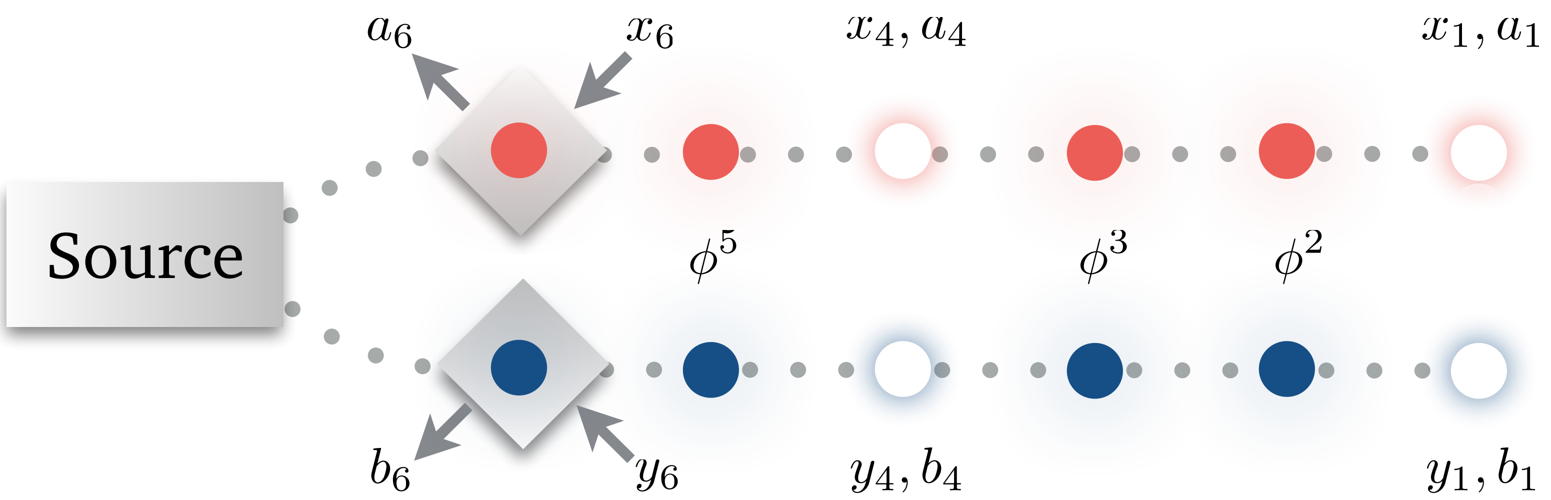
Device-Independent Certification



- Device-independent certification:
  - We don't have full information about the state and measurements
  - Limited information: the state ρ can be used to violate a given Bell inequality / win a non-local game
  - Goal: Certify a lower-bound on the state's entanglement
- Interested in **high-dimensional non-IID** states



The Model



- The model:
  - Distinction between the source and measurement devices; all the entanglement comes from the source
  - Cannot measure "past systems"
  - Structure of the Hilbert space: $\mathcal{H} = (\mathcal{H}_{Q_A} \otimes \mathcal{H}_{Q_B})^{\otimes n}$
- Necessary "assumption" to make sense of the task

Device-independent certification of one-shot distillable entanglement

Results

What Is a Device-Independent Entanglement Certification Protocol?

One-Shot Distillable Entanglement

- Interested in an operational protocol– wish to bound the entanglement left **after** the protocol

$$\rho^{\mathrm{in}} \to \rho^{\mathrm{out}} \to \rho^{\mathrm{out}}_{|\Omega}$$

Compare to QKD

One-shot distillable entanglement $E_D^{n,\varepsilon}$**:** # of EPR pairs that can be distilled, using local operations and classical communication (LOCC), from one copy of the state up to some small error

Device-Independent Certification of One-Shot Distillable Entanglement

- **Definition [informal]:** An LOCC protocol P, that transforms ϕ to ρ is called a **device-independent entanglement certification protocol** if:
  - **Soundness:** For **any** source and measurement devices, either P aborts with high probability or

    $$E_D^{n,\varepsilon}(\rho_{|\Omega}) \geq r \ .$$

  - **Completeness** (noise tolerance): P does not abort, with high probability, when the "**honest**" source and measurement devices are used.

Device-Independent Certification of One-Shot Distillable Entanglement

- **Definition [informal]:** An LOCC protocol P, that transforms ϕ to ρ is called a **device-independent entanglement certification protocol** if:
  - **Completeness** (noise tolerance): P does not abort, with high probability, when the "**honest**" source and measurement devices are used.

linear entanglement $\phi = \sigma^{\otimes n}$ $F\left(\sigma, \Phi^+\right) \geq 1 - \nu$ noise tolerance

Good, even though noisy, source!

(Protocols based on self-testing/rigidity abort on this state!)

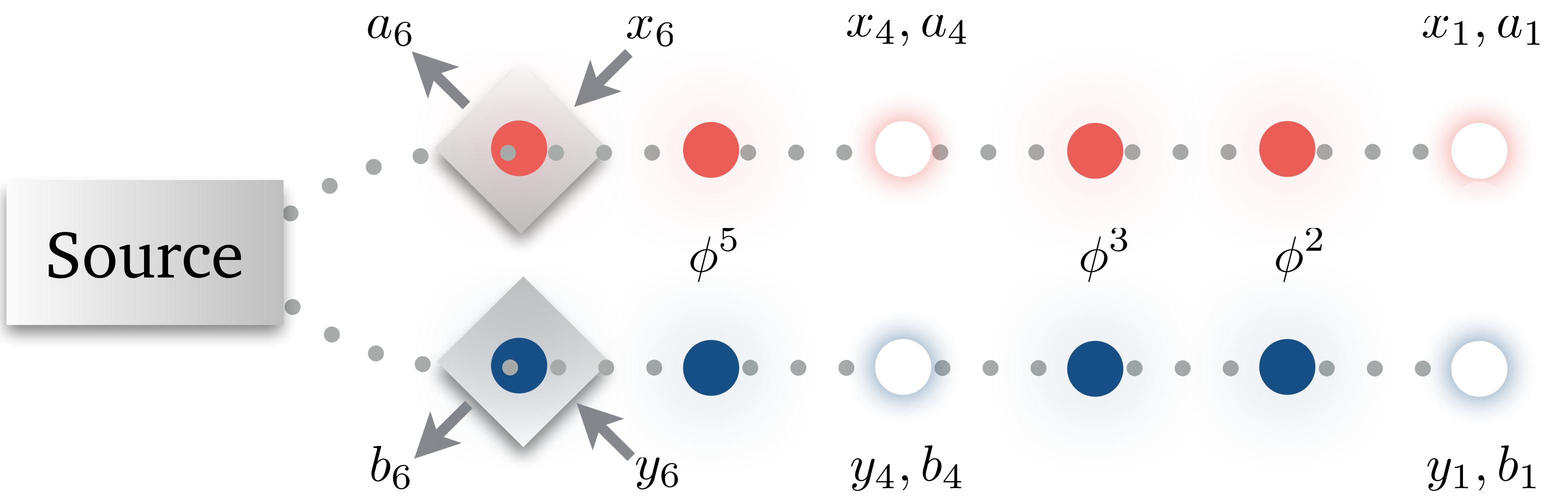
Realistic completeness

Protocol and Entanglement Rates

CHSH-Based Protocol

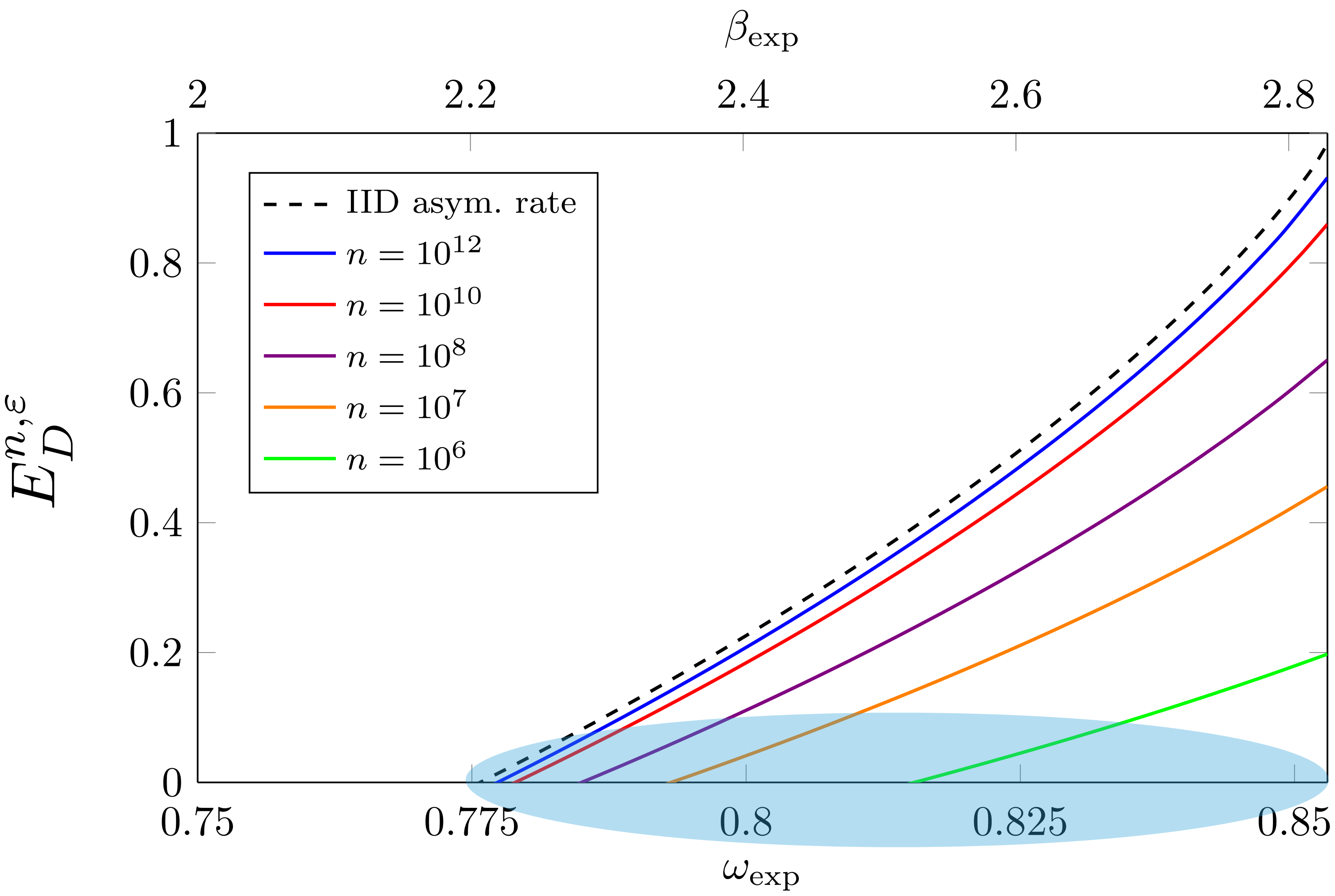
Sequential CHSH-based Protocol:

- In each round, choose randomly if this is a “test” or “entanglement” round
  - Test: play CHSH game
  - Entanglement: keep the state
- Abort if the fraction of games won is below a chosen threshold



CHSH-Based Protocol: Theorem

- **Theorem [informal]:** The CHSH Protocol is a DIEC protocol. Namely:
  - **Soundness**: For **any** source and measurement devices in the considered setting, either the protocol aborts with high probability or $E_D^{n,\varepsilon}(\rho_{|\Omega}) \geq r$
  - **Completeness** (noise tolerance): the protocol does not abort, with high probability, when the "**honest**" source and measurement devices are used



Proof Technique

Device-Independent Certification of One-Shot Distillable Entanglement [AFB19]

- Proof technique:

1. Relation to the smooth max-entropy [Wilde, Tomamichel, Berta 17]

$$E_D^{n,\varepsilon}\left(\rho_{Q_A Q_B}\right) = \sup\left\{\log(L)/n : \left(\sup_{\Lambda} F\left(\Lambda\left(\rho\right), \Phi_L^{+}\right)\right) = 1-\varepsilon\right\}$$

$\log(L) \geq -H_{\max}^{\varepsilon}(Q_A|Q_B) +$ "error term"

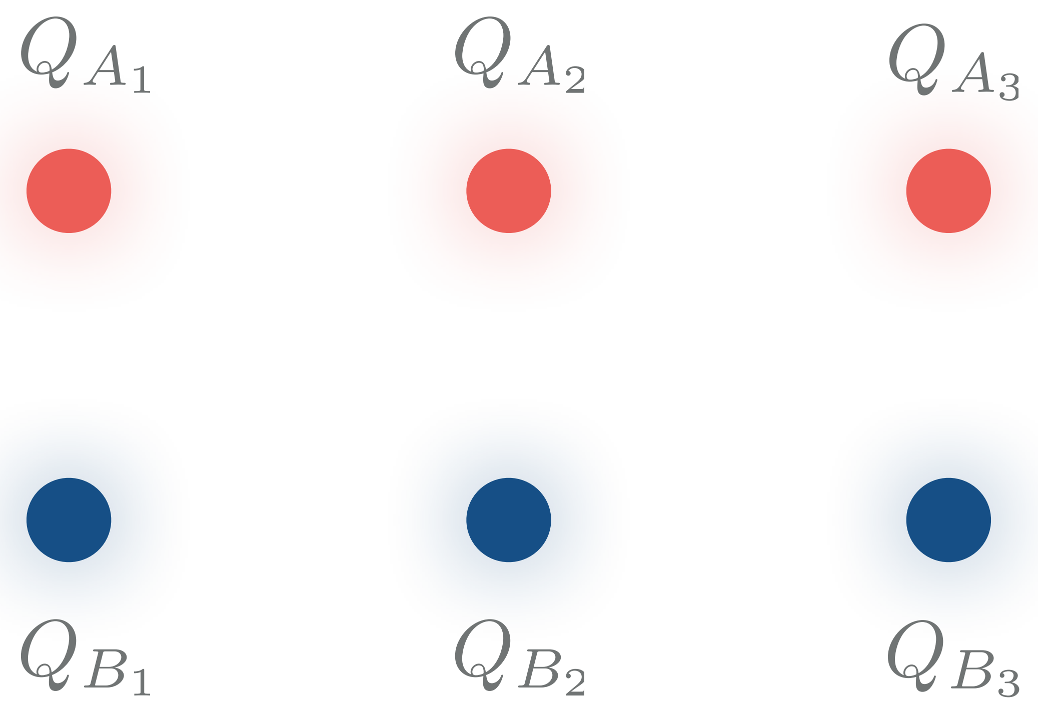
2. Entropy accumulation [Dupuis, Fawzi, Renner 16]

   - Markov-chain conditions **enforced!**
   - Max-tradeoff function

Device-Independent Certification of One-Shot Distillable Entanglement [AFB19]

- Enforcing the Markov-chain conditions:

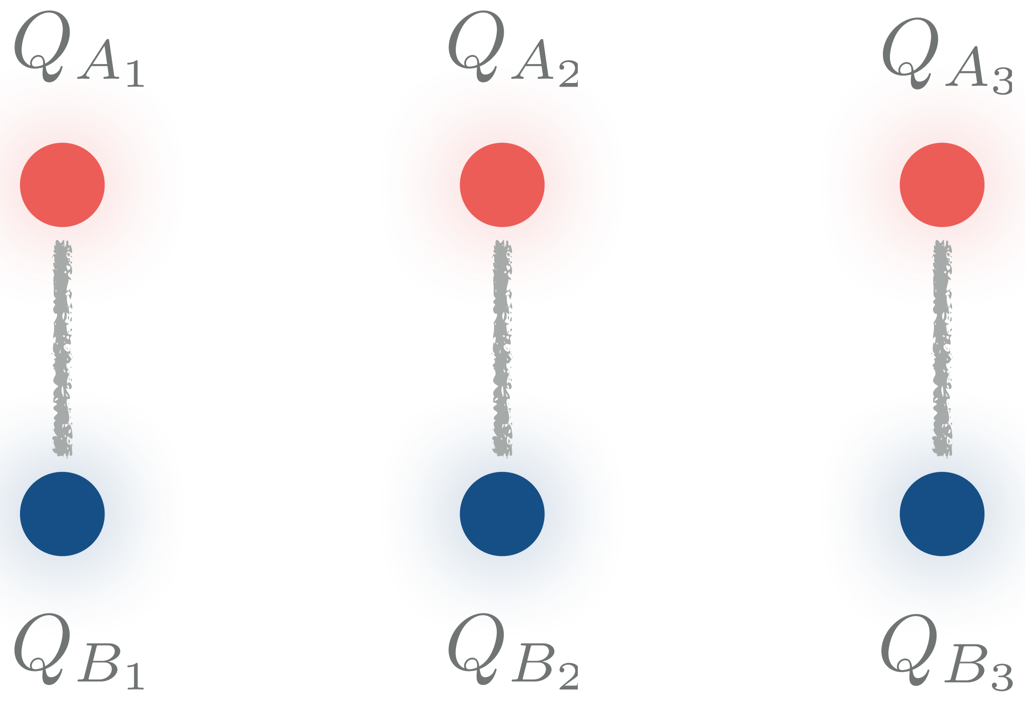
$$Q_{A_1} \leftrightarrow Q_{B_1} \leftrightarrow Q_{B_2}$$



Device-Independent Certification of One-Shot Distillable Entanglement [AFB19]

- Enforcing the Markov-chain conditions:

$$Q_{A_1} \leftrightarrow Q_{B_1} \leftrightarrow Q_{B_2}$$

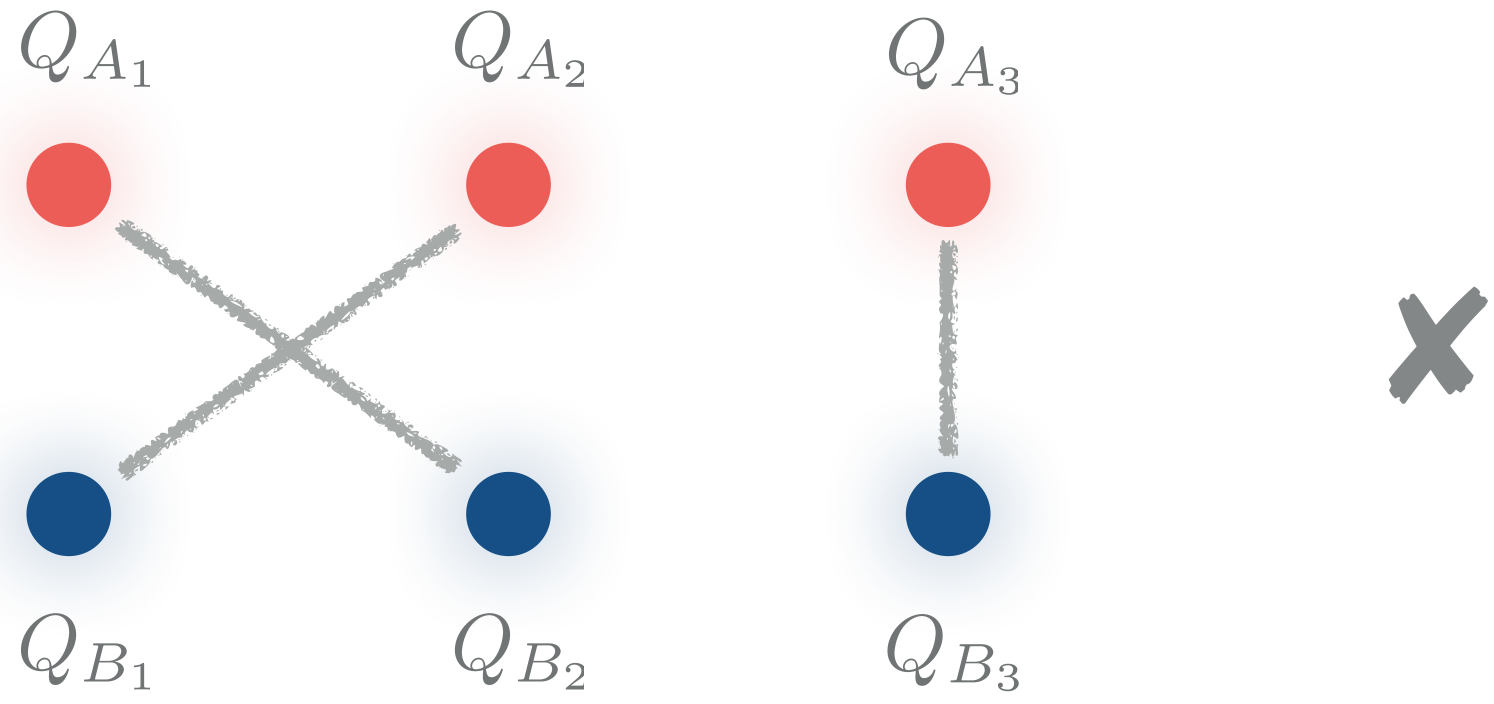


✓

Device-Independent Certification of One-Shot Distillable Entanglement [AFB19]

- Enforcing the Markov-chain conditions:

$$Q_{A_1} \leftrightarrow Q_{B_1} \leftrightarrow Q_{B_2}$$

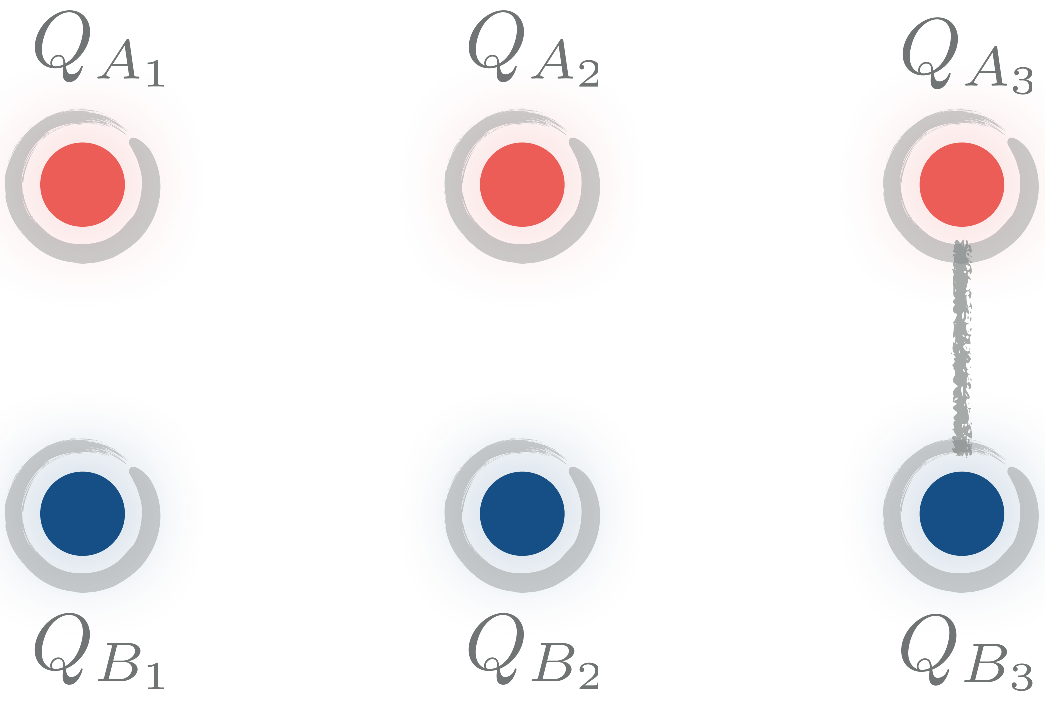


Device-Independent Certification of One-Shot Distillable Entanglement [AFB19]

- Enforcing the Markov-chain conditions:

$$Q_{A_1} \leftrightarrow Q_{B_1} \leftrightarrow Q_{B_2}$$

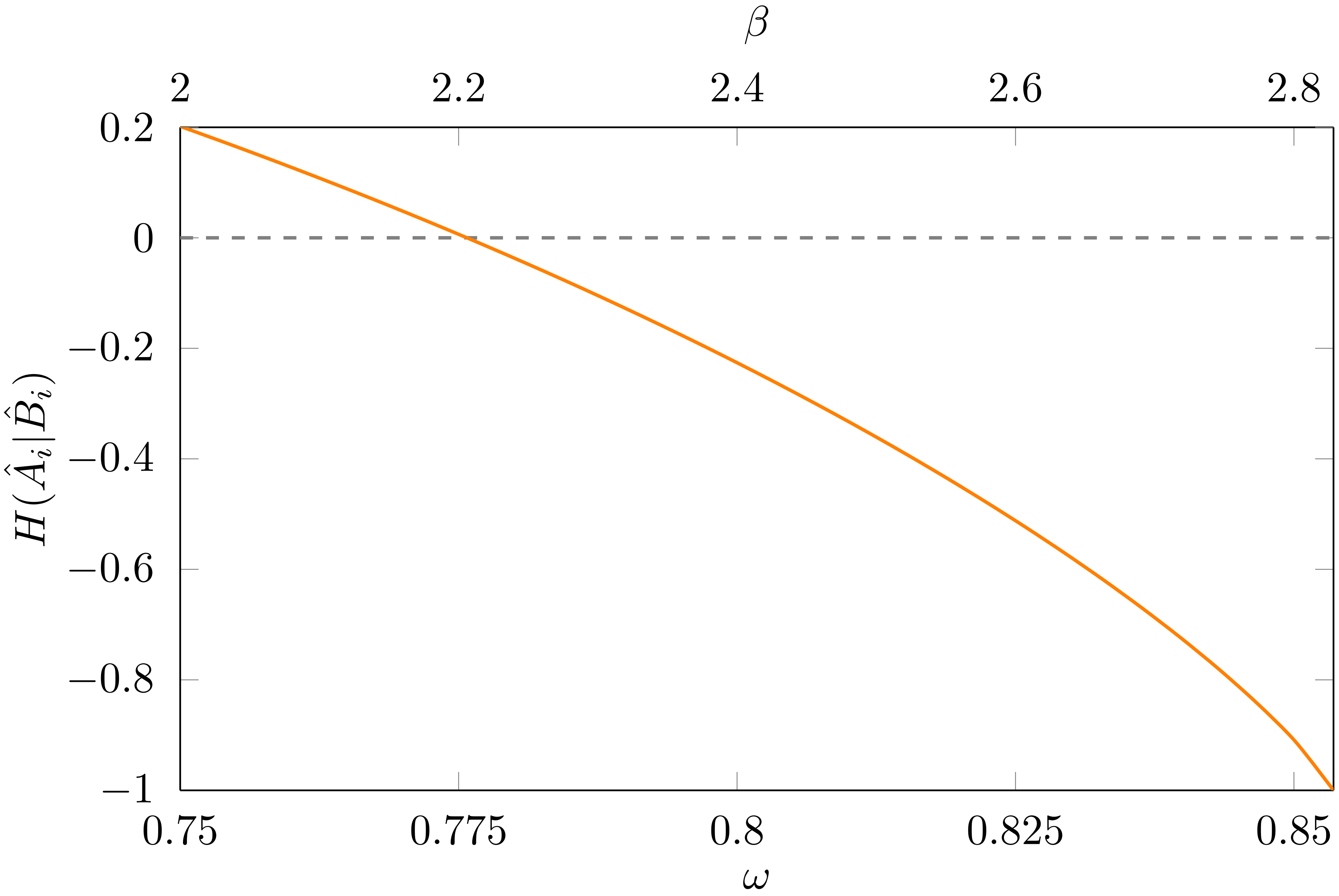
LOCC
(imaginary protocol)



✔

Device-Independent Certification of One-Shot Distillable Entanglement [AFB19]

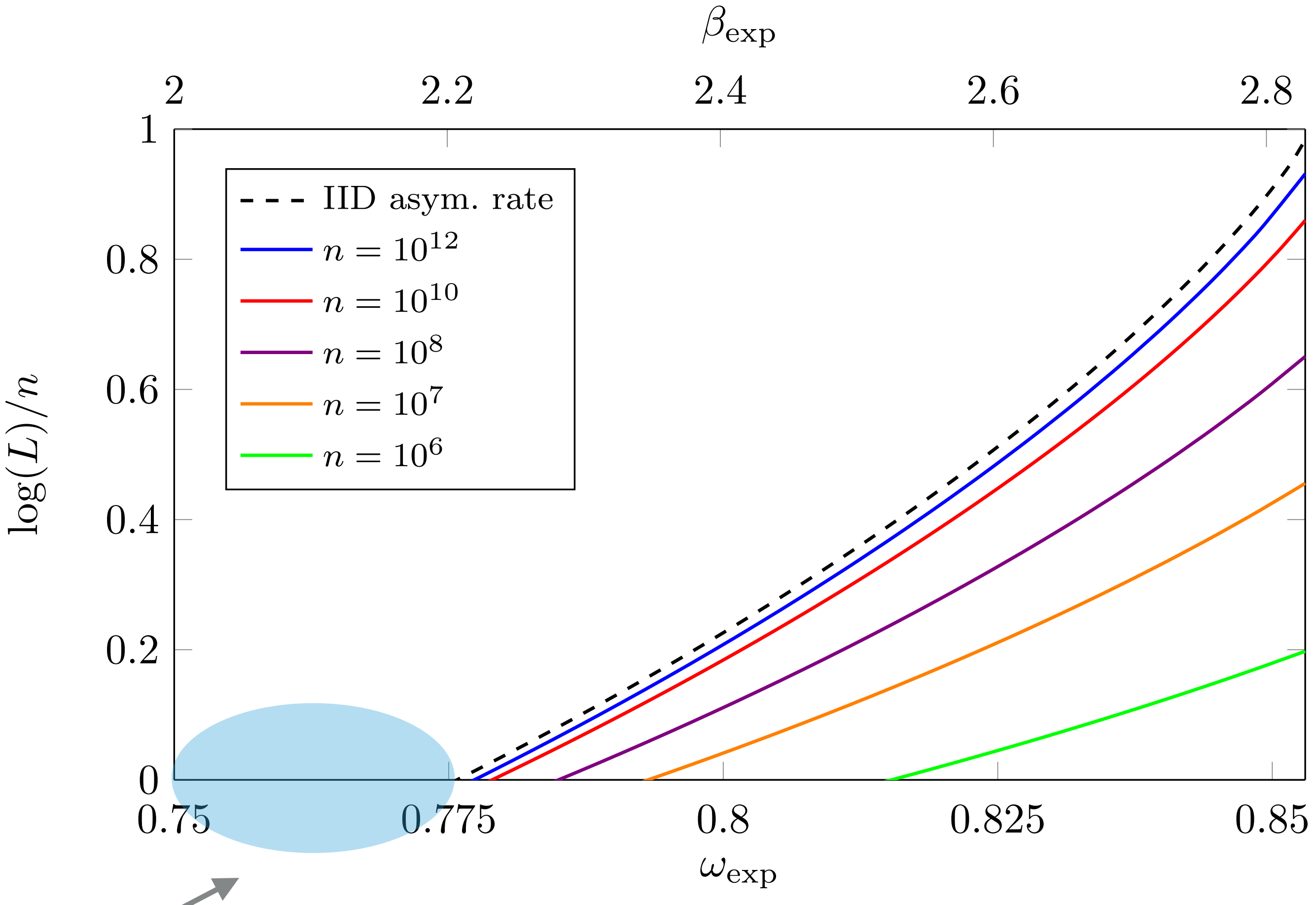
- Max-tradeoff function:



Open Questions

Open Questions

- Certify distillable entanglement from any CHSH violation



Bound entangled states?

No! [Masanes 06]

Smooth max-entropy is not the optimal description for the one-shot distillable entanglement

(we need better distillation protocols)

Open Questions

- Certify distillable entanglement from any CHSH violation
- Other non-local games and more parties
- Other entanglement measures
  - Separability preserving operations instead of LOCC, for example
- Are the Markov-chain conditions necessary?

Device-independent certification of one-shot distillable entanglement | RAF & Jean-Daniel Bancal

Thank You!

Rotem Arnon-Friedman | UC Berkeley

References

- [DFR16]: Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. arXiv preprint arXiv:1607.01796, 2016.
- [Mas06]: Lluís Masanes. Asymptotic violation of bell inequalities and distillability. Physical Review Letters, 97(5):050503, 2006.
- [WTB17]: Mark M Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. IEEE Transactions on Information Theory, 63(3):1792–1817, 2017.