Tutorial:

# Device-Independent Quantum Key Distribution

## Security Proofs and Practical Challenges

QCrypt | August 2019 | Montreal, Canada

**Rotem Arnon-Friedman** | UC Berkeley

# Outlook

- Introduction
- Protocol
- Proof techniques
- Challenges and open questions

1. What: Task

2. Why: Motivation

3. How: Intuition

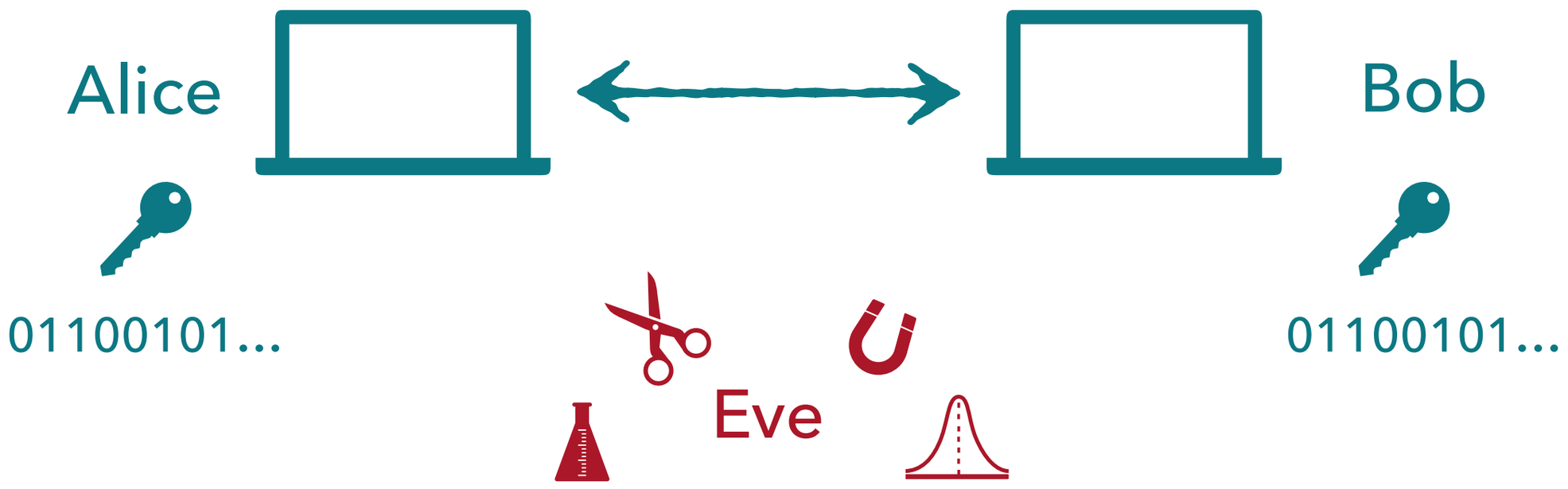
# Introduction

What?

# 1. The Task

# The Task: Key Distribution

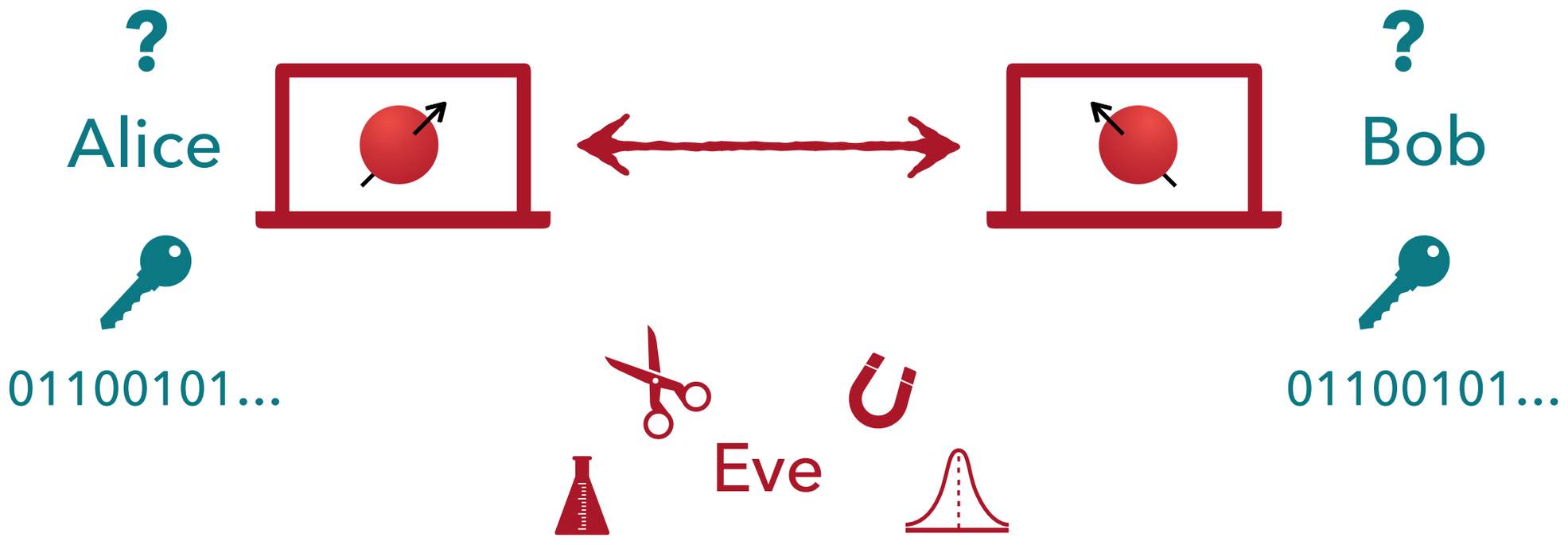
- Two honest parties: Alice and Bob
  - Alice and Bob's goal: share a private random key
- One dishonest party: Eve
  - Eve's goal: gain information about the key




(Whatever Norbert said...)

# The Task: Device-Independent Key Distribution

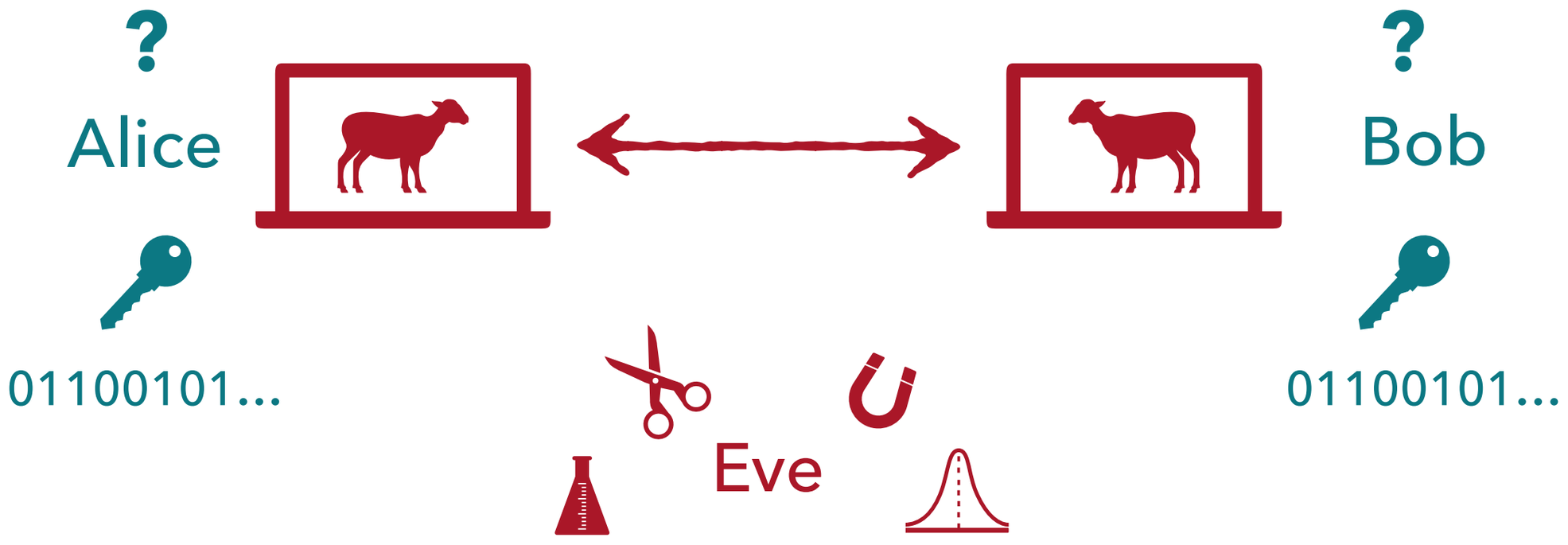
- Two honest parties: Alice and Bob
  - Alice and Bob's goal: share a private random key
- One dishonest party: Eve
  - Eve's goal: gain information about the key




(Whatever Norbert said...)

# The Task: Device-Independent Key Distribution

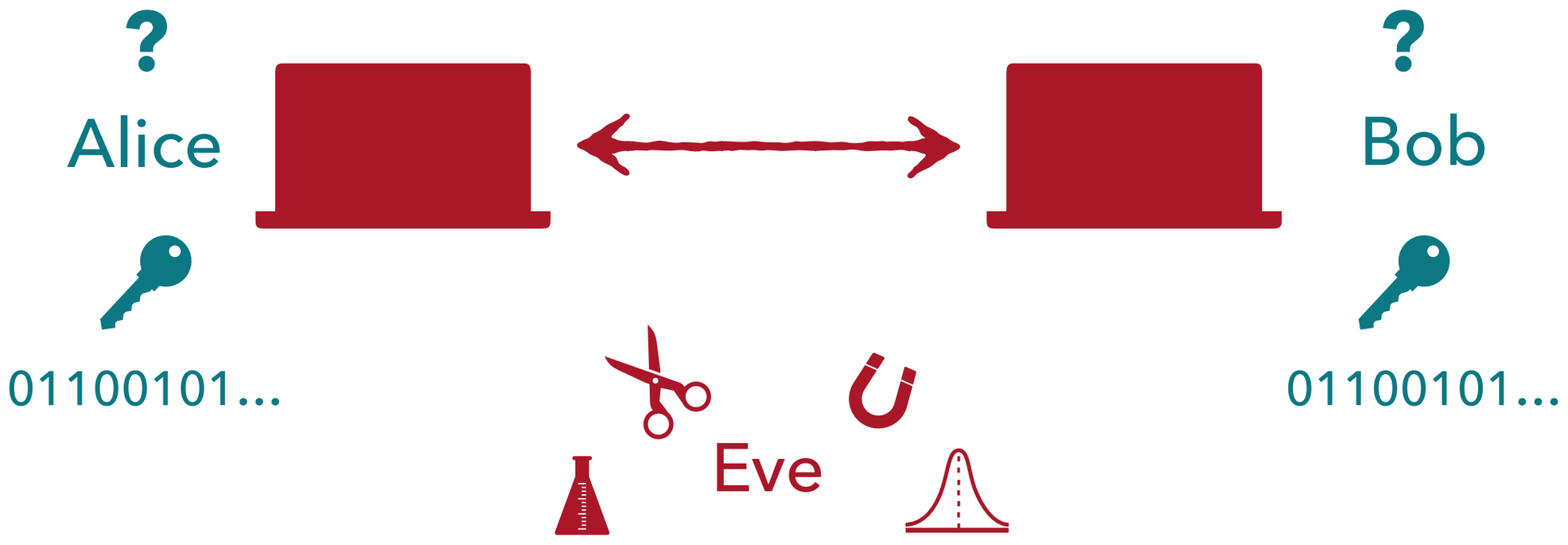
- Two honest parties: Alice and Bob
  - Alice and Bob's goal: share a private random key
- One dishonest party: Eve
  - Eve's goal: gain information about the key




(Whatever Norbert said...)

# The Task: Device-Independent Key Distribution

- Two honest parties: Alice and Bob
  - Alice and Bob's goal: share a private random key
- One dishonest party: Eve
  - Eve's goal: gain information about the key




(Whatever Norbert said...)

# 2. Motivation

# Motivation

- Device-independence = the security of the produced key is **independent** of the actual **implementation** of the physical devices

- Why?
  - Paranoid: Manufacturer may be **malicious**
  - Realistic: Physical devices are **imperfect** in ways that we cannot fully characterize (“device vs. model”)
  - Scientist: It’s interesting!
    - Fundamental aspects of quantum physics
    - Pushing cryptography to its limits
    - Motivates new models, e.g., semi-DI cryptography

How?

# 3. Intuition (As far as "quantum intuition" goes...)

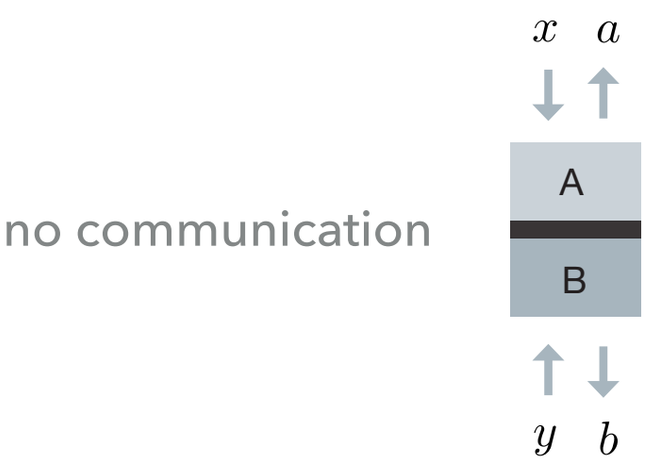
# Intuition

How can we do something useful?

# Intuition

How can we distinguish the two?

Play a non-local game!

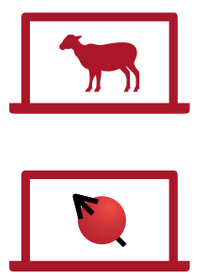



no communication

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: | $a \oplus b = x \cdot y$ | |

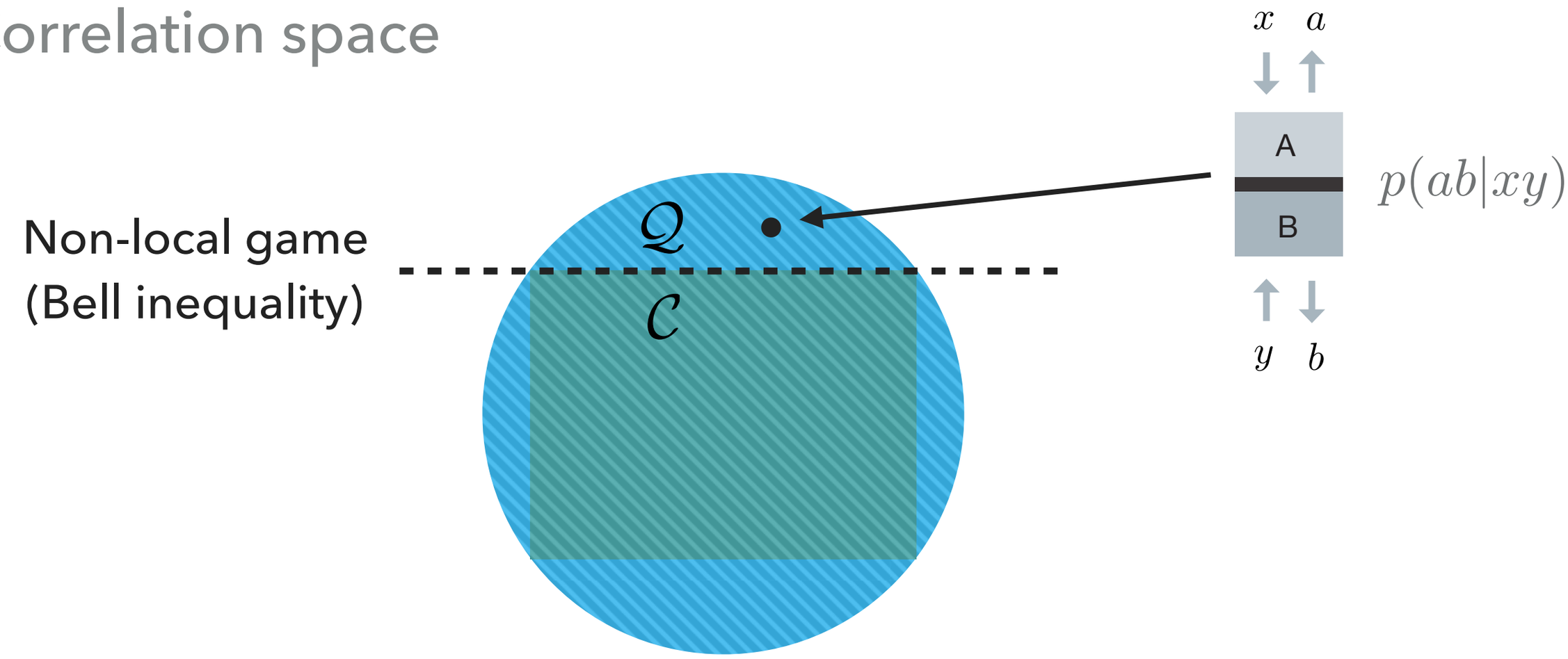
- Best classical strategy: 75% winning probability
- Best quantum strategy: ~85% winning probability



} Quantum advantage

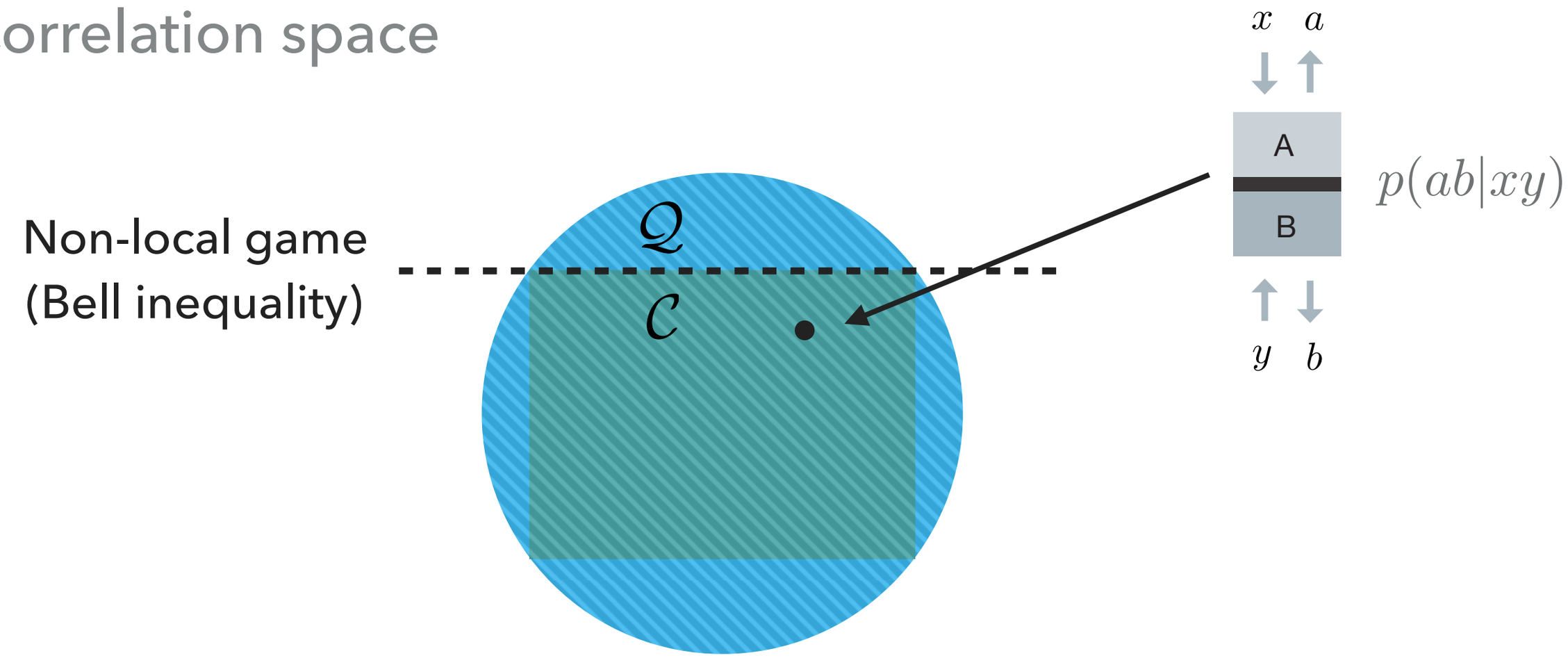
# Intuition

- Correlation space



# Intuition

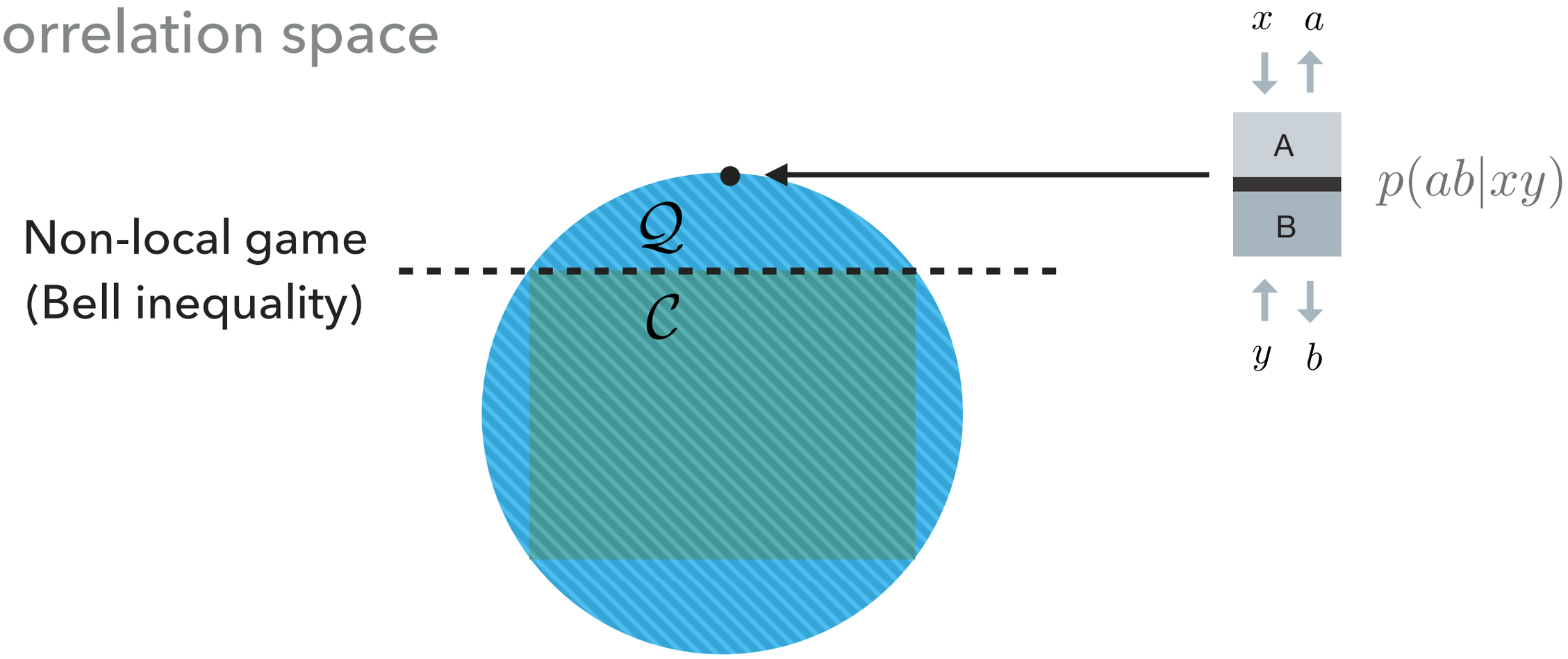
- Correlation space




- Two cases:
  - Classical strategy: $p(ab|xy) = \sum_{\lambda} p(\lambda)p(a|x\lambda)p(b|y\lambda)$

# Intuition

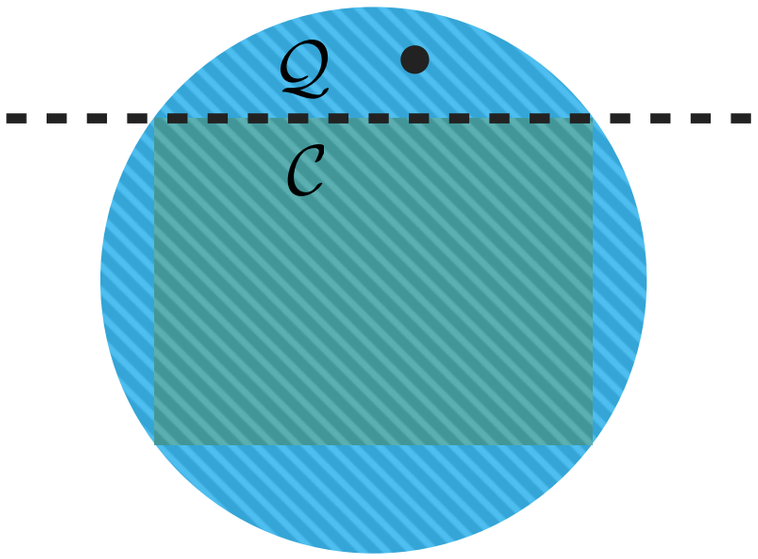
- Correlation space



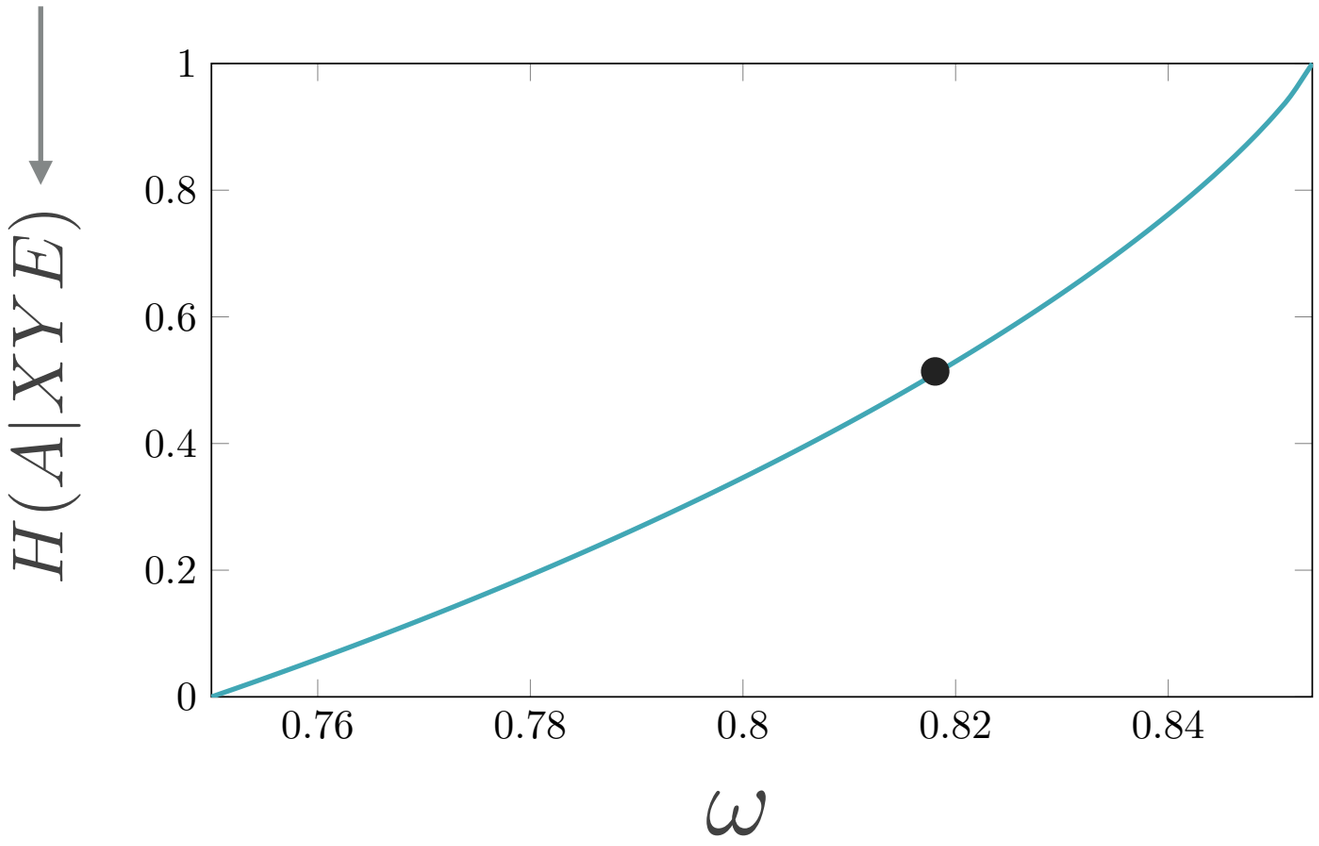

- Two cases:
  - Classical strategy: $p(ab|xy) = \sum_{\lambda} p(\lambda)p(a|x\lambda)p(b|y\lambda)$
  - Optimal CHSH quantum strategy: measuring $\Phi^{+}_{AB}$

# Intuition

- Correlation space




How random A is from Eve's point of view




- Two extreme cases:
  - Classical strategy: $p(ab|xy) = \sum_{\lambda} p(\lambda)p(a|x\lambda)p(b|y\lambda)$
  - Optimal CHSH quantum strategy: measuring $\Phi^{+}_{AB} \otimes \rho_E$

1. Assumptions

2. First step: Generating the raw data

3. Second step: Classical processing

# Protocol

# 1. Assumptions

# Assumptions

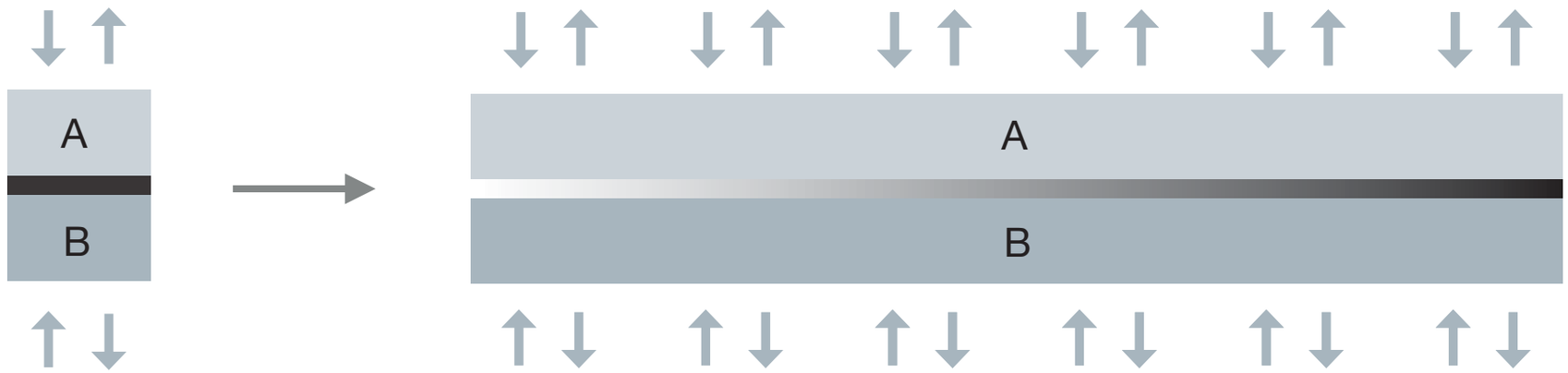
- Standard assumptions:
  - Alice and Bob's physical locations are secure (unwanted information cannot leak outside to Eve or between their devices)
  - Trusted random number generator
  - Trusted classical post-processing units
  - Authenticated, but public, classical channel
  - Quantum physics is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

First Step

# 2. Data Generation

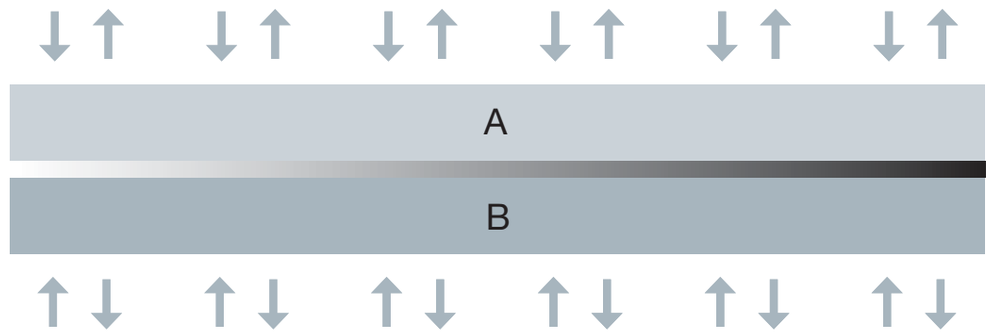
# DIQKD Protocol

- To generate a key playing one game with the device is not enough
- Many rounds of the game with one (big) device




- The generated data is used to **test** the device and to generate a key

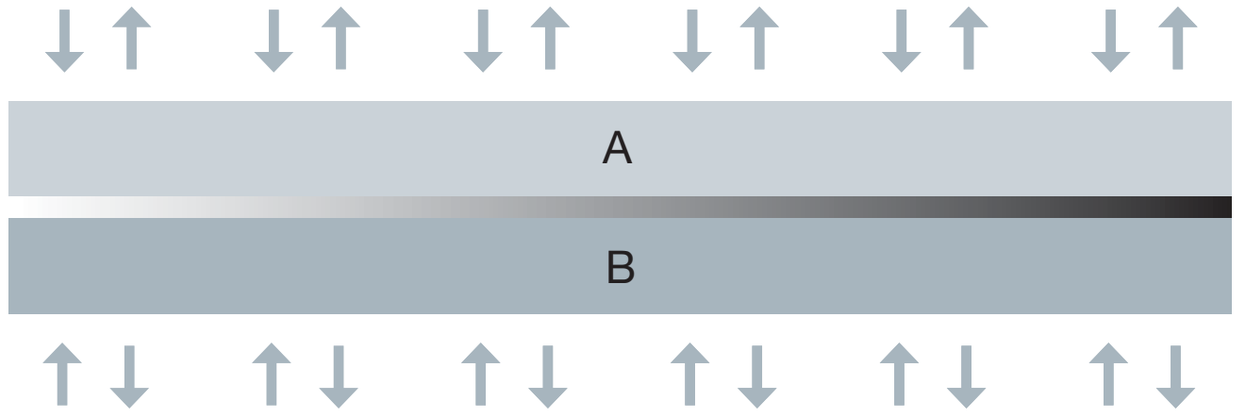
# DIQKD Protocol: Data Generation




- Step 1: Generate data by interacting classically with the physical devices
  - Randomly choose test/generation rounds
    - **Test round:**
      - Play the non-local game with the device (random inputs)
      - Recored the outputs for parameter estimation
    - **Generation round:**
      - Give the devices a pre-defined fixed input pair
      - Recored the outputs as the raw data for the key

Parallel / sequential interaction

# DIQKD Protocol: Data Generation




| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $x$: | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| $y$: | 2 | 0 | 1 | 2 | 1 | 0 | 0 | 0 | 1 | 0 | 2 | 2 | 2 | 1 | 1 | 0 | 0 | 2 | 0 | 2 | 1 | 1 | 2 | 2 | 0 | 0 |
| $a$: | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| $b$: | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |

- The crucial part: When $X = 0$, Alice's device cannot distinguish a test round from a generation round!

Second Step

# 3. Classical Processing

# DIQKD Protocol: Parameter Estimation

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| x: | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| y: | 2 | 0 | 1 | 2 | 1 | 0 | 0 | 0 | 1 | 0 | 2 | 2 | 2 | 1 | 1 | 0 | 0 | 2 | 0 | 2 | 1 | 1 | 2 | 2 | 0 | 0 |
| a: | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| b: | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✗ | ✓ | | ✓ | | ✓ | ✗ | | | ✓ | ✓ |

Parameter estimation: # of ✓ > threshold?

Yes– continue

No– abort

# DIQKD Protocol: Parameter Estimation

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| x: | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| y: | 2 | 0 | 1 | 2 | 1 | 0 | 0 | 0 | 1 | 0 | 2 | 2 | 2 | 1 | 1 | 0 | 0 | 2 | 0 | 2 | 1 | 1 | 2 | 2 | 0 | 0 |
| a: | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| b: | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| | | ✓ | ✓ | | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | | | | ✓ | ✓ | ✗ | ✓ | | ✓ | | ✓ | ✗ | | | ✓ | ✓ |

Parameter estimation: # of ✓ > threshold?

# of ✓ > threshold?

Yes– continue

No– abort

# DIQKD Protocol: Classical Processing

- Step 2: Classical post-processing
  - **Parameter estimation**: Check whether sufficiently many of the games (in the test rounds) are won
    - Yes– continue
    - No– abort
  - **Error correction**
    - Error correction protocol raises a flag– abort
    - Otherwise– continue
  - **Privacy amplification**

One-way communication

1. History

2. Security definition

3. Main task

4. Entropy accumulation in DIQKD

5. Classical post-processing

# Proof Techniques

# 1. History

# History

[Ekert, 91]
[Mayers & Yao, 98]
Main ideas

→ [Barrett, Hardy & Kent, 05]
Proof of concept

→ [Pironio *et al.*, 09]
IID + asymptotic:
tight rates & noise tolerance

↓

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

← [AF, Renner & Vidick, 16]
General security:
tight rates & noise tolerance

[Dupuis, Fawzi & Renner, 16]
[Dupuis & Fawzi, 18]
Entropy accumulation theorem

Sequential protocols

[Knill, Zhang & Bierhorst, 17]
Classical adversary

← [Knill, Zhang & Fu, 18]
General security:
tight rates & noise tolerance

Parallel

[Jain, Miller & Shi, 17]
Introduced

→ [Vidick, 17]
Simplified

The Most Important Thing

# 2. Security Definition

# Security Definition

- What does it mean to prove security?
  - If the device is sufficiently good– we would like to get a key:
    - Identical keys for Alice and Bob — Correctness
    - Unknown to Eve — Secrecy
  - If the device is not good– we would like to detect it and abort — Soundness
- There exists a sufficiently good device — **Completeness** (noise-tolerance)

# Security Definition

- **Def. [Security]:** A protocol is $\left(\varepsilon^{s}_{\mathrm{QKD}}, \varepsilon^{c}_{\mathrm{QKD}}, \ell\right)$-secure if:
  - **Soundness:** For any device $\mathrm{D}$, the protocol is $\varepsilon^{s}_{\mathrm{QKD}}$-sound, with $\varepsilon_{\mathrm{corr}} + \varepsilon_{\mathrm{sec}} = \varepsilon^{s}_{\mathrm{QKD}}$, if

    1. Correctness: $\Pr\left(K_A \neq K_B\right) \leq \varepsilon_{\mathrm{corr}}$

    2. Secrecy: $\left(1 - \Pr(\mathrm{abort})\right) \left\| \rho_{K_A E} - \rho_{U_\ell} \otimes \rho_E \right\| \leq \varepsilon_{\mathrm{sec}}$

  - **Completeness** (noise-tolerance): There exists a (noisy) device $\mathrm{D}$ such that the protocol aborts with probability at most $\varepsilon^{c}_{\mathrm{QKD}}$.

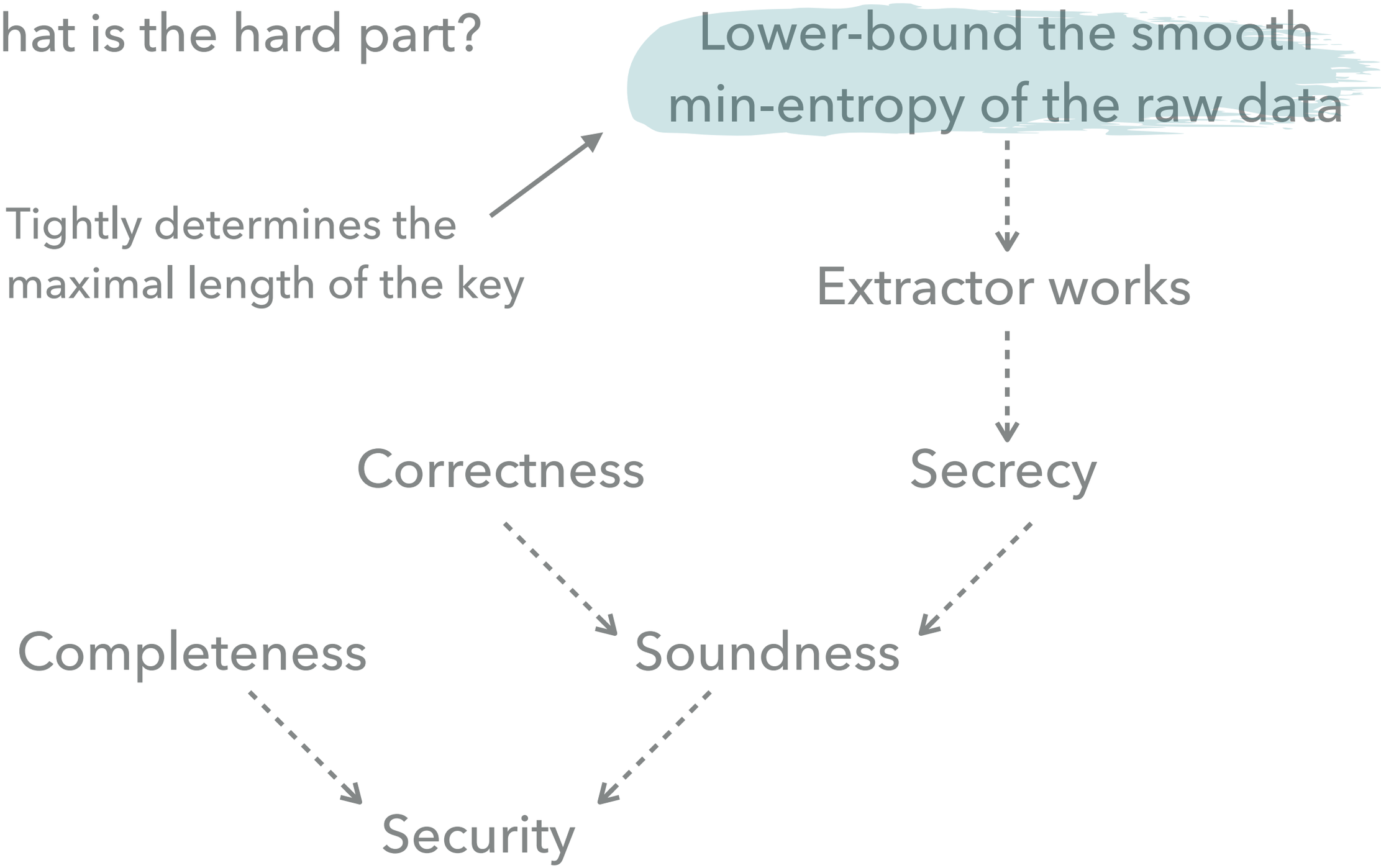
**For DIQKD: Not (fully) composable!**

- Security definitions do not fall from the sky… See Renato Renner's tutorial (QCrypt18) and Christopher Portmann's tutorial (QCrypt17).

# 3. Main Task When Proving Security

# Main Task When Proving Security

- What is the hard part?



# Main Task When Proving Security

Goal: Lower-bound the smooth min-entropy of the raw data

- Two (most recent & tight) approaches:
  - Entropy accumulation → Analytically oriented
    [AF, Dupuis, Fawzi, Renner, & Vidick, 16]
  - Probability estimators →Numerically oriented
    [Knill, Zhang, & Fu, 18]
    See talk on Thursday!

Also for other QKD models
and other protocols

Best Practices

→ RAF's PhD thesis | arXiv: 1812.10922

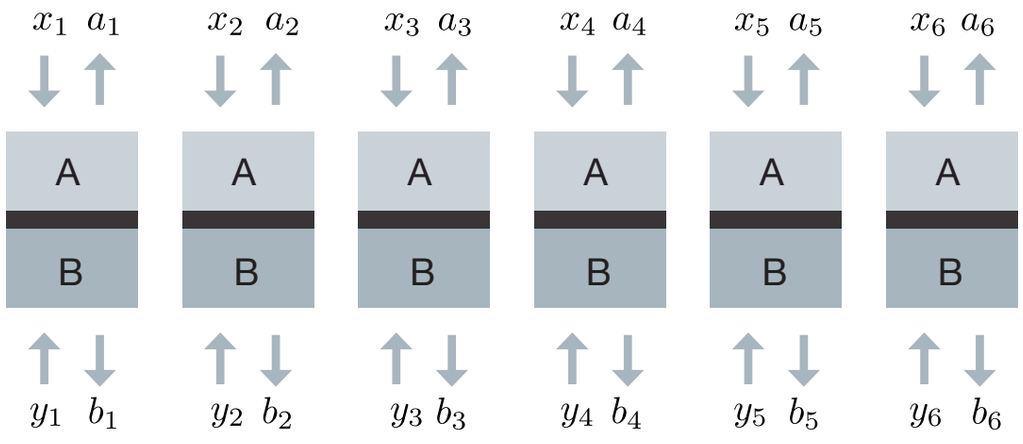
# 4. Entropy Accumulation in DIQKD

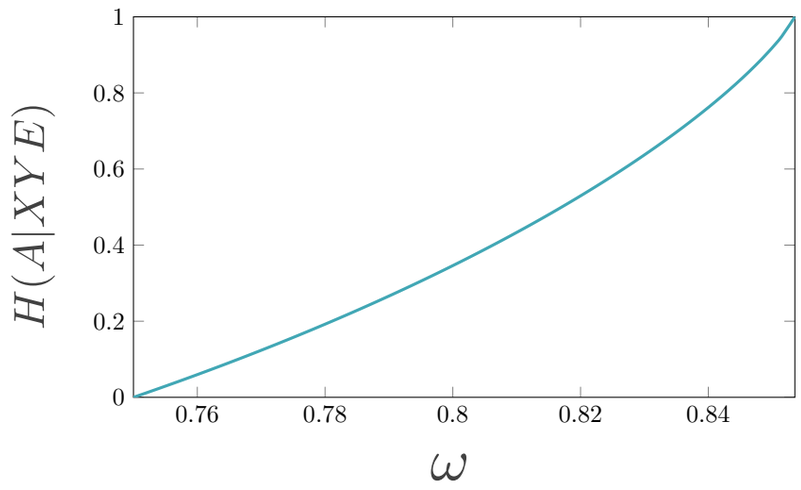
# Working Under the IID Assumption

- Security proof under the independent and identically distributed [IID] assumption (roughly):
  - Play the game many times independently and identically
  - Use the data to estimate the winning probability in a single game
  - Quantum asymptotic equipartition property [Tomamichel, Colbeck & Renner, 09]:

The total amount of entropy is roughly
the number games $\times$ entropy in one game

$$H_{\min}^{\varepsilon}(\mathbf{A}|\mathbf{XYE}) \geq nH(A|XYE) - c_{\varepsilon}\sqrt{n}$$



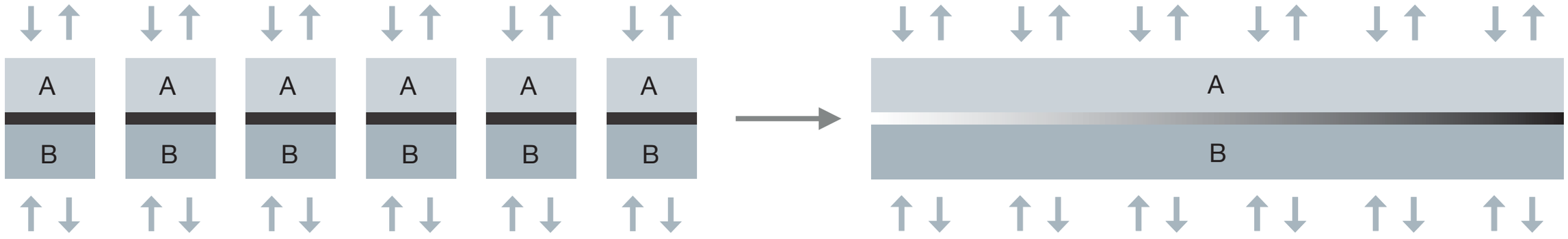



# Entropy Accumulation in DIQKD

- Moving on from the IID case: need to replace the QAEP; this is where the EAT enters [Dupuis, Fawzi, & Renner, 16]
- Goal:

$$H_{\min}^{\varepsilon}(\mathbf{A}|\mathbf{XYE}) \geq n\, t - c_{\varepsilon}\sqrt{n}$$

What is this?



# Entropy Accumulation in DIQKD

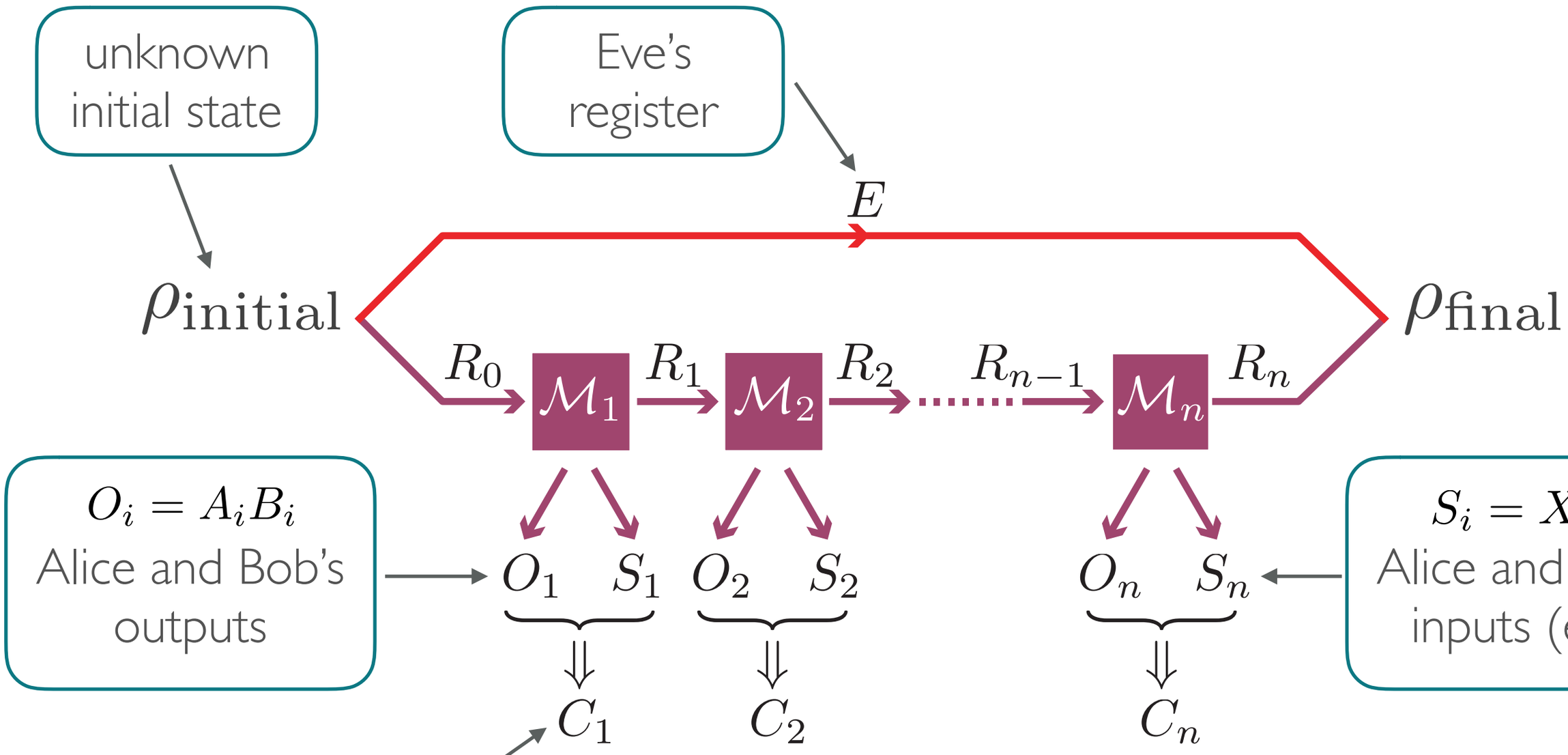
- EAT: a tool that can be used, **in some sense**, to reduce the analysis of a **sequential** device to that of an IID device

**Not a "black box reduction"!**
We cannot just analyze the IID case and be done

# Entropy Accumulation in DIQKD

- EAT: a tool that can be used, **in some sense**, to reduce the analysis of a **sequential** device to that of an IID device
- Before we can apply the EAT we need to define and construct certain objects and make sure that certain conditions hold:
  1. Sequential process: EAT channels
  2. Markov-chain conditions
  3. Min-tradeoff function
- Start by modeling the process: protocol + device

# Sequential Process: EAT Channels




**Goal:**

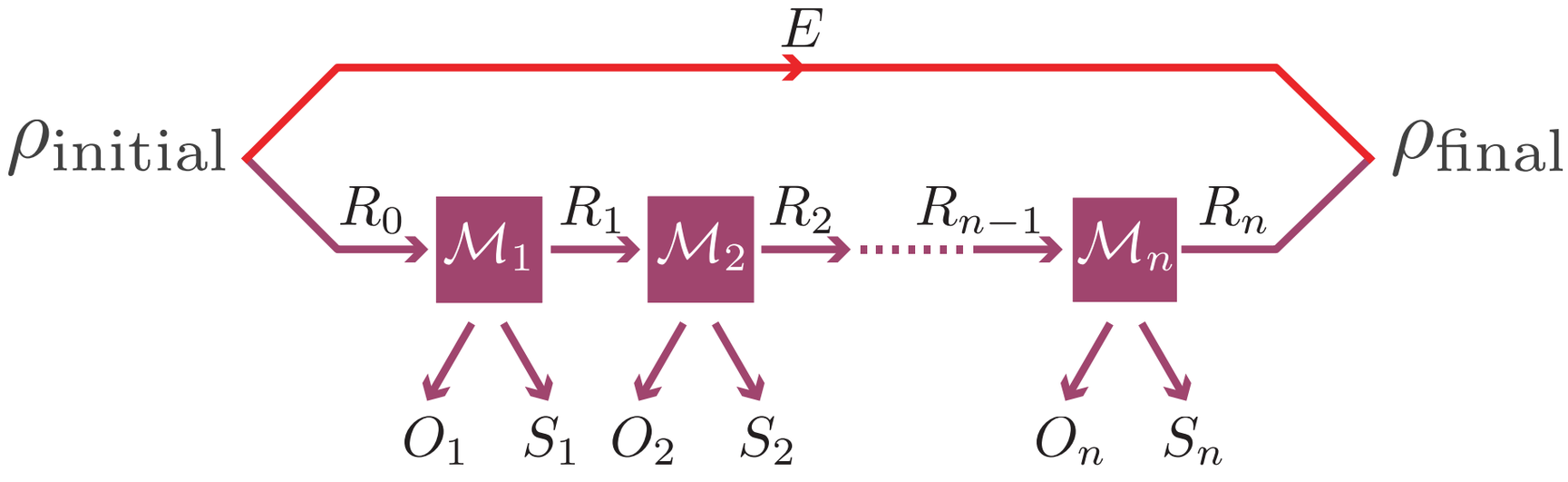
$$H_{\min}^{\varepsilon}(O|SE) = H_{\min}^{\varepsilon}(AB|XYE) = ?$$

# EAT Channels

- The EAT channels should fulfill certain conditions;
  Most important one:
  - For **any** initial state, the **final** state fulfills the Markov-chain conditions: for any $i$,

$$O_{1,\dots,i-1} \leftrightarrow S_{1,\dots,i-1} E \leftrightarrow S_i$$

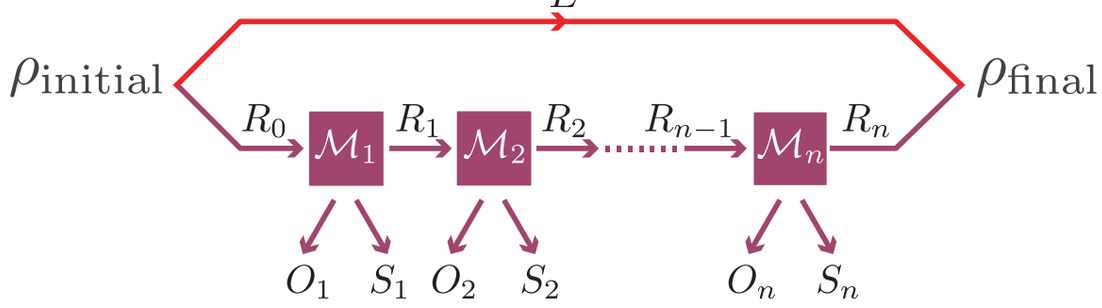
$$(AB)_{1,\dots,i-1} \leftrightarrow (XY)_{1,\dots,i-1} E \leftrightarrow (XY)_i$$



# Markov-Chain Conditions

- Markov-chain conditions make sure that entropy accumulates during the sequential process: Future steps do not reduce the entropy accumulated in the past

$$O_{1,\cdots,i-1} \leftrightarrow S_{1,\cdots,i-1}E \leftrightarrow S_i$$




- The **choice** of the sequential process may require some creativity:
  - The model affects the way we can use the EAT
  - Not trivial for all sequential processes (see later today)

# Min-Tradeoff Function

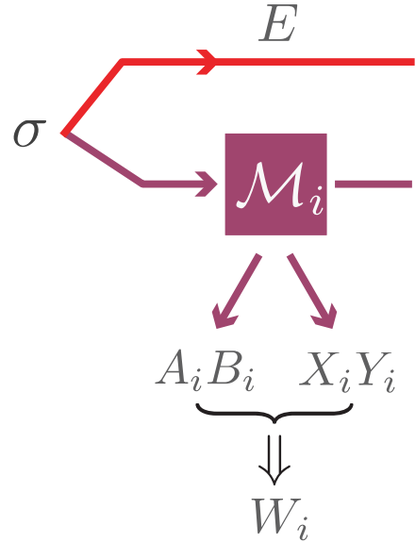
$$H_{\min}^{\varepsilon}\left(\mathbf{AB}|\mathbf{XYE}\right)_{\rho_{|\Omega}} \geq nt - \nu\sqrt{n}$$

What is this?

AEP (IID case):

$$t = H(AB|XYE)$$

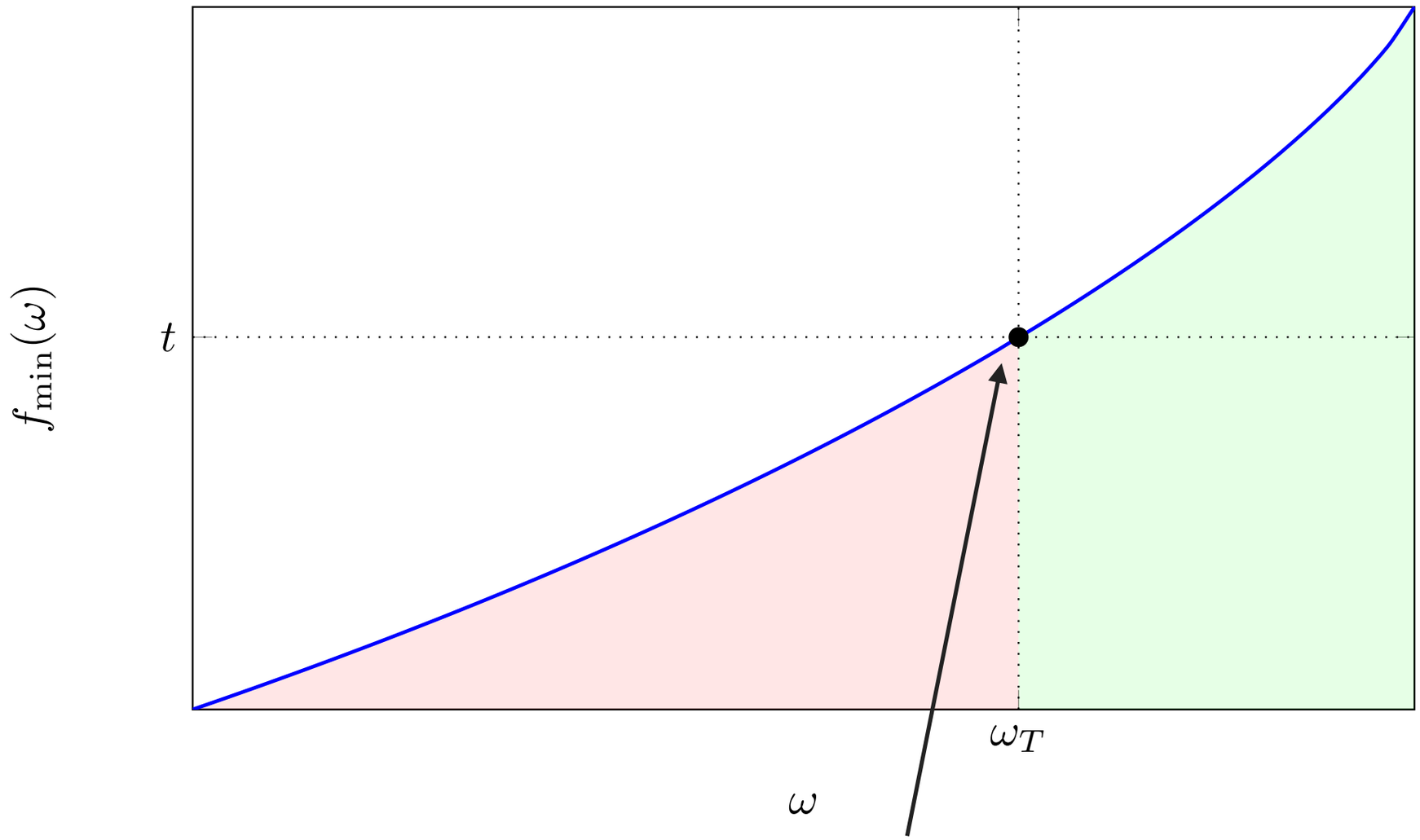
- Min-tradeoff function will allow us to get the right value of $t$
- $f_{\min}$ : The worst-case von Neumann entropy in a single round, restricted to the "correct average winning probability"




$$f_{\min}(\omega) \leq \inf_{\substack{\sigma \text{ with winning} \\ \text{prob.} \geq \omega}} H(AB|XYE)_{\mathcal{M}_i(\sigma)}$$

# Min-Tradeoff Function

$$f_{\min}(\omega) \leq \inf_{\substack{\sigma \text{ with winning} \\ \text{prob.} \geq \omega}} H(AB|XYE)_{\mathcal{M}_i(\sigma)}$$




$$H^{\varepsilon}_{\min}(\mathbf{AB}|\mathbf{XYE})_{\rho_{|\Omega}} \geq nt - \nu\sqrt{n}$$

# Entropy Accumulation

- The EAT gives us:

total smooth min-entropy

first and second order terms

$$H_{\min}^{\varepsilon}(\mathbf{AB}|\mathbf{XYE})_{\rho_{|\Omega}} \geq nt - \nu\sqrt{n}$$

final state conditioned on not aborting the protocol

the value given by the min-tradeoff function (for the observed statistics)

# 5. Classical Post-Processing

# Error Correction

- The hard part is done: we have a lower-bound on the smooth min-entropy of the raw keys


- Error correction: Alice sends classical information to Bob over a **public** authenticated channel

- Information is leaked to Eve $\Rightarrow$ we lose some of the entropy

$$H_{\min}^{\varepsilon}(\mathbf{A}|\mathbf{XYE}) \longrightarrow H_{\min}^{\varepsilon}(\mathbf{A}|\mathbf{XYE}) - \mathrm{leak}_{\mathrm{EC}}$$

- Positive entropy rate does not imply positive key rate

# Privacy Amplification

$\mathbf{a}$: 0 1 1 0 1 0 0 0 1

$\mathbf{b}$: 0 1 1 0 1 0 0 0 1

Privacy amplification →

$K_A$: 0 1 0 1 1 0

$K_B$: 0 1 0 1 1 0

- Removes the remaining correlations with Eve at the cost of reducing the key length
- Privacy amplification: Apply a **quantum-proof** randomness extractor $\mathbf{A} \xrightarrow{\text{EXT}} K_A$

$$H_{min}^{\varepsilon}(\mathbf{A}|\mathbf{XY}E) \geq \kappa \quad \Rightarrow \quad \left\|\rho_{K_A\mathbf{XY}E} - \rho_{U_\ell} \otimes \rho_{\mathbf{XY}E}\right\| \leq \varepsilon_{\text{sec}}$$

- See Amnon Ta-Shma's tutorial (QCrypt 13)

# “Closing the Loop”

$$H^{\varepsilon}_{min}(\mathbf{A}|\mathbf{XY}E) \geq \kappa$$

$$H^{\varepsilon}_{min}(\mathbf{A}|\mathbf{XY}E) \geq \kappa \;\; \Rightarrow$$

$$\left\|\rho_{K_A\mathbf{XY}SE} - \rho_{U_\ell} \otimes \rho_{\mathbf{XY}SE}\right\| \leq \varepsilon_{\text{sec}}$$

$$(1 - \Pr(\text{abort}))\left\|\rho_{K_AE} - \rho_{U_\ell} \otimes \rho_E\right\| \leq \varepsilon_{\text{sec}}$$

Lower-bound the smooth min-entropy of the raw data

Extractor works

Secrecy

Correctness

Soundness

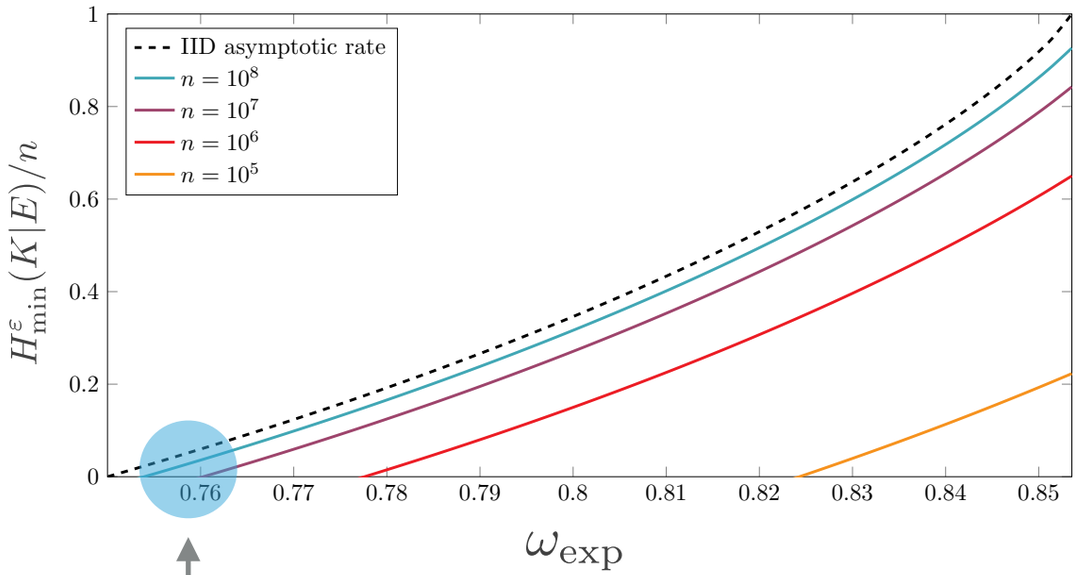
Completeness

Security

# Challenges

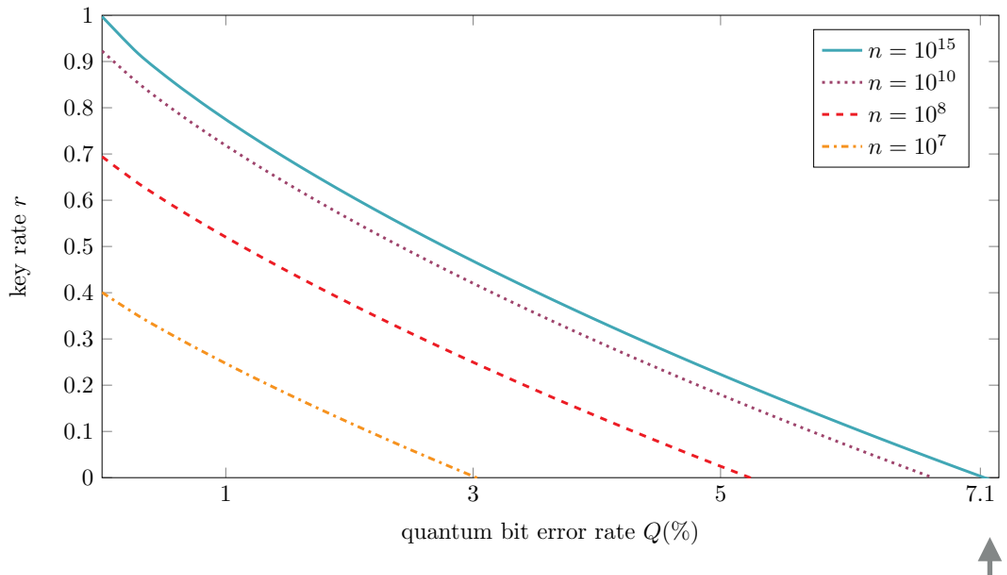
# Theory–Experiment Gap

## Entropy rate




current experiments

## DIQKD key rate

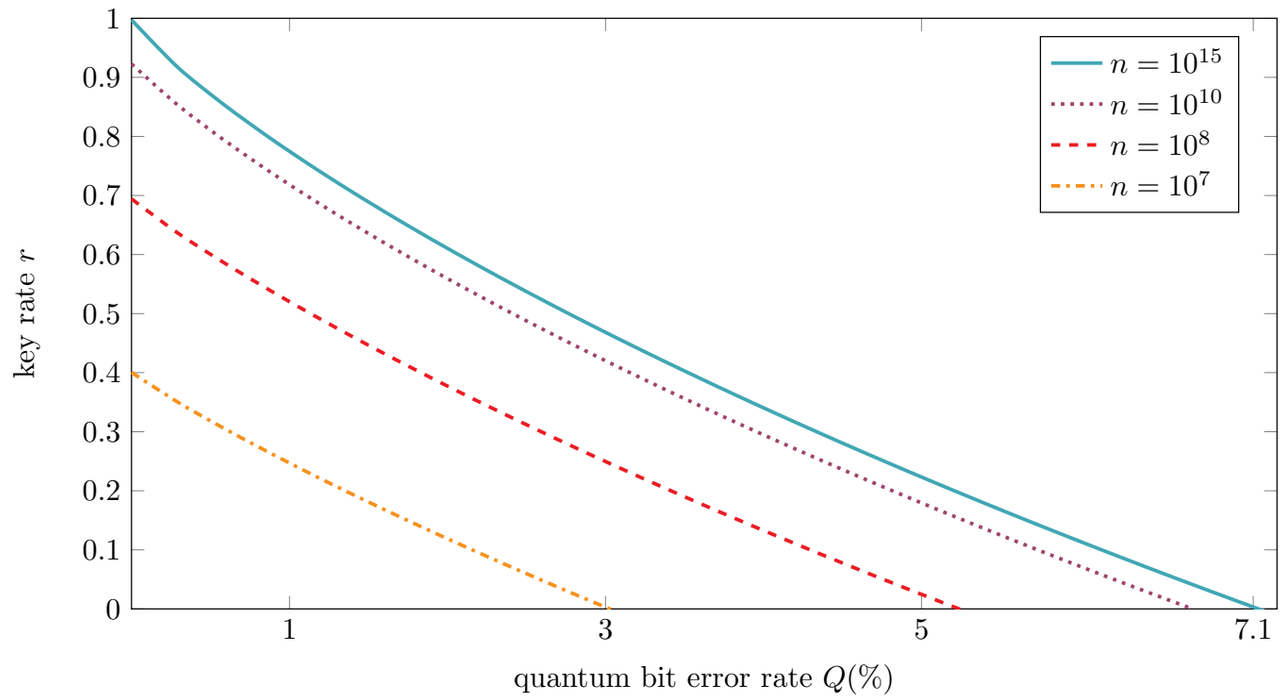



$\omega_{\exp} \approx 0.8$

- Still far from experimental abilities
- “Standard” DIQKD protocol key rates are asymptotically tight

# Theory–Experiment Gap

- How can we bridge the gap?
  - Better experiments :)
  - Better theory? What can we try to improve?



# The Quest for Better DIQKD Protocols

1. **Classical post-processing**: optimality of the rate is known only for protocols based on one-way communication post-processing.
    - Main challenge: Look for two-way advantage distillation protocols and prove their security

2. **Non-local game**: Is there a non-local game that can certify more key rate compared to the CHSH game?
    - Main challenge: Constructing a good min-tradeoff function (bound $H$, not $H_{\min}$)
        - Can numerical techniques help with that?

Stay for the next session!

# The Quest for Better DIQKD Protocols

3. Analysis of no-click event

- In photonics experiments, the Bell violation is low due to the effect of non-click events
- Cannot just drop them– that would open a “loophole”
- Can we take no-click events into account in a security proof in a more refined way?
  - E.g., modify the protocol to “announce” no-click events and incorporate this information to the min-tradeoff function

# The Quest for Better DIQKD Protocols

Maybe there are not (much) better protocols? :(

4. Look for **upper bounds** on DIQKD key rates

   - Main challenge: Argument should hold for any possible protocol (or family of protocols)
   - See the next talk by Eneet Kaur for a step in that direction

5. Consider **semi**-DIQKD protocols instead

   - Which model is relevant? Talk yesterday & on Thursday!
   - Perform tight non-asymptotic analysis: Can we really do better in the relevant regime of parameters?

# Device-Independent Quantum Key Distribution: Security Proofs and Challenges

# Thank You!

QCrypt | August 2019 | Montreal, Canada

**Rotem Arnon-Friedman** | UC Berkeley

# References


- [AFDF+18] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick. Practical device-independent quantum cryptography via entropy accumulation. Nature communications 9, no. 1: 459, 2018.
- [AFRV16] R. Arnon-Friedman, R. Renner, and T. Vidick. Simple and tight device-independent security proofs. *SIAM Journal on Computing* 48.1: 181-225, 2019.
- [BHK05] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. Physical Review Letters, 95(1):010503, 2005.
- [DF18] F. Dupuis, and O. Fawzi. Entropy accumulation with improved second-order term. IEEE Transactions on Information Theory, 2019.
- [DFR16] F. Dupuis, O. Fawzi, and R. Renner. Entropy accumulation. *arXiv preprint arXiv:1607.01796,* 2016.
- [Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. Physical review letters, 67(6):661, 1991.
- [JMS17] R. Jain, C. A. Miller, and Y. Shi. Parallel device-independent quantum key distribution. *arXiv:1703.05426,* 2017.
- [KZB17] E. Knill, Y. Zhang, and P. Bierhorst. Quantum randomness generation by probability estimation with classical side information. *arXiv: 1709.06159,* 2017.
- [KZF18] E. Knill, Y. Zhang, and H. Fu. Quantum probability estimation for randomness with quantum side information. *arXiv:1806.04553,* 2018.
- [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.
- [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.
- [TCR09] M. Tomamichel, R. Colbeck, and R. Renner. A fully quantum asymptotic equipartition property. IEEE Trans. Inform. Theory, 55:5840-5847, 2009.
- [Vid17] T. Vidick. Parallel DIQKD from parallel repetition. *arXiv:1703.08508,* 2017.
- [VV14] U. Vazirani and T. Vidick. Fully device-independent quantum key distribution. Physical review letters, 113(14):140501, 2014.