

Quantum adversaries via operator space theory

Mario Berta (IQIM Caltech), Omar Fawzi (ENS Lyon), Volkher Scholz (ETH Zurich) - partly based on arXiv:1409.3563

Outline

- Motivation
- Randomness extraction against quantum adversaries
- Results - mathematical framework based on operator space theory
- Summary and outlook

Outline

- Motivation
- Randomness extraction against quantum adversaries
- Results - mathematical framework based on operator space theory
- Summary and outlook

Motivation: Quantum Information

- Any theory of information processing depends on and underlying physical theory

Motivation: Quantum Information

- Any theory of information processing depends on and underlying physical theory
- Classical physics: bits

Motivation: Quantum Information

- Any theory of information processing depends on and underlying physical theory
- Classical physics: bits
- (Non-relativistic) quantum physics: qubits

Motivation: Quantum Information

- Any theory of information processing depends on and underlying physical theory
- Classical physics: bits
- (Non-relativistic) quantum physics: qubits
- Other examples: non-local boxes, quantum field theory, quantum gravity (?)

Motivation: Quantum Information

- Any theory of information processing depends on and underlying physical theory
- Classical physics: bits
- (Non-relativistic) quantum physics: qubits
- Other examples: non-local boxes, quantum field theory, quantum gravity (?)
- **Goal:** understand similarities and differences

Motivation: Bits vs. Qubits I

- **Computational complexity:** Shor's prime factorisation algorithm, Grover's search algorithm, simulation of quantum systems etc.

Motivation: Bits vs. Qubits I

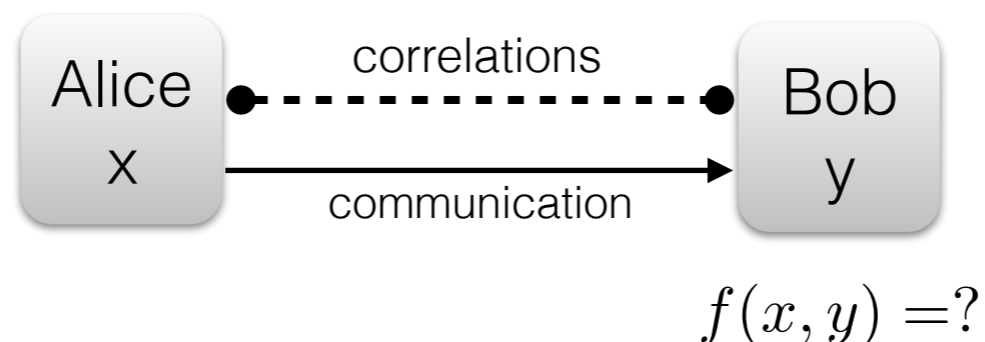
- **Computational complexity:** Shor's prime factorisation algorithm, Grover's search algorithm, simulation of quantum systems etc.
-> no classical/quantum super polynomial separation is proven (!)

Motivation: Bits vs. Qubits I

- **Computational complexity:** Shor's prime factorisation algorithm, Grover's search algorithm, simulation of quantum systems etc.

-> no classical/quantum super polynomial separation is proven (!)

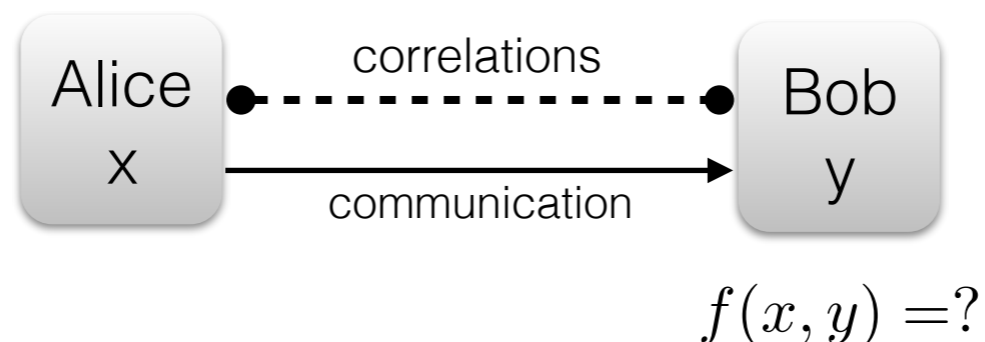
- **Communication complexity:** how much communication is needed to compute a given function with bipartite input?



Motivation: Bits vs. Qubits I

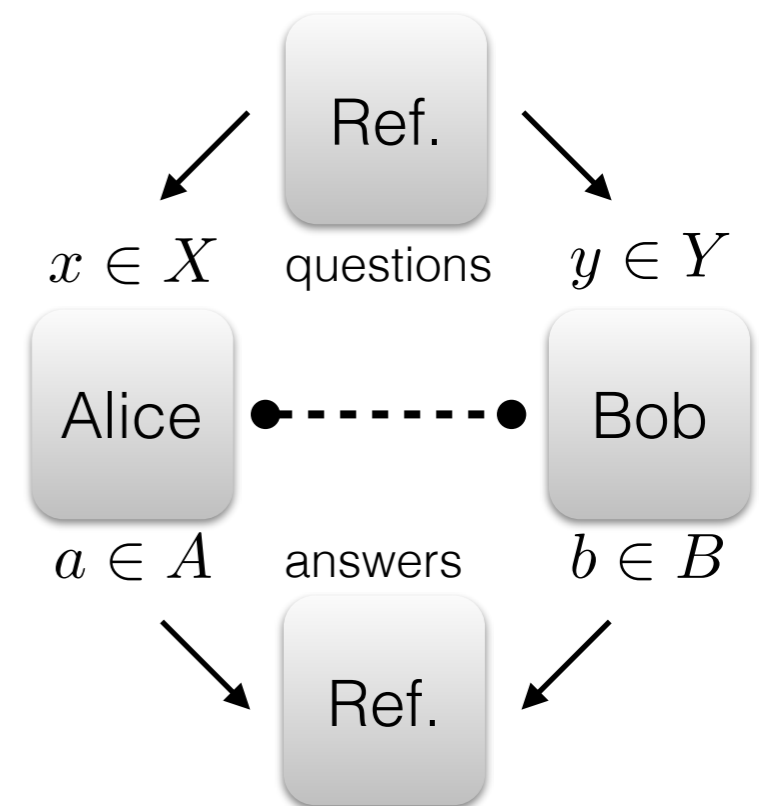
- **Computational complexity:** Shor's prime factorisation algorithm, Grover's search algorithm, simulation of quantum systems etc.
-> no classical/quantum super polynomial separation is proven (!)

- **Communication complexity:** how much communication is needed to compute a given function with bipartite input?
-> exponential classical/quantum separation is known (!)



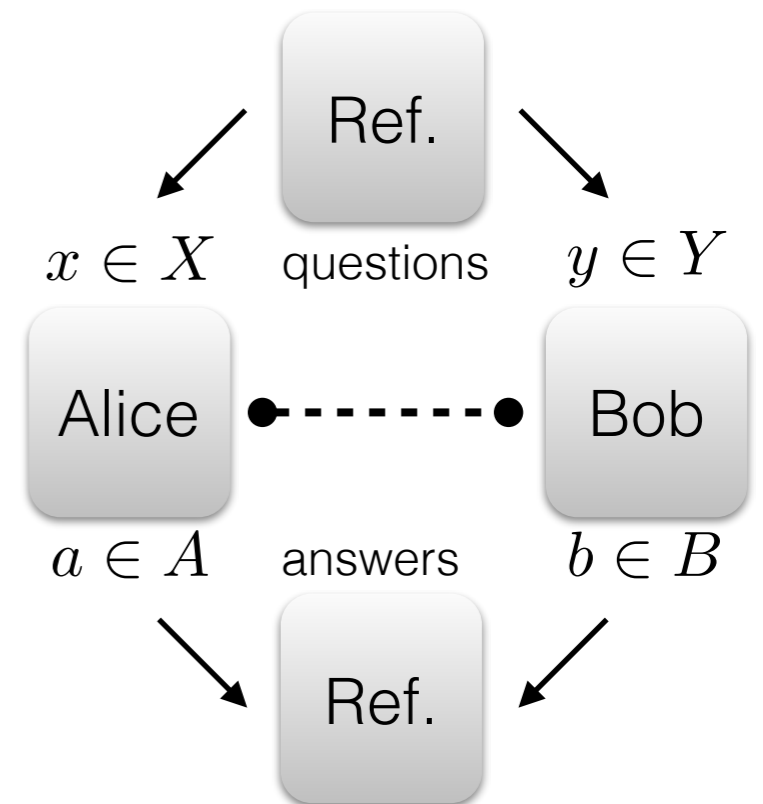
Motivation: Bits vs. Qubits II

- **Bell inequalities** (multi prover games): for a given game, what is the optimal winning probability (averaged over all possible questions)?
-> unbounded classical/quantum separation is known



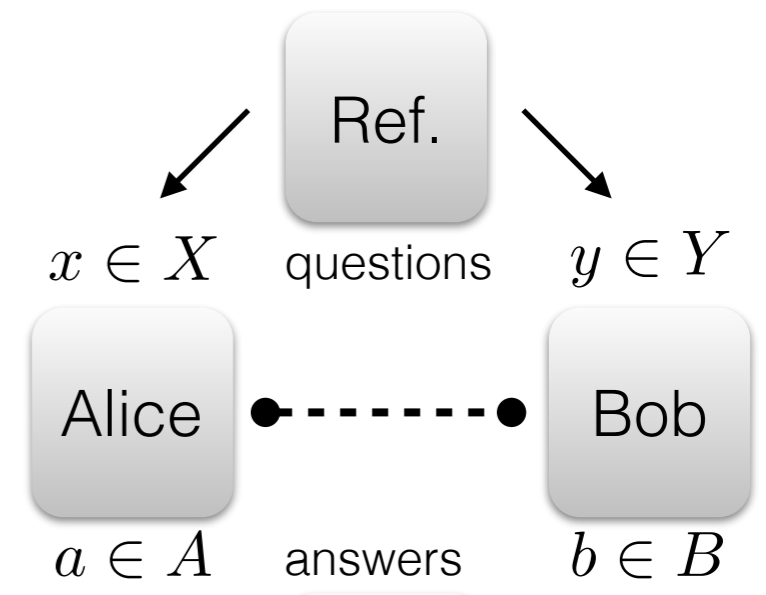
Motivation: Bits vs. Qubits II

- **Bell inequalities** (multi prover games): for a given game, what is the optimal winning probability (averaged over all possible questions)?
-> unbounded classical/quantum separation is known

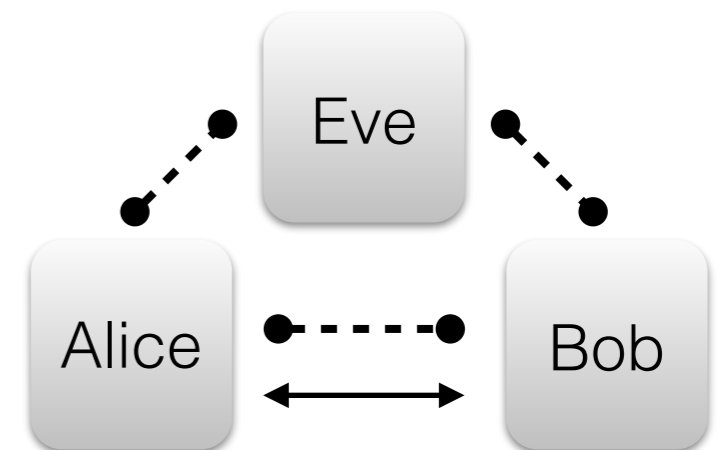


Motivation: Bits vs. Qubits II

- **Bell inequalities** (multi prover games): for a given game, what is the optimal winning probability (averaged over all possible questions)?
-> unbounded classical/quantum separation is known



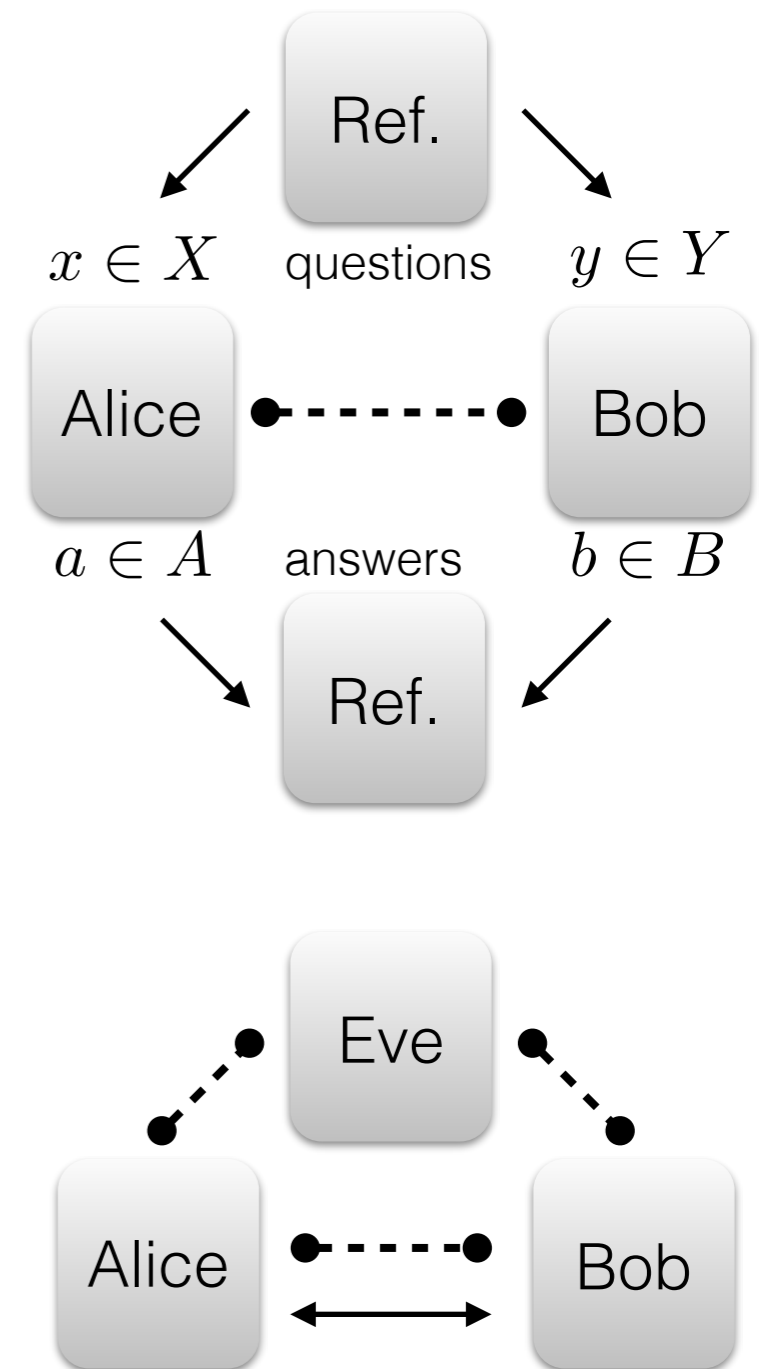
- **Cryptography**: key distribution, two-party cryptography, etc.
-> *strong* classical/quantum separation is known



Motivation: Bits vs. Qubits II

- **Bell inequalities** (multi prover games): for a given game, what is the optimal winning probability (averaged over all possible questions)?
-> unbounded classical/quantum separation is known

- **Cryptography**: key distribution, two-party cryptography, etc.
-> *strong* classical/quantum separation is known

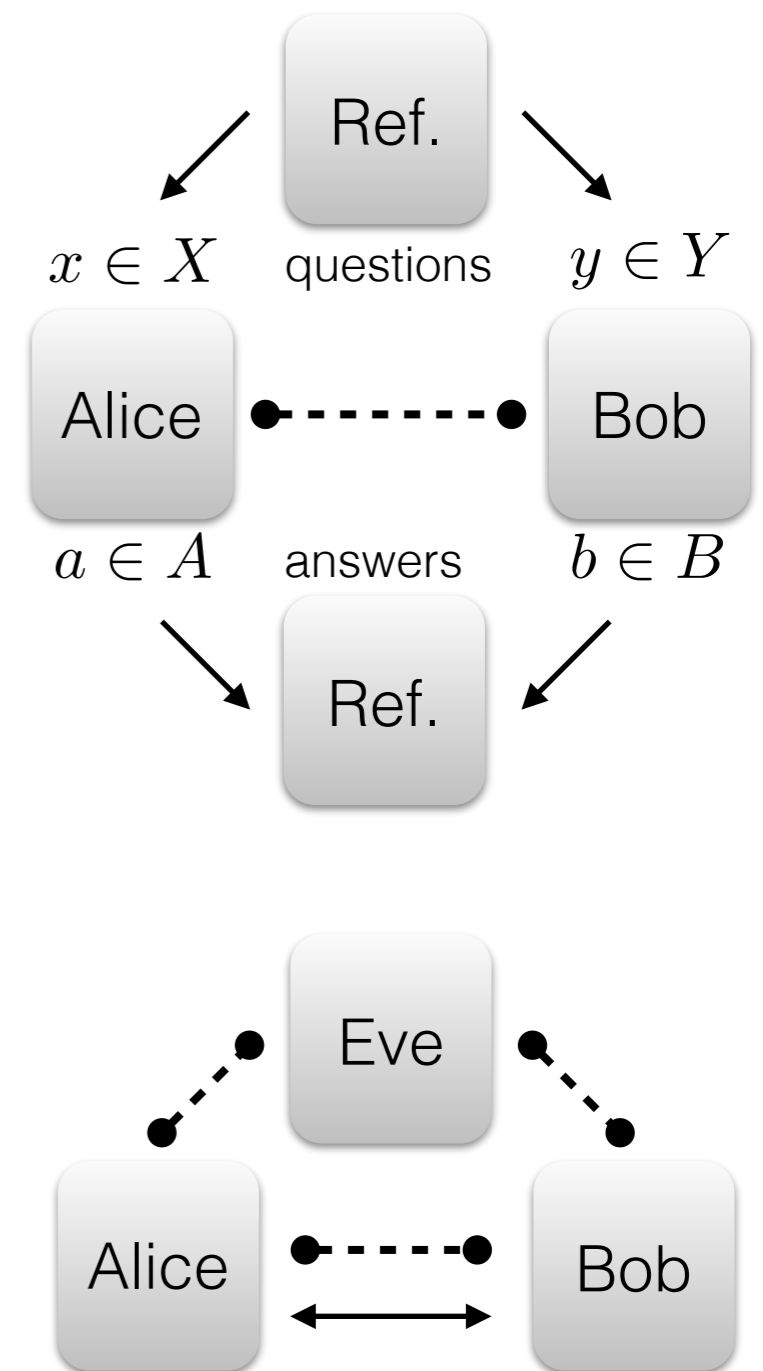


Motivation: Bits vs. Qubits II

- **Bell inequalities** (multi prover games): for a given game, what is the optimal winning probability (averaged over all possible questions)?
-> unbounded classical/quantum separation is known

- **Cryptography**: key distribution, two-party cryptography, etc.
-> *strong* classical/quantum separation is known

-> but also: quantum adversaries, post-quantum cryptography!

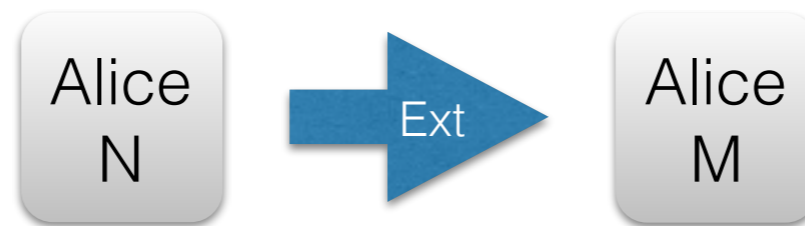


Outline

- Motivation
- Randomness extraction against quantum adversaries
- Results - mathematical framework based on operator space theory
- Summary and outlook

Randomness Extraction I

- **Goal:** transform only partly random classical source N into (almost perfectly) uniformly random source M (possibly over shorter alphabet)



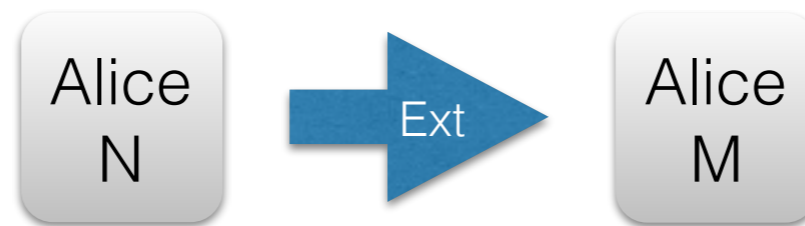
$$(2^m = M \subseteq N = 2^n)$$

- **Condition:** contains some randomness as measured by

$$p_{\text{guess}}(N)_P = \max_x p_x \leq 1/k$$

Randomness Extraction I

- **Goal:** transform only partly random classical source N into (almost perfectly) uniformly random source M (possibly over shorter alphabet)



$$(2^m = M \subseteq N = 2^n)$$

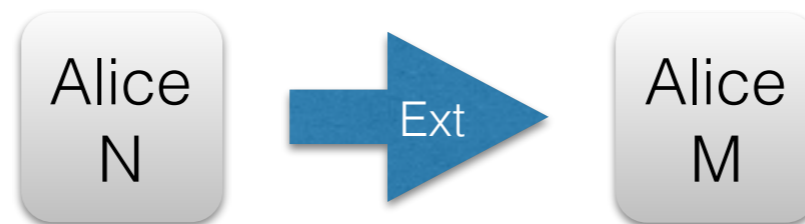
- **Condition:** contains some randomness as measured by

$$p_{\text{guess}}(N)_P = \max_x p_x \leq 1/k$$

- **Problem:** cannot be achieved in a deterministic way, if we require it to work for all sources satisfying the upper bound on the guessing probability
- **Solution:** can be achieved if the use of a catalyst is allowed, additional uniformly random source over alphabet $D = 2^d$ (called the seed)

Randomness Extraction I

- **Goal:** transform only partly random classical source N into (almost perfectly) uniformly random source M (possibly over shorter alphabet)



$$(2^m = M \subseteq N = 2^n)$$

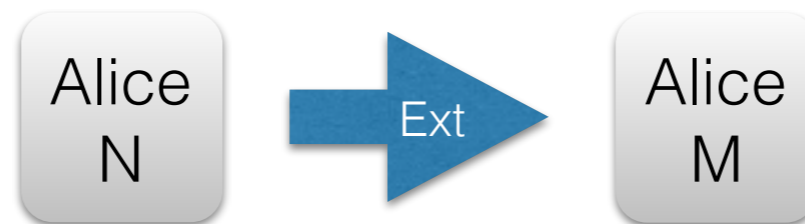
- **Definition:** A (k, ϵ) -**extractor** is a deterministic mapping $\text{Ext} : D \times N \rightarrow M$ such that for all distributions P_N with $p_{\text{guess}}(N)_P \leq 1/k$ we have that $(U_D, \text{Ext}(P_N, U_D))$ is ϵ -close in variational distance to (U_D, U_M) ,

$$C(\text{Ext}, k) = \max_{p_{\text{guess}}(N)_P \leq 1/k} \frac{1}{D} \sum_{i \in D} \|\text{Ext}(i, P) - U_M\|_1 \leq \epsilon$$

where the output distribution is given by $\mathbb{P}(\text{Ext}(i, P) = y) = \sum_{x \in N} p_x \cdot \delta_{\text{Ext}(i, x) = y}$

Randomness Extraction I

- **Goal:** transform only partly random classical source N into (almost perfectly) uniformly random source M (possibly over shorter alphabet)



$$(2^m = M \subseteq N = 2^n)$$

This objects actually exist (with “good” parameters)!

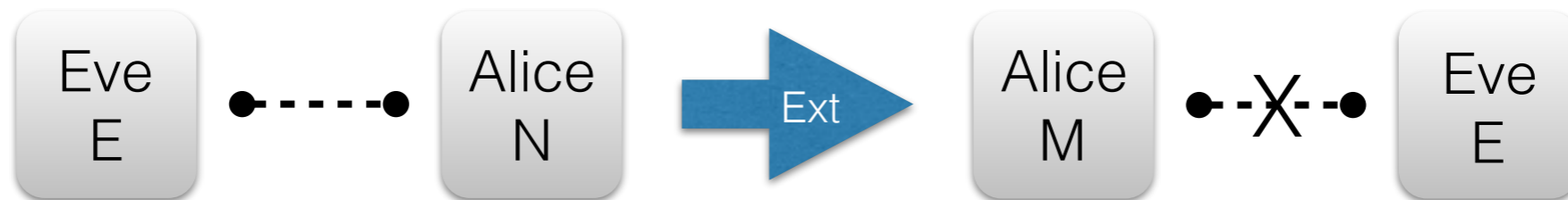
- **Definition:** A (k, ϵ) -**extractor** is a deterministic mapping $\text{Ext} : D \times N \rightarrow M$ such that for all distributions P_N with $p_{\text{guess}}(N)_P \leq 1/k$ we have that $(U_D, \text{Ext}(P_N, U_D))$ is ϵ -close in variational distance to (U_D, U_M) ,

$$C(\text{Ext}, k) = \max_{p_{\text{guess}}(N)_P \leq 1/k} \frac{1}{D} \sum_{i \in D} \|\text{Ext}(i, P) - U_M\|_1 \leq \epsilon$$

where the output distribution is given by $\mathbb{P}(\text{Ext}(i, P) = y) = \sum_{x \in N} p_x \cdot \delta_{\text{Ext}(i, x) = y}$

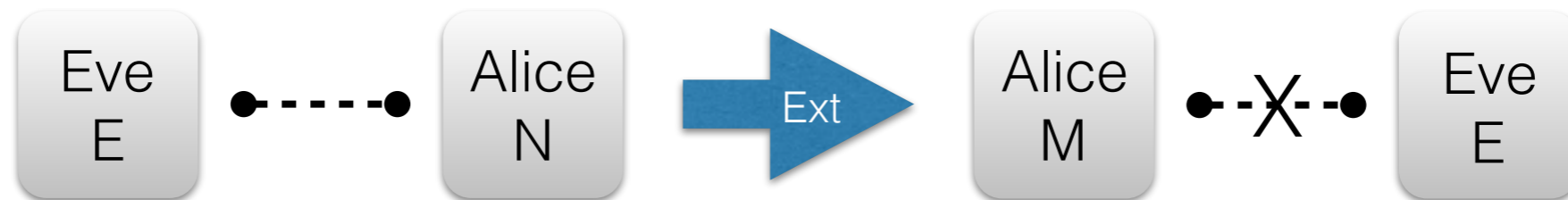
Randomness Extraction II

- **Goal:** transform only partly random classical source N into (almost perfectly) uniformly random **and private** source M (possibly over shorter alphabet)



Randomness Extraction II

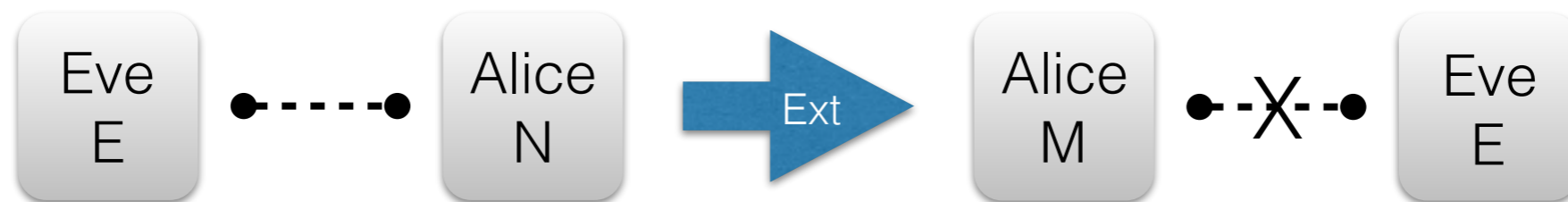
- **Goal:** transform only partly random classical source N into (almost perfectly) uniformly random **and private** source M (possibly over shorter alphabet)



- **Correlations:** if E is classical then the extractor still works but what happens for E quantum?
- **Motivation:** quantum cryptography, post-quantum cryptography, information theory —> compare classical to quantum memory

Randomness Extraction II

- **Goal:** transform only partly random classical source N into (almost perfectly) uniformly random **and private** source M (possibly over shorter alphabet)

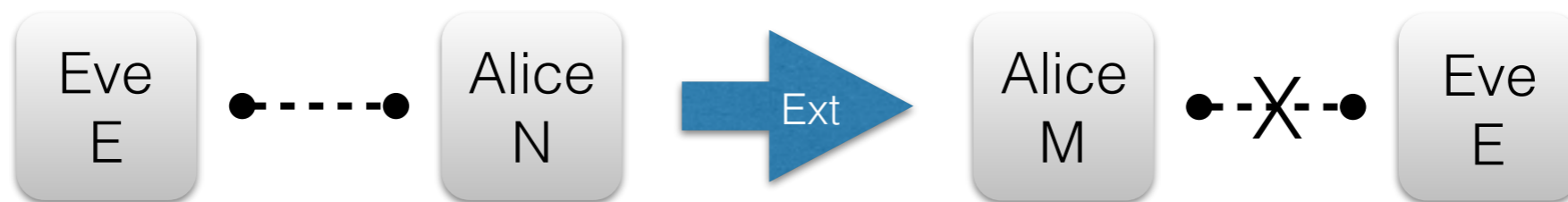


- **Correlations:** if E is classical then the extractor still works but what happens for E quantum?
- **Motivation:** quantum cryptography, post-quantum cryptography, information theory \rightarrow compare classical to quantum memory
- **Setup:** input is classical-quantum state with lower bound on the adversary's guessing probability of the secret N (given all her knowledge)

$$\rho_{NE} = \sum_{x \in N} |x\rangle\langle x|_N \otimes \rho_E^x \quad p_{\text{guess}}(N|E)_\rho = \max_{\Lambda = \{\Lambda^x\}} \sum_{x \in N} \text{tr} [\Lambda_E^x \rho_E^x] \leq 1/k$$

Randomness Extraction II

- **Goal:** transform only partly random classical source N into (almost perfectly) uniformly random **and private** source M (possibly over shorter alphabet)



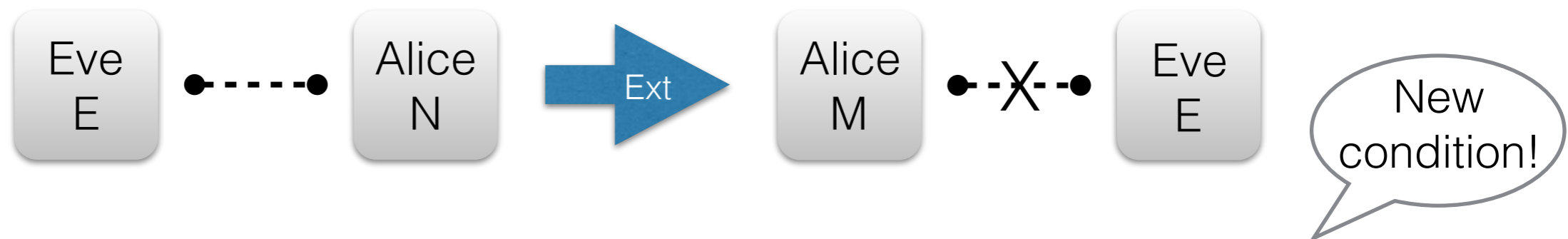
- **Definition:** A quantum-proof (k, ϵ) -**extractor** is a deterministic mapping $\text{Ext} : D \times N \rightarrow M$ such that for all classical-quantum states ρ_{NE} with $p_{\text{guess}}(N|E)_\rho \leq 1/k$,

$$Q(\text{Ext}, k) = \max_{p_{\text{guess}}(N|E)_\rho \leq 1/k} \frac{1}{D} \sum_{i \in D} \|(\text{Ext} \otimes \text{id}_E)(i, \rho_{NE}) - U_M \otimes \rho_E\|_1 \leq \epsilon$$

$$(\text{Ext} \otimes \text{id}_E) = \sum_{\substack{x \in N \\ y \in M}} \delta_{\text{Ext}(i,x)=y} |y\rangle \langle y|_M \otimes \rho_E^x$$

Randomness Extraction II

- **Goal:** transform only partly random classical source N into (almost perfectly) uniformly random **and private** source M (possibly over shorter alphabet)



- **Definition:** A quantum-proof (k, ϵ) -**extractor** is a deterministic mapping $\text{Ext} : D \times N \rightarrow M$ such that for all classical-quantum states ρ_{NE} with $p_{\text{guess}}(N|E)_\rho \leq 1/k$,

$$Q(\text{Ext}, k) = \max_{p_{\text{guess}}(N|E)_\rho \leq 1/k} \frac{1}{D} \sum_{i \in D} \|(\text{Ext} \otimes \text{id}_E)(i, \rho_{NE}) - U_M \otimes \rho_E\|_1 \leq \epsilon$$

$$(\text{Ext} \otimes \text{id}_E) = \sum_{\substack{x \in N \\ y \in M}} \delta_{\text{Ext}(i,x)=y} |y\rangle \langle y|_M \otimes \rho_E^x$$

Randomness Extraction III

$$C(\text{Ext}, k) \quad \text{vs.} \quad Q(\text{Ext}, k)$$

- **Motivation:** quantum cryptography, post-quantum cryptography, information theory \rightarrow compare classical to quantum memory

Randomness Extraction III

$$C(\text{Ext}, k) \quad \text{vs.} \quad Q(\text{Ext}, k)$$

- **Motivation:** quantum cryptography, post-quantum cryptography, information theory \rightarrow compare classical to quantum memory
- **Known:** some extractor constructions are quantum-proof, some are not \rightarrow there is a ***classical - quantum gap*** (only understood very poorly)
- **Goal:** understand this gap better, find (matching) upper and lower bounds on the size of the gap

Randomness Extraction III

$$C(\text{Ext}, k) \quad \text{vs.} \quad Q(\text{Ext}, k)$$

- **Motivation:** quantum cryptography, post-quantum cryptography, information theory \rightarrow compare classical to quantum memory
 - **Known:** some extractor constructions are quantum-proof, some are not \rightarrow there is a ***classical - quantum gap*** (only understood very poorly)
 - **Goal:** understand this gap better, find (matching) upper and lower bounds on the size of the gap
-
- **Our work:** we developed mathematical framework to study this question based on ***operator space theory*** (cf. Bell inequalities)

Randomness Extraction III

$$C(\text{Ext}, k) \quad \text{vs.} \quad Q(\text{Ext}, k)$$

- **Motivation:** quantum cryptography, post-quantum cryptography, information theory \rightarrow compare classical to quantum memory
 - **Known:** some extractor constructions are quantum-proof, some are not \rightarrow there is a **classical - quantum gap** (only understood very poorly)
 - **Goal:** understand this gap better, find (matching) upper and lower bounds on the size of the gap
-
- **Our work:** we developed mathematical framework to study this question based on **operator space theory** (cf. Bell inequalities)
 - **Results:** derive all known result with unified proof strategy (using semi-definite program relaxations), plus give new bounds on the classical - quantum gap
 - **Extra:** relate the question about the violation of Bell inequalities to the question about quantum-proof extractors

Outline

- Motivation
- Randomness extraction against quantum adversaries
- Results - mathematical framework based on operator space theory
- Summary and outlook

Overview

$C(\text{Ext}, k)$ vs. $Q(\text{Ext}, k)$

- Classical extractor property is expressed as **norm** of a linear mapping between **normed linear spaces**
- These normed spaces can be **quantised**, giving rise to **operator spaces**
- The property **quantum-proof** extractor can be formulated in terms of a **completely bounded norm** (norms between operator spaces)

Linear Normed Spaces

- Consider the **norm**: $\|\cdot\|_n = \max\{\|\cdot\|_1, k\|\cdot\|_\infty\}$

—> input constraint captured for distributions with $\|P\|_n \leq 1$

$$\text{(remember: } C(\text{Ext}, k) = \max_{p_{\text{guess}}(N)} \frac{1}{D} \sum_{i \in D} \|\text{Ext}(i, P) - U_M\|_1 \leq \epsilon)$$

Linear Normed Spaces

- Consider the **norm**: $\|\cdot\|_n = \max\{\|\cdot\|_1, k\|\cdot\|_\infty\}$

—> input constraint captured for distributions with $\|P\|_n \leq 1$

$$\text{(remember: } C(\text{Ext}, k) = \max_{p_{\text{guess}}(N)} \max_{P \leq 1/k} \frac{1}{D} \sum_{i \in D} \|\text{Ext}(i, P) - U_M\|_1 \leq \epsilon)$$

-
- Extractor characterised by **linear mapping** $\Delta[\text{Ext}] : \mathbb{R}^N \rightarrow \mathbb{R}^{DM}$:

$$\Delta[\text{Ext}](e_x) = \frac{1}{D} \sum_{\substack{i \in D \\ y \in M}} \left(\delta_{\text{Ext}(i,x)=y} - \frac{1}{M} \right) e_i \otimes e_y$$

with **bounded norm** constraint

$$C(\text{Ext}, k) = \|\Delta[\text{Ext}]\|_{n \rightarrow 1} = \max\{\|\Delta[\text{Ext}](z)\|_1 : \|x\|_n \leq 1\} \leq \epsilon$$

Operator Spaces

- Linear normed space W together with a **sequence of norms** on $W \otimes M_q$, $q \in \mathbb{N}$ satisfying some consistency conditions



classical



quantum

Operator Spaces

- Linear normed space W together with a **sequence of norms** on $W \otimes M_q$, $q \in \mathbb{N}$ satisfying some consistency conditions

classical

quantum

- A mapping $L : W \rightarrow V$ between operator spaces W and V has **completely bounded norm** (cb):

$$\|L\|_{\text{cb}} = \sup_{q \in \mathbb{N}} \{ \|L \otimes \text{id}_{M_q}\|_{W \otimes M_q \rightarrow V \otimes M_q} \}$$

Operator Spaces

- Linear normed space W together with a **sequence of norms** on $W \otimes M_q$, $q \in \mathbb{N}$ satisfying some consistency conditions

classical

quantum

- A mapping $L : W \rightarrow V$ between operator spaces W and V has **completely bounded norm** (cb):

$$\|L\|_{cb} = \sup_{q \in \mathbb{N}} \{ \|L \otimes \text{id}_{M_q}\|_{W \otimes M_q \rightarrow V \otimes M_q} \}$$

- There exist operator space extensions such that:

$$Q(\text{Ext}, k) = \|\Delta[\text{Ext}]\|_{cb, n \rightarrow 1} \leq \epsilon$$

Operator Spaces

- Linear normed space W together with a **sequence of norms** on $W \otimes M_q$, $q \in \mathbb{N}$ satisfying some consistency conditions

classical

quantum

- A mapping $L : W \rightarrow V$ between operator spaces W and V has **completely bounded norm** (cb):

$$\|L\|_{cb} = \sup_{q \in \mathbb{N}} \{ \|L \otimes \text{id}_{M_q}\|_{W \otimes M_q \rightarrow V \otimes M_q} \}$$

- There exist operator space extensions such that:

$$Q(\text{Ext}, k) = \|\Delta[\text{Ext}]\|_{cb, n \rightarrow 1} \leq \epsilon$$

- Analyse bounded vs. completely bounded norm: in general, but also for specific extractor constructions!

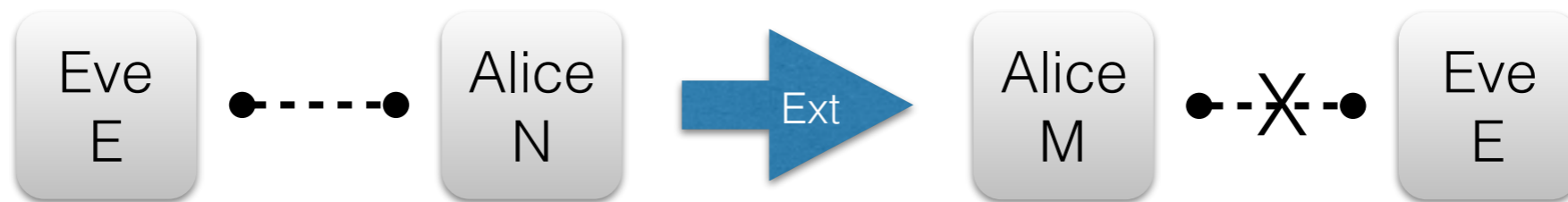
$$C(\text{Ext}, k) \text{ vs. } Q(\text{Ext}, k) \Leftrightarrow \|\Delta[\text{Ext}]\|_{n \rightarrow 1} \text{ vs. } \|\Delta[\text{Ext}]\|_{cb, n \rightarrow 1}$$

Outline

- Motivation
- Randomness extraction against quantum adversaries
- Results - mathematical framework based on operator space theory
- Summary and outlook

Summary and Outlook

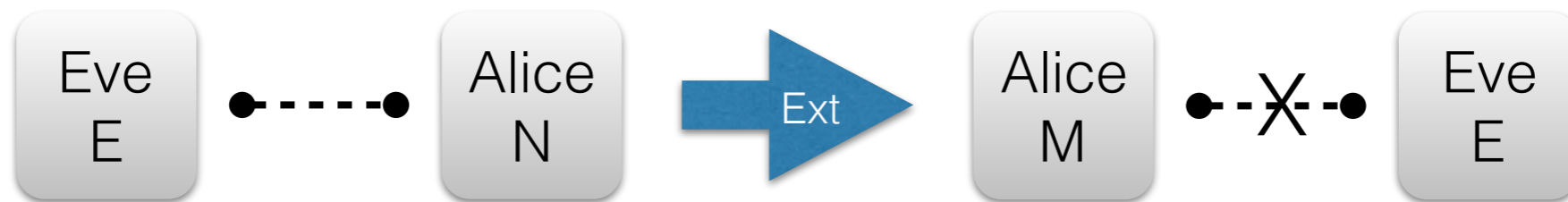
- Analyse differences (similarities) between classical and quantum information
- Randomness extraction against classical vs. quantum adversaries:



$C(\text{Ext}, k)$ vs. $Q(\text{Ext}, k)$

Summary and Outlook

- Analyse differences (similarities) between classical and quantum information
- Randomness extraction against classical vs. quantum adversaries:



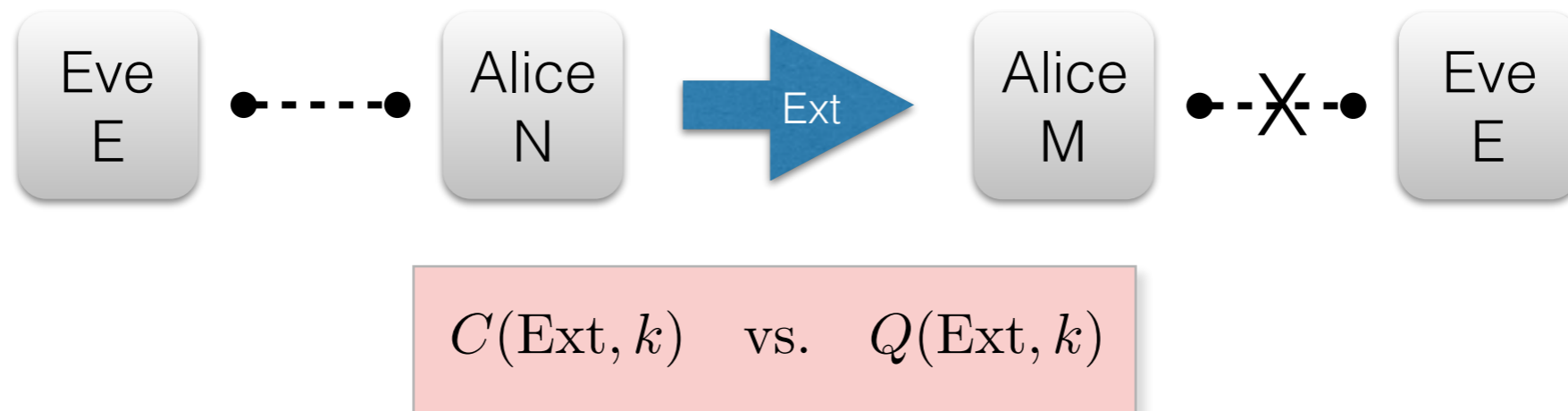
$C(\text{Ext}, k)$ vs. $Q(\text{Ext}, k)$

- We phrase the problem in terms of operator space theory:

$C(\text{Ext}, k)$ vs. $Q(\text{Ext}, k) \Leftrightarrow \|\Delta[\text{Ext}]\|_{\mathcal{N} \rightarrow 1}$ vs. $\|\Delta[\text{Ext}]\|_{\text{cb}, \mathcal{N} \rightarrow 1}$

Summary and Outlook

- Analyse differences (similarities) between classical and quantum information
- Randomness extraction against classical vs. quantum adversaries:



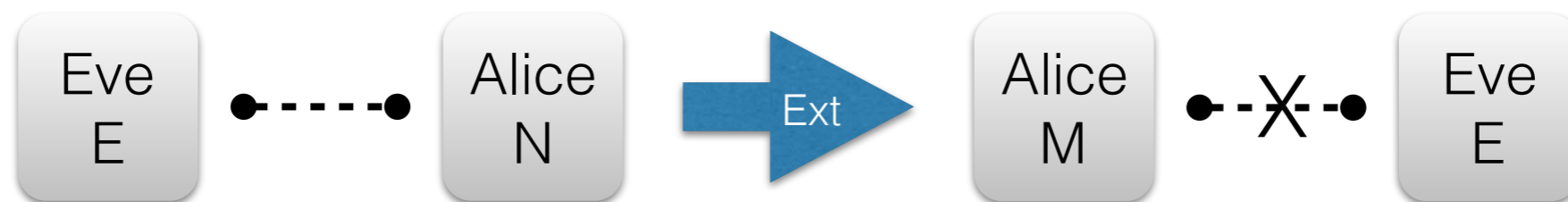
- We phrase the problem in terms of operator space theory:

$$C(\text{Ext}, k) \text{ vs. } Q(\text{Ext}, k) \Leftrightarrow \|\Delta[\text{Ext}]\|_{\mathcal{N} \rightarrow 1} \text{ vs. } \|\Delta[\text{Ext}]\|_{\text{cb}, \mathcal{N} \rightarrow 1}$$

- We derive all known result with a unified proof strategy (using semi-definite program relaxations), plus give new bounds on the classical - quantum gap
- Connection to Bell inequalities, extension to theory of pseudorandomness, etc.

Summary and Outlook

- Analyse differences (similarities) between classical and quantum information
- Randomness extraction against classical vs. quantum adversaries:



$C(\text{Ext}, k)$ vs. $Q(\text{Ext}, k)$

Main question remains largely open!

- We phrase the problem in terms of operator space theory:

$C(\text{Ext}, k)$ vs. $Q(\text{Ext}, k) \Leftrightarrow \|\Delta[\text{Ext}]\|_{\mathcal{N} \rightarrow 1}$ vs. $\|\Delta[\text{Ext}]\|_{\text{cb}, \mathcal{N} \rightarrow 1}$

- We derive all known result with a unified proof strategy (using semi-definite program relaxations), plus give new bounds on the classical - quantum gap
- Connection to Bell inequalities, extension to theory of pseudorandomness, etc.