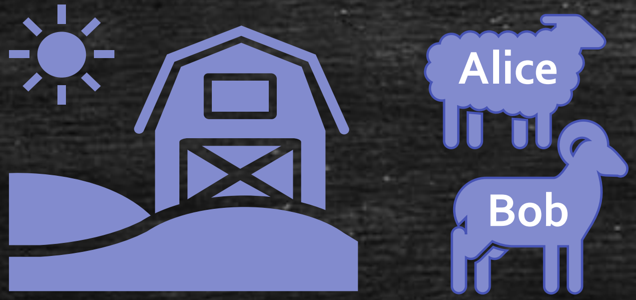


Computing secret key rates

Les Diablerets QKD Summer School 2026

Peter Brown

The key-rate problem

The key-rate problem

1001101…

1001111…

1. They generate raw keys using their devices.

The key-rate problem

1001101... 1001101...

1. They generate raw keys using their devices.
2. They correct errors (*information reconciliation*)

The key-rate problem

1. They generate raw keys using their devices.
2. They correct errors (*information reconciliation*)

The key-rate problem

1. They generate raw keys using their devices.
2. They correct errors (*information reconciliation*)
3. They extract randomness (*privacy amplification*)

The key-rate problem

1. They generate raw keys using their devices.
2. They correct errors (*information reconciliation*)
3. They extract randomness (*privacy amplification*)

Cost: $leak_{\mathrm{EC}}$

The key-rate problem

1. They generate raw keys using their devices.
2. They correct errors (*information reconciliation*)
3. They extract randomness (*privacy amplification*)

Cost: $leak_{\mathrm{EC}}$

Gain: $H(Z|E)$

The key-rate problem

1. They generate raw keys using their devices.
2. They correct errors (*information reconciliation*)
3. They extract randomness (*privacy amplification*)

Cost: $leak_{\mathrm{EC}}$

Gain: $H(Z|E)$

Key rate: $\min_{\text{attacks}} H(Z|E) - leak_{\mathrm{EC}}$ bits per round

The key-rate problem

1. They generate raw keys using their devices.
2. They correct errors (*information reconciliation*) Cost: $leak_{\mathrm{EC}}$
3. They extract randomness (*privacy amplification*) Gain: $H(Z|E)$ E unknown

Key rate: $\min_{\text{attacks}} H(Z|E) - leak_{\mathrm{EC}}$ bits per round

The entropy optimization problem

Want to study the following problem

$$\min_{\text{attacks}} H(Z|E)$$

The entropy optimization problem

Want to study the following problem

$$\min_{\text{attacks}} H(Z|E)$$

Set of "attacks" depends on security model and protocol:

<u>Device dependent</u>

Characterized system

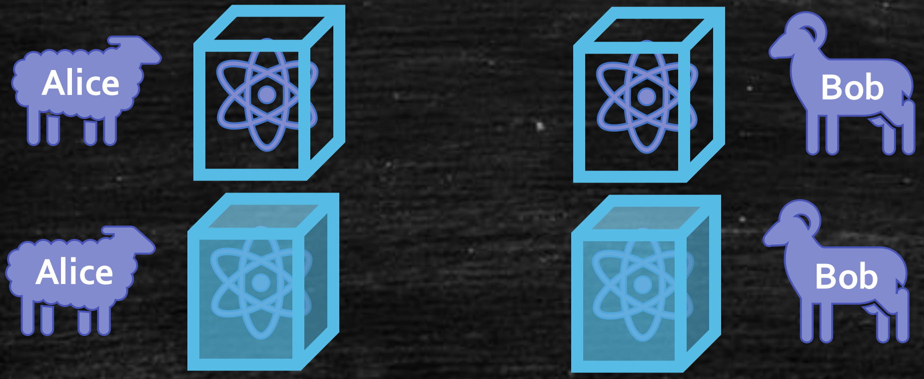
E.g. Known POVMs / state

The entropy optimization problem

Want to study the following problem

$$\min_{\text{attacks}} H(Z|E)$$

Set of "attacks" depends on security model and protocol:



<u>Device dependent</u>

Characterized system
E.g. Known POVMs / state

<u>Semi-device independent</u>

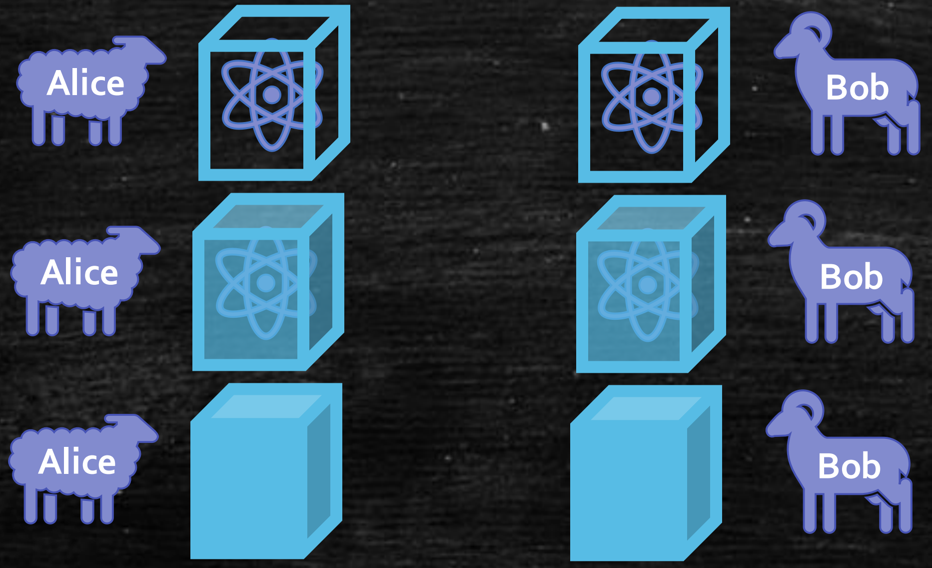
Partially characterized system
E.g. Known dimension

The entropy optimization problem

Want to study the following problem

$$\min_{\text{attacks}} \; H(Z|E)$$

Set of "attacks" depends on security model and protocol:



Device dependent — Characterized system
E.g. Known POVMs / state

Semi-device independent — Partially characterized system
E.g. Known dimension

Device independent — Fully uncharacterized system
E.g. We know it is quantum

The entropy optimization problem II

Things look difficult

$$\min_{\text{attacks}} H(Z|E)$$

The entropy optimization problem II

Things look difficult

$$\min_{\text{attacks}} H(Z|E)$$

- We really need to find the optima (or lower bound)!

Must assume Eve knows the optimal attack

The entropy optimization problem II

Things look difficult

$$\min_{\text{attacks}} H(Z|E)$$

- We really need to find the optima (or lower bound)!
- Potentially difficult to search the set of attacks?

Must assume Eve knows the optimal attack

The entropy optimization problem II

Things look difficult

$$\min_{\text{attacks}} H(Z|E)$$

- We really need to find the optima (or lower bound)!
- Potentially difficult to search the set of attacks?
  - Can we nicely characterise (mathematically)?

Must assume Eve knows the optimal attack

The entropy optimization problem II

Things look difficult

$$\min_{\text{attacks}} H(Z|E)$$

- We really need to find the optima (or lower bound)!
- Potentially difficult to search the set of attacks?
  - Can we nicely characterise (mathematically)?
  - Is there a (small) finite dimensional representation?

Must assume Eve knows the optimal attack

Our computers work with limited memory / time…

The entropy optimization problem II

Things look difficult

$$\min_{\text{attacks}} \ H(Z|E)$$

- We really need to find the optima (or lower bound)!

Must assume Eve knows the optimal attack

- Potentially difficult to search the set of attacks?
  - Can we nicely characterise (mathematically)?
  - Is there a (small) finite dimensional representation?

Our computers work with limited memory / time…

- Conditional entropy is concave

Not nice (for minimizing)

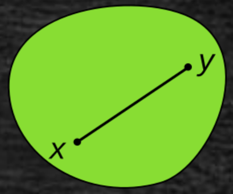
A Tool: Convex Optimisation

Convexity I

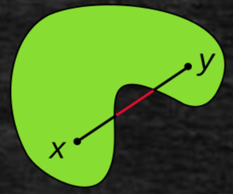
Definition:

A set X is convex if for all $x, y \in X$ and $\lambda \in [0,1]$ we have

$$\lambda x + (1-\lambda) y \in X \, .$$



Convex



Nonconvex

Examples:

- Quantum states

$$\mathcal{S} = \{\rho \;\mid\; \rho \succeq 0, \;\; , \mathrm{Tr}[\rho] = 1\}$$

- Quantum measurements

$$\mathcal{M} = \left\{ (M_1, \ldots, M_n) \;\mid\; \forall i \; M_i \succeq 0, \;\; , \sum_k M_k = \mathbb{I} \right\}$$

Convexity II

Convexity II

Definition:

A function $f : X \to \mathbb{R}$ is convex if for all $x, y \in X$ and $\lambda \in [0,1]$ we have

$$f\left(\lambda x + (1-\lambda)y\right) \leq \lambda f(x) + (1-\lambda)f(y)\,.$$

Convexity II

Definition:

A function $f : X \to \mathbb{R}$ is convex if for all $x, y \in X$ and $\lambda \in [0,1]$ we have

$$f\left(\lambda x + (1-\lambda) y\right) \leq \lambda f(x) + (1-\lambda) f(y)\,.$$

Examples:

- Surprisal $-\log(x)$
- Trace norm $\|X\|_1$
- Negative entropy $-H(A|B)$

Convex Optimisation

$$\begin{aligned} \min \quad & f(x) \\ \text{s.t.} \quad & x \in X \end{aligned}$$

Convex Optimisation

$$\begin{aligned} \min \quad & f(x) \\ \text{s.t.} \quad & x \in X \end{aligned}$$

Theorem:

If $f : X \to \mathbb{R}$ is convex and X is convex, then any *local minimum* is also a global minimum.

Convex Optimisation

$$\begin{aligned} \min \quad & f(x) \\ \text{s.t.} \quad & x \in X \end{aligned}$$

~~We really need to find the optima (or lower bound)!~~

Theorem:

If $f : X \to \mathbb{R}$ is convex and X is convex, then any *local minimum* is also a global minimum.

Convex Optimisation

$$\begin{aligned} \min \quad & f(x) \\ \text{s.t.} \quad & x \in X \end{aligned}$$

~~We really need to find the optima (or lower bound)!~~

✓

Theorem:

If $f : X \to \mathbb{R}$ is convex and X is convex, then any *local minimum* is also a global minimum.

Convexity does not imply efficiency though!

Semidefinite programming

Efficiently solvable convex optimisation problems exist:

$$\begin{aligned} \min_X \quad & \mathrm{Tr}[CX] \\ \text{s.t.} \quad & \mathrm{Tr}[F_i X] = b_i \quad \forall i \\ & X \succeq 0 \end{aligned}$$

Semidefinite programming

Efficiently solvable convex optimisation problems exist:

$$\begin{aligned} \min_{X} \quad & \mathrm{Tr}[CX] \\ \text{s.t.} \quad & \mathrm{Tr}[F_i X] = b_i \quad \forall i \\ & X \succeq 0 \end{aligned}$$

Linear objective function

Semidefinite programming

Efficiently solvable convex optimisation problems exist:

$$\begin{aligned} \min_{X} \quad & \mathrm{Tr}[CX] \\ \text{s.t.} \quad & \mathrm{Tr}[F_i X] = b_i \quad \forall i \\ & X \succeq 0 \end{aligned}$$

Linear objective function

Linear (in)equalities

Semidefinite programming

Efficiently solvable convex optimisation problems exist:

$$\begin{aligned} \min_{X} \quad & \mathrm{Tr}[CX] \\ \text{s.t.} \quad & \mathrm{Tr}[F_i X] = b_i \quad \forall i \\ & X \succeq 0 \end{aligned}$$

Linear objective function

Linear (in)equalities

Positive semidefinite inequalities

Semidefinite programming

Efficiently solvable convex optimisation problems exist:

max/min

$$\begin{aligned} \min_X \quad & \mathrm{Tr}[CX] \\ \text{s.t.} \quad & \mathrm{Tr}[F_i X] = b_i \quad \forall i \\ & X \succeq 0 \end{aligned}$$

Linear objective function

Linear (in)equalities

Positive semidefinite inequalities

Semidefinite programming

Efficiently solvable convex optimisation problems exist:

max/min

$$\begin{aligned} \min_X \quad & \mathrm{Tr}[CX] \\ \text{s.t.} \quad & \mathrm{Tr}[F_i X] = b_i \quad \forall i \\ & X \succeq 0 \end{aligned}$$

Linear objective function

Linear (in)equalities

Positive semidefinite inequalities

<u>Example (Min-entropy):</u>
Given a cq-state

$$\rho_{AE} = \sum_a p(a)|a\rangle\langle a| \otimes \rho_a$$

we have

$$H_{\min}(A|E) = -\log P_{\mathrm{guess}}(A|E)$$

Semidefinite programming

Efficiently solvable convex optimisation problems exist:

max/min

$$\begin{aligned} \min_{X} \quad & \mathrm{Tr}[CX] \\ \text{s.t.} \quad & \mathrm{Tr}[F_i X] = b_i \quad \forall i \\ & X \succeq 0 \end{aligned}$$

Linear objective function

Linear (in)equalities

Positive semidefinite inequalities

<u>Example (Min-entropy):</u>
Given a cq-state

$$\rho_{AE} = \sum_a p(a)|a\rangle\langle a| \otimes \rho_a$$

we have

$$H_{\min}(A|E) = -\log P_{\text{guess}}(A|E)$$

$$\begin{aligned} P_{\text{guess}}(A|E) = \max_{\{M_a\}_a} \quad & \sum_a p(a)\mathrm{Tr}[M_a \rho_a] \\ \text{s.t.} \quad & \sum_a M_a = \mathbb{I} \\ & M_a \succeq 0 \quad \forall a \end{aligned}$$

Core idea

Try to transform to a convex problem

$$\min_{\text{attacks}} H(Z|E) \quad \Longrightarrow \quad \begin{aligned} \min \quad & f(x) \\ \text{s.t.} \quad & x \in X \end{aligned}$$

Core idea

Try to transform to a convex problem

$$\min_{\text{attacks}} \; H(Z|E) \quad \Longrightarrow \quad \begin{aligned} \min \quad & f(x) \\ \text{s.t.} \quad & x \in X \end{aligned}$$

- Guaranteed optima
- Efficient (hopefully)
- Existing numerical software

Device-dependent rates

Hidden convexity

Device-dependent QKD – Eve's attacks

Device-dependent QKD – Eve's attacks

Eve can manipulate the transmitted state

$$\rho_{Q_A Q_B E}$$

Device-dependent QKD – Eve's attacks

Eve can manipulate the transmitted state

$$\rho_{Q_A Q_B E}$$

State at end of round

$$\rho_{ABPE} = (\mathcal{K} \otimes \mathcal{I}_E)(\rho_{Q_A Q_B E})$$

Device-dependent QKD – Eve's attacks

Eve can manipulate the transmitted state

$$\rho_{Q_A Q_B E}$$

State at end of round

$$\rho_{ABPE} = (\mathcal{K} \otimes \mathcal{I}_E)(\rho_{Q_A Q_B E})$$

But she is still constrained...

Device-dependent QKD – Eve's attacks

Eve can manipulate the transmitted state

$$\rho_{Q_A Q_B E}$$

State at end of round

$$\rho_{ABPE} = (\mathcal{K} \otimes \mathcal{I}_E)(\rho_{Q_A Q_B E})$$

But she is still constrained...

Statistical

$$\mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a, b, x, y)$$

Device-dependent QKD – Eve's attacks

Eve can manipulate the transmitted state

$$\rho_{Q_A Q_B E}$$

State at end of round

$$\rho_{ABPE} = (\mathcal{K} \otimes \mathcal{I}_E)(\rho_{Q_A Q_B E})$$

But she is still constrained…

Statistical

$$\mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y)$$

Prepare and measure

$$\mathrm{Tr}_{Q_B E}[\rho_{Q_A Q_B E}] = \rho_{Q_A}$$

DD-QKD key rate problem

How much certifiable randomness does Alice generate in one-round? $\min_{\text{Attacks}} H(A|PE)$

DD-QKD key rate problem

How much certifiable randomness does Alice generate in one-round?

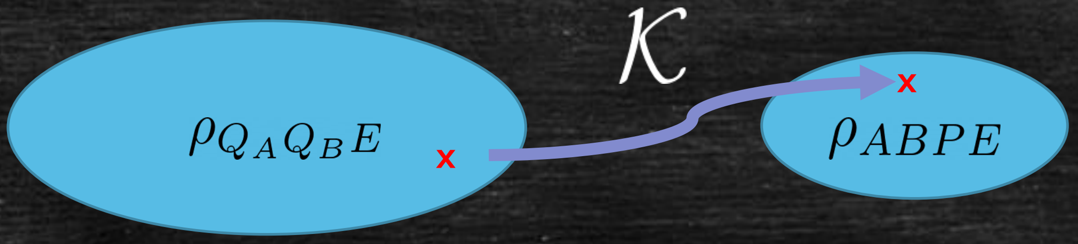
$$\min_{\text{Attacks}} H(A|PE)$$

Eve's attacks

DD-QKD key rate problem

How much certifiable randomness does Alice generate in one-round?

$$\min_{\text{Attacks}} H(A|PE)$$



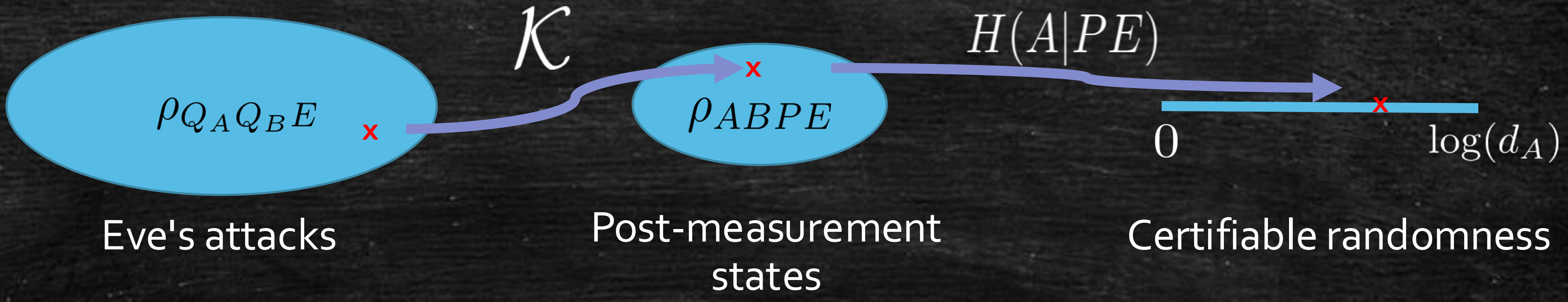
Eve's attacks

Post-measurement states

DD-QKD key rate problem

How much certifiable randomness does Alice generate in one-round?

$$\min_{\text{Attacks}} H(A|PE)$$



DD-QKD key rate problem

How much certifiable randomness does Alice generate in one-round?

$$\min_{\text{Attacks}} H(A|PE)$$

$$\begin{aligned} \min \quad & H(A|PE) \\ \text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(\rho_{Q_A Q_B E}) \\ & \rho_{Q_A Q_B E} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_A Q_B E}] = 1 \end{aligned}$$

Post-measurement state

Valid quantum state

DD-QKD key rate problem

How much certifiable randomness does Alice generate in one-round?

$$\min_{\text{Attacks}} H(A|PE)$$

Eve's attacks

Post-measurement states

Certifiable randomness

$$\begin{aligned} \min \quad & H(A|PE) \\ \text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(\rho_{Q_A Q_B E}) \\ & \rho_{Q_A Q_B E} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_A Q_B E}] = 1 \end{aligned}$$

Post-measurement state

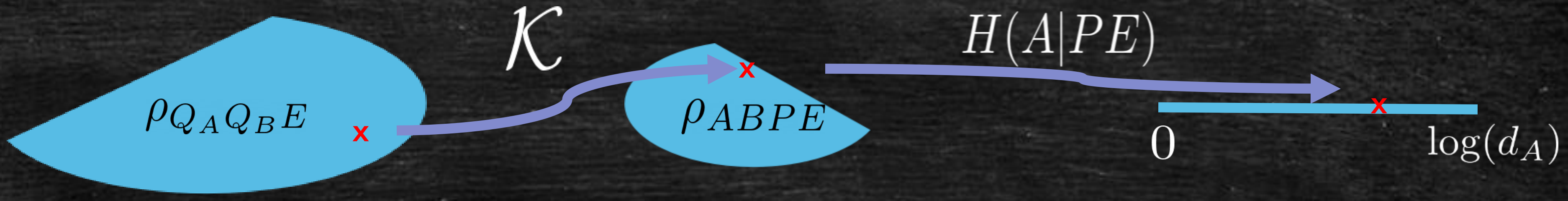
Valid quantum state

We have more constraints on Eve's attacks!

DD-QKD key rate problem

How much certifiable randomness does Alice generate in one-round?

$$\min_{\text{Attacks}} H(A|PE)$$



Eve's attacks

Post-measurement states

Certifiable randomness

$$\min \quad H(A|PE)$$

$$\text{s.t.} \quad \rho_{ABPE} = \mathcal{K}(\rho_{Q_A Q_B E})$$ Post-measurement state

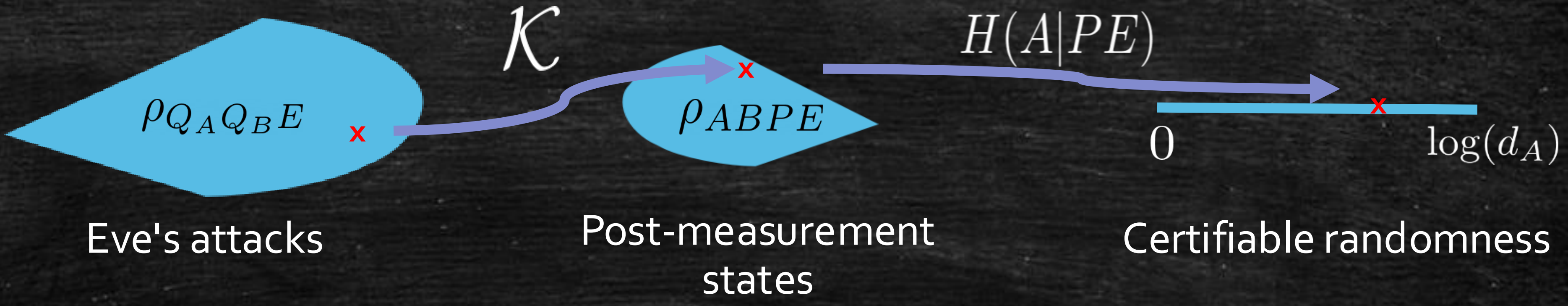
$$\rho_{Q_A Q_B E} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_A Q_B E}] = 1$$ Valid quantum state

$$\mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y)$$ Linear constraints on P(a,b,x,y)

DD-QKD key rate problem

How much certifiable randomness does Alice generate in one-round?

$$\min_{\text{Attacks}} H(A|PE)$$



$$
\begin{aligned}
\min \quad & H(A|PE) \\
\text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(\rho_{Q_AQ_BE}) \\
& \rho_{Q_AQ_BE} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_AQ_BE}] = 1 \\
& \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_AQ_B}] = p(a,b,x,y) \\
& \mathrm{Tr}_{Q_BE}[\rho_{Q_AQ_BE}] = \sigma
\end{aligned}
$$

Post-measurement state

Valid quantum state

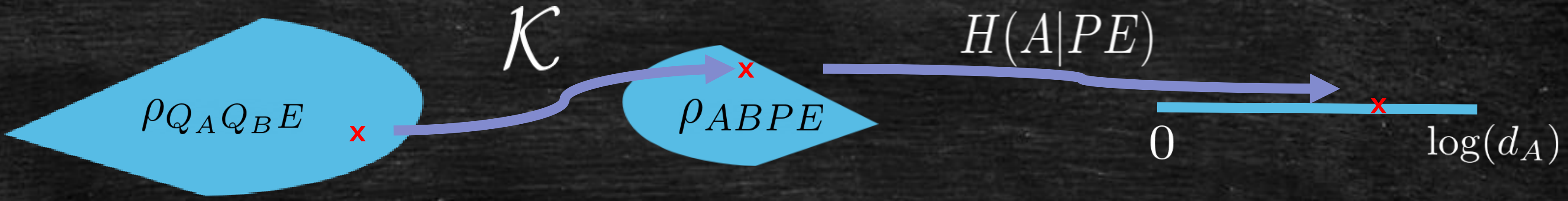
Linear constraints on P(a,b,x,y)

Prepare and measure constraint

DD-QKD key rate problem

How much certifiable randomness does Alice generate in one-round?

$$\min_{\text{Attacks}} H(A|PE)$$



$$\min \quad H(A|PE)$$

$$\text{s.t.} \quad \rho_{ABPE} = \mathcal{K}(\rho_{Q_AQ_BE})$$

$$\text{Attacks}\left\{\begin{array}{l} \rho_{Q_AQ_BE} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_AQ_BE}] = 1 \\ \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_AQ_B}] = p(a,b,x,y) \\ \mathrm{Tr}_{Q_BE}[\rho_{Q_AQ_BE}] = \sigma \end{array}\right.$$

Post-measurement state

Valid quantum state

Linear constraints on P(a,b,x,y)

Prepare and measure constraint

Simplifying the problem

$$
\begin{aligned}
\min \quad & H(A|PE) \\
\text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(\rho_{Q_A Q_B E}) \\
& \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y) \\
& \mathrm{Tr}_{Q_B E}[\rho_{Q_A Q_B E}] = \sigma \\
& \rho_{Q_A Q_B E} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_A Q_B E}] = 1
\end{aligned}
$$

Simplifying the problem

$$
\begin{aligned}
\min \quad & H(A|PE) \\
\text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(\rho_{Q_A Q_B E}) \\
& \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y) \\
& \mathrm{Tr}_{Q_B E}[\rho_{Q_A Q_B E}] = \sigma \\
& \rho_{Q_A Q_B E} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_A Q_B E}] = 1
\end{aligned}
$$

E dimension a priori unbounded

Simplifying the problem

$$
\begin{aligned}
\min \quad & H(A|PE) \\
\text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(\rho_{Q_AQ_BE}) \\
& \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_AQ_B}] = p(a,b,x,y) \\
& \mathrm{Tr}_{Q_BE}[\rho_{Q_AQ_BE}] = \sigma \\
& \rho_{Q_AQ_BE} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_AQ_BE}] = 1
\end{aligned}
$$

E dimension a priori unbounded

Minimizing a concave function

Simplifying the problem

$$
\begin{aligned}
\min \quad & H(A|PE) \\
\text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(\rho_{Q_A Q_B E}) \\
& \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y) \\
& \mathrm{Tr}_{Q_B E}[\rho_{Q_A Q_B E}] = \sigma \\
& \rho_{Q_A Q_B E} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_A Q_B E}] = 1
\end{aligned}
$$

E dimension a priori unbounded

Minimizing a concave function

Simplification 1:

Eve can always purify!

$$\rho_{Q_A Q_B E} \mapsto |\psi\rangle_{Q_A Q_B EF}$$

Simplifying the problem

$$\begin{aligned} \min \quad & H(A|PE) \\ \text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(\rho_{Q_AQ_BE}) \\ & \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_AQ_B}] = p(a,b,x,y) \\ & \mathrm{Tr}_{Q_BE}[\rho_{Q_AQ_BE}] = \sigma \\ & \rho_{Q_AQ_BE} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_AQ_BE}] = 1 \end{aligned}$$

E dimension a priori unbounded

Minimizing a concave function

<u>Simplification 1:</u>

Eve can always purify!

$$\rho_{Q_AQ_BE} \mapsto |\psi\rangle_{Q_AQ_BEF}$$

(strong subadditivity)

$$H(A|PEF) \leq H(A|PE)$$

Simplifying the problem

$$
\begin{aligned}
\min \quad & H(A|PE) \\
\text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(|\psi\rangle\langle\psi|_{Q_A Q_B E}) \\
& \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y) \\
& \mathrm{Tr}_{Q_B E}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = \sigma \\
& \mathrm{Tr}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = 1
\end{aligned}
$$

E dimension a priori unbounded

Minimizing a concave function

Simplification 1:

Eve can always purify!

$$\rho_{Q_A Q_B E} \mapsto |\psi\rangle_{Q_A Q_B E F}$$

(strong subadditivity)

$$H(A|PEF) \leq H(A|PE)$$

Simplifying the problem

$$\begin{aligned}\min \quad & H(A|PE) \\ \text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(|\psi\rangle\langle\psi|_{Q_A Q_B E}) \\ & \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y) \\ & \mathrm{Tr}_{Q_B E}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = \sigma \\ & \mathrm{Tr}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = 1\end{aligned}$$

E dimension a priori unbounded

Minimizing a concave function

Simplifying the problem

$$\begin{aligned} \min \quad & H(A|PE) \\ \text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(|\psi\rangle\langle\psi|_{Q_A Q_B E}) \\ & \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y) \\ & \mathrm{Tr}_{Q_B E}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = \sigma \\ & \mathrm{Tr}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = 1 \end{aligned}$$

E dimension a priori unbounded

Minimizing a concave function

<u>Tool: Isometric equivalence of purifications</u>

If $|\psi\rangle_{QE}$ and $|\phi\rangle_{QF}$ are both purifications of ρ_Q. Then there exists an isometry $V: E \to F$ or $V: F \to E$ such that

$$(I_Q \otimes V)|\psi\rangle = |\phi\rangle \quad \text{or} \quad (I_Q \otimes V)|\phi\rangle = |\psi\rangle$$

Simplifying the problem

$$\begin{aligned} \min \quad & H(A|PE) \\ \text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(|\psi\rangle\langle\psi|_{Q_A Q_B E}) \\ & \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y) \\ & \mathrm{Tr}_{Q_B E}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = \sigma \\ & \mathrm{Tr}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = 1 \end{aligned}$$

E dimension a priori unbounded

Minimizing a concave function

Isometric invariance of entropy $H(A|PE) = H(A|PF)$

<u>Tool: Isometric equivalence of purifications</u>

If $|\psi\rangle_{QE}$ and $|\phi\rangle_{QF}$ are both purifications of ρ_Q. Then there exists an isometry $V: E \to F$ or $V: F \to E$ such that

$$(I_Q \otimes V)|\psi\rangle = |\phi\rangle \quad \text{or} \quad (I_Q \otimes V)|\phi\rangle = |\psi\rangle$$

Simplifying the problem

$$\begin{aligned} \min \quad & H(A|PE) \\ \text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(|\psi\rangle\langle\psi|_{Q_A Q_B E}) \\ & \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y) \\ & \mathrm{Tr}_{Q_B E}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = \sigma \\ & \mathrm{Tr}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = 1 \end{aligned}$$

E dimension a priori unbounded

Minimizing a concave function

Simplification 2: All purifications are equivalent!

Simplifying the problem

$$\min \quad H(A|PE)$$

$$\text{s.t.} \quad \rho_{ABPE} = \mathcal{K}(|\psi\rangle\langle\psi|_{Q_A Q_B E})$$

$$\mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y)$$

$$\mathrm{Tr}_{Q_B E}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = \sigma$$

$$\mathrm{Tr}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = 1$$

E dimension bounded

Minimizing a concave function

Simplification 2: All purifications are equivalent!

$$|\psi\rangle_{Q_A Q_B E} = \sum_k \sqrt{\rho_{Q_A Q_B}} |k\rangle_{Q_A Q_B} \otimes |k\rangle_E$$

E system completely fixed now

Simplifying the problem

$$\min \quad H(A|PE)$$

$$\text{s.t.} \quad \rho_{ABPE} = \mathcal{K}(|\psi\rangle\langle\psi|_{Q_A Q_B E})$$

$$\mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y)$$

$$\mathrm{Tr}_{Q_B E}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = \sigma$$

$$\mathrm{Tr}[|\psi\rangle\langle\psi|_{Q_A Q_B E}] = 1$$

E dimension bounded

Minimizing a concave function

Simplification 2: All purifications are equivalent!

$$|\psi\rangle_{Q_A Q_B E} = \sum_k \sqrt{\rho_{Q_A Q_B}} |k\rangle_{Q_A Q_B} \otimes |k\rangle_E$$

E system completely fixed now

Optimization reduced to Q_A and Q_B only

Simplifying the problem

$$
\begin{aligned}
\min \quad & H(A|PE) \\
\text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(|\psi\rangle\langle\psi|_{Q_A Q_B E}) \\
& \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_A Q_B}] = p(a,b,x,y) \\
& \mathrm{Tr}_{Q_B}[\rho_{Q_A Q_B}] = \sigma \\
& \rho_{Q_A Q_B} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_A Q_B}] = 1
\end{aligned}
$$

E dimension bounded

Minimizing a concave function

<u>Simplification 2:</u> All purifications are equivalent!

$$
|\psi\rangle_{Q_A Q_B E} = \sum_k \sqrt{\rho_{Q_A Q_B}} |k\rangle_{Q_A Q_B} \otimes |k\rangle_E
$$

E system completely fixed now

Optimization reduced to Q_A and Q_B only

The simpler problem

The simpler problem

<u>Theorem:</u>

The device-dependent rate problem is
Equivalent to a **convex optimization problem**.

The simpler problem

<u>Theorem:</u>

The device-dependent rate problem is
Equivalent to a **convex optimization problem**.

Guaranteed to find optima!

The simpler problem

Theorem:

The device-dependent rate problem is
Equivalent to a **convex optimization problem**.

Guaranteed to find optima!

Efficient algorithms exist!

The simpler problem

<u>Theorem:</u>

The device-dependent rate problem is Equivalent to a **convex optimization problem**.

$$\begin{aligned}
\min \quad & H(A|PE) \\
\text{s.t.} \quad & \rho_{ABPE} = \mathcal{K}(|\psi\rangle\langle\psi|_{Q_AQ_BE}) \\
& \mathrm{Tr}[(M_{ax} \otimes N_{by})\rho_{Q_AQ_B}] = p(a,b,x,y) \\
& \mathrm{Tr}_{Q_B}[\rho_{Q_AQ_B}] = \sigma \\
& \rho_{Q_AQ_B} \succeq 0, \quad \mathrm{Tr}[\rho_{Q_AQ_B}] = 1
\end{aligned}$$

Guaranteed to find optima!

Efficient algorithms exist!

Current approaches

Computing DD key-rates is easy…

Current approaches

Computing DD key-rates is easy…

…because some nice people have done the hard work for us.

Current approaches

Computing DD key-rates is easy…

…because some nice people have done the hard work for us.

Ref.	Method	Language	Code
[OpenQKD]	Franke-Wolfe / Interior point	Matlab	https://openqkdsecurity.wordpress.com/
[LPCA24]	Conic optimization	Julia	github.com/araujoms/ConicQKD.jl
[QICS]	Conic optimization	Python	https://qics.readthedocs.io

Current approaches

Computing DD key-rates is easy…

…because some nice people have done the hard work for us.

Ref.	Method	Language	Code
[OpenQKD]	Franke-Wolfe / Interior point	Matlab	https://openqkdsecurity.wordpress.com/
[LPCA24]	Conic optimization	Julia	github.com/araujoms/ConicQKD.jl
[QICS]	Conic optimization	Python	https://qics.readthedocs.io

Specify protocol

Current approaches

Computing DD key-rates is easy…

…because some nice people have done the hard work for us.

Ref.	Method	Language	Code
[OpenQKD]	Franke-Wolfe / Interior point	Matlab	https://openqkdsecurity.wordpress.com/
[LPCA24]	Conic optimization	Julia	github.com/araujoms/ConicQKD.jl
[QICS]	Conic optimization	Python	https://qics.readthedocs.io

Specify protocol → Construct key channel

Current approaches

Computing DD key-rates is easy…

…because some nice people have done the hard work for us.

Ref.	Method	Language	Code
[OpenQKD]	Franke-Wolfe / Interior point	Matlab	https://openqkdsecurity.wordpress.com/
[LPCA24]	Conic optimization	Julia	github.com/araujoms/ConicQKD.jl
[QICS]	Conic optimization	Python	https://qics.readthedocs.io

Specify protocol → Construct key channel → Pass to a package

Example code (QICS – BB84)

```python
import numpy as np

import picos

qx = 0.25
qz = 0.75

X0 = np.array([[.5,  .5], [ .5, .5]])
X1 = np.array([[.5, -.5], [-.5, .5]])
Z0 = np.array([[1.,  0.], [ 0., 0.]])
Z1 = np.array([[0.,  0.], [ 0., 1.]])

Ax = np.kron(X0, X1) + np.kron(X1, X0)
Az = np.kron(Z0, Z1) + np.kron(Z1, Z0)

# Define problem
P = picos.Problem()
X = picos.SymmetricVariable("X", 4)

P.set_objective("min", picos.quantkeydist(X))
P.add_constraint(picos.trace(X) == 1)
P.add_constraint((X | Ax) == qx)
P.add_constraint((X | Az) == qz)

# Solve problem
P.solve(solver="qics")

analytic_rate = np.log(2) + (qx*np.log(qx) + qz*np.log(qz))
numerical_rate = P.value

print("Analytic key rate: ", analytic_rate)
print("Numerical key rate:", numerical_rate)
```

Device-independent rates

Making convexity

Device-independent QKD – Eve's attacks

Device-independent QKD – Eve's attacks

Eve can manipulate the transmitted state and measurements

$$\rho_{Q_A Q_B E} \qquad \{M_{a|x}\}_a \qquad \{N_{b|y}\}_b$$

Device-independent QKD – Eve's attacks

Eve can manipulate the transmitted state and measurements

$$\rho_{Q_A Q_B E} \qquad \{M_{a|x}\}_a \qquad \{N_{b|y}\}_b$$

State at end of round

$$\rho_{ABXYE} = \sum_{abxy} p(xy)|abxy\rangle\langle abxy| \otimes \mathrm{Tr}_{Q_A Q_B}[(M_{a|x} \otimes N_{b|y} \otimes \mathbb{I})\rho_{Q_A Q_B E}]$$

Device-independent QKD – Eve's attacks

Eve can manipulate the transmitted state and measurements

$$\rho_{Q_A Q_B E} \qquad \{M_{a|x}\}_a \qquad \{N_{b|y}\}_b$$

State at end of round

$$\rho_{ABXYE} = \sum_{abxy} p(xy)|abxy\rangle\langle abxy| \otimes \mathrm{Tr}_{Q_A Q_B}[(M_{a|x} \otimes N_{b|y} \otimes \mathbb{I})\rho_{Q_A Q_B E}]$$

But she is still constrained...

Device-independent QKD – Eve's attacks

Eve can manipulate the transmitted state and measurements

$$\rho_{Q_A Q_B E} \qquad \{M_{a|x}\}_a \qquad \{N_{b|y}\}_b$$

State at end of round

$$\rho_{ABXYE} = \sum_{abxy} p(xy)|abxy\rangle\langle abxy| \otimes \mathrm{Tr}_{Q_A Q_B}[(M_{a|x} \otimes N_{b|y} \otimes \mathbb{I})\rho_{Q_A Q_B E}]$$

But she is still constrained…

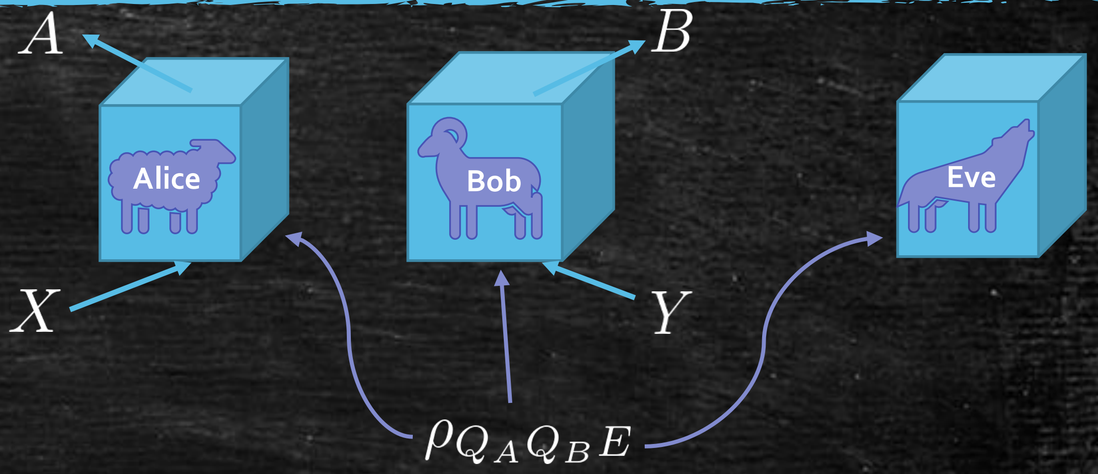
Statistical (e.g. Bell-inequality violation)

$$\mathrm{Tr}[(M_{a|x} \otimes N_{b|y} \otimes I_E)\rho_{Q_A Q_B E}] = p(a,b|x,y)$$

The DI randomness problem

$$\min_{\text{Attacks}} H(A|X=0,E)$$

How much randomness is generated from Alice's device when x=0?



The DI randomness problem

$$\min_{\text{Attacks}} H(A|X=0,E)$$

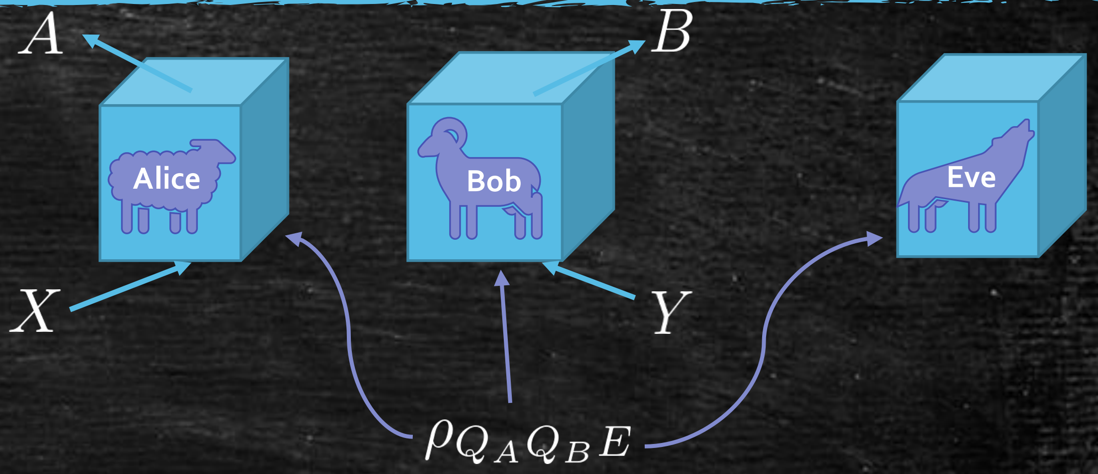
How much randomness is generated from Alice's device when x=0?

Eve is more powerful

$\rho_{Q_A Q_B E}$

$\{M_{a|x}\}$

$\{N_{b|y}\}$

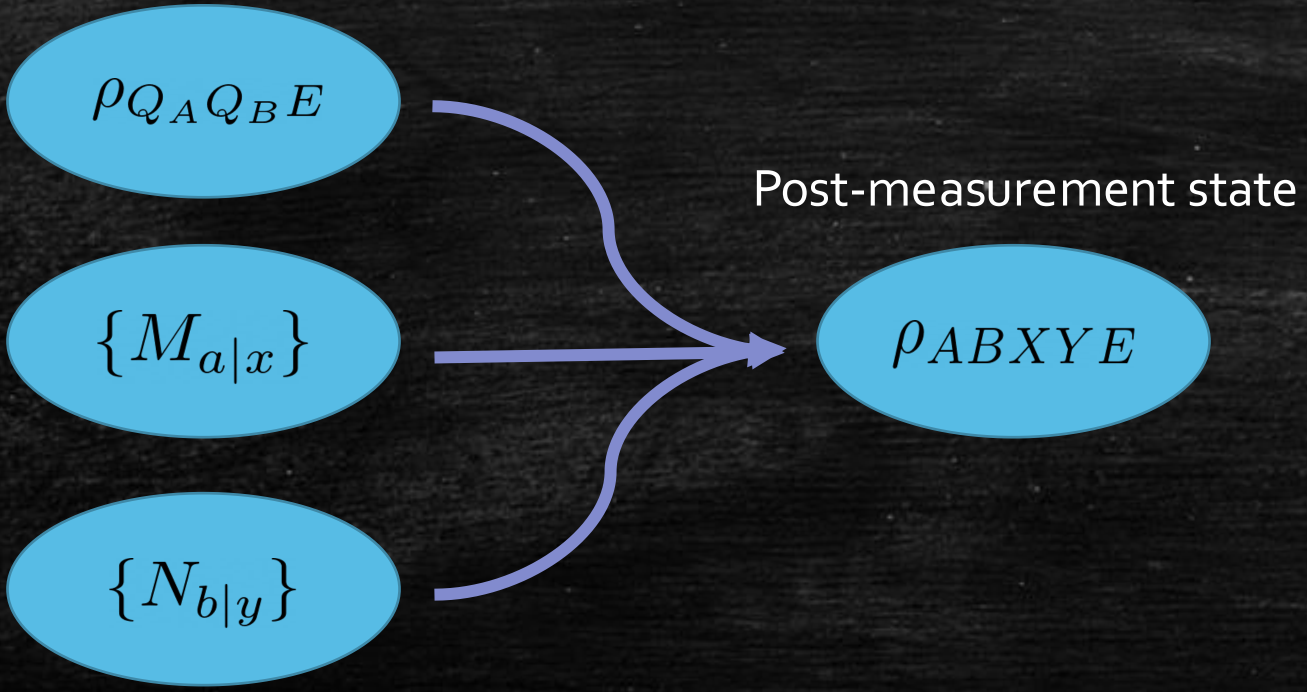


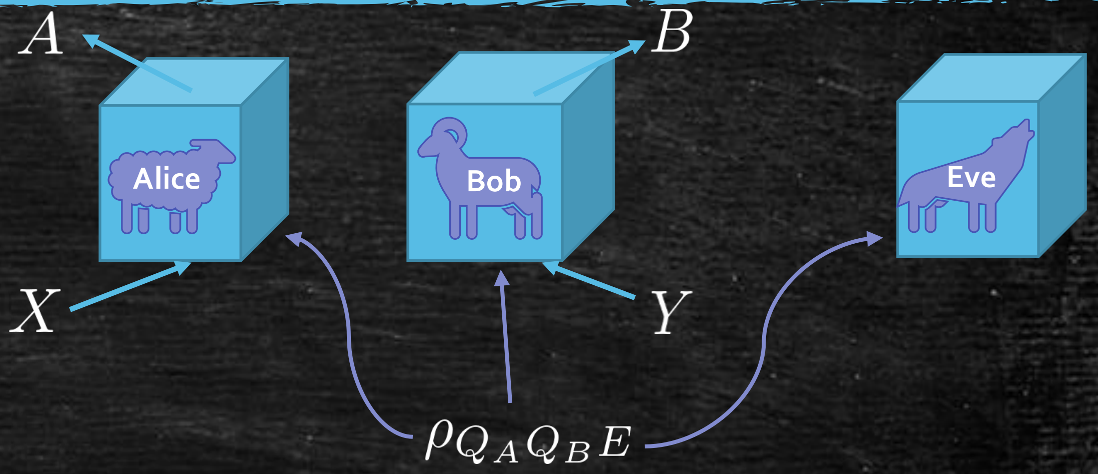
The DI randomness problem

$$\min_{\text{Attacks}} \; H(A|X=0,E)$$

How much randomness is generated from Alice's device when x=0?

Eve is more powerful

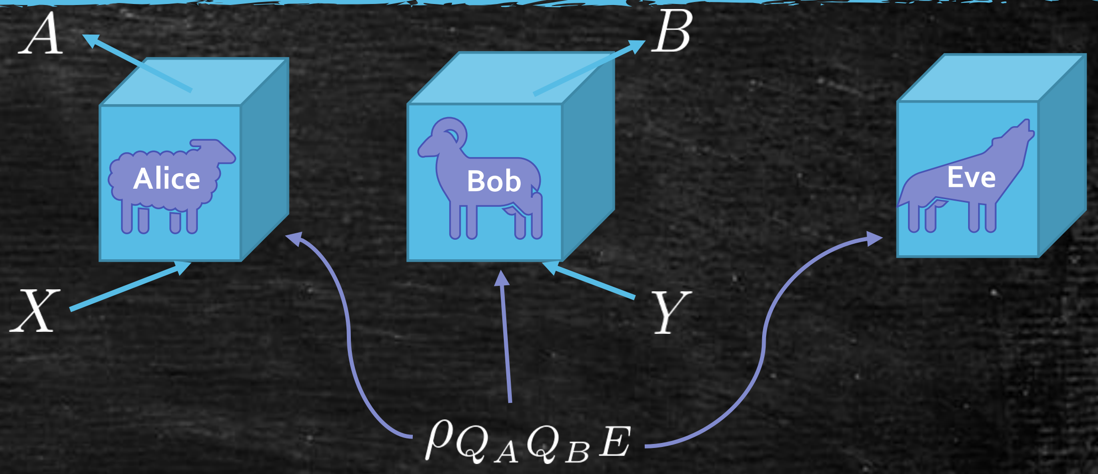




The DI randomness problem

$$\min_{\text{Attacks}} H(A|X=0,E)$$

How much randomness is generated from Alice's device when x=0?



Eve is more powerful

$\rho_{Q_A Q_B E}$

$\{M_{a|x}\}$

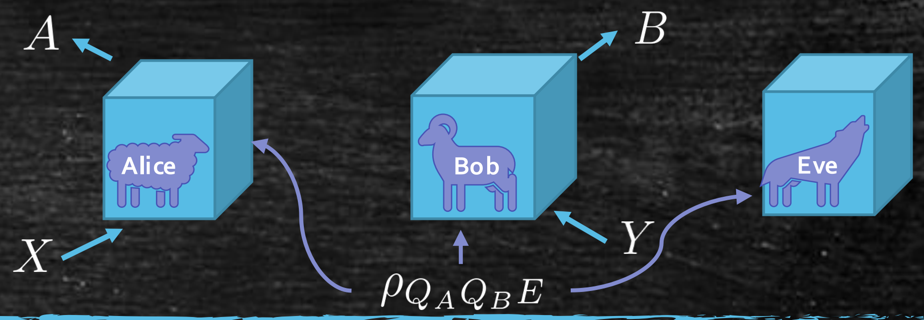
$\{N_{b|y}\}$

Post-measurement state

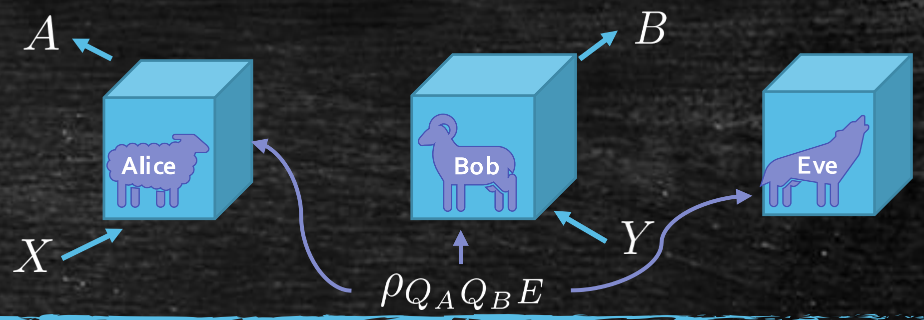
ρ_{ABXYE} $\xrightarrow{H(A|X=0,E)}$

0 $\quad$ $\log(d_A)$

The DI randomness problem



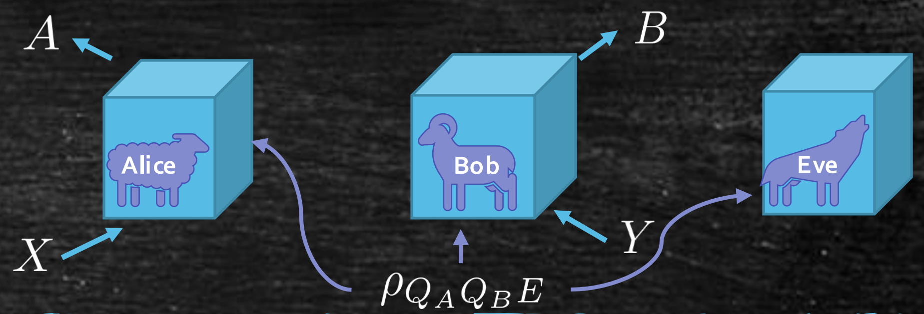
The DI randomness problem



How much randomness is generated from Alice's device when x=0?

$$
\begin{aligned}
f(p) := \min \quad & H(A|X=0,E) \\
\text{s.t.} \quad & \rho_{AE} = \sum_a |a\rangle\langle a| \otimes \mathrm{Tr}_{Q_A Q_B}[(M_{a|0} \otimes I_{Q_B E})\rho_{Q_A Q_B E}] \\
& \mathrm{Tr}[(M_{a|x} \otimes N_{b|y} \otimes I_E)\rho_{Q_A Q_B E}] = p(a,b|x,y) \\
& \rho_{Q_A Q_B E} \succeq 0, \quad M_{a|x} \succeq 0, \quad N_{b|y} \succeq 0 \\
& \mathrm{Tr}[\rho_{Q_A Q_B E}] = 1, \quad \sum_a M_{a|x} = I_A, \quad \sum_b N_{b|y} = I_B
\end{aligned}
$$

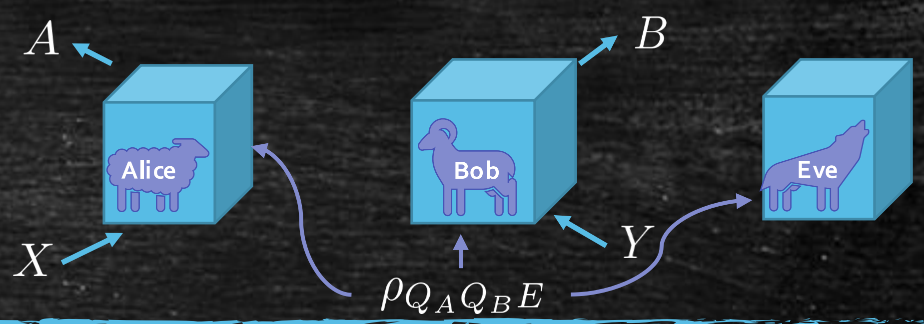
The DI randomness problem



How much randomness is generated from Alice's device when x=0?

$$
\begin{aligned}
f(p) := \min \quad & H(A|X=0,E) \\
\text{s.t.} \quad & \rho_{AE} = \sum_a |a\rangle\langle a| \otimes \mathrm{Tr}_{Q_A Q_B}[(M_{a|0} \otimes I_{Q_B E})\rho_{Q_A Q_B E}] \quad \text{(Post-measurement state)} \\
& \mathrm{Tr}[(M_{a|x} \otimes N_{b|y} \otimes I_E)\rho_{Q_A Q_B E}] = p(a,b|x,y) \\
& \rho_{Q_A Q_B E} \succeq 0, \quad M_{a|x} \succeq 0, \quad N_{b|y} \succeq 0 \\
& \mathrm{Tr}[\rho_{Q_A Q_B E}] = 1, \quad \sum_a M_{a|x} = I_A, \quad \sum_b N_{b|y} = I_B
\end{aligned}
$$

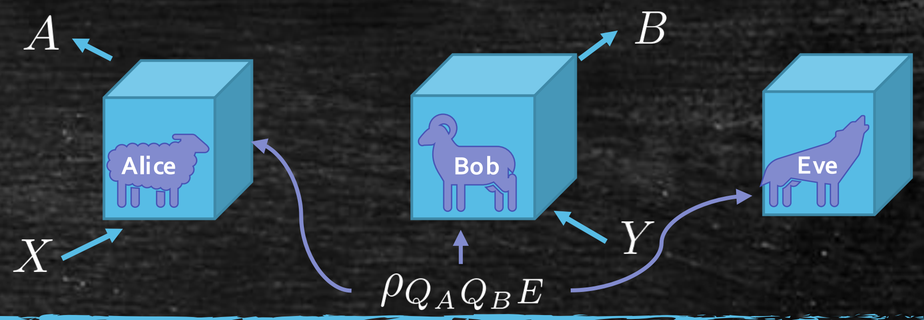
The DI randomness problem



How much randomness is generated from Alice's device when x=0?

$$
\begin{aligned}
f(p) := \min \quad & H(A|X=0,E) \\
\text{s.t.} \quad & \rho_{AE} = \sum_a |a\rangle\langle a| \otimes \mathrm{Tr}_{Q_AQ_B}[(M_{a|0} \otimes I_{Q_BE})\rho_{Q_AQ_BE}] && \text{(Post-measurement state)} \\
& \mathrm{Tr}[(M_{a|x} \otimes N_{b|y} \otimes I_E)\rho_{Q_AQ_BE}] = p(a,b|x,y) && \text{(Statistical constraints)} \\
& \rho_{Q_AQ_BE} \succeq 0, \quad M_{a|x} \succeq 0, \quad N_{b|y} \succeq 0 \\
& \mathrm{Tr}[\rho_{Q_AQ_BE}] = 1, \quad \sum_a M_{a|x} = I_A, \quad \sum_b N_{b|y} = I_B
\end{aligned}
$$

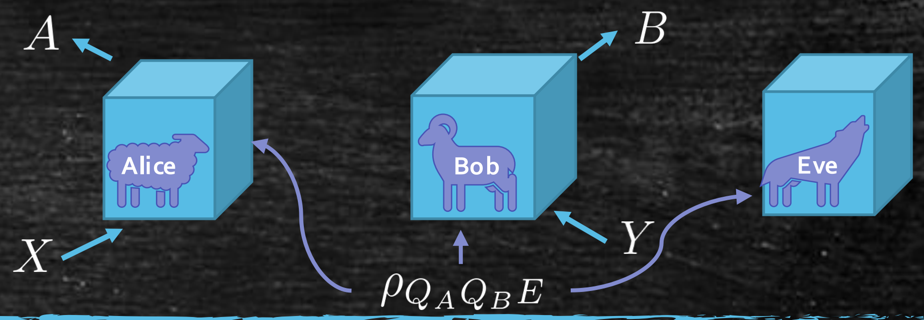
The DI randomness problem



How much randomness is generated from Alice's device when x=0?

$$
\begin{aligned}
f(p) := \min \quad & H(A|X=0,E) \\
\text{s.t.} \quad & \rho_{AE} = \sum_a |a\rangle\langle a| \otimes \mathrm{Tr}_{Q_AQ_B}[(M_{a|0}\otimes I_{Q_BE})\rho_{Q_AQ_BE}] && \text{(Post-measurement state)} \\
& \mathrm{Tr}[(M_{a|x}\otimes N_{b|y}\otimes I_E)\rho_{Q_AQ_BE}] = p(a,b|x,y) && \text{(Statistical constraints)} \\
& \rho_{Q_AQ_BE} \succeq 0, \quad M_{a|x}\succeq 0, \quad N_{b|y}\succeq 0 && \text{(Valid quantum system)} \\
& \mathrm{Tr}[\rho_{Q_AQ_BE}] = 1, \quad \sum_a M_{a|x} = I_A, \quad \sum_b N_{b|y} = I_B
\end{aligned}
$$

The DI randomness problem



How much randomness is generated from Alice's device when x=0?

$$
\begin{aligned}
f(p) := \min \quad & H(A|X=0,E) \\
\text{s.t.} \quad & \rho_{AE} = \sum_a |a\rangle\langle a| \otimes \mathrm{Tr}_{Q_A Q_B}[(M_{a|0} \otimes I_{Q_B E})\rho_{Q_A Q_B E}] \\
& \mathrm{Tr}[(M_{a|x} \otimes N_{b|y} \otimes I_E)\rho_{Q_A Q_B E}] = p(a,b|x,y) \\
& \rho_{Q_A Q_B E} \succeq 0, \quad M_{a|x} \succeq 0, \quad N_{b|y} \succeq 0 \\
& \mathrm{Tr}[\rho_{Q_A Q_B E}] = 1, \quad \sum_a M_{a|x} = I_A, \quad \sum_b N_{b|y} = I_B
\end{aligned}
$$

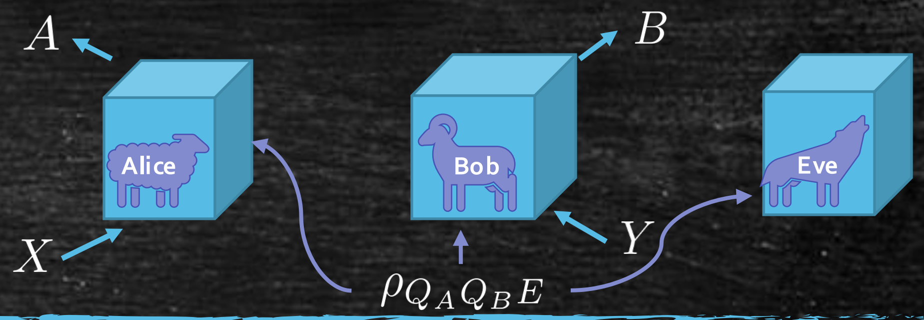
(Post-measurement state)

Can be replaced with *any* linear constraints on p(a,b|x,y).

(Statistical constraints)

(Valid quantum system)

The DI randomness problem



How much randomness is generated from Alice's device when x=0?

$$
\begin{aligned}
f(p) := \min \quad & H(A|X=0,E) \\
\text{s.t.} \quad & \rho_{AE} = \sum_a |a\rangle\langle a| \otimes \mathrm{Tr}_{Q_A Q_B}[(M_{a|0} \otimes I_{Q_B E})\rho_{Q_A Q_B E}] \\
& \mathrm{Tr}[(M_{a|x} \otimes N_{b|y} \otimes I_E)\rho_{Q_A Q_B E}] = p(a,b|x,y) \\
& \rho_{Q_A Q_B E} \succeq 0, \quad M_{a|x} \succeq 0, \quad N_{b|y} \succeq 0 \\
& \mathrm{Tr}[\rho_{Q_A Q_B E}] = 1, \quad \sum_a M_{a|x} = I_A, \quad \sum_b N_{b|y} = I_B
\end{aligned}
$$

(Post-measurement state)

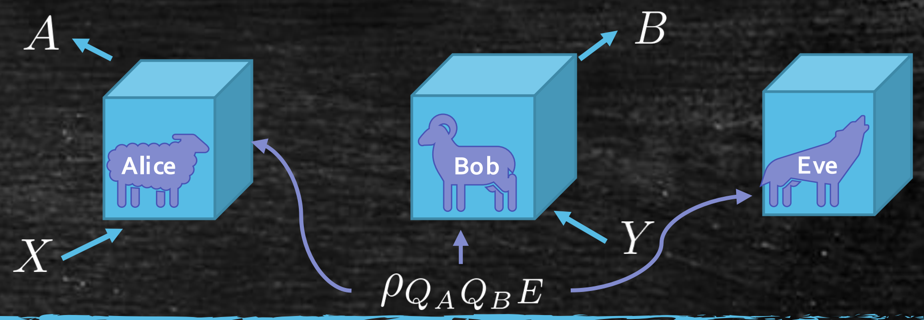
Can be replaced with *any* linear constraints on p(a,b|x,y).

(Statistical constraints)

(Valid quantum system)

Dimension of all quantum systems is unbounded…

The DI randomness problem



How much randomness is generated from Alice's device when x=0?

$$f(p) := \min \quad H(A|X=0,E)$$

$$\text{s.t.} \quad \rho_{AE} = \sum_a |a\rangle\langle a| \otimes \mathrm{Tr}_{Q_A Q_B}[(M_{a|0} \otimes I_{Q_B E})\rho_{Q_A Q_B E}]$$

(Post-measurement state)

Can be replaced with *any* linear constraints on p(a,b|x,y).

$$\mathrm{Tr}[(M_{a|x} \otimes N_{b|y} \otimes I_E)\rho_{Q_A Q_B E}] = p(a,b|x,y)$$

(Statistical constraints)

$$\rho_{Q_A Q_B E} \succeq 0, \quad M_{a|x} \succeq 0, \quad N_{b|y} \succeq 0$$

$$\mathrm{Tr}[\rho_{Q_A Q_B E}] = 1, \quad \sum_a M_{a|x} = I_A, \quad \sum_b N_{b|y} = I_B$$

(Valid quantum system)

Dimension of all quantum systems is unbounded…

…need a new perspective

Toolbox: Polynomial optimization [NPA07, PNA10]

Let's look at a simpler problem:

$$
\begin{aligned}
\max \quad & \mathrm{Tr}[\rho(X_1 X_2 + X_2 X_1)] \\
\text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\
& \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\
& \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0
\end{aligned}
$$

Toolbox: Polynomial optimization [NPA07, PNA10]

Let's look at a simpler problem:

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

Dimension still unbounded

Toolbox: Polynomial optimization [NPA07, PNA10]

Let's look at a simpler problem:

$$\begin{aligned}
\max \quad & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\
\text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\
& \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\
& \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0
\end{aligned}$$

Dimension still unbounded

X are Hermitian

Toolbox: Polynomial optimization [NPA07, PNA10]

Let's look at a simpler problem:

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

Dimension still unbounded

X are Hermitian

Parameter
$\alpha \in [-1, 1]$

Toolbox: Polynomial optimization [NPA07, PNA10]

Let's look at a simpler problem:

$$
\begin{aligned}
\max \quad & \mathrm{Tr}[\rho(X_1X_2+X_2X_1)] \\
\text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\
& \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\
& \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0
\end{aligned}
$$

Dimension still unbounded

X are Hermitian

Parameter
$\alpha \in [-1, 1]$

Need a dimension-free compressed representation of a system...

Toolbox: Polynomial optimization [NPA07, PNA10]

Let's look at a simpler problem:

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1 X_2 + X_2 X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

Dimension still unbounded

X are Hermitian

Parameter
$\alpha \in [-1, 1]$

Need a dimension-free compressed representation of a system…

… re-express everything in terms of moments! $\mathrm{Tr}[\rho X^m]$

Toolbox: Polynomial optimization

Building a moment matrix:

1. Gather the operators of your problem

$$\{I, X_1, X_2\}$$

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1 X_2 + X_2 X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

Toolbox: Polynomial optimization

Building a moment matrix:

1. Gather the operators of your problem

$$\{I, X_1, X_2\}$$

2. Index a matrix with the operators, the (X,Y) entry represents

$$\mathrm{Tr}[\rho X^\dagger Y]$$

$$\begin{aligned}
\max \quad & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\
\text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\
& \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\
& \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0
\end{aligned}$$

Toolbox: Polynomial optimization

Building a moment matrix:

1. Gather the operators of your problem

$$\{I, X_1, X_2\}$$

2. Index a matrix with the operators, the (X,Y) entry represents

$$\mathrm{Tr}[\rho X^\dagger Y]$$

$$\begin{array}{ll} \max & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{array}$$

Compressed representation of the system
Infinite dimensions -> 3x3

$$\begin{array}{c c} & \begin{array}{ccc} I & X_1 & X_2 \end{array} \\ \begin{array}{c} I \\ X_1 \\ X_2 \end{array} & \begin{pmatrix} \mathrm{Tr}[\rho] & \mathrm{Tr}[\rho X_1] & \mathrm{Tr}[\rho X_2] \\ \mathrm{Tr}[\rho X_1^\dagger] & \mathrm{Tr}[\rho X_1^\dagger X_1] & \mathrm{Tr}[\rho X_1^\dagger X_2] \\ \mathrm{Tr}[\rho X_2^\dagger] & \mathrm{Tr}[\rho X_2^\dagger X_1] & \mathrm{Tr}[\rho X_2^\dagger X_2] \end{pmatrix} \end{array}$$

Toolbox: Polynomial optimization

Building a moment matrix:

1. Gather the operators of your problem

$$\{I, X_1, X_2\}$$

2. Index a matrix with the operators, the (X,Y) entry represents

$$\mathrm{Tr}[\rho X^\dagger Y]$$

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

Compressed representation of the system
Infinite dimensions -> 3x3

$$\begin{array}{c|ccc} & I & X_1 & X_2 \\ \hline I & \mathrm{Tr}[\rho] & \mathrm{Tr}[\rho X_1] & \mathrm{Tr}[\rho X_2] \\ X_1 & \mathrm{Tr}[\rho X_1] & \mathrm{Tr}[\rho X_1^2] & \mathrm{Tr}[\rho X_1 X_2] \\ X_2 & \mathrm{Tr}[\rho X_2] & \mathrm{Tr}[\rho X_2 X_1] & \mathrm{Tr}[\rho X_2^2] \end{array}$$

We can simplify!

- Hermitian X

Toolbox: Polynomial optimization

Building a moment matrix:

1. Gather the operators of your problem

$$\{I, X_1, X_2\}$$

2. Index a matrix with the operators, the (X,Y) entry represents

$$\mathrm{Tr}[\rho X^\dagger Y]$$

$$\begin{array}{ll} \max & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{array}$$

Compressed representation of the system
Infinite dimensions -> 3x3

$$\begin{array}{c|c} & \begin{array}{ccc} I & X_1 & X_2 \end{array} \\ \begin{array}{c} I \\ X_1 \\ X_2 \end{array} & \begin{pmatrix} 1 & \mathrm{Tr}[\rho X_1] & \mathrm{Tr}[\rho X_2] \\ \mathrm{Tr}[\rho X_1] & \mathrm{Tr}[\rho X_1^2] & \mathrm{Tr}[\rho X_1 X_2] \\ \mathrm{Tr}[\rho X_2] & \mathrm{Tr}[\rho X_2 X_1] & \mathrm{Tr}[\rho X_2^2] \end{pmatrix} \end{array}$$

We can simplify!

- Hermitian X
- Tr[rho] = 1

Toolbox: Polynomial optimization

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

Building a moment matrix:

1. Gather the operators of your problem

$$\{I, X_1, X_2\}$$

2. Index a matrix with the operators, the (X,Y) entry represents

$$\mathrm{Tr}[\rho X^\dagger Y]$$

Compressed representation of the system
Infinite dimensions -> 3x3

$$\begin{array}{c} \\ I \\ X_1 \\ X_2 \end{array} \begin{array}{c} \begin{array}{ccc} I & X_1 & X_2 \end{array} \\ \begin{pmatrix} 1 & \alpha & \mathrm{Tr}[\rho X_2] \\ \alpha & \mathrm{Tr}[\rho X_1^2] & \mathrm{Tr}[\rho X_1 X_2] \\ \mathrm{Tr}[\rho X_2] & \mathrm{Tr}[\rho X_2 X_1] & \mathrm{Tr}[\rho X_2^2] \end{pmatrix} \end{array}$$

We can simplify!

- Hermitian X
- Tr[rho] = 1
- Tr[rho X1] = a

Toolbox: Polynomial optimization

Building a moment matrix:

1. Gather the operators of your problem

$$\{I, X_1, X_2\}$$

2. Index a matrix with the operators, the (X,Y) entry represents

$$\mathrm{Tr}[\rho X^\dagger Y]$$

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

Compressed representation of the system

Infinite dimensions -> 3x3

$$\begin{array}{cc} & \begin{array}{ccc} I & X_1 & X_2 \end{array} \\ \begin{array}{c} I \\ X_1 \\ X_2 \end{array} & \begin{pmatrix} 1 & \alpha & 0 \\ \alpha & \mathrm{Tr}[\rho X_1^2] & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & \mathrm{Tr}[\rho X_2^2] \end{pmatrix} \end{array}$$

We can simplify!

- Hermitian X
- Tr[rho] = 1
- Tr[rho X1] = a
- Tr[rho X2] = 0

Toolbox: Polynomial optimization

Building a moment matrix:

1. Gather the operators of your problem

$$\{I, X_1, X_2\}$$

2. Index a matrix with the operators, the (X,Y) entry represents

$$\mathrm{Tr}[\rho X^\dagger Y]$$

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

Compressed representation of the system
Infinite dimensions -> 3x3

$$\begin{array}{c c} & \begin{array}{ccc} I & X_1 & X_2 \end{array} \\ \begin{array}{c} I \\ X_1 \\ X_2 \end{array} & \begin{pmatrix} 1 & \alpha & 0 \\ \alpha & \mathrm{Tr}[\rho] & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & \mathrm{Tr}[\rho] \end{pmatrix} \end{array}$$

We can simplify!

- Hermitian X
- Tr[rho] = 1
- Tr[rho X1] = a
- Tr[rho X2] = 0
- Xi^2 = Id

Toolbox: Polynomial optimization

Building a moment matrix:

1. Gather the operators of your problem

$$\{I, X_1, X_2\}$$

2. Index a matrix with the operators, the (X,Y) entry represents

$$\mathrm{Tr}[\rho X^\dagger Y]$$

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

Compressed representation
of the system
Infinite dimensions -> 3x3

$$\begin{array}{c} \\ I \\ X_1 \\ X_2 \end{array} \begin{array}{c} \begin{array}{ccc} I & X_1 & X_2 \end{array} \\ \begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & 1 \end{pmatrix} \end{array}$$

We can simplify!

- Hermitian X
- Tr[rho] = 1
- Tr[rho X1] = a
- Tr[rho X2] = 0
- Xi^2 = Id
- Tr[rho] = 1

Toolbox: Polynomial optimization

Any **feasible** quantum system has a moment matrix of the form

$$\begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & 1 \end{pmatrix}$$

Toolbox: Polynomial optimization

Any **feasible** quantum system has a moment matrix of the form

$$\begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & 1 \end{pmatrix} \succeq 0$$

Important: Moment matrices are ***always*** positive semidefinite.

Toolbox: Polynomial optimization

Any **feasible** quantum system has a moment matrix of the form

$$\begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & 1 \end{pmatrix} \succeq 0$$

Important: Moment matrices are ***always*** positive semidefinite.

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1 X_2 + X_2 X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

Toolbox: Polynomial optimization

Any **feasible** quantum system has a moment matrix of the form

$$\begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & 1 \end{pmatrix} \succeq 0$$

Important: Moment matrices are ***always*** positive semidefinite.

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1 X_2 + X_2 X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

$$\begin{aligned} \max \quad & u + \overline{u} \\ \text{s.t.} \quad & \begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & u \\ 0 & \overline{u} & 1 \end{pmatrix} \succeq 0 \end{aligned}$$

Toolbox: Polynomial optimization

Any **feasible** quantum system has a moment matrix of the form

$$\begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & 1 \end{pmatrix} \succeq 0$$

Important: Moment matrices are ***always*** positive semidefinite.

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1 X_2 + X_2 X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned} \quad \leq \quad \begin{aligned} \max \quad & u + \overline{u} \\ \text{s.t.} \quad & \begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & u \\ 0 & \overline{u} & 1 \end{pmatrix} \succeq 0 \end{aligned}$$

Toolbox: Polynomial optimization

Any **feasible** quantum system has a moment matrix of the form

$$\begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & 1 \end{pmatrix} \succeq 0$$

Important: Moment matrices are ***always*** positive semidefinite.

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1 X_2 + X_2 X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned} \quad \leq \quad \begin{aligned} \max \quad & u + \overline{u} \\ \text{s.t.} \quad & \begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & u \\ 0 & \overline{u} & 1 \end{pmatrix} \succeq 0 \end{aligned}$$

Not tight
in general

Toolbox: Polynomial optimization

Any **feasible** quantum system has a moment matrix of the form

$$\begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & 1 \end{pmatrix} \succeq 0$$

Important: Moment matrices are ***always*** positive semidefinite.

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

$$\leq$$

Not tight
in general

$$\begin{aligned} \max \quad & u + \overline{u} \\ \text{s.t.} \quad & \begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & u \\ 0 & \overline{u} & 1 \end{pmatrix} \succeq 0 \end{aligned}$$

Semidefinite program (SDP)
- Efficient algorithms
- Guaranteed optima

Toolbox: Polynomial optimization

Any **feasible** quantum system has a moment matrix of the form

$$\begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & 1 \end{pmatrix} \succeq 0$$

Important: Moment matrices are ***always*** positive semidefinite.

$$\begin{array}{ll} \max & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{array} \quad \leq \quad \begin{array}{ll} \max & u + \overline{u} \\ \text{s.t.} & \begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & u \\ 0 & \overline{u} & 1 \end{pmatrix} \succeq 0 \end{array}$$

Not tight
in general

Semidefinite program (SDP)
- Efficient algorithms
- Guaranteed optima

$$u = \sqrt{1 - \alpha^2}$$

Toolbox: Polynomial optimization

Any **feasible** quantum system has a moment matrix of the form

$$\begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & \mathrm{Tr}[\rho X_1 X_2] \\ 0 & \mathrm{Tr}[\rho X_2 X_1] & 1 \end{pmatrix} \succeq 0$$

Important: Moment matrices are ***always*** positive semidefinite.

$$\begin{aligned} \max \quad & \mathrm{Tr}[\rho(X_1X_2 + X_2X_1)] \\ \text{s.t.} \quad & X_1^2 = I, \qquad X_2^2 = I \\ & \mathrm{Tr}[\rho X_1] = \alpha, \qquad \mathrm{Tr}[\rho X_2] = 0 \\ & \mathrm{Tr}[\rho] = 1, \qquad \rho \succeq 0 \end{aligned}$$

$$\leq$$

Not tight
in general

$$\begin{aligned} \max \quad & u + \overline{u} \\ \text{s.t.} \quad & \begin{pmatrix} 1 & \alpha & 0 \\ \alpha & 1 & u \\ 0 & \overline{u} & 1 \end{pmatrix} \succeq 0 \end{aligned}$$

Achievable!

$$\rho = |0\rangle\langle 0| \qquad X_1 = \alpha\sigma_Z + \sqrt{1-\alpha^2}\,\sigma_X$$
$$X_2 = \sigma_X$$

Semidefinite program (SDP)
- Efficient algorithms
- Guaranteed optima

$$u = \sqrt{1-\alpha^2}$$

Toolbox: Polynomial optimization

- Moment matrix method gives SDP relaxations.

Toolbox: Polynomial optimization

- Moment matrix method gives SDP relaxations.
- Better relaxations possible with larger indexing sets

$$\{I, X_1, X_2, X_1^2, X_1X_2, X_2X_1, X_2^2\}$$

"Level 2" relaxation

Toolbox: Polynomial optimization

- Moment matrix method gives SDP relaxations.
- Better relaxations possible with larger indexing sets

$$\{I, X_1, X_2, X_1^2, X_1X_2, X_2X_1, X_2^2\}$$

"Level 2" relaxation

- Relaxations converge to actual optima under mild conditions

Bounded operators sufficient

Toolbox: Polynomial optimization

- Moment matrix method gives SDP relaxations.
- Better relaxations possible with larger indexing sets

$$\{I, X_1, X_2, X_1^2, X_1X_2, X_2X_1, X_2^2\}$$

"Level 2" relaxation

- Relaxations converge to actual optima under mild conditions

Bounded operators sufficient

- Applies to very general polynomial problems

$$\begin{aligned} \max / \min \quad & \mathrm{Tr}[\rho\, P(X_1, \ldots, X_n)] \\ & \mathrm{Tr}[\rho\, Q_i(X_1, \ldots, X_n)] \leq q_i \\ & R_j(X_1, \ldots, X_n) \succeq 0 \\ & \rho \succeq 0 \end{aligned}$$

Expectation of polynomial

Equalities and inequalities

Operator constraints

Toolbox: Polynomial optimization

- Moment matrix method gives SDP relaxations.
- Better relaxations possible with larger indexing sets

$$\{I, X_1, X_2, X_1^2, X_1X_2, X_2X_1, X_2^2\}$$

"Level 2" relaxation

- Relaxations converge to actual optima under mild conditions

Bounded operators sufficient

- Applies to very general polynomial problems

$$\begin{aligned} \max / \min \quad & \mathrm{Tr}[\rho\, P(X_1, \dots, X_n)] \\ & \mathrm{Tr}[\rho\, Q_i(X_1, \dots, X_n)] \leq q_i \\ & R_j(X_1, \dots, X_n) \succeq 0 \\ & \rho \succeq 0 \end{aligned}$$

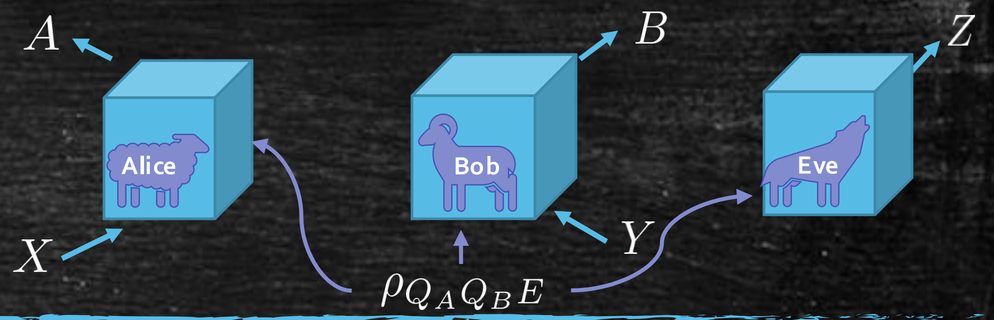
Expectation of polynomial

Equalities and inequalities

Operator constraints

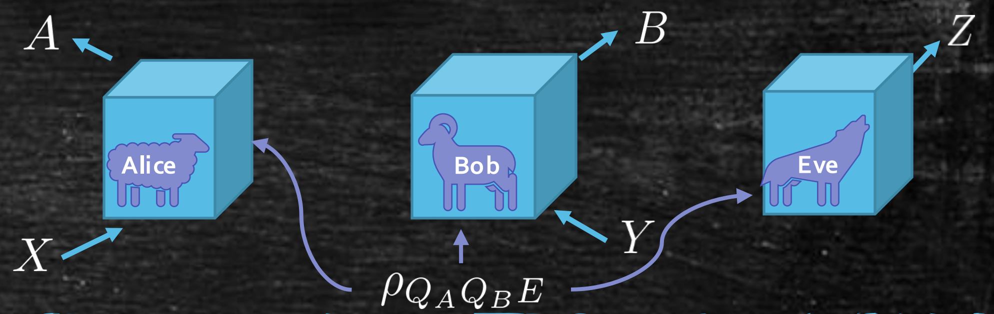
Lots of applications
beyond DI cryptography
Review [TPBA24]

Simple DI key-rate bounds



The von Neumann entropy is complicated, so let's make things easier

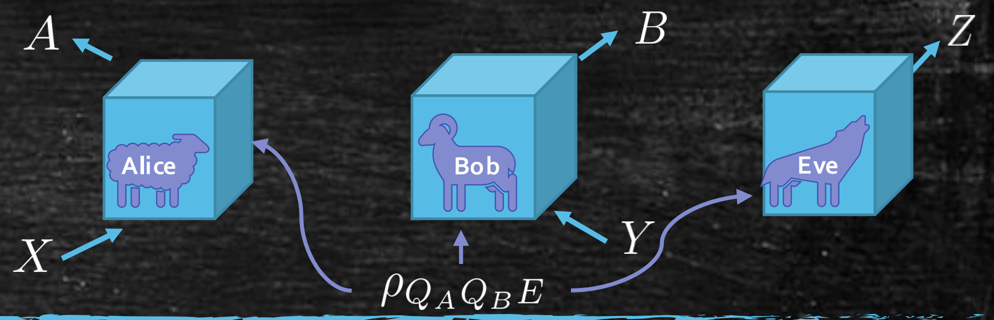
Simple DI key-rate bounds



The von Neumann entropy is complicated, so let's make things easier

$$\min_{\text{Attacks}} H(A|X=0,E) \geq \min_{\text{attacks}} H_{\min}(A|X=0,E)$$

Simple DI key-rate bounds

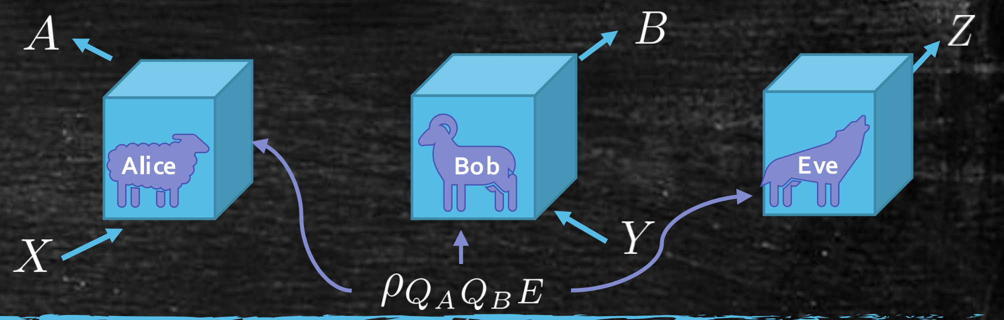


The von Neumann entropy is complicated, so let's make things easier

$$\min_{\text{Attacks}} H(A|X=0,E) \geq \min_{\text{attacks}} H_{\min}(A|X=0,E)$$

$$= \min_{\text{attacks}} -\log P_{\text{guess}}(A|X=0,E)$$

Simple DI key-rate bounds



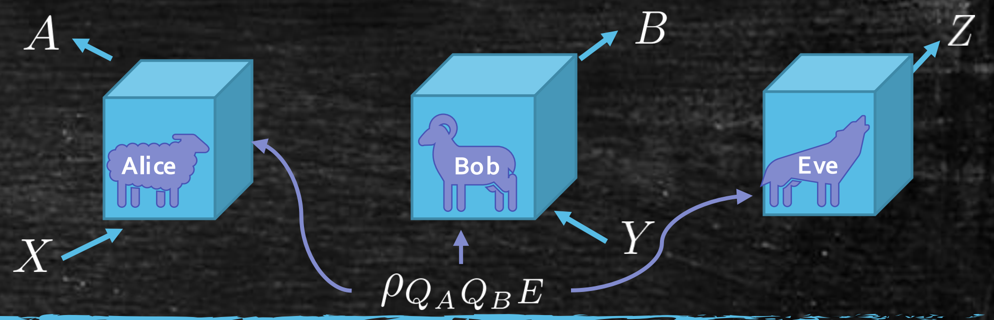
The von Neumann entropy is complicated, so let's make things easier

$$\min_{\text{Attacks}} H(A|X=0,E) \geq \min_{\text{attacks}} H_{\min}(A|X=0,E)$$

$$= \min_{\text{attacks}} -\log P_{\text{guess}}(A|X=0,E)$$

$$= -\log \max_{\text{attacks}} P_{\text{guess}}(A|X=0,E)$$

Simple DI key-rate bounds



The von Neumann entropy is complicated, so let's make things easier

$$\min_{\text{Attacks}} H(A|X=0,E) \geq \min_{\text{attacks}} H_{\min}(A|X=0,E)$$

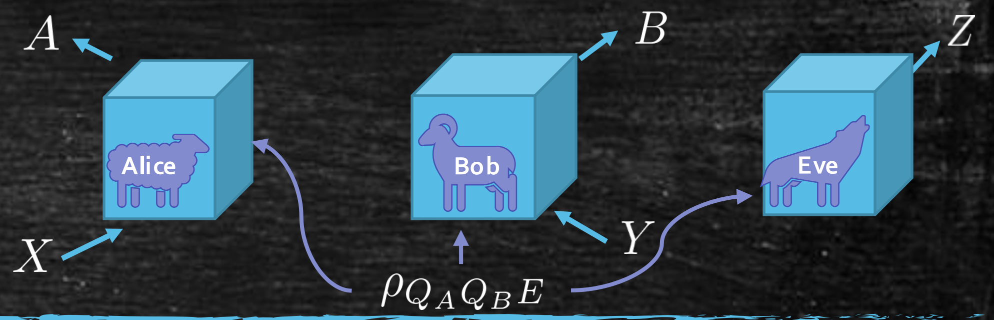
$$= \min_{\text{attacks}} -\log P_{\text{guess}}(A|X=0,E)$$

$$= -\log \max_{\text{attacks}} P_{\text{guess}}(A|X=0,E)$$

So we will try to solve

$$\max_{\text{attacks}} P_{\text{guess}}(A|X=0,E)$$

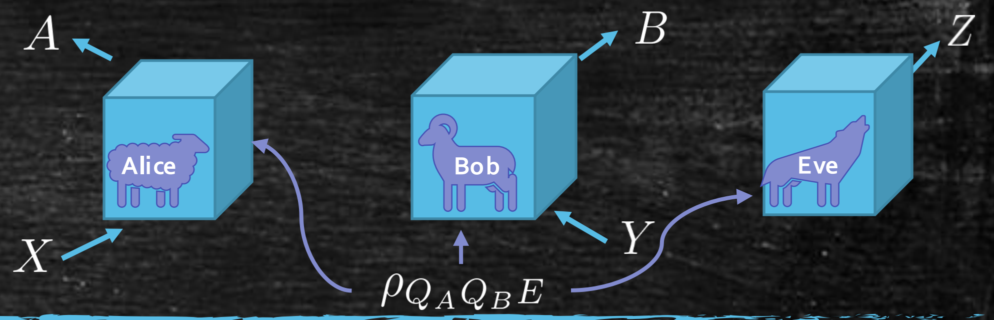
CHSH example



Guessing probability problem

$$
\begin{aligned}
g(\omega) := \max \quad & \sum_a \mathrm{Tr}[(M_{a|0} \otimes I_B \otimes Z_a)\rho_{Q_A Q_B E}] \\
\text{s.t.} \quad & \frac{1}{4} \sum_{a \oplus b = xy} \mathrm{Tr}[(M_{a|x} \otimes N_{b|y} \otimes I_E)\rho_{Q_A Q_B E}] = \omega \\
& \rho_{Q_A Q_B E} \succeq 0, \quad M_{a|x} \succeq 0, \quad N_{b|y} \succeq 0, \quad Z_c \succeq 0 \\
& \mathrm{Tr}[\rho_{Q_A Q_B E}] = 1, \quad \sum_a M_{a|x} = I_A, \quad \sum_b N_{b|y} = I_B, \quad \sum_c Z_c = I_E
\end{aligned}
$$

CHSH example



Guessing probability problem

$$g(\omega) := \max \sum_a \mathrm{Tr}[(M_{a|0} \otimes I_B \otimes Z_a)\rho_{Q_A Q_B E}]$$

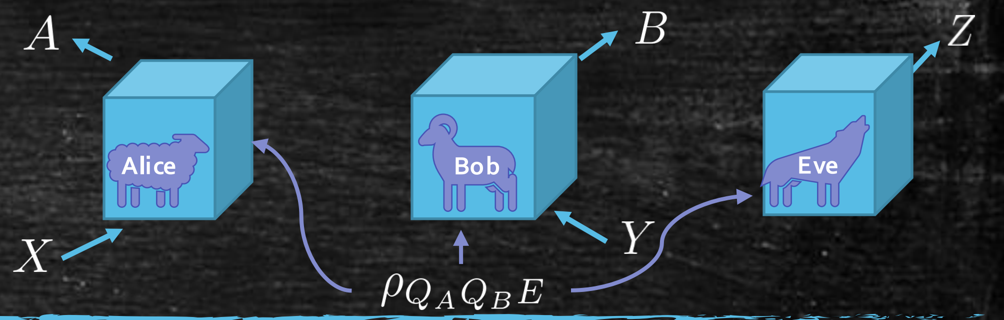
$$\text{s.t.} \quad \frac{1}{4} \sum_{a \oplus b = xy} \mathrm{Tr}[(M_{a|x} \otimes N_{b|y} \otimes I_E)\rho_{Q_A Q_B E}] = \omega$$

$$\rho_{Q_A Q_B E} \succeq 0, \quad M_{a|x} \succeq 0, \quad N_{b|y} \succeq 0, \quad Z_c \succeq 0$$

$$\mathrm{Tr}[\rho_{Q_A Q_B E}] = 1, \quad \sum_a M_{a|x} = I_A, \quad \sum_b N_{b|y} = I_B, \quad \sum_c Z_c = I_E$$

Not quite a polynomial problem yet

CHSH example



Guessing probability problem

$$g(\omega) := \max \sum_a \mathrm{Tr}[(M_{a|0} \otimes I_B \otimes Z_a)\rho_{Q_A Q_B E}]$$

$$\text{s.t.} \quad \frac{1}{4} \sum_{a \oplus b = xy} \mathrm{Tr}[(M_{a|x} \otimes N_{b|y} \otimes I_E)\rho_{Q_A Q_B E}] = \omega$$

$$\rho_{Q_A Q_B E} \succeq 0, \quad M_{a|x} \succeq 0, \quad N_{b|y} \succeq 0, \quad Z_c \succeq 0$$

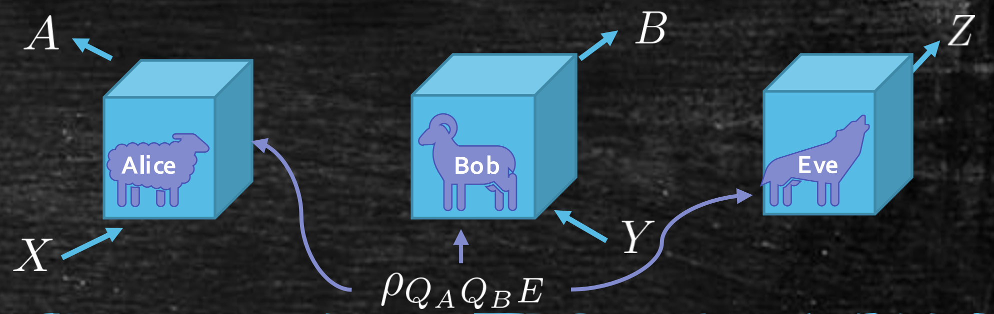
$$\mathrm{Tr}[\rho_{Q_A Q_B E}] = 1, \quad \sum_a M_{a|x} = I_A, \quad \sum_b N_{b|y} = I_B, \quad \sum_c Z_c = I_E$$

Not quite a polynomial problem yet

Need to "forget" the tensor product

$$\widehat{M}_{a|x} = M_{a|x} \otimes I_{Q_B} \otimes I_E \qquad \hat{N}_{b|y} = I_{Q_A} \otimes N_{b|y} \otimes I_E \qquad \hat{Z}_c = I_{Q_A} \otimes I_{Q_B} \otimes Z_c$$

CHSH example



Guessing probability problem

$$g(\omega) \leq \max \sum_a \mathrm{Tr}[\widehat{M}_{a|0} \hat{Z}_a \rho]$$

Not quite a polynomial problem yet

$$\text{s.t.} \quad \frac{1}{4} \sum_{a \oplus b = xy} \mathrm{Tr}[\widehat{M}_{a|x} \hat{N}_{b|y} \rho] = \omega$$

$$\rho \succeq 0, \quad \widehat{M}_{a|x} \succeq 0, \quad \hat{N}_{b|y} \succeq 0, \quad \hat{Z}_c \succeq 0$$

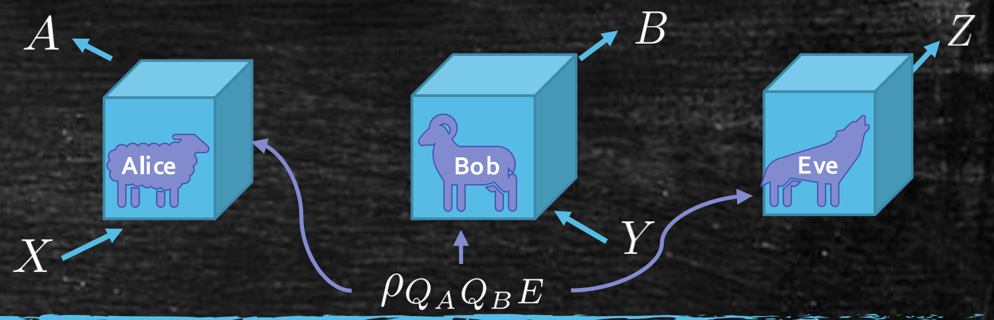
$$\mathrm{Tr}[\rho] = 1, \quad \sum_a \widehat{M}_{a|x} = I, \quad \sum_b \hat{N}_{b|y} = I, \quad \sum_c \hat{Z}_c = I$$

$$[\widehat{M}_{a|x}, \hat{N}_{b|y}] = 0, \quad [\widehat{M}_{a|x}, \hat{Z}_c] = 0, \quad [\hat{N}_{b|y}, Z_c] = 0$$

Need to "forget" the tensor product

$$\widehat{M}_{a|x} = M_{a|x} \otimes I_{Q_B} \otimes I_E \qquad \hat{N}_{b|y} = I_{Q_A} \otimes N_{b|y} \otimes I_E \qquad \hat{Z}_c = I_{Q_A} \otimes I_{Q_B} \otimes Z_c$$

CHSH example



Guessing probability problem

$$g(\omega) \leq \max \sum_a \mathrm{Tr}[\widehat{M}_{a|0} \widehat{Z}_a \rho]$$

$$\text{s.t.} \quad \frac{1}{4} \sum_{a \oplus b = xy} \mathrm{Tr}[\widehat{M}_{a|x} \widehat{N}_{b|y} \rho] = \omega$$

Not quite a polynomial problem yet

$$\rho \succeq 0, \quad \widehat{M}_{a|x} \succeq 0, \quad \widehat{N}_{b|y} \succeq 0, \quad \widehat{Z}_c \succeq 0$$

$$\mathrm{Tr}[\rho] = 1, \quad \sum_a \widehat{M}_{a|x} = I, \quad \sum_b \widehat{N}_{b|y} = I, \quad \sum_c \widehat{Z}_c = I$$

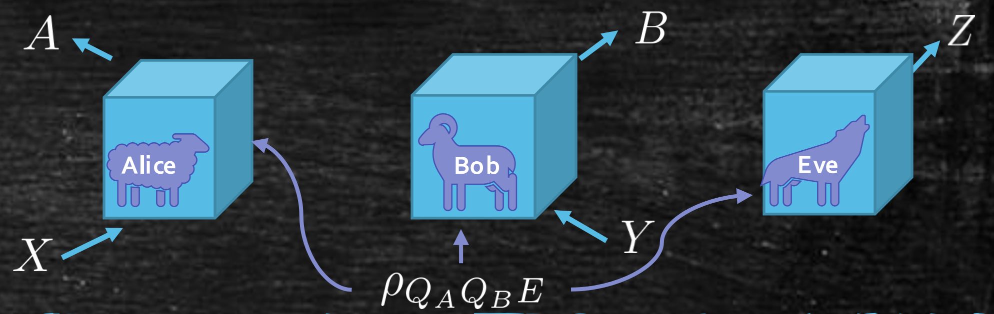
$$[\widehat{M}_{a|x}, \widehat{N}_{b|y}] = 0, \quad [\widehat{M}_{a|x}, \widehat{Z}_c] = 0, \quad [\widehat{N}_{b|y}, Z_c] = 0$$

Relaxes the tensor product constraint.

Need to "forget" the tensor product

$$\widehat{M}_{a|x} = M_{a|x} \otimes I_{Q_B} \otimes I_E \qquad \widehat{N}_{b|y} = I_{Q_A} \otimes N_{b|y} \otimes I_E \qquad \widehat{Z}_c = I_{Q_A} \otimes I_{Q_B} \otimes Z_c$$

CHSH example



Guessing probability problem

$$g(\omega) \leq \max \sum_a \mathrm{Tr}[\widehat{M}_{a|0} \widehat{Z}_a \rho]$$

Not quite a polynomial problem yet

$$\text{s.t.} \quad \frac{1}{4} \sum_{a \oplus b = xy} \mathrm{Tr}[\widehat{M}_{a|x} \widehat{N}_{b|y} \rho] = \omega$$

$$\rho \succeq 0, \quad \widehat{M}_{a|x} \succeq 0, \quad \widehat{N}_{b|y} \succeq 0, \quad \widehat{Z}_c \succeq 0$$

Now we have a polynomial problem!

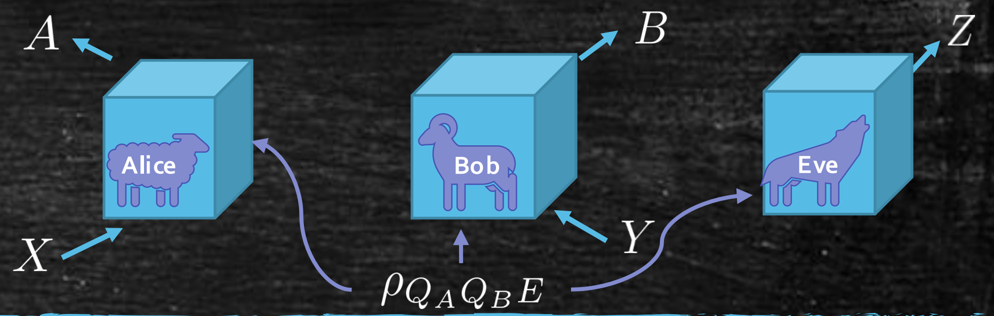
$$\mathrm{Tr}[\rho] = 1, \quad \sum_a \widehat{M}_{a|x} = I, \quad \sum_b \widehat{N}_{b|y} = I, \quad \sum_c \widehat{Z}_c = I$$

$$[\widehat{M}_{a|x}, \widehat{N}_{b|y}] = 0, \quad [\widehat{M}_{a|x}, \widehat{Z}_c] = 0, \quad [\widehat{N}_{b|y}, Z_c] = 0$$

Relaxes the tensor product constraint.

Need to "forget" the tensor product

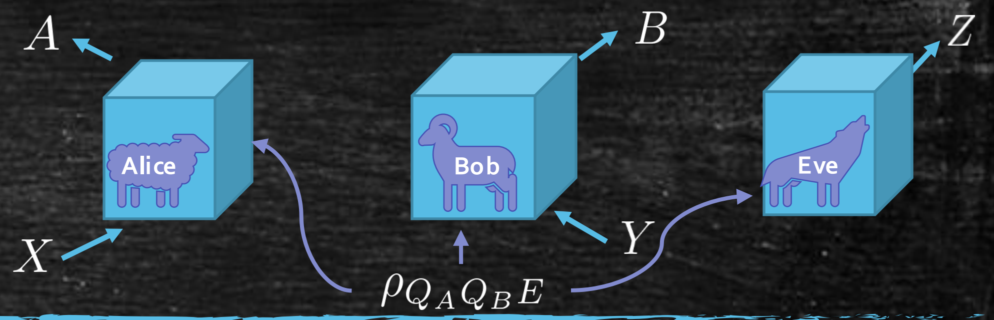
$$\widehat{M}_{a|x} = M_{a|x} \otimes I_{Q_B} \otimes I_E \qquad \widehat{N}_{b|y} = I_{Q_A} \otimes N_{b|y} \otimes I_E \qquad \widehat{Z}_c = I_{Q_A} \otimes I_{Q_B} \otimes Z_c$$



CHSH example

DI rates are also easy to compute

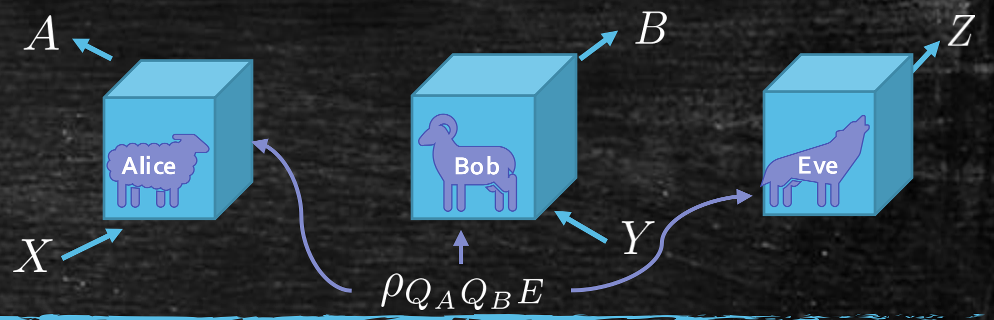
CHSH example



DI rates are also easy to compute

Name	Language	Code
PCPOP.jl	Julia	https://abh1mishra.github.io/PCPOP.jl/dev/
moment	Matlab	https://github.com/ajpgarner/moment
ncpoleon	Python	https://github.com/ncpoleon/ncpoleon

CHSH example



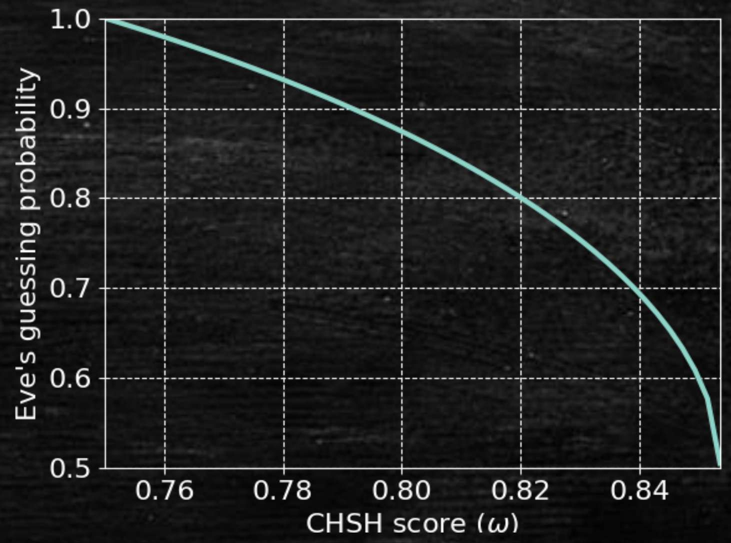
DI rates are also easy to compute

Name	Language	Code
PCPOP.jl	Julia	https://abh1mishra.github.io/PCPOP.jl/dev/
moment	Matlab	https://github.com/ajpgarner/moment
ncpoleon	Python	https://github.com/ncpoleon/ncpoleon

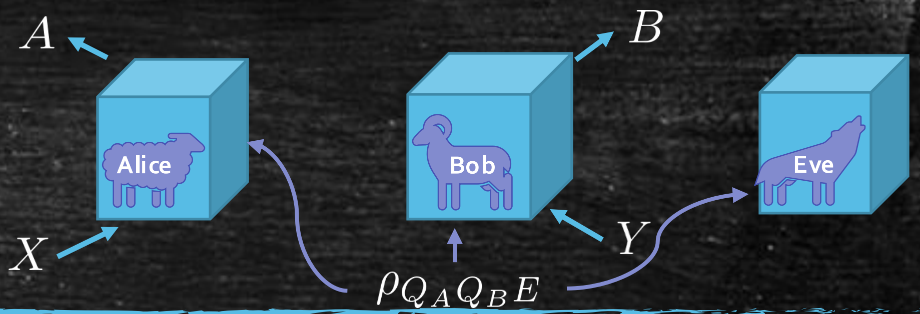
Running the numerics we find:

- Level 1 is not sufficient
- Level 2 gives optimal bound [MPA11]

$$g(\omega) = \frac{1 + \sqrt{2 - (8\omega - 4)^2/4}}{2}$$



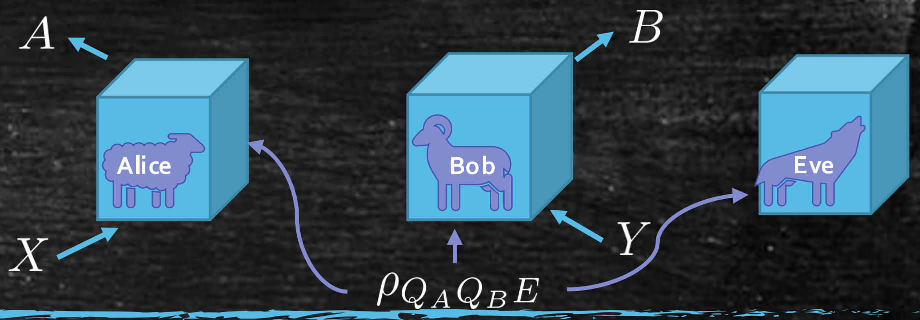
Min vs. von Neumann entropy



Guessing probability gives us a min-entropy bound

$$\min_{\text{Attacks}} H_{\min}(A|X=0,E) \geq -\log g(\omega)$$

Min vs. von Neumann entropy

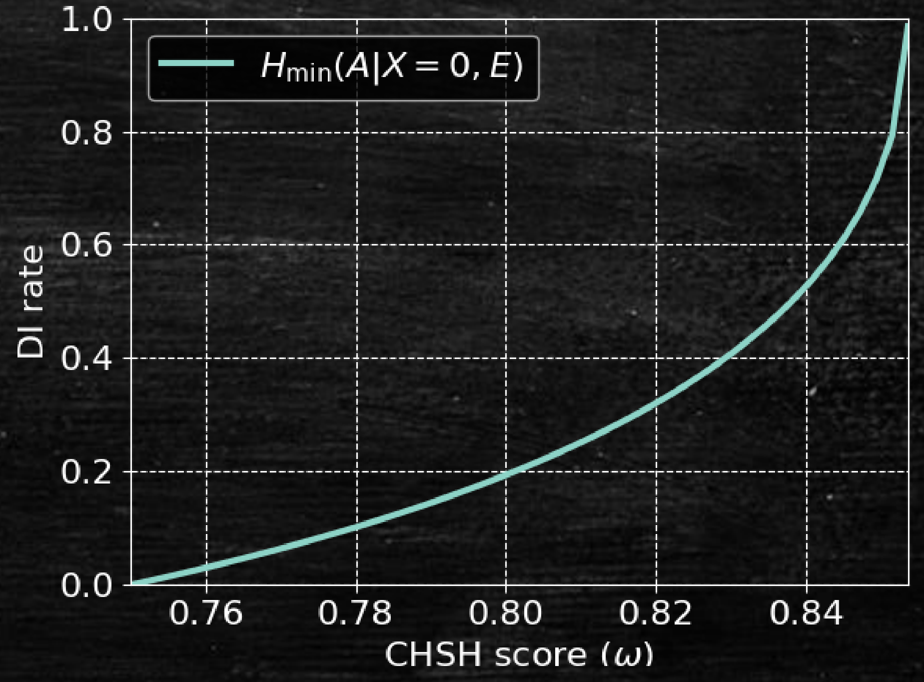


Guessing probability gives us a min-entropy bound

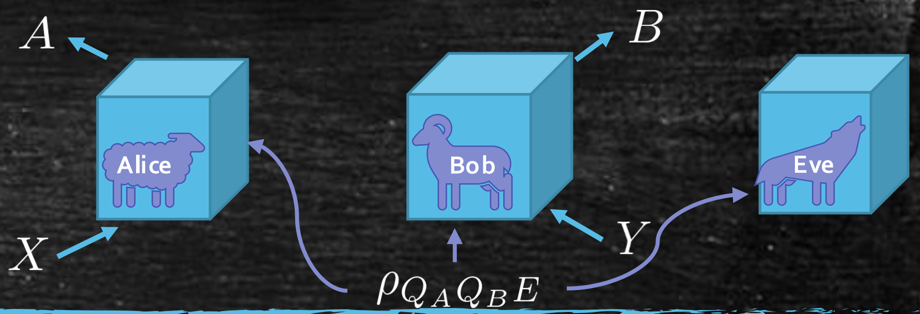
$$\min_{\text{Attacks}} H_{\min}(A|X=0,E) \geq -\log g(\omega)$$

This lower bounds the von Neumann entropy $H_{\min}(A|X=0,E) \leq H(A|X=0,E)$

Valid lower bound on our randomness rates



Min vs. von Neumann entropy



Guessing probability gives us a min-entropy bound

$$\min_{\text{Attacks}} H_{\min}(A|X=0,E) \geq -\log g(\omega)$$

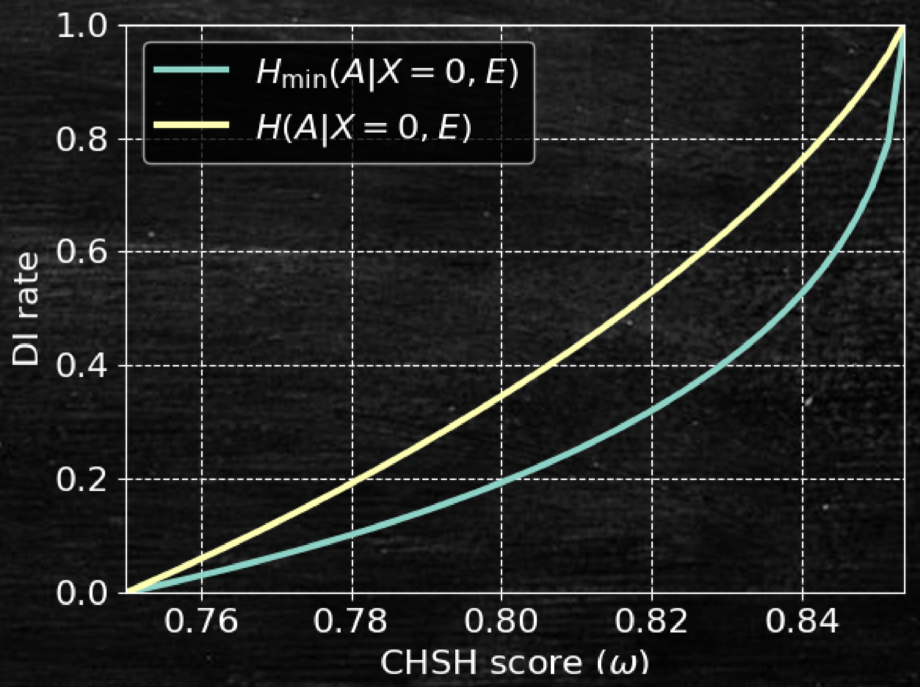
This lower bounds the von Neumann entropy $H_{\min}(A|X=0,E) \leq H(A|X=0,E)$

Valid lower bound on our randomness rates

Far from optimal…

$$\min_{\text{Attacks}} H(A|X=0,E) = 1 - h\left(\tfrac{1}{2} + \tfrac{1}{4}\sqrt{(8\omega-4)^2-4}\right)$$

[PABGMS09]



Better bounds on H(A|E)?

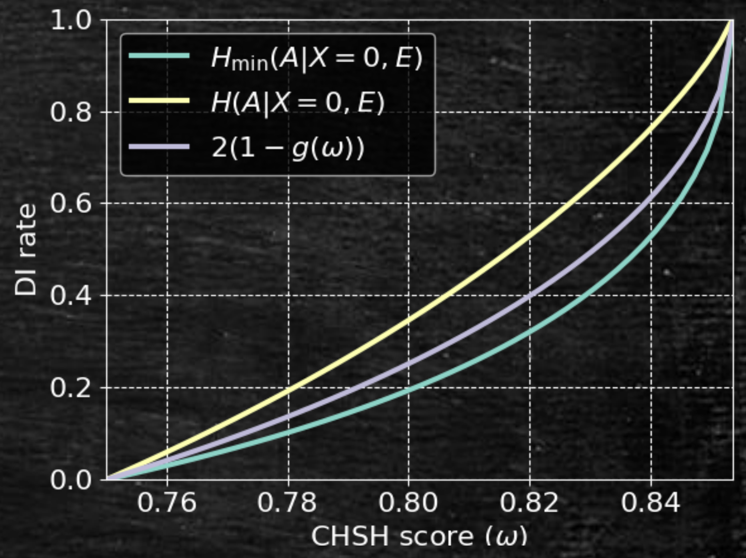
Goal: Find better numerical bounds on H(A|E)…

Better bounds on H(A|E)?

Goal: Find better numerical bounds on H(A|E)…

<u>Better entropy inequalities:</u> If A is uniform and binary then

$$H(A|E) \geq 2(1 - P_{\text{guess}}(A|E)) \qquad \text{[BH09]}$$



Better bounds on H(A|E)?

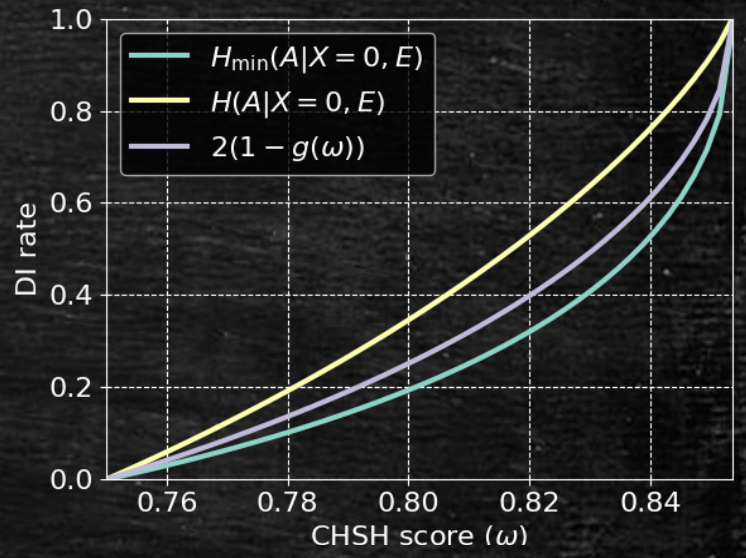
Goal: Find better numerical bounds on H(A|E)…

Better entropy inequalities: If A is uniform and binary then

$$H(A|E) \geq 2(1 - P_{\text{guess}}(A|E)) \qquad \text{[BH09]}$$

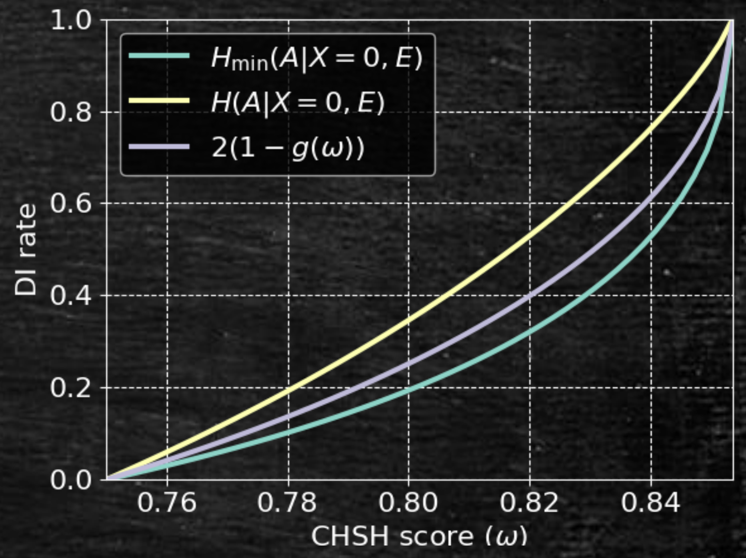
Cheap fix

Limited scope



Better bounds on H(A|E)?

Goal: Find better numerical bounds on H(A|E)...



Better entropy inequalities: If A is uniform and binary then

$$H(A|E) \geq 2(1 - P_{\text{guess}}(A|E))$$ [BH09]

Cheap fix

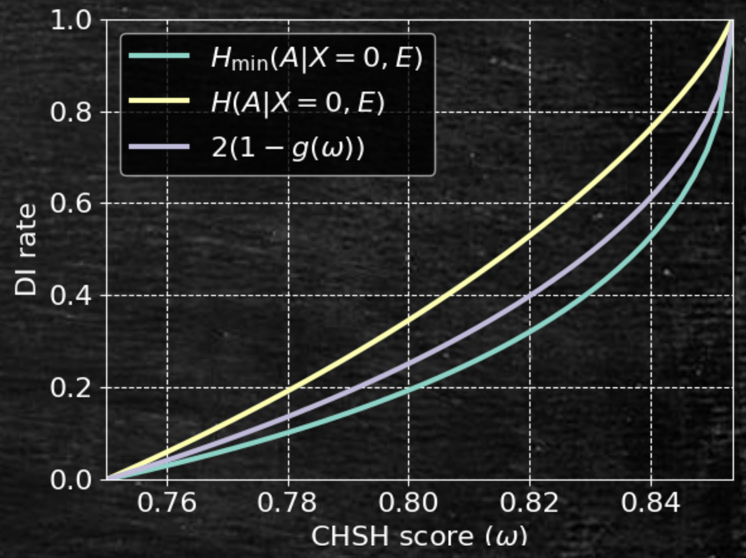
Limited scope

Better polynomial bounds: Bounds of the form

$$H(A|E) \geq \min \quad \mathrm{Tr}[\rho P(M,N,Z)] \quad \text{s.t.} \quad \ldots$$ [TSGPL21, BFF21, BFF24, KS25]

Better bounds on H(A|E)?

Goal: Find better numerical bounds on H(A|E)…



Better entropy inequalities: If A is uniform and binary then

$$H(A|E) \geq 2(1 - P_{\text{guess}}(A|E))$$ [BH09]

Cheap fix

Limited scope

Better polynomial bounds: Bounds of the form

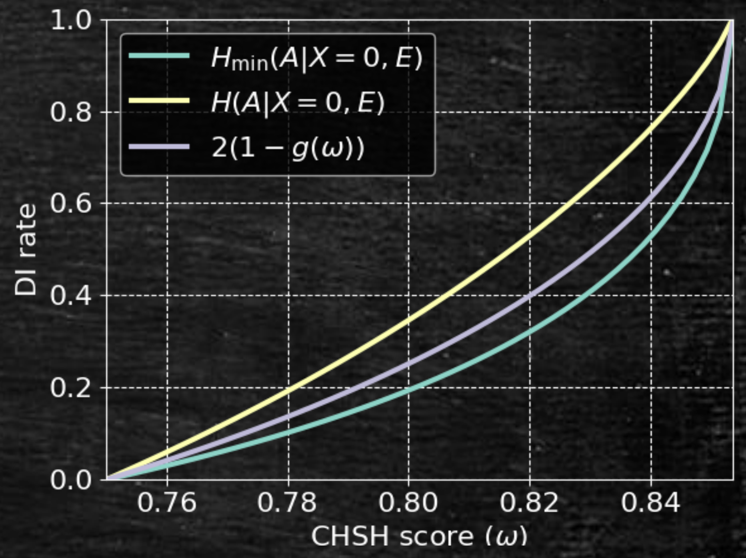
General and tight*

Quickly too expensive

$$\begin{aligned} H(A|E) \geq \min \quad & \mathrm{Tr}[\rho P(M,N,Z)] \\ \text{s.t.} \quad & \ldots \end{aligned}$$ [TSGPL21, BFF21, BFF24, KS25]

Better bounds on H(A|E)?

Goal: Find better numerical bounds on H(A|E)…



Better entropy inequalities: If A is uniform and binary then

$$H(A|E) \geq 2(1 - P_{\text{guess}}(A|E))$$ [BH09]

Cheap fix

Limited scope

Better polynomial bounds: Bounds of the form

General and tight*

Quickly too expensive

$$H(A|E) \geq \min \quad \mathrm{Tr}[\rho P(M,N,Z)] \quad \text{s.t.} \quad \ldots$$ [TSGPL21, BFF21, BFF24, KS25]

Hybrid bounds: Analytical reductions + numerics

$$\min_{\text{Attacks}} H(A|E) \longmapsto \min_{\text{Qubit attacks}} H(A|E)$$ [MPW22]

Better bounds on H(A|E)?

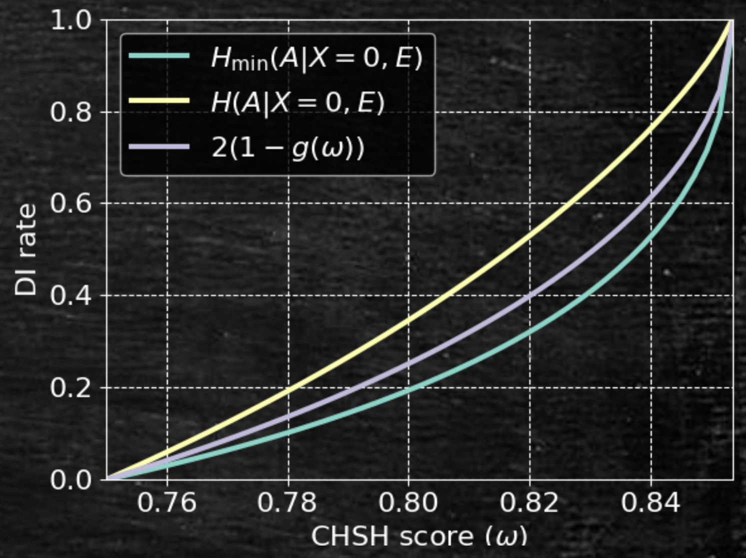
Goal: Find better numerical bounds on H(A|E)…

Better entropy inequalities: If A is uniform and binary then

$$H(A|E) \geq 2(1 - P_{\text{guess}}(A|E))$$ [BH09]

Cheap fix

Limited scope



Better polynomial bounds: Bounds of the form

General and tight*

Quickly too expensive

$$H(A|E) \geq \min \quad \mathrm{Tr}[\rho P(M,N,Z)]$$
$$\text{s.t.} \quad \ldots$$

[TSGPL21, BFF21, BFF24, KS25]

Hybrid bounds: Analytical reductions + numerics

Fast and tight

Limited scope

$$\min_{\text{Attacks}} H(A|E) \longmapsto \min_{\text{Qubit attacks}} H(A|E)$$

[MPW22]

What's next?

Further topics

Further topics / directions

Further topics / directions

Semi-DI protocols

- Different assumptions / attacks
- New convex relaxations (see posters)

Further topics / directions

Semi-DI protocols

- Different assumptions / attacks
- New convex relaxations (see posters)

Scalability

- Exploit symmetries
- Analytical solutions
- High-dimensional techniques

Further topics / directions

Semi-DI protocols

- Different assumptions / attacks
- New convex relaxations (see posters)

Scalability

- Exploit symmetries
- Analytical solutions
- High-dimensional techniques

Optimizing protocols

- Duality theory
- Protocols tailored to hardware

Further topics / directions

Semi-DI protocols

- Different assumptions / attacks
- New convex relaxations (see posters)

Scalability

- Exploit symmetries
- Analytical solutions
- High-dimensional techniques

Optimizing protocols

- Duality theory
- Protocols tailored to hardware

Practical applications

- Finite-precision computations
- Numerical stability
- Side channel attacks

Further topics / directions

Semi-DI protocols

- Different assumptions / attacks
- New convex relaxations (see posters)

Scalability

- Exploit symmetries
- Analytical solutions
- High-dimensional techniques

Finite size protocols

- Different entropic quantities
- New convex relaxations

Optimizing protocols

- Duality theory
- Protocols tailored to hardware

Practical applications

- Finite-precision computations
- Numerical stability
- Side channel attacks

References

- **[PABGMS09]** Pironio, Stefano, et al. "Device-independent quantum key distribution secure against collective attacks." *New Journal of Physics* 11.4 (2009): 045021.
- **[NPA07]** Navascués, Miguel, Stefano Pironio, and Antonio Acín. "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations." New Journal of Physics 10.7 (2008): 073013.
- **[PNA10]** Pironio, Stefano, Miguel Navascués, and Antonio Acin. "Convergent relaxations of polynomial optimization problems with noncommuting variables." SIAM Journal on Optimization 20.5 (2010): 2157-2180.
- **[TPBA24]** Tavakoli, Armin, et al. "Semidefinite programming relaxations for quantum correlations." Accepted in Rev. Mod. Phys. arXiv:2307.02551 (2023).
- **[BFF21]** Brown, Peter, Hamza Fawzi, and Omar Fawzi. "Computing conditional entropies for quantum correlations." Nature communications 12.1 (2021): 575.
- **[BFF24]** Brown, Peter, Hamza Fawzi, and Omar Fawzi. "Device-independent lower bounds on the conditional von Neumann entropy" Quantum 8 (2024): 1445.
- **[TSGPL21]** Tan, Ernest Y-Z., et al. "Computing secure key rates for quantum cryptography with untrusted devices." npj Quantum Information 7.1 (2021): 158.
- **[KS25]** Koßmann, Gereon and Schwonnek, René. "Reliable Entropy Estimation from Observed Statistics for Device-Independent Quantum Cryptography" arXiv:2411.04858
- **[MPW22]** Masini, Michele, Stefano Pironio, and Erik Woodhead. "Simple and practical DIQKD security analysis via BB84-type uncertainty relations and Pauli correlation constraints." Quantum 6 (2022): 843.
- **[BH09]** Briët, Jop, and Peter Harremoës. "Properties of classical and quantum Jensen-Shannon divergence." Physical Review A—Atomic, Molecular, and Optical Physics 79.5 (2009): 052311.