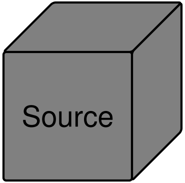
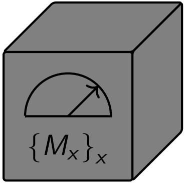
How much secure randomness is in a quantum state?

Young Quantum Information Scientists 2024

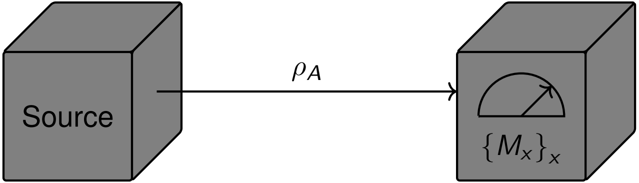
Kriss Gutierrez Anco, Tristan Nemoz, Peter Brown
tristan.nemoz@telecom-paris.fr
November 8, 2024

Problem setup

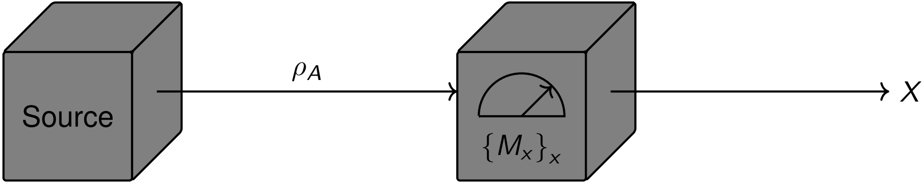




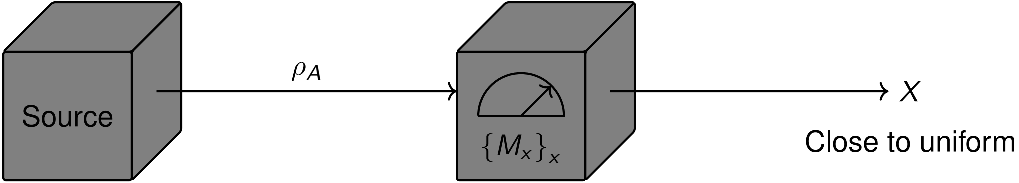
Problem setup



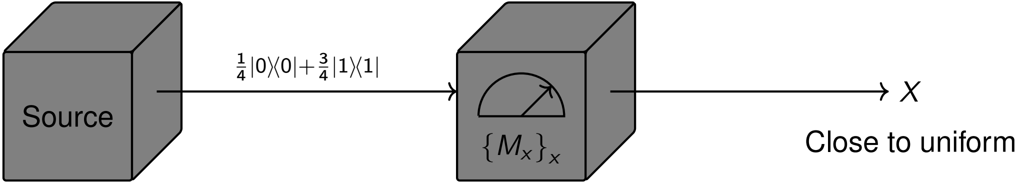
Problem setup



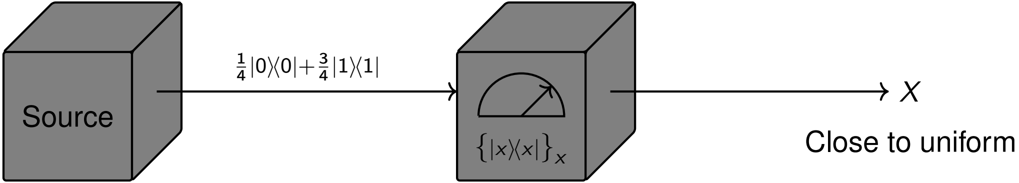
Problem setup



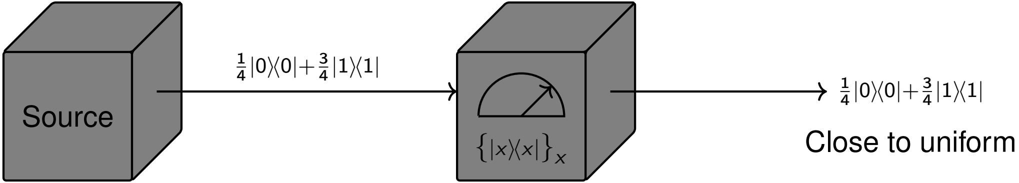
Problem setup



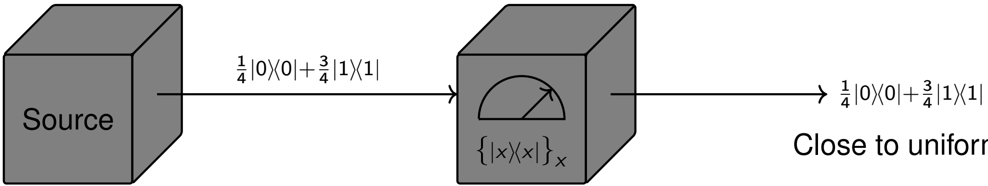
Problem setup



Problem setup

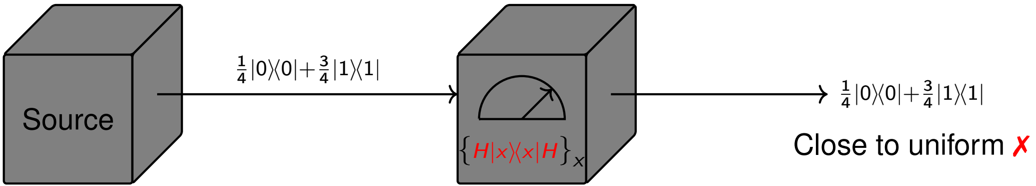


Problem setup

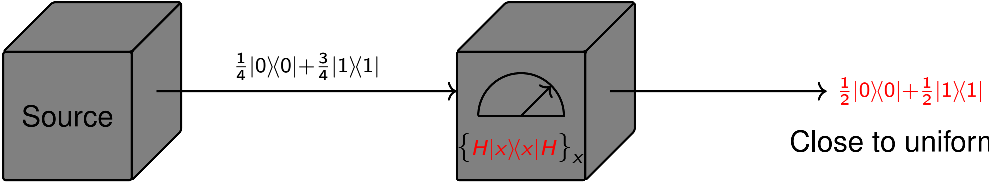


Close to uniform ✗

Problem setup

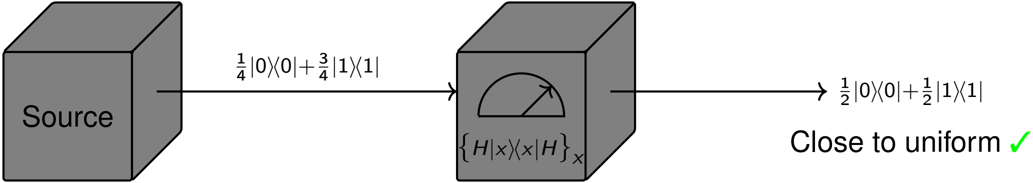


Problem setup



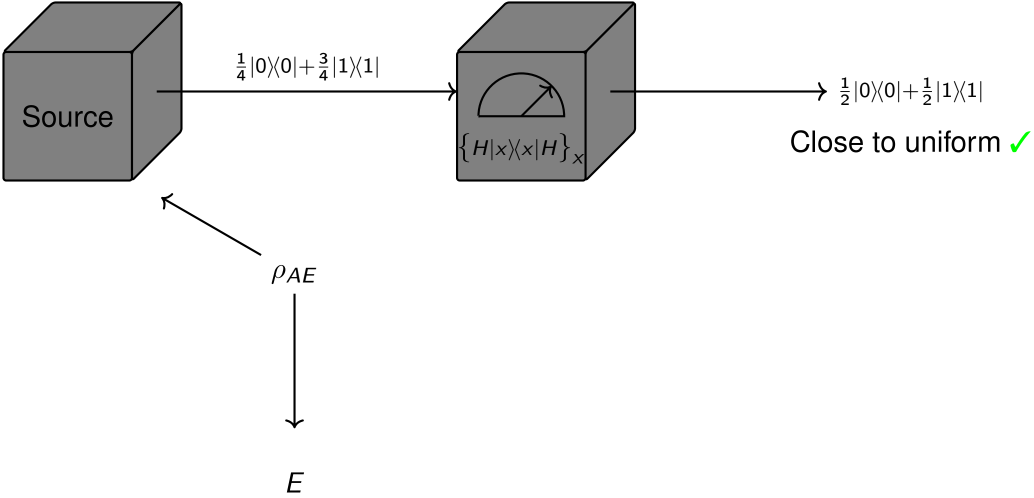
Close to uniform ✓

Problem setup

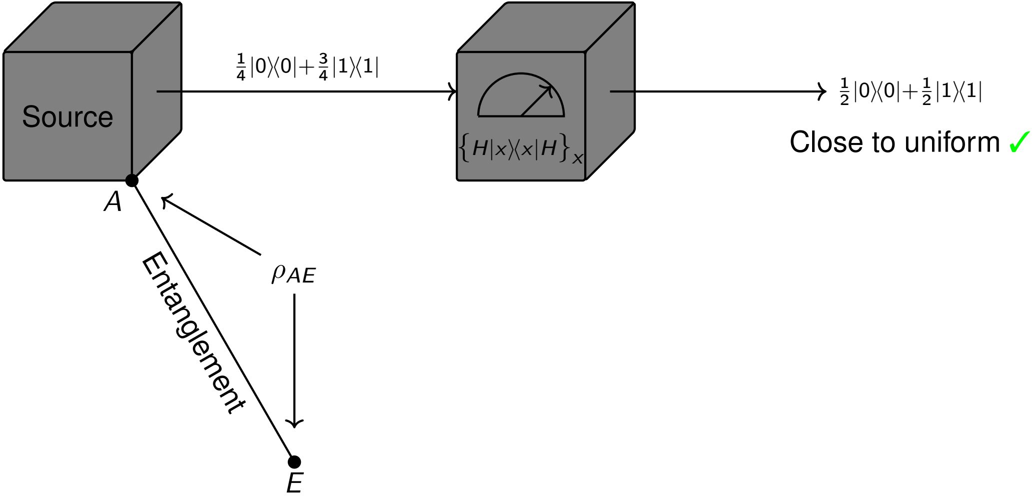


But what if an adversary had information about the source?

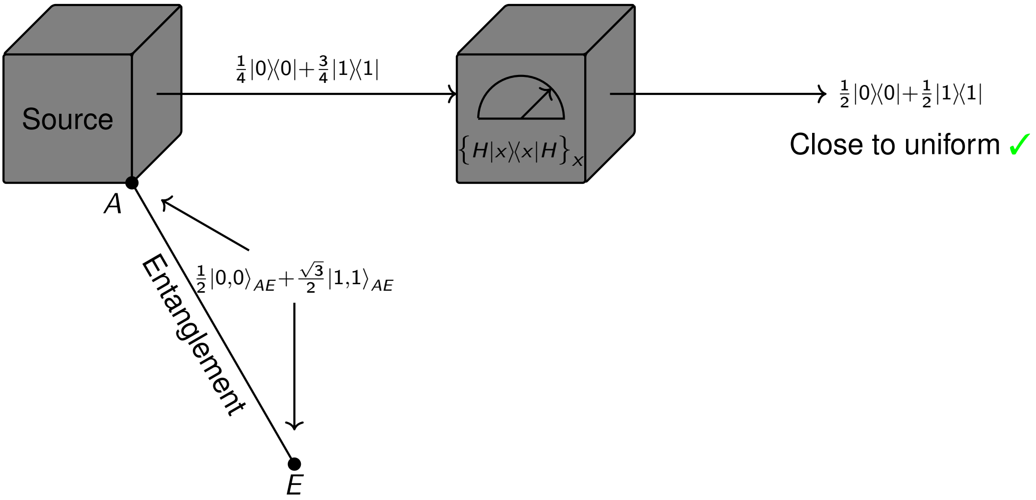
Problem setup



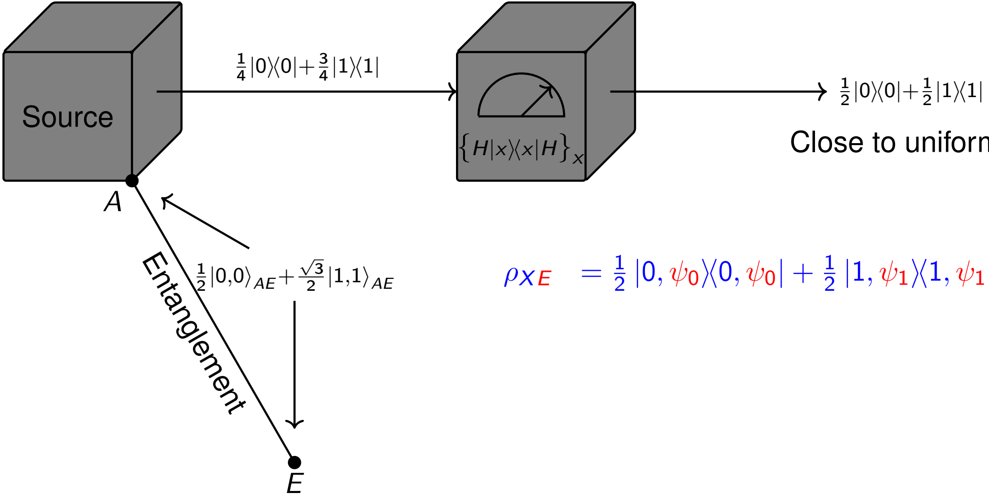
Problem setup



Problem setup



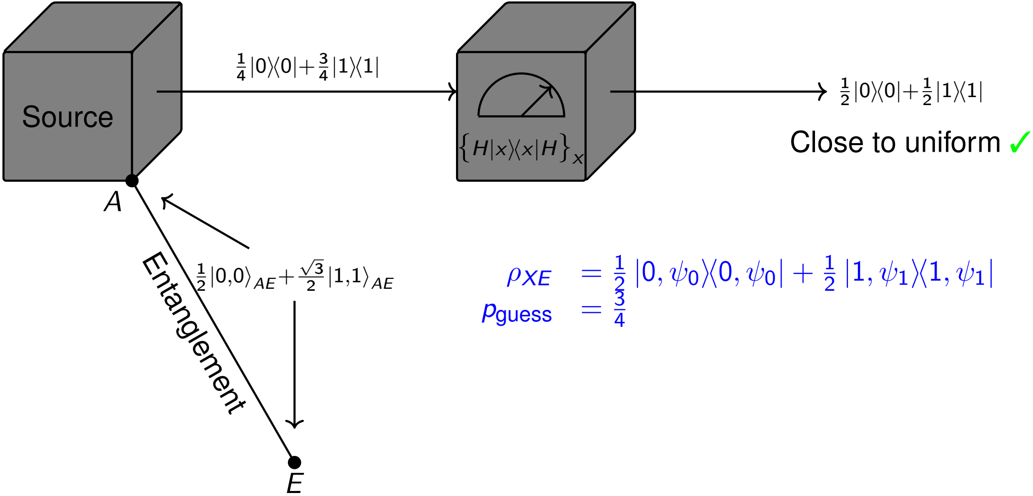
Problem setup



Close to uniform ✓

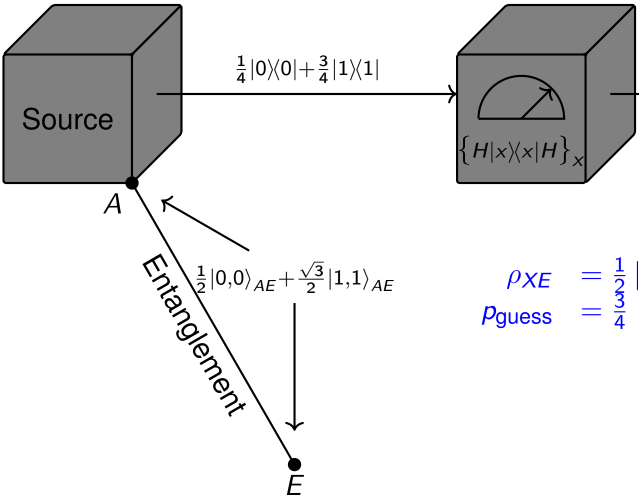
$$\rho_{XE} = \frac{1}{2}|0,\psi_0\rangle\langle 0,\psi_0| + \frac{1}{2}|1,\psi_1\rangle\langle 1,\psi_1|$$

Problem setup



$$
\begin{aligned}
\rho_{XE} &= \frac{1}{2}\,|0,\psi_0\rangle\langle 0,\psi_0| + \frac{1}{2}\,|1,\psi_1\rangle\langle 1,\psi_1| \\
p_{\text{guess}} &= \frac{3}{4}
\end{aligned}
$$

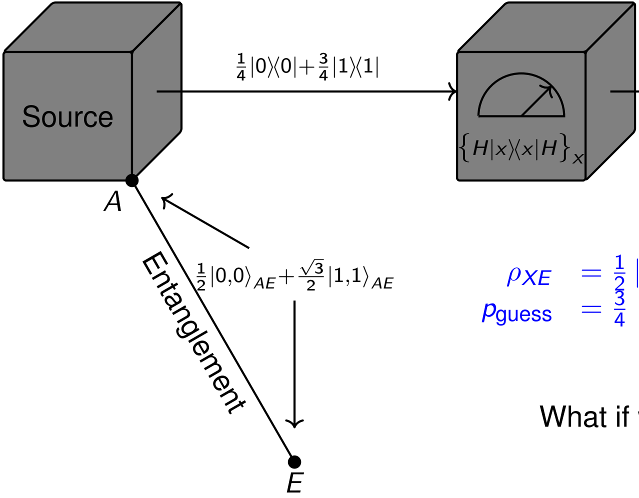
Problem setup



Close to uniform ✓
Secret ✗

$$\rho_{XE} = \frac{1}{2}\,|0,\psi_0\rangle\langle 0,\psi_0| + \frac{1}{2}\,|1,\psi_1\rangle\langle 1,\psi_1|$$
$$p_{\text{guess}} = \frac{3}{4}$$

Problem setup

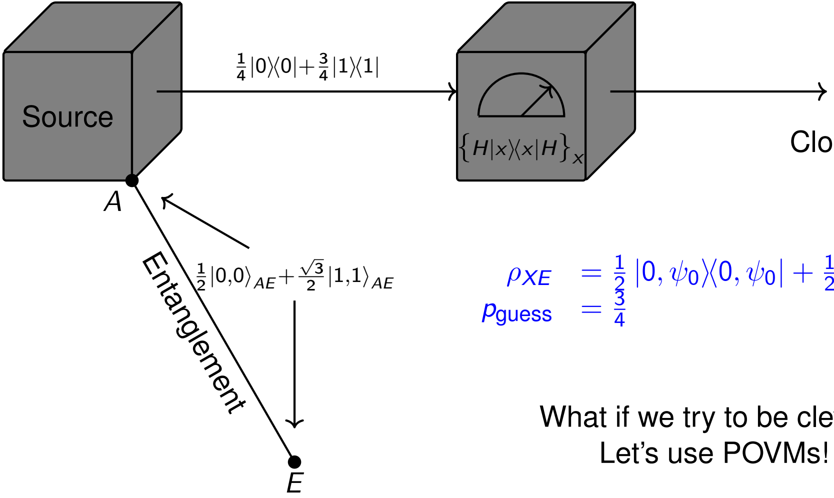


Close to uniform ✓
Secret ✗

$$\rho_{XE} = \frac{1}{2}\,|0,\psi_0\rangle\langle 0,\psi_0| + \frac{1}{2}\,|1,\psi_1\rangle\langle 1,\psi_1|$$
$$p_{\text{guess}} = \frac{3}{4}$$

What if we try to be clever?

Problem setup

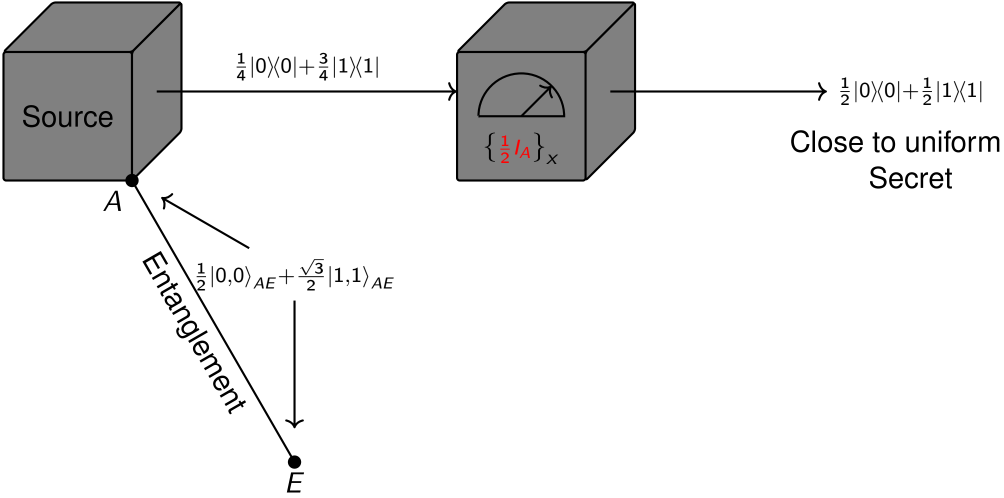


Close to uniform ✓
Secret ✗

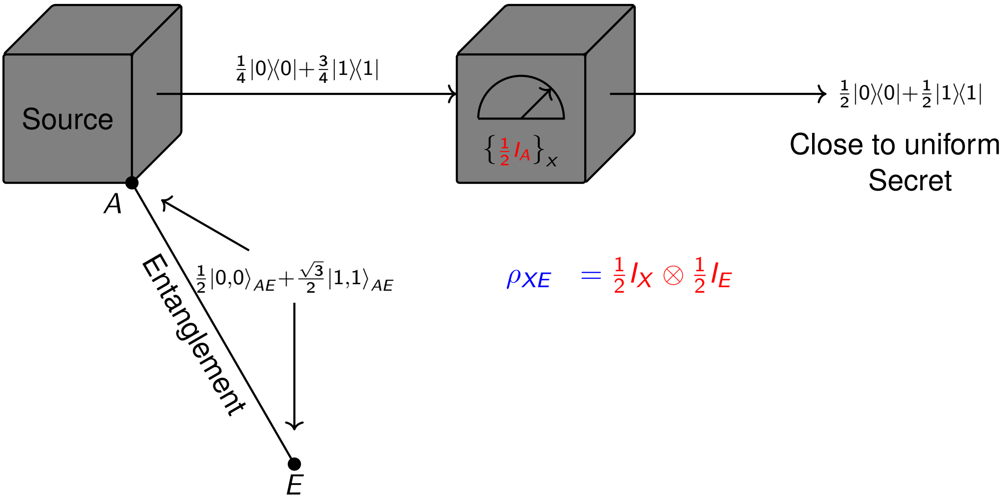
$$\begin{aligned} \rho_{XE} &= \frac{1}{2}\,|0,\psi_0\rangle\langle 0,\psi_0| + \frac{1}{2}\,|1,\psi_1\rangle\langle 1,\psi_1| \\ p_{\text{guess}} &= \frac{3}{4} \end{aligned}$$

What if we try to be clever?
Let's use POVMs!

Problem setup

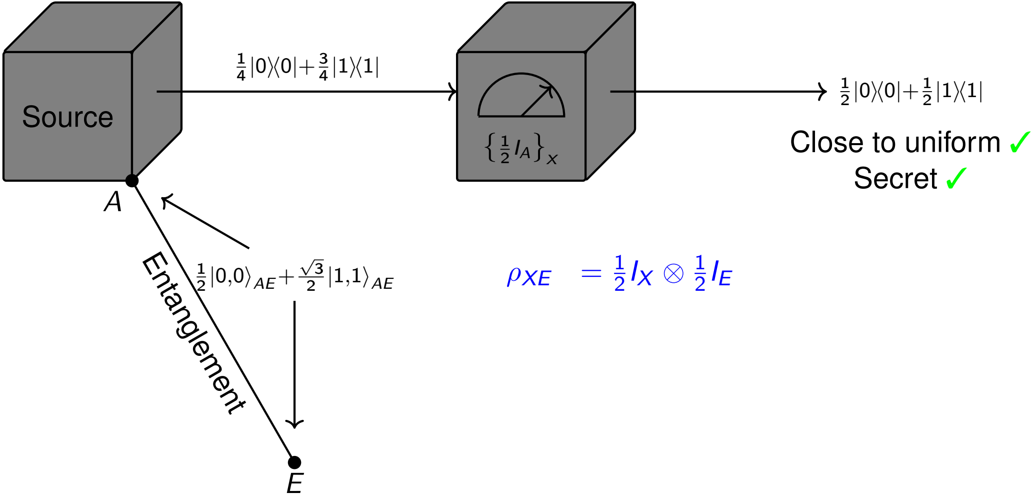


Problem setup



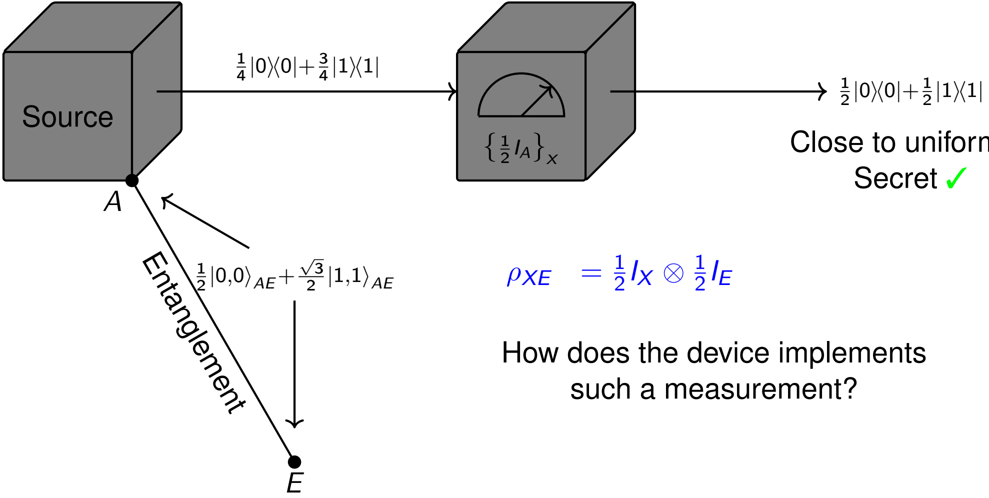
$$\rho_{XE} = \frac{1}{2}I_X \otimes \frac{1}{2}I_E$$

Problem setup



$$\rho_{XE} = \frac{1}{2}I_X \otimes \frac{1}{2}I_E$$

Problem setup



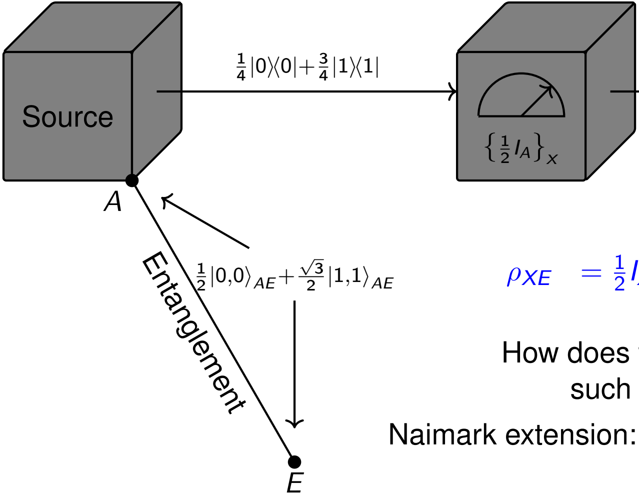
Close to uniform ✓

Secret ✓

$$\rho_{XE} = \frac{1}{2}I_X \otimes \frac{1}{2}I_E$$

How does the device implements such a measurement?

Problem setup



$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$

Close to uniform ✓
Secret ✓

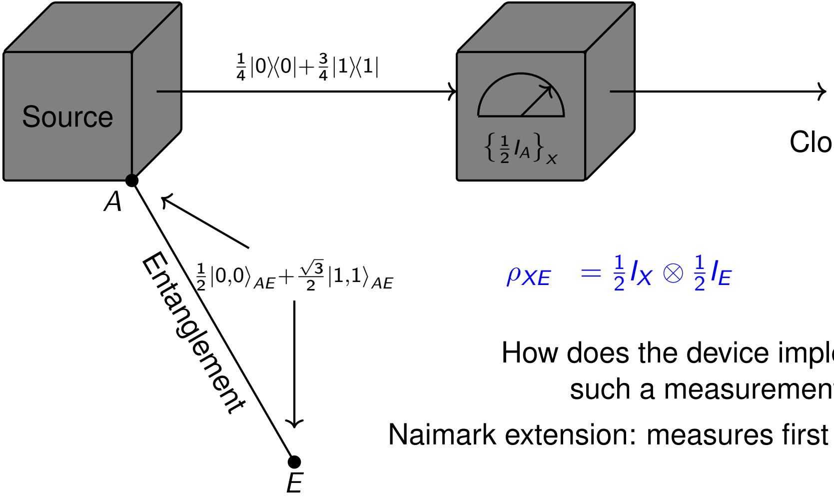
$$\rho_{XE} = \frac{1}{2} I_X \otimes \frac{1}{2} I_E$$

How does the device implements such a measurement?

Naimark extension: measures first qubit of $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

TELECOM Paris IP PARIS

Problem setup



$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$

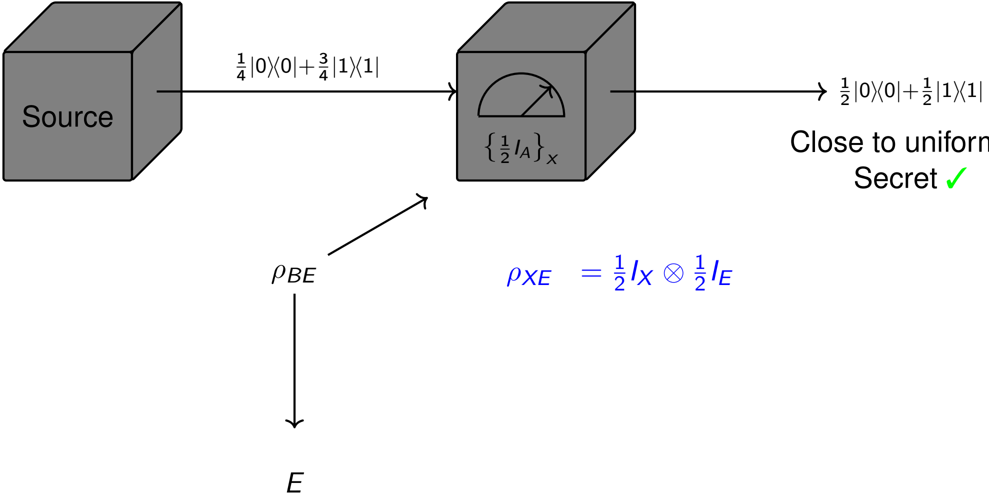
Close to uniform ✓

Secret ✓

$$\rho_{XE} = \frac{1}{2} I_X \otimes \frac{1}{2} I_E$$

How does the device implements such a measurement?

Naimark extension: measures first qubit of $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

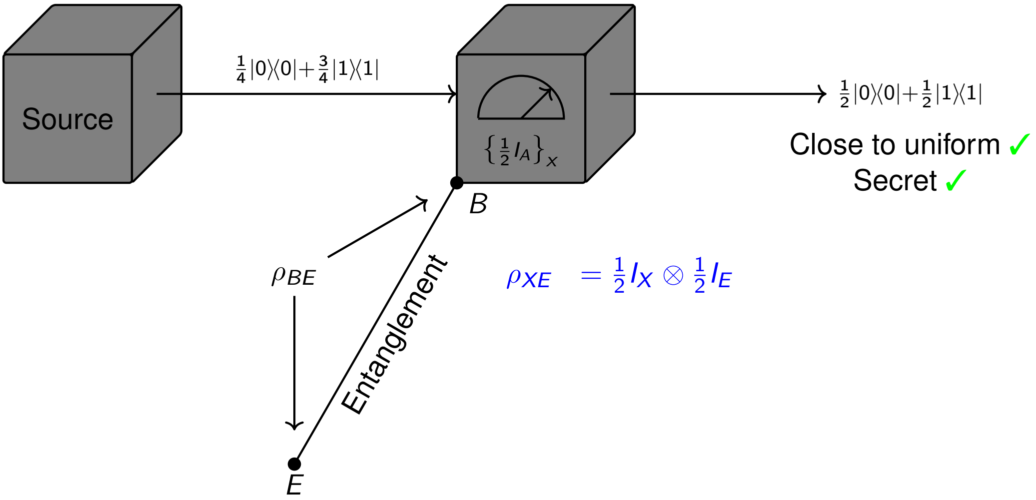


Close to uniform ✓

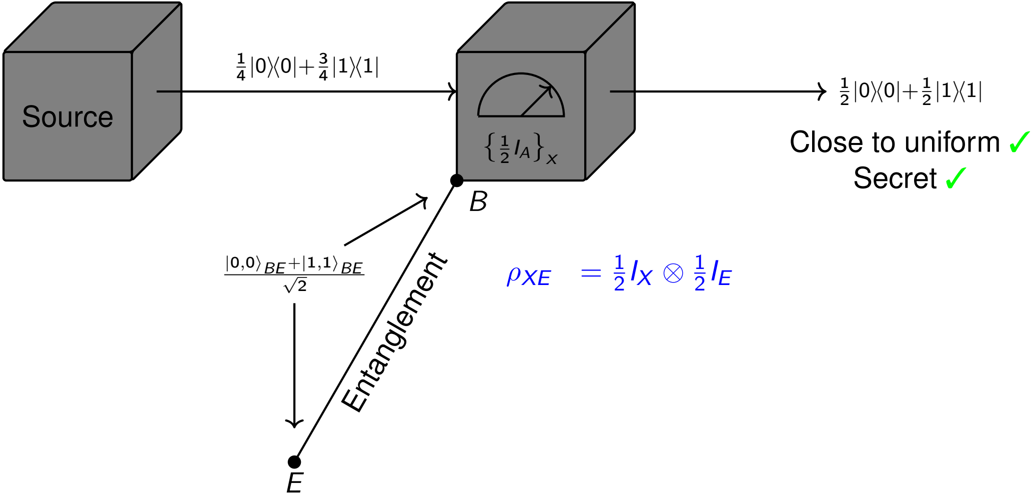
Secret ✓

$$\rho_{XE} = \frac{1}{2} I_X \otimes \frac{1}{2} I_E$$

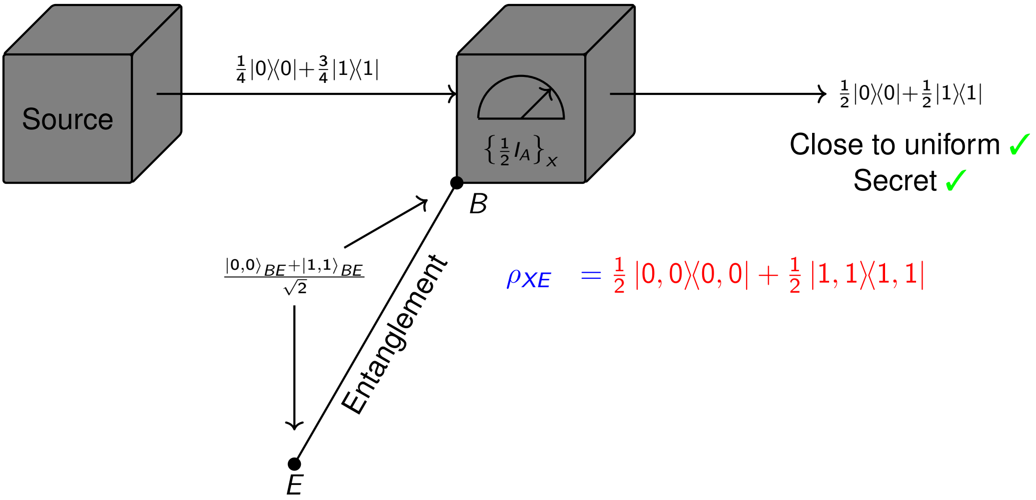
Problem setup



Problem setup

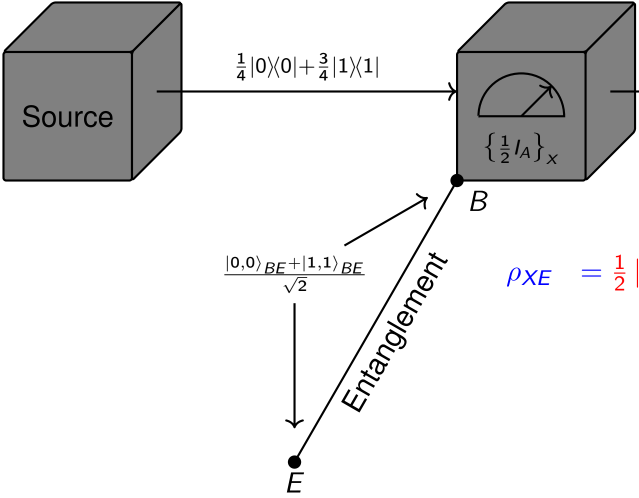


Problem setup



$$\rho_{XE} = \frac{1}{2}\,|0,0\rangle\langle 0,0| + \frac{1}{2}\,|1,1\rangle\langle 1,1|$$

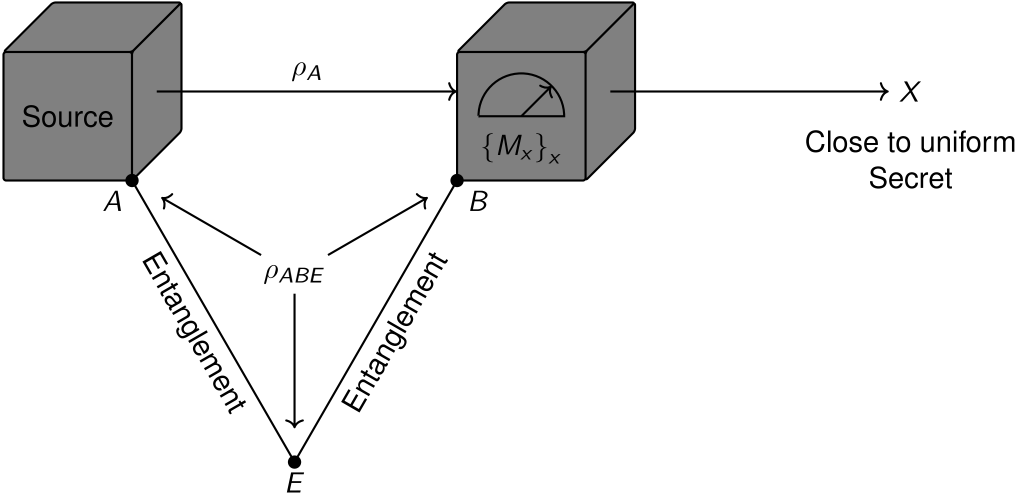
Problem setup



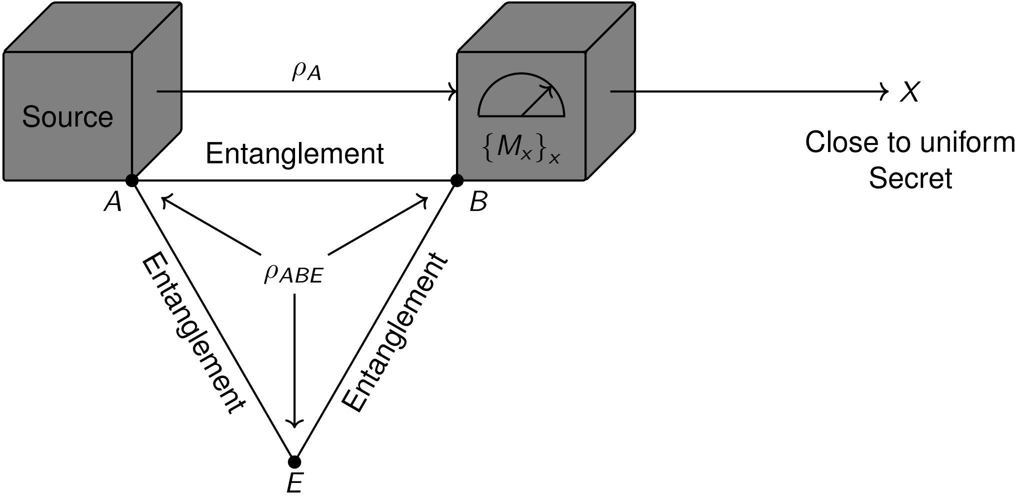
Close to uniform ✓
Secret ✗

$$\rho_{XE} = \frac{1}{2}|0,0\rangle\langle 0,0| + \frac{1}{2}|1,1\rangle\langle 1,1|$$

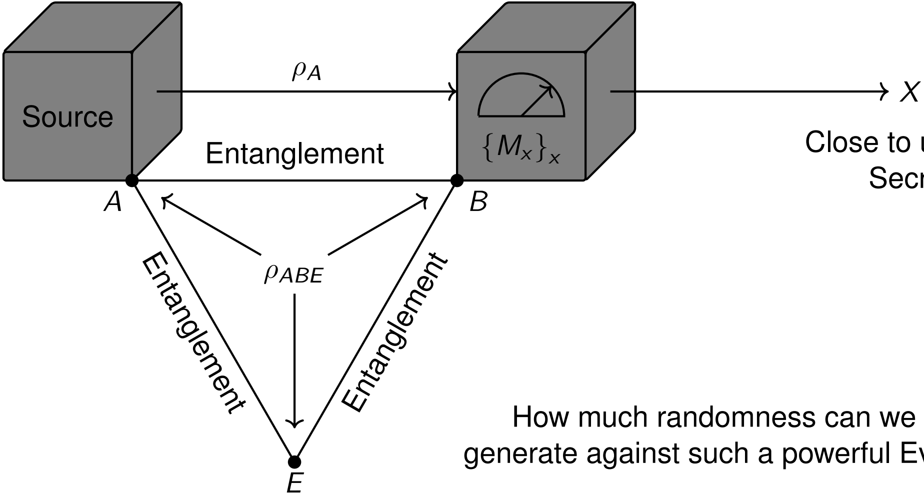
Problem setup



Problem setup



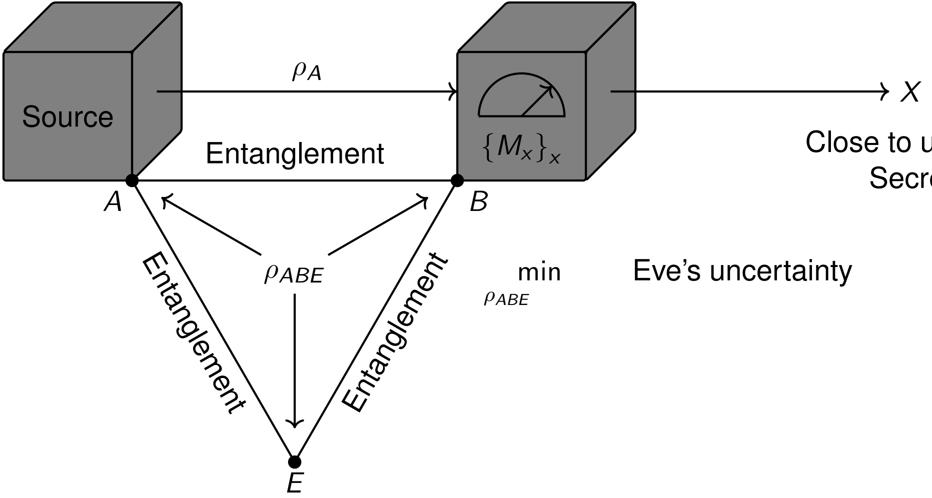
Problem setup



Close to uniform
Secret

How much randomness can we generate against such a powerful Eve?

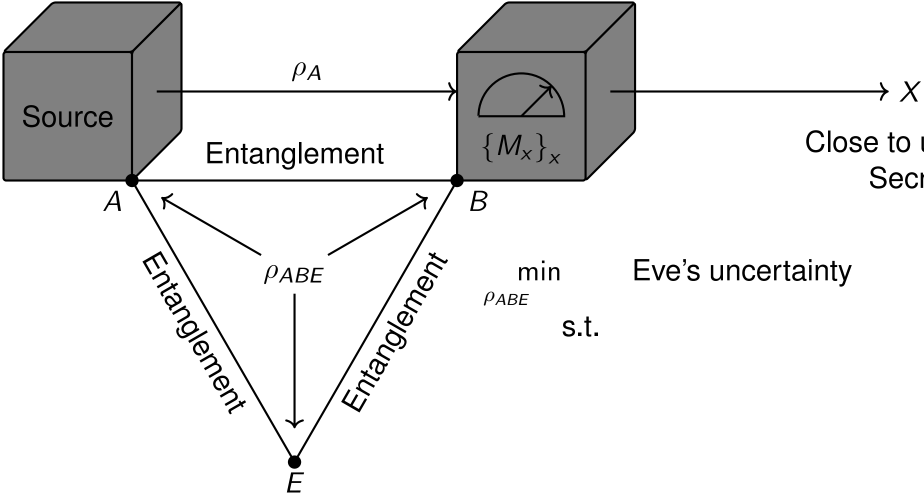
Problem setup



Close to uniform
Secret

$\min_{\rho_{ABE}}$ Eve's uncertainty

Problem setup

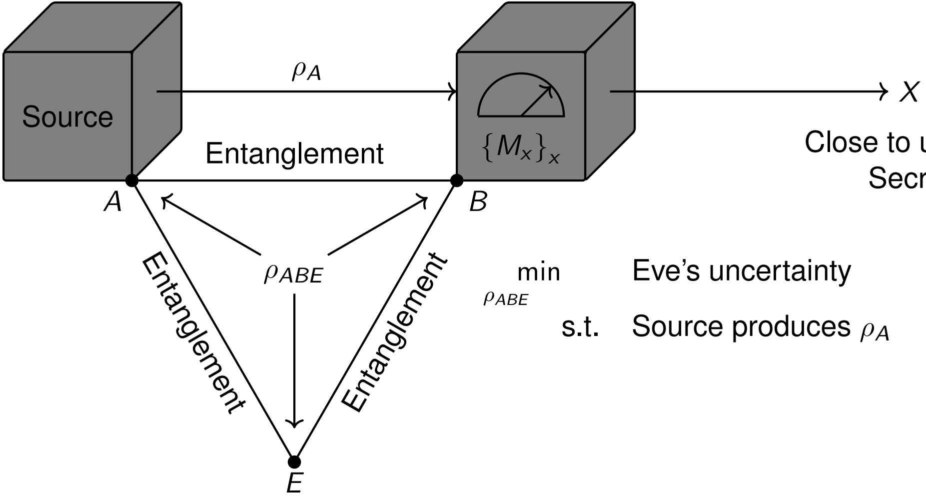


Close to uniform
Secret

$\min_{\rho_{ABE}}$ Eve's uncertainty

s.t.

Problem setup

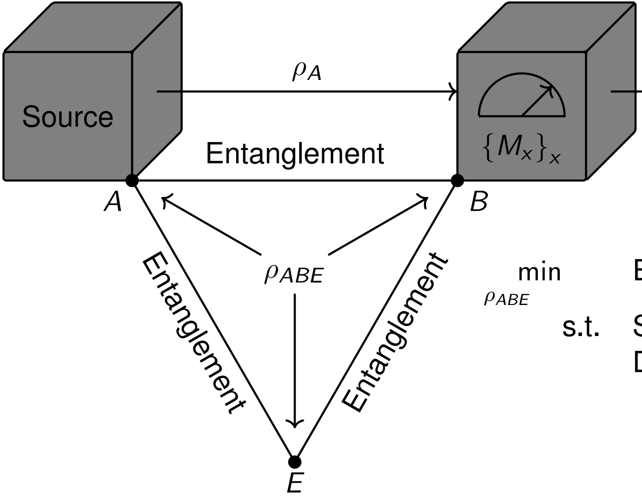


Close to uniform
Secret

$$\min_{\rho_{ABE}} \quad \text{Eve's uncertainty}$$
$$\text{s.t.} \quad \text{Source produces } \rho_A$$

TELECOM Paris
IP PARIS

Problem setup

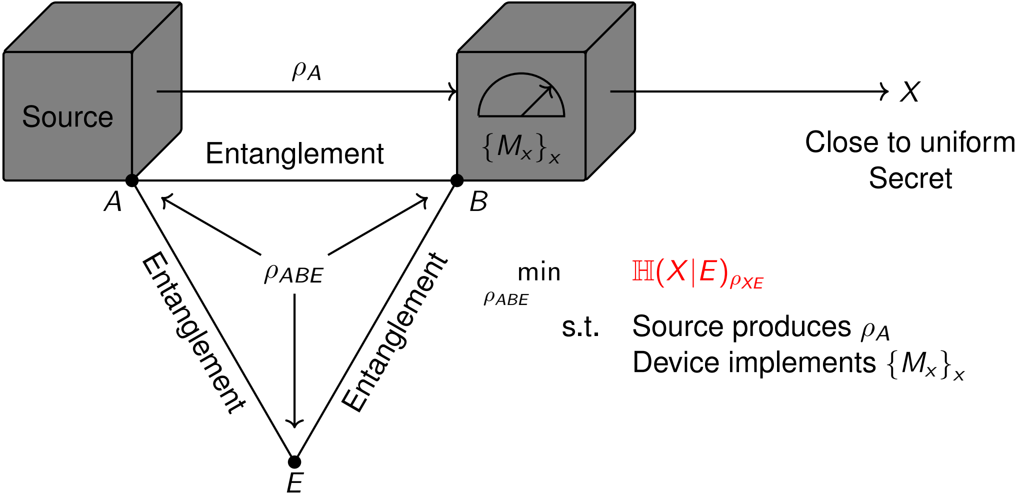


Close to uniform
Secret

$$\min_{\rho_{ABE}} \quad \text{Eve's uncertainty}$$

s.t. Source produces ρ_A
Device implements $\{M_x\}_x$

Problem setup

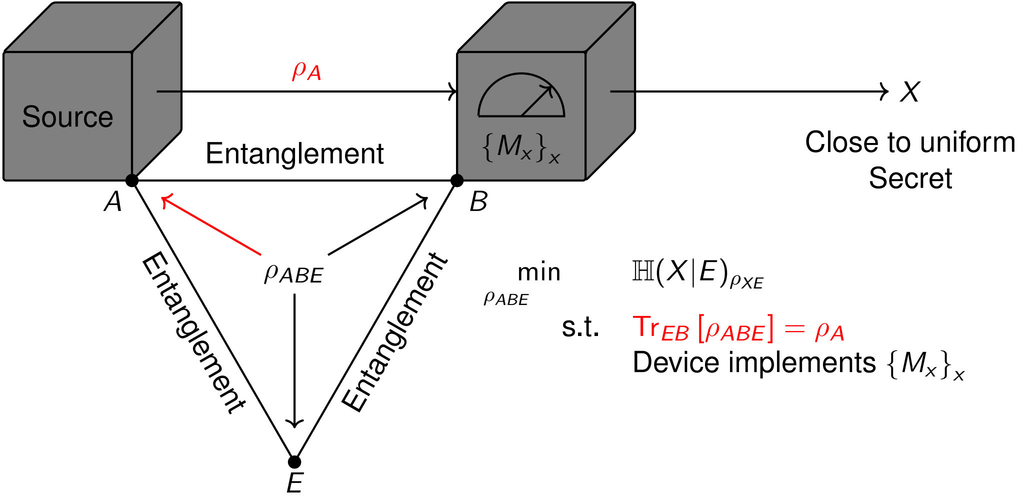


$$\min_{\rho_{ABE}} \quad \mathbb{H}(X|E)_{\rho_{XE}}$$

s.t. Source produces ρ_A

Device implements $\{M_x\}_x$

Problem setup

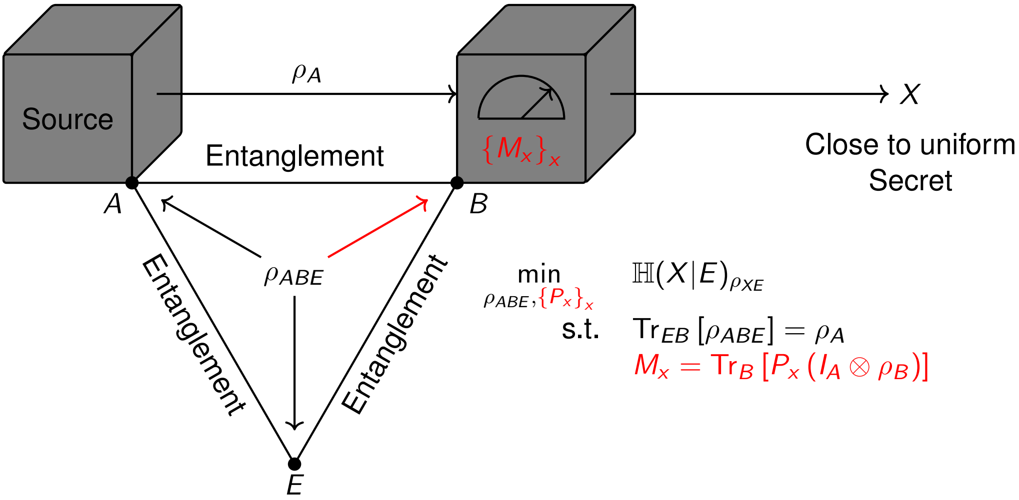


$$\min_{\rho_{ABE}} \quad \mathbb{H}(X|E)_{\rho_{XE}}$$

$$\text{s.t.} \quad \mathrm{Tr}_{EB}\left[\rho_{ABE}\right] = \rho_A$$

Device implements $\{M_x\}_x$

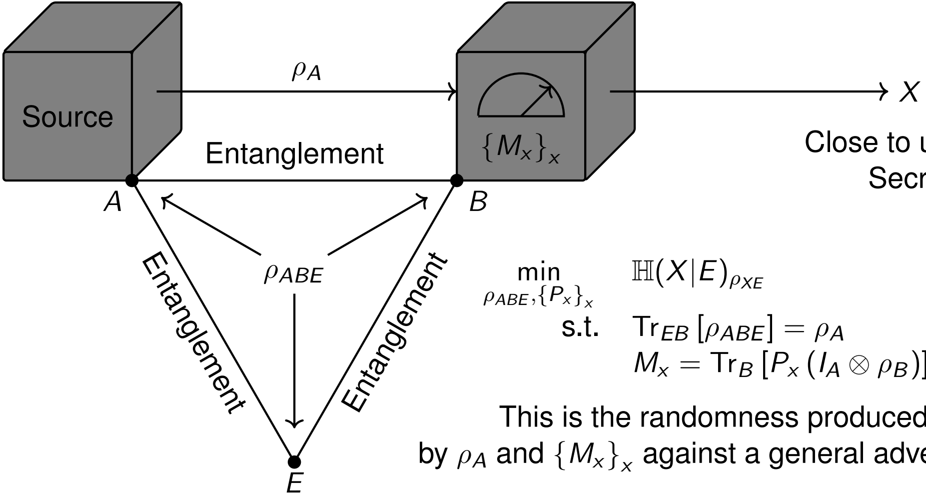
Problem setup



$$\min_{\rho_{ABE},\{P_x\}_x} \quad \mathbb{H}(X|E)_{\rho_{XE}}$$
$$\text{s.t.} \quad \mathrm{Tr}_{EB}[\rho_{ABE}] = \rho_A$$
$$M_x = \mathrm{Tr}_B[P_x(I_A \otimes \rho_B)]$$

TELECOM Paris IP PARIS

Problem setup



Close to uniform
Secret

$$\min_{\rho_{ABE},\{P_x\}_x} \quad \mathbb{H}(X|E)_{\rho_{XE}}$$

$$\text{s.t.} \quad \mathrm{Tr}_{EB}\left[\rho_{ABE}\right] = \rho_A$$

$$M_x = \mathrm{Tr}_B\left[P_x\left(I_A \otimes \rho_B\right)\right]$$

This is the randomness produced by ρ_A and $\{M_x\}_x$ against a general adversary!

TELECOM Paris IP PARIS

Problem statement

- Randomness hand-waved using entropies

Problem statement

- Randomness hand-waved using entropies
- ε-secure randomness:

$$\rho_{XE} \approx_\varepsilon \frac{1}{d_X} I_X \otimes \rho_E$$

TELECOM Paris IP PARIS

Problem statement

- Randomness hand-waved using entropies
- ε-secure randomness:

$$\rho_{XE} \approx_\varepsilon \frac{1}{d_X} I_X \otimes \rho_E$$

  - Uniformly random

Problem statement

- Randomness hand-waved using entropies
- ε-secure randomness:

$$\rho_{XE} \approx_{\varepsilon} \frac{1}{d_X} I_X \otimes \rho_E$$

  - Uniformly random, independent of Eve

Problem statement

- Randomness hand-waved using entropies
- ε-secure randomness:

$$\rho_{XE} \approx_{\varepsilon} \frac{1}{d_X} I_X \otimes \rho_E$$

  - Uniformly random, independent of Eve
  - (Dupuis, 2023): link with sandwiched Rényi entropies H_α

Problem statement

- Randomness hand-waved using entropies
- ε-secure randomness:

$$\rho_{XE} \approx_\varepsilon \frac{1}{d_X} I_X \otimes \rho_E$$

  - Uniformly random, independent of Eve
  - (Dupuis, 2023): link with sandwiched Rényi entropies H_α

$$\min_{\rho_{AEB}, \{P_x\}_x} \mathbb{H}(X|E)_{\rho_{XE}} = \qquad \text{randomness produced by } \rho_A \text{ and } \{M_x\}_x$$

Problem statement

- Randomness hand-waved using entropies
- ε-secure randomness:

$$\rho_{XE} \approx_\varepsilon \frac{1}{d_X} I_X \otimes \rho_E$$

  - Uniformly random, independent of Eve
  - (Dupuis, 2023): link with sandwiched Rényi entropies H_α

$$\sup_{\{M_x\}_x} \min_{\rho_{AEB}, \{P_x\}_x} \mathbb{H}(X|E)_{\rho_{XE}} = \text{maximal randomness produced by } \rho_A$$

TELECOM Paris
IP PARIS

Problem statement

- Randomness hand-waved using entropies
- ε-secure randomness:

$$\rho_{XE} \approx_\varepsilon \frac{1}{d_X} I_X \otimes \rho_E$$

  - Uniformly random, independent of Eve
  - (Dupuis, 2023): link with sandwiched Rényi entropies H_α

$$\sup_{\{M_x\}_x} \min_{\rho_{AEB},\{P_x\}_x} \mathbb{H}(X|E)_{\rho_{XE}} = \text{ maximal randomness produced by } \rho_A$$

- "$\max \min$" problem

Problem statement

- Randomness hand-waved using entropies
- ε-secure randomness:

$$\rho_{XE} \approx_{\varepsilon} \frac{1}{d_X} I_X \otimes \rho_E$$

  - Uniformly random, independent of Eve
  - (Dupuis, 2023): link with sandwiched Rényi entropies H_α

$$\sup_{\{M_x\}_x} \min_{\rho_{AEB},\{P_x\}_x} \mathbb{H}(X|E)_{\rho_{XE}} = \text{ maximal randomness produced by } \rho_A$$

- "$\max\min$" problem
- $\dim(E)$ arbitrary

Problem statement

- Randomness hand-waved using entropies
- ε-secure randomness:

$$\rho_{XE} \approx_\varepsilon \frac{1}{d_X} I_X \otimes \rho_E$$

  - Uniformly random, independent of Eve
  - (Dupuis, 2023): link with sandwiched Rényi entropies H_α

$$\sup_{\{M_x\}_x} \min_{\rho_{AEB},\{P_x\}_x} \mathbb{H}(X|E)_{\rho_{XE}} = \text{ maximal randomness produced by } \rho_A$$

- "$\max\min$" problem
- $\dim(E)$ arbitrary

- Optimize over all Naimark extensions

Problem statement

- Randomness hand-waved using entropies
- ε-secure randomness:

$$\rho_{XE} \approx_\varepsilon \frac{1}{d_X} I_X \otimes \rho_E$$

  - Uniformly random, independent of Eve
  - (Dupuis, 2023): link with sandwiched Rényi entropies H_α

$$\sup_{\{M_x\}_x} \min_{\rho_{AEB},\{P_x\}_x} \mathbb{H}(X|E)_{\rho_{XE}} = \text{maximal randomness produced by } \rho_A$$

- "$\max\min$" problem
- $\dim(E)$ arbitrary

- Optimize over all Naimark extensions
  - $\dim(B)$ arbitrary

TELECOM Paris
IP PARIS

Problem statement

- Randomness hand-waved using entropies
- ε-secure randomness:

$$\rho_{XE} \approx_\varepsilon \frac{1}{d_X} I_X \otimes \rho_E$$

  - Uniformly random, independent of Eve
  - (Dupuis, 2023): link with sandwiched Rényi entropies H_α

$$\sup_{\{M_x\}_x} \min_{\rho_{AEB},\{P_x\}_x} \mathbb{H}(X|E)_{\rho_{XE}} = \text{ maximal randomness produced by } \rho_A$$

- "$\max\min$" problem
- $\dim(E)$ arbitrary

- Optimize over all Naimark extensions
  - $\dim(B)$ arbitrary
- $\implies$ Not trivial!

Reductions

$$
\begin{aligned}
\sup_{\text{POVM } \{M_x\}_x} \min_{\substack{\rho_{ABE} \\ \text{PVM } \{P_x\}_x}} \quad & \mathbb{H}(X|E)_{\rho_{XE}} \\
\text{s.t.} \quad & \mathrm{Tr}_{BE}\left[\rho_{ABE}\right] = \rho_A \\
& M_x = \mathrm{Tr}_B\left[P_x\left(I_A \otimes \mathrm{Tr}_{AE}\left[\rho_{ABE}\right]\right)\right]
\end{aligned}
$$

Reductions

$$\sup_{\text{POVM } \{M_x\}_x} \min_{\substack{\rho_{ABE} \\ \text{PVM } \{P_x\}_x}} \mathbb{H}(X|E)_{\rho_{XE}}$$

$$\text{s.t.} \quad \mathrm{Tr}_{BE}\left[\rho_{ABE}\right] = \rho_A$$

$$M_x = \mathrm{Tr}_B\left[P_x\left(I_A \otimes \mathrm{Tr}_{AE}\left[\rho_{ABE}\right]\right)\right]$$

- Eve: purifies ρ_{AB}

Reductions

$$\sup_{\text{POVM } \{M_x\}_x} \min_{\substack{|\psi_{ABE}\rangle \\ \text{PVM } \{P_x\}_x}} \mathbb{H}(X|E)_{\rho_{XE}}$$

$$\text{s.t.} \quad \mathrm{Tr}_{BE}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right] = \rho_A$$

$$M_x = \mathrm{Tr}_B\left[P_x\left(I_A \otimes \mathrm{Tr}_{AE}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right]\right)\right]$$

- Eve: purifies ρ_{AB}

Reductions

$$\sup_{\text{POVM } \{M_x\}_x} \min_{\substack{|\psi_{ABE}\rangle \\ \text{PVM } \{P_x\}_x}} \mathbb{H}(X|E)_{\rho_{XE}}$$

$$\text{s.t.} \quad \mathrm{Tr}_{BE}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right] = \rho_A$$

$$M_x = \mathrm{Tr}_B\left[P_x\left(I_A \otimes \mathrm{Tr}_{AE}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right]\right)\right]$$

- Eve: purifies ρ_{AB}
- Alice: picks rank-1 extremal POVM

Reductions

$$\sup_{\text{Extremal rank-1 POVM } \{M_x\}_x} \; \min_{\substack{|\psi_{ABE}\rangle \\ \text{PVM } \{P_x\}_x}} \; \mathbb{H}(X|E)_{\rho_{XE}}$$

$$\text{s.t.} \quad \mathrm{Tr}_{BE}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right] = \rho_A$$

$$M_x = \mathrm{Tr}_B\left[P_x\left(I_A \otimes \mathrm{Tr}_{AE}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right]\right)\right]$$

- Eve: purifies ρ_{AB}
- Alice: picks rank-1 extremal POVM

Reductions

$$\sup_{\text{Extremal rank-1 POVM } \{M_x\}_x} \min_{\substack{|\psi_{ABE}\rangle \\ \text{PVM } \{P_x\}_x}} \mathbb{H}(X|E)_{\rho_{XE}}$$

$$\text{s.t.} \quad \mathrm{Tr}_{BE}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right] = \rho_A$$

$$M_x = \mathrm{Tr}_B\left[P_x\left(I_A \otimes \mathrm{Tr}_{AE}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right]\right)\right]$$

- Eve: purifies ρ_{AB}
- Alice: picks rank-1 extremal POVM
- Technical result: M rank-1 extremal $\implies \rho_{XE} \perp\!\!\!\perp \rho_B$

TELECOM Paris
IP PARIS

Reductions

$$\sup_{\text{Extremal rank-1 POVM } \{M_x\}_x} \min_{|\psi_{ABE}\rangle} \mathbb{H}(X|E)_{\rho_{XE}}$$

$$\text{s.t.} \quad \mathrm{Tr}_{BE}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right] = \rho_A$$

- Eve: purifies ρ_{AB}
- Alice: picks rank-1 extremal POVM
- Technical result: M rank-1 extremal $\implies \rho_{XE} \perp\!\!\!\perp \rho_B$

Reductions

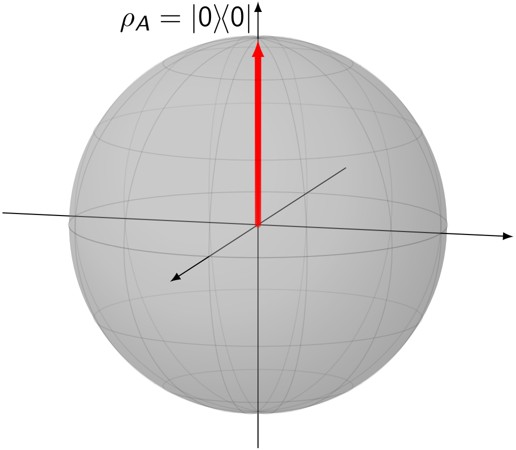
$$\sup_{\text{Extremal rank-1 POVM } \{M_x\}_x} \quad \min_{|\psi_{ABE}\rangle} \quad \mathbb{H}(X|E)_{\rho_{XE}}$$

$$\text{s.t.} \quad \mathrm{Tr}_{BE}\left[|\psi_{ABE}\rangle\langle\psi_{ABE}|\right] = \rho_A$$

- Eve: purifies ρ_{AB}
- Alice: picks rank-1 extremal POVM
- Technical result: M rank-1 extremal $\implies \rho_{XE} \perp\!\!\!\perp \rho_B$

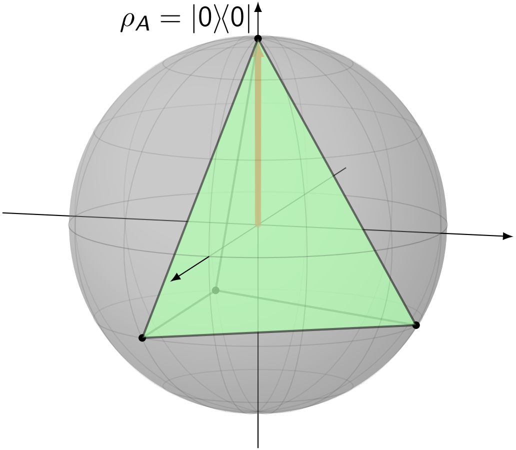
$\implies$ We only need to find the best rank-1 extremal POVM!

A simple case

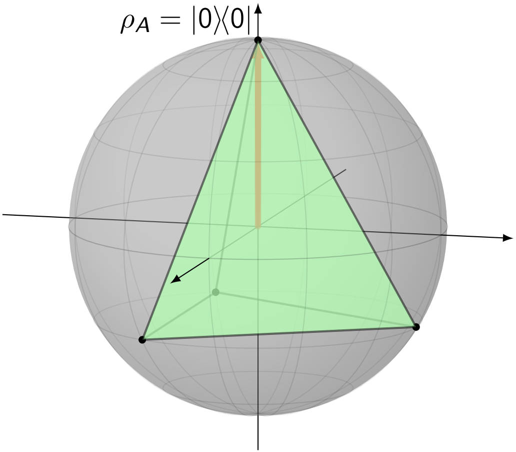


A simple case

Extremal

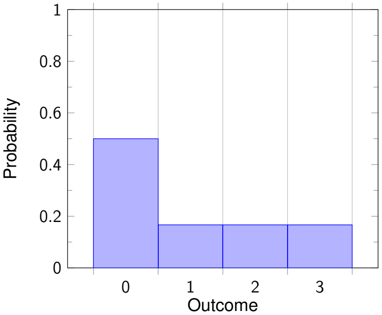


A simple case

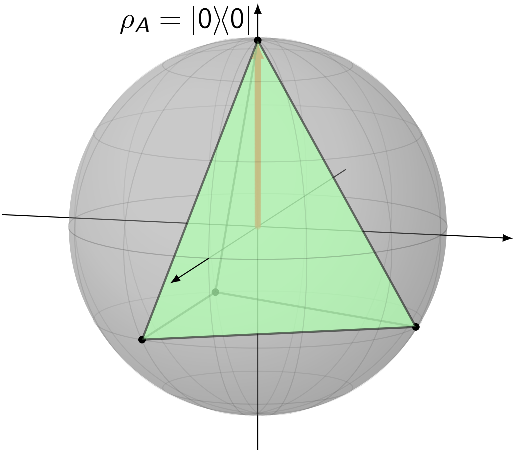


Extremal

$\min \mathbb{H}(X|E) \approx 1.792$



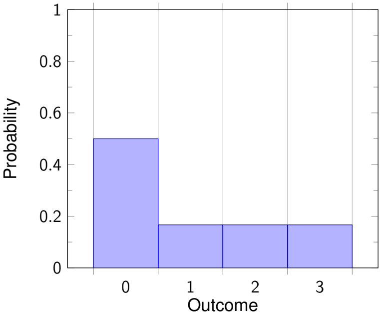
A simple case



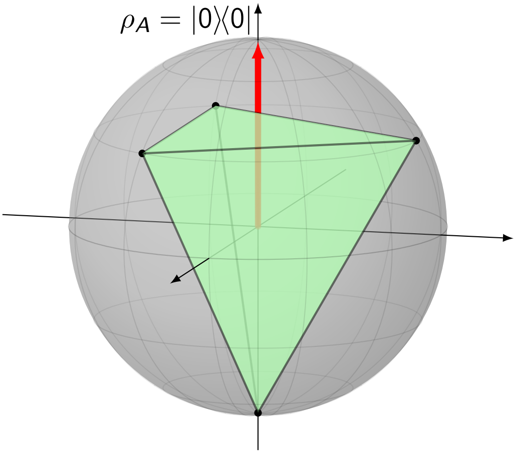
Extremal

$\min \mathbb{H}(X|E) \approx 1.792$

SIC-POVM



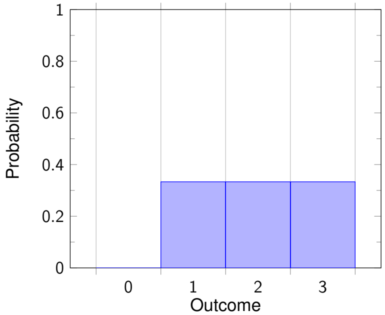
A simple case



Extremal

$\min \mathbb{H}(X|E) \approx 1.585$

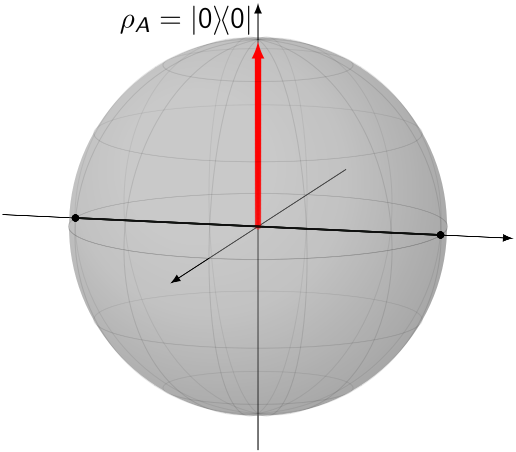
SIC-POVM

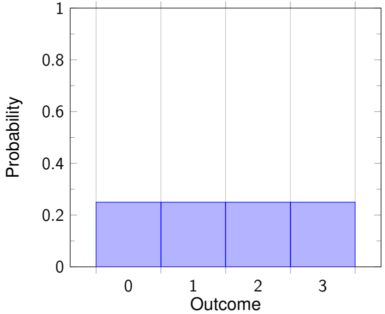


A simple case

Not extremal

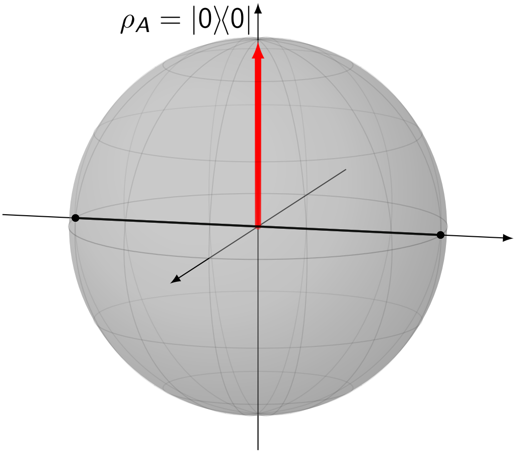
$\min \mathbb{H}(X|E) = 1$





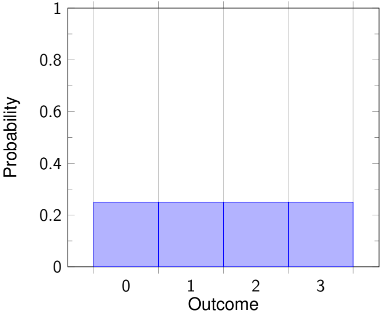
$$M = \left\{ \tfrac{1}{2} \left|+\right\rangle\!\left\langle+\right| , \tfrac{1}{2} \left|+\right\rangle\!\left\langle+\right| , \tfrac{1}{2} \left|-\right\rangle\!\left\langle-\right| , \tfrac{1}{2} \left|-\right\rangle\!\left\langle-\right| \right\}$$

A simple case



Not extremal

$\min \mathbb{H}(X|E) = 1$

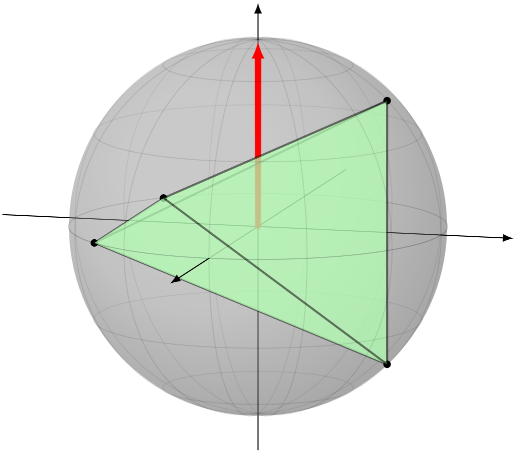


Key result: extremal rank-1 POVMs are dense within rank-1 POVMs

TELECOM Paris

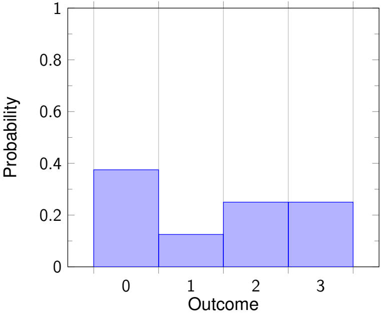
IP PARIS

A simple case



Extremal

$\min \mathbb{H}(X|E) \approx 2$



Analytical solution

Solve exactly for (operationally-relevant) sandwiched Rényi entropies H_α

TELECOM Paris IP PARIS

Analytical solution

Solve exactly for (operationally-relevant) sandwiched Rényi entropies H_α

$$\underbrace{\sup_{\{M_x\}_x} \min_{\rho_{AEB},\{P_x\}_x} H_\alpha(X|E)_{\rho_{XE}}} = \underbrace{\log\left(d_A^2\right)} - \underbrace{H_{\frac{\alpha}{2\alpha-1}}(A)}$$

Analytical solution

Solve exactly for (operationally-relevant) sandwiched Rényi entropies H_α

$$\underbrace{\sup_{\{M_x\}_x} \min_{\rho_{AEB},\{P_x\}_x} H_\alpha(X|E)_{\rho_{XE}}}_{\text{Maximum } H_\alpha\text{-randomness}} = \underbrace{\log\left(d_A^2\right)} - \underbrace{H_{\frac{\alpha}{2\alpha-1}}(A)}$$

Analytical solution

Solve exactly for (operationally-relevant) sandwiched Rényi entropies H_α

$$\underbrace{\sup_{\{M_x\}_x} \min_{\rho_{AEB}, \{P_x\}_x} H_\alpha(X|E)_{\rho_{XE}}}_{\text{Maximum } H_\alpha\text{-randomness}} = \underbrace{\log\left(d_A^2\right)}_{\text{Upper-bound}} - \underbrace{H_{\frac{\alpha}{2\alpha-1}}(A)}$$

Analytical solution

Solve exactly for (operationally-relevant) sandwiched Rényi entropies H_α

Extremal POVM

$$\underbrace{\sup_{\{M_x\}_x} \min_{\rho_{AEB},\{P_x\}_x} H_\alpha(X|E)_{\rho_{XE}}}_{\text{Maximum } H_\alpha\text{-randomness}} = \underbrace{\log\left(d_A^2\right)}_{\text{Upper-bound}} - \underbrace{H_{\frac{\alpha}{2\alpha-1}}(A)}$$

TELECOM Paris IP PARIS

Analytical solution

Solve exactly for (operationally-relevant) sandwiched Rényi entropies H_α

$$\underbrace{\sup_{\{M_x\}_x} \min_{\rho_{AEB},\{P_x\}_x} H_\alpha(X|E)_{\rho_{XE}}}_{\text{Maximum } H_\alpha\text{-randomness}} = \underbrace{\log\left(d_A^2\right)}_{\text{Upper-bound}} - \underbrace{H_{\frac{\alpha}{2\alpha-1}}(A)}_{\text{Side-information}}$$

Analytical solution

Solve exactly for (operationally-relevant) sandwiched Rényi entropies H_α

$$\underbrace{\sup_{\{M_x\}_x} \min_{\rho_{AEB},\{P_x\}_x} H_\alpha(X|E)_{\rho_{XE}}}_{\text{Maximum } H_\alpha\text{-randomness}} = \underbrace{\log\left(d_A^2\right)}_{\text{Upper-bound}} - \underbrace{H_{\frac{\alpha}{2\alpha-1}}(A)}_{\text{Side-information}}$$

Recovers the results of (Meng et al., 2024) if:

Analytical solution

Solve exactly for (operationally-relevant) sandwiched Rényi entropies H_α

$$\underbrace{\sup_{\{M_x\}_x} \min_{\rho_{AEB}, \{P_x\}_x} H_\alpha(X|E)_{\rho_{XE}}}_{\text{Maximum } H_\alpha\text{-randomness}} = \underbrace{\log\left(d_A^2\right)}_{\text{Upper-bound}} - \underbrace{H_{\frac{\alpha}{2\alpha-1}}(A)}_{\text{Side-information}}$$

Recovers the results of (Meng et al., 2024) if:

- Restrict to PVMs

Analytical solution

Solve exactly for (operationally-relevant) sandwiched Rényi entropies H_α

$$\underbrace{\sup_{\{M_x\}_x} \min_{\rho_{AEB},\{P_x\}_x} H_\alpha(X|E)_{\rho_{XE}}}_{\text{Maximum } H_\alpha\text{-randomness}} = \underbrace{\log\left(d_A^2\right)}_{\text{Upper-bound}} - \underbrace{H_{\frac{\alpha}{2\alpha-1}}(A)}_{\text{Side-information}}$$

Recovers the results of (Meng et al., 2024) if:

- Restrict to PVMs
- Pick $\alpha \to 1$ or $\alpha \to \infty$

TELECOM Paris IP PARIS

Main result

Main result

Let be a source producing a d-dimensional quantum state ρ_A.

Main result

Main result

Let be a source producing a d-dimensional quantum state ρ_A. There exists a protocol that extracts up to

$$\log\left(d_A^2\right) - \min_{\alpha \in (1,2]} \left(H_{\frac{\alpha}{2\alpha-1}} - \frac{\alpha}{\alpha-1}\log(\varepsilon) \right)$$

bits of ε-secure randomness.

Main result

Let be a source producing a d-dimensional quantum state ρ_A. There exists a protocol that extracts up to

$$\log\left(d_A^2\right) - \min_{\alpha \in (1,2]} \left(H_{\frac{\alpha}{2\alpha-1}} - \frac{\alpha}{\alpha-1} \log(\varepsilon) \right)$$

bits of ε-secure randomness.

- Quantifies how useful a given source is for QRNG

TELECOM Paris
IP PARIS

Main result

Let be a source producing a d-dimensional quantum state ρ_A. There exists a protocol that extracts up to

$$\log\left(d_A^2\right) - \min_{\alpha\in(1,2]}\left(H_{\frac{\alpha}{2\alpha-1}} - \frac{\alpha}{\alpha-1}\log(\varepsilon)\right)$$

bits of ε-secure randomness.

- Quantifies how useful a given source is for QRNG
- Easy-to-compute benchmarking tool

TELECOM Paris IP PARIS

Conclusion and future steps

- Conclusion
  - Analytical solutions to the maximal intrinsic randomness problem for operationally-relevant Rényi entropies

Conclusion and future steps

- Conclusion
  - Analytical solutions to the maximal intrinsic randomness problem for operationally-relevant Rényi entropies
  - Accounts for most general adversaries

TELECOM Paris IP PARIS

Conclusion and future steps

- Conclusion
  - Analytical solutions to the maximal intrinsic randomness problem for operationally-relevant Rényi entropies
  - Accounts for most general adversaries
  - Strong applications: simple-to-compute benchmarking tool for QRNG

Conclusion and future steps

- Conclusion
  - Analytical solutions to the maximal intrinsic randomness problem for operationally-relevant Rényi entropies
  - Accounts for most general adversaries
  - Strong applications: simple-to-compute benchmarking tool for QRNG
- Future steps
  - Limiting argument

Conclusion and future steps

- Conclusion
  - Analytical solutions to the maximal intrinsic randomness problem for operationally-relevant Rényi entropies
  - Accounts for most general adversaries
  - Strong applications: simple-to-compute benchmarking tool for QRNG
- Future steps
  - Limiting argument
    - Discontinuities $\implies$ hard to implement

Conclusion and future steps

- **Conclusion**
  - Analytical solutions to the maximal intrinsic randomness problem for operationally-relevant Rényi entropies
  - Accounts for most general adversaries
  - Strong applications: simple-to-compute benchmarking tool for QRNG
- **Future steps**
  - Limiting argument
    - Discontinuities $\implies$ hard to implement
    - Bound holds and is tight for general $d \cdots$

TELECOM Paris IP PARIS

Conclusion and future steps

- Conclusion
  - Analytical solutions to the maximal intrinsic randomness problem for operationally-relevant Rényi entropies
  - Accounts for most general adversaries
  - Strong applications: simple-to-compute benchmarking tool for QRNG
- Future steps
  - Limiting argument
    - Discontinuities $\Longrightarrow$ hard to implement
    - Bound holds and is tight for general $d \cdots$
    - $\cdots$ but reachability is only proven in the qubit case!

Conclusion and future steps

- Conclusion
  - Analytical solutions to the maximal intrinsic randomness problem for operationally-relevant Rényi entropies
  - Accounts for most general adversaries
  - Strong applications: simple-to-compute benchmarking tool for QRNG
- Future steps
  - Limiting argument
    - Discontinuities $\Longrightarrow$ hard to implement
    - Bound holds and is tight for general $d \cdots$
    - $\cdots$ but reachability is only proven in the qubit case!

Thanks!

Bibliography I

Dupuis, Frédéric (2023). “Privacy Amplification and Decoupling Without Smoothing”. In: *IEEE Transactions on Information Theory* 69.12, pp. 7784–7792. DOI: 10.1109/TIT.2023.3301812. arXiv: 2105.05342.

Meng, Shuyang et al. (July 2024). “Maximal intrinsic randomness of a quantum state”. In: *Phys. Rev. A* 110 (1), p. L010403. DOI: 10.1103/PhysRevA.110.L010403. arXiv: 2307.15708. URL: https://link.aps.org/doi/10.1103/PhysRevA.110.L010403.