The Uncertainty Relation and its Applications in Cryptography

Marco Tomamichel and Renato Renner

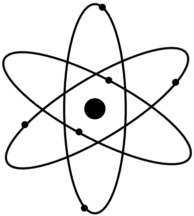
Institute for Theoretical Physics, ETH Zurich

partly joint work with Charles Ci Wen Lim and Nicolas Gisin
Group of Applied Physics, University of Geneva

[PRL **106**, 110506 (2011)] and [arXiv: 1103.4130]

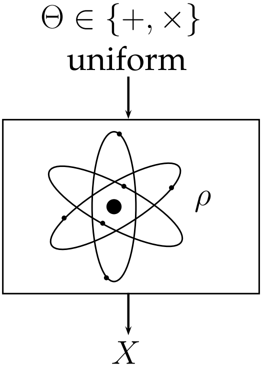
QCrypt, Zürich, September 2011

Classical Observers

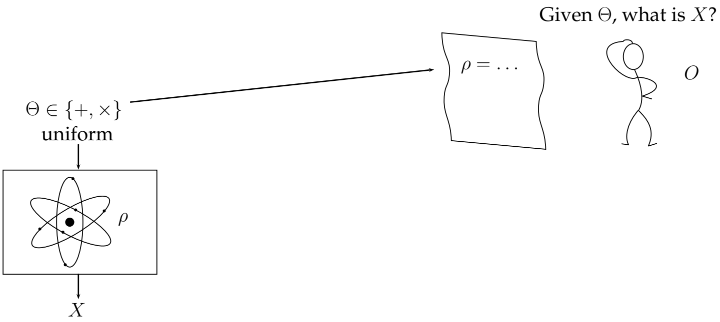


ρ

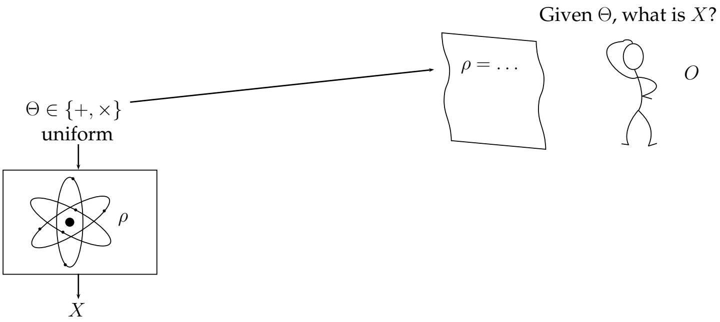
Classical Observers



Classical Observers

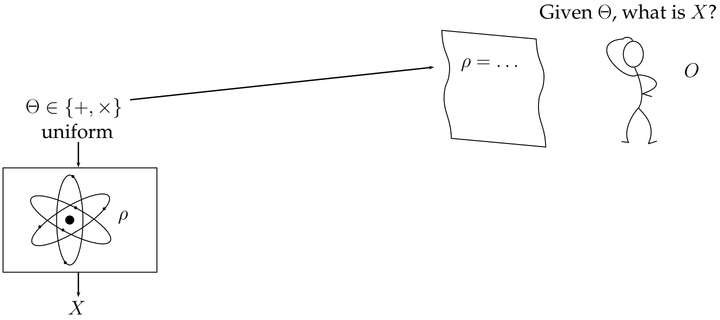


Classical Observers



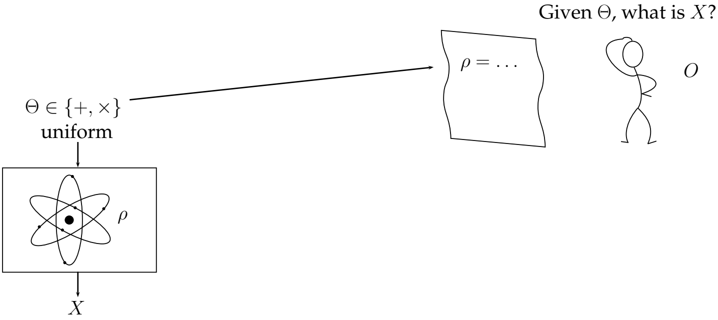
- Heisenberg uncertainty principle:
  Observer cannot predict outcome of both measurements.

Classical Observers



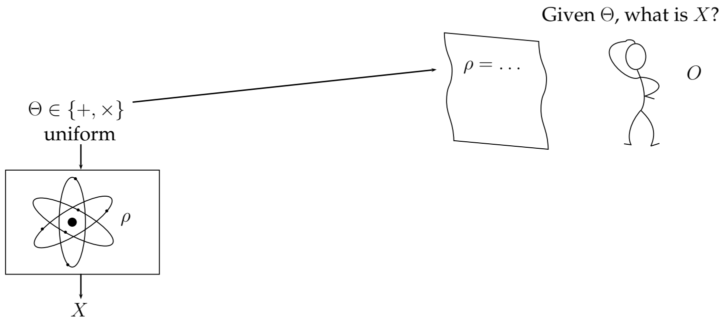
- Heisenberg uncertainty principle:
  Observer cannot predict outcome of both measurements.
- For qubits, unbiased bases and ρ eigenstate of '$+$':

$$H(X|O,\Theta) = \frac{1}{2}H(X|O,\Theta{=}+) + \frac{1}{2}H(X|O,\Theta{=}\times) = 0 + \frac{1}{2}.$$



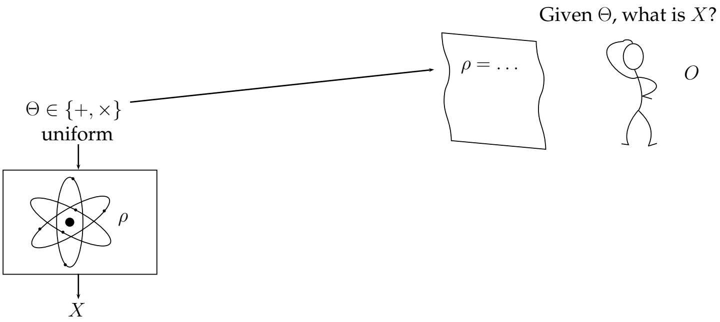
Deutsch, Maassen/Uffink 1988

For unbiased bases and qubits: $H(X|O,\Theta) \geq \frac{1}{2}$.



Deutsch, Maassen/Uffink 1988

For unbiased bases: $H(X|O,\Theta) \geq \frac{1}{2}\log_2 d$.

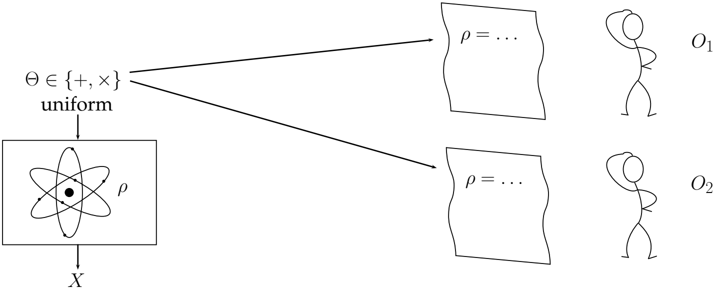


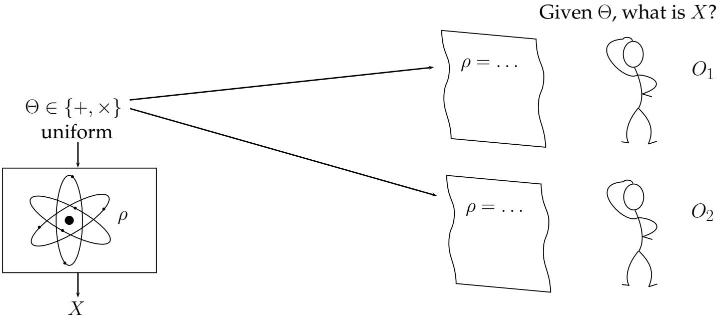
Deutsch, Maassen/Uffink 1988

$$H(X|O,\Theta) \geq \frac{1}{2}\log_2\frac{1}{c}, \quad c = \max_{x,y}\left|\langle x|y\rangle\right|^2,$$

where $|x\rangle$ and $|y\rangle$ are eigenvectors of the two measurements.

Given Θ, what is X?

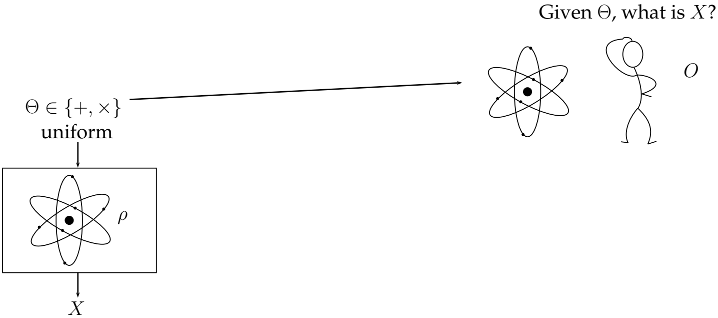


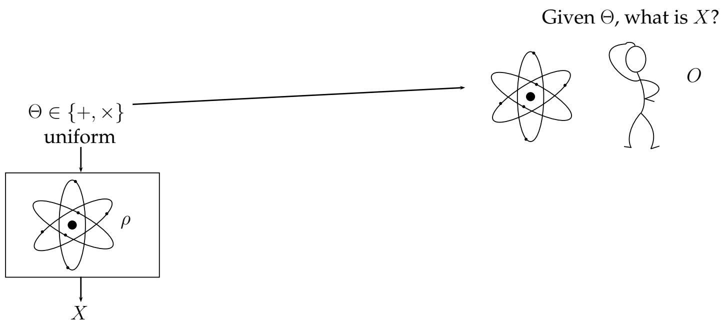


Deutsch, Maassen/Uffink 1988

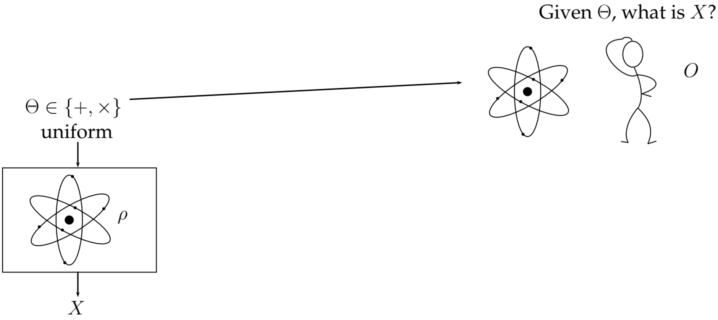
$$H(X|O_1, \Theta) + H(X|O_2, \Theta) \geq \log_2 \frac{1}{c} \, .$$

Quantum Observers

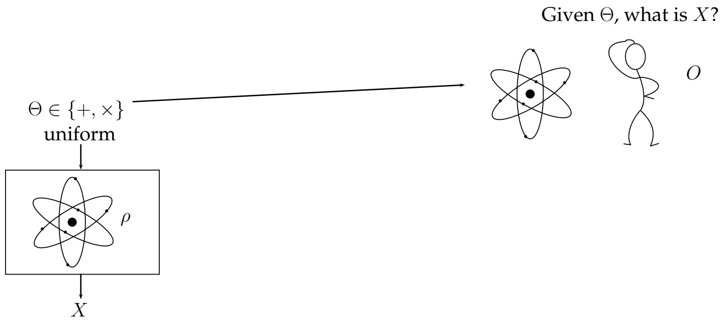




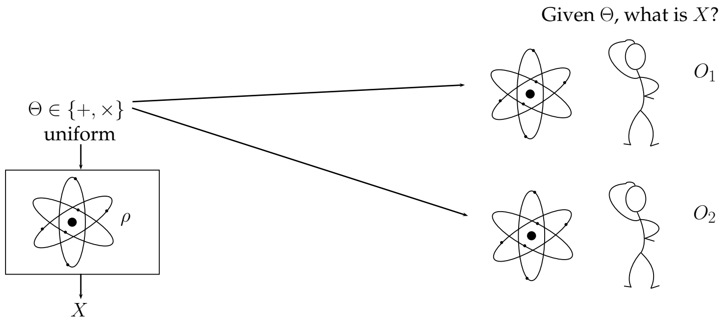
- Consider joint state ρ_{AO}.



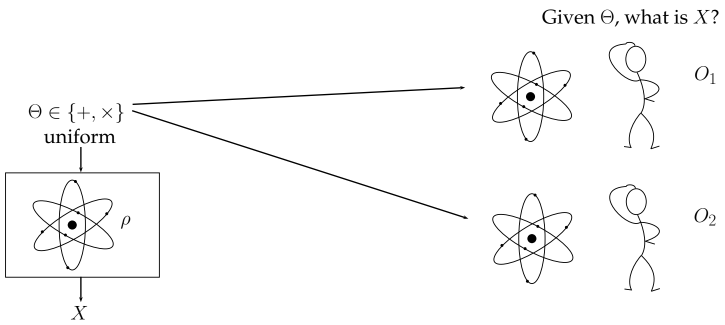
- Consider joint state ρ_{AO}.
- If $\rho_{AO} = |\psi\rangle\langle\psi|$ is fully entangled, then $H(X|O, \Theta) = 0$. (Observer chooses measurement on O — depending on Θ — to get perfect correlation with X.)



- Consider joint state ρ_{AO}.
- If $\rho_{AO} = |\psi\rangle\langle\psi|$ is fully entangled, then $H(X|O, \Theta) = 0$. (Observer chooses measurement on O — depending on Θ — to get perfect correlation with X.)
- No uncertainty relation here!

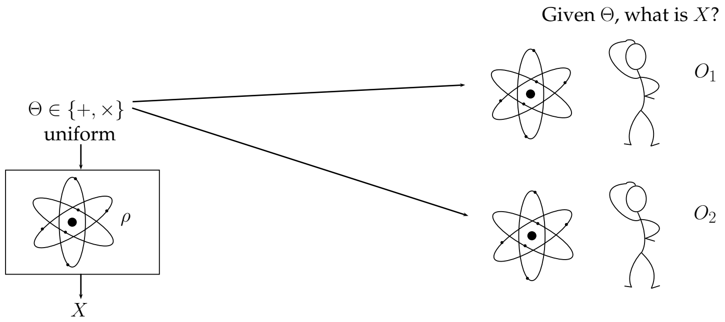


Can monogamy of entanglement help?

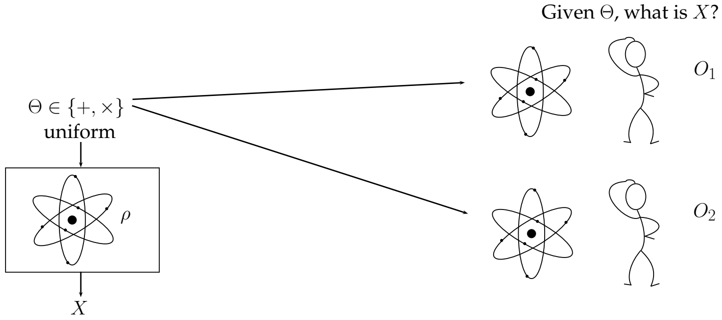


Berta et al. 2010, Coles et al. 2011

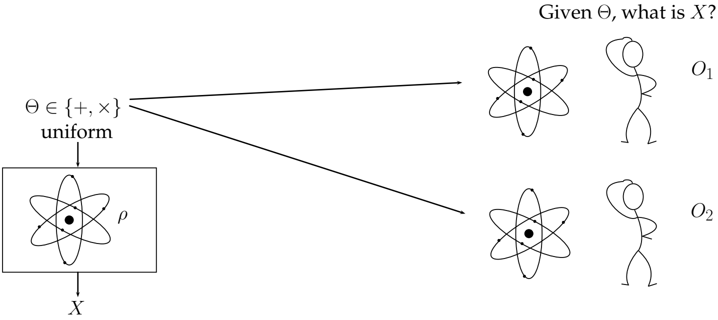
$$H(X|O_1, \Theta) + H(X|O_2, \Theta) \geq \log_2 \frac{1}{c}\,.$$



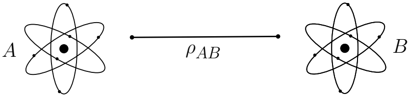
- (Conditional) von Neumann entropies have many applications.



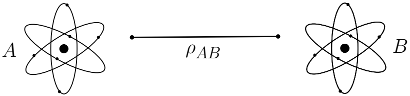
- (Conditional) von Neumann entropies have many applications.
- In some settings, e.g. in cryptography, other entropies are more relevant.



- (Conditional) von Neumann entropies have many applications.
- In some settings, e.g. in cryptography, other entropies are more relevant.
- We now extend the uncertainty relation to smooth entropies.

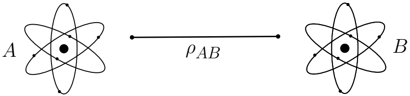


- A perfect observer B of a quantum system A is described by a state $|\psi\rangle\langle\psi|_{AB'} \otimes \sigma_{B''}$, where $|\psi\rangle$ is fully entangled.



- A perfect observer B of a quantum system A is described by a state $|\psi\rangle\langle\psi|_{AB'} \otimes \sigma_{B''}$, where $|\psi\rangle$ is fully entangled.
- Proximity to a perfect observer:

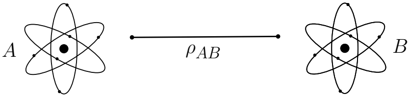
$$F_{\text{perfect}}(A|B) = \max_{B \to B'B''} \max_{\sigma} F\left(\rho_{AB'B''}, |\psi\rangle\langle\psi|_{AB'} \otimes \sigma_{B''}\right).$$



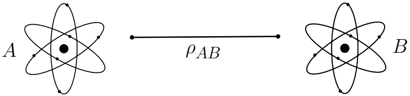
- A perfect observer B of a quantum system A is described by a state $|\psi\rangle\langle\psi|_{AB'} \otimes \sigma_{B''}$, where $|\psi\rangle$ is fully entangled.
- Proximity to a perfect observer:

$$F_{\text{perfect}}(A|B) = \max_{B \to B'B''} \max_{\sigma} F\big(\rho_{AB'B''}, |\psi\rangle\langle\psi|_{AB'} \otimes \sigma_{B''}\big).$$

- Min-Entropy: $H_{\min}(A|B) := -\log F^2_{\text{perfect}}(A|B)$.

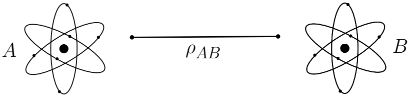


- An ignorant observer B of a quantum system A is described by a state $\omega_A \otimes \sigma_B$, where ω_A is completely mixed.



- An ignorant observer B of a quantum system A is described by a state $\omega_A \otimes \sigma_B$, where ω_A is completely mixed.
- Proximity to an ignorant observer:

$$F_{\text{ignorant}}(A|B) = \max_{\sigma} \; F\big(\rho_{AB}, \omega_A \otimes \sigma_B\big).$$



- An ignorant observer B of a quantum system A is described by a state $\omega_A \otimes \sigma_B$, where ω_A is completely mixed.
- Proximity to an ignorant observer:

$$F_{\text{ignorant}}(A|B) = \max_{\sigma} \; F\big(\rho_{AB}, \omega_A \otimes \sigma_B\big).$$

- Max-Entropy: $H_{\max}(A|B) := \log F^2_{\text{ignorant}}(A|B)$.

- We optimize entropies over a ball of close states, $\mathcal{B}^{\varepsilon}(\rho)$.

- We optimize entropies over a ball of close states, $\mathcal{B}^{\varepsilon}(\rho)$.
- Smooth Min-Entropy:

$$H_{\min}^{\varepsilon}(A|B)_{\rho} := \max_{\tilde{\rho}\in\mathcal{B}^{\varepsilon}(\rho)} H_{\min}(A|B)_{\tilde{\rho}}\,.$$

- We optimize entropies over a ball of close states, $\mathcal{B}^{\varepsilon}(\rho)$.
- Smooth Min-Entropy:

$$H_{\min}^{\varepsilon}(A|B)_{\rho} := \max_{\tilde{\rho} \in \mathcal{B}^{\varepsilon}(\rho)} H_{\min}(A|B)_{\tilde{\rho}} \,.$$

- For classical $A = X$, it characterizes the extractable independent randomness:

Renner 2005, MT/Schaffner/Smith/Renner 2011

The number of random bits — independent of a (quantum) memory B — that can be extracted from X is

$$\ell_{\text{extr}} \approx H_{\min}^{\varepsilon}(X|B) \,.$$

- Smooth Max-Entropy:

$$H_{\max}^{\varepsilon}(A|B)_{\rho} \;:=\; \min_{\tilde{\rho}\in\mathcal{B}^{\varepsilon}(\rho)} H_{\max}(A|B)_{\tilde{\rho}}\,.$$

- Smooth Max-Entropy:

$$H^{\varepsilon}_{\max}(A|B)_{\rho} \; := \min_{\tilde{\rho} \in \mathcal{B}^{\varepsilon}(\rho)} H_{\max}(A|B)_{\tilde{\rho}} \, .$$

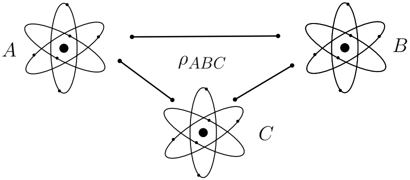
- For classical $A = X$, it characterizes the encoding length for data reconciliation:

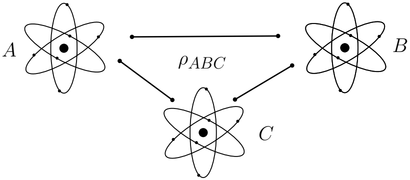
Renner/Renes 2010 [arXiv:1008.0452]

The number of bits needed to reconstruct X from a (quantum) memory B is

$$\ell_{\text{enc}} \approx H^{\varepsilon}_{\max}(X|B) \, .$$

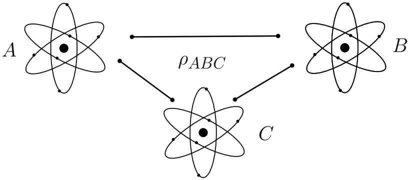
Duality





- Quantum mechanics implies uniqueness of perfect observer due to monogamy of entanglement. Moreover,

$$F_{\text{perfect}}(A|B) \leq F_{\text{ignorant}}(A|C)\,.$$

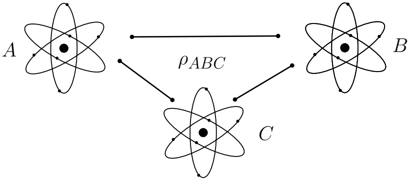


- Quantum mechanics implies uniqueness of perfect observer due to monogamy of entanglement. Moreover,

$$F_{\text{perfect}}(A|B) \leq F_{\text{ignorant}}(A|C)\,.$$

- In terms of entropies [König/Renner/Schafner, 2008]:

$$H_{\min}(A|B) + H_{\max}(A|C) \geq 0\,.$$



- Quantum mechanics implies uniqueness of perfect observer due to monogamy of entanglement. Moreover,

$$F_{\text{perfect}}(A|B) \leq F_{\text{ignorant}}(A|C) .$$

- In terms of entropies [König/Renner/Schafner, 2008]:

$$H_{\min}(A|B) + H_{\max}(A|C) \geq 0 .$$

- And smooth entropies [MT/Colbeck/Renner, 2010]:

$$H^{\varepsilon}_{\min}(A|B) + H^{\varepsilon}_{\max}(A|C) \geq 0 .$$

The uncertainty relation for smooth entropies:

MT/Renner 2011

For any state $\rho_{AO_1O_2}$, $\varepsilon \geq 0$ and POVMs $\{M_x\}$ and $\{N_y\}$ on A:

$$H^{\varepsilon}_{\min}(X|O_1, \Theta) + H^{\varepsilon}_{\max}(X|O_2, \Theta) \geq \log_2 \frac{1}{c},$$

$$c = \max_{x,y} \left\| \sqrt{M_x}\sqrt{N_y} \right\|^2_{\infty}.$$

- Overlap is $c = \max_{x,y} \left|\langle x|y\rangle\right|^2$ for projective measurements.

The uncertainty relation for smooth entropies:

MT/Renner 2011

For any state $\rho_{AO_1O_2}$, $\varepsilon \geq 0$ and POVMs $\{M_x\}$ and $\{N_y\}$ on A:

$$H^{\varepsilon}_{\min}(X|O_1,\Theta) + H^{\varepsilon}_{\max}(X|O_2,\Theta) \geq \log_2 \frac{1}{c},$$

$$c = \max_{x,y} \left\| \sqrt{M_x}\sqrt{N_y} \right\|^2_{\infty}.$$

- Overlap is $c = \max_{x,y} \left|\langle x|y\rangle\right|^2$ for projective measurements.
- This implies previous results for the von Neumann entropy due to asymptotic equipartition [MT/Colbeck/Renner, 2009]

$$\frac{1}{n} H^{\varepsilon}_{\min/\max}(A^n|B^n) \xrightarrow{n\to\infty,\,\varepsilon\to 0} H(A|B).$$

The uncertainty relation for smooth entropies:

MT/Renner 2011

For any state $\rho_{AO_1O_2}$, $\varepsilon \geq 0$ and POVMs $\{M_x\}$ and $\{N_y\}$ on A:

$$H^{\varepsilon}_{\min}(X|O_1,\Theta) + H^{\varepsilon}_{\max}(X|O_2,\Theta) \geq \log_2 \frac{1}{c},$$

$$c = \max_{x,y} \left\| \sqrt{M_x}\sqrt{N_y} \right\|^2_{\infty}.$$

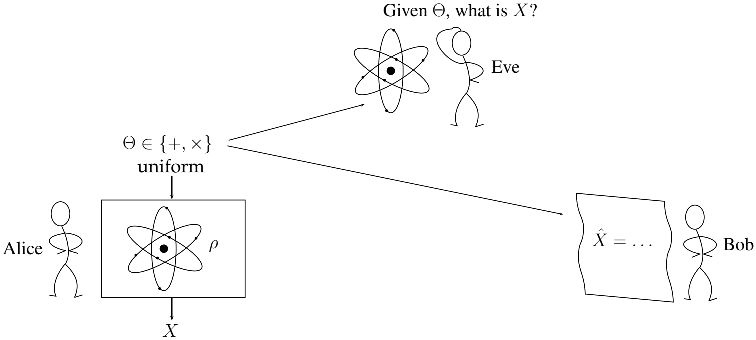
- Overlap is $c = \max_{x,y} \left|\langle x|y\rangle\right|^2$ for projective measurements.
- This implies previous results for the von Neumann entropy due to asymptotic equipartition [MT/Colbeck/Renner, 2009]

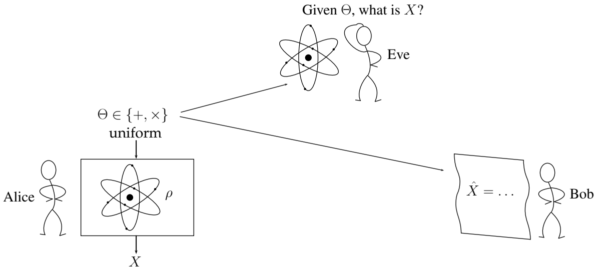
$$\frac{1}{n} H^{\varepsilon}_{\min/\max}(A^n|B^n) \xrightarrow{n\to\infty,\ \varepsilon\to 0} H(A|B).$$

- Operational quantities $\Longrightarrow$ Applications in cryptography.

- We consider the entanglement-based Bennett-Brassard 1984 protocol [Bennett/Brassard/Mermin, 1992]

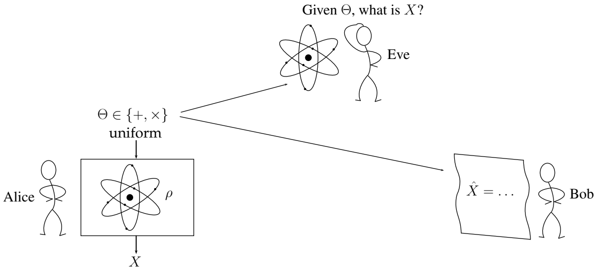
- We consider the entanglement-based Bennett-Brassard 1984 protocol [Bennett/Brassard/Mermin, 1992]
- The situation after Bob measured and holds an estimate $\hat{X}$ of X looks as follows:



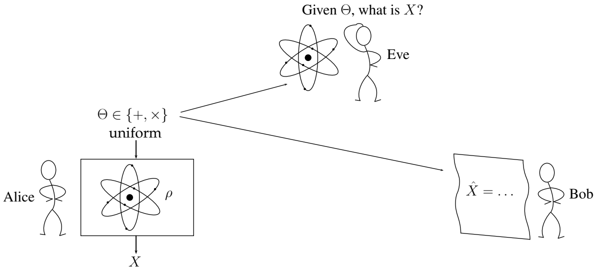


- Overlap: $\log_2 \frac{1}{c} = 1$ per bit. (qubits and unbiased bases)

Security Proof Sketch

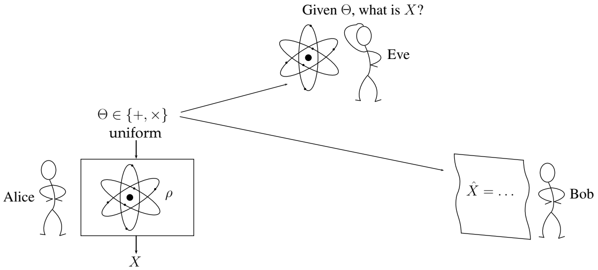


- Overlap: $\log_2 \frac{1}{c} = 1$ per bit. (qubits and unbiased bases)
- Uncertainty for n bits: $H^{\varepsilon}_{\min}(X^n|E, \Theta^n) \geq n - H^{\varepsilon}_{\max}(X^n|\hat{X}^n)$.



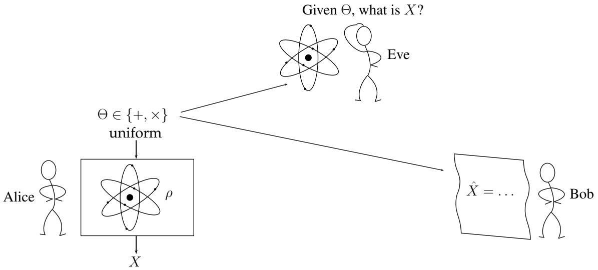
- Overlap: $\log_2 \frac{1}{c} = 1$ per bit. (qubits and unbiased bases)
- Uncertainty for n bits: $H_{\min}^{\varepsilon}(X^n|E,\Theta^n) \geq n - H_{\max}^{\varepsilon}(X^n|\hat{X}^n)$.
- Secret key:

$$\ell_{\mathrm{sec}} \gtrsim \ell_{\mathrm{extr}} - \ell_{\mathrm{enc}}$$



- Overlap: $\log_2 \frac{1}{c} = 1$ per bit. (qubits and unbiased bases)
- Uncertainty for n bits: $H_{\min}^{\varepsilon}(X^n|E,\Theta^n) \geq n - H_{\max}^{\varepsilon}(X^n|\hat{X}^n)$.
- Secret key:

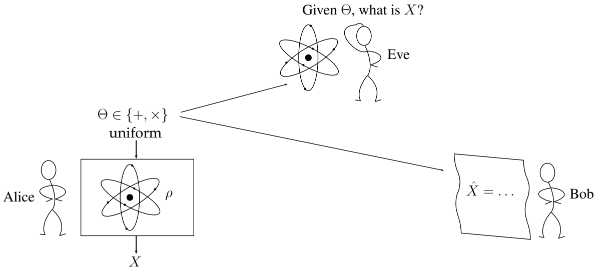
$$\begin{aligned} \ell_{\text{sec}} &\gtrsim \ell_{\text{extr}} - \ell_{\text{enc}} \\ &\approx H_{\min}^{\varepsilon}(X^n|E,\Theta^n) - H_{\max}^{\varepsilon}(X^n|\hat{X}^n) \end{aligned}$$



- Overlap: $\log_2 \frac{1}{c} = 1$ per bit. (qubits and unbiased bases)
- Uncertainty for n bits: $H_{\min}^{\varepsilon}(X^n|E,\Theta^n) \geq n - H_{\max}^{\varepsilon}(X^n|\hat{X}^n)$.
- Secret key:

$$\begin{aligned}\ell_{\text{sec}} &\gtrsim \ell_{\text{extr}} - \ell_{\text{enc}} \\ &\approx H_{\min}^{\varepsilon}(X^n|E,\Theta^n) - H_{\max}^{\varepsilon}(X^n|\hat{X}^n) \\ &\geq n - 2H_{\max}^{\varepsilon}(X^n|\hat{X}^n)\,.\end{aligned}$$

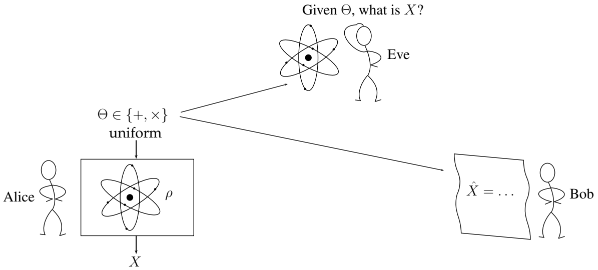
Security Proof Sketch



- Overlap: $\log_2 \frac{1}{c} = 1$ per bit. (qubits and unbiased bases)
- Uncertainty for n bits: $H_{\min}^{\varepsilon}(X^n|E, \Theta^n) \geq n - H_{\max}^{\varepsilon}(X^n|\hat{X}^n)$.
- Secret key:

$$\ell_{\text{sec}} \gtrsim n - 2H_{\max}^{\varepsilon}(X^n|\hat{X}^n)$$

- Parameter esimation: $\lambda = \frac{1}{k}|X^k \oplus \hat{X}^k|$.



- Overlap: $\log_2 \frac{1}{c} = 1$ per bit. (qubits and unbiased bases)
- Uncertainty for n bits: $H_{\min}^{\varepsilon}(X^n|E, \Theta^n) \geq n - H_{\max}^{\varepsilon}(X^n|\hat{X}^n)$.
- Secret key:

$$\ell_{\text{sec}} \gtrsim n - 2H_{\max}^{\varepsilon}(X^n|\hat{X}^n)$$

- Parameter esimation: $\lambda = \frac{1}{k}|X^k \oplus \hat{X}^k|$.
- Then, estimate $H_{\max}^{\varepsilon}(X^n|\hat{X}^n) \lesssim nh(\lambda)$.

The extractable ϵ-secure key per block of size $N = n + k$ is

$$\ell^{\epsilon} \leq n\big(1 - h(Q_{\text{tol}} + \mu)\big) - 3\log(3/\epsilon) - \text{leak}_{\text{EC}}$$

- $\mu \approx \sqrt{1/k \cdot \ln(1/\epsilon)}$ is the statistical deviation from the tolerated channel noise, Q_{tol}.
- $\text{leak}_{\text{EC}} \approx nh(Q_{\text{tol}})$ is the information about the key leaked during error correction.
- The achievable key rate, ℓ/N, deviates from its optimal asymptotic value, $1 - 2h(Q)$, only by (unavoidable) terms that are due to finite statistics.

- The improved finite key bounds are due to the simplicity of the proof via the uncertainty relation.
  - Tomography of single quantum systems is unnecessary. Instead, the min-entropy of X^n is bounded directly.
  - Security against general attacks comes for free — no De Finetti or Post-Selection necessary.
- This proof technique can be applied to other problems in 3-party quantum cryptography.
- As pointed out by Hayashi/Tsurumaru [`arXiv:1107.0589`], the key rates can be improved if we allow a dynamic protocol that chooses a different ℓ in each run.

- The smooth entropies and uncertainty relation have been generalized to von Neumann algebras. [Berta/Furrer/Scholz, `arXiv: 1107.5460`].
- It was shown that the (effective) overlap of two measurements can be bounded by the CHSH violation that can be achieved with them. [Hänggi/MT, `arXiv: 1108.5349`]
  This opens new avenues for device-independent cryptography.

- The smooth entropies and uncertainty relation have been generalized to von Neumann algebras. [Berta/Furrer/Scholz, `arXiv: 1107.5460`].
- It was shown that the (effective) overlap of two measurements can be bounded by the CHSH violation that can be achieved with them. [Hänggi/MT, `arXiv: 1108.5349`]
  This opens new avenues for device-independent cryptography.

Thank you for your attention.