Entropic Uncertainty Relations and their Applications in Quantum Cryptography

Marco Tomamichel

Centre for Quantum Technologies (CQT), National University of Singapore

ICITS 2013, Singapore
November 29, 2013

Take Home Message

Entropic uncertainty relations allow us to formalize physical intuition in information theoretic terms.

$+$

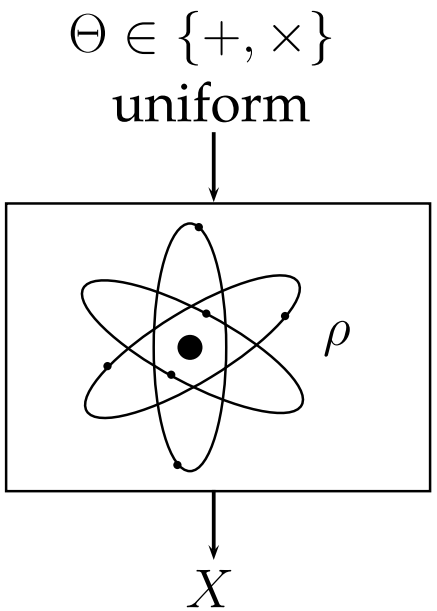
The min-entropy is the preferred measure of uncertainty for cryptographic applications.

$=$

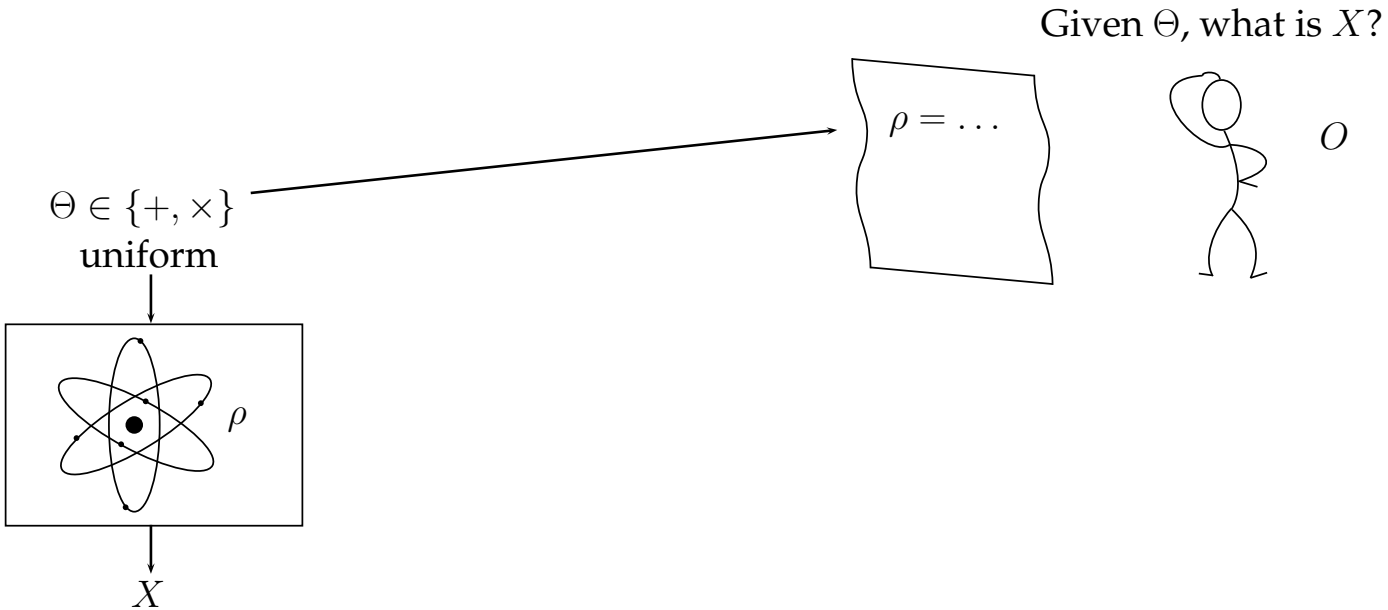
Uncertainty relations in terms of the min-entropy consequently have a wide range of applications in quantum cryptography.

From Quantum Systems to Random Variables

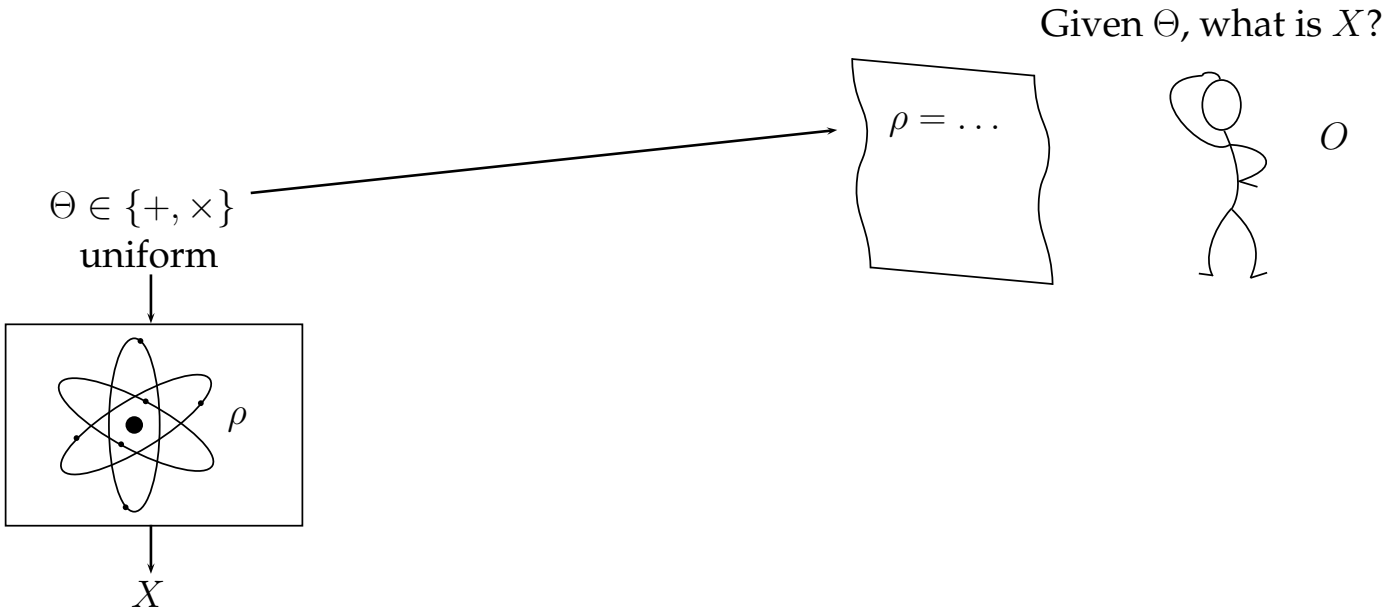
- Simplest example: Measure photon polarization in rectilinear '$+$' or diagonal '$\times$' basis.
- More generally, we consider two arbitrary measurements on an arbitrary quantum system in state ρ.



Uncertainty Relation with Classical Observer

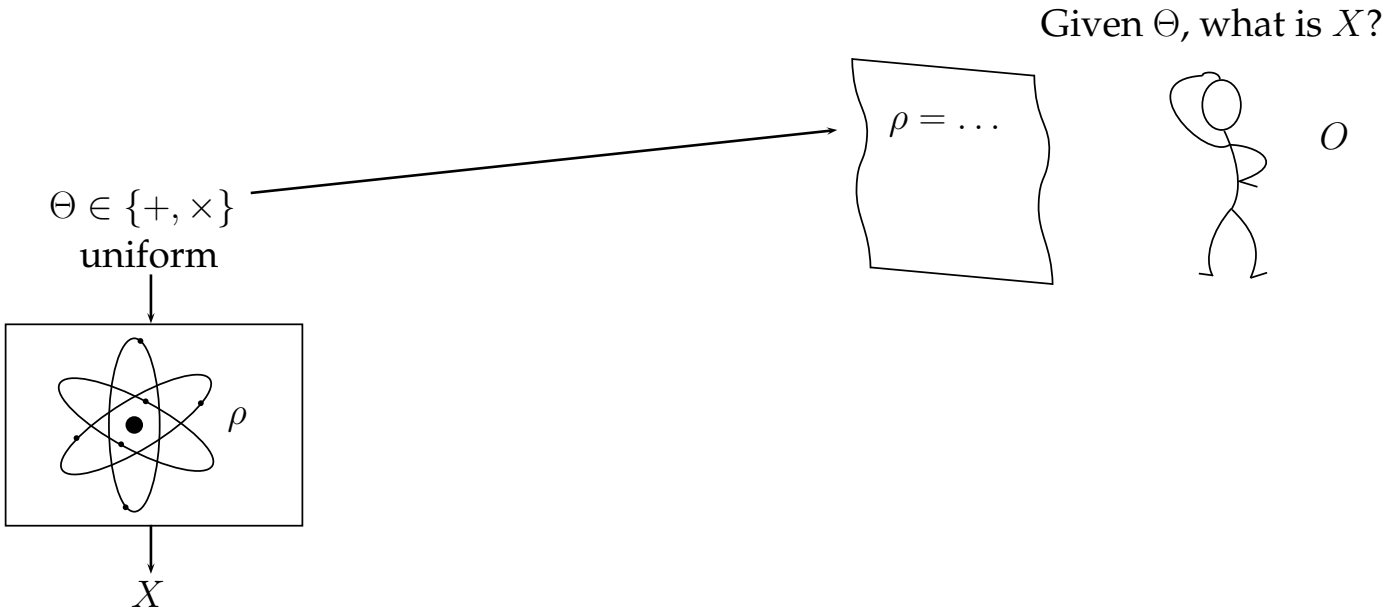


Uncertainty Relation with Classical Observer



- Heisenberg's uncertainty principle [Hei27]:
  It is impossible to predict the outcome of both measurements.

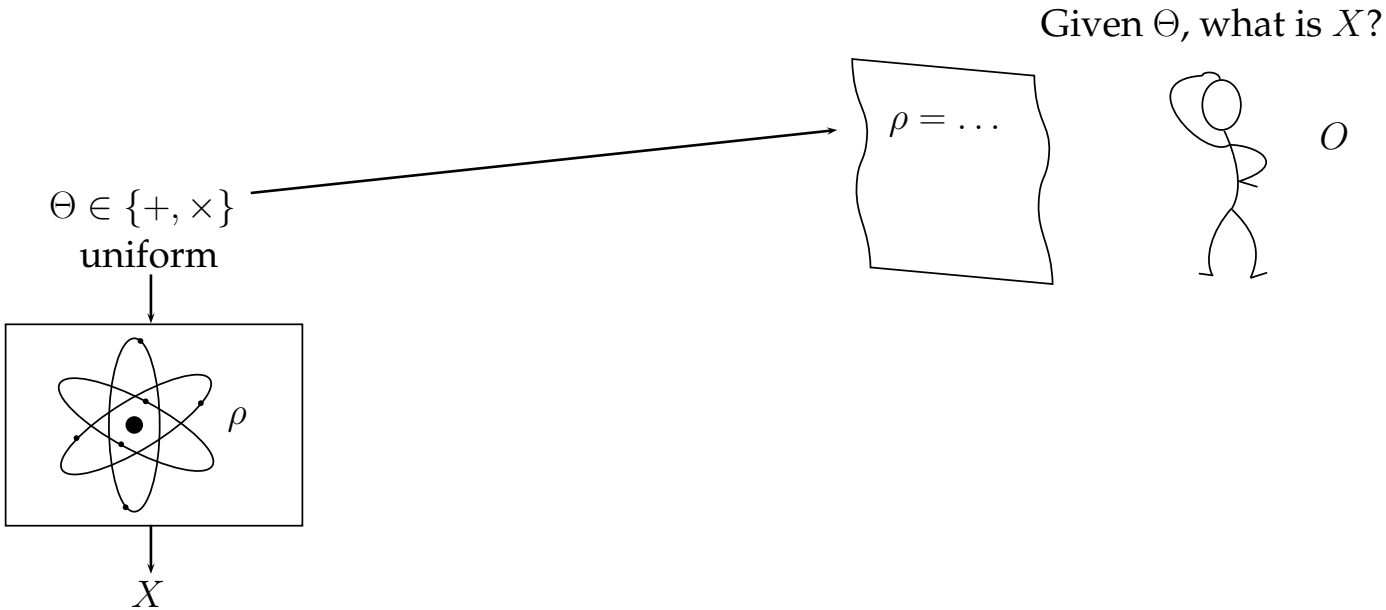
Uncertainty Relation with Classical Observer



- Heisenberg's uncertainty principle [Hei27]:
  It is impossible to predict the outcome of both measurements.
- Deutsch [Deu83] proposed to characterize this uncertainty in terms of the Shannon entropy [Sha48].

$$H(X) := \sum_x P_X(x) \log \frac{1}{P_X(x)}, \quad H(X|Y) := \sum_y P_Y(y)\, H(X|Y=y).$$

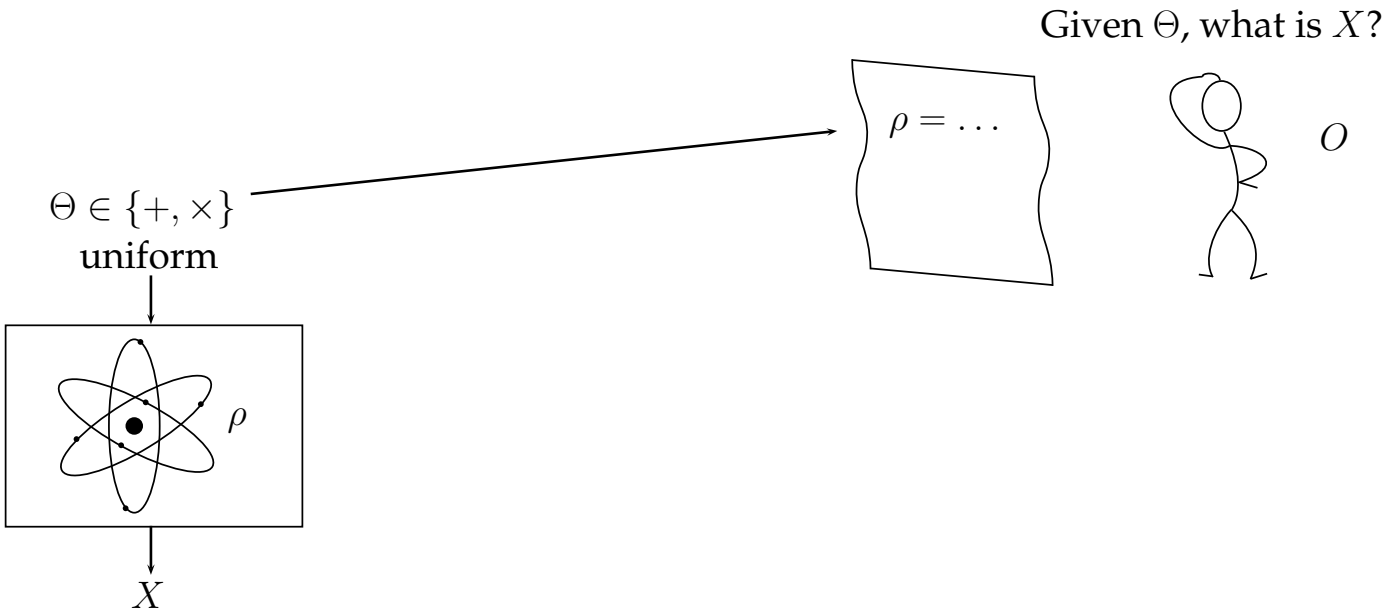
Uncertainty Relation with Classical Observer



- Simplest example: measure polarization for photon prepared in the rectilinear '+' basis.

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

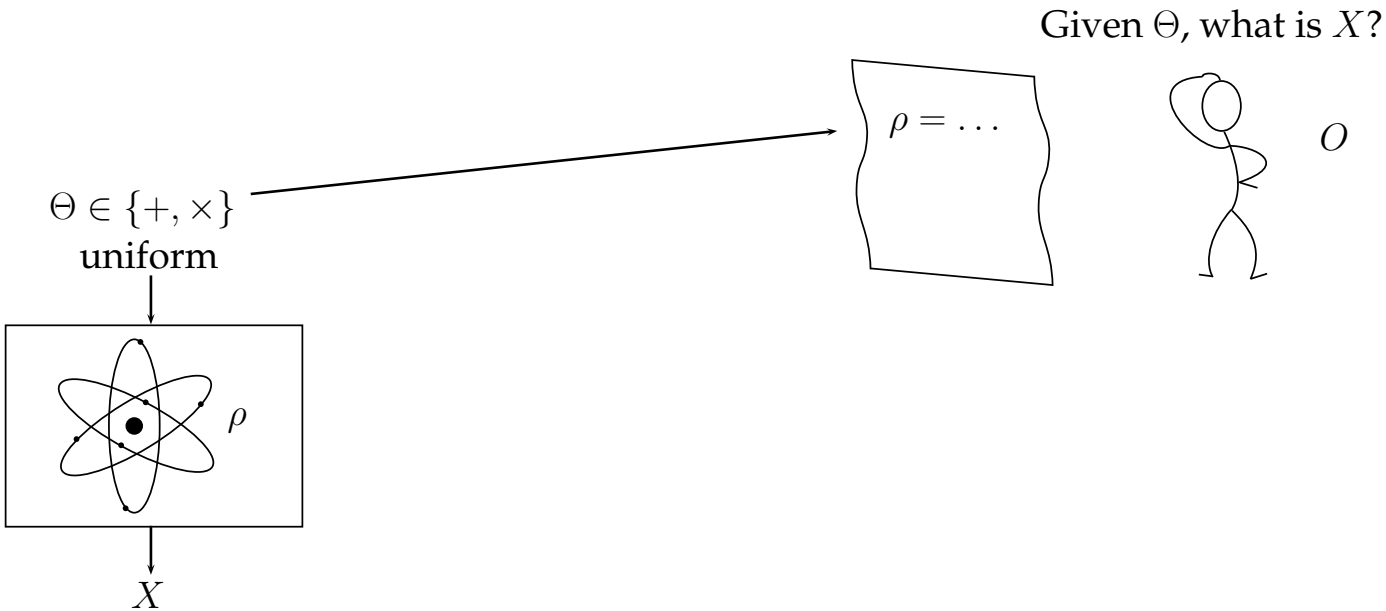
Uncertainty Relation with Classical Observer



- Simplest example: measure polarization for photon prepared in the rectilinear '+' basis.

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

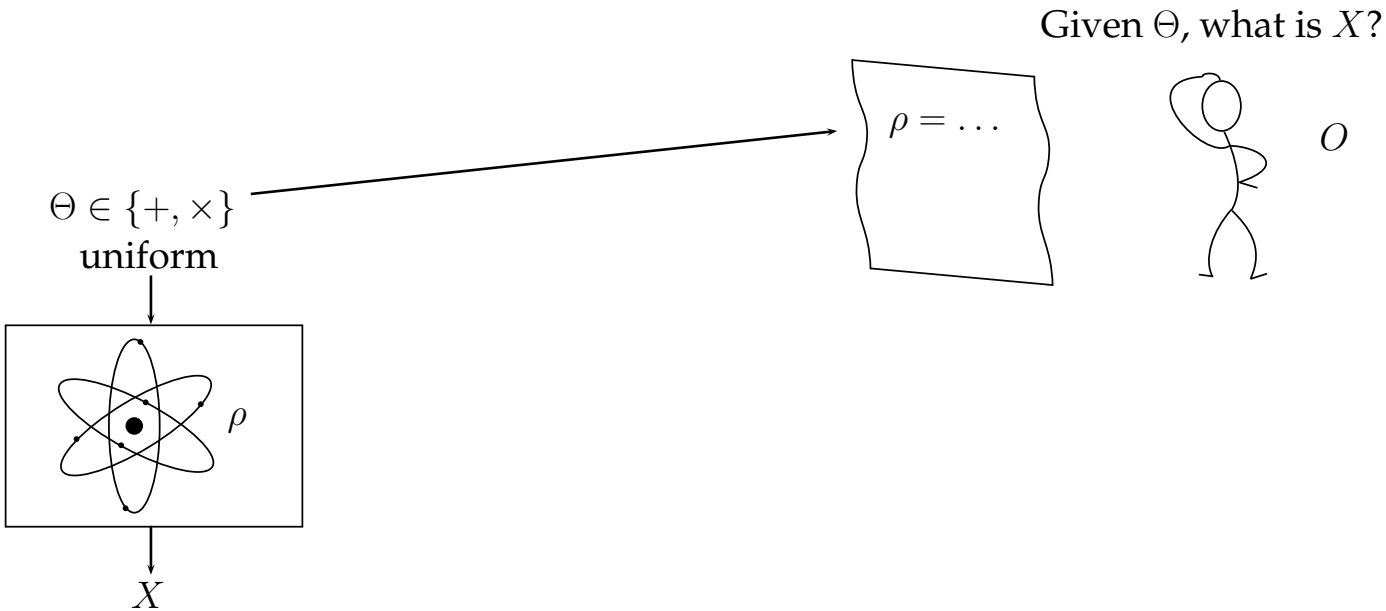
Uncertainty Relation with Classical Observer



- Simplest example: measure polarization for photon prepared in the rectilinear '+' basis.

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

Uncertainty Relation with Classical Observer

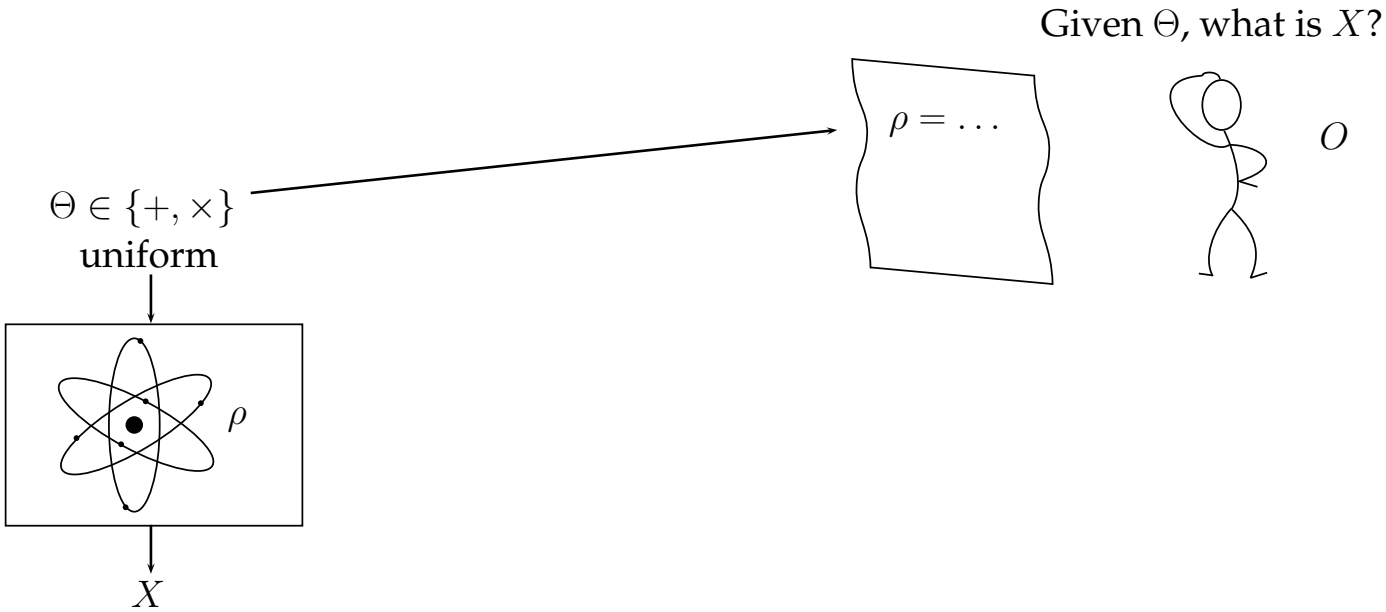


- Simplest example: measure polarization for photon prepared in the rectilinear '+' basis.

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

- In fact, the bound $H(X|O,\Theta) \geq \frac{1}{2}$ holds independently of how the state ρ is prepared!

Uncertainty Relation with Classical Observer



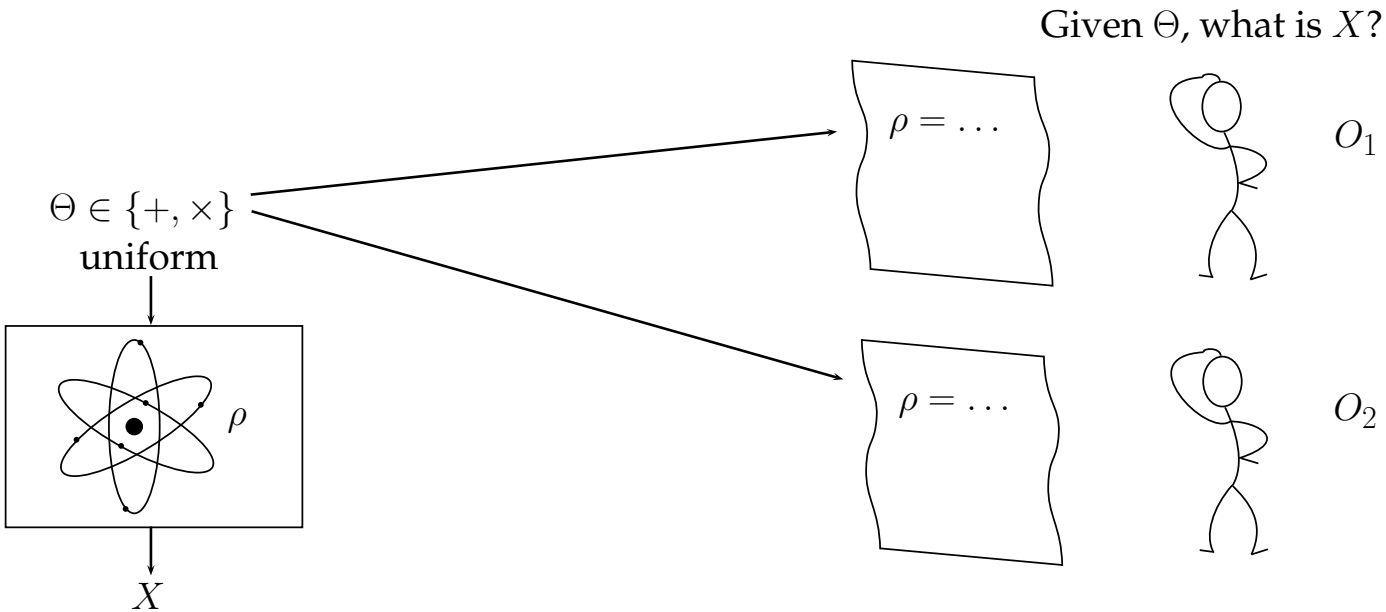
More generally, for arbitrary projective measurements:

Maassen & Uffink [MU88]

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

where c is called *overlap* and $\left\{|\phi_x^+\rangle\right\}_x$ and $\left\{|\phi_y^\times\rangle\right\}_y$ are the eigenvectors of the respective measurements.

Uncertainty Relation with Two Classical Observers

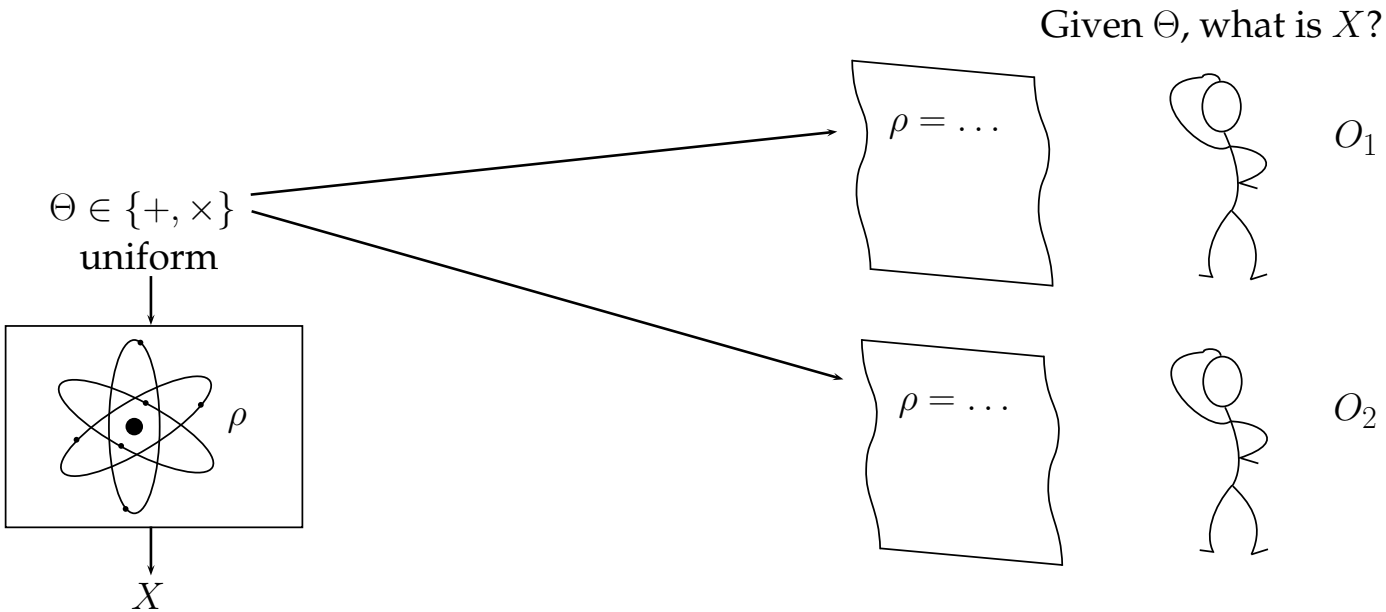


The previous relations trivially extends to two observers:

Maassen & Uffink [MU88]

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

Uncertainty Relation with Two Classical Observers



More generally, the relation also holds for Rényi entropies [Rén61]:

Maassen & Uffink [MU88]

$$H_\alpha(X|O_1,\Theta) + H_\beta(X|O_2,\Theta) \geq \log \frac{1}{c}, \quad \text{where} \quad \frac{1}{\alpha} + \frac{1}{\beta} = 2.$$

Classical Rényi Entropy Intermezzo

- Rényi [Rén61] defined a family of divergences for $\alpha \in [0, \infty]$ as

$$D_\alpha(P\|Q) := \frac{1}{\alpha - 1} \log \sum_z P(z)^\alpha Q(z)^{1-\alpha},$$

taking limits where necessary.

Classical Rényi Entropy Intermezzo

- Rényi [Rén61] defined a family of divergences for $\alpha \in [0, \infty]$ as

$$D_\alpha(P\|Q) := \frac{1}{\alpha - 1} \log \sum_z P(z)^\alpha Q(z)^{1-\alpha},$$

  taking limits where necessary.
- The Rényi entropy is related to the divergence,

$$H_\alpha(X) := \frac{1}{1-\alpha} \log \sum_x P_X(x)^\alpha = -D_\alpha(P_X\|1_X)\,.$$

- The proper extension to conditional Rényi entropy is disputed. Here we employ a definition due to Arimoto [Ari73]:

$$H_\alpha(X|Y) := \frac{\alpha}{1-\alpha} \log \left(\sum_y P_Y(y) \exp\left(\frac{1-\alpha}{\alpha} H_\alpha(X|Y=y) \right) \right)$$

Classical Rényi Entropy Intermezzo

- Rényi [Rén61] defined a family of divergences for $\alpha \in [0, \infty]$ as

$$D_\alpha(P\|Q) := \frac{1}{\alpha - 1} \log \sum_z P(z)^\alpha Q(z)^{1-\alpha},$$

  taking limits where necessary.
- The Rényi entropy is related to the divergence,

$$H_\alpha(X) := \frac{1}{1-\alpha} \log \sum_x P_X(x)^\alpha = -D_\alpha(P_X\|1_X)\,.$$

- The proper extension to conditional Rényi entropy is disputed. Here we employ a definition due to Arimoto [Ari73]:

$$H_\alpha(X|Y) := \frac{\alpha}{1-\alpha} \log \left(\sum_y P_Y(y) \exp\left(\frac{1-\alpha}{\alpha} H_\alpha(X|Y=y) \right) \right)$$

$$= \frac{\alpha}{1-\alpha} \log \left(\sum_y P_Y(y) \left(\sum_x P_{X|Y}(x)^\alpha \right)^{\frac{1}{\alpha}} \right).$$

Classical Rényi Entropy Intermezzo

- Rényi [Rén61] defined a family of divergences for $\alpha \in [0, \infty]$ as

$$D_\alpha(P\|Q) := \frac{1}{\alpha - 1} \log \sum_z P(z)^\alpha Q(z)^{1-\alpha},$$

  taking limits where necessary.
- The Rényi entropy is related to the divergence,

$$H_\alpha(X) := \frac{1}{1-\alpha} \log \sum_x P_X(x)^\alpha = -D_\alpha(P_X\|1_X)\,.$$

- The proper extension to conditional Rényi entropy is disputed. Here we employ a definition due to Arimoto [Ari73]:

$$H_\alpha(X|Y) := \frac{\alpha}{1-\alpha} \log \left(\sum_y P_Y(y) \exp\left(\frac{1-\alpha}{\alpha} H_\alpha(X|Y=y) \right) \right).$$

- This extension is closely related to the Rényi divergence,

$$H_\alpha(X|Y) = \sup_{Q_Y} -D_\alpha(P_{XY}\|1_X \times Q_Y).$$

Classical Rényi Entropy Intermezzo

- The function $\alpha \to H_\alpha(X|Y)$ is monotonically decreasing.
- The Shannon entropy is $\lim_{\alpha\to 1} H_\alpha(X|Y) = H(X|Y)$.
- It satisfies a data-processing inequality. For any channel $Y \to Z$, we have

$$H_\alpha(X|Y) \leq H_\alpha(X|Z).$$

  Operationally, the uncertainty of X increases when we manipulate the side information Y.
- The quantity has found operational significance. In particular,

$$\lim_{\alpha\to\infty} H_\alpha(X|Y) = H_{\min}(X|Y) = -\log p_{\text{guess}}(X|Y),$$

  where $p_{\text{guess}}(X|Y) = \sum_y P_Y(y) \max_x P_{X|Y}(x)$ is the (average) probability of correctly guessing X given Y.

Min-Entropy and "Leftover Hashing"

- The omnipresence of the min-entropy in cryptography is due to the "Leftover Hashing" Lemma.

Bennett *et al.* [BBR88] & Impagliazzo *et al.* [ILL89, IZ89]

Let $X \in \mathcal{X}$ be such that $H_{\min}(X|E) \geq k$, and $\ell \in \mathbb{N}$. Then, there exists a family of Hash function $\{f_s\}_s$ from $\mathcal{X}$ to $\{0,1\}^\ell$ such that $f_S(X)$ is δ-close to uniform and independent of E and S, where

$$\delta \sim \sqrt{2^{\ell-k}}$$

and S is chosen uniformly at random.

Min-Entropy and "Leftover Hashing"

- The omnipresence of the min-entropy in cryptography is due to the "Leftover Hashing" Lemma.

Bennett *et al.* [BBR88] & Impagliazzo *et al.* [ILL89, IZ89]

Let $X \in \mathcal{X}$ be such that $H_{\min}^{\varepsilon}(X|E) \geq k$, and $\ell \in \mathbb{N}$. Then, there exists a family of Hash function $\{f_s\}_s$ from $\mathcal{X}$ to $\{0,1\}^{\ell}$ such that $f_S(X)$ is δ-close to uniform and independent of E and S, where

$$\delta \sim \sqrt{2^{\ell-k}} + 2\varepsilon$$

and S is chosen uniformly at random.

Min-Entropy and "Leftover Hashing"

- The omnipresence of the min-entropy in cryptography is due to the "Leftover Hashing" Lemma.

Bennett *et al.* [BBR88] & Impagliazzo *et al.* [ILL89, IZ89]

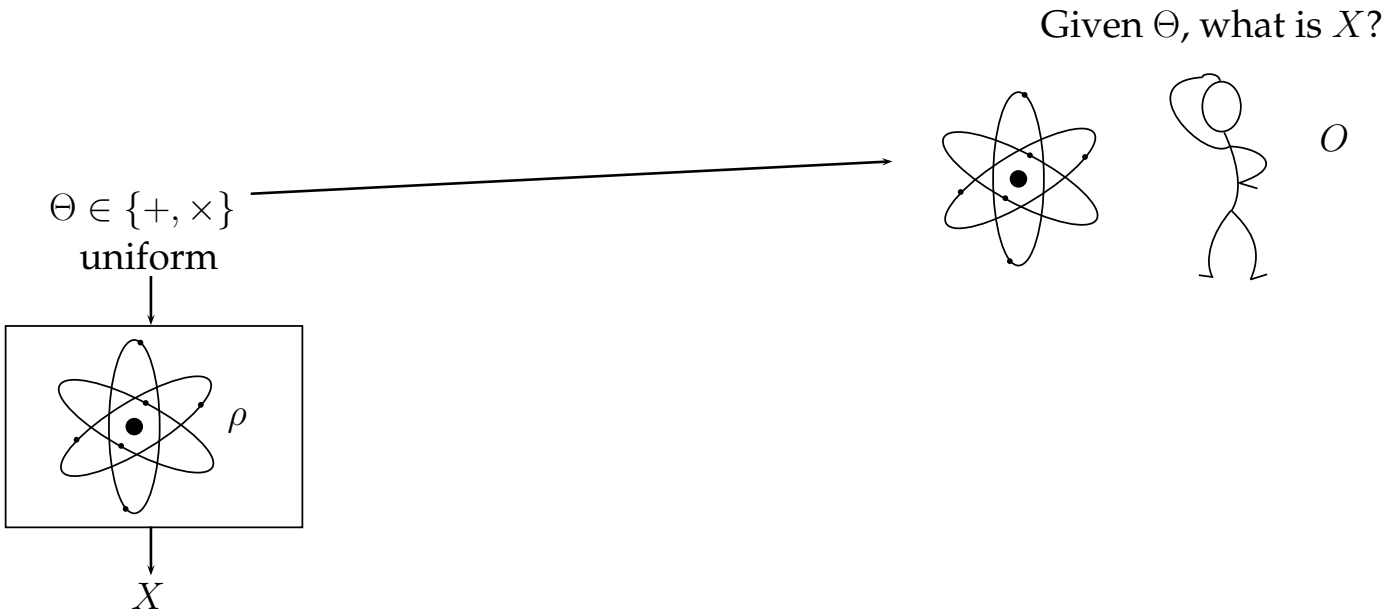
Let $X \in \mathcal{X}$ be such that $H_{\min}^{\varepsilon}(X|E) \geq k$, and $\ell \in \mathbb{N}$. Then, there exists a family of Hash function $\{f_s\}_s$ from $\mathcal{X}$ to $\{0,1\}^{\ell}$ such that $f_S(X)$ is δ-close to uniform and independent of E and S, where

$$\delta \sim \sqrt{2^{\ell-k}} + 2\varepsilon$$

and S is chosen uniformly at random.

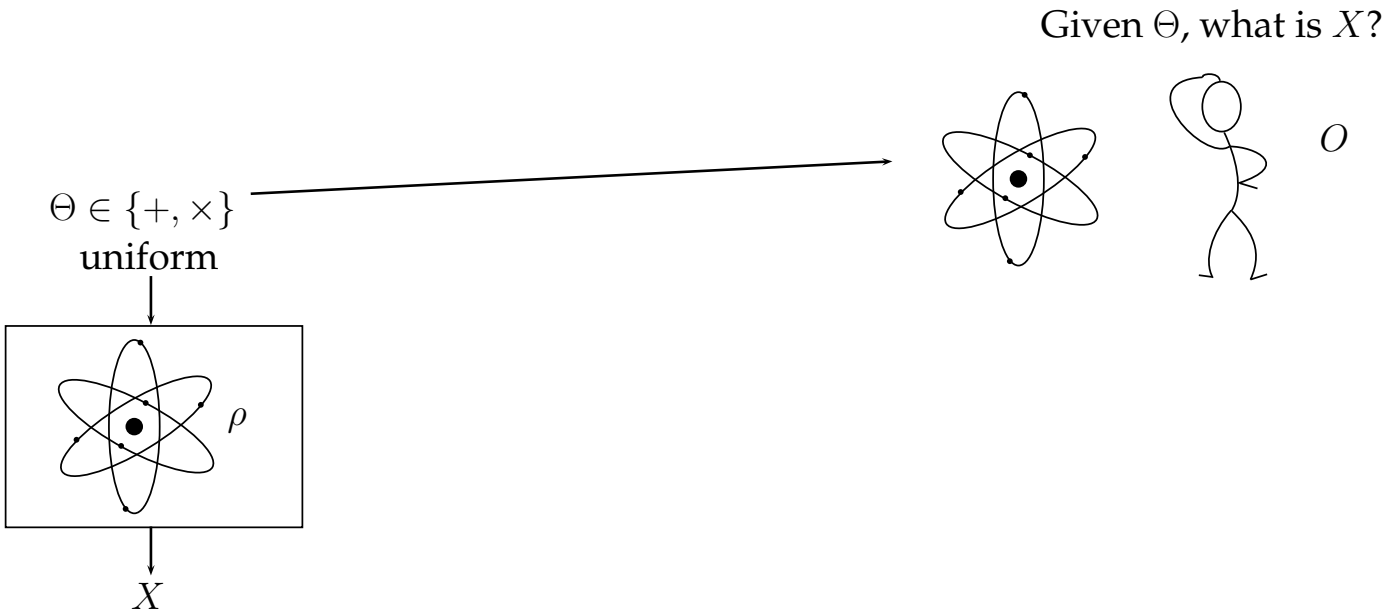
- This is "tight" in the sense that one cannot expect to extract more than $H_{\min}^{\varepsilon}(X|E)$ bits of uniform and independent randomness.

Uncertainty vs. Entanglement



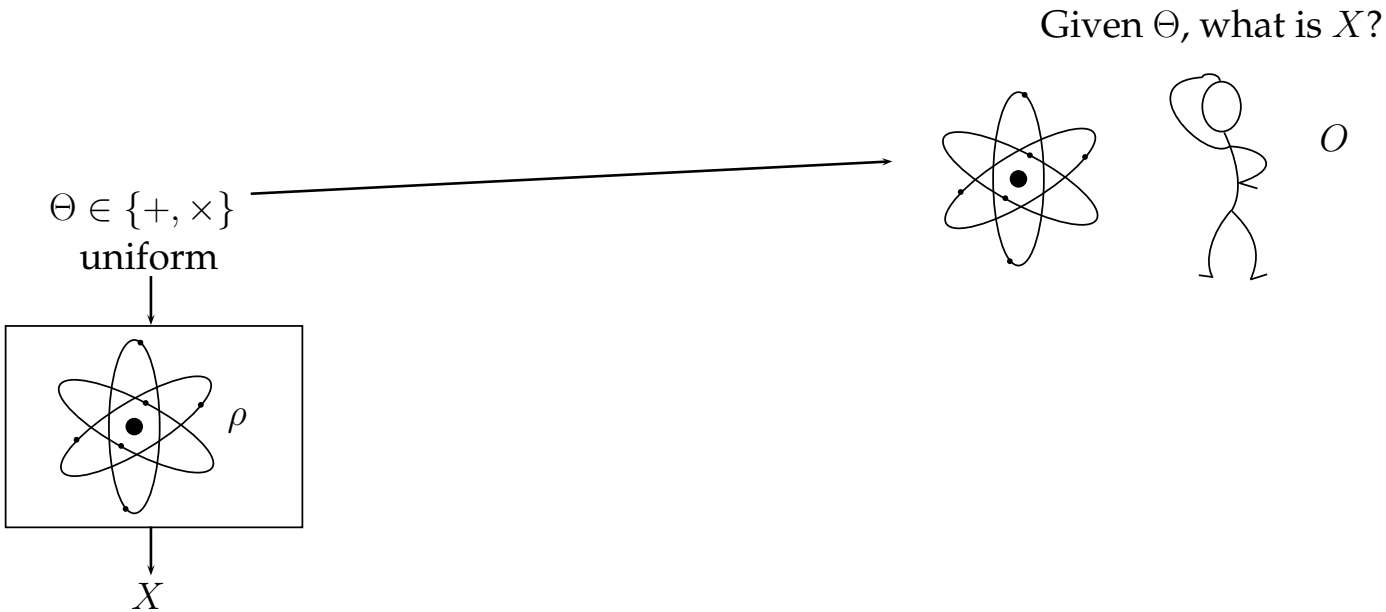
- Consider a joint quantum state ρ_{AO}.

Uncertainty vs. Entanglement



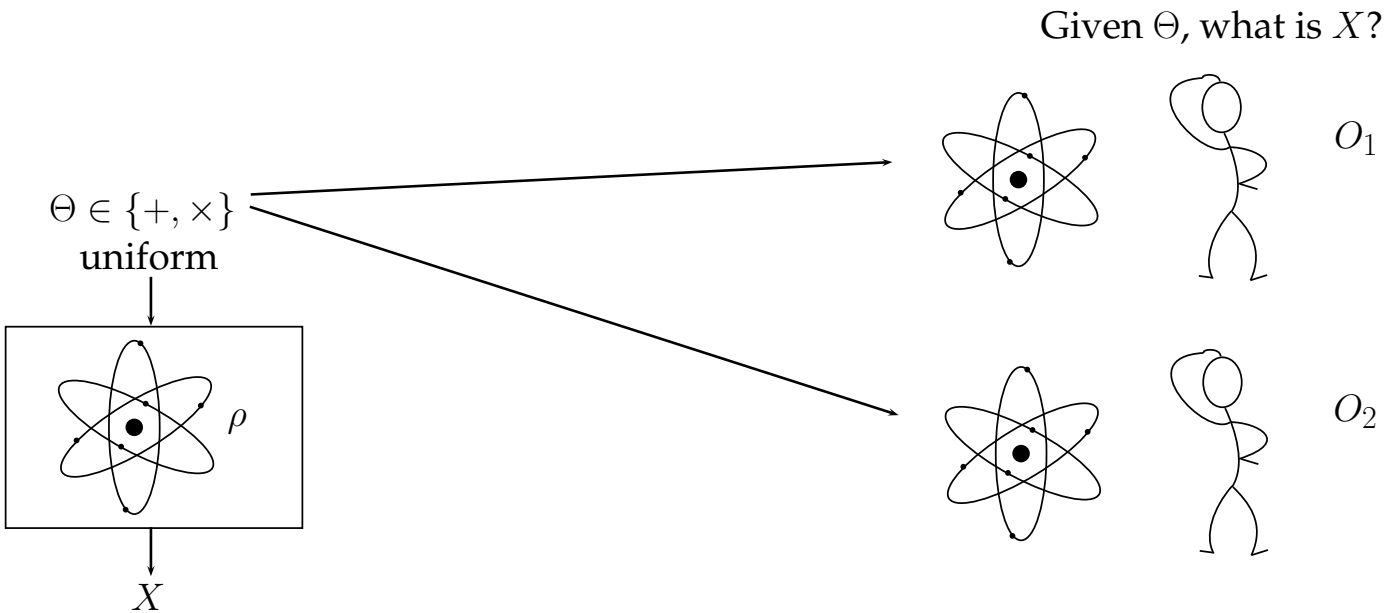
- Consider a joint quantum state ρ_{AO}.
- If $\rho_{AO} = |\psi\rangle\langle\psi|$ is maximally entangled then $H(X|O,\Theta) = 0$.
  - Why? The observer may choose a measurement on O — depending on Θ — to get perfect correlation with X.

Uncertainty vs. Entanglement



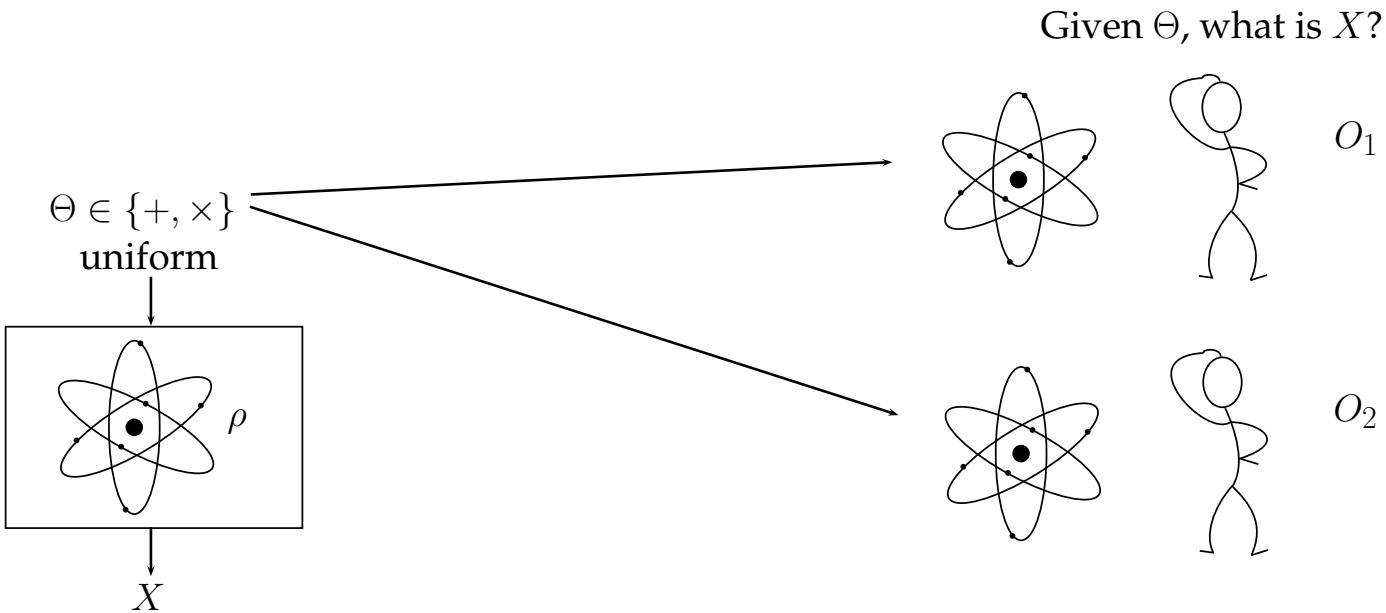
- Consider a joint quantum state ρ_{AO}.
- If $\rho_{AO} = |\psi\rangle\langle\psi|$ is maximally entangled then $H(X|O,\Theta) = 0$.
  - Why? The observer may choose a measurement on O — depending on Θ — to get perfect correlation with X.
- No uncertainty relation here!

Uncertainty and Monogamy of Entanglement



Can monogamy of entanglement help?

Uncertainty and Monogamy of Entanglement



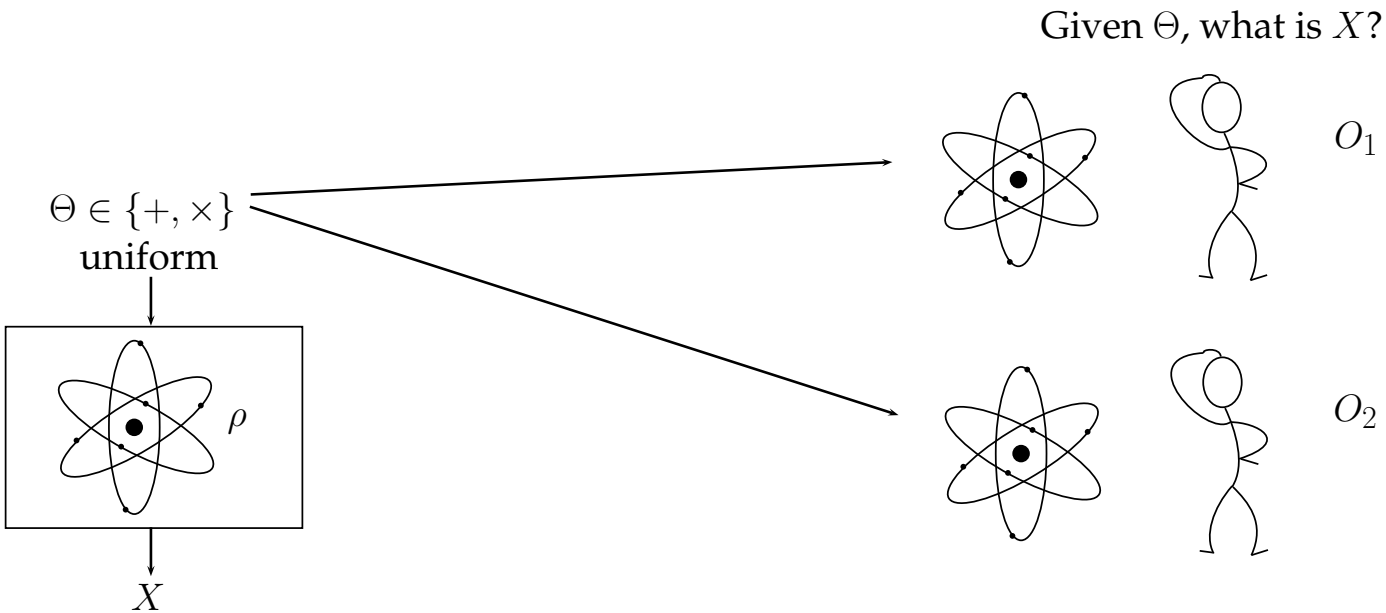
Can monogamy of entanglement help?

Berta, Christandl, Colbeck, Renes & Renner [BCC$^+$10]

The post-measurement states satisfy

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

Uncertainty and Monogamy of Entanglement



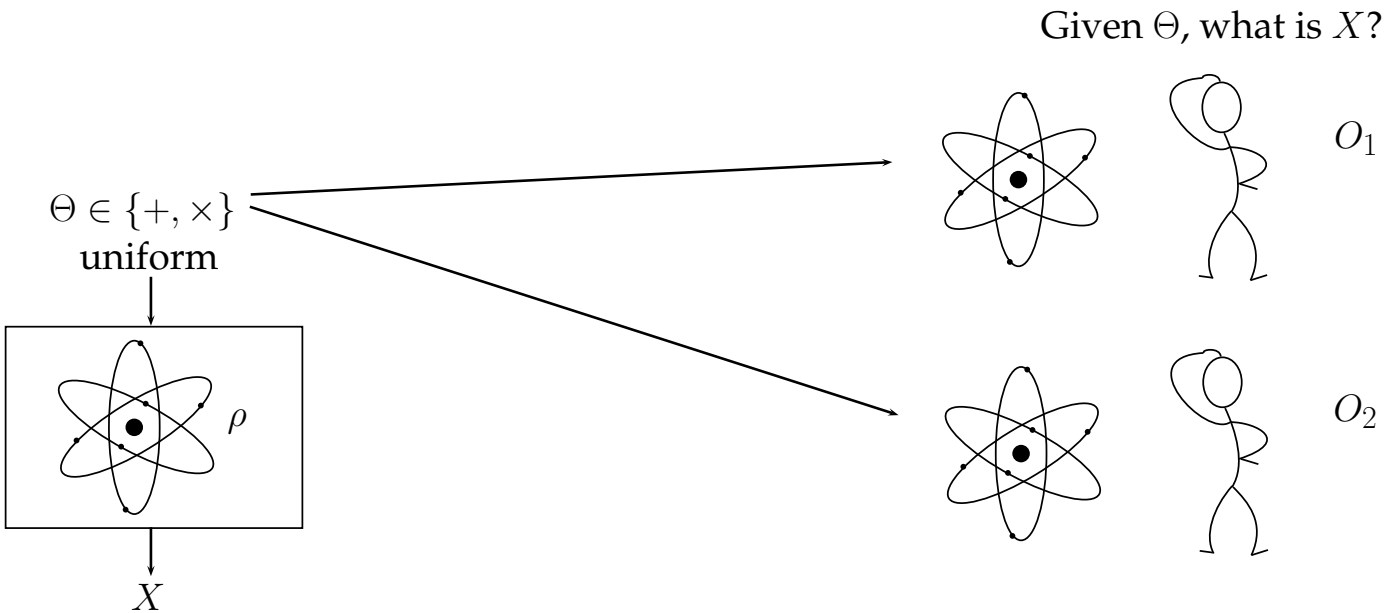
Berta, Christandl, Colbeck, Renes & Renner [BCC+10]

The post-measurement states satisfy

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

- $H(A|B) := H(AB) - H(B)$ is the von Neumann entropy.
- The overlap c is defined as in the classical relation.

Uncertainty and Monogamy of Entanglement



Berta, Christandl, Colbeck, Renes & Renner [BCC+10]

The post-measurement states satisfy

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

- Can this be generalized to quantum Rényi entropies, in particular the min-entropy?

Quantum Guessing Probability and the Min-Entropy

- The guessing probability naturally generalizes to the case of classical quantum states $\rho_{XE} = \bigoplus_x P(x)\rho_E^x$:

$$p_{\text{guess}}(X|E) := \sup\left\{ \sum_x P(x)\,\text{tr}(\rho_E^x M_E^x) \,\middle|\, \{M_E^x\} \text{ a POVM} \right\}.$$

Quantum Guessing Probability and the Min-Entropy

- The guessing probability naturally generalizes to the case of classical quantum states $\rho_{XE} = \bigoplus_x P(x)\rho_E^x$:

$$p_{\text{guess}}(X|E) := \sup\left\{ \sum_x P(x)\,\text{tr}(\rho_E^x M_E^x) \,\middle|\, \{M_E^x\} \text{ a POVM} \right\}.$$

- Then, we retain $H_{\min}(X|E) := -\log p_{\text{guess}}(X|E)$ as proposed by König, Renner & Schaffner [KRS09].

Quantum Guessing Probability and the Min-Entropy

- The guessing probability naturally generalizes to the case of classical quantum states $\rho_{XE} = \bigoplus_x P(x)\rho_E^x$:

$$p_{\text{guess}}(X|E) := \sup\left\{ \sum_x P(x)\,\text{tr}(\rho_E^x M_E^x) \,\middle|\, \{M_E^x\} \text{ a POVM} \right\}.$$

- Then, we retain $H_{\min}(X|E) := -\log p_{\text{guess}}(X|E)$ as proposed by König, Renner & Schaffner [KRS09].
- The operational interpretation remains intact:

Renner [Ren05]: Quantum Leftover Hash Lemma

Let $X \in \mathcal{X}$ be such that $H_{\min}^{\varepsilon}(X|E) \geq k$, and $\ell \in \mathbb{N}$. Then, there exists a family of Hash function $\{f_s\}_s$ from $\mathcal{X}$ to $\{0,1\}^\ell$ such that $f_S(X)$ is δ-close to uniform and independent of E and S, where

$$\delta \sim \sqrt{2^{\ell-k}} + 2\varepsilon.$$

Uncertainty Relation for min-/max Entropies

T & Renner [TR11]: Min-Max Entropic Uncertainty

For any state $\rho_{AO_1O_2}$ and POVMs $\{M_x\}$ and $\{N_x\}$ on A:

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

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

- Reduces to overlap defined previously for projective measurements.

Uncertainty Relation for min-/max Entropies

T & Renner [TR11]: Smooth Entropic Uncertainty

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

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

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

- Reduces to overlap defined previously for projective measurements.

Uncertainty Relation for min-/max Entropies

T & Renner [TR11]: Smooth Entropic Uncertainty

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

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

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

- Reduces to overlap defined previously for projective measurements.
- This also generalizes the previous result for the von Neumann entropy due to asymptotic equipartition [TCR09]:

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

Uncertainty Relation for min-/max Entropies

T & Renner [TR11]: Smooth Entropic Uncertainty

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

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

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

- Reduces to overlap defined previously for projective measurements.
- This also generalizes the previous result for the von Neumann entropy due to asymptotic equipartition [TCR09]:

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

- What about general Rényi entropies?

Quantum Rényi Entropy Intermezzo

We want to find a quantum generalization of the Rényi entropy that satisfies the following

- It evaluates to the von Neumann, min-, and max-entropies for $\alpha = 1, \infty, \frac{1}{2}$, respectively.
- It has mathematical properties that we expect from an operational quantity, e.g. a data-processing inequality:

$$H_\alpha(A|B) \leq H_\alpha(A|C) \quad \text{for any quantum channel } \mathcal{E} : B \to C.$$

Such a generalization was recently proposed by Müller-Lennert, Dupuis, Szehr, Fehr & T [MLDS$^+$13] (see also [WWY13]).

Uncertainty Relation for Quantum Rényi Entropy

Such a generalization was recently proposed by Müller-Lennert, Dupuis, Szehr, Fehr & T [MLDS$^+$13] (see also [WWY13]).

Müller-Lennert *et al.* [MLDS$^+$13]: Quantum Rényi Entropy

The quantum conditional Rény entropy is, for $\alpha \geq \frac{1}{2}$,

$$H_\alpha(A|B) := \sup_{\sigma_B} -D_\alpha(\rho_{AB} \| 1_A \otimes \sigma_B),$$

where $D_\alpha(\rho\|\sigma) := \frac{2\alpha}{\alpha-1} \log \left\| \rho^{\frac{1}{2}} \sigma^{\frac{1-\alpha}{2\alpha}} \right\|_{2\alpha}$ uses the Schatten norm.

Uncertainty Relation for Quantum Rényi Entropy

Such a generalization was recently proposed by Müller-Lennert, Dupuis, Szehr, Fehr & T [MLDS$^+$13] (see also [WWY13]).

Müller-Lennert *et al.* [MLDS$^+$13]: Quantum Rényi Entropy

The quantum conditional Rény entropy is, for $\alpha \geq \frac{1}{2}$,

$$H_\alpha(A|B) := \sup_{\sigma_B} -D_\alpha(\rho_{AB} \| 1_A \otimes \sigma_B),$$

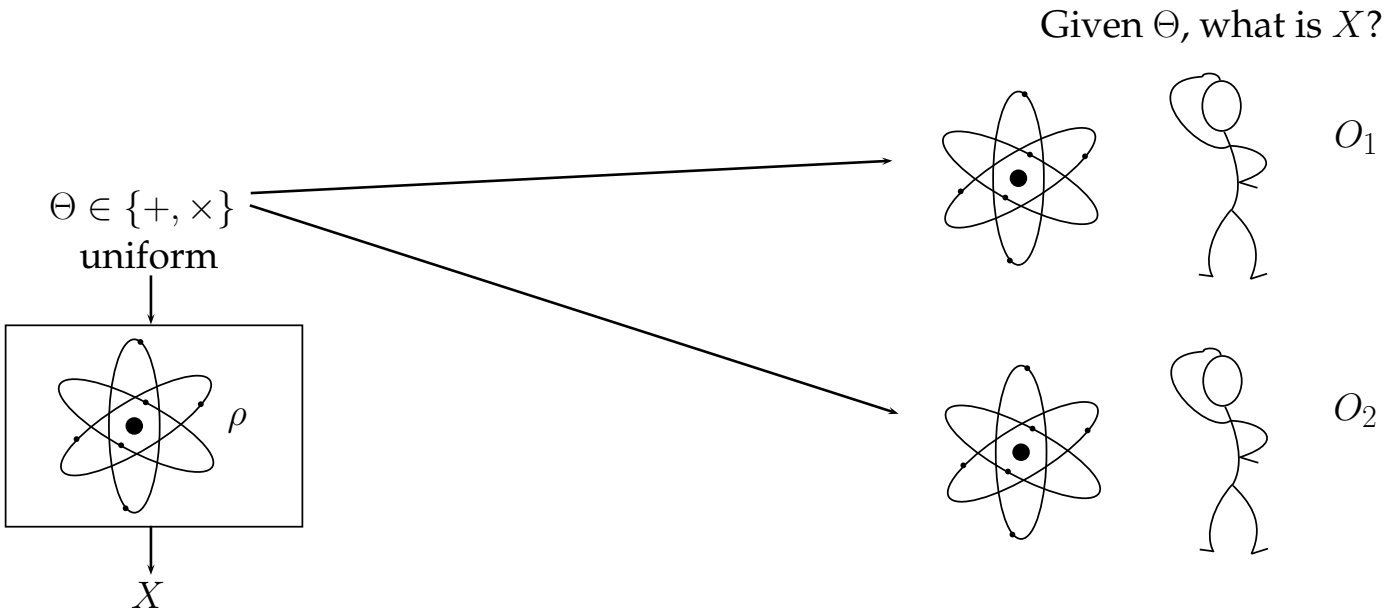
where $D_\alpha(\rho\|\sigma) := \frac{2\alpha}{\alpha-1} \log \left\| \rho^{\frac{1}{2}} \sigma^{\frac{1-\alpha}{2\alpha}} \right\|_{2\alpha}$ uses the Schatten norm.

- We recover the well-known special cases for $\alpha = \infty, \frac{1}{2}$:

$$H_{\min}(A|B) = \sup \left\{ \lambda \in \mathbb{R} \,\middle|\, \exists \sigma_B : \rho_{AB} \leq 2^{-\lambda} 1_A \otimes \sigma_B \right\},$$

$$H_{\max}(A|B) = \sup_{\sigma_B} \left(2 \log F(\rho_{AB}, 1_A \otimes \sigma_B) \right).$$

Generalized Masseen & Uffink Relation



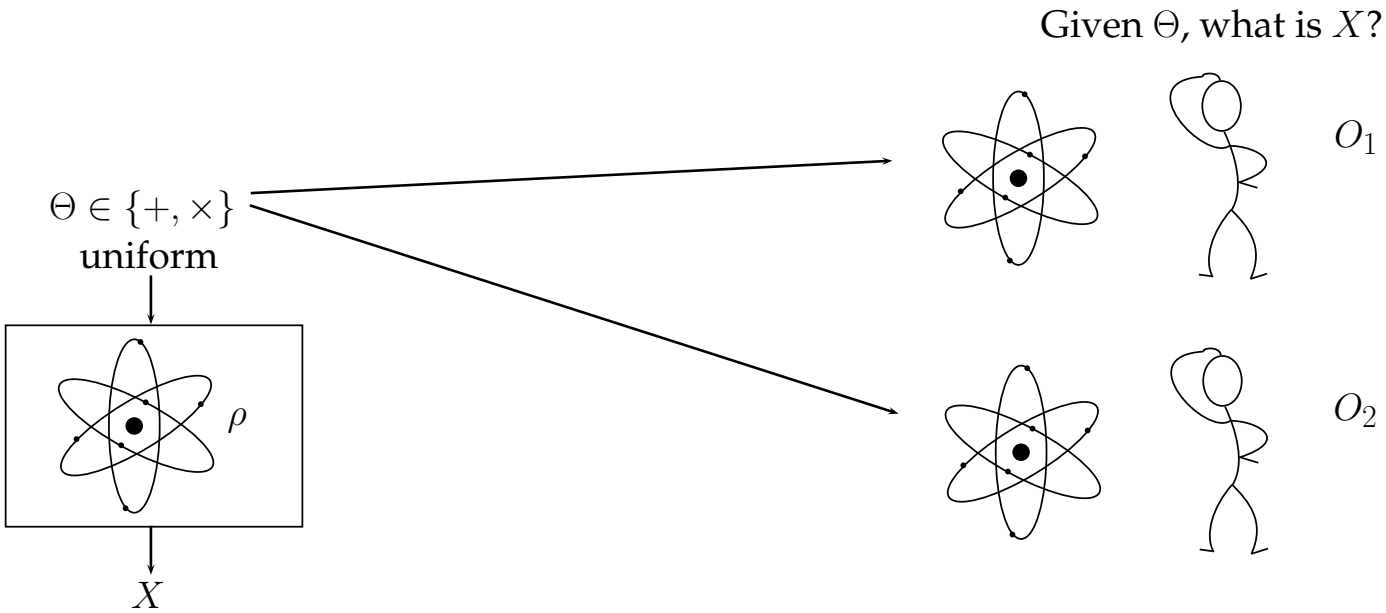
Müller-Lennert *et al.* [MLDS+13]: General Entropic Uncertainty

For any state $\rho_{AO_1O_2}$ and POVMs $\{M_x\}$ and $\{N_x\}$ on A:

$$H_\alpha(X|O_1,\Theta) + H_\beta(X|O_2,\Theta) \geq \log_2 \frac{1}{c}, \quad \text{where}$$

$$\frac{1}{\alpha} + \frac{1}{\beta} = 2, \quad \text{and} \quad c = \max_{x,y} \left\| \sqrt{M_x}\sqrt{N_y} \right\|_\infty^2 .$$

Generalized Masseen & Uffink Relation



Müller-Lennert *et al.* [MLDS+13]: General Entropic Uncertainty

For any state $\rho_{AO_1O_2}$ and POVMs $\{M_x\}$ and $\{N_x\}$ on A:

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

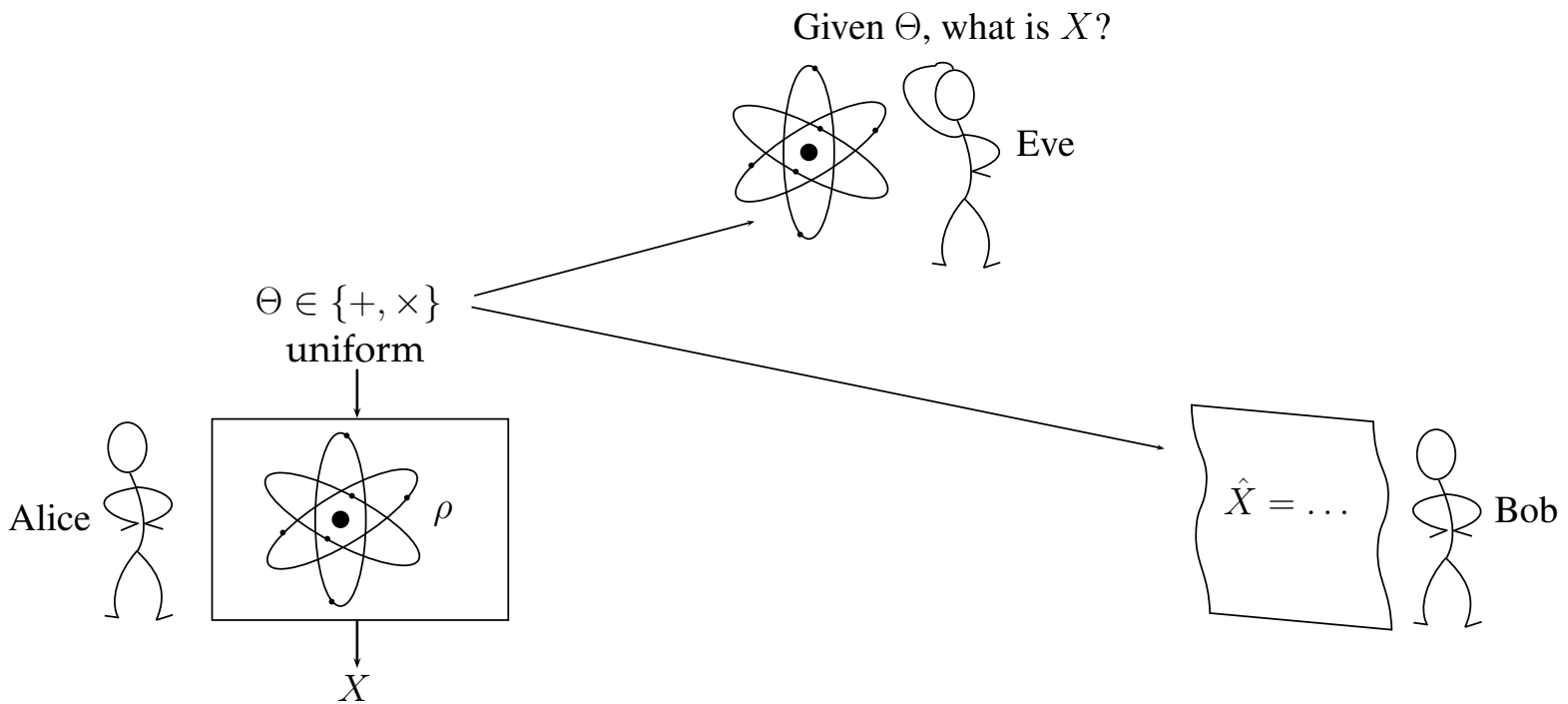
- Proof only uses a few basic properties of H_α and employs a strategy by Coles, Colbeck, Yu & Zwolak [CCYZ12].

Setup for Quantum Key Distribution

- We consider the entanglement-based Bennett-Brassard 1984 protocol [BB84, BBM92]

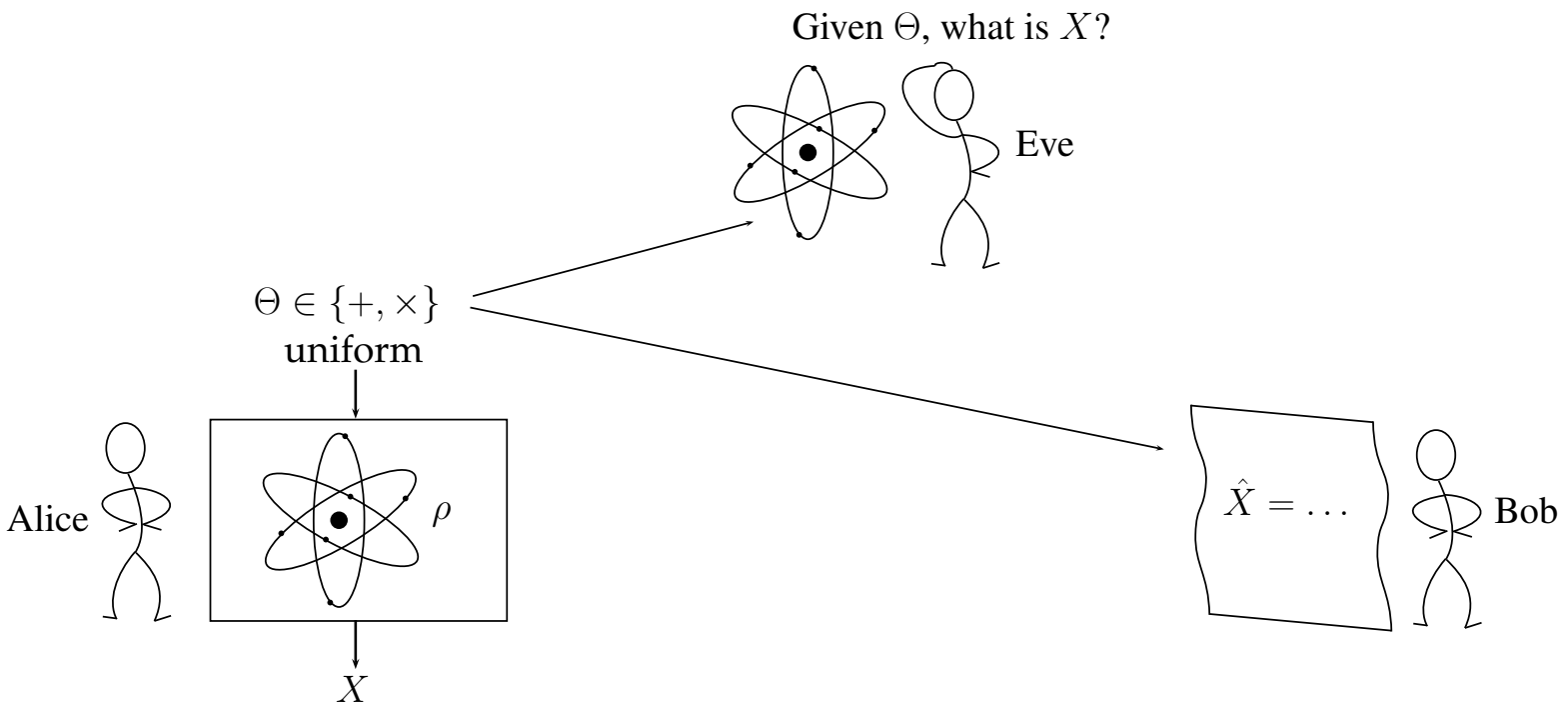
Setup for Quantum Key Distribution

- We consider the entanglement-based Bennett-Brassard 1984 protocol [BB84, BBM92]
- The situation after Bob measured and holds an estimate $\hat{X}$ of X looks as follows:



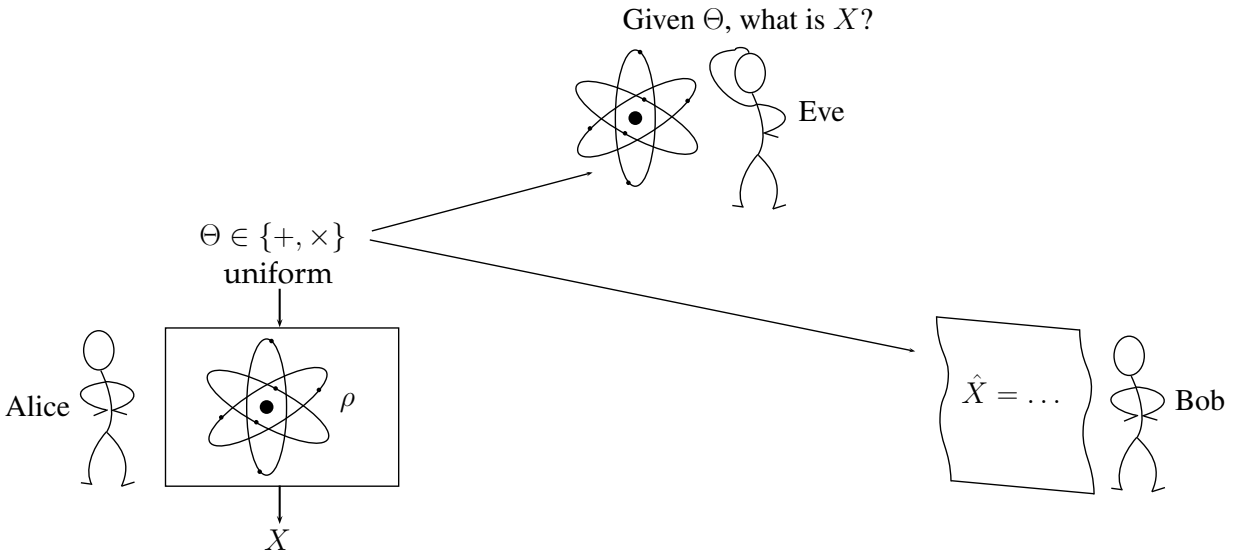
Setup for Quantum Key Distribution

- We consider the entanglement-based Bennett-Brassard 1984 protocol [BB84, BBM92]
- The situation after Bob measured and holds an estimate $\hat{X}$ of X looks as follows:



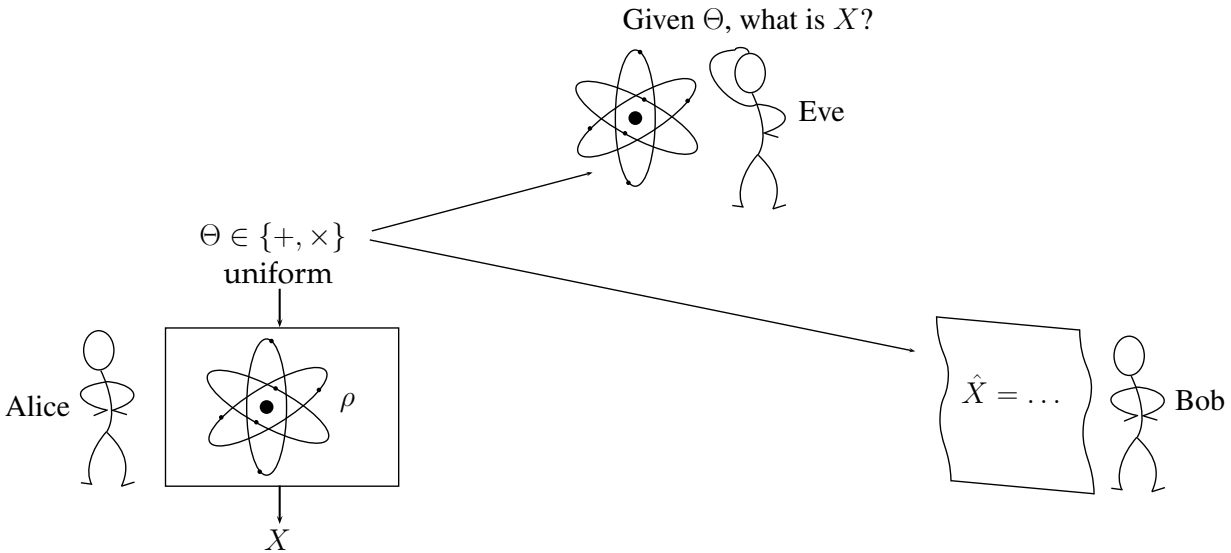
- Here, Θ, X and $\hat{X}$ are n-bit strings.

Uncertainty Relation for n Systems



- Measure either all n systems in '$+$' or in '$\times$'.

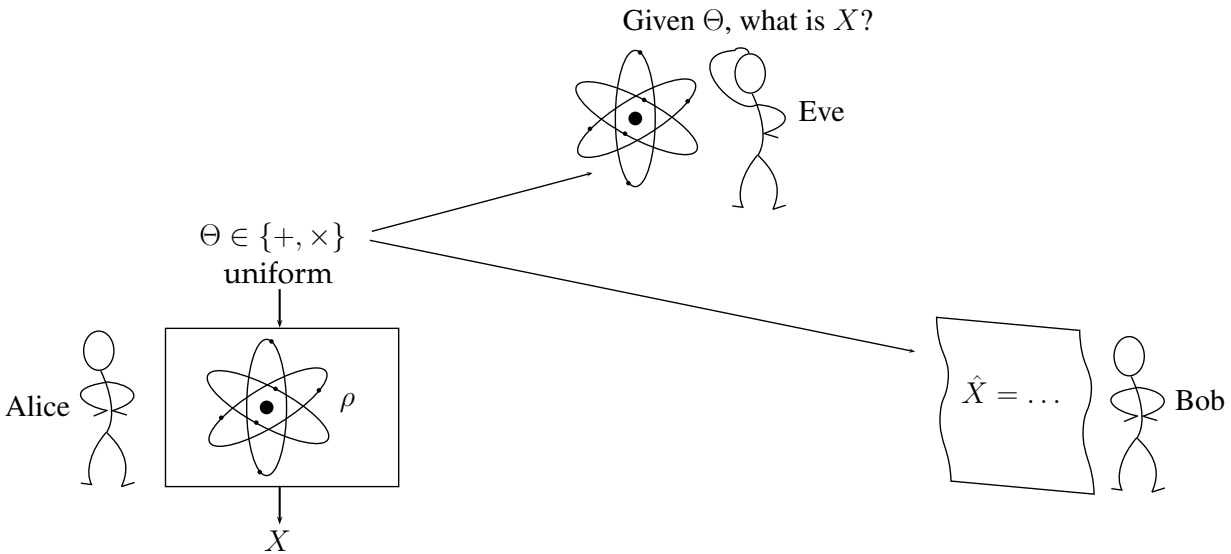
Uncertainty Relation for n Systems



- Measure either all n systems in '$+$' or in '$\times$'.
- Define $F_0 := \{\text{`}++\ldots+\text{'}, \text{`}\times\times\ldots\times\text{'}\}$.

$$H_{\min}(X|E, \Theta \in F_0) + H_{\max}(X|B, \Theta \in F_0) \geq n \log \frac{1}{c}.$$

Uncertainty Relation for n Systems



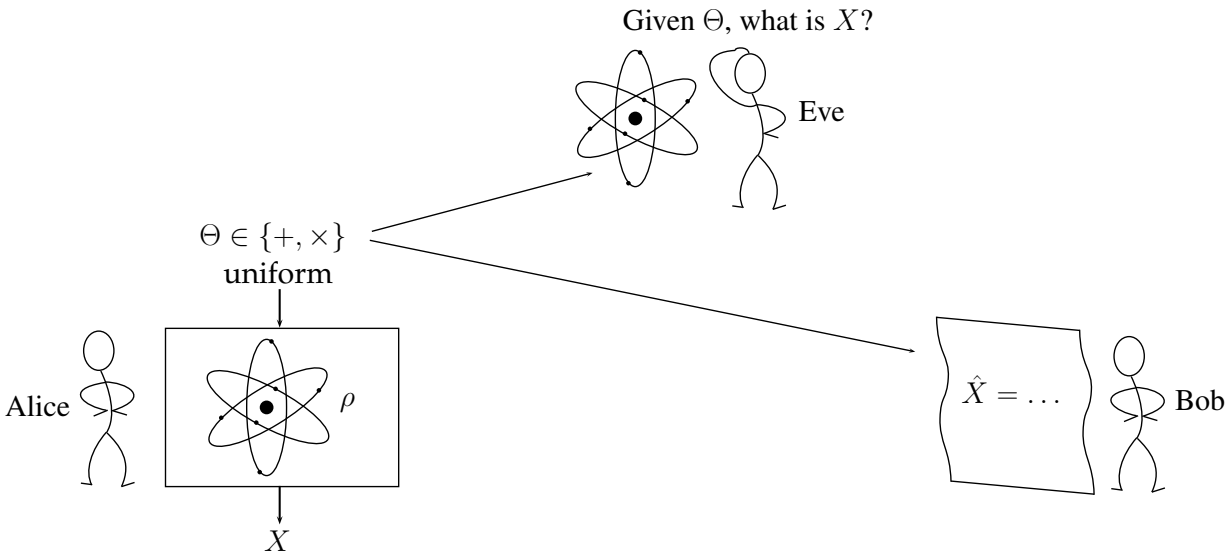
- Measure either all n systems in '+' or in '×'.
- Define $F_0 := \{\text{`}{+}{+}\ldots{+}\text{'}, \text{`}{\times}{\times}\ldots{\times}\text{'}\}$.

$$H_{\min}(X|E, \Theta \in F_0) + H_{\max}(X|B, \Theta \in F_0) \geq n \log \frac{1}{c}.$$

- Analogously for $F_1 := \{\text{`}{\times}{+}{+}\ldots{+}\text{'}, \text{`}{+}{\times}{\times}\ldots{\times}\text{'}\}$, and so on. Then take the average to get

$$H_{\min}(X|E, \Theta) + H_{\max}(X|B, \Theta) \geq n \log \frac{1}{c}.$$

Uncertainty Relation for n Systems



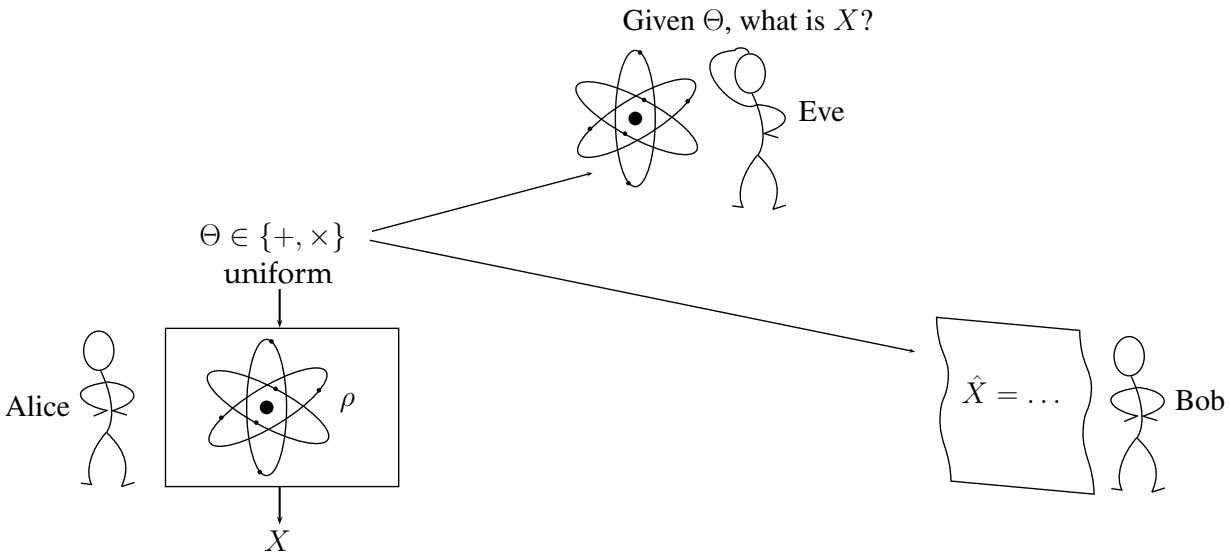
- Measure either all n systems in '+' or in '×'.
- Define $F_0 := \{\text{`}++\ldots+\text{'}, \text{`}\times\times\ldots\times\text{'}\}$.

$$H_{\min}(X|E, \Theta \in F_0) + H_{\max}(X|B, \Theta \in F_0) \geq n \log \frac{1}{c}.$$

- Analogously for $F_1 := \{\text{`}\times++\ldots+\text{'}, \text{`}+\times\times\ldots\times\text{'}\}$, and so on. Then take the average and use data-processing to get

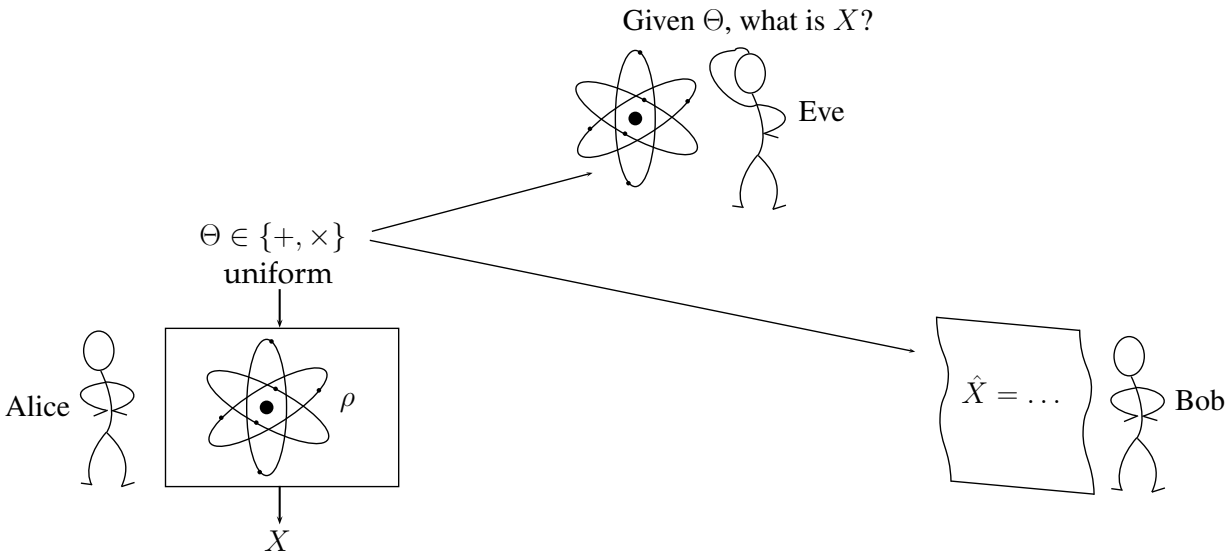
$$H_{\min}(X|E, \Theta) + H_{\max}(X|\hat{X}) \geq n \log \frac{1}{c}.$$

Security Proof Sketch



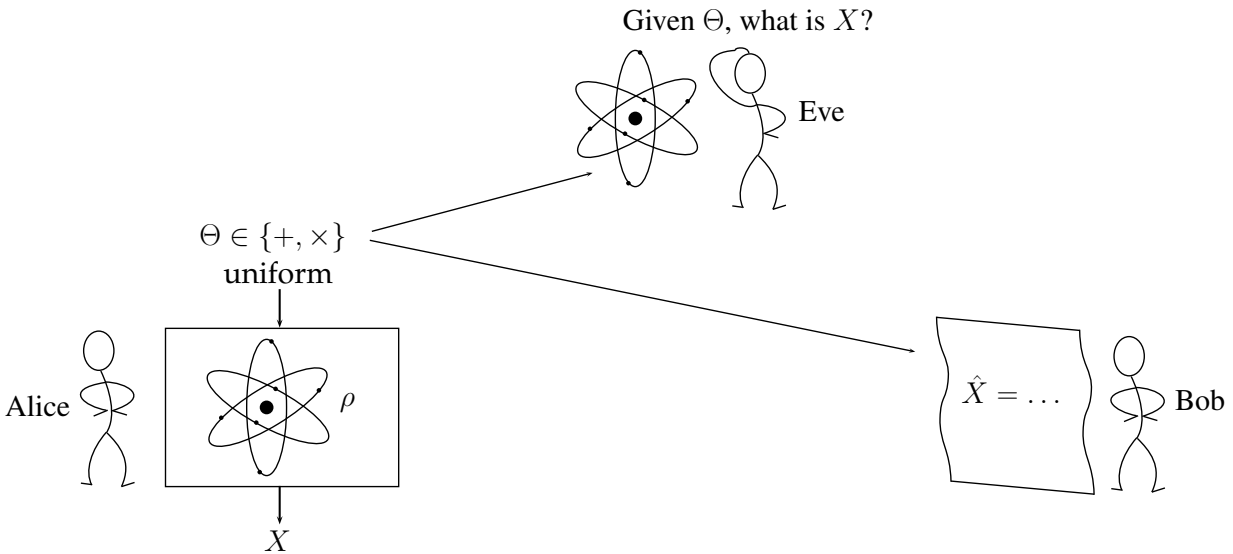
- Overlap: $\log_2 \frac{1}{c} = 1$ (qubits and unbiased bases).

Security Proof Sketch



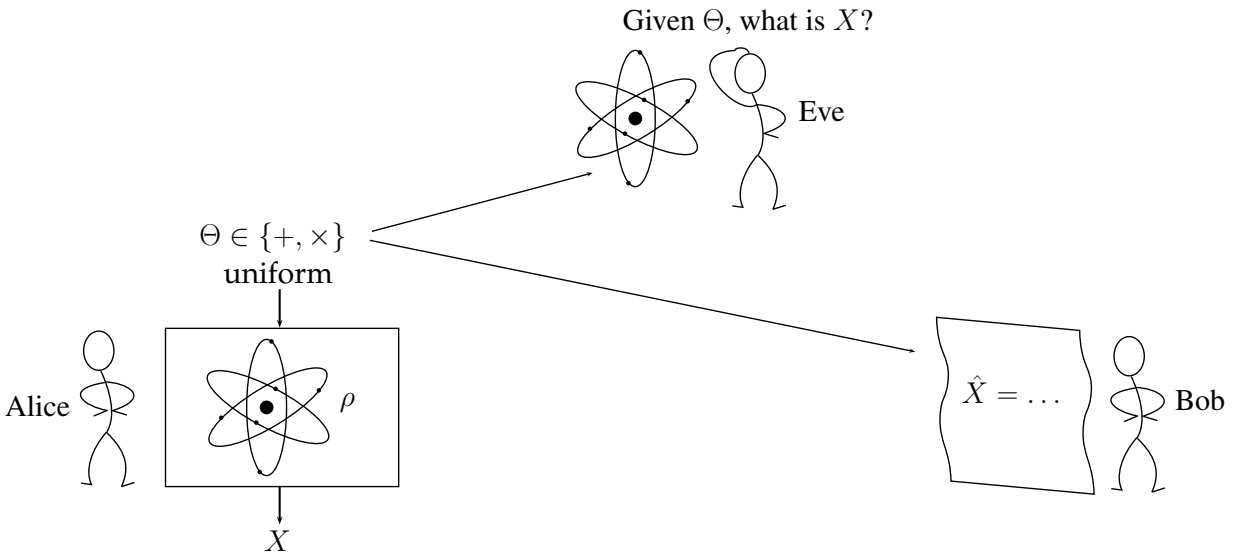
- Overlap: $\log_2 \frac{1}{c} = 1$ (qubits and unbiased bases).
- Uncertainty for n bits: $H_{\min}^{\varepsilon}(X|E,\Theta) \geq n - H_{\max}^{\varepsilon}(X|\hat{X})$.

Security Proof Sketch



- Overlap: $\log_2 \frac{1}{c} = 1$ (qubits and unbiased bases).
- Uncertainty for n bits: $H^{\varepsilon}_{\min}(X|E,\Theta) \geq n - H^{\varepsilon}_{\max}(X|\hat{X})$.
- Secret key: We need to show that $H_{\min}(X|E,\Theta,C)$ is large!

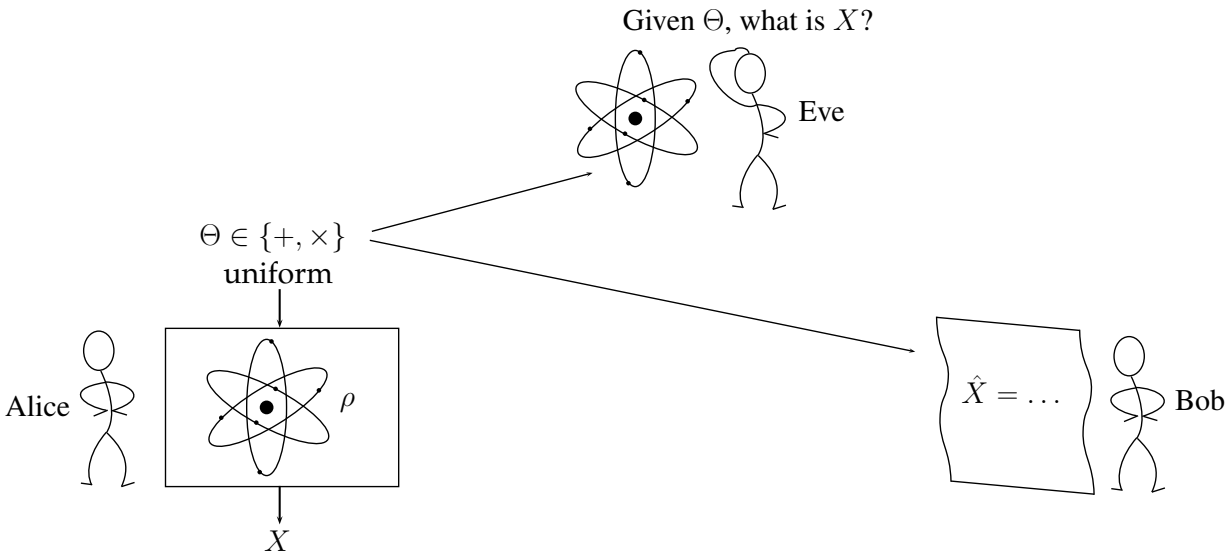
Security Proof Sketch



- Overlap: $\log_2 \frac{1}{c} = 1$ (qubits and unbiased bases).
- Uncertainty for n bits: $H^{\varepsilon}_{\min}(X|E,\Theta) \geq n - H^{\varepsilon}_{\max}(X|\hat{X})$.
- Secret key: We need to show that $H_{\min}(X|E,\Theta,C)$ is large!

$$H^{\varepsilon}_{\min}(X|E,\Theta,C) \geq H^{\varepsilon}_{\min}(X|E,\Theta) - \mathrm{leak}_{\mathrm{EC}}$$

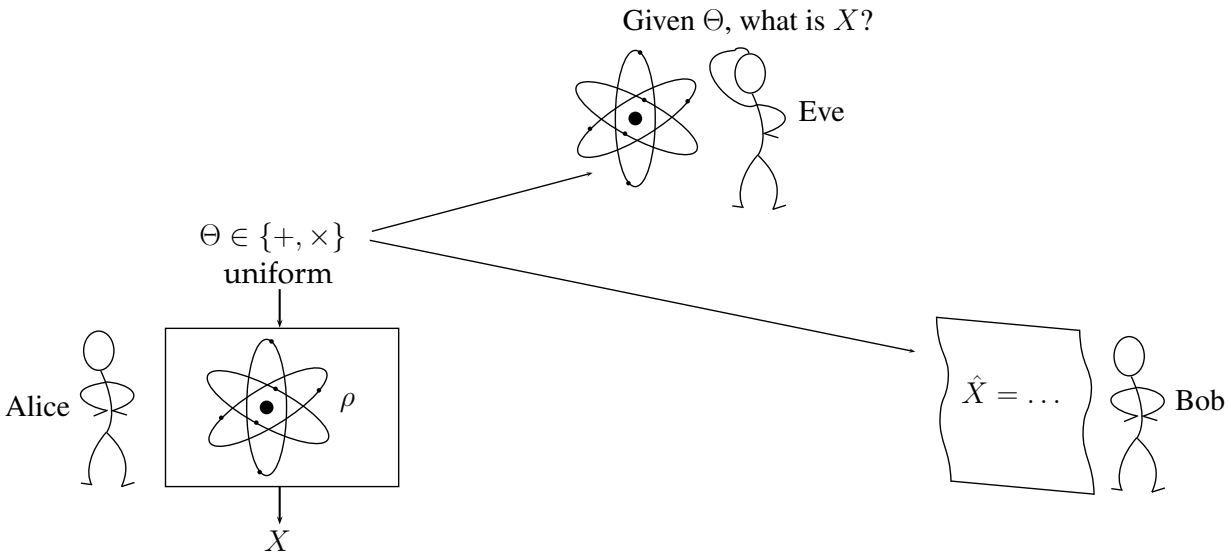
Security Proof Sketch



- Overlap: $\log_2 \frac{1}{c} = 1$ (qubits and unbiased bases).
- Uncertainty for n bits: $H^{\varepsilon}_{\min}(X|E,\Theta) \geq n - H^{\varepsilon}_{\max}(X|\hat{X})$.
- Secret key: We need to show that $H_{\min}(X|E,\Theta,C)$ is large!

$$H^{\varepsilon}_{\min}(X|E,\Theta,C) \geq n - H^{\varepsilon}_{\max}(X|\hat{X}) - \mathrm{leak}_{\mathrm{EC}}.$$

Security Proof Sketch

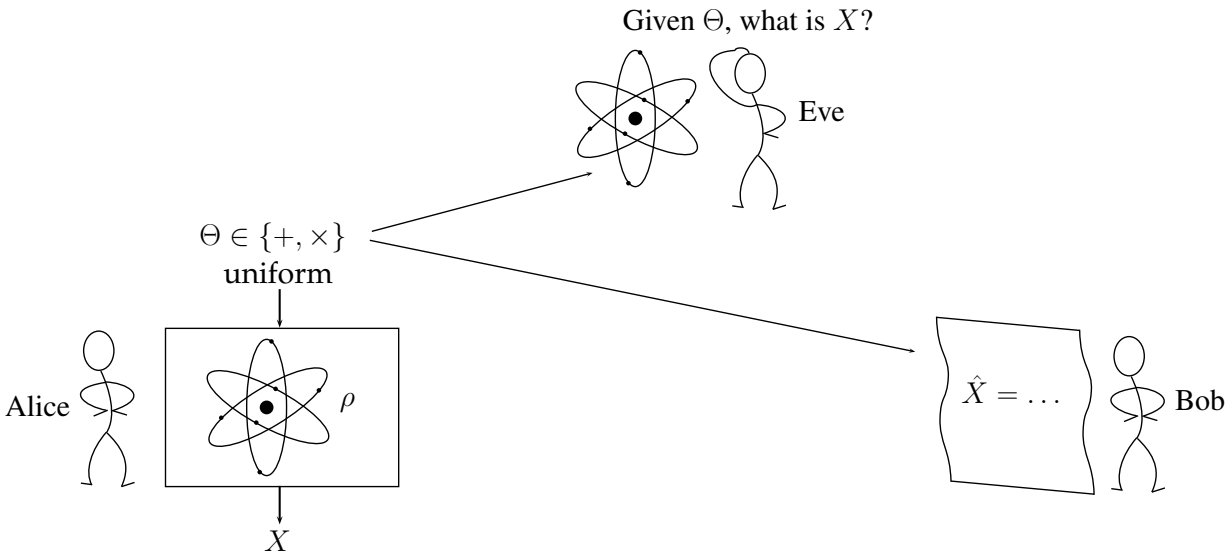


- Overlap: $\log_2 \frac{1}{c} = 1$ (qubits and unbiased bases).
- Uncertainty for n bits: $H^{\varepsilon}_{\min}(X|E,\Theta) \geq n - H^{\varepsilon}_{\max}(X|\hat{X})$.
- Secret key: We need to show that $H_{\min}(X|E,\Theta,C)$ is large!

$$H^{\varepsilon}_{\min}(X|E,\Theta,C) \geq n - H^{\varepsilon}_{\max}(X|\hat{X}) - \mathrm{leak}_{\mathrm{EC}}.$$

- Estimation: $\lambda = \frac{1}{k}\sum_{i\in\Gamma} X_i \oplus \hat{X}_i$ on random sample Γ.

Security Proof Sketch



- Overlap: $\log_2 \frac{1}{c} = 1$ (qubits and unbiased bases).
- Uncertainty for n bits: $H^{\varepsilon}_{\min}(X|E,\Theta) \geq n - H^{\varepsilon}_{\max}(X|\hat{X})$.
- Secret key: We need to show that $H_{\min}(X|E,\Theta,C)$ is large!

$$H^{\varepsilon}_{\min}(X|E,\Theta,C) \geq n - H^{\varepsilon}_{\max}(X|\hat{X}) - \mathrm{leak}_{\mathrm{EC}}.$$

- Estimation: $\lambda = \frac{1}{k}\sum_{i\in\Gamma} X_i \oplus \hat{X}_i$ on random sample Γ.
- Then, estimate $H^{\varepsilon}_{\max}(X|\hat{X}) \lesssim nh(\lambda)$.

Uncertainty Relations for Several Measurements

Various uncertainty relations for classical observers are used to prove security of two-party quantum cryptography, for example in the bounded storage model [DFSS08].

Uncertainty Relations for Several Measurements

Various uncertainty relations for classical observers are used to prove security of two-party quantum cryptography, for example in the bounded storage model [DFSS08].

- For a set of d anti-commuting measurements [WW08], we get

$$H(X|\Theta) \geq 1 - \frac{1}{d}.$$

Uncertainty Relations for Several Measurements

Various uncertainty relations for classical observers are used to prove security of two-party quantum cryptography, for example in the bounded storage model [DFSS08].

- For a set of d anti-commuting measurements [WW08], we get

$$H(X|\Theta) \geq 1 - \frac{1}{d}.$$

- Uncertainty relations for the smooth min-entropy of the form

$$H_{\min}^{\varepsilon}(X|\Theta) \geq \dots$$

are, for example, discussed in [NBW12]. They can be used to prove security for practical implementations [NJM+12].

Uncertainty Relations for Several Measurements

Various uncertainty relations for classical observers are used to prove security of two-party quantum cryptography, for example in the bounded storage model [DFSS08].

- For a set of d anti-commuting measurements [WW08], we get

$$H(X|\Theta) \geq 1 - \frac{1}{d}.$$

- Uncertainty relations for the smooth min-entropy of the form

$$H_{\min}^{\varepsilon}(X|\Theta) \geq \dots$$

  are, for example, discussed in [NBW12]. They can be used to prove security for practical implementations [NJM+12].
- See also the survey by Wehner & Winter [WW10].

Uncertainty Relations for Continuous Variables

- Heisenberg originally considered position and momentum uncertainty, as formalized by Kennard [Ken27]:

$$\Delta_Q \cdot \Delta_P \geq \frac{\hbar}{2}$$

Uncertainty Relations for Continuous Variables

- Heisenberg originally considered position and momentum uncertainty, as formalized by Kennard [Ken27]:

$$\Delta_Q \cdot \Delta_P \geq \frac{\hbar}{2}$$

- This can be expressed in terms of (differential) entropies and extended to side information [BCF+13].

$$h(Q|O_1) + h(P|O_2) \geq \log 2\pi$$
$$h_{\min}(Q|O_1) + h_{\max}(P|O_2) \geq \log 2\pi.$$

Uncertainty Relations for Continuous Variables

- Heisenberg originally considered position and momentum uncertainty, as formalized by Kennard [Ken27]:

$$\Delta_Q \cdot \Delta_P \geq \frac{\hbar}{2}$$

- This can be expressed in terms of (differential) entropies and extended to side information [BCF+13].

$$h(Q|O_1) + h(P|O_2) \geq \log 2\pi$$
$$h_{\min}(Q|O_1) + h_{\max}(P|O_2) \geq \log 2\pi.$$

- This has applications in continuous variable quantum cryptography (CV-QKD). In Furrer *et al.* [FFB+12], we show security for a protocol based on squeezed Gaussian states.
  - In the finite key length regime and for general attacks!
  - Previous security proofs of CV-QKD only provided security under unrealistic assumptions on the eavesdropper.

Take Home Message

Entropic uncertainty relations allow us to formalize physical intuition in information theoretic terms.

$+$

The min-entropy is the preferred measure of uncertainty for cryptographic applications.

$=$

Uncertainty relations in terms of the min-entropy consequently have a wide range of applications in quantum cryptography.

Bibliography I

[Ari73] S. Arimoto, *On the Converse to the Coding Theorem for Discrete Memoryless Channels*, IEEE Trans. Inf. Theory **19** (1973), no. 3, 357–359 (English).

[BB84] Charles H. Bennett and Gilles Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc. IEEE Int. Conf. Comp., Sys. Signal Process. (Bangalore), IEEE, 1984, pp. 175–179.

[BBM92] Charles Bennett, Gilles Brassard, and N. Mermin, *Quantum Cryptography Without Bells Theorem*, Phys. Rev. Lett. **68** (1992), no. 5, 557–559.

[BBR88] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert, *Privacy Amplification by Public Discussion*, SIAM J. Comput. **17** (1988), no. 2, 210.

[BCC+10] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner, *The Uncertainty Principle in the Presence of Quantum Memory*, Nat. Phys. **6** (2010), no. 9, 659–662.

[BCF+13] Mario Berta, Matthias Christandl, Fabian Furrer, Volkher B. Scholz, and Marco Tomamichel, *Continuous Variable Entropic Uncertainty Relations in the Presence of Quantum Memory*.

[CCYZ12] Patrick J. Coles, Roger Colbeck, Li Yu, and Michael Zwolak, *Uncertainty Relations from Simple Entropic Properties*, Phys. Rev. Lett. **108** (2012), no. 21, 210405.

[Deu83] David Deutsch, *Uncertainty in Quantum Measurements*, Phys. Rev. Lett. **50** (1983), no. 9, 631–633.

[DFSS08] Ivan B. Damgå rd, Serge Fehr, Louis Salvail, and Christian Schaffner, *Cryptography in the Bounded-Quantum-Storage Model*, SIAM J. Comput. **37** (2008), no. 6, 1865.

[FFB+12] Fabian Furrer, Torsten Franz, Mario Berta, Anthony Leverrier, Volkher B. Scholz, Marco Tomamichel, and Reinhard F. Werner, *Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks*, Phys. Rev. Lett. **109** (2012), no. 10, 100502.

Bibliography II

[Hei27] W. Heisenberg, *Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik*, Z. Phys. **43** (1927), no. 3-4, 172–198.

[ILL89] R. Impagliazzo, L. A. Levin, and M. Luby, *Pseudo-random generation from one-way functions*, Proc. ACM STOC, ACM Press, 1989, pp. 12–24.

[IZ89] R. Impagliazzo and David Zuckerman, *How to Recycle Random Bits*, Proc. IEEE Symp. Found. Comp. Sc., 1989, pp. 248–253.

[Ken27] E. H. Kennard, *Zur Quantenmechanik einfacher Bewegungstypen*, Z. Phys. **44** (1927), no. 4-5, 326–352.

[KRS09] Robert König, Renato Renner, and Christian Schaffner, *The Operational Meaning of Min- and Max-Entropy*, IEEE Trans. Inf. Theory **55** (2009), no. 9, 4337–4347.

[MLDS+13] Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel, *On quantum Rényi entropies: a new generalization and some properties*.

[MU88] Hans Maassen and J. Uffink, *Generalized Entropic Uncertainty Relations*, Phys. Rev. Lett. **60** (1988), no. 12, 1103–1106.

[NBW12] Nelly Huei Ying Ng, Mario Berta, and Stephanie Wehner, *Min-Entropy Uncertainty Relation for Finite-Size Cryptography*, Phys. Rev. A **86** (2012), no. 4, 042315.

[NJM+12] Nelly Huei Ying Ng, Siddarth K Joshi, Chia Chen Ming, Christian Kurtsiefer, and Stephanie Wehner, *Experimental implementation of bit commitment in the noisy-storage model.*, Nat. Commun. **3** (2012), 1326.

[Rén61] A. Rényi, *On Measures of Information and Entropy*, Proc. Symp. Math., Stat. Probab. (Berkeley), University of California Press, 1961, pp. 547–561.

[Ren05] Renato Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, ETH Zurich, December 2005.

Bibliography III

[Sha48] C. Shannon, *A Mathematical Theory of Communication*, Bell Syst. Tech. J. **27** (1948), 379–423.

[TCR09] Marco Tomamichel, Roger Colbeck, and Renato Renner, *A Fully Quantum Asymptotic Equipartition Property*, IEEE Trans. Inf. Theory **55** (2009), no. 12, 5840–5847.

[TR11] Marco Tomamichel and Renato Renner, *Uncertainty Relation for Smooth Entropies*, Phys. Rev. Lett. **106** (2011), no. 11.

[WW08] Stephanie Wehner and Andreas Winter, *Higher entropic uncertainty relations for anti-commuting observables*, J. Math. Phys. **49** (2008), no. 6, 062105 (en).

[WW10] ———, *Entropic Uncertainty Relations—A Survey*, New J. Phys. **12** (2010), no. 2, 025009.

[WWY13] Mark M. Wilde, Andreas Winter, and Dong Yang, *Strong Converse for the Classical Capacity of Entanglement-Breaking and Hadamard Channels*.