# From Low-distortion Norm Embeddings to Explicit Uncertainty Relations and Efficient Information Locking

**Omar Fawzi**[1] Patrick Hayden[1 2] Pranab Sen[3 1]

[1] McGill School of Computer Science

[2] Perimeter Institute for Theoretical Physics

[3] Tata Institute of Fundamental Research

arXiv:1010.3007

# Encryption of a classical message

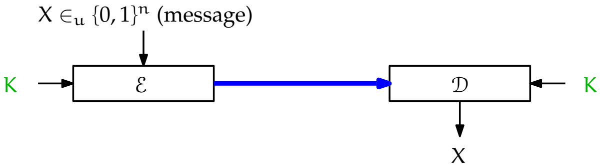

Resources

Shared secret key $K \in_u \{0,1\}^s$

Public communication channel
classical or quantum

Task

Transmit $X$ to Bob




- Bob: $K$ known $\rightarrow$ Decode $\mathcal{E}(X, K)$ using $K$ to get $X$

# Encryption of a classical message

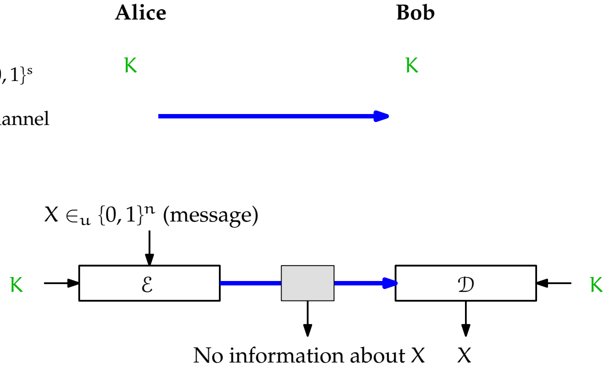
Resources

Shared secret key $K \in_u \{0,1\}^s$

Public communication channel
classical or quantum

Task

Transmit X to Bob



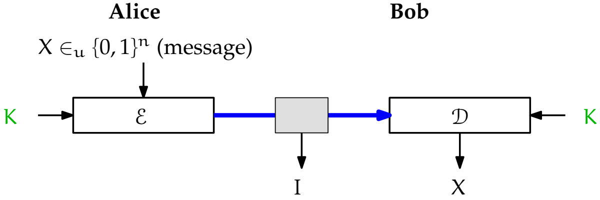

- Bob: $K$ known $\rightarrow$ Decode $\mathcal{E}(X,K)$ using $K$ to get $X$
- Eve: $K$ unknown $\rightarrow$ $\mathcal{E}(X,K)$ gives no information about $X$

# Encryption of a classical message

Task

Transmit $X$ to Bob

$K \in_u \{0,1\}^s$



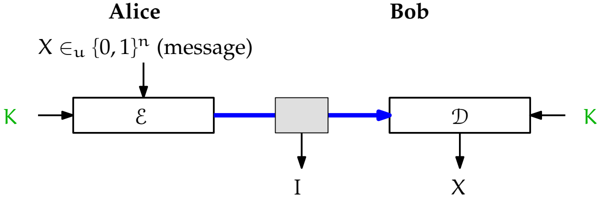

1. **Perfect secrecy**: $X$ and $I$ are independent

# Encryption of a classical message

Task

Transmit X to Bob

$K \in_u \{0,1\}^s$



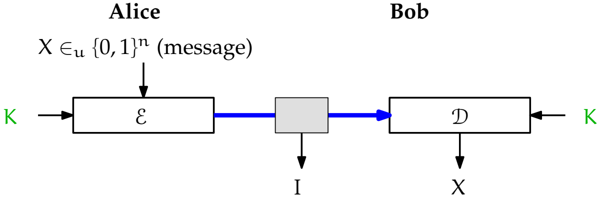

1. **Perfect secrecy**: $X$ and $I$ are independent
   - Must have $s \geqslant n$ (classical or quantum channels)

# Encryption of a classical message

Task

Transmit X to Bob

$K \in_u \{0,1\}^s$



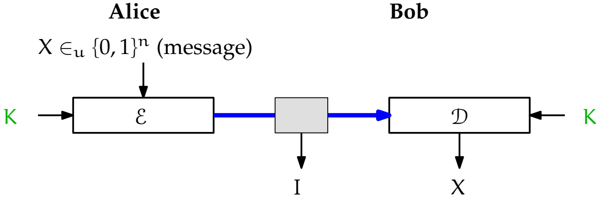

1. **Perfect secrecy**: $X$ and $I$ are independent
   - Must have $s \geqslant n$ (classical or quantum channels)
   - Possible with $s = n$: $\mathcal{E}(X, K) = X \oplus K$ [One-time pad]

# Encryption of a classical message

<u>Task</u>

Transmit X to Bob

$K \in_u \{0,1\}^s$



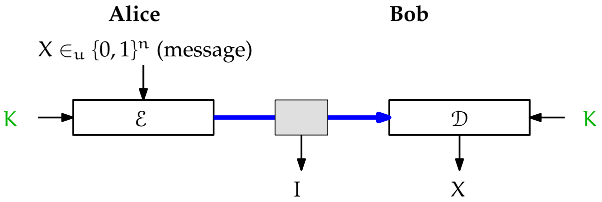

1. **Perfect secrecy**: $X$ and $I$ are independent
   - Must have $s \geqslant n$ (classical or quantum channels)
   - Possible with $s = n$: $\mathcal{E}(X, K) = X \oplus K$ [One-time pad]
2. **Approximate secrecy**: $X$ and $I$ $\epsilon$-close to independent
   - Classical channel: $s \geqslant n - 1$ for $\epsilon < 1/2$

# Encryption of a classical message

Task

Transmit $X$ to Bob

$K \in_u \{0,1\}^s$



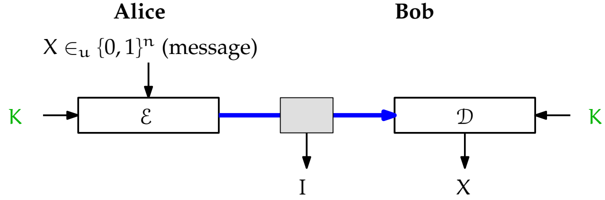

1. **Perfect secrecy**: $X$ and $I$ are independent
   - Must have $s \geqslant n$ (classical or quantum channels)
   - Possible with $s = n$: $\mathcal{E}(X, K) = X \oplus K$ [One-time pad]
2. **Approximate secrecy**: $X$ and $I$ $\epsilon$-close to independent
   - Classical channel: $s \geqslant n - 1$ for $\epsilon < 1/2$
   - Quantum channel:

# Encryption of a classical message

<u>Task</u>

Transmit X to Bob

$K \in_u \{0,1\}^s$




1. **Perfect secrecy**: $X$ and $I$ are independent
   - Must have $s \geqslant n$ (classical or quantum channels)
   - Possible with $s = n$: $\mathcal{E}(X, K) = X \oplus K$ [One-time pad]
2. **Approximate secrecy**: $X$ and $I$ $\epsilon$-close to independent
   - Classical channel: $s \geqslant n - 1$ for $\epsilon < 1/2$
   - Quantum channel:

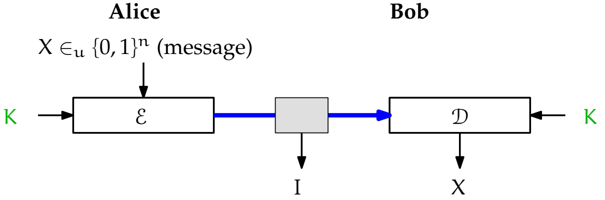
$$\boxed{\text{There exists } \mathcal{E}, \mathcal{D} \text{ with } s = 3\log(1/\epsilon)}$$

# Encryption of a classical message

<u>Task</u>

Transmit X to Bob

$K \in_u \{0,1\}^s$




1. **Perfect secrecy**: $X$ and $I$ are independent
   - Must have $s \geqslant n$ (classical or quantum channels)
   - Possible with $s = n$: $\mathcal{E}(X, K) = X \oplus K$ [One-time pad]
2. **Approximate secrecy**: $X$ and $I$ $\epsilon$-close to independent
   - Classical channel: $s \geqslant n - 1$ for $\epsilon < 1/2$
   - Quantum channel:

$$\boxed{\text{There exists } \mathcal{E}, \mathcal{D} \text{ with } s = 3\log(1/\epsilon)}$$

$$\boxed{\text{There exists } \mathcal{E}, \mathcal{D} \text{ efficient quantum circuits with } s = O(\log(n/\epsilon))}$$

# Outline

# Outline

# Uncertainty relations

**Property of:**

- A set of measurements $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}\}$ (bases here)
- **Notational convenience:** $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}\} \leftrightarrow \{U_0, U_1, \ldots, U_{t-1}\}$ where $U_k : \mathcal{B}_k \mapsto \{|x\rangle\}_{x \in \{0,1\}^n}$ fixed computational basis

$$\text{Measure } \mathcal{B}_k \quad \Longleftrightarrow \quad \text{apply } U_k \text{ and measure } \{|x\rangle\}_{x \in \{0,1\}^n}$$

# Uncertainty relations

**Property of:**

- A set of measurements $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}\}$ (bases here)
- **Notational convenience:** $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}\} \leftrightarrow \{U_0, U_1, \ldots, U_{t-1}\}$ where $U_k : \mathcal{B}_k \mapsto \{|x\rangle\}_{x\in\{0,1\}^n}$ fixed computational basis

$$\text{Measure } \mathcal{B}_k \quad \Longleftrightarrow \quad \text{apply } U_k \text{ and measure } \{|x\rangle\}_{x\in\{0,1\}^n}$$

**Expresses:**

- Uncertainty of outcome distributions
- Measurements "incompatible"

# Uncertainty relations

**Property of:**

- A set of measurements $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}\}$ (bases here)
- **Notational convenience:** $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}\} \leftrightarrow \{U_0, U_1, \ldots, U_{t-1}\}$ where $U_k : \mathcal{B}_k \mapsto \{|x\rangle\}_{x\in\{0,1\}^n}$ fixed computational basis

$$\text{Measure } \mathcal{B}_k \quad \Longleftrightarrow \quad \text{apply } U_k \text{ and measure } \{|x\rangle\}_{x\in\{0,1\}^n}$$

**Expresses:**

- Uncertainty of outcome distributions $\left\{p_{U_0|\psi\rangle}, \ldots, p_{U_{t-1}|\psi\rangle}\right\}$ $\forall|\psi\rangle$
- Measurements "incompatible"

**Example:** $\{+, \times\} \leftrightarrow \{I, H\}$

$$p_{I|\psi\rangle} = \left[|\langle 0|I|\psi\rangle|^2, |\langle 1|I|\psi\rangle|^2\right] = \left[|\alpha|^2, |\beta|^2\right]$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$p_{H|\psi\rangle} = \left[|\langle 0|H|\psi\rangle|^2, |\langle 1|H|\psi\rangle|^2\right] = \left[\tfrac{|\alpha+\beta|^2}{2}, \tfrac{|\alpha-\beta|^2}{2}\right]$$

Incompatibility of $+$ and $\times$:

$$\text{For all } |\psi\rangle, \quad \text{uncertainty}(p_{I|\psi\rangle}) + \text{uncertainty}(p_{H|\psi\rangle}) \geqslant \text{large}$$

# Quantifying uncertainty

$$\text{For all } |\psi\rangle, \quad \sum_{k=0}^{t-1} \text{uncertainty}(p_{U_k|\psi\rangle}) \geqslant \text{large}$$

# Quantifying uncertainty

$$\text{For all } |\psi\rangle, \quad \sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geqslant \text{large}$$

**Uncertainty:**

- Entropy $\mathbf{H}(\cdot)$

# Quantifying uncertainty

$$\text{For all } |\psi\rangle, \quad \sum_{k=0}^{t-1} \Delta(p_{U_k|\psi\rangle}, \text{unif}) \leqslant \text{small}$$

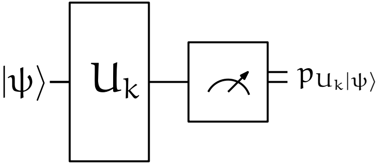
**Uncertainty:**

- Entropy $\mathbf{H}(\cdot)$
- Closeness to uniform $\Delta(\cdot, \text{unif})$
  (the smaller, the more uncertain)
  $\Delta(p, q) \stackrel{\text{def}}{=} \frac{1}{2} \sum_{x \in \mathcal{X}} |p(x) - q(x)|$ total variation distance

# Metric uncertainty relations

**Recap of definitions:**

$$p_{U_k|\psi\rangle}(x) \stackrel{\text{def}}{=} |\langle x|U_k|\psi\rangle|^2$$




$\Delta(p,q) \stackrel{\text{def}}{=} \frac{1}{2}\sum_{x\in\mathcal{X}} |p(x) - q(x)|$ total variation distance

## Definition (Metric uncertainty relation)

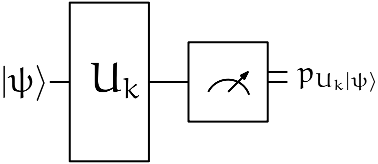
$\{U_0, \ldots, U_{t-1}\}$ acting on $(\mathbb{C}^2)^{\otimes n}$

For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ $\quad \displaystyle\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^n)\right) \leqslant \epsilon$

# Metric uncertainty relations

**Recap of definitions:**

$$p_{U_k|\psi\rangle}(x) \stackrel{\text{def}}{=} |\langle x|U_k|\psi\rangle|^2$$




$$\Delta(p,q) \stackrel{\text{def}}{=} \frac{1}{2}\sum_{x\in\mathcal{X}} |p(x)-q(x)|$$ total variation distance

**Definition (Metric uncertainty relation)**

$\{U_0, \dots, U_{t-1}\}$ acting on $(\mathbb{C}^2)^{\otimes n}$

For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ $$\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^n)\right) \leqslant \epsilon$$

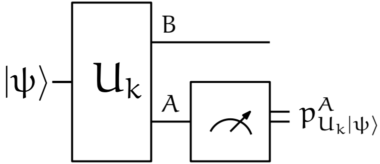
**Intuition:** $\forall|\psi\rangle$, for most values of $k$, $\Delta\left(p_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^n)\right) \lessapprox \epsilon$

**Objectives:** $t, \epsilon$ small

# Metric uncertainty relations

**Recap of definitions:**

$$p^A_{U_k|\psi\rangle}(a) \stackrel{\text{def}}{=} \sum_{b\in\{0,1\}^{n_B}} |\langle a|^A \langle b|^B U_k|\psi\rangle|^2$$




$$\Delta(p,q) \stackrel{\text{def}}{=} \frac{1}{2} \sum_{x\in\mathcal{X}} |p(x) - q(x)|$$ total variation distance

**Definition (Metric uncertainty relation)**

$\{U_0, \ldots, U_{t-1}\}$ acting on $(\mathbb{C}^2)^{\otimes n} = A \otimes B$ with $A = (\mathbb{C}^2)^{\otimes n_A}$ and $B = (\mathbb{C}^2)^{\otimes n_B}$

For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ $$\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$$

**Intuition:** $\forall |\psi\rangle$, for most values of $k$, $\Delta\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) \lessapprox \epsilon$

**Objectives:** $t, \epsilon$ small and $n_A$ large

# Metric and entropic uncertainty relations

**Entropic uncertainty relations**
Use (Shannon) entropy [Bialynicki-Birula, Mycielski, 1975; Deutsch, 1983]

**Definition (Metric uncertainty relation)**

For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ $\quad \frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$

$$\mathbf{H}(p_{U_k|\psi\rangle}) \geqslant \mathbf{H}(p^A_{U_k|\psi\rangle}) \qquad \text{recall } p^A_{U_k|\psi\rangle}(a) = \sum_b p_{U_k|\psi\rangle}(a,b)$$

# Metric and entropic uncertainty relations

**Entropic uncertainty relations**
Use (Shannon) entropy [Bialynicki-Birula, Mycielski, 1975; Deutsch, 1983]

**Definition (Metric uncertainty relation)**

$$\text{For all } |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \qquad \frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$$

$$\mathbf{H}(p_{U_k|\psi\rangle}) \geqslant \mathbf{H}(p^A_{U_k|\psi\rangle}) \qquad \text{recall } p^A_{U_k|\psi\rangle}(a) = \sum_b p_{U_k|\psi\rangle}(a,b)$$

**Proposition (Metric UR $\Rightarrow$ Entropic UR)**

*$U_0, \ldots, U_{t-1}$ define an $\epsilon$-metric UR, then*

$$\textit{For all } |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \qquad \frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geqslant (1-2\epsilon)n_A - \eta(\epsilon)$$

Proof: Fannes' inequality □

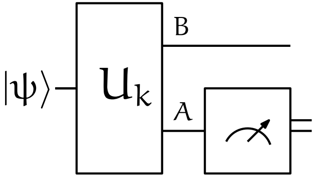
# Metric uncertainty relations: parameters

## Theorem (Metric uncertainty relations)

$\exists\, U_0, \dots, U_{t-1}$ *acting on* $(\mathbb{C}^2)^{\otimes n} = A \otimes B$ *with*

| | $\log t$ | $n_A$ |
|---|---|---|
| *Non-explicit* | $3 \log(1/\epsilon)$ | $n - 2\log(1/\epsilon)$ |
| *Efficient* | $O(\log(n/\epsilon))$ | $0.99n$ |
| *Efficient* | $O(\log^2(n/\epsilon))$ | $n - O(\log(n/\epsilon))$ |

$$\textit{for all } |\psi\rangle \qquad \frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \textit{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon.$$




$$p^A_{U_k|\psi\rangle} \approx_\epsilon \mathrm{unif}(\{0,1\}^{n_A})$$

for most values of k

# Encryption of classical messages

## Definition (Locking scheme)

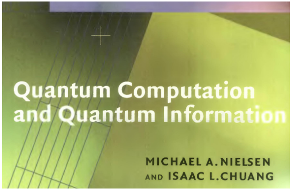
Message $X \in_u \{0,1\}^n$, key $K \in_u \{0,1\}^s$ (think $s \ll n$)

$\mathcal{E}$ is $\epsilon$-locking scheme if:

Knowing $K$, can determine $X$ using $\mathcal{E}(X, K)$

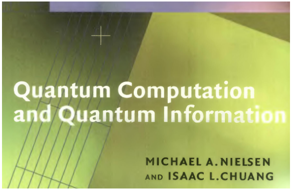
Not knowing $K$, for any measurement whose outcome is $I$: $\Delta(p_{XI}, p_X \times p_I) \leqslant \epsilon$

# Composability




A QKD protocol is defined as being *secure* if, for any security parameters $s > 0$ and $\ell > 0$ chosen by Alice and Bob, and for any eavesdropping strategy, either the scheme aborts, or it succeeds with probability at least $1 - O(2^{-s})$, and guarantees that Eve's mutual information with the final key is less than $2^{-\ell}$. The key string must also be essentially random.

# Composability




A QKD protocol is defined as being *secure* if, for any security parameters $s > 0$ and $\ell > 0$ chosen by Alice and Bob, and for any eavesdropping strategy, either the scheme aborts, or it succeeds with probability at least $1 - O(2^{-s})$, and guarantees that Eve's mutual information with the final key is less than $2^{-\ell}$. The key string must also be essentially random.

---

**Security of**
**Quantum Key Distribution**

A dissertation submitted to

SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZURICH

for the degree of
tor of Natural Sciences

presented by

**Renato Renner**
**Dipl. Phys. ETH**

### 2.2.1 Standard security definitions are not universal

Unfortunately, many security definitions that are commonly used in quantum cryptography are not universal. For instance, the security of the key $S$ generated by a QKD scheme is typically defined in terms of the mutual information $I(S;W)$ between $S$ and the classical outcome $W$ of a measurement of the adversary's system (see, e.g., [LC99, SP00, NC00, GL03, LCA05] and also the discussion in [BOHL+05] and [RK05]). Formally, $S$ is said to be secure if, for some small $\varepsilon$,

$$\max_W I(S;W) \leq \varepsilon \,, \tag{2.5}$$

where the maximum ranges over all measurements on the adversary's system with output $W$. Such a definition—although it looks reasonable—does, however, not guarantee that the key $S$ can safely be used in applications. Roughly speaking, the reason for this flaw is that criterion (2.5) does not account for the fact that an adversary might wait with the measurement of her system until she learns parts of the key. (We also refer to [RK05]

Not necessarily composable!

[Ben-Or, Horodecki, Leung, Mayers, Oppenheim, 2005; Konig, Renner, Bariska, Maurer, 2007]

# Information locking: History

[DiVincenzo, Horodecki, Leung, Smolin, Terhal, 2004]

- $X \in_u \{0,1\}^n$ (message) and $K \in_u \{0,1\}$ (key)
- If $K = 0$, $\mathcal{E}(x, 0) = |x\rangle$
- If $K = 1$, $\mathcal{E}(x, 1) = H^{\otimes n}|x\rangle$

Knowing $K$, can determine $X$

Without knowing $K$, for any measurement whose outcome is $I$: $\mathbf{I}(X; I) \leqslant n/2$

One bit of information ($K$) can unlock $\frac{n}{2}$ bits about $X$ hidden in the quantum system $\mathcal{E}(X, K)$

# Information locking: History

[DiVincenzo, Horodecki, Leung, Smolin, Terhal, 2004]

- $X \in_u \{0,1\}^n$ (message) and $K \in_u \{0,1\}$ (key)
- If $K = 0$, $\mathcal{E}(x, 0) = |x\rangle$
- If $K = 1$, $\mathcal{E}(x, 1) = H^{\otimes n}|x\rangle$

Knowing $K$, can determine $X$

Without knowing $K$, for any measurement whose outcome is $I$: $\mathbf{I}(X; I) \leqslant n/2$

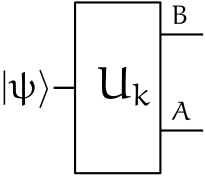
One bit of information ($K$) can unlock $\frac{n}{2}$ bits about $X$ hidden in the quantum system $\mathcal{E}(X, K)$

Encoding in random bases

- [Hayden, Leung, Shor, Winter, 2004] $\mathbf{I}(X; I) \leqslant 3$ with $K \in \{0,1\}^{4 \log n}$
- [Dupuis, Florjanczyk, Hayden, Leung, 2010] $\mathbf{I}(X; I) \leqslant \epsilon$ with $K \in \{0,1\}^{O(\log(n/\epsilon))}$ and stronger definition

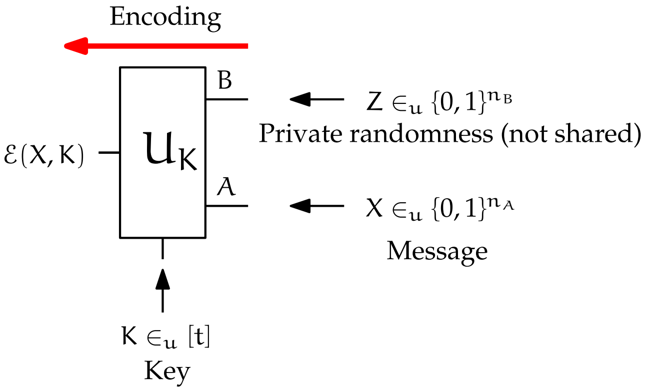
# Locking scheme from a metric uncertainty relation

$\{U_k\}$ satisfies metric uncertainty relation



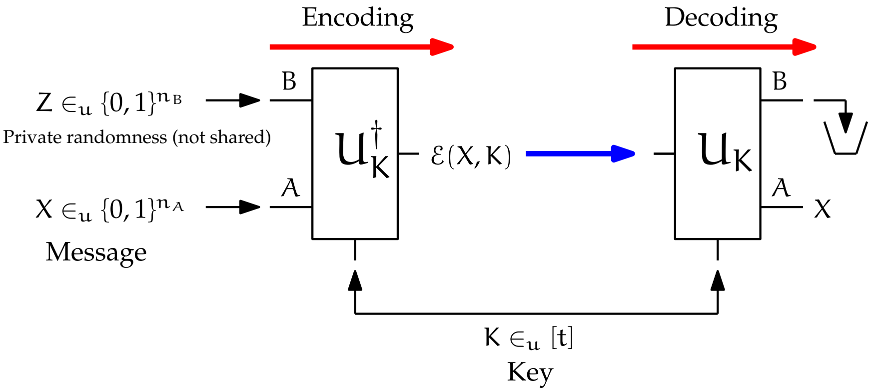
# Locking scheme from a metric uncertainty relation

$\{U_k\}$ satisfies metric uncertainty relation



# Locking scheme from a metric uncertainty relation

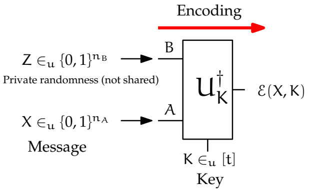
$\{U_k\}$ satisfies metric uncertainty relation



# Locking scheme from a metric UR: proof

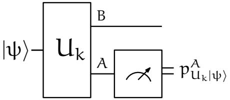
For $a \in \{0,1\}^{n_A}$ and $k \in [t]$

$$\mathcal{E}(a,k) = U_k^\dagger \left( |a\rangle\langle a|^A \otimes \frac{\mathbb{I}^B}{2^{n_B}} \right) U_k$$




- Can assume measurement $\{\xi_i |e_i\rangle\langle e_i|\}_i$
- Outcome $I$
- Unknown $K$:

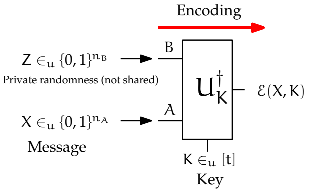
$$\mathbf{P}\{X = a | I = i\} = \frac{1}{t} \sum_{k=0}^{t-1} p^A_{U_k|e_i\rangle}(a)$$



# Locking scheme from a metric UR: proof

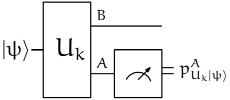
For $a \in \{0,1\}^{n_A}$ and $k \in [t]$

$$\mathcal{E}(a,k) = U_k^\dagger \left( |a\rangle\langle a|^A \otimes \frac{\mathbb{I}^B}{2^{n_B}} \right) U_k$$




- Can assume measurement $\{\xi_i |e_i\rangle\langle e_i|\}_i$
- Outcome $I$
- Unknown $K$:

$$\mathbf{P}\{X = a | I = i\} = \frac{1}{t} \sum_{k=0}^{t-1} p^A_{U_k|e_i\rangle}(a)$$




By definition of metric UR: $\Delta\left(\frac{1}{t}\sum_{k=0}^{t-1} p^A_{U_k|e_i\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$

$\Rightarrow \quad \Delta\left(p_{X|I=i}, \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$ for any $i$ $\square$

# Parameters of locking scheme

**Theorem**

*There exists $\epsilon$-locking schemes*

| | *Bits of key* | *Qubits of $\mathcal{E}(x,k)$* |
|---|---|---|
| *Non-explicit* | $5\log(1/\epsilon)$ | $n$ |
| *Efficient* | $O(\log(n/\epsilon))$ | $1.01n$ |
| *Efficient* | $O(\log^2(n/\epsilon))$ | $n$ |

| | Inf. leakage | Key | Ciphertext | Efficient ? |
|---|---|---|---|---|
| [DHLST04] | $n/2$ | 1 | $n$ | yes |
| [HLSW04] | 3 | $4\log(n)$ | $n$ | no |
| [DFHL10] | $\epsilon n$ | $2\log(n/\epsilon^2)$ | $n$ | no |
| I | $\epsilon n$ | $5\log(1/\epsilon)$ | $n$ | no |
| II | $\epsilon n$ | $O(\log(n/\epsilon))$ | $1.01n$ | yes |
| III | $\epsilon n$ | $O(\log^2(n/\epsilon))$ | $n$ | yes |

**Note:** Can take $\epsilon = \eta/n$

# Another application: Quantum equality testing

**Quantum identification** or **approximate measurement simulation**

| | **Alice** | **Bob** |
|---|---|---|
| *Inputs* | $\|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ | description of $\|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$ |
| *Ouput* | | YES with prob $\|\langle\psi\|\phi\rangle\|^2 \pm \epsilon$ |
| | | NO with prob $1 - \|\langle\psi\|\phi\rangle\|^2 \pm \epsilon$ |
| *Objective* | Minimize quantum communication | |

Relaxation of quantum info transmission [Winter, 2004]

# Another application: Quantum equality testing

## **Quantum identification** or **approximate measurement simulation**

| | **Alice** | **Bob** |
|---|---|---|
| *Inputs* | $\lvert\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ | description of $\lvert\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$ |
| *Ouput* | | YES with prob $\lvert\langle\psi\lvert\phi\rangle\rvert^2 \pm \epsilon$ |
| | | NO with prob $1 - \lvert\langle\psi\lvert\phi\rangle\rvert^2 \pm \epsilon$ |
| *Objective* | Minimize quantum communication | |

Relaxation of quantum info transmission [Winter, 2004]

## **Classical equality testing** or **identification**

| | **Alice** | **Bob** |
|---|---|---|
| *Inputs* | $x \in \{0,1\}^n$ | $y \in \{0,1\}^n$ |
| *Ouput* | | YES with prob $\mathbf{1}_{x=y} \pm \epsilon$ |
| | | NO with prob $\mathbf{1}_{x\neq y} \pm \epsilon$ |
| *Objective* | Minimize classical communication | |

Communication complexity EQUALITY

**Remark:** Communication is one way

# Quantum equality testing

| | **Alice** | **Bob** |
|---|---|---|
| *Inputs* | $\|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ | description of $\|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$ |
| *Ouput* | | YES with prob $\|\langle\psi\|\phi\rangle\|^2 \pm \epsilon$ |
| | | NO with prob $1 - \|\langle\psi\|\phi\rangle\|^2 \pm \epsilon$ |
| *Resource* | quantum communication $\longrightarrow$ | |

- Optimal quantum communication $\approx n/2$ qubits [Winter, 2004]

# Quantum equality testing

| | **Alice** | **Bob** |
|---|---|---|
| *Inputs* | $\|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ | description of $\|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$ |
| *Ouput* | | YES with prob $\|\langle\psi\|\phi\rangle\|^2 \pm \epsilon$ |
| | | NO with prob $1 - \|\langle\psi\|\phi\rangle\|^2 \pm \epsilon$ |
| *Resource* | $\xrightarrow{\text{quantum communication}}$ | |

- Optimal quantum communication $\approx n/2$ qubits [Winter, 2004]
- With free classical communication: $o(n)$ qubits [Hayden, Winter, 2010]
  - Remark: classical communication alone is useless

# Quantum equality testing

| | **Alice** | **Bob** |
|---|---|---|
| *Inputs* | $\|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ | description of $\|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$ |
| *Ouput* | | YES with prob $\|\langle\psi\|\phi\rangle\|^2 \pm \epsilon$ |
| | | NO with prob $1 - \|\langle\psi\|\phi\rangle\|^2 \pm \epsilon$ |
| *Resource* | quantum communication $\longrightarrow$ | |

- Optimal quantum communication $\approx n/2$ qubits [Winter, 2004]
- With free classical communication: $o(n)$ qubits [Hayden, Winter, 2010]
  - Remark: classical communication alone is useless

**Theorem (Quantum equality testing)**

*Using free classical communication*

- *There exists a protocol using $O(\log(1/\epsilon))$ qubits communication*
- *There exists an efficient protocol using $O(\log^2(n/\epsilon))$ qubits communication*

# Quantum equality testing

| | **Alice** | **Bob** |
|---|---|---|
| *Inputs* | $\lvert\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ | description of $\lvert\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$ |
| *Ouput* | | YES with prob $\lvert\langle\psi\vert\phi\rangle\rvert^2 \pm \epsilon$ <br> NO with prob $1 - \lvert\langle\psi\vert\phi\rangle\rvert^2 \pm \epsilon$ |
| *Resource* | quantum communication $\longrightarrow$ | |

- Optimal quantum communication $\approx n/2$ qubits [Winter, 2004]
- With free classical communication: $o(n)$ qubits [Hayden, Winter, 2010]
  - Remark: classical communication alone is useless

**Theorem (Quantum equality testing)**

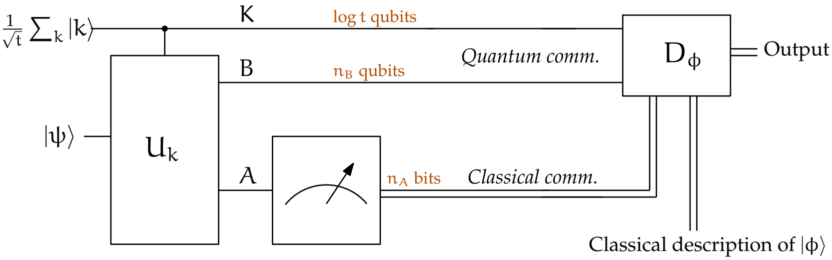
*Using free classical communication*

- *There exists a protocol using* $O(\log(1/\epsilon))$ *qubits communication*
- *There exists an efficient protocol using* $O(\log^2(n/\epsilon))$ *qubits communication*

Classical equality testing:

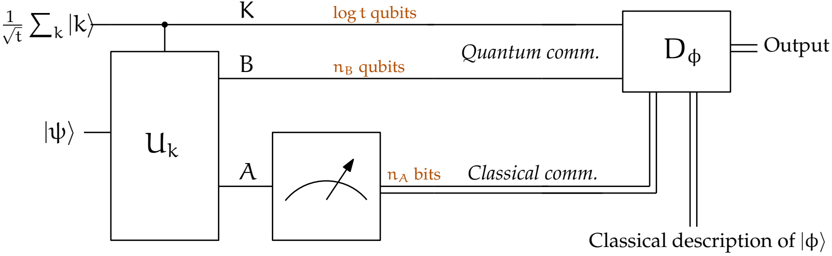
- With free shared randomness: $O(\log(1/\epsilon))$ bits communication
- Public-coin randomized comm. complexity of EQUALITY is $O(\log(1/\epsilon))$

# From metric UR to quantum equality testing




Quantum communication: $\log t + n_B$ qubits
Classical communication: $n_A$ bits

# From metric UR to quantum equality testing

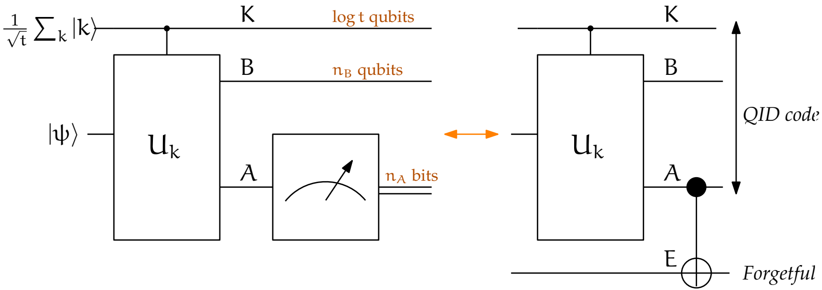



Quantum communication: $\log t + n_B$ qubits
Classical communication: $n_A$ bits

Proof: via duality between

*forgetfulness* and *geometry preservation* [Hayden, Winter, 2010]

# From metric UR to quantum equality testing




Quantum communication: $\log t + n_B$ qubits
Classical communication: $n_A$ bits

Proof: via duality between

*forgetfulness* and *geometry preservation* [Hayden, Winter, 2010]

# Outline

1. Metric uncertainty relations: definition and applications
   - Definition
   - Application: Encryption
   - Application: Quantum equality testing
2. Metric uncertainty relations: constructions
   - Known constructions
   - Metric interpretation
   - Efficient metric uncertainty relation

# Entropic URs with $t = 2$ measurements

Rectilinear and diagonal basis

- $I, H^{\otimes n}$

$$\frac{1}{2}\left(\mathbf{H}(p_{|\psi\rangle}) + \mathbf{H}(p_{H^{\otimes n}|\psi\rangle})\right) \geqslant \frac{1}{2}n$$

- $U_0, U_1$ mutually unbiased: $\forall x, y \in \{0,1\}^n \ |\langle x|U_0 U_1^\dagger|y\rangle|^2 = \frac{1}{2^n}$

$$\frac{1}{2}\left(\mathbf{H}(p_{U_0|\psi\rangle}) + \mathbf{H}(p_{U_1|\psi\rangle})\right) \geqslant \frac{1}{2}n$$

[Maassen, Uffink, 1989]

**Recall:** $p_{|\psi\rangle}(x) = |\langle x|\psi\rangle|^2$

The factor $1/2$ is optimal for $t = 2$ measurements

# Entropic URs with $t = 2$ measurements

Rectilinear and diagonal basis

- $I, H^{\otimes n}$

$$\frac{1}{2}\left(\mathbf{H}(p_{|\psi\rangle}) + \mathbf{H}(p_{H^{\otimes n}|\psi\rangle})\right) \geqslant \frac{1}{2}n$$

- $U_0, U_1$ mutually unbiased: $\forall x, y \in \{0,1\}^n \; |\langle x|U_0 U_1^\dagger|y\rangle|^2 = \frac{1}{2^n}$

$$\frac{1}{2}\left(\mathbf{H}(p_{U_0|\psi\rangle}) + \mathbf{H}(p_{U_1|\psi\rangle})\right) \geqslant \frac{1}{2}n$$

[Maassen, Uffink, 1989]

**Recall:** $p_{|\psi\rangle}(x) = |\langle x|\psi\rangle|^2$

The factor $1/2$ is optimal for $t = 2$ measurements

To increase the lower bound, need $t > 2$ measurements

# Entropic URs with $t > 2$ measurements

Want: $$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geqslant h(t) \qquad \text{for all } |\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$$

with $h(t) > n/2$ large

Natural candidate: Take $t$ mutually unbiased bases (MUBs)

# Entropic URs with $t > 2$ measurements

Want: $$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geqslant h(t) \qquad \text{for all } |\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$$

with $h(t) > n/2$ large

Natural candidate: Take $t$ mutually unbiased bases (MUBs)

## Definition (Mutually unbiased bases)

$U_0, \ldots, U_{t-1}$ define MUBs if for all $x, y \in \{0,1\}^n$ and all $k \neq k'$

$$|\langle x|U_k U_{k'}^\dagger|y\rangle| \leqslant \frac{1}{2^{n/2}}$$

# Entropic URs with $t > 2$ measurements

Want: $$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geqslant h(t) \qquad \text{for all } |\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$$

with $h(t) > n/2$ large

Natural candidate: Take $t$ mutually unbiased bases (MUBs)

**Definition (Mutually unbiased bases)**

$U_0, \ldots, U_{t-1}$ define MUBs if for all $x, y \in \{0,1\}^n$ and all $k \neq k'$

$$|\langle x|U_k U_{k'}^\dagger|y\rangle| \leqslant \frac{1}{2^{n/2}}$$

- For $t = 2^n + 1$ (full set of MUBs):
  $h(t) \geqslant \log(2^n + 1) - 1 \geqslant n - 1$ [Sanchez, 1993; Ivanovic, 1994]

# Entropic URs with $t > 2$ measurements

Want: $$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geqslant h(t) \qquad \text{for all } |\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$$

with $h(t) > n/2$ large

Natural candidate: Take $t$ mutually unbiased bases (MUBs)

**Definition (Mutually unbiased bases)**

$U_0, \ldots, U_{t-1}$ define MUBs if for all $x, y \in \{0,1\}^n$ and all $k \neq k'$

$$|\langle x|U_k U_{k'}^\dagger|y\rangle| \leqslant \frac{1}{2^{n/2}}$$

- For $t = 2^n + 1$ (full set of MUBs): $h(t) \geqslant \log(2^n + 1) - 1 \geqslant n - 1$ [Sanchez, 1993; Ivanovic, 1994]
- For $t < 2^{n/2}$, general MUBs do not work well: $\exists t$ MUBs with $h(t) \approx n/2$ [Ballester and Wehner, 2007; Ambainis, 2009]

# Entropic URs with $t > 2$ measurements

Want: $$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geqslant h(t) \qquad \text{for all } |\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$$

with $h(t) > n/2$ large

Other candidate: random bases [Hayden, Leung, Shor, Winter, 2004]
For $t = n^4$, there exists $U_0, \ldots, U_{t-1}$

$$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geqslant n - 3$$

**Remark:** Not explicit

# Metric URs: metric interpretation

**Definition (Metric uncertainty relation)**

$$\text{For all } |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \qquad \frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$$

In terms of fidelity

$1 - \epsilon \leqslant \frac{1}{t}\sum_k F\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right)$

# Metric URs: metric interpretation

**Definition (Metric uncertainty relation)**

For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ $\quad \frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$

In terms of fidelity

$$1-\epsilon \leqslant \frac{1}{t}\sum_k F\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) = \frac{1}{t}\sum_k \sum_{a\in\{0,1\}^n} |\langle a|U_k|\psi\rangle| \cdot \frac{1}{\sqrt{2^n}}$$

# Metric URs: metric interpretation

**Definition (Metric uncertainty relation)**

For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ $$\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$$

In terms of fidelity

$$1-\epsilon \leqslant \frac{1}{t}\sum_k F\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) = \frac{1}{t}\sum_k \sum_{a\in\{0,1\}^n} |\langle a|U_k|\psi\rangle| \cdot \frac{1}{\sqrt{2^n}}$$

Define $$V : |\psi\rangle \mapsto \frac{1}{\sqrt{t}}\sum_k |k\rangle \otimes U_k|\psi\rangle$$

For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, $$\| V|\psi\rangle \|_1 \geqslant (1-\epsilon)\sqrt{t2^n}\||\psi\rangle\|_2$$

# Metric URs: metric interpretation

**Definition (Metric uncertainty relation)**

For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ $\quad \frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$

In terms of fidelity

$$1-\epsilon \leqslant \frac{1}{t}\sum_k F\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) = \frac{1}{t}\sum_k \sum_{a\in\{0,1\}^n} |\langle a|U_k|\psi\rangle| \cdot \frac{1}{\sqrt{2^n}}$$

Define $\quad V : |\psi\rangle \mapsto \frac{1}{\sqrt{t}}\sum_k |k\rangle \otimes U_k|\psi\rangle$

For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, $\quad \sqrt{t2^n}\||\psi\rangle\|_2 \geqslant \|V|\psi\rangle\|_1 \geqslant (1-\epsilon)\sqrt{t2^n}\||\psi\rangle\|_2$

$V$ is a low-distortion embedding $(\mathbb{C}^{2^n}, \ell_2) \hookrightarrow (\mathbb{C}^{t2^n}, \ell_1)$

# Metric URs: metric interpretation

**Definition (Metric uncertainty relation)**

For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ $$\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$$

In terms of fidelity

$$1-\epsilon \leqslant \frac{1}{t}\sum_k F\left(p^A_{U_k|\psi\rangle}, \mathrm{unif}(\{0,1\}^{n_A})\right) = \frac{1}{t}\sum_{k,a} \sqrt{\sum_b |\langle a|\langle b|U_k|\psi\rangle|^2} \cdot \frac{1}{\sqrt{2^{n_A}}}$$

Define $$V : |\psi\rangle \mapsto \frac{1}{\sqrt{t}} \sum_k |k\rangle \otimes U_k|\psi\rangle$$

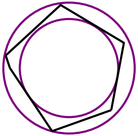
For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, $\sqrt{t2^n}\||\psi\rangle\|_2 \geqslant \|V|\psi\rangle\|_{\ell_1(\ell_2)} \geqslant (1-\epsilon)\sqrt{t2^n}\||\psi\rangle\|_2$

$V$ is a low-distortion embedding $(\mathbb{C}^{2^n}, \ell_2) \hookrightarrow (\mathbb{C}^{t2^n}, \ell_1(\ell_2))$

For $|\psi\rangle \in A \otimes B$, $\||\psi\rangle\|_{\ell_1^A(\ell_2^B)} = \sum_{a\in\{0,1\}^{n_A}} \|\langle a|\psi\rangle\|_2$

# $\ell_2 \hookrightarrow \ell_1$ embeddings

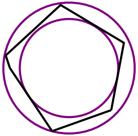
Dvoretzky's theorem:
For any normed space $(\mathbb{R}^d, \|\cdot\|)$, there is a large subspace $\|\cdot\| \approx_\epsilon \|\cdot\|_2$
[Dvoretzky, 1961; Milman, 1971; Milman and Schechtman, 1986;...]



Most common proof uses probabilistic method

# $\ell_2 \hookrightarrow \ell_1$ embeddings

Dvoretzky's theorem:
For any normed space $(\mathbb{R}^d, \|\cdot\|)$, there is a large subspace $\|\cdot\| \approx_\epsilon \|\cdot\|_2$
[Dvoretzky, 1961; Milman, 1971; Milman and Schechtman, 1986;...]



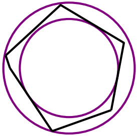
Most common proof uses probabilistic method

For $\ell_1$ norm

- Explicit constructions [Indyk, 2007; Guruswami, Lee, Razborov, 2009;...]
- Applications: high-dimensional nearest neighbour search and compressed sensing

# $\ell_2 \hookrightarrow \ell_1$ embeddings

Dvoretzky's theorem:
For any normed space $(\mathbb{R}^d, \|\cdot\|)$, there is a large subspace $\|\cdot\| \approx_\epsilon \|\cdot\|_2$
[Dvoretzky, 1961; Milman, 1971; Milman and Schechtman, 1986;...]



Most common proof uses probabilistic method

For $\ell_1$ norm

- Explicit constructions [Indyk, 2007; Guruswami, Lee, Razborov, 2009;...]
- Applications: high-dimensional nearest neighbour search and compressed sensing

For Schatten $p$-norms [Aubrun, Szarek, Werner, 2010]

- Counterexample additivity minimum output entropy [Hayden and Winter 2008; Hastings, 2009]

# Metric uncertainty relations: existence

**Theorem (Metric uncertainty relations)**

*$\exists\, U_0, \dots, U_{t-1}$ acting on $(\mathbb{C}^2)^{\otimes n} = A \otimes B$ with*

$$\log t = 3 \log(1/\epsilon) \qquad \text{and} \qquad n_A = n - 2\log(1/\epsilon)$$

$$\text{for all } |\psi\rangle \qquad \frac{1}{t} \sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, unif(\{0,1\}^{n_A})\right) \leqslant \epsilon.$$

Proof: Probabilistic argument, $U_0, \dots, U_{t-1}$ at random [Milman, 1971]

# Efficient metric UR: Structure of the construction

Use ideas of explicit $\ell_2$ into $\ell_1$ embedding of [Indyk, 2007]

Two ingredients:

1. Min-entropy uncertainty relation (mutually unbiased bases)
2. Permutation extractors

# Min-entropy uncertainty relation

**Lemma (MUBs define min-entropy uncertainty relations)**

*$V_0, \ldots, V_{r-1}$ define MUBs with $r = 1/\epsilon^2$, for all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$*

$$\frac{1}{r}\sum_{j=0}^{r-1} \mathbf{H}_{\min}^{\epsilon}(p_{V_j|\psi\rangle}) \gtrapprox (1-\epsilon)n/2$$

$$\mathbf{H}_{\min}(p) = -\log \max_{x\in\mathcal{X}} p(x)$$

$$\mathbf{H}_{\min}^{\epsilon}(p) = \max_{q:\Delta(p,q)\leqslant\epsilon} \mathbf{H}_{\min}(q)$$

# Min-entropy uncertainty relation

**Lemma (MUBs define min-entropy uncertainty relations)**

*$V_0, \ldots, V_{r-1}$ define MUBs with $r = 1/\epsilon^2$, for all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$*

$$\frac{1}{r} \sum_{j=0}^{r-1} \mathbf{H}^{\epsilon}_{\min}(p_{V_j|\psi\rangle}) \gtrsim (1-\epsilon)n/2$$

$$\mathbf{H}_{\min}(p) = -\log \max_{x \in \mathcal{X}} p(x)$$

$$\mathbf{H}^{\epsilon}_{\min}(p) = \max_{q:\Delta(p,q) \leqslant \epsilon} \mathbf{H}_{\min}(q)$$

**Remarks**

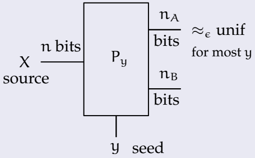
- Interpret as: for most values of $j$, $\mathbf{H}^{\epsilon}_{\min}(p_{V_j|\psi\rangle}) \gtrsim (1-\epsilon)n/2$
- Min-entropy UR of [Damgaard, Fehr, Renner, Salvail, Schaffner, 2007] uses $r = 2^n$ bases
- Rate $1/2$ is best possible

# Permutation extractors

**Definition (Strong permutation extractor)**

$P_0, \ldots, P_{s-1}$ permutations of $\{0,1\}^n$

$\mathbf{H}_{\min}(X) \geqslant \ell$

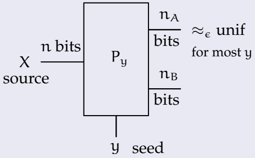


# Permutation extractors

## Definition (Strong permutation extractor)

$P_0, \dots, P_{s-1}$ permutations of $\{0,1\}^n$

$$\mathbf{H}_{\min}(X) \geqslant \ell \Rightarrow \frac{1}{s} \sum_{y=0}^{s-1} \Delta\left(P_y^A(X), \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$$



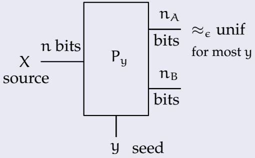

$P^A(x)$: first $n_A$ bits of $P(x)$

# Permutation extractors

**Definition (Strong permutation extractor)**

$P_0, \ldots, P_{s-1}$ permutations of $\{0,1\}^n$

$$\mathbf{H}_{\min}(X) \geqslant \ell \Rightarrow \frac{1}{s}\sum_{y=0}^{s-1} \Delta\left(P_y^A(X), \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$$




$P^A(x)$: first $n_A$ bits of $P(x)$

**Remarks:**

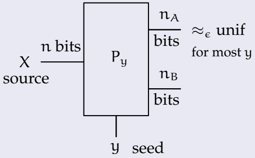
- Has to work for any $X$
- Want $n_A$ large (hopefully $n_A \approx \ell$) and $s$ small
- Special kind of randomness extractor (complexity and cryptography)
- Want efficient $P_y$ and $P_y^{-1}$

# Permutation extractors

## Definition (Strong permutation extractor)

$P_0, \ldots, P_{s-1}$ permutations of $\{0,1\}^n$

$$\mathbf{H}_{\min}(X) \geqslant \ell \Rightarrow \frac{1}{s}\sum_{y=0}^{s-1} \Delta\left(P_y^A(X), \mathrm{unif}(\{0,1\}^{n_A})\right) \leqslant \epsilon$$




$P^A(x)$: first $n_A$ bits of $P(x)$

**Remarks:**

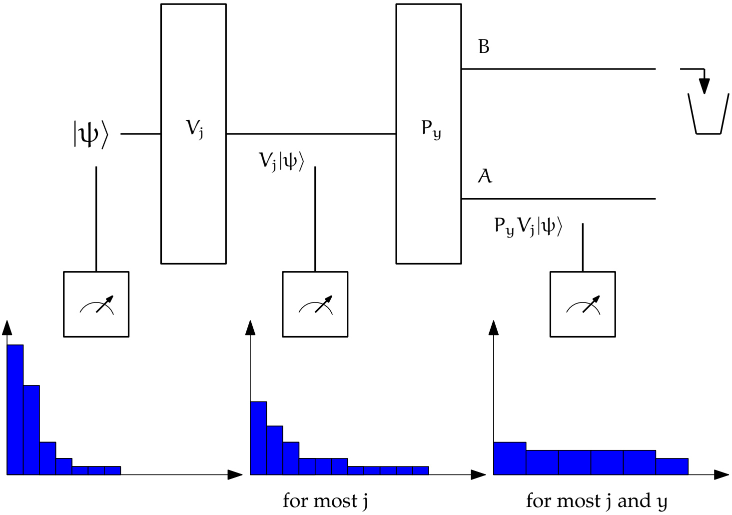
- Has to work for any $X$
- Want $n_A$ large (hopefully $n_A \approx \ell$) and $s$ small
- Special kind of randomness extractor (complexity and cryptography)
- Want efficient $P_y$ and $P_y^{-1}$

Adapting [Guruswami, Umans, Vadhan, 2009]

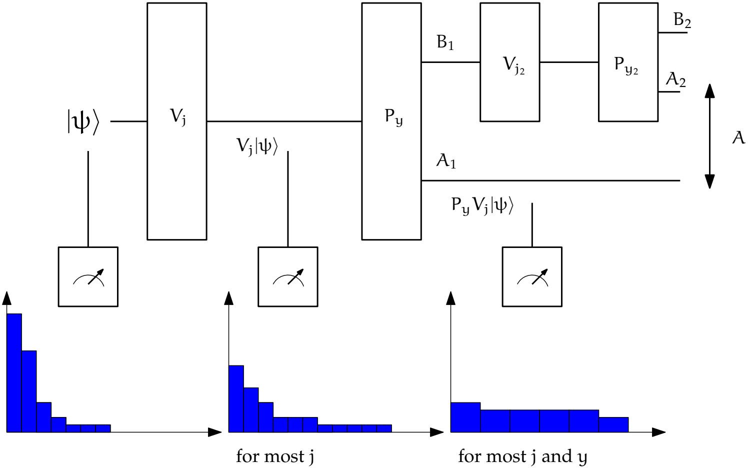
## Theorem

*∃ efficient strong perm. extractor with* $\log s = O(\log(n/\epsilon))$ *and* $n_A = (1-\delta)\ell$

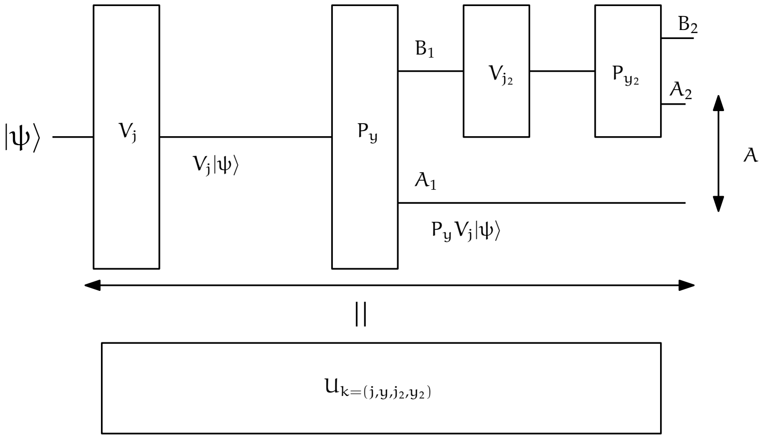
# Putting things together



# Putting things together



# Putting things together



# Parameters of the metric uncertainty relation

**Theorem (Efficient MURs: key optimized)**

$\exists U_0, \ldots, U_{t-1}$ *with* $\log t = c_\delta \log(n/\epsilon)$ *and* $n_A = (1-\delta)n$

$$\text{For all } |\psi\rangle, \qquad \frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, unif(\{0,1\}^{n_A})\right) \leqslant \epsilon$$

$U_0, \ldots, U_{t-1}$ *have quantum circuits of size* $O(n \operatorname{polylog}(n/\epsilon))$

**Theorem (Efficient MURs: *A* system maximized)**

$\exists U_0, \ldots, U_{t-1}$ *with* $\log t = c \log^2(n/\epsilon)$ *and* $n_A = n - O(\log(1/\epsilon) + \log\log n)$

$$\text{For all } |\psi\rangle, \qquad \frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, unif(\{0,1\}^{n_A})\right) \leqslant \epsilon$$

$U_0, \ldots, U_{t-1}$ *have quantum circuits of size* $O(n \operatorname{polylog}(n/\epsilon))$

# Summary

Inspired by definitions and results in asymptotic geometric analysis:

- Define metric uncertainty relations
- Prove random bases satisfy URs with better params
- Construct efficient metric URs
- First efficient strong information locking schemes
  - One of the schemes uses only Hadamard gates and classical computation
- Quantum equality testing
- Other results in paper:
  - Quantum hiding fingerprint [Gavinsky, Ito, 2010]
  - String commitment protocol [Buhrman, Christandl, Hayden, Lo, Wehner, 2006]

# Open questions

- Other cryptographic applications? Bounded/noisy storage model?
- Explicit constructions of UR matching probabilistic argument?
- Existence results of UR matching lower bounds? Are there $U_0, \ldots, U_{t-1}$

$$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geqslant \left(1 - \frac{1}{t}\right) n \quad \text{for } t > 2?$$

# Open questions

- Other cryptographic applications? Bounded/noisy storage model?
- Explicit constructions of UR matching probabilistic argument?
- Existence results of UR matching lower bounds? Are there $U_0, \ldots, U_{t-1}$

$$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geqslant \left(1 - \frac{1}{t}\right) n \quad \text{for } t > 2?$$

Thank you!

`arXiv:1010.3007`

See also `arXiv:1011.1612` [Dupuis, Florjancyk, Hayden, Leung, 2010]

Many thanks to Ivan Savov for comments on the presentation

# Extra: Proof of min-entropy uncertainty relation

**Lemma (MUBs define min-entropy uncertainty relations)**

*For "most" values of $j$, there exists $q_j$ s.t.* $\Delta\left(p_{V_j|\psi\rangle}, q_j\right) \leqslant \epsilon$ *and* $q_j(x) \lessapprox 2^{-n/2}$

Proof:

$$\vec{v} = \begin{bmatrix} V_0 \\ \vdots \\ V_{r-1} \end{bmatrix} |\psi\rangle \in \mathbb{C}^{r2^n} \qquad \vec{v}_{j,x} = \langle x|V_j|\psi\rangle \qquad V = \begin{bmatrix} V_0 \\ \vdots \\ V_{r-1} \end{bmatrix} \in \mathbb{C}^{r2^n \times 2^n}$$

1. $\vec{v}$ is spread: for any $|S| \leqslant 2^{n/2}$, $\|\vec{v}_S\|_2^2 \leqslant \frac{2}{r}\|\vec{v}\|_2^2$
   - $\vec{v}_S = V_S|\psi\rangle$
   - $\|\vec{v}_S\|_2^2 = |\langle\psi|V_S^\dagger V_S|\psi\rangle| \leqslant \max$ eigenvalue of $V_S^\dagger V_S$

$$V_S^\dagger V_S = \begin{bmatrix} 1 & \langle y|V_{j'}^\dagger V_j|x\rangle & \dots \\ \langle x|V_j^\dagger V_{j'}|y\rangle & \ddots & \vdots \\ \vdots & \dots & 1 \end{bmatrix}$$

   - $\max$ eigenvalue of $V_S^\dagger V_S \leqslant 1 + |S|2^{-n/2} \leftarrow$ use MUB here

# Extra: Proof of min-entropy uncertainty relation

**Lemma (MUBs define min-entropy uncertainty relations)**

*For "most" values of j, there exists $q_j$ s.t.* $\Delta\left(p_{V_j|\psi\rangle}, q_j\right) \leqslant \epsilon$ *and* $q_j(x) \lessapprox 2^{-n/2}$

Proof:

$$\vec{v} = \begin{bmatrix} V_0 \\ \vdots \\ V_{r-1} \end{bmatrix} |\psi\rangle \in \mathbb{C}^{r2^n} \qquad \vec{v}_{j,x} = \langle x|V_j|\psi\rangle \qquad V = \begin{bmatrix} V_0 \\ \vdots \\ V_{r-1} \end{bmatrix} \in \mathbb{C}^{r2^n \times 2^n}$$

1. $\vec{v}$ is spread: for any $|S| \leqslant 2^{n/2}$, $\|\vec{v}_S\|_2^2 \leqslant \frac{2}{r}\|\vec{v}\|_2^2$
2. $S =$ largest $2^{n/2}$ indices of $\vec{v}$ $\qquad \vec{w}_{j,x} = \begin{cases} \vec{v}_{j,x} & \text{if } (j,x) \notin S \\ 0 & \text{if } (j,x) \in S \end{cases}$
3. Define $q_j(x) = |w_{j,x}|^2$ (recall $p_{V_j|\psi\rangle}(x) = |\vec{v}_{j,x}|^2$)
4. For "most" values of $j$, $q_j \approx_\epsilon$ distribution
5. $|S| \cdot q_j(x) \leqslant \|\vec{v}\|_2^2 = r \quad \Rightarrow \quad q_j(x) \leqslant r2^{-n/2}$ $\square$

# Extra: Proof of min-entropy uncertainty relation

**Lemma (MUBs define min-entropy uncertainty relations)**

*For "most" values of $j$, there exists $q_j$ s.t.* $\Delta\left(p_{V_j|\psi\rangle}, q_j\right) \leqslant \epsilon$ *and* $q_j(x) \lessapprox 2^{-n/2}$

Proof:

$$\vec{v} = \begin{bmatrix} V_0 \\ \vdots \\ V_{r-1} \end{bmatrix} |\psi\rangle \in \mathbb{C}^{r2^n} \qquad \vec{v}_{j,x} = \langle x|V_j|\psi\rangle \qquad V = \begin{bmatrix} V_0 \\ \vdots \\ V_{r-1} \end{bmatrix} \in \mathbb{C}^{r2^n \times 2^n}$$

1. $\vec{v}$ is spread: for any $|S| \leqslant 2^{n/2}$, $\|\vec{v}_S\|_2^2 \leqslant \frac{2}{r}\|\vec{v}\|_2^2$
2. $S =$ largest $2^{n/2}$ indices of $\vec{v}$ $\qquad \vec{w}_{j,x} = \begin{cases} \vec{v}_{j,x} & \text{if } (j,x) \notin S \\ 0 & \text{if } (j,x) \in S \end{cases}$
3. Define $q_j(x) = |w_{j,x}|^2$ (recall $p_{V_j|\psi\rangle}(x) = |\vec{v}_{j,x}|^2$)
4. For "most" values of $j$, $q_j \approx_\epsilon$ distribution
5. $|S| \cdot q_j(x) \leqslant \|\vec{v}\|_2^2 = r \quad \Rightarrow \quad q_j(x) \leqslant r2^{-n/2}$ $\square$

## Extra: Min-entropy uncertainty relation (generalized)

Approximate MUB: $\forall x, y \; |\langle x|V_j V_{j'}^\dagger|y\rangle| \leqslant \frac{1}{2^{\gamma n/2}}$ $\gamma \in [0,1]$

**Lemma (Min-entropy uncertainty relations)**

*$V_0, \ldots, V_{r-1}$ define $\gamma$-MUBs with $r = 1/\epsilon^2$, for all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$*

$$\frac{1}{r}\sum_{j=0}^{r-1} \mathbf{H}_{\min}^{\epsilon}(p_{V_j|\psi\rangle}) \gtrapprox (1-\epsilon)\gamma n/2$$

# Extra: Min-entropy uncertainty relation (generalized)

Approximate MUB: $\forall x, y \; |\langle x|V_j V_{j'}^{\dagger}|y\rangle| \leqslant \frac{1}{2^{\gamma n/2}}$ $\quad \gamma \in [0,1]$

**Lemma (Min-entropy uncertainty relations)**

*$V_0, \ldots, V_{r-1}$ define $\gamma$-MUBs with $r = 1/\epsilon^2$, for all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$*

$$\frac{1}{r} \sum_{j=0}^{r-1} \mathbf{H}_{\min}^{\epsilon}(p_{V_j|\psi\rangle}) \gtrapprox (1-\epsilon)\gamma n/2$$

**Lemma (1/2-MUBs with single qubit unitaries)**

*There exist $V_j \in \left\{ H^{u_1} \otimes H^{u_2} \otimes \cdots \otimes H^{u_n} : u_i \in \{0,1\} \right\}$ for $j \in [t]$ that define $1/2$-MUBs*

$H$: transforms $+$ to $\times$