

Quantum Encryption of Classical Messages Using Mutually Unbiased Bases

Louis Salvail

(joint work with I. Damgård, and T. Pedersen)

BRICS, Department of Computer Science
University of Aarhus



Entropic Relations: The Setting

- Let $|\psi\rangle \in \mathcal{H}_N$ be an arbitrary quantum state of $n = \log N$ qubits.
- Let $B = \{|b_i\rangle\}_{i=1}$ be an **orthonormal basis** in \mathcal{H}_N .

Entropic Relations: The Setting

- Let $|\psi\rangle \in \mathcal{H}_N$ be an arbitrary quantum state of $n = \log N$ qubits.
- Let $\mathbf{B} = \{|b_i\rangle\}_{i=1}$ be an **orthonormal basis** in \mathcal{H}_N .

We define the probability distribution:

$$B_\psi(i) = \|\langle b_i | \psi \rangle\|^2 \text{ for } 1 \leq i \leq N.$$

We write:

$$H(\mathbf{B}_\psi) \equiv - \sum_i B_\psi(i) \log B_\psi(i).$$

Entropic Relations: The Setting

- Let $|\psi\rangle \in \mathcal{H}_N$ be an arbitrary quantum state of $n = \log N$ qubits.
- Let $\mathbf{B} = \{|b_i\rangle\}_{i=1}$ be an orthonormal basis in \mathcal{H}_N .

We define the probability distribution:

$$B_\psi(i) = \|\langle b_i | \psi \rangle\|^2 \text{ for } 1 \leq i \leq N.$$

We write:

$$H(\mathbf{B}_\psi) \equiv - \sum_i B_\psi(i) \log B_\psi(i).$$

More generally, for $-1 < \alpha < \infty$, the Renyi entropy of order α is

$$H_\alpha(\mathbf{B}_\psi) = -\log \left(\sum_i B_\psi(i)^{1+\alpha} \right)^{1/\alpha}, \text{ and } \begin{cases} H_0(\mathbf{B}_\psi) \equiv H(\mathbf{B}_\psi), \\ H_\infty(\mathbf{B}_\psi) \equiv -\log(\max_i (B_\psi(i))). \end{cases}$$

Mutually Unbiased Bases

Definition: A set of orthonormal bases \mathfrak{B} for \mathcal{H}_N is said to be *mutually unbiased* if

$$(\forall B \neq B' \in \mathfrak{B})(\forall b \in B)(\forall b' \in B')[|\langle b|b' \rangle| = 1/\sqrt{N}].$$

Mutually Unbiased Bases

Definition: A set of orthonormal bases \mathfrak{B} for \mathcal{H}_N is said to be *mutually unbiased* if

$$(\forall \mathbf{B} \neq \mathbf{B}' \in \mathfrak{B})(\forall b \in \mathbf{B})(\forall b' \in \mathbf{B}') [|\langle b|b' \rangle| = 1/\sqrt{N}].$$

Example: $\mathfrak{B} = \{+^n, \times^n, \circ^n\}$ is a set of 3 *mutually unbiased* bases for $\mathcal{H}_{2^n}, n \geq 1$.

Mutually Unbiased Bases

Definition: A set of orthonormal bases \mathfrak{B} for \mathcal{H}_N is said to be *mutually unbiased* if

$$(\forall \mathbf{B} \neq \mathbf{B}' \in \mathfrak{B})(\forall b \in \mathbf{B})(\forall b' \in \mathbf{B}') [|\langle b | b' \rangle| = 1/\sqrt{N}].$$

Example: $\mathfrak{B} = \{+^n, \times^n, \circ^n\}$ is a set of 3 *mutually unbiased* bases for $\mathcal{H}_{2^n}, n \geq 1$.

Theorem [Wootters-Field88]: There are sets \mathfrak{B} of $N + 1$ (and no more) *mutually unbiased* bases for \mathcal{H}_N .

Mutually Unbiased Bases

Definition: A set of orthonormal bases \mathfrak{B} for \mathcal{H}_N is said to be *mutually unbiased* if

$$(\forall \mathbf{B} \neq \mathbf{B}' \in \mathfrak{B})(\forall b \in \mathbf{B})(\forall b' \in \mathbf{B}') [|\langle b | b' \rangle| = 1/\sqrt{N}].$$

Example: $\mathfrak{B} = \{+^n, \times^n, \circ^n\}$ is a set of 3 *mutually unbiased* bases for $\mathcal{H}_{2^n}, n \geq 1$.

Theorem [Wootters-Field88]: There are sets \mathfrak{B} of $N + 1$ (and no more) *mutually unbiased* bases for \mathcal{H}_N .

- There is a quantum circuit $\mathcal{G}_{\mathbf{B}}$ running in $O(n^3)$ that computes the mapping $\psi_{\mathbf{B}} : \{0, 1\}^n \mapsto \mathbf{B}$ where $\langle \psi_{\mathbf{B}}(a) | \psi_{\mathbf{B}}(a') \rangle = \delta_{a,a'}$ for all $\mathbf{B} \in \mathfrak{B}$.

Entropic Relations

Theorem[Maassen-Uffink88]: *For any pair of mutually unbiased bases P and Q for \mathcal{H}_N and for any state $|\psi\rangle \in \mathcal{H}_N$:*

$$H(P_\psi) + H(Q_\psi) \geq \log N.$$

Entropic Relations

Theorem[Maassen-Uffink88]: For any pair of mutually unbiased bases P and Q for \mathcal{H}_N and for any state $|\psi\rangle \in \mathcal{H}_N$:

$$H(P_\psi) + H(Q_\psi) \geq \log N.$$

Theorem[Larsen]: Let $\mathfrak{B} = \{B^{(i)}\}_{i=1}^{N+1}$ be a maximal set of mutually unbiased bases for \mathcal{H}_N . Then, for any state $|\psi\rangle \in \mathcal{H}_N$,

$$\sum_i \sum_j \left(B_\psi^{(i)}(j) \right)^2 = 2.$$

Q-Encryption of Classical Messages

Definition: An (m, n) -cipher consists of:

Plaintexts: The set of n -bit messages,

Encryption: For all keys $k \in \{0, 1\}^m$ and messages $\mathbf{p} \in \{0, 1\}^n$

$\mathcal{E}_k(\mathbf{p}) = E_k(|\mathbf{p}\rangle \otimes |0\rangle)$, where E_k is unitary.

Q-Encryption of Classical Messages

Definition: An (m, n) -cipher consists of:

Plaintexts: The set of n -bit messages,

Encryption: For all keys $k \in \{0, 1\}^m$ and messages $\mathbf{p} \in \{0, 1\}^n$
 $\mathcal{E}_k(\mathbf{p}) = E_k(|\mathbf{p}\rangle \otimes |0\rangle)$, where E_k is unitary.

Furthermore we require:

Perfect security: For all plaintext \mathbf{p} and \mathbf{p}' ,

$$\sum_{k \in \{0,1\}^m} 2^{-m} \mathcal{E}_k(\mathbf{p}) = \sum_{k \in \{0,1\}^m} 2^{-m} \mathcal{E}_k(\mathbf{p}').$$

Key hiding: For all keys $k, k' \in \{0, 1\}^m$,

$$\sum_{\mathbf{p} \in \{0,1\}^n} 2^{-n} \mathcal{E}_k(\mathbf{p}) = \sum_{\mathbf{p} \in \{0,1\}^n} 2^{-n} \mathcal{E}_{k'}(\mathbf{p}).$$

Secret-Key Min-Entropy

Consider:

Secret-Key Min-Entropy

Consider:

- The **min-entropy** $H_\infty(p_1, \dots, p_n) := -\log_2(\max\{p_1, \dots, p_n\})$ of a probability distribution.

Secret-Key Min-Entropy

Consider:

- The **min-entropy** $H_\infty(p_1, \dots, p_n) := -\log_2(\max\{p_1, \dots, p_n\})$ of a probability distribution.
- In our case, this is related the best guessing probability for the **key** after having seen a **ciphertext** together with its associated **plaintext**.

Secret-Key Min-Entropy

Consider:

- The **min-entropy** $H_\infty(p_1, \dots, p_n) := -\log_2(\max\{p_1, \dots, p_n\})$ of a probability distribution.
- In our case, this is related the best guessing probability for the **key** after having seen a **ciphertext** together with its associated **plaintext**.

Theorem[Folk]: *Any classical (m, n) -cipher has secret-key **min-entropy** at most $m - n$ bits.*

Secret-Key Min-Entropy

Consider:

- The **min-entropy** $H_\infty(p_1, \dots, p_n) := -\log_2(\max\{p_1, \dots, p_n\})$ of a probability distribution.
- In our case, this is related the best guessing probability for the **key** after having seen a **ciphertext** together with its associated **plaintext**.

Theorem[Folk]: *Any classical (m, n) -cipher has secret-key **min-entropy** at most $m - n$ bits.*

Theorem: *Any quantum (m, n) -cipher has secret-key **min-entropy** at most $m - n$ bits.*

Secret-Key Min-Entropy

Consider:

- The **min-entropy** $H_\infty(p_1, \dots, p_n) := -\log_2(\max\{p_1, \dots, p_n\})$ of a probability distribution.
- In our case, this is related the best guessing probability for the **key** after having seen a **ciphertext** together with its associated **plaintext**.

Theorem[Folk]: *Any classical (m, n) -cipher has secret-key **min-entropy** at most $m - n$ bits.*

Theorem: *Any quantum (m, n) -cipher has secret-key **min-entropy** at most $m - n$ bits.*

- We are given plaintext $\mathbf{p} \in \{0, 1\}^m$.
- Define measurement operators $M_k \equiv 2^{n-m} \mathcal{E}_k(\mathbf{p}) \mathcal{E}_k(\mathbf{p})^\dagger$, $k \in \{0, 1\}^m$
- $\{M_k\}_{k \in \{0, 1\}^m}$ is a POVM.
- For all keys k , $\text{Tr}(M_k \mathcal{E}_k(\mathbf{p})) = 2^{n-m}$.

Ciphers

H_n : is a $(n+1, n)$ -cipher. Let $k = (x, b)$ where $x \in \{0, 1\}^n$ and $b \in \{0, 1\}$ be the secret-key. For message $p \in \{0, 1\}^n$, the encryption works as follows:

$$E_k : |p\rangle \mapsto (H^{\otimes n})^b |p \oplus x\rangle.$$

Ciphers

H_n : is a $(n+1, n)$ -cipher. Let $k = (x, b)$ where $x \in \{0, 1\}^n$ and $b \in \{0, 1\}$ be the secret-key. For message $p \in \{0, 1\}^n$, the encryption works as follows:

$$E_k : |p\rangle \mapsto (H^{\otimes n})^b |p \oplus x\rangle.$$

W_n : is a $(2n, n)$ -cipher. Let $k = (x, b)$ where $x, b \in \{0, 1\}^n$ and let $\mathfrak{B} = \{B^{(z)}\}_{z \in \{0, 1\}^n}$ be a set of 2^n mutually unbiased bases. For message $p \in \{0, 1\}^n$, the encryption works as follows:

$$E_k : |p\rangle \mapsto \mathcal{G}_{B^{(b)}} |p \oplus x\rangle.$$

Ciphers

H_n : is a $(n+1, n)$ -cipher. Let $k = (x, b)$ where $x \in \{0, 1\}^n$ and $b \in \{0, 1\}$ be the secret-key. For message $p \in \{0, 1\}^n$, the encryption works as follows:

$$E_k : |p\rangle \mapsto (H^{\otimes n})^b |p \oplus x\rangle.$$

W_n : is a $(2n, n)$ -cipher. Let $k = (x, b)$ where $x, b \in \{0, 1\}^n$ and let $\mathfrak{B} = \{B^{(z)}\}_{z \in \{0, 1\}^n}$ be a set of 2^n mutually unbiased bases. For message $p \in \{0, 1\}^n$, the encryption works as follows:

$$E_k : |p\rangle \mapsto \mathcal{G}_{B^{(b)}} |p \oplus x\rangle.$$

$C_n(\mathfrak{B})$: \mathfrak{B} is a set of 2^t mutually unbiased bases. This is a $(n+t, n)$ -cipher where the encryption is defined similarly to the previous case.

Secret-Key Uncertainty

- Consider the Shannon entropy on the secret-key given a pair $(\mathbf{p}, \mathcal{E}_k(\mathbf{p}))$ of plaintext and associated cipherstate.
- $H(K | (\mathbf{p}, \mathcal{E}_k(\mathbf{p})))$ denotes the *secret-key uncertainty* for cipher \mathcal{E}_k .

Secret-Key Uncertainty

- Consider the Shannon entropy on the secret-key given a pair $(\mathbf{p}, \mathcal{E}_k(\mathbf{p}))$ of plaintext and associated cipherstate.
- $H(K | (\mathbf{p}, \mathcal{E}_k(\mathbf{p})))$ denotes the *secret-key uncertainty* for cipher \mathcal{E}_k .

Theorem[Folk]: Any classical (m, n) cipher has secret-key uncertainty at most $m - n$ bits.

Secret-Key Uncertainty

- Consider the Shannon entropy on the secret-key given a pair $(\mathbf{p}, \mathcal{E}_k(\mathbf{p}))$ of plaintext and associated cipherstate.
- $H(K | (\mathbf{p}, \mathcal{E}_k(\mathbf{p})))$ denotes the *secret-key uncertainty* for cipher \mathcal{E}_k .

Theorem[Folk]: Any classical (m, n) cipher has secret-key uncertainty at most $m - n$ bits.

Theorem: H_n is a $(n + 1, n)$ -cipher with secret-key uncertainty equals to $n/2 + 1$ bits. The bound holds for all outcomes of any measurement.

- This is similar to (un)locking classical correlation[DHLST03].

Secret-Key Uncertainty

- Consider the Shannon entropy on the secret-key given a pair $(\mathbf{p}, \mathcal{E}_k(\mathbf{p}))$ of plaintext and associated cipherstate.
- $H(K | (\mathbf{p}, \mathcal{E}_k(\mathbf{p})))$ denotes the *secret-key uncertainty* for cipher \mathcal{E}_k .

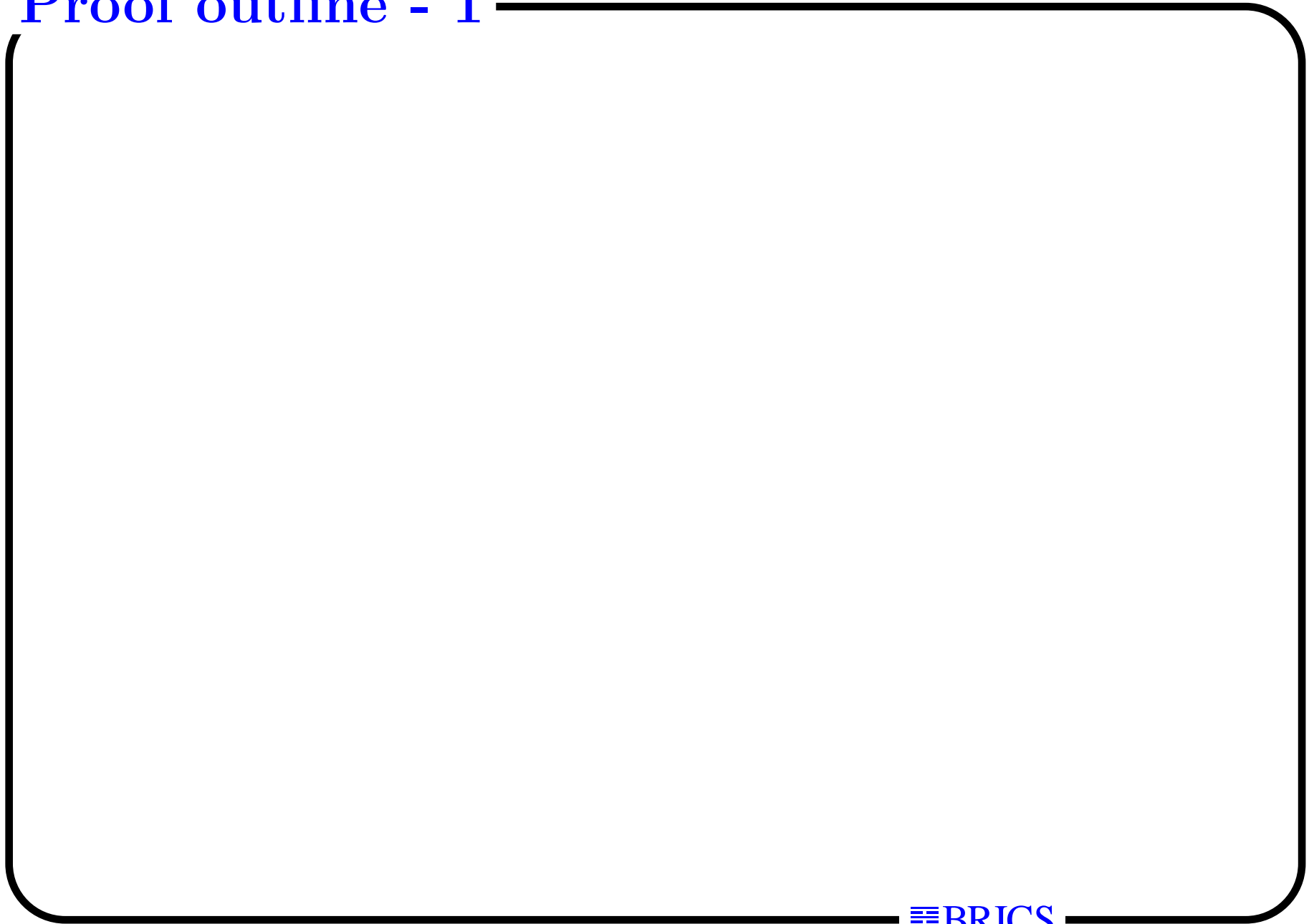
Theorem[Folk]: Any classical (m, n) cipher has secret-key uncertainty at most $m - n$ bits.

Theorem: H_n is a $(n + 1, n)$ -cipher with secret-key uncertainty equals to $n/2 + 1$ bits. The bound holds for all outcomes of any measurement.

- This is similar to (un)locking classical correlation[DHLST03].

Theorem: W_n is a $(2n, n)$ -cipher with secret-key uncertainty (and collision entropy) at least $2n - 1$ bits. This bound holds for all outcomes of any measurement.

Proof outline - 1



Proof outline - 1

General bound

- Known plaintext $\mathbf{p} \in \{0, 1\}^n$ is encrypted and $\mathcal{E}_k(\mathbf{p})$ is given to the adversary together with \mathbf{p} .
- The attacker applies the *optimal measurement* \mathcal{M}^* and gets outcome $|u\rangle \in \mathcal{H}_N$.

Proof outline - 1

General bound

- Known plaintext $\mathbf{p} \in \{0, 1\}^n$ is encrypted and $\mathcal{E}_k(\mathbf{p})$ is given to the adversary together with \mathbf{p} .
- The attacker applies the *optimal measurement* \mathcal{M}^* and gets outcome $|u\rangle \in \mathcal{H}_N$.

Minimization problem

- $H(K | U) = \sum_u P[U = u]H(K | U = u) \geq \min_u \{H(K | U = u)\}.$

Proof outline - 1

General bound

- Known plaintext $\mathbf{p} \in \{0, 1\}^n$ is encrypted and $\mathcal{E}_k(\mathbf{p})$ is given to the adversary together with \mathbf{p} .
- The attacker applies the *optimal measurement* \mathcal{M}^* and gets outcome $|u\rangle \in \mathcal{H}_N$.

Minimization problem

- $H(K | U) = \sum_u P[U = u]H(K | U = u) \geq \min_u \{H(K | U = u)\}$.

Connection to uncertainty relations

- $\text{MES}(\mathfrak{B}) := \min_u \{ \sum_{B \in \mathfrak{B}} H(B_u) \}$
- $H(K | U) \geq \text{MES}(\mathfrak{B})/2^{m-n} + (m - n)$.

Proof outline - 2

Remember:

- $H(K | U) \geq \text{MES}(\mathfrak{B})/2^{m-n} + (m - n)$.

Proof outline - 2

Remember:

- $H(K | U) \geq \text{MES}(\mathfrak{B})/2^{m-n} + (m - n)$.

H_n :

Proof outline - 2

Remember:

- $H(K | U) \geq \text{MES}(\mathfrak{B})/2^{m-n} + (m - n)$.

H_n :

- The result of [Maassen-Uffink] gives:

$$\text{MES}(\mathfrak{B}) = n.$$

Proof outline - 2

Remember:

- $H(K | U) \geq \text{MES}(\mathfrak{B})/2^{m-n} + (m - n)$.

H_n :

- The result of [Maassen-Uffink] gives:

$$\text{MES}(\mathfrak{B}) = n.$$

- $H(K | U) = n/2 + 1$.

Proof outline - 2

Remember:

- $H(K | U) \geq \text{MES}(\mathfrak{B})/2^{m-n} + (m - n)$.

H_n :

- The result of [Maassen-Uffink] gives:

$$\text{MES}(\mathfrak{B}) = n.$$

- $H(K | U) = n/2 + 1$.
- This bound is tight.

Proof outline - 2

Remember:

- $H(K | U) \geq \text{MES}(\mathfrak{B})/2^{m-n} + (m - n)$.

H_n :

- The result of [Maassen-Uffink] gives:

$$\text{MES}(\mathfrak{B}) = n.$$

- $H(K | U) = n/2 + 1$.
- This bound is tight.

W_n :

Proof outline - 2

Remember:

- $H(K | U) \geq \text{MES}(\mathfrak{B})/2^{m-n} + (m - n)$.

H_n :

- The result of [Maassen-Uffink] gives:

$$\text{MES}(\mathfrak{B}) = n.$$

- $H(K | U) = n/2 + 1$.
- This bound is tight.

W_n :

- The result of [Larsen] together with a result by [Sánchez-Ruiz] gives $\text{MES}(\mathfrak{B}) \geq 2^n(n - 1)$.

Proof outline - 2

Remember:

- $H(K | U) \geq \text{MES}(\mathfrak{B})/2^{m-n} + (m - n)$.

H_n :

- The result of [Maassen-Uffink] gives:

$$\text{MES}(\mathfrak{B}) = n.$$

- $H(K | U) = n/2 + 1$.
- This bound is tight.

W_n :

- The result of [Larsen] together with a result by [Sánchez-Ruiz] gives $\text{MES}(\mathfrak{B}) \geq 2^n(n - 1)$.
- $H(K | U) \geq 2n - 1$ and also $H_2(K | U) \geq 2n - 1$.

Conjecture #1

The entropic uncertainty relation for a set \mathfrak{B}_ℓ of 2^ℓ mutually unbiased bases is not known precisely.

Conjecture #1

The entropic uncertainty relation for a set \mathfrak{B}_ℓ of 2^ℓ mutually unbiased bases is not known precisely. However,

$$\text{MES}(\mathfrak{B}_\ell) \leq (2^\ell - 1)n.$$

Conjecture #1

The entropic uncertainty relation for a set \mathfrak{B}_ℓ of 2^ℓ mutually unbiased bases is not known precisely. However,

$$\text{MES}(\mathfrak{B}_\ell) \leq (2^\ell - 1)n.$$

Let's define:

$$\Delta(n, \ell) = (2^\ell - 1)n - \text{MES}(\mathfrak{B}_\ell).$$

Conjecture #1

The entropic uncertainty relation for a set \mathfrak{B}_ℓ of 2^ℓ mutually unbiased bases is not known precisely. However,

$$\text{MES}(\mathfrak{B}_\ell) \leq (2^\ell - 1)n.$$

Let's define:

$$\Delta(n, \ell) = (2^\ell - 1)n - \text{MES}(\mathfrak{B}_\ell).$$

We know:

$$\Delta(n, 1) = 0 \text{ and } \Delta(n, n) \leq (2^n - 1)n - 2^n(n - 1) = 2^n - n.$$

Conjecture #1

The entropic uncertainty relation for a set \mathfrak{B}_ℓ of 2^ℓ mutually unbiased bases is not known precisely. However,

$$\text{MES}(\mathfrak{B}_\ell) \leq (2^\ell - 1)n.$$

Let's define:

$$\Delta(n, \ell) = (2^\ell - 1)n - \text{MES}(\mathfrak{B}_\ell).$$

We know:

$$\Delta(n, 1) = 0 \text{ and } \Delta(n, n) \leq (2^n - 1)n - 2^n(n - 1) = 2^n - n.$$

Conjecture 1: *For any set of mutually unbiased bases \mathfrak{B}_n , it holds that $2^{-n} \Delta(n, n) \in o(1)$.*

Conjecture #1

The entropic uncertainty relation for a set \mathfrak{B}_ℓ of 2^ℓ mutually unbiased bases is not known precisely. However,

$$\text{MES}(\mathfrak{B}_\ell) \leq (2^\ell - 1)n.$$

Let's define:

$$\Delta(n, \ell) = (2^\ell - 1)n - \text{MES}(\mathfrak{B}_\ell).$$

We know:

$$\Delta(n, 1) = 0 \text{ and } \Delta(n, n) \leq (2^n - 1)n - 2^n(n - 1) = 2^n - n.$$

Conjecture 1: *For any set of mutually unbiased bases \mathfrak{B}_n , it holds that $2^{-n}\Delta(n, n) \in o(1)$.*

Lemma: *Under Conjecture 1, W_n has key-uncertainty at least $2n - o(1)$ bits.*

Composing Ciphers

Consider the composition of the $(t + n, n)$ -cipher $C_n(\mathfrak{B})$ using independent and random secret-keys.

Composing Ciphers

Consider the composition of the $(t + n, n)$ -cipher $C_n(\mathfrak{B})$ using independent and random secret-keys.

What is the key-uncertainty of cipher $C_n^2(\mathfrak{B}) \equiv C_n(\mathfrak{B}) \times C_n(\mathfrak{B})$?

Composing Ciphers

Consider the composition of the $(t + n, n)$ -cipher $C_n(\mathfrak{B})$ using independent and random secret-keys.

What is the key-uncertainty of cipher $C_n^2(\mathfrak{B}) \equiv C_n(\mathfrak{B}) \times C_n(\mathfrak{B})$?

- $C_n^2(\mathfrak{B})$ is a $(2(n + t), 2n)$ -cipher,

Composing Ciphers

Consider the composition of the $(t + n, n)$ -cipher $C_n(\mathfrak{B})$ using independent and random secret-keys.

What is the key-uncertainty of cipher $C_n^2(\mathfrak{B}) \equiv C_n(\mathfrak{B}) \times C_n(\mathfrak{B})$?

- $C_n^2(\mathfrak{B})$ is a $(2(n + t), 2n)$ -cipher,
- If $\mathfrak{B} = \{B_0, \dots, B_{2^t}\}$ then the possible bases for $C_n^2(\mathfrak{B})$ are:

$$\mathfrak{B} \otimes \mathfrak{B} = \{B_i \otimes B_j\}_{i,j}.$$

Composing Ciphers

Consider the composition of the $(t + n, n)$ -cipher $C_n(\mathfrak{B})$ using independent and random secret-keys.

What is the key-uncertainty of cipher $C_n^2(\mathfrak{B}) \equiv C_n(\mathfrak{B}) \times C_n(\mathfrak{B})$?

- $C_n^2(\mathfrak{B})$ is a $(2(n + t), 2n)$ -cipher,
- If $\mathfrak{B} = \{B_0, \dots, B_{2^t}\}$ then the possible bases for $C_n^2(\mathfrak{B})$ are:

$$\mathfrak{B} \otimes \mathfrak{B} = \{B_i \otimes B_j\}_{i,j}.$$

- $\mathfrak{B} \otimes \mathfrak{B}$ is **not a set** of mutually unbiased bases!

Composing Ciphers

Consider the composition of the $(t + n, n)$ -cipher $C_n(\mathfrak{B})$ using independent and random secret-keys.

What is the key-uncertainty of cipher $C_n^2(\mathfrak{B}) \equiv C_n(\mathfrak{B}) \times C_n(\mathfrak{B})$?

- $C_n^2(\mathfrak{B})$ is a $(2(n + t), 2n)$ -cipher,
- If $\mathfrak{B} = \{B_0, \dots, B_{2^t}\}$ then the possible bases for $C_n^2(\mathfrak{B})$ are:

$$\mathfrak{B} \otimes \mathfrak{B} = \{B_i \otimes B_j\}_{i,j}.$$

- $\mathfrak{B} \otimes \mathfrak{B}$ is **not a set** of mutually unbiased bases!
- The adversary applies a measurement that minimizes the uncertainty about the state picked given the plaintexts.

Composing Ciphers(II)

We split $\mathfrak{B} \otimes \mathfrak{B} = \{\mathfrak{B}_i\}_{i=1}^{2^t}$ as follows:

Composing Ciphers(II)

We split $\mathfrak{B} \otimes \mathfrak{B} = \{\mathfrak{B}_i\}_{i=1}^{2^t}$ as follows:

$$\mathfrak{B}_i = \{B_j \otimes B_{j+i \bmod 2^t} \mid j = 0, \dots, 2^t - 1\}$$

Composing Ciphers(II)

We split $\mathfrak{B} \otimes \mathfrak{B} = \{\mathfrak{B}_i\}_{i=1}^{2^t}$ as follows:

$$\mathfrak{B}_i = \{B_j \otimes B_{j+i \bmod 2^t} \mid j = 0, \dots, 2^t - 1\} \Rightarrow \bigcup_{i=1}^{2^t} \mathfrak{B}_i = \mathfrak{B} \otimes \mathfrak{B}.$$

Composing Ciphers(II)

We split $\mathfrak{B} \otimes \mathfrak{B} = \{\mathfrak{B}_i\}_{i=1}^{2^t}$ as follows:

$$\mathfrak{B}_i = \{B_j \otimes B_{j+i \pmod{2^t}} \mid j = 0, \dots, 2^t - 1\} \Rightarrow \bigcup_{i=1}^{2^t} \mathfrak{B}_i = \mathfrak{B} \otimes \mathfrak{B}.$$

Choosing a random state in $\mathfrak{B} \otimes \mathfrak{B}$ is equivalent to:

Composing Ciphers(II)

We split $\mathfrak{B} \otimes \mathfrak{B} = \{\mathfrak{B}_i\}_{i=1}^{2^t}$ as follows:

$$\mathfrak{B}_i = \{B_j \otimes B_{j+i \pmod{2^t}} \mid j = 0, \dots, 2^t - 1\} \Rightarrow \bigcup_{i=1}^{2^t} \mathfrak{B}_i = \mathfrak{B} \otimes \mathfrak{B}.$$

Choosing a random state in $\mathfrak{B} \otimes \mathfrak{B}$ is equivalent to:

- Picking $i \in_R \{1, \dots, 2^t\}$ (corresponding to r.v. I),

Composing Ciphers(II)

We split $\mathfrak{B} \otimes \mathfrak{B} = \{\mathfrak{B}_i\}_{i=1}^{2^t}$ as follows:

$$\mathfrak{B}_i = \{B_j \otimes B_{j+i \bmod 2^t} \mid j = 0, \dots, 2^t - 1\} \Rightarrow \bigcup_{i=1}^{2^t} \mathfrak{B}_i = \mathfrak{B} \otimes \mathfrak{B}.$$

Choosing a random state in $\mathfrak{B} \otimes \mathfrak{B}$ is equivalent to:

- Picking $i \in_R \{1, \dots, 2^t\}$ (corresponding to r.v. I),
- Picking a random state in \mathfrak{B}_i (corresponding to r.v. J).

Composing Ciphers(II)

We split $\mathfrak{B} \otimes \mathfrak{B} = \{\mathfrak{B}_i\}_{i=1}^{2^t}$ as follows:

$$\mathfrak{B}_i = \{B_j \otimes B_{j+i \bmod 2^t} \mid j = 0, \dots, 2^t - 1\} \Rightarrow \bigcup_{i=1}^{2^t} \mathfrak{B}_i = \mathfrak{B} \otimes \mathfrak{B}.$$

Choosing a random state in $\mathfrak{B} \otimes \mathfrak{B}$ is equivalent to:

- Picking $i \in_R \{1, \dots, 2^t\}$ (corresponding to r.v. I),
- Picking a random state in \mathfrak{B}_i (corresponding to r.v. J).

Let U be the random variable for the adversary's measurement outcomes:

Composing Ciphers(II)

We split $\mathfrak{B} \otimes \mathfrak{B} = \{\mathfrak{B}_i\}_{i=1}^{2^t}$ as follows:

$$\mathfrak{B}_i = \{B_j \otimes B_{j+i \bmod 2^t} \mid j = 0, \dots, 2^t - 1\} \Rightarrow \bigcup_{i=1}^{2^t} \mathfrak{B}_i = \mathfrak{B} \otimes \mathfrak{B}.$$

Choosing a random state in $\mathfrak{B} \otimes \mathfrak{B}$ is equivalent to:

- Picking $i \in_R \{1, \dots, 2^t\}$ (corresponding to r.v. I),
- Picking a random state in \mathfrak{B}_i (corresponding to r.v. J).

Let U be the random variable for the adversary's measurement outcomes:

$$H(K \mid U) = H((I, J) \mid U) = H(I \mid U) + H(J \mid I, U).$$

Composing Ciphers(III)

$$H((I, J) | U) = H(I | U) + H(J | I, U).$$

Composing Ciphers(III)

$$H((I, J) | U) = H(I | U) + H(J | I, U).$$

- $H(I | U) = t$ since for each \mathfrak{B}_i , a random state produces the same mixture.

Composing Ciphers(III)

$$H((I, J) | U) = H(I | U) + H(J | I, U).$$

- $H(I | U) = t$ since for each \mathfrak{B}_i , a random state produces the same mixture.
- $\mathfrak{B}_i = \{B_j \otimes B_{j+i \bmod 2^t} \mid j = 0, \dots, 2^t - 1\}$ is a set of 2^t mutually unbiased bases in a space of $2n$ qubits:

$$H(J | I = i, U) \geq t + \frac{\text{MES}(\mathfrak{B}_i)}{2^t}.$$

Composing Ciphers(III)

$$H((I, J) | U) = H(I | U) + H(J | I, U).$$

- $H(I | U) = t$ since for each \mathfrak{B}_i , a random state produces the same mixture.
- $\mathfrak{B}_i = \{B_j \otimes B_{j+i \bmod 2^t} \mid j = 0, \dots, 2^t - 1\}$ is a set of 2^t mutually unbiased bases in a space of $2n$ qubits:

$$H(J | I = i, U) \geq t + \frac{\text{MES}(\mathfrak{B}_i)}{2^t}.$$

- We define $M_2(\mathfrak{B}) := \min_i (\text{MES}(\mathfrak{B}_i))$

Composing Ciphers(III)

$$H((I, J) | U) = H(I | U) + H(J | I, U).$$

- $H(I | U) = t$ since for each \mathfrak{B}_i , a random state produces the same mixture.
- $\mathfrak{B}_i = \{B_j \otimes B_{j+i \bmod 2^t} \mid j = 0, \dots, 2^t - 1\}$ is a set of 2^t mutually unbiased bases in a space of $2n$ qubits:

$$H(J | I = i, U) \geq t + \frac{\text{MES}(\mathfrak{B}_i)}{2^t}.$$

- We define $M_2(\mathfrak{B}) := \min_i (\text{MES}(\mathfrak{B}_i))$

Lemma: $C_n^2(\mathfrak{B})$ has key-uncertainty at least $2t + M_2(\mathfrak{B})/2^t$.

Composing Ciphers(III)

$$H((I, J) | U) = H(I | U) + H(J | I, U).$$

- $H(I | U) = t$ since for each \mathfrak{B}_i , a random state produces the same mixture.
- $\mathfrak{B}_i = \{B_j \otimes B_{j+i \bmod 2^t} \mid j = 0, \dots, 2^t - 1\}$ is a set of 2^t mutually unbiased bases in a space of $2n$ qubits:

$$H(J | I = i, U) \geq t + \frac{\text{MES}(\mathfrak{B}_i)}{2^t}.$$

- We define $M_2(\mathfrak{B}) := \min_i (\text{MES}(\mathfrak{B}_i))$

Lemma: $C_n^2(\mathfrak{B})$ has key-uncertainty at least $2t + M_2(\mathfrak{B})/2^t$.

Lemma: $C_n^v(\mathfrak{B})$ has key-uncertainty at least $vt + M_v(\mathfrak{B})/2^t$.

Composing Ciphers(IV)

Theorem: H_n^v has Shannon key-uncertainty $v(n/2 + 1)$.

- Good results for minimal-entropy-sum of any set of mutually unbiased bases with cardinality different from 2 or *close to* $2^n + 1$ are unknown to us.

Composing Ciphers(IV)

Theorem: H_n^v has Shannon key-uncertainty $v(n/2 + 1)$.

- Good results for minimal-entropy-sum of any set of mutually unbiased bases with cardinality different from 2 or *close to* $2^n + 1$ are unknown to us.

Conjecture 2: For any set of 2^n mutually unbiased bases \mathfrak{B} in a space of dimension 2^{vn} , it holds that $\Delta(vn, n) \leq 2^n - vn$.

Composing Ciphers(IV)

Theorem: H_n^v has Shannon key-uncertainty $v(n/2 + 1)$.

- Good results for minimal-entropy-sum of any set of mutually unbiased bases with cardinality different from 2 or *close to* $2^n + 1$ are unknown to us.

Conjecture 2: For any set of 2^n mutually unbiased bases \mathfrak{B} in a space of dimension 2^{vn} , it holds that $\Delta(vn, n) \leq 2^n - vn$.

It follows easily that,

Lemma: Under *Conjecture 2*, W_n^v has Shannon key-uncertainty at least $2vn - 1$ bits.