A Clonable Solution to the Unclonable Encryption Problem



Prabhanjan Ananth



Seyoon Ragavan



Amit Sahai

Charles River Crypto Day

October 2, 2026

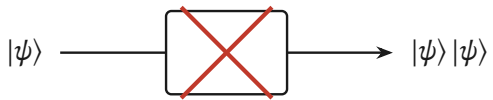
Roadmap

- Part I: The Unclonable Encryption Problem
- Part II: The Proof
- Part III: Follow-Up and Related Works

Roadmap

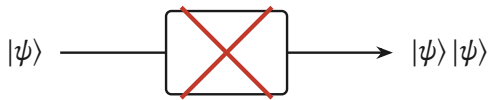
- Part I: The Unclonable Encryption Problem
- Part II: The Proof
- Part III: Follow-Up and Related Works

The No-Cloning Theorem [WZ82]



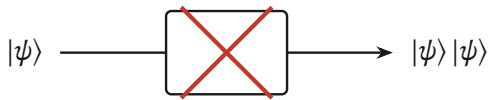
- Informally: quantum information cannot be copied and pasted

The No-Cloning Theorem [WZ82]



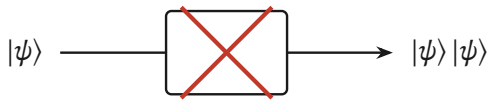
- Informally: quantum information cannot be copied and pasted
- Robust variant [Wer98]: it is not even possible to generate something close to $|\psi\rangle|\psi\rangle$ (in trace distance)

The No-Cloning Theorem [WZ82]



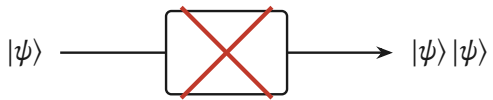
- Informally: quantum information cannot be copied and pasted
- Robust variant [Wer98]: it is not even possible to generate something close to $|\psi\rangle|\psi\rangle$ (in trace distance)
- Provides hope for unclonable cryptography: applications where we want to safeguard against duplication of information

The No-Cloning Theorem [WZ82]



- Informally: quantum information cannot be copied and pasted
- Robust variant [Wer98]: it is not even possible to generate something close to $|\psi\rangle|\psi\rangle$ (in trace distance)
- Provides hope for unclonable cryptography: applications where we want to safeguard against duplication of information
  - However, it is rarely sufficient

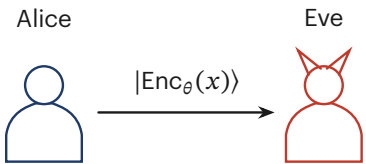
The No-Cloning Theorem [WZ82]



- Informally: quantum information cannot be copied and pasted
- Robust variant [Wer98]: it is not even possible to generate something close to $|\psi\rangle|\psi\rangle$ (in trace distance)
- Provides hope for unclonable cryptography: applications where we want to safeguard against duplication of information
  - However, it is rarely sufficient
  - Want "useful" variants (even stronger than robust): it is not even possible for both states to have "some property" in common with $|\psi\rangle$

Unclonable Encryption [Got03,BL20]

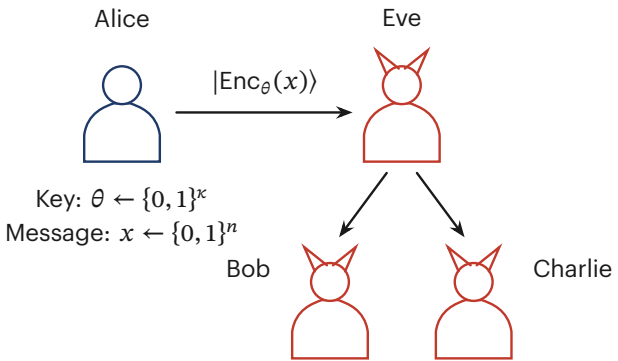
Goal: a ciphertext that cannot be split in two



1. Alice samples a key θ and sends $|\mathrm{Enc}_\theta(x)\rangle$ to Eve

Unclonable Encryption [Got03,BL20]

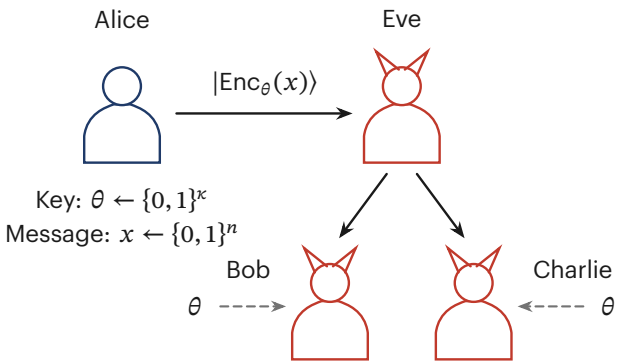
Goal: a ciphertext that cannot be split in two



1. Alice samples a key θ and sends $|\mathrm{Enc}_\theta(x)\rangle$ to Eve
2. Eve sends some bipartite state to Bob and Charlie

Unclonable Encryption [Got03,BL20]

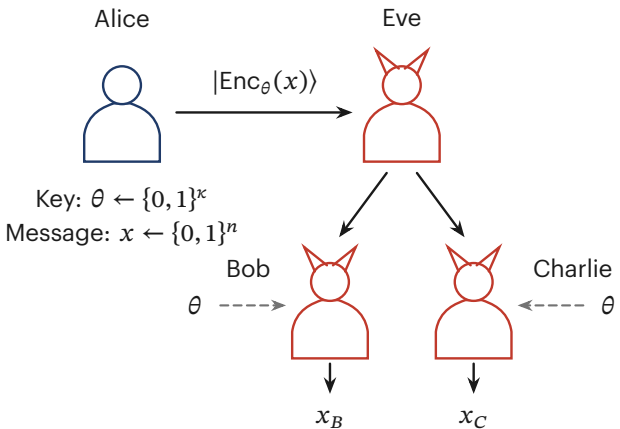
Goal: a ciphertext that cannot be split in two



1. Alice samples a key θ and sends $|\mathrm{Enc}_\theta(x)\rangle$ to Eve
2. Eve sends some bipartite state to Bob and Charlie
3. Bob and Charlie get access to θ

Unclonable Encryption [Got03,BL20]

Goal: a ciphertext that cannot be split in two



1. Alice samples a key θ and sends $|\mathrm{Enc}_\theta(x)\rangle$ to Eve
2. Eve sends some bipartite state to Bob and Charlie
3. Bob and Charlie get access to θ
4. They guess x_B, x_C and win if both guesses are correct

Search Security

Definition (Search security)

For every splitting strategy and every pair of decoders,

$$\Pr[x_B = x_C = x] \leq \mathsf{negl}(n, \varkappa).$$

Search Security

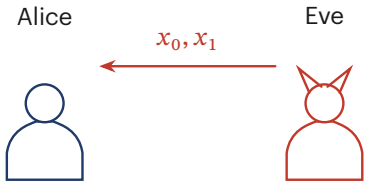
Definition (Search security)

For every splitting strategy and every pair of decoders,

$$\Pr[x_B = x_C = x] \leq \mathrm{negl}(n, \varkappa).$$

- Trivial strategy: forward the ciphertext to Bob
- Bob can decrypt but Charlie has to guess randomly ⇒ success probability 2^{-n}

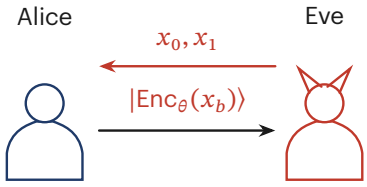
The Ideal Notion: IND Security [BL20]



Key: $\theta \leftarrow \{0,1\}^\kappa$

1. Eve sends two challenge messages x_0, x_1 to Alice

The Ideal Notion: IND Security [BL20]

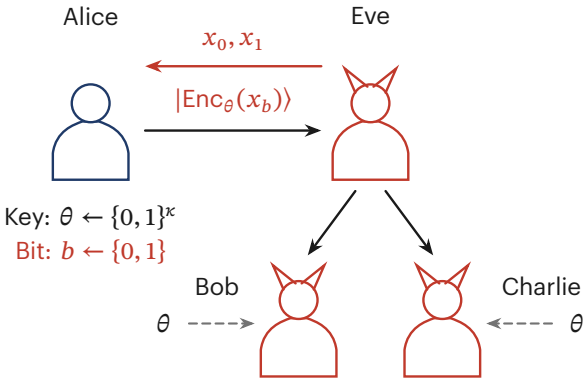


Key: $\theta \leftarrow \{0,1\}^\kappa$

Bit: $b \leftarrow \{0,1\}$

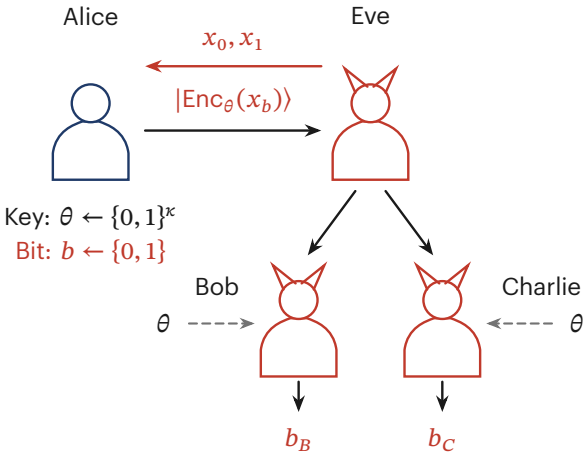
1. Eve sends two challenge messages x_0, x_1 to Alice
2. Alice encrypts one of them at random and sends it back

The Ideal Notion: IND Security [BL20]



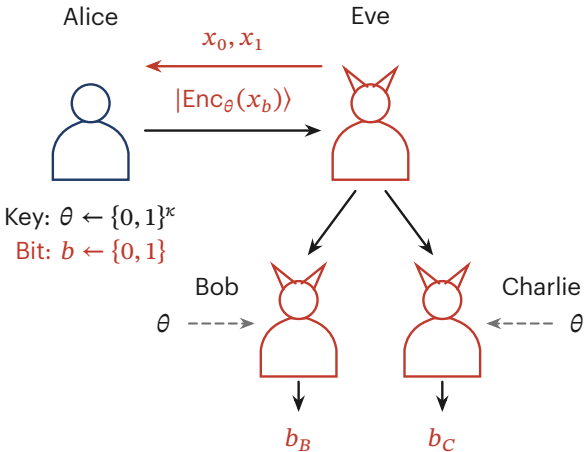
1. Eve sends two challenge messages x_0, x_1 to Alice
2. Alice encrypts one of them at random and sends it back
3. As before: split, then Bob and Charlie get θ

The Ideal Notion: IND Security [BL20]



1. Eve sends two challenge messages x_0, x_1 to Alice
2. Alice encrypts one of them at random and sends it back
3. As before: split, then Bob and Charlie get θ
4. They guess b_B, b_C; want $\Pr[b_B = b_C = b] \leq \frac{1}{2} + \mathrm{negl}(\kappa)$

The Ideal Notion: IND Security [BL20]



1. Eve sends two challenge messages x_0, x_1 to Alice
2. Alice encrypts one of them at random and sends it back
3. As before: split, then Bob and Charlie get θ
4. They guess b_B, b_C; want $\Pr[b_B = b_C = b] \leq \frac{1}{2} + \mathrm{negl}(\kappa)$

Central single-bit case:
$x_0 = 0$, $x_1 = 1$
Necessary, and sufficient assuming PRUs [BG26a]

Unclonable Encryption Through the Years

As of June 2026 (ancient history)

	Security	Model	Other caveats
[BL20]	search	plain	

Unclonable Encryption Through the Years

As of June 2026 (ancient history)

	Security	Model	Other caveats
[BL20]	search	plain	
[AKL+22]	IND	ROM	

ROM: the random oracle model, with quantum query access

Unclonable Encryption Through the Years

As of June 2026 (ancient history)

	Security	Model	Other caveats
[BL20]	search	plain	
[AKL+22]	IND	ROM	
[AKY25]	IND	plain	quantum decryption keys

Unclonable Encryption Through the Years

As of June 2026 (ancient history)

	Security	Model	Other caveats
[BL20]	search	plain	
[AKL+22]	IND	ROM	
[AKY25]	IND	plain	quantum decryption keys
[BC26]	IND	plain	$1/\mathrm{poly}(\kappa)$ security loss

Unclonable Encryption Through the Years

As of June 2026 (ancient history)

	Security	Model	Other caveats
[BL20]	search	plain	
[AKL+22]	IND	ROM	
[AKY25]	IND	plain	quantum decryption keys
[BC26]	IND	plain	$1/\mathrm{poly}(\kappa)$ security loss
[BBC26a]	IND	plain	inefficient Enc/Dec

Unclonable Encryption Through the Years

As of June 2026 (ancient history)

	Security	Model	Other caveats
[BL20]	search	plain	
[AKL+22]	IND	ROM	
[AKY25]	IND	plain	quantum decryption keys
[BC26]	IND	plain	$1/\mathrm{poly}(\kappa)$ security loss
[BBC26a]	IND	plain	inefficient Enc/Dec
[BG26b]	IND	QHROM	

QHROM: the quantum Haar random oracle model

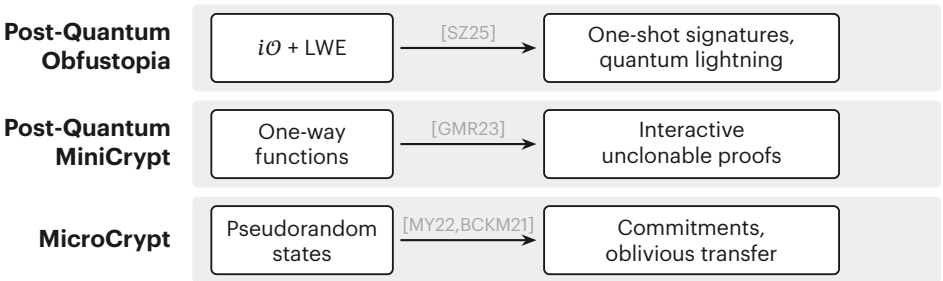
Unclonable Encryption Through the Years

As of June 2026 (ancient history)

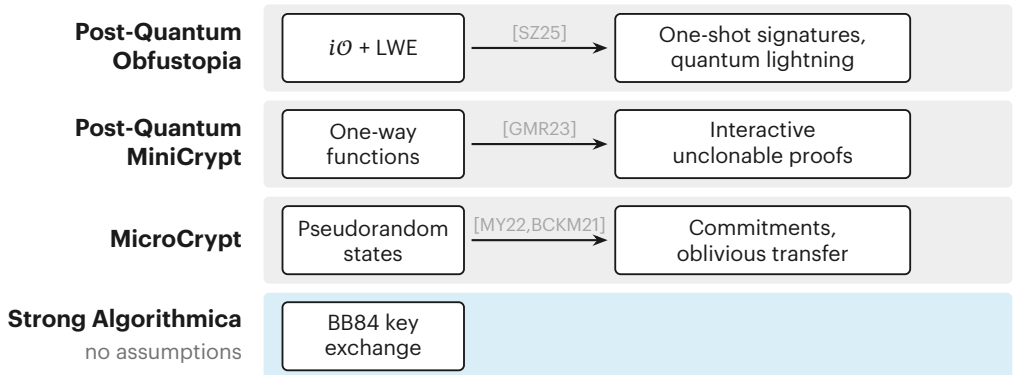
	Security	Model	Other caveats
[BL20]	search	plain	
[AKL+22]	IND	ROM	
[AKY25]	IND	plain	quantum decryption keys
[BC26]	IND	plain	$1/\mathrm{poly}(\kappa)$ security loss
[BBC26a]	IND	plain	inefficient Enc/Dec
[BG26b]	IND	QHROM	

Lower bound [BCR25]:
no scheme with κ-qubit ciphertexts keeps both receivers below $1/2 + \Omega(2^{-\kappa/2})$.

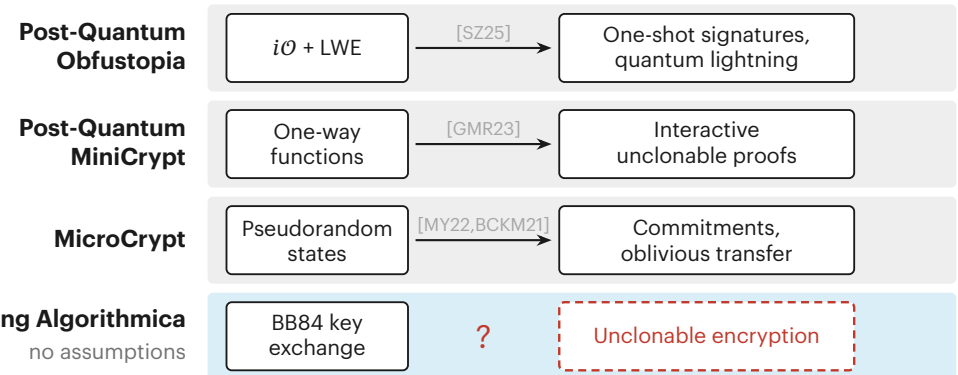
Where Unclonable Encryption Should Live



Where Unclonable Encryption Should Live

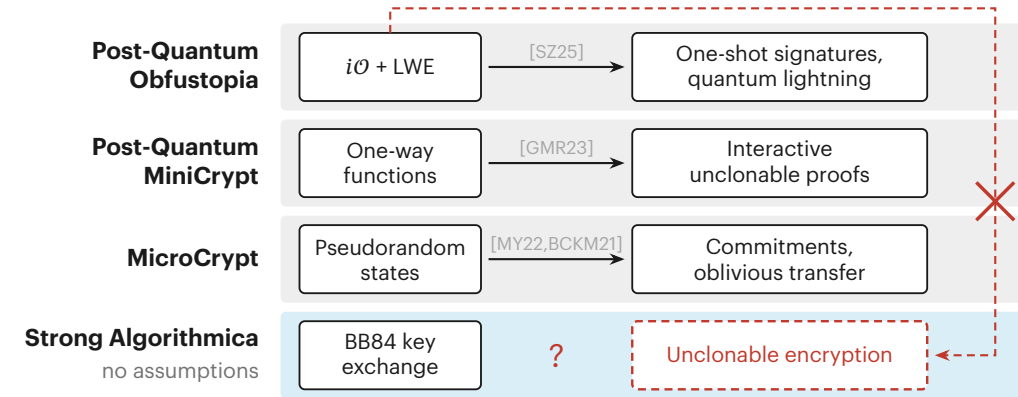


Where Unclonable Encryption Should Live



Unclonable encryption: plausibly does not need any hardness at all

Where Unclonable Encryption Should Live



Unclonable encryption: plausibly does not need any hardness at all

And yet, as of June 2026, no construction anywhere — not even from $i\mathcal{O}$

Quantum Preliminaries

- Classical bit: 0 or 1

Quantum Preliminaries

- Classical bit: 0 or 1
- Qubit: $|0\rangle$, $|1\rangle$, and any linear combination $a|0\rangle + b|1\rangle$ $(a, b \in \mathbb{C})$
  - Concatenating qubits corresponds to tensoring the vector spaces $\Rightarrow$ denote n-qubit states by $|\psi\rangle \in \mathbb{C}^{2^n}$

Quantum Preliminaries

- Classical bit: 0 or 1
- Qubit: $|0\rangle$, $|1\rangle$, and any linear combination $a|0\rangle + b|1\rangle$ ($a, b \in \mathbb{C}$)
  - Concatenating qubits corresponds to tensoring the vector spaces $\Rightarrow$ denote n-qubit states by $|\psi\rangle \in \mathbb{C}^{2^n}$
- Can perfectly distinguish any two orthogonal states
  - Example 1 (Z basis): $\{|0\rangle, |1\rangle\} = \{(1,0), (0,1)\}$
  - Example 2 (X basis): $\{|+\rangle, |-\rangle\} = \{|0\rangle + |1\rangle, |0\rangle - |1\rangle\} = \{(1,1), (1,-1)\}$

Quantum Preliminaries

- Classical bit: 0 or 1
- Qubit: $|0\rangle$, $|1\rangle$, and any linear combination $a|0\rangle + b|1\rangle$ ($a, b \in \mathbb{C}$)
  - Concatenating qubits corresponds to tensoring the vector spaces $\Rightarrow$ denote n-qubit states by $|\psi\rangle \in \mathbb{C}^{2^n}$
- Can perfectly distinguish any two orthogonal states
  - Example 1 (Z basis): $\{|0\rangle, |1\rangle\} = \{(1,0), (0,1)\}$
  - Example 2 (X basis): $\{|+\rangle, |-\rangle\} = \{|0\rangle + |1\rangle, |0\rangle - |1\rangle\} = \{(1,1), (1,-1)\}$
- Can encode a classical bit in either the $\{|0\rangle, |1\rangle\}$ or the $\{|+\rangle, |-\rangle\}$ basis
  - Without knowing the basis, hard to recover the encoded classical bit
  - Also hard to clone

Quantum Preliminaries: Pauli Matrices

- The single-qubit Paulis: X, Y, Z

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Quantum Preliminaries: Pauli Matrices

- The single-qubit Paulis: X, Y, Z
- Each is Hermitian and squares to I, so its eigenvalues are ± 1

	eigenstates		
	$+1$	-1	
Z	$\|0\rangle$	$\|1\rangle$	the Z basis
X	$\|+\rangle$	$\|-\rangle$	the X basis
Y	$\|+i\rangle$	$\|-i\rangle$	the Y basis

Quantum Preliminaries: Pauli Matrices

- The single-qubit Paulis: X, Y, Z
- Each is Hermitian and squares to I, so its eigenvalues are ± 1

	eigenstates		
	$+1$	-1	
Z	$\|0\rangle$	$\|1\rangle$	the Z basis
X	$\|+\rangle$	$\|-\rangle$	the X basis
Y	$\|+i\rangle$	$\|-i\rangle$	the Y basis

- An n-qubit Pauli is a tensor product $P = P_1 \otimes \cdots \otimes P_n$, and there are 4^n of them

Quantum Preliminaries: Pauli Matrices

- The single-qubit Paulis: X, Y, Z
- Each is Hermitian and squares to I, so its eigenvalues are ± 1

	eigenstates		
	$+1$	-1	
Z	$\|0\rangle$	$\|1\rangle$	the Z basis
X	$\|+\rangle$	$\|-\rangle$	the X basis
Y	$\|+i\rangle$	$\|-i\rangle$	the Y basis

- An n-qubit Pauli is a tensor product $P = P_1 \otimes \cdots \otimes P_n$, and there are 4^n of them
- Any two Paulis either commute or anticommute: $PQ \in \{QP, -QP\}$

Quantum Preliminaries: Pauli Matrices

- The single-qubit Paulis: X, Y, Z
- Each is Hermitian and squares to I, so its eigenvalues are ± 1

	eigenstates		
	$+1$	-1	
Z	$\|0\rangle$	$\|1\rangle$	the Z basis
X	$\|+\rangle$	$\|-\rangle$	the X basis
Y	$\|+i\rangle$	$\|-i\rangle$	the Y basis

- An n-qubit Pauli is a tensor product $P = P_1 \otimes \cdots \otimes P_n$, and there are 4^n of them
- Any two Paulis either commute or anticommute: $PQ \in \{QP, -QP\}$
- Every $P \neq I^{\otimes n}$ splits $\mathbb{C}^{2^n}$ into $+1$ and -1 eigenspaces, each of dimension 2^{n-1}

Approach: Pauli Eigenstates

Proposed by [Bot+24]

- Key: a *non-identity Pauli* P on κ qubits

Approach: Pauli Eigenstates

Proposed by [Bot+24]

- Key: a *non-identity Pauli* P on κ qubits
- Enc($a \in \{0,1\}$): send a random $(-1)^a$ eigenstate of P

Approach: Pauli Eigenstates

Proposed by [Bot+24]

- Key: a *non-identity Pauli* P on κ qubits
- Enc($a \in \{0,1\}$): send a random $(-1)^a$ eigenstate of P
- Decrypt: measure P

Unclonable Encryption from Pauli Eigenstates [ARS26]

Informal theorem statement

The Pauli eigenstate approach of [Bot+24] gives information-theoretic unclonable encryption for one bit, with efficient encryption and decryption. With κ-qubit ciphertexts,

$$\Pr[b_B = b_C = b] \leq \frac{1}{2} + O(2^{-\kappa/2}).$$

Unclonable Encryption from Pauli Eigenstates [ARS26]

Informal theorem statement

The Pauli eigenstate approach of [Bot+24] gives information-theoretic unclonable encryption for one bit, with efficient encryption and decryption. With κ-qubit ciphertexts,

$$\Pr[b_B = b_C = b] \leq \frac{1}{2} + O(2^{-\kappa/2}).$$

- Optimal for κ-qubit ciphertexts [BCR25]

Unclonable Encryption from Pauli Eigenstates [ARS26]

Informal theorem statement

The Pauli eigenstate approach of [Bot+24] gives information-theoretic unclonable encryption for one bit, with efficient encryption and decryption. With κ-qubit ciphertexts,

$$\Pr[b_B = b_C = b] \leq \frac{1}{2} + O(2^{-\kappa/2}).$$

- Optimal for κ-qubit ciphertexts [BCR25]
- Found by GPT-5.6 Sol Ultra



Follow-Up Work

Bhattacharyya–Broadbent–Culf [BBC26b]

Extends the [ARS26] construction to messages of arbitrary length, while remaining information-theoretic

Follow-Up Work

Bhattacharyya–Broadbent–Culf [BBC26b]

Extends the [ARS26] construction to messages of arbitrary length, while remaining information-theoretic

Coladangelo–Liu–Xie [CLX26] and Ananth [Ana26]

Proves that a different approach based on Goldreich–Levin is also information-theoretically secure

Follow-Up Work

Bhattacharyya–Broadbent–Culf [BBC26b]

Extends the [ARS26] construction to messages of arbitrary length, while remaining information-theoretic

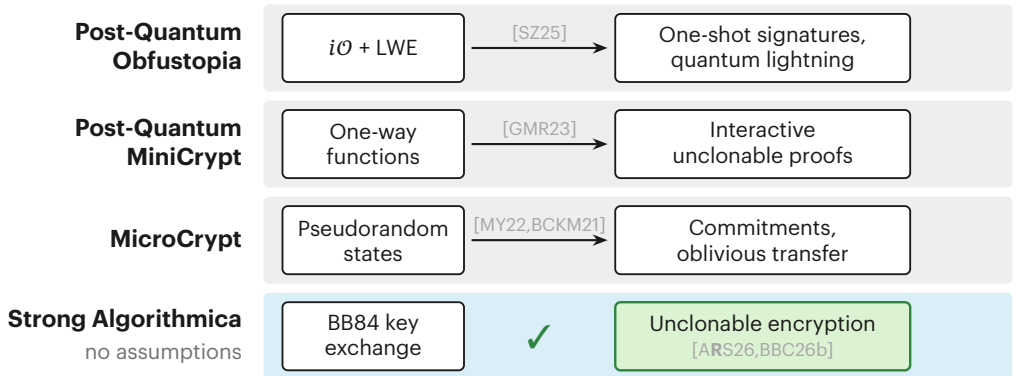
Coladangelo–Liu–Xie [CLX26] **and Ananth** [Ana26]

Proves that a different approach based on Goldreich–Levin is also information-theoretically secure

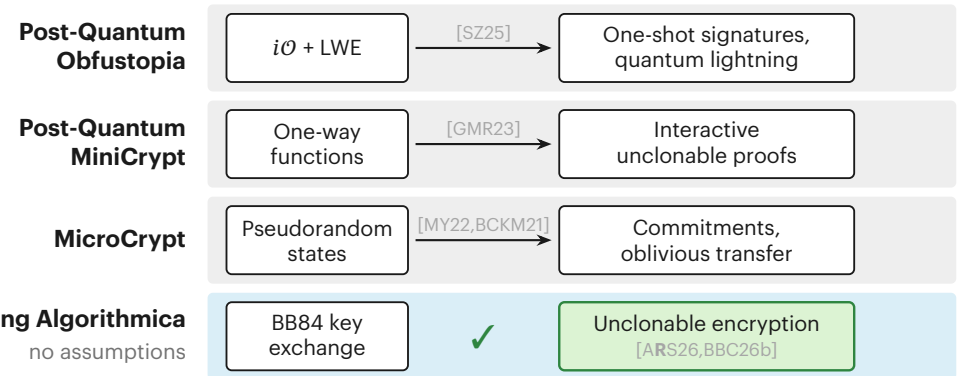
Botteron–Designolle–Fawzi [BDF26]

Further results on the Pauli eigenstate template, in more generality

Where Unclonable Encryption Lives Now



Where Unclonable Encryption Lives Now



Both candidate approaches work

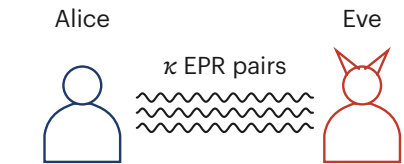
Pauli eigenstates [ARS26] and Goldreich–Levin bootstrapping [CLX26,Ana26]

Roadmap

- Part I: The Unclonable Encryption Problem
- ➜ Part II: The Proof
- Part III: Follow-Up and Related Works

Step 1: Ricochet Transformation [BL20]

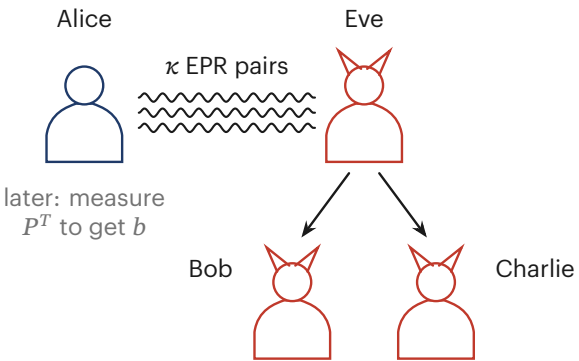
Standard step: from UE to monogamy-of-entanglement



1. Alice sends Eve half of κ EPR pairs

Step 1: Ricochet Transformation [BL20]

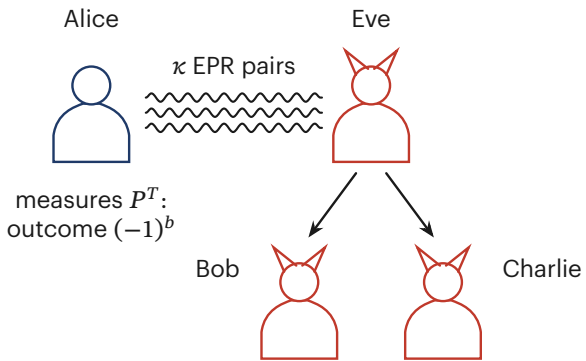
Standard step: from UE to monogamy-of-entanglement



1. Alice sends Eve half of κ EPR pairs
2. Eve splits those qubits between Bob and Charlie

Step 1: Ricochet Transformation [BL20]

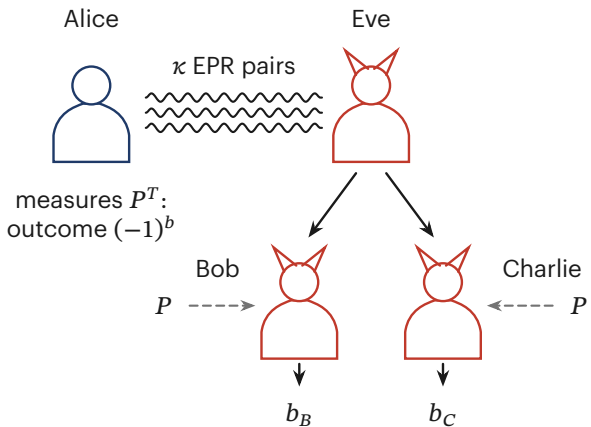
Standard step: from UE to monogamy-of-entanglement



1. Alice sends Eve half of κ EPR pairs
2. Eve splits those qubits between Bob and Charlie
3. Alice samples P and measures P^T on her half, getting $(-1)^b$ for a uniform bit b

Step 1: Ricochet Transformation [BL20]

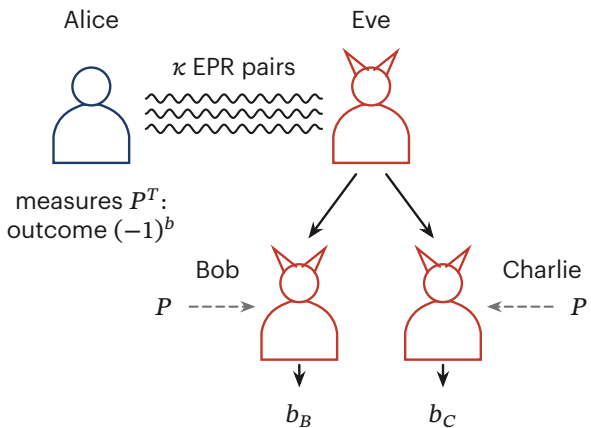
Standard step: from UE to monogamy-of-entanglement



1. Alice sends Eve half of κ EPR pairs
2. Eve splits those qubits between Bob and Charlie
3. Alice samples P and measures P^T on her half, getting $(-1)^b$ for a uniform bit b
4. Bob and Charlie get P and guess b

Step 1: Ricochet Transformation [BL20]

Standard step: from UE to monogamy-of-entanglement

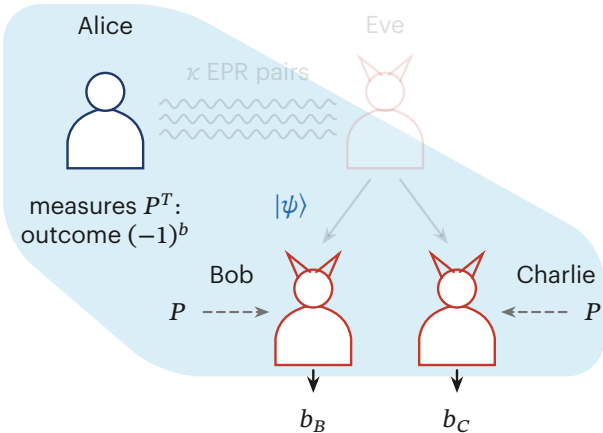


1. Alice sends Eve half of κ EPR pairs
2. Eve splits those qubits between Bob and Charlie
3. Alice samples P and measures P^T on her half, getting $(-1)^b$ for a uniform bit b
4. Bob and Charlie get P and guess b

Same game: outcome $(-1)^b$ leaves Eve's half looking exactly like a ciphertext for b

Step 1: Ricochet Transformation [BL20]

Standard step: from UE to monogamy-of-entanglement

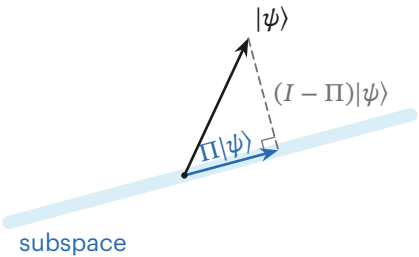


1. Alice sends Eve half of κ EPR pairs
2. Eve splits those qubits between Bob and Charlie
3. Alice samples P and measures P^T on her half, getting $(-1)^b$ for a uniform bit b
4. Bob and Charlie get P and guess b

Same game: outcome $(-1)^b$ leaves Eve's half looking exactly like a ciphertext for b

Step 2: Three Operators

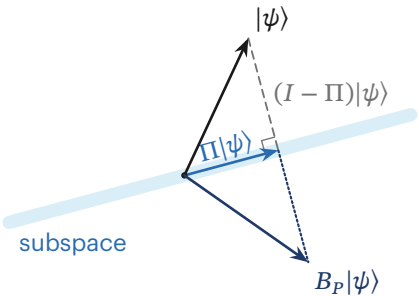
- On key P, Bob and Charlie each project onto a subspace, and output 0 if the projection succeeds and 1 if it fails



$$\Pr[0] = \|\Pi|\psi\rangle\|^2$$
$$\Pr[1] = \|(I-\Pi)|\psi\rangle\|^2$$

Step 2: Three Operators

- On key P, Bob and Charlie each project onto a subspace, and output 0 if the projection succeeds and 1 if it fails



$\Pr[0] = \|\Pi|\psi\rangle\|^2$
$\Pr[1] = \|(I-\Pi)|\psi\rangle\|^2$

$B_P := 2\Pi - I$ is the reflection about the subspace

So $\langle\psi|B_P|\psi\rangle = \Pr[0] - \Pr[1]$, and likewise C_P for Charlie

Step 2: Three Operators

- On key P, Bob and Charlie each project onto a subspace, and output 0 if the projection succeeds and 1 if it fails

$$\mathsf{E}_B = \mathbb{E}_P\left[P^T \otimes B_P \otimes I\right] \qquad \langle\psi|\mathsf{E}_B|\psi\rangle = 2\Pr[\text{Bob correct}] - 1$$
$$\mathsf{E}_C = \mathbb{E}_P\left[P^T \otimes I \otimes C_P\right] \qquad \langle\psi|\mathsf{E}_C|\psi\rangle = 2\Pr[\text{Charlie correct}] - 1$$

Step 2: Three Operators

- On key P, Bob and Charlie each project onto a subspace, and output 0 if the projection succeeds and 1 if it fails

$$\mathsf{E}_B = \mathbb{E}_P\left[P^T \otimes B_P \otimes I\right] \qquad \langle\psi|\mathsf{E}_B|\psi\rangle = 2\Pr[\text{Bob correct}] - 1$$
$$\mathsf{E}_C = \mathbb{E}_P\left[P^T \otimes I \otimes C_P\right] \qquad \langle\psi|\mathsf{E}_C|\psi\rangle = 2\Pr[\text{Charlie correct}] - 1$$
$$\mathsf{D} = I - \mathbb{E}_P\left[I \otimes B_P \otimes C_P\right] \qquad \langle\psi|\mathsf{D}|\psi\rangle = 2\Pr[\text{they disagree}]$$

Step 2: Three Operators

- On key P, Bob and Charlie each project onto a subspace, and output 0 if the projection succeeds and 1 if it fails

$$\mathsf{E}_B = \mathbb{E}_P\left[P^T \otimes B_P \otimes I\right] \qquad \langle\psi|\mathsf{E}_B|\psi\rangle = 2\Pr[\text{Bob correct}] - 1$$
$$\mathsf{E}_C = \mathbb{E}_P\left[P^T \otimes I \otimes C_P\right] \qquad \langle\psi|\mathsf{E}_C|\psi\rangle = 2\Pr[\text{Charlie correct}] - 1$$
$$\mathsf{D} = I - \mathbb{E}_P\left[I \otimes B_P \otimes C_P\right] \qquad \langle\psi|\mathsf{D}|\psi\rangle = 2\Pr[\text{they disagree}]$$

$$\text{both correct} = \frac{1}{2}(\text{Bob correct} + \text{Charlie correct} - \text{disagree})$$

Step 2: Three Operators

- On key P, Bob and Charlie each project onto a subspace, and output 0 if the projection succeeds and 1 if it fails

$$\mathsf{E}_B = \mathbb{E}_P\left[P^T \otimes B_P \otimes I\right] \qquad \langle\psi|\mathsf{E}_B|\psi\rangle = 2\Pr[\text{Bob correct}] - 1$$
$$\mathsf{E}_C = \mathbb{E}_P\left[P^T \otimes I \otimes C_P\right] \qquad \langle\psi|\mathsf{E}_C|\psi\rangle = 2\Pr[\text{Charlie correct}] - 1$$
$$\mathsf{D} = I - \mathbb{E}_P\left[I \otimes B_P \otimes C_P\right] \qquad \langle\psi|\mathsf{D}|\psi\rangle = 2\Pr[\text{they disagree}]$$

$$\text{both correct} = \tfrac{1}{2}(\text{Bob correct} + \text{Charlie correct} - \text{disagree})$$

$$\Pr[b_B = b_C = b] = \frac{1}{2}\Big(1 + \langle\psi|\underbrace{\tfrac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})}_{\mathsf{G}}|\psi\rangle\Big)$$

Step 2: Three Operators

- On key P, Bob and Charlie each project onto a subspace, and output 0 if the projection succeeds and 1 if it fails

$$\mathsf{E}_B = \mathbb{E}_P\left[P^T \otimes B_P \otimes I\right] \qquad \langle\psi|\mathsf{E}_B|\psi\rangle = 2\Pr[\text{Bob correct}] - 1$$
$$\mathsf{E}_C = \mathbb{E}_P\left[P^T \otimes I \otimes C_P\right] \qquad \langle\psi|\mathsf{E}_C|\psi\rangle = 2\Pr[\text{Charlie correct}] - 1$$
$$\mathsf{D} = I - \mathbb{E}_P\left[I \otimes B_P \otimes C_P\right] \qquad \langle\psi|\mathsf{D}|\psi\rangle = 2\Pr[\text{they disagree}]$$

$$\text{both correct} = \tfrac{1}{2}(\text{Bob correct} + \text{Charlie correct} - \text{disagree})$$

$$\Pr[b_B = b_C = b] = \tfrac{1}{2}\left(1 + \langle\psi|\underbrace{\tfrac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})}_{\mathsf{G}}|\psi\rangle\right) \le \tfrac{1}{2}\left(1 + \lambda_{\max}(\mathsf{G})\right)$$

Step 2: Three Operators

- On key P, Bob and Charlie each project onto a subspace, and output 0 if the projection succeeds and 1 if it fails

$$\mathsf{E}_B = \mathbb{E}_P\left[P^T \otimes B_P \otimes I\right] \qquad \langle\psi|\mathsf{E}_B|\psi\rangle = 2\Pr[\text{Bob correct}] - 1$$
$$\mathsf{E}_C = \mathbb{E}_P\left[P^T \otimes I \otimes C_P\right] \qquad \langle\psi|\mathsf{E}_C|\psi\rangle = 2\Pr[\text{Charlie correct}] - 1$$
$$\mathsf{D} = I - \mathbb{E}_P\left[I \otimes B_P \otimes C_P\right] \qquad \langle\psi|\mathsf{D}|\psi\rangle = 2\Pr[\text{they disagree}]$$

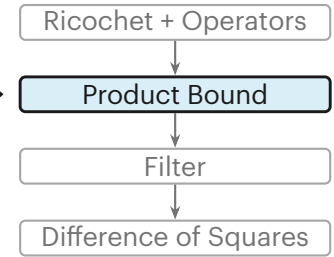
$$\text{both correct} = \tfrac{1}{2}(\text{Bob correct} + \text{Charlie correct} - \text{disagree})$$

$$\Pr[b_B = b_C = b] = \tfrac{1}{2}\Big(1 + \langle\psi|\underbrace{\tfrac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})}_{\mathsf{G}}|\psi\rangle\Big) \le \tfrac{1}{2}\big(1 + \lambda_{\max}(\mathsf{G})\big)$$

To show: $\lambda_{\max}(\mathsf{G}) \le \sqrt{d/K} = \Theta(2^{-\kappa/2})$, where $d = 2^\kappa$ and $K = 4^\kappa - 1$

Proof Roadmap

Goal: $t = \lambda_{\max}(\mathsf{G}) \le \sqrt{d/K}$



$\Pr[b_B = b_C = b] \le \frac{1}{2} + \frac{1}{2}\lambda_{\max}(\mathsf{G})$, where $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$
disagreement: $\mathsf{D} = I - \mathbb{E}_P[I \otimes B_P \otimes C_P]$

$\|\mathsf{E}_B\mathsf{E}_C\| \le d/K$
via Pauli (anti)commutation [Rag26] or orthogonality [AS26]

$\|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\| \le d/K$, where $\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$
via the Taylor expansion of F

$t^2 \le \|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\|$. Combine with the above ⇒ done!

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · $d = 2^\kappa$, $K = 4^\kappa - 1$
D: disagreement · F: the filter · G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Step 3: The Product Bound

Goal: $\|\mathsf{E}_B\mathsf{E}_C\| \leq d/K$ for any decoders

Proof A [Rag26]

- Multiply out: $\mathsf{E}_B\mathsf{E}_C = \frac{1}{K^2}\sum_{P,Q} P^T Q^T \otimes B_P \otimes C_Q$

$d = 2^\kappa$: dimension · $K = 4^\kappa - 1$: number of keys
$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success

Step 3: The Product Bound

Goal: $\|\mathsf{E}_B\mathsf{E}_C\| \leq d/K$ for any decoders

Proof A [Rag26]

- Multiply out: $\mathsf{E}_B\mathsf{E}_C = \frac{1}{K^2}\sum_{P,Q} P^T Q^T \otimes B_P \otimes C_Q$
- Swapping the Paulis costs a sign: $P^T Q^T = s_{PQ}\, Q^T P^T$ with $s_{PQ} = \pm 1$, so

$$\mathsf{E}_B\mathsf{E}_C = \frac{1}{K^2}\sum_{P,Q} s_{PQ} \underbrace{(Q^T \otimes I \otimes C_Q)}_{\text{Charlie's piece}} \underbrace{(P^T \otimes B_P \otimes I)}_{\text{Bob's piece}}$$

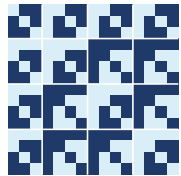
$d = 2^\kappa$: dimension · $K = 4^\kappa - 1$: number of keys
$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success

Step 3: Proof A in Block Matrices

signs s_{PQ}, each times I

Charlie's pieces
$Q^T \otimes I \otimes C_Q$

$$\mathsf{E}_B\mathsf{E}_C = \frac{1}{K^2}$$

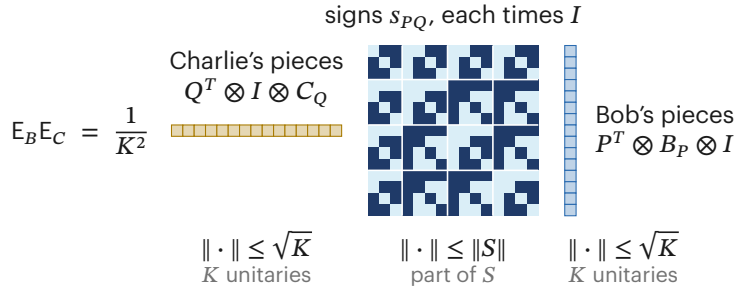




Bob's pieces
$P^T \otimes B_P \otimes I$

$d = 2^\kappa$: dimension · $K = 4^\kappa - 1$: number of keys · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success

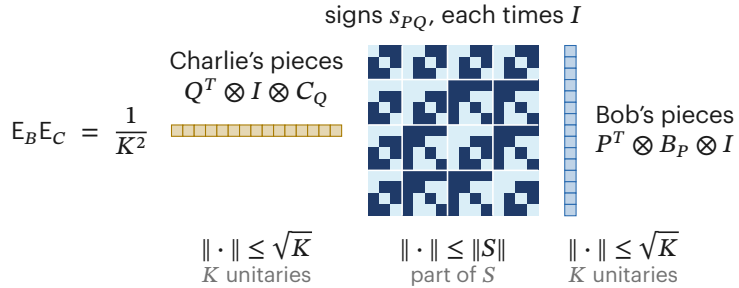
Step 3: Proof A in Block Matrices



S: the signs s_{PQ} for all 4^κ Paulis P, Q, identity included

$d = 2^\kappa$: dimension · $K = 4^\kappa - 1$: number of keys · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success

Step 3: Proof A in Block Matrices



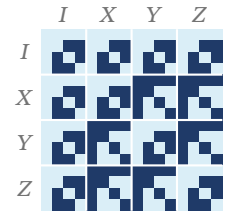
S: the signs s_{PQ} for all 4^κ Paulis P, Q, identity included

$\|\mathsf{E}_B\mathsf{E}_C\| \le \frac{1}{K^2} \cdot \sqrt{K} \cdot \|S\| \cdot \sqrt{K} = \|S\|/K$: it all comes down to $\|S\|$

$d = 2^\kappa$: dimension · $K = 4^\kappa - 1$: number of keys · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success

Step 3: The Sign Matrix

- The rows of S are orthogonal

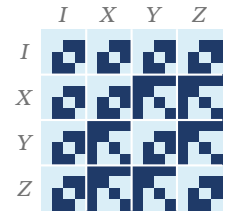


$\kappa = 2$: dark where $s_{PQ} = -1$
A column-permuted Hadamard matrix

$d = 2^\kappa$: dimension · $K = 4^\kappa - 1$: number of keys · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success

Step 3: The Sign Matrix

- The rows of S are orthogonal
- So $\|S\| = 2^\kappa$

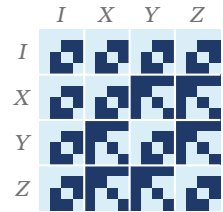


$\kappa = 2$: dark where $s_{PQ} = -1$
A column-permuted Hadamard matrix

$d = 2^\kappa$: dimension · $K = 4^\kappa - 1$: number of keys · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success

Step 3: The Sign Matrix

- The rows of S are orthogonal
- So $\|S\| = 2^\kappa$
  - Without the commutation trick, S would be all 1s, and then $\|S\| = 4^\kappa$

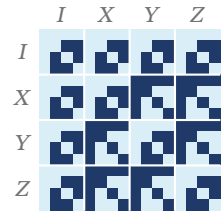


$\kappa = 2$: dark where $s_{PQ} = -1$
A column-permuted Hadamard matrix

$d = 2^\kappa$: dimension · $K = 4^\kappa - 1$: number of keys · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success

Step 3: The Sign Matrix

- The rows of S are orthogonal
- So $\|S\| = 2^\kappa$
  - Without the commutation trick, S would be all 1s, and then $\|S\| = 4^\kappa$
- Hence $\|\mathsf{E}_B\mathsf{E}_C\| \leq \|S\|/K = 2^\kappa/K = d/K$

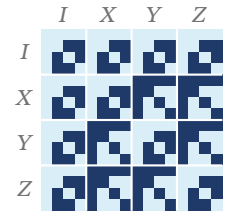


$\kappa = 2$: dark where $s_{PQ} = -1$
A column-permuted Hadamard matrix

$d = 2^\kappa$: dimension · $K = 4^\kappa - 1$: number of keys · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success

Step 3: The Sign Matrix

- The rows of S are orthogonal
- So $\|S\| = 2^\kappa$
  - Without the commutation trick, S would be all 1s, and then $\|S\| = 4^\kappa$
- Hence $\|\mathsf{E}_B \mathsf{E}_C\| \leq \|S\|/K = 2^\kappa/K = d/K$



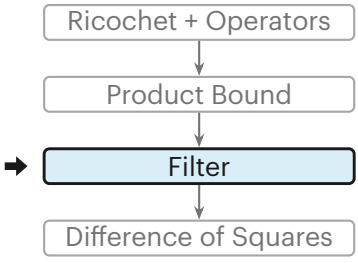
$\kappa = 2$: dark where $s_{PQ} = -1$
A column-permuted Hadamard matrix

Proof B idea [AS26]**:** use Pauli orthogonality ($\mathrm{Tr}[PQ] = d\,\delta_{PQ}$) together with a Cauchy–Schwarz lemma

$d = 2^\kappa$: dimension · $K = 4^\kappa - 1$: number of keys · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success

Proof Roadmap

Goal: $t = \lambda_{\max}(\mathsf{G}) \le \sqrt{d/K}$



$\Pr[b_B = b_C = b] \le \frac{1}{2} + \frac{1}{2}\lambda_{\max}(\mathsf{G})$, where $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$
disagreement: $\mathsf{D} = I - \mathbb{E}_P[I \otimes B_P \otimes C_P]$

$\|\mathsf{E}_B\mathsf{E}_C\| \le d/K$
via Pauli (anti)commutation [Rag26] or orthogonality [AS26]

$\|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\| \le d/K$, where $\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$
via the Taylor expansion of F

$t^2 \le \|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\|$. Combine with the above ⇒ done!

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · $d = 2^\kappa$, $K = 4^\kappa - 1$
D: disagreement · F: the filter · G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Aside: A Cautionary Tale

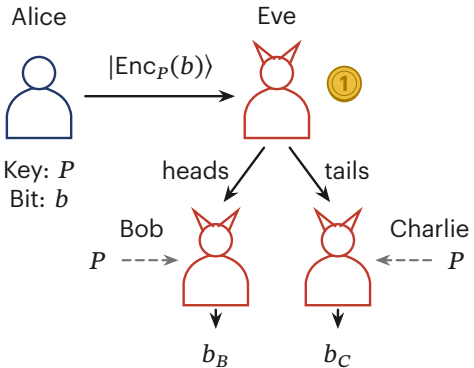
- Naive hope 1: show Pr[Bob correct] + Pr[Charlie correct] $\leq \frac{1}{2} + \frac{1}{2} = 1$

Aside: A Cautionary Tale

- Naive hope 1: show $\Pr[\text{Bob correct}] + \Pr[\text{Charlie correct}] \leq \frac{1}{2} + \frac{1}{2} = 1$
- Naive hope 2: show $\min(\Pr[\text{Bob correct}], \Pr[\text{Charlie correct}]) \leq \frac{1}{2}$

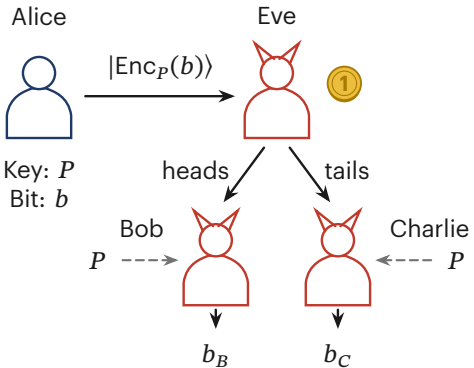
Aside: A Cautionary Tale

- Naive hope 1: show Pr[Bob correct] + Pr[Charlie correct] $\leq \frac{1}{2} + \frac{1}{2} = 1$
- Naive hope 2: show min(Pr[Bob correct], Pr[Charlie correct]) $\leq \frac{1}{2}$



Aside: A Cautionary Tale

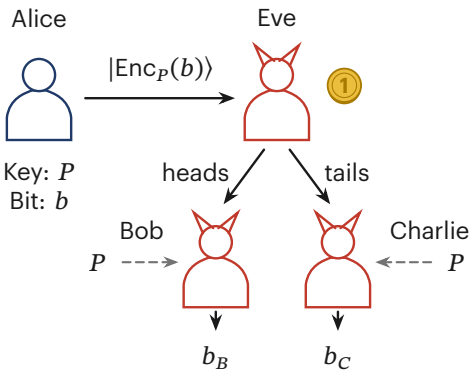
- Naive hope 1: show Pr[Bob correct] + Pr[Charlie correct] $\leq \frac{1}{2} + \frac{1}{2} = 1$
- Naive hope 2: show min(Pr[Bob correct], Pr[Charlie correct]) $\leq \frac{1}{2}$



Pr[correct]	Bob	Charlie	both
heads	1	1/2	1/2
tails	1/2	1	1/2

Aside: A Cautionary Tale

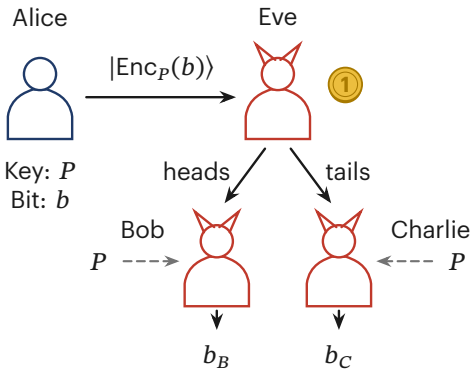
- Naive hope 1: show Pr[Bob correct] + Pr[Charlie correct] $\leq \frac{1}{2} + \frac{1}{2} = 1$
- Naive hope 2: show min(Pr[Bob correct], Pr[Charlie correct]) $\leq \frac{1}{2}$



Pr[correct]	Bob	Charlie	both
heads	1	1/2	1/2
tails	1/2	1	1/2
overall	3/4	3/4	1/2

Aside: A Cautionary Tale

- Naive hope 1: show Pr[Bob correct] + Pr[Charlie correct] $\leq \frac{1}{2} + \frac{1}{2} = 1$
- Naive hope 2: show min(Pr[Bob correct], Pr[Charlie correct]) $\leq \frac{1}{2}$

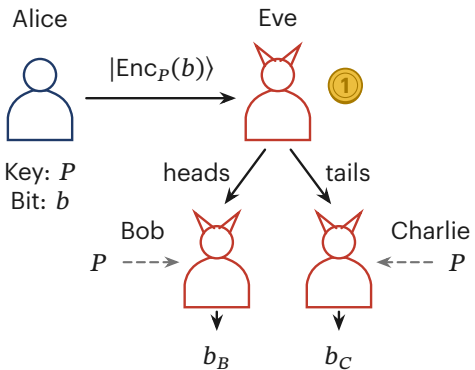


Pr[correct]	Bob	Charlie	both
heads	1	1/2	1/2
tails	1/2	1	1/2
overall	3/4	3/4	1/2

- Random forwarding thwarts both: $3/4 + 3/4 > 1$ and $\min(3/4, 3/4) > 1/2$

Aside: A Cautionary Tale

- Naive hope 1: show Pr[Bob correct] + Pr[Charlie correct] $\leq \frac{1}{2} + \frac{1}{2} = 1$
- Naive hope 2: show min(Pr[Bob correct], Pr[Charlie correct]) $\leq \frac{1}{2}$



Pr[correct]	Bob	Charlie	both
heads	1	1/2	1/2
tails	1/2	1	1/2
overall	3/4	3/4	1/2

- Random forwarding thwarts both: $3/4 + 3/4 > 1$ and $\min(3/4, 3/4) > 1/2$
- But Bob and Charlie get this "advantage" in situations where they disagree and lose ⇒ need to account for this

Step 4: Filter by Disagreement

- Cautionary tale: our analysis still needs to somehow leverage the cases where Bob and Charlie disagree

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement
G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Step 4: Filter by Disagreement

- Cautionary tale: our analysis still needs to somehow leverage the cases where Bob and Charlie disagree
- So down-weight disagreement:

$$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}, \quad \text{where } t = \lambda_{\max}(\mathsf{G})$$

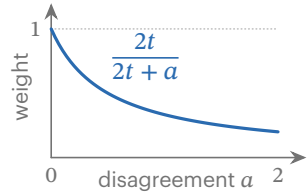
$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement
G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Step 4: Filter by Disagreement

- Cautionary tale: our analysis still needs to somehow leverage the cases where Bob and Charlie disagree
- So down-weight disagreement:

$$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}, \quad \text{where } t = \lambda_{\max}(\mathsf{G})$$

- On an eigenvector of D with eigenvalue $a \in [0, 2]$, F acts as $2t/(2t + a) \in (0, 1]$



Full weight where Bob and Charlie agree, less the more they disagree

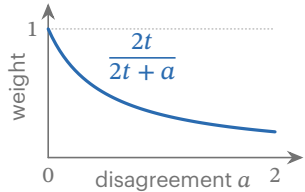
$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement
G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Step 4: Filter by Disagreement

- Cautionary tale: our analysis still needs to somehow leverage the cases where Bob and Charlie disagree
- So down-weight disagreement:

$$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}, \quad \text{where } t = \lambda_{\max}(\mathsf{G})$$

- On an eigenvector of D with eigenvalue $a \in [0, 2]$, F acts as $2t/(2t + a) \in (0, 1]$



Full weight where Bob and Charlie agree, less the more they disagree

Goal: prove $\|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\| \le d/K$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement
G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Step 4: The Filter as a Taylor Series

- Agreement is $\mathsf{E}_{BC} = I - \mathsf{D} = \mathbb{E}_Q[I \otimes B_Q \otimes C_Q]$, so

$$\mathsf{F} = 2t\big((2t+1)I - \mathsf{E}_{BC}\big)^{-1} = \sum_{\ell \geq 0} c_\ell \, \mathsf{E}_{BC}^{\ell}, \qquad c_\ell = \frac{2t}{(2t+1)^{\ell+1}} \geq 0, \quad \sum_{\ell} c_\ell = 1$$

$\mathsf{E}_{BC} = I - \mathsf{D}$: agreement · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success
F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Step 4: The Filter as a Taylor Series

- Agreement is $\mathsf{E}_{BC} = I - \mathsf{D} = \mathbb{E}_Q[I \otimes B_Q \otimes C_Q]$, so

$$\mathsf{F} = 2t\big((2t+1)I - \mathsf{E}_{BC}\big)^{-1} = \sum_{\ell \geq 0} c_\ell \, \mathsf{E}_{BC}^{\ell}, \qquad c_\ell = \frac{2t}{(2t+1)^{\ell+1}} \geq 0, \quad \sum_{\ell} c_\ell = 1$$

- By the triangle inequality, $\|\mathsf{E}_B \mathsf{F} \mathsf{E}_C\| \leq \sum_\ell c_\ell \, \|\mathsf{E}_B \mathsf{E}_{BC}^{\ell} \mathsf{E}_C\|$

$\mathsf{E}_{BC} = I - \mathsf{D}$: agreement · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success
F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Step 4: The Filter as a Taylor Series

- Agreement is $\mathsf{E}_{BC} = I - \mathsf{D} = \mathbb{E}_Q[I \otimes B_Q \otimes C_Q]$, so

$$\mathsf{F} = 2t\big((2t+1)I - \mathsf{E}_{BC}\big)^{-1} = \sum_{\ell \geq 0} c_\ell \, \mathsf{E}_{BC}^{\ell}, \qquad c_\ell = \frac{2t}{(2t+1)^{\ell+1}} \geq 0, \quad \sum_{\ell} c_\ell = 1$$

- By the triangle inequality, $\|\mathsf{E}_B \mathsf{F} \mathsf{E}_C\| \leq \sum_\ell c_\ell \, \|\mathsf{E}_B \mathsf{E}_{BC}^{\ell} \mathsf{E}_C\|$
- Since $\sum_\ell c_\ell = 1$, it suffices to show $\|\mathsf{E}_B \mathsf{E}_{BC}^{\ell} \mathsf{E}_C\| \leq \|\mathsf{E}_B \mathsf{E}_C\|$ for every ℓ

$\mathsf{E}_{BC} = I - \mathsf{D}$: agreement · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success
F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Step 4: The Filter as a Taylor Series

This slide: the $\ell = 1$ case (general case is analogous)

- C_Q commutes with E_B, and B_Q with E_C (different registers)

$$\mathsf{E}_B\,\mathsf{E}_{BC}\,\mathsf{E}_C = \mathbb{E}_Q\big[\,\mathsf{E}_B\; B_Q\; C_Q\;\mathsf{E}_C\,\big]$$

$\mathsf{E}_{BC} = I - \mathrm{D}$: agreement · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success
F: the filter · $t = \lambda_{\max}(\mathrm{G})$

Step 4: The Filter as a Taylor Series

This slide: the $\ell = 1$ case (general case is analogous)

- C_Q commutes with E_B, and B_Q with E_C (different registers)

$$\mathsf{E}_B\,\mathsf{E}_{BC}\,\mathsf{E}_C = \mathbb{E}_Q\big[\,\mathsf{E}_B\; B_Q\; C_Q\;\mathsf{E}_C\,\big]$$

$\mathsf{E}_{BC} = I - \mathsf{D}$: agreement · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success
F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Step 4: The Filter as a Taylor Series

This slide: the $\ell = 1$ case (general case is analogous)

- C_Q commutes with E_B, and B_Q with E_C (different registers)

$$\mathsf{E}_B\,\mathsf{E}_{BC}\,\mathsf{E}_C = \mathbb{E}_Q\big[\,\mathsf{E}_B\,B_Q\,C_Q\,\mathsf{E}_C\,\big]$$

$$= \mathbb{E}_Q\big[\,C_Q\,\mathsf{E}_B\,\mathsf{E}_C\,B_Q\,\big]$$

$\mathsf{E}_{BC} = I - \mathsf{D}$: agreement · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success
F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Step 4: The Filter as a Taylor Series

This slide: the $\ell = 1$ case (general case is analogous)

- C_Q commutes with E_B, and B_Q with E_C (different registers)
- Multiplying by unitaries such as B_Q, C_Q preserves the norm

$$\mathsf{E}_B\,\mathsf{E}_{BC}\,\mathsf{E}_C = \mathbb{E}_Q\big[\,\mathsf{E}_B\; B_Q\; C_Q\; \mathsf{E}_C\,\big]$$

$$= \mathbb{E}_Q\big[\,C_Q\,\mathsf{E}_B\,\mathsf{E}_C\,B_Q\,\big]$$

$$\|\mathsf{E}_B\mathsf{E}_{BC}\mathsf{E}_C\| = \Big\|\mathbb{E}_Q[C_Q\,\mathsf{E}_B\mathsf{E}_C\,B_Q]\Big\| \le \mathbb{E}_Q\,\|C_Q\,\mathsf{E}_B\mathsf{E}_C\,B_Q\| = \|\mathsf{E}_B\mathsf{E}_C\|$$

triangle inequality — unitaries

$\mathsf{E}_{BC} = I - \mathsf{D}$: agreement · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success
F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Step 4: The Filter as a Taylor Series

This slide: the $\ell = 1$ case (general case is analogous)

- C_Q commutes with E_B, and B_Q with E_C (different registers)
- Multiplying by unitaries such as B_Q, C_Q preserves the norm

$$\mathsf{E}_B\,\mathsf{E}_{BC}\,\mathsf{E}_C = \mathbb{E}_Q\big[\,\mathsf{E}_B\; B_Q\; C_Q\; \mathsf{E}_C\,\big]$$

$$= \mathbb{E}_Q\big[\,C_Q\,\mathsf{E}_B\,\mathsf{E}_C\,B_Q\,\big]$$

$$\|\mathsf{E}_B\mathsf{E}_{BC}\mathsf{E}_C\| = \Big\|\mathbb{E}_Q[C_Q\,\mathsf{E}_B\mathsf{E}_C\,B_Q]\Big\| \le \mathbb{E}_Q\,\|C_Q\,\mathsf{E}_B\mathsf{E}_C\,B_Q\| = \|\mathsf{E}_B\mathsf{E}_C\|$$

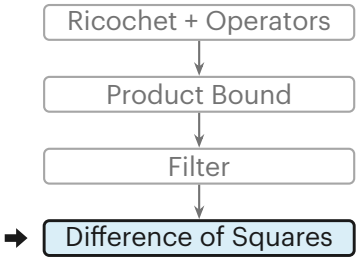
triangle inequality — unitaries

Recap: $\|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\| \le \sum_\ell c_\ell\,\|\mathsf{E}_B\mathsf{E}_{BC}^{\ell}\mathsf{E}_C\| \le \|\mathsf{E}_B\mathsf{E}_C\| \le d/K$

$\mathsf{E}_{BC} = I - \mathsf{D}$: agreement · $\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success
F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Proof Roadmap

Goal: $t = \lambda_{\max}(\mathsf{G}) \le \sqrt{d/K}$



$\Pr[b_B = b_C = b] \le \frac{1}{2} + \frac{1}{2}\lambda_{\max}(\mathsf{G})$, where $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$
disagreement: $\mathsf{D} = I - \mathbb{E}_P[I \otimes B_P \otimes C_P]$

$\|\mathsf{E}_B\mathsf{E}_C\| \le d/K$
via Pauli (anti)commutation [Rag26] or orthogonality [AS26]

$\|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\| \le d/K$, where $\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$
via the Taylor expansion of F

$t^2 \le \|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\|$. Combine with the above ⇒ done!

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · $d = 2^\kappa$, $K = 4^\kappa - 1$
D: disagreement · F: the filter · G: joint success · $t = \lambda_{\max}(\mathsf{G})$

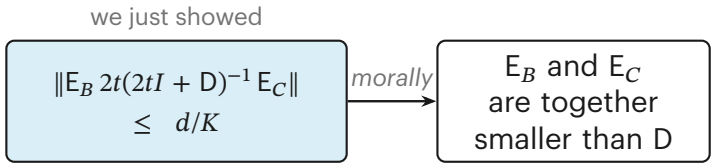
Step 5: Where We Stand

we just showed

$$\|\mathsf{E}_B\, 2t(2tI + \mathsf{D})^{-1}\, \mathsf{E}_C\| \leq d/K$$

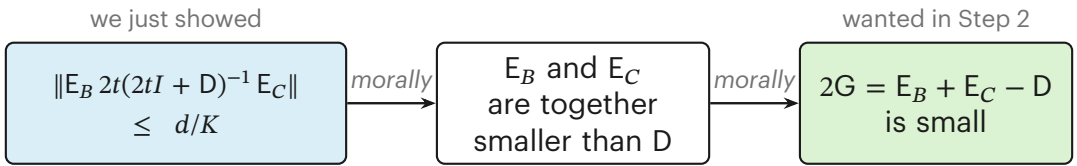
$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement
G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Where We Stand



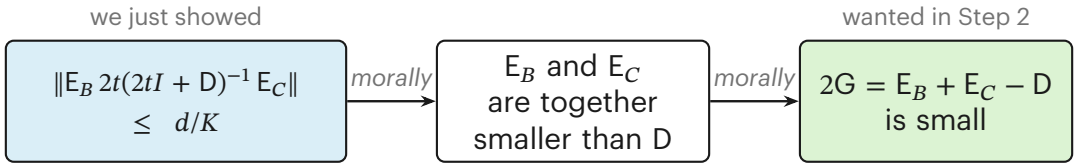
$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement
G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Where We Stand



$\mathrm{E}_B, \mathrm{E}_C$: Bob's, Charlie's success · D: disagreement
G: joint success · $t = \lambda_{\max}(\mathrm{G})$

Step 5: Where We Stand



This intuition actually works!

$\mathrm{E}_B, \mathrm{E}_C$: Bob's, Charlie's success · D: disagreement
G: joint success · $t = \lambda_{\max}(\mathrm{G})$

Step 5: A Difference of Squares

- Scalar warm-up: $(x+y)^2 - (x-y)^2 = 4xy$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · $d = 2^\kappa$, $K = 4^\kappa - 1$
F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Step 5: A Difference of Squares

- Scalar warm-up: $(x+y)^2-(x-y)^2=4xy$
- The same expansion, with F in the middle:

$$(\mathsf{E}_B+\mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B+\mathsf{E}_C)-(\mathsf{E}_B-\mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B-\mathsf{E}_C)=2\,\mathsf{E}_B\mathsf{F}\mathsf{E}_C+2\,\mathsf{E}_C\mathsf{F}\mathsf{E}_B$$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · $d=2^\kappa$, $K=4^\kappa-1$
F: the filter · $t=\lambda_{\max}(\mathsf{G})$

Step 5: A Difference of Squares

- Scalar warm-up: $(x+y)^2 - (x-y)^2 = 4xy$
- The same expansion, with F in the middle:

$$(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C) - (\mathsf{E}_B - \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B - \mathsf{E}_C) = \underbrace{2\,\mathsf{E}_B\mathsf{F}\mathsf{E}_C + 2\,\mathsf{E}_C\mathsf{F}\mathsf{E}_B}_{\preceq\,(4d/K)\,I \text{ by Step 4}}$$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · $d = 2^\kappa$, $K = 4^\kappa - 1$
F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Bounding the Difference Term

Claim: with the filter written out,

$$(\mathsf{E}_B - \mathsf{E}_C) \cdot 2t\,(2tI + \mathsf{D})^{-1} \cdot (\mathsf{E}_B - \mathsf{E}_C) \;\preceq\; 2t\,\mathsf{D}$$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement
$t = \lambda_{\max}(\mathsf{G})$

Step 5: Bounding the Difference Term

Claim: with the filter written out,

$$(\mathrm{E}_B - \mathrm{E}_C) \cdot 2t\,(2tI + \mathrm{D})^{-1} \cdot (\mathrm{E}_B - \mathrm{E}_C) \;\preceq\; 2t\,\mathrm{D}$$

- Intuition: $\mathrm{E}_B - \mathrm{E}_C \preceq \mathrm{D}$ and $\mathrm{E}_C - \mathrm{E}_B \preceq \mathrm{D}$, since Bob and Charlie can differ in success only when they disagree

$\mathrm{E}_B, \mathrm{E}_C$: Bob's, Charlie's success · D: disagreement
$t = \lambda_{\max}(\mathrm{G})$

Step 5: Bounding the Difference Term

Claim: with the filter written out,

$$(\mathrm{E}_B - \mathrm{E}_C) \cdot 2t\,(2tI + \mathrm{D})^{-1} \cdot (\mathrm{E}_B - \mathrm{E}_C) \;\preceq\; 2t\,\mathrm{D}$$

- Intuition: $\mathrm{E}_B - \mathrm{E}_C \preceq \mathrm{D}$ and $\mathrm{E}_C - \mathrm{E}_B \preceq \mathrm{D}$, since Bob and Charlie can differ in success only when they disagree
- So, morally, replace $\mathrm{E}_B - \mathrm{E}_C$ by D: $\mathrm{D} \cdot 2t\,(2tI + \mathrm{D})^{-1} \cdot \mathrm{D} \preceq 2t\,\mathrm{D}$, since $\mathrm{D} \preceq 2tI + \mathrm{D}$

$\mathrm{E}_B, \mathrm{E}_C$: Bob's, Charlie's success · D: disagreement
$t = \lambda_{\max}(\mathrm{G})$

Step 5: Putting It Together

- Rearrange the difference of squares, and bound each piece:

$$(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C) = (\mathsf{E}_B - \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B - \mathsf{E}_C) + \underbrace{2\,\mathsf{E}_B\mathsf{F}\mathsf{E}_C + 2\,\mathsf{E}_C\mathsf{F}\mathsf{E}_B}_{\preceq\,(4d/K)\,I \text{ by Step 4}}$$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement · $d = 2^\kappa$, $K = 4^\kappa - 1$
F: the filter · $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$ · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Putting It Together

- Rearrange the difference of squares, and bound each piece:

$$(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C) = \underbrace{(\mathsf{E}_B - \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B - \mathsf{E}_C)}_{\preceq\, 2t\,\mathsf{D}\text{ (just shown)}} + \underbrace{2\,\mathsf{E}_B\mathsf{F}\mathsf{E}_C + 2\,\mathsf{E}_C\mathsf{F}\mathsf{E}_B}_{\preceq\,(4d/K)\,I\text{ by Step 4}}$$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement · $d = 2^\kappa$, $K = 4^\kappa - 1$
F: the filter · $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$ · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Putting It Together

- Rearrange the difference of squares, and bound each piece:

$$(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C) = \underbrace{(\mathsf{E}_B - \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B - \mathsf{E}_C)}_{\preceq\, 2t\,\mathsf{D}\text{ (just shown)}} + \underbrace{2\,\mathsf{E}_B\mathsf{F}\mathsf{E}_C + 2\,\mathsf{E}_C\mathsf{F}\mathsf{E}_B}_{\preceq\,(4d/K)\,I\text{ by Step 4}}$$

Therefore $\boxed{(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C) \preceq 2t\,\mathsf{D} + (4d/K)\,I}$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement · $d = 2^\kappa$, $K = 4^\kappa - 1$
F: the filter · $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$ · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Putting It Together

- Rearrange the difference of squares, and bound each piece:

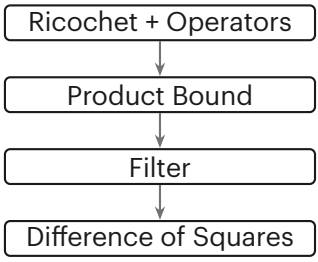
$$(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C) = \underbrace{(\mathsf{E}_B - \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B - \mathsf{E}_C)}_{\preceq\, 2t\,\mathsf{D}\text{ (just shown)}} + \underbrace{2\,\mathsf{E}_B\mathsf{F}\mathsf{E}_C + 2\,\mathsf{E}_C\mathsf{F}\mathsf{E}_B}_{\preceq\,(4d/K)\,I\text{ by Step 4}}$$

Therefore $\boxed{(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C) \preceq 2t\,\mathsf{D} + (4d/K)\,I}$

Massage this to get $\lambda_{\max}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D}) = 2t \le 2\sqrt{d/K}$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement · $d = 2^\kappa$, $K = 4^\kappa - 1$
F: the filter · $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$ · $t = \lambda_{\max}(\mathsf{G})$

Part II: Summary



$\Pr[b_B = b_C = b] \le \frac{1}{2} + \frac{1}{2}\lambda_{\max}(\mathsf{G})$, where $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$

disagreement: $\mathsf{D} = I - \mathbb{E}_P[I \otimes B_P \otimes C_P]$

$\|\mathsf{E}_B\mathsf{E}_C\| \le d/K$

via Pauli (anti)commutation [Rag26] or orthogonality [AS26]

$\|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\| \le d/K$, where $\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$

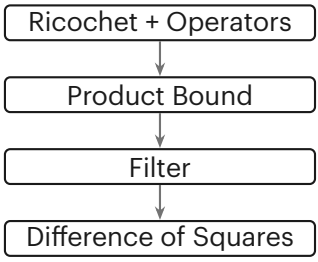
via the Taylor expansion of F

$t^2 \le \|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\|$. Combine with the above ⇒ done!

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · $d = 2^\kappa$, $K = 4^\kappa - 1$

D: disagreement · F: the filter · G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Part II: Summary



$\Pr[b_B = b_C = b] \le \frac{1}{2} + \frac{1}{2}\lambda_{\max}(\mathsf{G})$, where $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$

disagreement: $\mathsf{D} = I - \mathbb{E}_P[I \otimes B_P \otimes C_P]$

$\|\mathsf{E}_B\mathsf{E}_C\| \le d/K$

via Pauli (anti)commutation [Rag26] or orthogonality [AS26]

$\|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\| \le d/K$, where $\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$

via the Taylor expansion of F

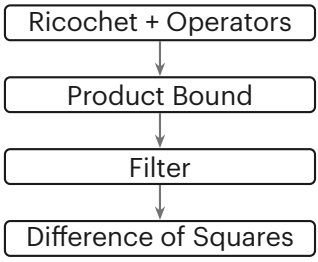
$t^2 \le \|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\|$. Combine with the above ⇒ done!

Theorem [ARS26]**:** $\Pr[b_B = b_C = b] \le \frac{1}{2} + \frac{1}{2}\sqrt{d/K}$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · $d = 2^\kappa$, $K = 4^\kappa - 1$

D: disagreement · F: the filter · G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Part II: Summary



$\Pr[b_B = b_C = b] \le \frac{1}{2} + \frac{1}{2}\lambda_{\max}(\mathsf{G})$, where $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$

disagreement: $\mathsf{D} = I - \mathbb{E}_P[I \otimes B_P \otimes C_P]$

$\|\mathsf{E}_B\mathsf{E}_C\| \le d/K$

via Pauli (anti)commutation [Rag26] or orthogonality [AS26]

$\|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\| \le d/K$, where $\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$

via the Taylor expansion of F

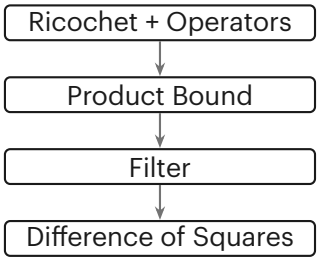
$t^2 \le \|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\|$. Combine with the above ⇒ done!

Theorem [ARS26]**:** $\Pr[b_B = b_C = b] \le \frac{1}{2} + \frac{1}{2}\sqrt{d/K} = \frac{1}{2} + \frac{1}{2}\sqrt{2^\kappa/(4^\kappa - 1)}$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · $d = 2^\kappa$, $K = 4^\kappa - 1$

D: disagreement · F: the filter · G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Part II: Summary



$\Pr[b_B = b_C = b] \le \frac{1}{2} + \frac{1}{2}\lambda_{\max}(\mathsf{G})$, where $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$

disagreement: $\mathsf{D} = I - \mathbb{E}_P[I \otimes B_P \otimes C_P]$

$\|\mathsf{E}_B\mathsf{E}_C\| \le d/K$

via Pauli (anti)commutation [Rag26] or orthogonality [AS26]

$\|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\| \le d/K$, where $\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$

via the Taylor expansion of F

$t^2 \le \|\mathsf{E}_B\mathsf{F}\mathsf{E}_C\|$. Combine with the above ⇒ done!

Theorem [ARS26]**:** $\Pr[b_B = b_C = b] \le \frac{1}{2} + \frac{1}{2}\sqrt{d/K} = \frac{1}{2} + \frac{1}{2}\sqrt{2^\kappa/(4^\kappa - 1)}$

The main new idea: using a disagreement filter F

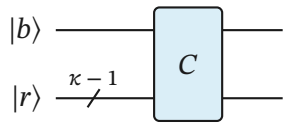
$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · $d = 2^\kappa$, $K = 4^\kappa - 1$
D: disagreement · F: the filter · G: joint success · $t = \lambda_{\max}(\mathsf{G})$

Roadmap

- Part I: The Unclonable Encryption Problem
- Part II: The Proof
- ➜ Part III: Follow-Up and Related Works

Messages of Any Length [BBC26b]

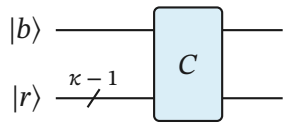
The one-bit encryption circuit, rewritten



key: a uniformly random Clifford C

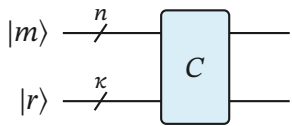
Messages of Any Length [BBC26b]

The one-bit encryption circuit, rewritten



key: a uniformly random Clifford C

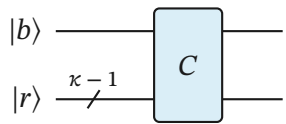
Generalising this to encrypt arbitrary-length messages



key: a random Clifford on $n + \kappa$ qubits

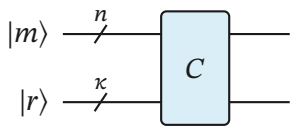
Messages of Any Length [BBC26b]

The one-bit encryption circuit, rewritten



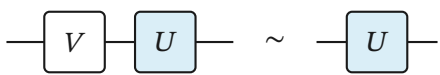
key: a uniformly random Clifford C

Generalising this to encrypt arbitrary-length messages



key: a random Clifford on $n + \kappa$ qubits

Security proof sketch: a random Clifford absorbs any fixed Clifford V



so the arbitrary-length scheme's security generically reduces to the one-bit scheme's security

Different Approach via Goldreich–Levin

- Secret key: (θ, r) for $\theta \leftarrow$ SearchEnc.KeyGen and $r \leftarrow \{0,1\}^n$

Different Approach via Goldreich–Levin

- Secret key: (θ, r) for $\theta \leftarrow \mathsf{SearchEnc.KeyGen}$ and $r \leftarrow \{0,1\}^n$
- Encryption for $b \in \{0,1\}$: sample $m \leftarrow \{0,1\}^n$ and output:

$$\mathsf{INDEnc}_{\theta,r}(b) = \left(|\mathsf{SearchEnc}_\theta(m)\rangle,\ b \oplus \langle r, m\rangle\right)$$

Different Approach via Goldreich–Levin

- Secret key: (θ, r) for $\theta \leftarrow \mathsf{SearchEnc.KeyGen}$ and $r \leftarrow \{0,1\}^n$
- Encryption for $b \in \{0,1\}$: sample $m \leftarrow \{0,1\}^n$ and output:

$$\mathsf{INDEnc}_{\theta,r}(b) = \left(|\mathsf{SearchEnc}_\theta(m)\rangle,\ b \oplus \langle r, m\rangle\right)$$

- Hope from Goldreich–Levin [GL89]: predicting $\langle r, m\rangle$ for random r should reveal m and hence break search security

Different Approach via Goldreich–Levin

- Secret key: (θ, r) for $\theta \leftarrow \mathsf{SearchEnc.KeyGen}$ and $r \leftarrow \{0,1\}^n$
- Encryption for $b \in \{0,1\}$: sample $m \leftarrow \{0,1\}^n$ and output:

$$\mathsf{INDEnc}_{\theta,r}(b) = \left(|\mathsf{SearchEnc}_\theta(m)\rangle,\ b \oplus \langle r, m\rangle\right)$$

- Hope from Goldreich–Levin [GL89]: predicting $\langle r, m\rangle$ for random r should reveal m and hence break search security
- The challenge: two non-communicating parties receiving the same challenge r — need a *simultaneous Goldreich–Levin reduction*

Simultaneous Goldreich–Levin [CLX26,Ana26]

Goal: from guessing $\langle r, m \rangle$ with a shared challenge r, to both recovering m

Recall from Step 4: with agreement $\mathsf{E}_{BC} = I - \mathsf{D} = \mathbb{E}_Q[I \otimes B_Q \otimes C_Q]$,

$$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1} = \sum_{\ell \geq 0} c_\ell\, \mathsf{E}_{BC}^{\ell}, \qquad c_\ell = \frac{2t}{(2t+1)^{\ell+1}} \geq 0, \quad \sum_{\ell} c_\ell = 1$$

$\mathsf{E}_{BC} = I - \mathsf{D}$: agreement · F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Simultaneous Goldreich–Levin [CLX26,Ana26]

Goal: from guessing $\langle r, m \rangle$ with a shared challenge r, to both recovering m

Recall from Step 4: with agreement $\mathsf{E}_{BC} = I - \mathsf{D} = \mathbb{E}_Q[I \otimes B_Q \otimes C_Q]$,

$$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1} = \sum_{\ell \geq 0} c_\ell\, \mathsf{E}_{BC}^{\ell}, \qquad c_\ell = \frac{2t}{(2t+1)^{\ell+1}} \geq 0, \quad \sum_{\ell} c_\ell = 1$$

- Essentially, the reduction samples term ℓ of this series with probability c_ℓ, and applies it before running Goldreich–Levin

$\mathsf{E}_{BC} = I - \mathsf{D}$: agreement · F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Simultaneous Goldreich–Levin [CLX26,Ana26]

Goal: from guessing $\langle r, m \rangle$ with a shared challenge r, to both recovering m

Recall from Step 4: with agreement $\mathsf{E}_{BC} = I - \mathsf{D} = \mathbb{E}_Q[I \otimes B_Q \otimes C_Q]$,

$$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1} = \sum_{\ell \geq 0} c_\ell\, \mathsf{E}_{BC}^{\ell}, \qquad c_\ell = \frac{2t}{(2t+1)^{\ell+1}} \geq 0, \quad \sum_{\ell} c_\ell = 1$$

- Essentially, the reduction samples term ℓ of this series with probability c_ℓ, and applies it before running Goldreich–Levin
- This shoehorns the filter F into the simultaneous Goldreich–Levin reduction

$\mathsf{E}_{BC} = I - \mathsf{D}$: agreement · F: the filter · $t = \lambda_{\max}(\mathsf{G})$

Simultaneous Goldreich–Levin [CLX26,Ana26]

Goal: from guessing $\langle r, m \rangle$ with a shared challenge r, to both recovering m

Recall from Step 4: with agreement $\mathsf{E}_{BC} = I - \mathsf{D} = \mathbb{E}_Q[I \otimes B_Q \otimes C_Q]$,

$$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1} = \sum_{\ell \geq 0} c_\ell\, \mathsf{E}_{BC}^{\ell}, \qquad c_\ell = \frac{2t}{(2t+1)^{\ell+1}} \geq 0, \quad \sum_{\ell} c_\ell = 1$$

- Essentially, the reduction samples term ℓ of this series with probability c_ℓ, and applies it before running Goldreich–Levin
- This shoehorns the filter F into the simultaneous Goldreich–Levin reduction

Note: here the filter is actually part of the reduction, not merely an analytical device

$\mathsf{E}_{BC} = I - \mathsf{D}$: agreement · F: the filter · $t = \lambda_{\max}(\mathsf{G})$

What the F Operator?

What the F Operator?

F = $(I + \mathrm{D}/2t)^{-1}$ is a *resolvent* (from operator theory)

What the F Operator?

F = $(I + \mathrm{D}/2t)^{-1}$ is a *resolvent* (from operator theory)

Beyond [ARS26] and [CLX26], it keeps turning up in AI-assisted quantum results as a tool for discounting a bad event:


Limits to black-box amplification in QMA

Scott Aaronson[1], Phillip Harris[2], and Freek Witteveen[3]

No-go for QMA amplification [AHW25]
GPT-5-Thinking suggested the function
tr $P_{\mathrm{rej}}(\theta)^{-1}$

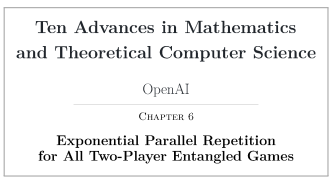
What the F Operator?

F = $(I + \mathrm{D}/2t)^{-1}$ is a *resolvent* (from operator theory)

Beyond [ARS26] and [CLX26], it keeps turning up in AI-assisted quantum results as a tool for discounting a bad event:


Limits to black-box amplification in QMA

Scott Aaronson[1], Phillip Harris[2], and Freek Witteveen[3]


Ten Advances in Mathematics and Theoretical Computer Science

OpenAI

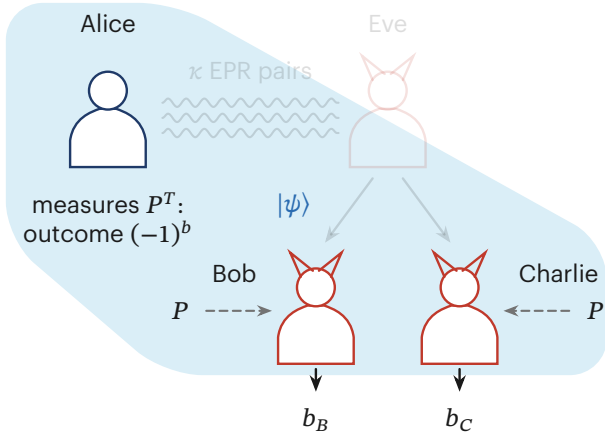
Chapter 6

Exponential Parallel Repetition for All Two-Player Entangled Games

No-go for QMA amplification [AHW25]
GPT-5-Thinking suggested the function
tr $P_{\mathrm{rej}}(\theta)^{-1}$

Quantum parallel repetition [Ope26]
GPT-6 Astra's key tool: a *resolvent purification*, $F\,(F + uI)^{-1}$

Thank you! Questions?



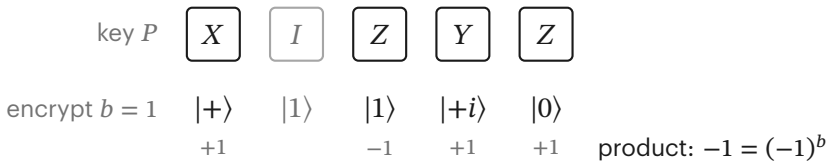
Bonus Slides

How Encryption and Decryption Work, Concretely [Bot+24]



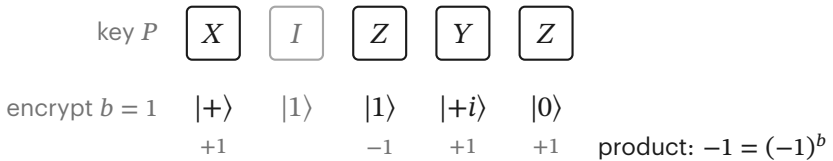
- Key: a uniformly random non-identity Pauli P, one of $K = 4^\kappa - 1$

How Encryption and Decryption Work, Concretely [Bot+24]



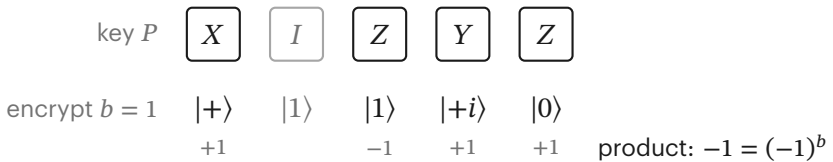
- Key: a uniformly random non-identity Pauli P, one of $K = 4^\kappa - 1$
- Encrypt b: a random eigenstate of each factor, with signs multiplying to $(-1)^b$, and a random $|0\rangle$ or $|1\rangle$ under each I

How Encryption and Decryption Work, Concretely [Bot+24]



- Key: a uniformly random non-identity Pauli P, one of $K = 4^\kappa - 1$
- Encrypt b: a random eigenstate of each factor, with signs multiplying to $(-1)^b$, and a random $|0\rangle$ or $|1\rangle$ under each I
- Equivalently: a uniformly random state in the $(-1)^b$ eigenspace of P

How Encryption and Decryption Work, Concretely [Bot+24]



- Key: a uniformly random non-identity Pauli P, one of $K = 4^\kappa - 1$
- Encrypt b: a random eigenstate of each factor, with signs multiplying to $(-1)^b$, and a random $|0\rangle$ or $|1\rangle$ under each I
- Equivalently: a uniformly random state in the $(-1)^b$ eigenspace of P
- Decrypt: measure each qubit in its own Pauli and multiply the signs

Step 5: Details I

Why $(\mathsf{E}_B - \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B - \mathsf{E}_C) \preceq 2t\,\mathsf{D}$

Fact (block matrices; $\succeq 0$ means positive semidefinite)**:**

(1) If $C \succ 0$: $\begin{pmatrix} A & B \\ B & C \end{pmatrix} \succeq 0 \iff A - BC^{-1}B \succeq 0$ (2) $\begin{pmatrix} A & B \\ B & A \end{pmatrix} \succeq 0 \iff A \pm B \succeq 0$

- Recall: $-\mathsf{D} \preceq \mathsf{E}_B - \mathsf{E}_C \preceq \mathsf{D}$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement
$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$: the filter · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Details I

Why $(\mathsf{E}_B - \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B - \mathsf{E}_C) \preceq 2t\,\mathsf{D}$

Fact (block matrices; $\succeq 0$ means positive semidefinite)**:**

(1) If $C \succ 0$: $\begin{pmatrix} A & B \\ B & C \end{pmatrix} \succeq 0 \iff A - BC^{-1}B \succeq 0$ (2) $\begin{pmatrix} A & B \\ B & A \end{pmatrix} \succeq 0 \iff A \pm B \succeq 0$

- Recall: $-\mathsf{D} \preceq \mathsf{E}_B - \mathsf{E}_C \preceq \mathsf{D}$
- By (2), and since adding $2tI$ to a corner preserves positive semidefiniteness,

$$\begin{pmatrix} \mathsf{D} & \mathsf{E}_B - \mathsf{E}_C \\ \mathsf{E}_B - \mathsf{E}_C & \mathsf{D} \end{pmatrix} \succeq 0 \implies \begin{pmatrix} \mathsf{D} & \mathsf{E}_B - \mathsf{E}_C \\ \mathsf{E}_B - \mathsf{E}_C & \mathsf{D} + 2tI \end{pmatrix} \succeq 0$$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement
$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$: the filter · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Details I

Why $(\mathsf{E}_B - \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B - \mathsf{E}_C) \preceq 2t\,\mathsf{D}$

Fact (block matrices; $\succeq 0$ means positive semidefinite)**:**

(1) If $C \succ 0$: $\begin{pmatrix} A & B \\ B & C \end{pmatrix} \succeq 0 \iff A - BC^{-1}B \succeq 0$ (2) $\begin{pmatrix} A & B \\ B & A \end{pmatrix} \succeq 0 \iff A \pm B \succeq 0$

- Recall: $-\mathsf{D} \preceq \mathsf{E}_B - \mathsf{E}_C \preceq \mathsf{D}$
- By (2), and since adding $2tI$ to a corner preserves positive semidefiniteness,

$$\begin{pmatrix} \mathsf{D} & \mathsf{E}_B - \mathsf{E}_C \\ \mathsf{E}_B - \mathsf{E}_C & \mathsf{D} \end{pmatrix} \succeq 0 \implies \begin{pmatrix} \mathsf{D} & \mathsf{E}_B - \mathsf{E}_C \\ \mathsf{E}_B - \mathsf{E}_C & \mathsf{D} + 2tI \end{pmatrix} \succeq 0$$

- By (1): $\mathsf{D} - (\mathsf{E}_B - \mathsf{E}_C)\,(2tI + \mathsf{D})^{-1}\,(\mathsf{E}_B - \mathsf{E}_C) \succeq 0$. Multiply by $2t \Rightarrow$ done!

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement
$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$: the filter · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Details II

Why $(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C) \preceq 2t\,\mathsf{D} + (4d/K)\,I$ finishes the proof

- Take a unit top eigenvector $|\psi\rangle$ of $\mathsf{E}_B + \mathsf{E}_C - \mathsf{D} = 2\mathsf{G}$:

$$(\mathsf{E}_B + \mathsf{E}_C)\,|\psi\rangle = (2tI + \mathsf{D})\,|\psi\rangle$$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement · $d = 2^\kappa$, $K = 4^\kappa - 1$
$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$: the filter · $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$ · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Details II

Why $(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C) \preceq 2t\,\mathsf{D} + (4d/K)\,I$ finishes the proof

- Take a unit top eigenvector $|\psi\rangle$ of $\mathsf{E}_B + \mathsf{E}_C - \mathsf{D} = 2\mathsf{G}$:

$$(\mathsf{E}_B + \mathsf{E}_C)\,|\psi\rangle = (2tI + \mathsf{D})\,|\psi\rangle$$

- Left side: $\langle\psi|(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C)|\psi\rangle = 2t\,\langle\psi|(2tI + \mathsf{D})|\psi\rangle = 4t^2 + 2t\,\langle\psi|\mathsf{D}|\psi\rangle$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement · $d = 2^\kappa$, $K = 4^\kappa - 1$
$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$: the filter · $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$ · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Details II

Why $(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C) \preceq 2t\,\mathsf{D} + (4d/K)\,I$ finishes the proof

- Take a unit top eigenvector $|\psi\rangle$ of $\mathsf{E}_B + \mathsf{E}_C - \mathsf{D} = 2\mathsf{G}$:

$$(\mathsf{E}_B + \mathsf{E}_C)\,|\psi\rangle = (2tI + \mathsf{D})\,|\psi\rangle$$

- Left side: $\langle\psi|(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C)|\psi\rangle = 2t\,\langle\psi|(2tI + \mathsf{D})|\psi\rangle = 4t^2 + 2t\,\langle\psi|\mathsf{D}|\psi\rangle$
- Right side: $\langle\psi|\big(2t\,\mathsf{D} + (4d/K)\,I\big)|\psi\rangle = 2t\,\langle\psi|\mathsf{D}|\psi\rangle + 4d/K$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement · $d = 2^\kappa$, $K = 4^\kappa - 1$
$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$: the filter · $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$ · $t = \lambda_{\max}(\mathsf{G})$

Step 5: Details II

Why $(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C) \preceq 2t\,\mathsf{D} + (4d/K)\,I$ finishes the proof

- Take a unit top eigenvector $|\psi\rangle$ of $\mathsf{E}_B + \mathsf{E}_C - \mathsf{D} = 2\mathsf{G}$:

$$(\mathsf{E}_B + \mathsf{E}_C)\,|\psi\rangle = (2tI + \mathsf{D})\,|\psi\rangle$$

- Left side: $\langle\psi|(\mathsf{E}_B + \mathsf{E}_C)\,\mathsf{F}\,(\mathsf{E}_B + \mathsf{E}_C)|\psi\rangle = 2t\,\langle\psi|(2tI + \mathsf{D})|\psi\rangle = 4t^2 + 2t\,\langle\psi|\mathsf{D}|\psi\rangle$
- Right side: $\langle\psi|\big(2t\,\mathsf{D} + (4d/K)\,I\big)|\psi\rangle = 2t\,\langle\psi|\mathsf{D}|\psi\rangle + 4d/K$
- Cancel $2t\,\langle\psi|\mathsf{D}|\psi\rangle$: $4t^2 \le 4d/K$, so $t \le \sqrt{d/K}$ $\square$

$\mathsf{E}_B, \mathsf{E}_C$: Bob's, Charlie's success · D: disagreement · $d = 2^\kappa$, $K = 4^\kappa - 1$
$\mathsf{F} = 2t\,(2tI + \mathsf{D})^{-1}$: the filter · $\mathsf{G} = \frac{1}{2}(\mathsf{E}_B + \mathsf{E}_C - \mathsf{D})$ · $t = \lambda_{\max}(\mathsf{G})$