Optimal Untelegraphable Encryption

Denis Rochette Anne Broadbent Eric Culf

JIQ 26 – Bordeaux

January 16, 2026

No-cloning & no-telegraphing theorems

No-cloning theorem (Wootters and Zurek, 1982)

No quantum operation can clone an arbitrary quantum state.

No-cloning & no-telegraphing theorems

No-cloning theorem (Wootters and Zurek, 1982)

No quantum operation can clone an arbitrary quantum state.

No-telegraphing theorem (Werner, 1998)

Arbitrary quantum state cannot be transmitted through classical channels without pre-shared entanglement.

Equivalence of no-cloning and no-telegraphing

These two no-go theorems are informationally equivalent:

Equivalence of no-cloning and no-telegraphing

These two no-go theorems are informationally equivalent:

- If telegraphing were possible, one could telegraph the state and copy the classical information to create two clones.

Equivalence of no-cloning and no-telegraphing

These two no-go theorems are informationally equivalent:

- If telegraphing were possible, one could telegraph the state and copy the classical information to create two clones.
- If cloning were possible, one could clone the state many times and perform tomography to obtain a classical description of the state and then telegraph this description.

Equivalence of no-cloning and no-telegraphing

These two no-go theorems are informationally equivalent:

- If telegraphing were possible, one could telegraph the state and copy the classical information to create two clones.
- If cloning were possible, one could clone the state many times and perform tomography to obtain a classical description of the state and then telegraph this description.

However, they are not computationally equivalent (Nehoran and Zhandry, 2024).

Uncloneable encryption

Uncloneable encryption is a symmetric-key encryption scheme with classical messages & keys, and quantum ciphertexts.

Uncloneable encryption

Uncloneable encryption is a symmetric-key encryption scheme with classical messages & keys, and quantum ciphertexts.

Encryption Scheme

Generation: $\mathsf{Gen}(\mathsf{security}) = \mathsf{key}$

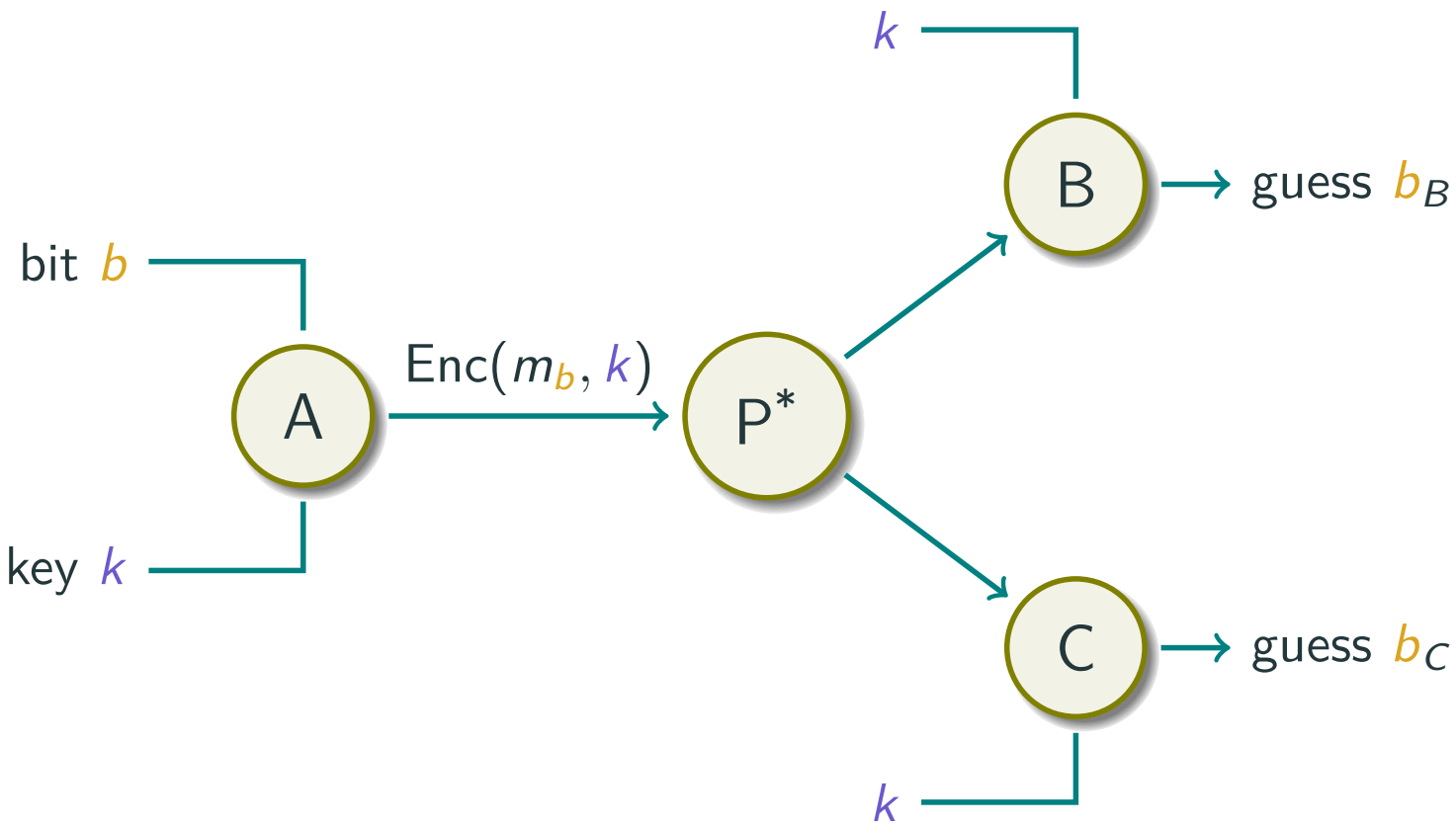
Encryption: $\mathsf{Enc}(\mathsf{message}, \mathsf{key}) = \mathsf{ciphertext}$

Decryption: $\mathsf{Dec}(\mathsf{ciphertext}, \mathsf{key}) = \mathsf{message}$

Security is defined against a cloning attack: a single quantum ciphertext is processed once and then used to enable two separated parties, both holding the key, to recover information about the message.

Untelegraphable encryption

As uncloneable encryption, but restricted to telegraphing attacks:



Goal: Prevent parties B and C from simultaneously guessing bit b with high probability.

---

*P is a quantum-to-classical CPTP map.

Haar-measure encryption

For a $\log(n)$-bit message $m \in [n]$ and a Haar-random unitary $U \in \mathrm{U}(d)$ as the key:

$$\mathrm{Enc}(m, U) = U\Big(\underbrace{|m\rangle\langle m|}_{n\times n \text{ matrix}} \otimes \underbrace{I_{d/n}}_{\text{identity}} \Big) U^*$$

Haar-measure encryption

For a $\log(n)$-bit message $m \in [n]$ and a Haar-random unitary $U \in \mathrm{U}(d)$ as the key:

$$\mathrm{Enc}(m, U) = U\Big(\underbrace{|m\rangle\langle m|}_{n\times n \text{ matrix}} \otimes \underbrace{I_{d/n}}_{\text{identity}} \Big) U^*$$

Efficiency (plain model vs. computational model)

Sampling a Haar-random U is not efficient.

Plain model $\Rightarrow$ unitary t-design (bounded moments security analysis).

Computational model $\Rightarrow$ pseudorandom unitary.

Result 1

Untelegraphable-indistinguishability

The Haar-measure encryption scheme for classical bits (2 messages) achieves untelegraphable-indistinguishable security, with telegraphing attack success probability upper bounded by

$$\frac{1}{2} + \underbrace{\frac{1}{2\sqrt{d+1}}}_{\text{negligible}}.$$

Result 1

Untelegraphable-indistinguishability

The Haar-measure encryption scheme for classical bits (2 messages) achieves untelegraphable-indistinguishable security, with telegraphing attack success probability upper bounded by

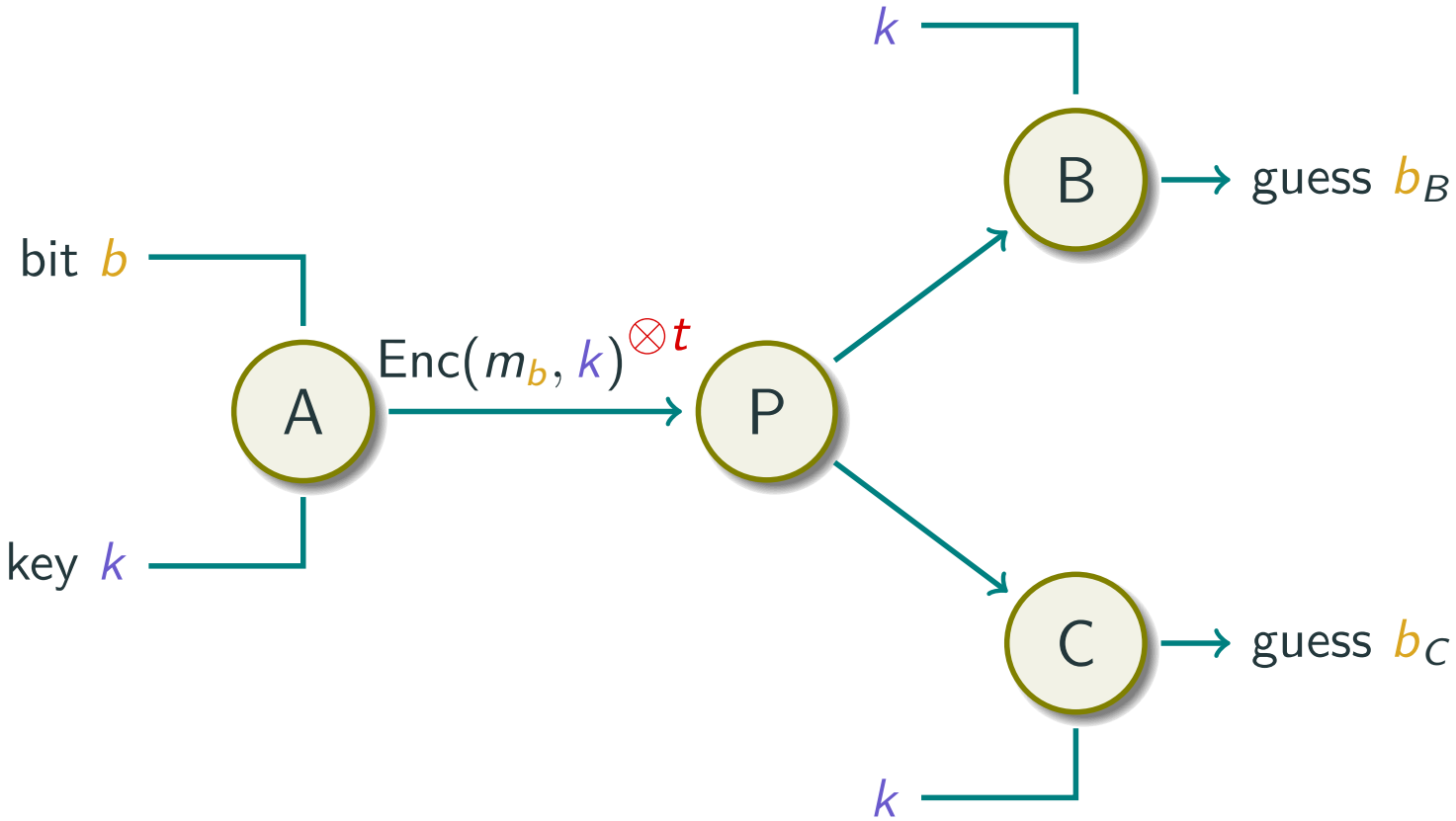
$$\frac{1}{2} + \underbrace{\frac{1}{2\sqrt{d+1}}}_{\text{negligible}}.$$

In contrast, the best known upper bound for cloning attack is (Bhattacharyya and Culf, 2025):

$$\frac{1}{2} + \underbrace{\frac{3\log\log d}{2\log d}}_{\text{not negligible}}.$$

t-copy untelegraphable encryption

Unlike uncloneable encryption, untelegraphable encryption admits a stronger adversarial model where P receives t copies of the ciphertext.



Result 2

t-copy untelegraphable-indistinguishability

The Haar-measure encryption scheme for n classical messages achieves t-copy untelegraphable-indistinguishable security, with telegraphing attack success probability upper bounded by

$$\frac{1}{2} + \underbrace{\frac{7t\sqrt{n}}{\sqrt{d}}}_{\text{negligible}}.$$

Result 2

t-copy untelegraphable-indistinguishability

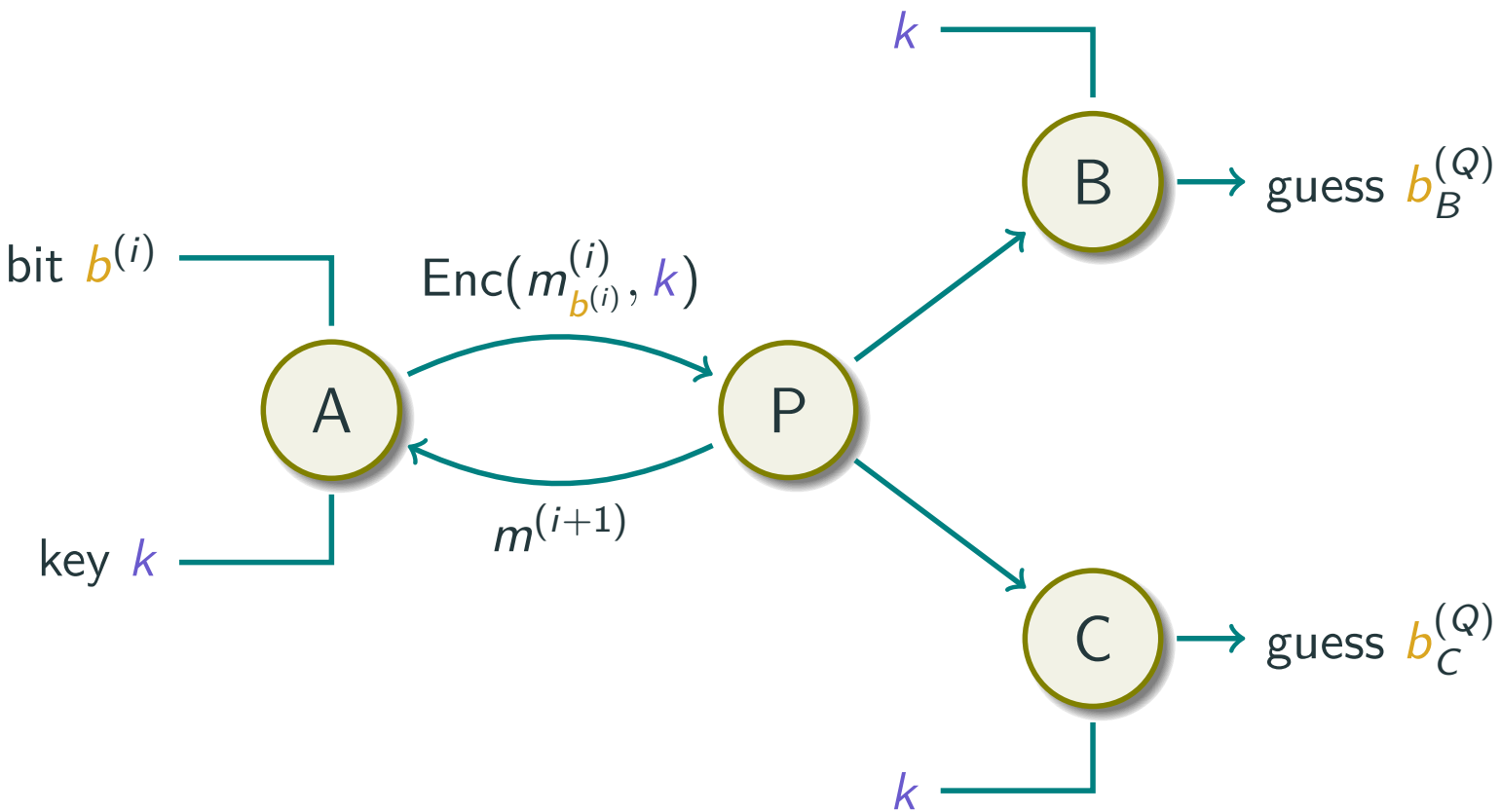
The Haar-measure encryption scheme for n classical messages achieves t-copy untelegraphable-indistinguishable security, with telegraphing attack success probability upper bounded by

$$\frac{1}{2} + \underbrace{\frac{7t\sqrt{n}}{\sqrt{d}}}_{\text{negligible}}.$$

The proof relies on Haar moments up to order $2t$, and therefore requires a unitary $2t$-design.

Collusion-resistant untelegraphable encryption

In a collusion attack, the adversary P adaptively interacts with the sender A across successive Q rounds.



Result 3 & 4

Collusion-resistant untelegraphable-indistinguishability

The Haar-measure encryption scheme for n classical messages achieves Q-round collusion-resistant untelegraphable-indistinguishable security, with telegraphing attack success probability upper bounded by

$$\frac{1}{2} + \underbrace{\frac{7Q\sqrt{n}}{\sqrt{d}}}_{\text{negligible}}.$$

*The adversaries are computationally bounded.

Result 3 & 4

Collusion-resistant untelegraphable-indistinguishability

The Haar-measure encryption scheme for n classical messages achieves Q-round collusion-resistant untelegraphable-indistinguishable security, with telegraphing attack success probability upper bounded by

$$\frac{1}{2} + \underbrace{\frac{7Q\sqrt{n}}{\sqrt{d}}}_{\text{negligible}}.$$

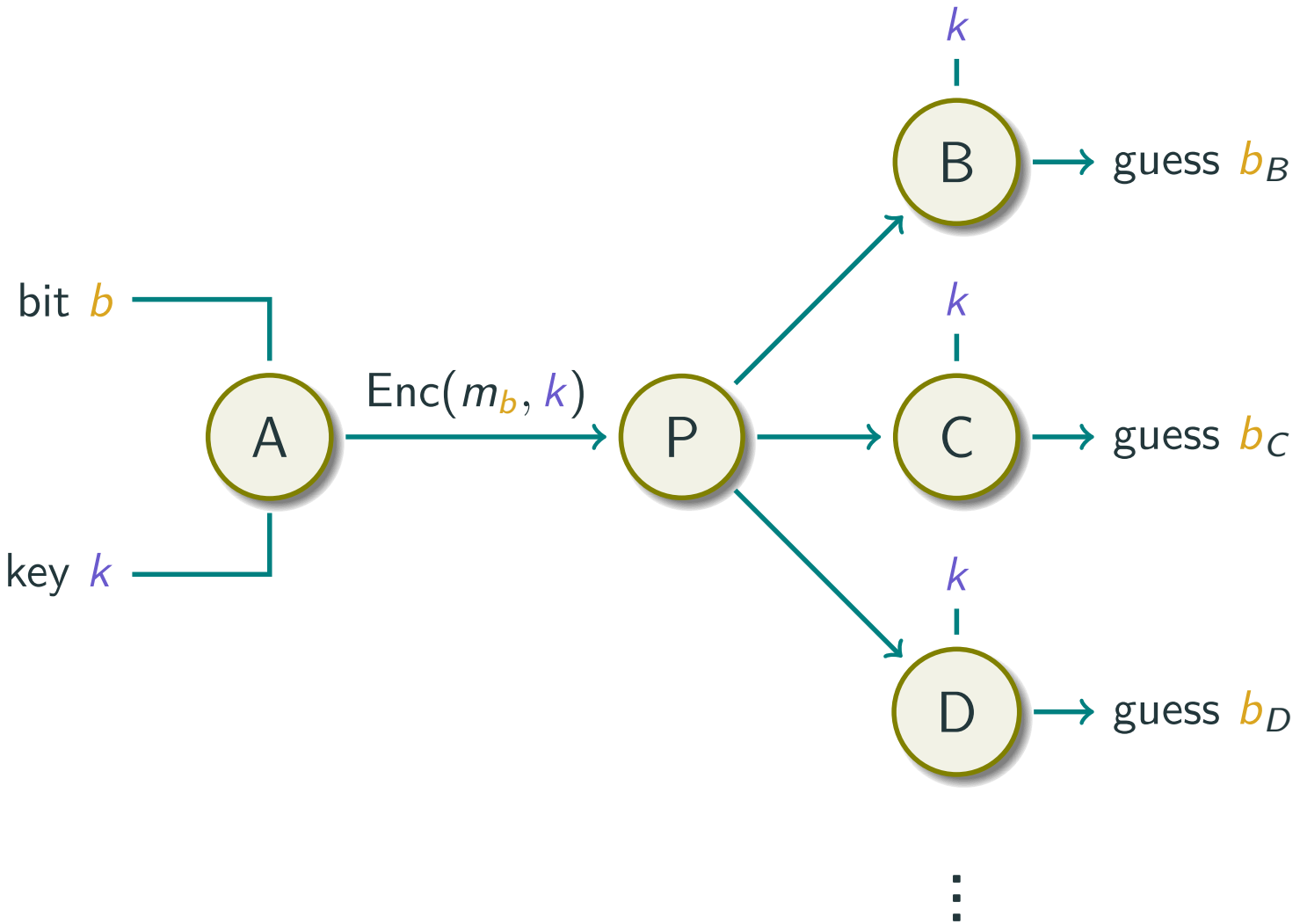
Everlasting security

Unconditional security holds for polynomially many rounds, and everlasting* security for arbitrarily many rounds under pseudorandom unitaries.

*The adversaries are computationally bounded.

s-receiver untelegraphable encryption

The telegraphing attack is extended to s receivers, each given classical information and the key.



Result 5

In analogy with the informational equivalence of no-cloning and no-telegraphing, untelegraphable encryption emerges as a limiting case of uncloneable encryption when the number of receivers grows.

Convergence of cloning to telegraphing attacks

For any uncloneable encryption scheme, the success probability of the cloning attack with s-receiver converges to that of the telegraphing attack at rate

$$\mathcal{O}\left(\frac{1}{\sqrt[3]{s}}\right)$$

Result 6

Minimality of the Haar-measure scheme

Among all quantum encryption schemes, the Haar-measure encryption has the smallest possible success probability against cloning and telegraphing attacks.

Result 6

Minimality of the Haar-measure scheme

Among all quantum encryption schemes, the Haar-measure encryption has the smallest possible success probability against cloning and telegraphing attacks.

Lower bounds for uncloneable and untelegraphable encryption

For any quantum encryption scheme with ciphertext dimension d, the success probability against cloning and telegraphing attacks is lower bounded by

$$\frac{1}{2} + \Omega\left(\frac{1}{\sqrt{d}}\right).$$

The previous best known lower bound was (Majenz, Schaffner and Tahmasbi, 2021):

$$\frac{1}{2} + \Omega\left(\frac{1}{d}\right).$$

Questions?