

— Open Question —

Does the uncloneable bit exist?

Towards Unconditional Uncloneable Encryption [6]

Pierre Botteron¹, Anne Broadbent², Eric Culf³, Ion Nechita¹, Clément Pellegrini¹, Denis Rochette².

¹Université de Toulouse (France); ²University of Ottawa (Canada); ³University of Waterloo (Canada).

1 Goal

Have a secure cryptographic scheme against cloning attacks.

2 Idea

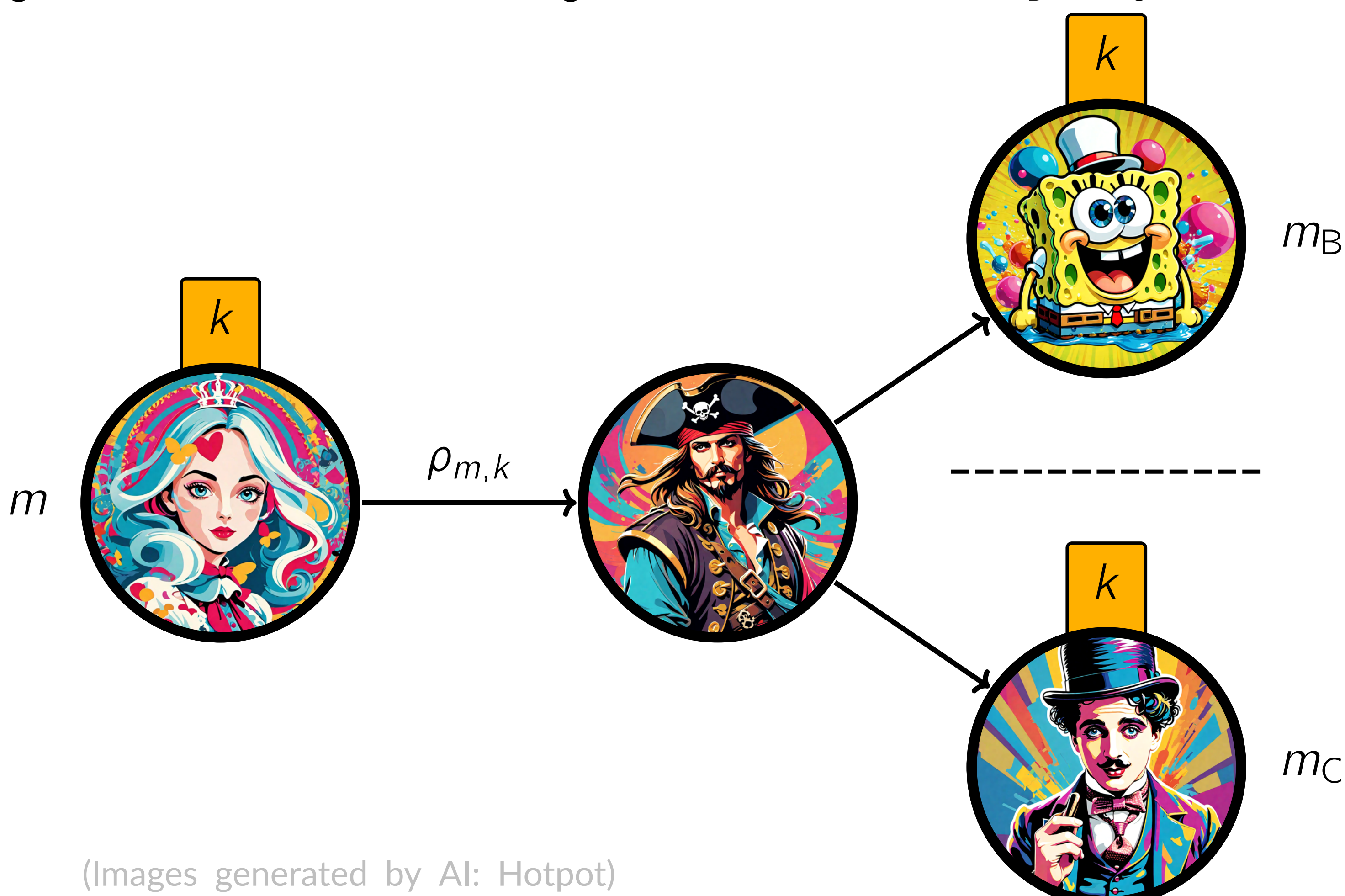
Leverage the quantum no-cloning theorem.

3 Consequences

Applications to private-key quantum money [8], preventing storage attacks [8], quantum functional encryption [13], quantum copy-protection [2], uncloneable decryption [11, 15, 12], and quantum position verification [10].

1. Uncloneable Bit

4 No-Cloning Game. Alice encrypts a message $m \in \{0, 1\}$ with a key $k \in \{1, \dots, K\}$ into a quantum state $\rho_{m,k}$. She sends it via a quantum channel but a pirate (P) intercepts it. Without knowing the key k , the pirate tries to share the information with two non-communicating parties, Bob (B) and Charlie (C), so that both of them may retrieve Alice's message m . We say that the adversary team (P, B, C) wins the game if both Bob's and Charlie's guesses are correct, i.e. if $m_B = m_C = m$.



(Images generated by AI: Hotpot)

5 Definition (Correctness)

The encryption protocol $(m, k) \mapsto \rho_{m,k}$ is said to be *correct* if there exists a way to retrieve m from $\rho_{m,k}$ and k .

6 Definition (Security)

A protocol $(m, k) \mapsto \rho_{m,k}$ is said to be *uncloneable-indistinguishable secure* if:

$$\mathbb{P}((P, B, C) \text{ win the game}) \leq \frac{1}{2} + f(\lambda),$$
where $f(\lambda) \rightarrow 0$ as $\lambda \rightarrow \infty$, and where λ is the security parameter. Additionally, this security is said to be *strong* if moreover $f(\lambda) = \text{negl}(\lambda)$.

8 Former Work

Efforts have focused on its achievability under various models and definitions, including:

- in the quantum random oracle model (QROM) [8, 3, 4],
- in an interactive version of the scenario [7],
- in a device-independent variant with variable keys [12],
- assuming the existence of specific types of obfuscation [1, 9],
- in a variant with quantum keys [5],
- and a "succinct" variant [14].

7 Open Question (Uncloneable Bit) [8]

Is there an encryption scheme $(m, k) \mapsto \rho_{m,k}$ that is both correct and uncloneable-indistinguishable secure?

2. Candidate Scheme and Conjecture

9 Candidate Scheme: Clifford Algebra

Let $\Gamma_1, \dots, \Gamma_K$ be Hermitian unitaries that anti-commute. Consider the following encryption:

$$\rho_{m,k} := \frac{2}{d} \frac{I_d + (-1)^m \Gamma_k}{2},$$

where $m \in \{0, 1\}$ and $k \in \{1, \dots, K\}$. This encryption protocol is correct since one can retrieve m from measuring $\rho_{m,k}$ in the eigenbasis of Γ_k . It remains to show the security.

10 Example. It is possible to produce such Γ_k 's using pairwise anti-commuting Pauli strings. Indeed, if $K = 2n$, consider:

$\Gamma_k := X^{\otimes(k-1)} \otimes Y \otimes I^{\otimes(n-k)}$ and $\Gamma_{n+k} := X^{\otimes(k-1)} \otimes Z \otimes I^{\otimes(n-k)}$, for $k \in \{1, \dots, n\}$. Otherwise, if $K = 2n + 1$, consider the same operators and add $\Gamma_{2n+1} := X^{\otimes n}$.

11 Conjecture

This scheme is uncloneable-indistinguishable secure:

$$\mathbb{P}((P, B, C) \text{ win the game}) \leq \frac{1}{2} + \frac{1}{2\sqrt{K}}.$$

Remark. Here $K \sim 2\lambda$, but ideally $K \sim 2^\lambda$ (strong security).

3. Results

12 Proposition (Sufficient Formula)

To achieve the security of the Conjecture, it is sufficient to prove the following upper bound for all Hermitian unitaries $\{U_k\}$:

$$\left\| \underbrace{\sum_{k=1}^K (\Gamma_k \otimes U_k \otimes I + \Gamma_k \otimes I \otimes U_k + I \otimes U_k \otimes U_k)}_{=: W_K} \right\|_{\text{op}} \leq K + 2\sqrt{K}.$$

13 Remarks. The value $K + 2\sqrt{K}$ is achieved when considering $U_k = I$ for all k . Moreover, the formula trivially holds if we assume that the operators U_k commute.

14 Theorem 1

The Conjecture is valid for $K \leq 7$.

Proof. When $K \leq 7$, we find the following sum-of-squares (SoS) decomposition:

$$(K + 2\sqrt{K})I - W_K = \sum_{k=1}^K \alpha_k A_k^2$$

for some explicit coefficients $\alpha_k \geq 0$ and operators A_k . Hence $(K + 2\sqrt{K})I - W_K \succcurlyeq 0$ and therefore $K + 2\sqrt{K} \geq \|W_K\|_{\text{op}}$. \square

15 Numerical Results

The Conjecture is numerically confirmed for $K \leq 17$ (NPA level-2 algorithm) and $K \leq 18$ (Seesaw algorithm).

16 Theorem 2

Asymptotically, the winning probability of the no-cloning game for our candidate scheme is upper-bounded by $5/8$.

References

- [1] Ananth and Behera. "A Modular Approach to Uncloneable Cryptography". In: 2024. DOI: 10.1007/978-3-031-68394-7_1.
- [2] Ananth and Kaleoglu. "Uncloneable Encryption, Revisited". In: 2021. DOI: 10.1007/978-3-030-90459-3_11.
- [3] Ananth, Kaleoglu, Li, Liu, and Zhandry. "On the Feasibility of Uncloneable Encryption, and More". In: 2022. DOI: 10.1007/978-3-031-15979-4_8.
- [4] Ananth, Kaleoglu, and Liu. "Cloning Games: A General Framework for Uncloneable Primitives". In: 2023. DOI: 10.1007/978-3-031-38554-4_3.
- [5] Ananth, Kaleoglu, and Yuen. "Simultaneous Haar Indistinguishability with Applications to Uncloneable Cryptography". 2024. arXiv: 2405.10274.
- [6] Botteron, Broadbent, Culf, Nechita, Pellegrini, and Rochette. "Towards Unconditional Uncloneable Encryption". 2024. arXiv: 2410.23064.

- [7] Broadbent and Culf. "Uncloneable Cryptographic Primitives with Interaction". 2023. arXiv: 2303.00048.
- [8] Broadbent and Lord. "Uncloneable Quantum Encryption via Oracles". In: 2020. DOI: 10.4230/LIPICS.TQC.2020.4.
- [9] Chevalier, Hermouet, and Vu. "Towards Uncloneable Cryptography in the Plain Model". 2024. arXiv: 2311.16663.
- [10] George, Allertorfer, Verduyn Lunel, and Chitambar. "Orthogonality Broadcasting and Quantum Position Verification". 2025. arXiv: 2311.00677.
- [11] Georgiou and Zhandry. "Uncloneable Encryption Keys". 2020. URL: <https://eprint.iacr.org/2020/877>.
- [12] Kundu and Tan. "Device-independent uncloneable encryption". In: (2025). DOI: 10.22331/q-2025-01-08-1582.
- [13] Mehta and Müller. "Uncloneable Functional Encryption". 2024. arXiv: 2410.06029.
- [14] Poremba, Ragavan, and Vaikuntanathan. "Cloning Games, Black Holes and Cryptography". 2024. arXiv: 2411.04730.
- [15] Sattath and Wyborski. "Uncloneable Decryptors from Quantum Copy-Protection". 2022. arXiv: 2203.05866.



Scan the QR code to get the full paper