Does the Uncloneable Bit Exist?

Reference: arXiv:2410.23064 [1].

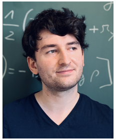
Pierre Botteron
(Toulouse & Ottawa)

Anne Broadbent
(Ottawa)

Eric Culf
(Waterloo)

Ion Nechita
(Toulouse)

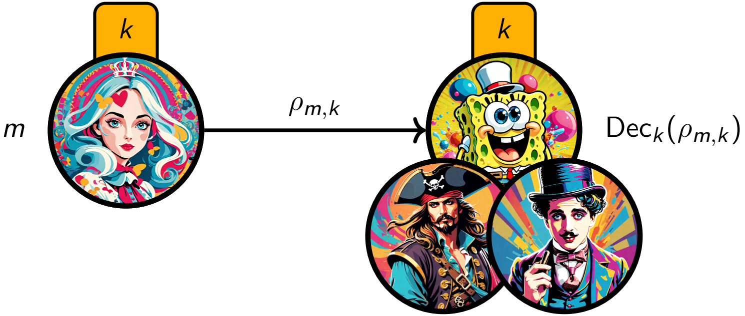
Clément Pellegrini
(Toulouse)



Denis Rochette
(Ottawa)

INTRIQ, May 13, 2025

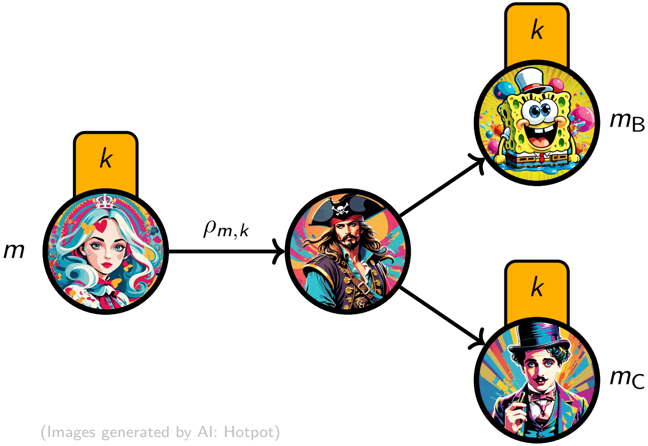
Uncloneable Bit



Correctness: $\forall m, \forall k, \quad \mathrm{Dec}_k(\rho_{m,k}) \overset{a.s.}{=} m.$

(Images generated by AI: Hotpot)

Uncloneable Bit



(Images generated by AI: Hotpot)

- **Rule:** The malicious team $(\mathrm{P}, \mathrm{B}, \mathrm{C})$ wins iff. $m_{\mathrm{B}} = m_{\mathrm{C}} = m$.
- **Def (Uncloneable-Indistinguishable Security):** The encryption scheme $(m, k) \mapsto \rho_{m,k}$ is said *weakly secure* if:

$$\mathbb{P}\Big((\mathrm{P}, \mathrm{B}, \mathrm{C}) \text{ win}\Big) \leqslant \frac{1}{2} + f(\lambda),$$

where $\lim f(\lambda) = 0$, and where λ is the security parameter. It is *strongly secure* if $f(\lambda) = \mathrm{negl}(\lambda)$.

- **Uncloneable Bit Problem (**Broadbent–Lord'20**):** Is there an encryption scheme $(m, k) \mapsto \rho_{m,k}$ that is both correct and strongly secure?

Candidate Scheme

Let $k \in \{1, .., K\}$. We construct a family $\{\Gamma_1, \dots, \Gamma_K\}$ of Hermitian unitaries that pairwise anti-commute. If K even, consider:

$$\Gamma_j := X^{\otimes(j-1)} \otimes Y \otimes I^{\otimes(\frac{K}{2}-j)} \quad \text{and} \quad \Gamma_{\frac{K}{2}+j} := X^{\otimes(j-1)} \otimes Z \otimes I^{\otimes(\frac{K}{2}-j)},$$

for any $j \in \{1, .., \frac{K}{2}\}$. If K odd, add $X^{\otimes \frac{K-1}{2}}$.

Candidate Scheme

For $m \in \{0, 1\}$ and $k \in \{1, .., K\}$, consider:

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

Security of the Candidate Scheme

Consider $W_K(U_1, .., U_K) := \sum_{k=1}^K \Big(\Gamma_k \otimes U_k \otimes I + \Gamma_k \otimes I \otimes U_k + I \otimes U_k \otimes U_k \Big)$.

Theorem 1

If for all Hermitian unitaries $U_1, .., U_K$:

$$\Big\| W_K(U_1, .., U_K) \Big\|_{\mathrm{op}} \leqslant K + 2\sqrt{K}\,, \tag{1}$$

then, the scheme defined by the Γ_k's is weakly secure:

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

Remark: The value $K + 2\sqrt{K}$ in eq. (1) is achieved when considering $U_k = I$ for all k. Moreover, eq. (1) easily holds if we assume that the operators U_k commute.

Partial Proof of Inequality (1)

Inequality (1): $\forall U_1, \dots, U_K, \quad \left\| W_K(U_1, .., U_K) \right\|_{\text{op}} \leqslant K + 2\sqrt{K}.$

Recall: $W_K(U_1, .., U_K) := \sum_{k=1}^{K} \left(\Gamma_k \otimes U_k \otimes I + \Gamma_k \otimes I \otimes U_k + I \otimes U_k \otimes U_k \right).$

Theorem 2

Inequality (1) is valid for small key sizes ($K \leqslant 7$).

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

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

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

Numerical Evidence for Larger Key Sizes

Inequality (1) is also numerically confirmed:

- at least until $K \leqslant 17$ with the NPA level-2 algorithm, and
- at least until $K \leqslant 18$ using the Seesaw algorithm.

The complete proof (for all $K \in \mathbb{N}$) is open.

Asymptotic Upper Bound

Theorem 3

In the asymptotic regime $K \to \infty$, the following upper bound holds:

$$\lim_{K\to\infty} \mathbb{P}\Big((\mathrm{P}, \mathrm{B}, \mathrm{C}) \text{ win the game}\Big) \leqslant \frac{5}{8}.$$

Proof Idea. Compute the analytical NPA hierarchy level 1. $\square$

Conclusion

Take Away

- We suggest the first encryption protocol in the plain model for the uncloneable bit problem. It expresses explicitly in terms of Pauli strings.
- We prove the weak security for small key sizes K.
- We provide strong numerical evidence that it should hold for all $K \in \mathbb{N}$.
- We obtain the asymptotic upper bound $5/8$ on the adversaries winning probability.

Other Recent Result

A different encryption scheme was recently suggested with different methods, using nonlocal games and 2-designs [Bhattacharyya–Culf'25]. The authors prove the weak security for all $K \in \mathbb{N}$.

Future Work

The uncloneable bit problem with *strong* security is still open.

Thank you!

Bibliography

[1] P. Botteron, A. Broadbent, E. Culf, I. Nechita, C. Pellegrini, and D. Rochette, "Towards unconditional uncloneable encryption," 2024. arXiv:2410.23064.

[2] A. Broadbent and S. Lord, "Uncloneable Quantum Encryption via Oracles," in *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, vol. 158, pp. 4:1–4:22, 2020. DOI: 10.4230/LIPIcs.TQC.2020.4.

[3] A. Bhattacharyya and E. Culf, "Uncloneable encryption from decoupling," 2025. arXiv:2503.19125.