# Towards the Unclonable Bit

Reference: arXiv:2410.23064 [1].

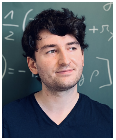

Pierre Botteron
(Toulouse & Ottawa)

Anne Broadbent
(Ottawa)

Eric Culf
(Waterloo)

Ion Nechita
(Toulouse)

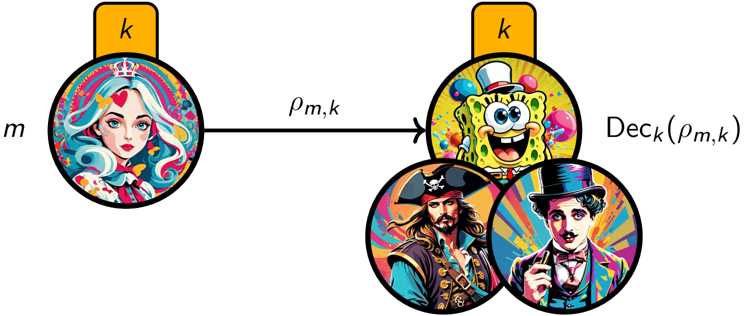
Clément Pellegrini
(Toulouse)



Denis Rochette
(Ottawa)


**QUORUM Ottawa**, April 30, 2025

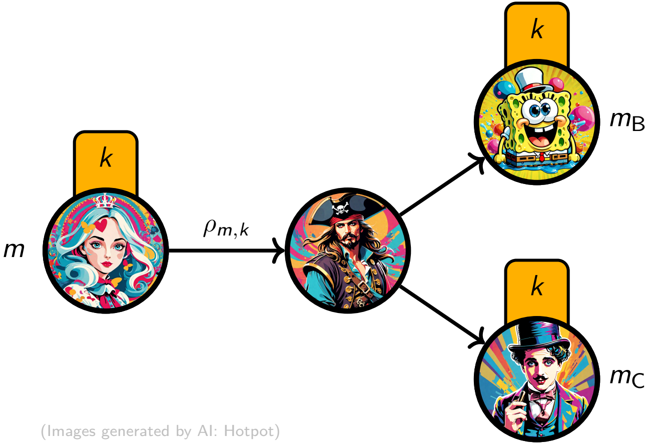
# Unclonable Bit




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

(Images generated by AI: Hotpot)

# Unclonable Bit




(Images generated by AI: Hotpot)

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

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

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

- **Open Question (**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 $\{\Gamma_1, \ldots, \Gamma_K\}$ 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

## Theorem 1

Consider $W_K(U_1,..,U_K) := \sum_{k=1}^K \Big(\Gamma_k \otimes U_k \otimes I + \Gamma_k \otimes I \otimes U_k + I \otimes U_k \otimes U_k\Big)$. If we have the following operator norm inequality for all Hermitian unitaries $U_1,..,U_K$:

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

then, the scheme is weakly secure:

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

## Theorem 2

Using sum-of-squares methods, equation (1) is valid for small key sizes ($K \leqslant 7$).

**Remark.** Equation (1) is also numerically confirmed for $K \leqslant 17$ (NPA level-2 algorithm) and $K \leqslant 18$ (Seesaw algorithm).

## Conclusion

- We proved the weak security for small $K$.
- The weak security was recently extended to any $K$ [Bhattacharyya–Culf'25].
- The 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.