Quantum Unclonable Cryptography: Does the Unclonable Bit Exist?

Reference: arXiv:2410.23064 [1].

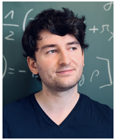
Pierre Botteron
(Toulouse & Ottawa)

Anne Broadbent
(Ottawa)

Eric Culf
(Waterloo)

Ion Nechita
(Toulouse)

Clément Pellegrini
(Toulouse)



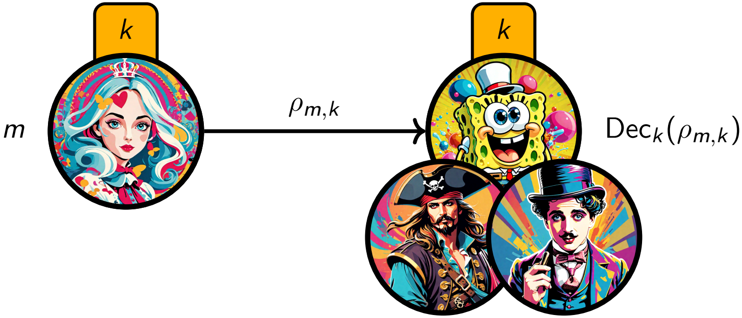
Denis Rochette
(Ottawa)

Lyon, June 25, 2025

— Part 1 —

The Unclonable Bit Problem

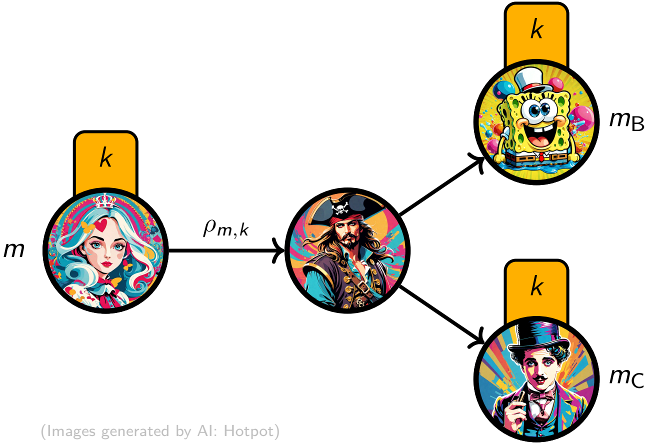
Scenario



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

(Images generated by AI: Hotpot)

Cloning Game



(Images generated by AI: Hotpot)

- **Rule:** The malicious team (P, B, C) wins iff. $m_{\mathrm{B}} = m_{\mathrm{C}} = m$.
- **Def (Unclonable-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 $f(\lambda) = \mathrm{negl}(\lambda)$.

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

Preliminary Upper Bouds

The winning probability at the no-cloning game is expressed as follows:

$$\mathbb{P}\Big((\mathsf{P},\mathsf{B},\mathsf{C})\text{ win}\Big) = \sup_{\substack{\Phi \\ \{B_{i|k}\},\{C_{j|k}\}}} \mathop{\mathbb{E}}_{\substack{m\in\{0,1\} \\ k\leftarrow \mathsf{Gen}(1^\lambda)}} \sum_{m_\mathsf{B},m_\mathsf{C}\in\{0,1\}} \mathbf{1}_{\{m_\mathsf{B}=m_\mathsf{C}=m\}} \operatorname{Tr}\Big[\Phi(\rho_{m,k})\big(B_{m_\mathsf{B}|k}\otimes C_{m_\mathsf{C}|k}\big)\Big]$$

$$= \sup_{\Phi,\{B_{i|k}\},\{C_{j|k}\}} \mathop{\mathbb{E}}_{m,k} \operatorname{Tr}\Big[\Phi(\rho_{m,k})\big(B_{m|k}\otimes C_{m|k}\big)\Big].$$

Using the Choi matrix C_Φ of the quantum channel Φ, we can rephrase it as follows:

$$\mathbb{P}\Big((\mathsf{P},\mathsf{B},\mathsf{C})\text{ win}\Big) = \sup_{C_\Phi,\{B_{i|k}\},\{C_{j|k}\}} \mathop{\mathbb{E}}_{m,k} \operatorname{Tr}\Big[C_\Phi\left(\rho_{m,k}^\top\otimes B_{m|k}\otimes C_{m|k}\right)\Big],$$

over all $C_\Phi \succcurlyeq \mathbf{0}$ such that $\operatorname{Tr}_{(\mathsf{B},\mathsf{C})}[C_\Phi] = \mathbb{I}_d$. Relax it into $\operatorname{Tr}[C_\Phi] = d$, and consider $\sigma := \frac{1}{d}C_\Phi$:

$$\mathbb{P}\Big((\mathsf{P},\mathsf{B},\mathsf{C})\text{ win}\Big) \leqslant \sup_{\sigma,\{B_{i|k}\},\{C_{j|k}\}} \mathop{\mathbb{E}}_{m,k} \operatorname{Tr}\Big[\sigma\left(d\cdot\rho_{m,k}^\top\otimes B_{m|k}\otimes C_{m|k}\right)\Big],$$

over all $\sigma \succcurlyeq \mathbf{0}$ such that $\operatorname{Tr}[\sigma] = 1$.

Recall: $\mathbb{P}\Big((\mathsf{P},\mathsf{B},\mathsf{C}) \text{ win}\Big) \leqslant \sup_{\sigma,\{B_{i|k}\},\{C_{j|k}\}} \mathbb{E}_{m,k} \operatorname{Tr}\Big[\sigma\left(d \cdot \rho_{m,k}^{\top} \otimes B_{m|k} \otimes C_{m|k}\right)\Big]$.

By linearity in σ and convexity of the set of quantum states, we may assume $\sigma = |\psi\rangle\langle\psi|$:

$$\mathbb{P}\Big((\mathsf{P},\mathsf{B},\mathsf{C}) \text{ win}\Big) \leqslant \sup_{\psi,\{B_{i|k}\},\{C_{j|k}\}} \langle\psi| \mathbb{E}_{m,k}\left[d \cdot \rho_{m,k}^{\top} \otimes B_{m|k} \otimes C_{m|k}\right]|\psi\rangle \leqslant \sup_{\{B_{i|k}\},\{C_{j|k}\}} \left\|\mathbb{E}_{m,k}\left[d \cdot \rho_{m,k}^{\top} \otimes B_{m|k} \otimes C_{m|k}\right]\right\|_{\mathrm{op}}.$$

By Naimark's Dilation theorem, we may assume that the POVMs $\{B_{i|k}\}_i$ and $\{C_{j|k}\}_j$ are PVMs. Moreover, the adversaries Bob and Charlie can always be *symmetrized*: same space $(\mathcal{H}_{\mathsf{B}},\mathcal{H}_{\mathsf{C}}) \mapsto \mathcal{H}_{\mathsf{B}} \oplus \mathcal{H}_{\mathsf{C}}$ and same PVMs $\left(\{B_{i|k}\}_i,\{C_{j|k}\}_j\right) \mapsto \{B_{i|k} \oplus C_{i|k}\}_i =: \{M_{i|k}\}_i$. Hence:

$$\mathbb{P}\Big((\mathsf{P},\mathsf{B},\mathsf{C}) \text{ win}\Big) \leqslant \sup_{\{M_{i|k}\}} \left\|\mathbb{E}_{m,k}\left[d \cdot \rho_{m,k}^{\top} \otimes M_{m|k} \otimes M_{m|k}\right]\right\|_{\mathrm{op}}.$$

Finally, by writing $U_k := M_{0|k} - M_{1|k}$, we have $M_{m|k} = \frac{\mathbb{I}_D + (-1)^m U_k}{2}$ and therefore:

$$\boxed{\mathbb{P}\Big((\mathsf{P},\mathsf{B},\mathsf{C}) \text{ win}\Big) \leqslant \sup_{\{U_k\}} \frac{1}{2K} \left\|\sum_{m,k} d \cdot \rho_{m,k}^{\top} \otimes \frac{\mathbb{I}_D + (-1)^m U_k}{2} \otimes \frac{\mathbb{I}_D + (-1)^m U_k}{2}\right\|_{\mathrm{op}}},$$

over all U_k Hermitian unitaries.

— Part 2 —

Candidate Scheme

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:

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

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:

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

Observation

This scheme is correct.

Proof. Given k and $\rho_{m,k}$, measure $\rho_{m,k}$ in an eigenbasis of Γ_k. Obtain 1 or -1, and recover the value of m. □

Further Upper Bounds

We plug the formula $\rho_{m,k} := \frac{2}{d}\,\frac{\mathbb{I}_d+(-1)^m\,\Gamma_k}{2}$ into the former upper bound:

$$\mathbb{P}\Big((\mathrm{P},\mathrm{B},\mathrm{C})\text{ win}\Big) \leqslant \sup_{\{U_k\}} \frac{1}{2K} \left\| \sum_{m,k} d\cdot\frac{2}{d}\,\frac{\mathbb{I}_d+(-1)^m\,\Gamma_k}{2} \otimes \frac{\mathbb{I}_D+(-1)^m U_k}{2} \otimes \frac{\mathbb{I}_D+(-1)^m U_k}{2} \right\|_{\mathrm{op}} .$$

over all U_k Hermitian unitaries. We develop and we get:

$$\mathbb{P}\Big((\mathrm{P},\mathrm{B},\mathrm{C})\text{ win}\Big) \leqslant \frac{1}{4} + \frac{1}{4K} \sup_{\{U_k\}} \Bigg\| \underbrace{\sum_{k=1}^{K} \Big(\Gamma_k\otimes U_k\otimes \mathbb{I}_D + \Gamma_k\otimes\mathbb{I}_D\otimes U_k + \mathbb{I}_d\otimes U_k\otimes U_k\Big)}_{=:W_K(U_1,\ldots,U_K)} \Bigg\|_{\mathrm{op}} .$$

Remark. *With a naive triangular inequality, we obtain the following trivial upper bound:*

$$\mathbb{P}\Big((\mathrm{P},\mathrm{B},\mathrm{C})\ \mathit{win}\Big) \leqslant \frac{1}{4} + \frac{1}{4K}\cdot 3K = 1 .$$

— *Part 3* —

Security of the Candidate Scheme

Sufficient Condition for the Weak Security

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

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:

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

Now, we want to prove:

Conjecture

Let $K \geqslant 2$ be an integer, $\Gamma_1, .., \Gamma_K$ Hermitian unitaries that pairwise anti-commute, and $U_1, .., U_K$ Hermitian unitaries. Then:

$$\sup_{\{\Gamma_k\},\{U_k\}} \left\| \sum_{k=1}^{K} \left(\Gamma_k \otimes U_k \otimes \mathbb{I} + \Gamma_k \otimes \mathbb{I} \otimes U_k + \mathbb{I} \otimes U_k \otimes U_k \right) \right\|_{\mathrm{op}} \leqslant K + 2\sqrt{K}\,.$$

Observation 1

The value $K + 2\sqrt{K}$ is achieved when considering $U_k = \mathbb{I}$ for all k.

Proof. $\left\|\sum_k (2\Gamma_k + \mathbb{I})\right\|_{\mathrm{op}} = \left\|2(\sum_k \Gamma_k) + K\,\mathbb{I}\right\|_{\mathrm{op}} = 2\left\|\sum_k \Gamma_k\right\|_{\mathrm{op}} + K = 2\sqrt{K} + K.$ □

True in the Commuting Case

Observation 2

The Conjecture holds if we assume that the operators U_k commute.

Proof. If the operators U_k commute, then they are diagonalizable in a common basis. But they are Hermitian and unitaries, so their eigenvalues are ± 1 and we may assume:

$$U_k = \begin{pmatrix} \pm 1 & & \\ & \ddots & \\ & & \pm 1 \end{pmatrix} .$$

Then, using the triangular inequality, we obtain:

$$\begin{aligned} \|W_K\|_{\text{op}} &\leqslant \left\| \sum_{k=1}^{K} \Gamma_k \otimes (\pm 1) \otimes 1 \right\|_{\text{op}} + \left\| \sum_{k=1}^{K} \Gamma_k \otimes 1 \otimes (\pm 1) \right\|_{\text{op}} + \sum_{k=1}^{K} \left\| \begin{pmatrix} \pm 1 & & \\ & \ddots & \\ & & \pm 1 \end{pmatrix} \right\|_{\text{op}} \\ &= \left\| \sum_{k=1}^{K} \Gamma_k \right\|_{\text{op}} + \left\| \sum_{k=1}^{K} \Gamma_k \right\|_{\text{op}} + \sum_{k=1}^{K} 1 = \sqrt{K} + \sqrt{K} + K . \quad \square \end{aligned}$$

Conjecture in the General Case

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

Conjecture: $\forall U_1, ..., U_K, \quad \Big\| W_K(U_1, .., U_K) \Big\|_{\mathrm{op}} \leqslant K + 2\sqrt{K}$.

Theorem 2

The Conjecture is valid for small key sizes ($K \leqslant 7$).

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

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

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

Numerical Evidence for Larger Key Sizes

The Conjecture is also numerically confirmed:
- at least for $K \leqslant 17$ with the NPA level-2 algorithm, and
- at least for $K \leqslant 18$ 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:

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

Proof Idea. Compute the analytical NPA hierarchy level 1. □

Conclusion

Take Away

- We suggest the first encryption protocol in the plain model for the unclonable 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.

More 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 unclonable 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.