Nonlocal Games Through Communication Complexity and Quantum Cryptography

Ph.D. defense

Pierre Botteron (Université de Toulouse)
Under the joint supervision of Dr. Anne Broadbent,
Dr. Ion Nechita, and Dr. Clément Pellegrini.

Toulouse, July 9, 2025

Manuscripts in this Thesis

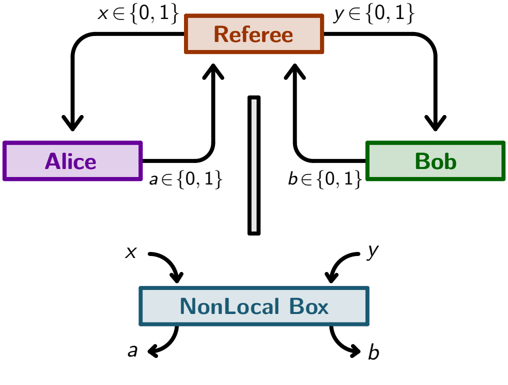
- P. Botteron, A. Broadbent, and M.-O. Proulx, "Extending the known region of nonlocal boxes that collapse communication complexity," *Physical Review Letters*, vol. 132, p. 070201, 02 (2024).
- P. Botteron, A. Broadbent, R. Chhaibi, I. Nechita, and C. Pellegrini, "Algebra of Nonlocal Boxes and the Collapse of Communication Complexity," *Quantum*, vol. 8, p. 1402, 07 (2024).
- P. Botteron and M. Weber, "Communication complexity of graph isomorphism, coloring, and distance games," arXiv:2406.02199 (2024).
- P. Botteron, A. Broadbent, E. Culf, I. Nechita, C. Pellegrini, and D. Rochette, "Towards unconditional uncloneable encryption," arXiv:2410.23064 (2024).

Contents

— Part 1 —

Background Notions

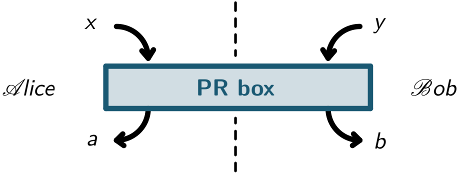
The Clauser–Horne–Shimony–Holt Game



Win at CHSH $\iff$ $a \oplus b = x\,y$.

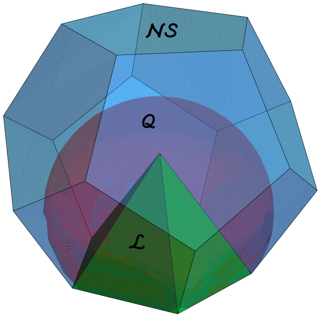
- **Strategy.** Conditional probability distribution:
$$\mathcal{S} = \Big\{ \mathrm{P} : \{0,1\}^4 \to \mathbb{R} \,:\, \mathrm{P}(a,b\,|\,x,y) \geqslant 0 \text{ and } \textstyle\sum_{a,b} \mathrm{P}(a,b\,|\,x,y) = 1 \Big\}.$$
- **Deterministic Strategies.**
$$\mathcal{L}_{\text{det}} := \Big\{ \mathrm{P} \in \mathcal{S} \,:\, \exists f, g \text{ s.t. } a = f(x) \text{ and } b = g(y) \Big\}.$$
$\rightsquigarrow \max_{\mathrm{P} \in \mathcal{L}_{\text{det}}} \mathbb{P}(\mathrm{P} \text{ win}) = 75\%.$
- **Classical Strategies.**
$$\mathcal{L} := \Big\{ \mathrm{P} = \textstyle\sum_i \lambda_i \mathrm{P}_i \,:\, \lambda_i \geqslant 0, \sum_i \lambda_i = 1, \mathrm{P}_i \in \mathcal{L}_{\text{det}} \Big\}.$$
$\rightsquigarrow \max_{\mathrm{P} \in \mathcal{L}} \mathbb{P}(\mathrm{P} \text{ win}) = 75\%.$
- **Quantum Strategies.**
$$\mathcal{Q} := \Big\{ \mathrm{P} = \langle \psi | E_{a|x} \otimes F_{b|y} | \psi \rangle \,:\, \begin{array}{c} |\psi\rangle \text{ is a quantum state} \\ \{E_{a|x}\} \,\&\, \{F_{b|y}\} \text{ are q. meas.} \end{array} \Big\}.$$
$\rightsquigarrow \max_{\mathrm{P} \in \mathcal{Q}} \mathbb{P}(\mathrm{P} \text{ win}) = \cos^2\left(\frac{\pi}{8}\right) \approx 85\%.$
- **Non-Signaling Strategies.**
$$\mathcal{NS} := \Big\{ \mathrm{P} \in \mathcal{S} : \textstyle\sum_a \mathrm{P}(a,b|x,y) = \mathrm{P}(b|y), \sum_b \mathrm{P}(a,b|x,y) = \mathrm{P}(a|x) \Big\}.$$
$\rightsquigarrow \max_{\mathrm{P} \in \mathcal{NS}} \mathbb{P}(\mathrm{P} \text{ win}) = 100\%.$

The Popescu–Rohrlich Box

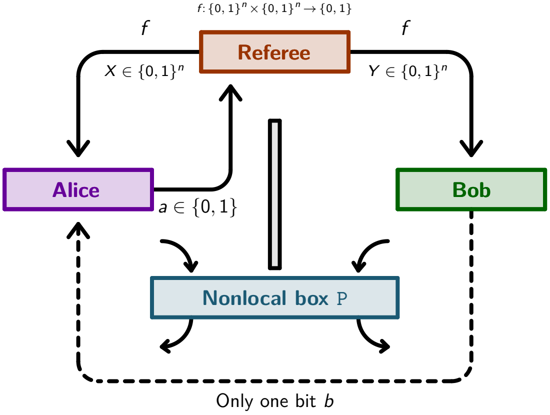


such that $a \oplus b = xy$.

$$\mathtt{PR}(a, b \mid x, y) := \frac{1}{2} \mathbf{1}_{a \oplus b = xy} .$$



Collapse of Communication Complexity



Win $\iff a = f(X,Y)$.

Def. *A function f is said to be* **trivial** *(in the sense of communication complexity) if Alice correctly guesses any value $f(X,Y)$ with only one bit transmitted from Bob to Alice, for any X and Y.*

Ex. For $n=2$, $X=(x_1,x_2)$, $Y=(y_1,y_2)$:

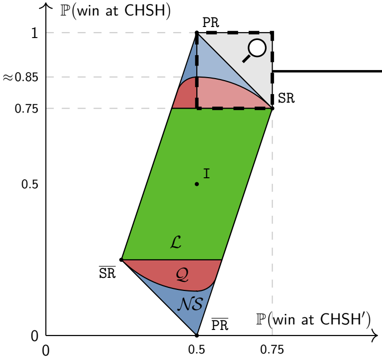
- $f := x_1 \oplus y_1 \oplus x_2 \oplus y_2 \oplus 1$ is trivial.
- $g := (x_1\, x_2) \oplus (y_1\, y_2)$ is trivial.
- $h := (x_1\, y_1) \oplus (x_2\, y_2)$ is NOT trivial.

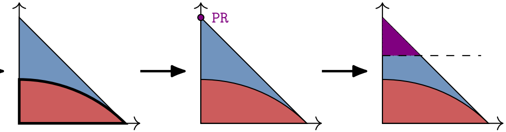
Def. *We say that a nonlocal box* P **collapses CC** *if $\exists\, \mathfrak{p} > 1/2$ such that $\forall n\in\mathbb{N}$, $\forall f : \{0,1\}^{2n}\to\{0,1\}$, and $\forall X,Y\in\{0,1\}^n$, we have:*

$$\mathbb{P}(a = f(X,Y)\,|\,X,Y,\mathrm{P}) \geqslant \mathfrak{p}\,.$$

Ex.
- The PR box is collapsing [van Dam'99].
- Local ($\mathcal{L}$) and quantum ($\mathcal{Q}$) boxes are NOT collapsing [Cleve *et al.*'99].

Collapse of Communication Complexity

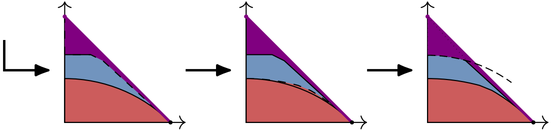




1999: Quantum boxes are **non-collapsing** [4].

1999: The PR box is **collapsing** [5].

2006: **Collapsing** region above ≈ 0.91 [6].



2009–2024: The thickened diagonal is **collapsing** (numerical results) [2, 3, 7, 8].

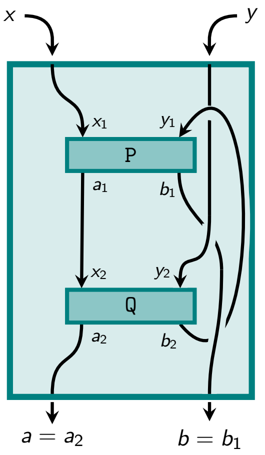
2015: Almost quantum boxes are **non-collapsing** [9].

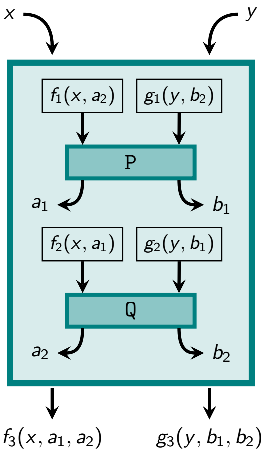
2024: **Collapsing** region above an ellipse (analytical result) [10].

— *Part* 2 —

Algebra of Boxes

Wiring of Nonlocal Boxes





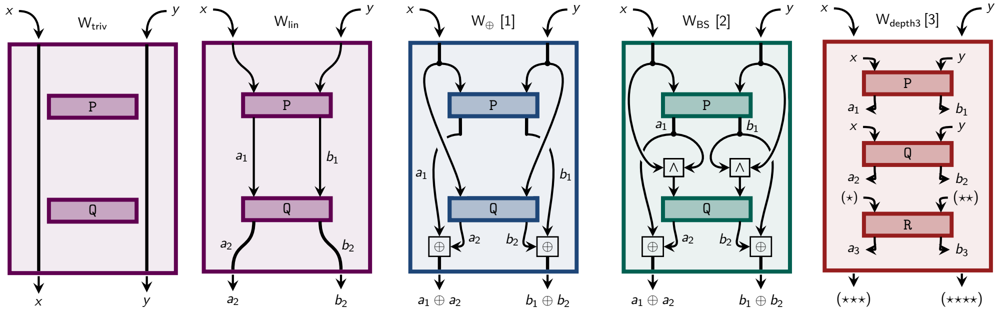
Definition. A **wiring** W between two boxes $\mathtt{P}, \mathtt{Q} \in \mathcal{NS}$ consists in six functions $f_1, f_2, g_1, g_2 : \{0,1\}^2 \to [0,1]$ and $f_3, g_3 : \{0,1\}^3 \to [0,1]$ satisfying the *non-cyclicity conditions* for all x, y:

$$f_1(x,0) \neq f_1(x,1) \Rightarrow f_2(x,0) = f_2(x,1),$$
$$f_2(x,0) \neq f_2(x,1) \Rightarrow f_1(x,0) = f_1(x,1),$$

and similarly for g_1, g_2.
The new box is denoted:

$$\mathtt{P} \boxtimes_{\mathrm{W}} \mathtt{Q} \in \mathcal{NS}\,.$$

Examples of Wirings in the Literature



where $\overline{x} := x \oplus 1$; $(\star) := xa_2 \vee x\overline{a_1} \vee \overline{x}\,\overline{a_2}a_1$; $(\star\star) := yb_2 \vee y\overline{b_1}$;

$(\star\star\star) := a_3a_2 \vee a_3\overline{a_1} \vee \overline{a_3}\,\overline{a_2}a_1$; and $(\star\star\star\star) := b_3b_2 \vee b_3\overline{b_1} \vee \overline{b_3}\,\overline{b_2}b_1$.

Algebra of Boxes

Observation: Given a wiring $\mathtt{W} = (f_1, g_1, f_2, g_2, f_3, g_3)$, the map $(\mathtt{P}, \mathtt{Q}) \mapsto \mathtt{P} \boxtimes_{\mathtt{W}} \mathtt{Q}$ is bilinear:

$$\mathtt{P} \boxtimes_{\mathtt{W}} \mathtt{Q}\big(a, b \,|\, x, y\big) := \sum_{a_1, a_2, b_1, b_2} \mathtt{P}\big(a_1,\ b_1 \,|\, f_1(x, a_2),\ g_1(y, b_2)\big) \\ \times \mathtt{Q}\big(a_2,\ b_2 \,|\, f_2(x, a_1),\ g_2(y, b_1)\big) \times \mathbf{1}_{a=f_3(x,a_1,a_2)} \times \mathbf{1}_{b=g_3(y,b_1,b_2)}\,.$$

$\Rightarrow$ The vector space $\mathcal{B}_{\mathtt{W}} := \big(\{boxes\}, \boxtimes_{\mathtt{W}}\big)$ is an algebra, that we call the **algebra of boxes**.

Proposition (B.–Broadbent–Chhaibi–Nechita–Pellegrini'24)

Assume W is a wiring such that $f_1 = f_2 = f(x)$ and $g_1 = g_2 = g(y)$. Then:

1. $\mathcal{B}_{\mathtt{W}}$ is commutative $\iff$ $f_3(x, a_1, a_2) = f_3(x, a_2, a_1)$ and $g_3(y, b_1, b_2) = g_3(y, b_2, b_1)$.

If in addition $f(x) = x$ and $g(y) = y$:

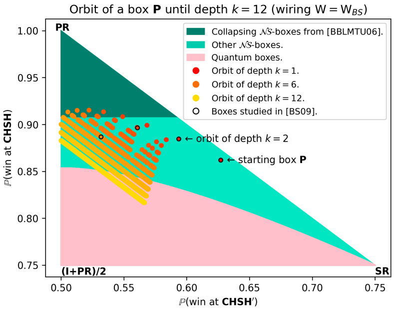
2. $\mathcal{B}_{\mathtt{W}}$ is associative $\iff$ $f_3(x, a_1, f_3(x, a_2, a_3)) = f_3(x, f_3(x, a_1, a_2), a_3)$ and $g_3(y, b_1, g_3(y, b_2, b_3)) = g_3(y, g_3(y, b_1, b_2), b_3)$.

Orbit of a Box

$$\mathrm{Orbit}_{\mathrm{W}}^{(3)}(\mathrm{P}) = \left\{ (\mathrm{P} \boxtimes \mathrm{P}) \boxtimes \mathrm{P},\ \mathrm{P} \boxtimes (\mathrm{P} \boxtimes \mathrm{P}) \right\},$$

$$\mathrm{Orbit}_{\mathrm{W}}^{(4)}(\mathrm{P}) = \Big\{ \big((\mathrm{P}\boxtimes\mathrm{P})\boxtimes\mathrm{P}\big)\boxtimes\mathrm{P},\ \big(\mathrm{P}\boxtimes(\mathrm{P}\boxtimes\mathrm{P})\big)\boxtimes\mathrm{P},\ (\mathrm{P}\boxtimes\mathrm{P})\boxtimes(\mathrm{P}\boxtimes\mathrm{P}),\ \mathrm{P}\boxtimes\big((\mathrm{P}\boxtimes\mathrm{P})\boxtimes\mathrm{P}\big),\ \mathrm{P}\boxtimes\big(\mathrm{P}\boxtimes(\mathrm{P}\boxtimes\mathrm{P})\big) \Big\},$$

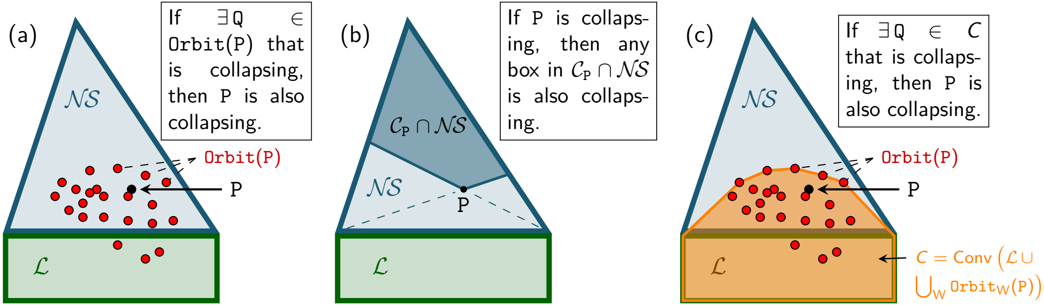
$\mathrm{Orbit}_{\mathrm{W}}^{(k)}(\mathrm{P}) := \big\{$ all possible products with k times the term P, using the multiplication $\boxtimes_{\mathrm{W}}$ $\big\}$.



Theorem (B.–Broadbent–Chhaibi–Nechita–Pellegrini'24)

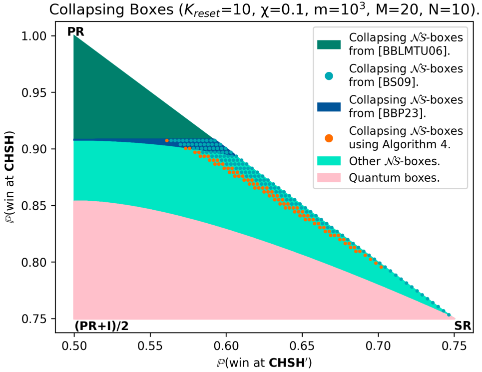
For fixed k, the points of the k-orbit are aligned, and the highest CHSH-value is achieved by the parenthesization with multiplication only on the right: $\mathrm{P}^{\boxtimes k} := \Big(\big((\mathrm{P} \boxtimes \mathrm{P}) \boxtimes \mathrm{P}\big) \cdots \Big) \boxtimes \mathrm{P}\,.$

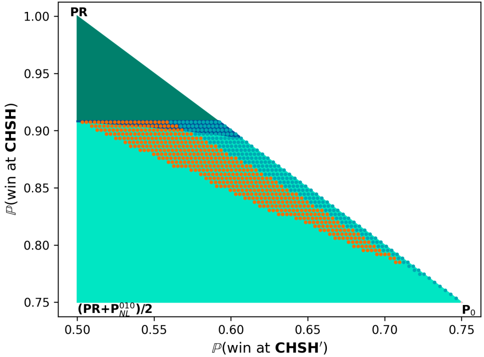
Here is the consequence to Communication Complexity:



Numerical Results

Using a gradient descent algorithm, we obtain in **orange** new collapsing boxes (this result is similar to the independent and concurrent work of [Eftaxias et al.'23] [3]):





Collapse of CC from Multiplication Tables

Theorem (B.–Broadbent–Chhaibi–Nechita–Pellegrini'24)

Let $\mathtt{Q}, \mathtt{R} \in \mathcal{NS}$ be boxes. Assume there exists a wiring $\mathsf{W} \in \mathcal{W}$ that induces the following multiplication table:

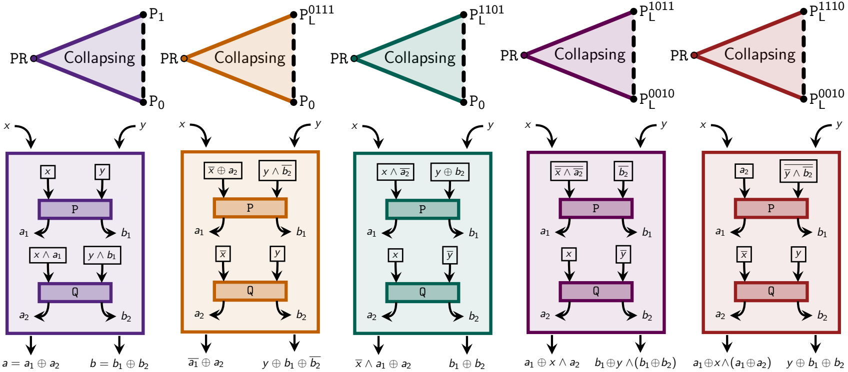
	$\mathtt{PR}$	$\mathtt{Q}$	$\mathtt{R}$
$\mathtt{PR}$	$\mathtt{PR}$	$\mathtt{PR}$	$\mathtt{PR}$
$\mathtt{Q}$	$\frac{1}{2}\left(\mathtt{Q}+\mathtt{R}\right)$	$\mathtt{Q}$	$\mathtt{R}$
$\mathtt{R}$	$\mathtt{PR}$	$\mathtt{R}$	$\mathtt{Q}$

Then the triangle $\mathrm{Conv}\{\mathtt{PR}, \mathtt{Q}, \mathtt{R}\} \setminus \mathrm{Conv}\{\mathtt{Q}, \mathtt{R}\}$ is collapsing.

Collapse of CC

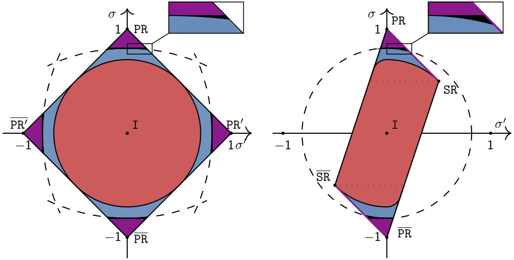
Corollary (B.–Broadbent–Chhaibi–Nechita–Pellegrini'24)

All the triangles drawn below are collapsing.

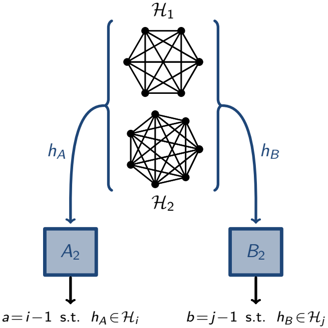


Examples of Other Methods to Collapse CC

B.–Broadbent–Proulx, PRL:132 (7 2024) [10].
Using bias amplification by majority function, one can prove that all the boxes above an explicit ellipse collapse CC:



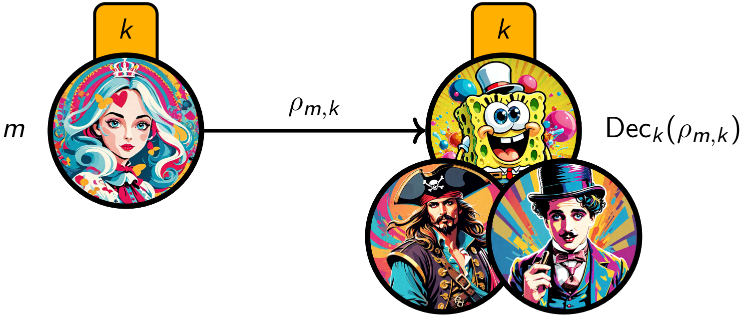
B.–Weber, arXiv:2406.02199 [11].
In other nonlocal games related to graphs, one can show that some non-signaling correlations collapse CC:



— *Part 3* —

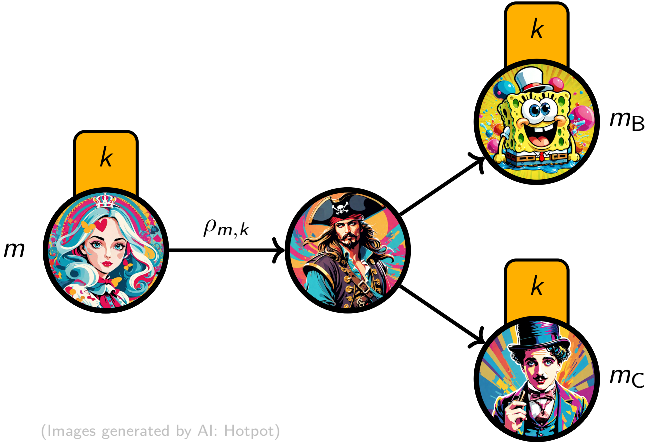
Unclonable Bit

Scenario



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

No-Cloning Game



(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 (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?

Mathematical Translation

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

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

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

Goal

Find the most secure encryption scheme against the strongest attack, *i.e.* solve:

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

Candidate Scheme

Let $k \in \{1, .., K\}$. Consider a family $\{\Gamma_1, \ldots, \Gamma_K\}$ that is:

- Hermitian (*i.e.* $\Gamma_k^\dagger = \Gamma_k$ for all k); and
- Unitary (*i.e.* $\Gamma_K^\dagger \Gamma_k = \Gamma_K \Gamma_k^\dagger = \mathbb{I}$ for all k); and
- Pairwise anti-commuting (*i.e.* $\Gamma_k \Gamma_j = -\Gamma_j \Gamma_k$ for all $j \neq k$).

Why? Because then $\left\| \sum_{k=1}^K v_k \Gamma_k \right\|_{\mathrm{op}} = \|v\|_2$ for any $v = (v_1, .., v_K) \in \mathbb{R}^K$, and in particular:

$$\left\| \sum_{k=1}^K \Gamma_k \right\|_{\mathrm{op}} = \left\| (1, .., 1) \right\|_2 = \sqrt{1^2 + \cdots + 1^2} = \sqrt{K}.$$

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. □

Upper Bound on the Winning Probability

Using the candidate scheme, we obtain the following upper bound on the *best* winning probability (where the U_k are Hermitian unitaries):

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

Theorem
(B.–Broadbent–Culf–Nechita–Pellegrini–Rochette'24)

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

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

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, $\Gamma_1, .., \Gamma_K$ be Hermitian unitaries that pairwise anti-commute, and $U_1, .., U_K$ be Hermitian unitaries. Then:

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

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:

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

Conjecture in the General Case

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

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

Theorem (B.–Broadbent–Culf–Nechita–Pellegrini–Rochette'24)

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.

Conclusion

Conclusion

Summary

- We prove the collapse of communication using various methods: wiring of boxes, bias amplification, and graph properties.
- We propose a candidate scheme for the unclonable bit problem in the plain model. We partially prove the weak security and provide numerical evidence that it holds for any key size.

Future Work

- Find other methods to discard non-physical correlations using communication complexity or any other information-based principle.
- Study the strong security in the unclonable bit problem.

Thank you!

Bibliography

[1] M. Forster, S. Winkler, and S. Wolf, "Distilling nonlocality," *Phys. Rev. Lett.*, vol. 102, Mar. 2009.

[2] N. Brunner and P. Skrzypczyk, "Nonlocality distillation and postquantum theories with trivial communication complexity," *Phys. Rev. Lett.*, vol. 102, Apr. 2009.

[3] G. Eftaxias, M. Weilenmann, and R. Colbeck, "Advantages of multicopy nonlocality distillation and its application to minimizing communication complexity," *Phys. Rev. Lett.*, vol. 130, Mar. 2023.

[4] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, *Quantum Entanglement and the Communication Complexity of the Inner Product Function*, pp. 61–74. Springer Berlin Heidelberg, 1999.

[5] W. van Dam, *Nonlocality & Communication Complexity*. Ph.d. thesis., University of Oxford, Departement of Physics, 1999.

[6] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger, "Limit on nonlocality in any world in which communication complexity is not trivial," *Phys. Rev. Lett.*, vol. 96, June 2006.

[7] P. Botteron, A. Broadbent, R. Chhaibi, I. Nechita, and C. Pellegrini, "Algebra of Nonlocal Boxes and the Collapse of Communication Complexity," *Quantum*, vol. 8, p. 1402, 07 2024.

[8] S. G. A. Brito, M. G. M. Moreno, A. Rai, and R. Chaves, "Nonlocality distillation and quantum voids," *Phys. Rev. A*, vol. 100, July 2019.

[9] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín, "Almost quantum correlations," *Nature Communications*, vol. 6, Feb. 2015.

[10] P. Botteron, A. Broadbent, and M.-O. Proulx, "Extending the known region of nonlocal boxes that collapse communication complexity," *Phys. Rev. Lett.*, vol. 132, p. 070201, 02 2024.

[11] P. Botteron and M. Weber, "Communication complexity of graph isomorphism, coloring, and distance games," 2024. arXiv:2406.02199.

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