arXiv:2410.23064v2 [quant-ph] 25 Jun 2026

Towards Unconditional Uncloneable Encryption

Pierre Botteron [1], Anne Broadbent [2], Eric Culf[3], Ion Nechita [4], Clément Pellegrini[1], and Denis Rochette [2]

[1]Institut de Mathématiques de Toulouse, Université de Toulouse, UPS, France.
[2]Department of Mathematics and Statistics, University of Ottawa, Ottawa, Canada.
[3]Institute for Quantum Computing, University of Waterloo, Waterloo, Canada.
[4]Laboratoire de Physique Théorique, Université de Toulouse, UPS, France.

Uncloneable encryption is a cryptographic primitive which encrypts a classical message into a quantum ciphertext, such that two quantum adversaries are limited in their capacity of being able to simultaneously decrypt, given the key and quantum side-information produced from the ciphertext. Since its initial proposal and scheme in the random oracle model by Broadbent and Lord [TQC 2020], uncloneable encryption has developed into an important primitive at the foundation of quantum uncloneability for cryptographic primitives. Despite sustained efforts, however, the question of unconditional uncloneable encryption (and in particular of the simplest case, called an "uncloneable bit") has remained elusive. Here, we propose a candidate for the unconditional uncloneable bit problem, and provide strong evidence that the adversary's success probability in the related security game converges quadratically as $\frac{1}{2} + \frac{1}{2\sqrt{K}}$, where K is polynomial in the size of the encoding, representing the number of keys and $\frac{1}{2}$ is trivially achievable. We prove this bound's validity for K ranging from 2 to 7 and demonstrate the validity up to $K = 17$ using computations based on the NPA hierarchy. We furthermore provide compelling heuristic evidence towards the general case. In addition, we prove an asymptotic upper-bound of $\frac{5}{8}$ and give a numerical upper-bound of ~ 0.5980, which to our knowledge is the best-known value in the unconditional model.

Contents

1 Introduction **2**
1.1 Results . . . 3
1.2 Future Work . . . 5
1.3 Organization of the Paper . . . 5

2 Preliminaries **5**
2.1 Uncloneable Encryption . . . 6
2.2 Bound for Unconditional No-Cloning Game . . . 7
2.3 Link with Monogamy-of-Entanglement Games . . . 8

3 Candidate Scheme **9**
3.1 Clifford Algebra . . . 10
3.2 Definition of the Scheme . . . 10
3.3 Conjecture . . . 11
3.4 Basic Properties . . . 12
3.5 Indistinguishability . . . 14

4 Analytical and Numerical Results for Conjecture 1 **15**
4.1 Elementary Proofs for $K = 2$ . . . 16
4.2 Proofs for $K \leqslant 7$ and Asymptotic Upper-Bound . . . 17
4.3 Numerical Result with NPA Hierarchy Level 2 for $K \leqslant 17$ . . . 21
4.4 Numerical Result with the Alternating Optimization Algorithm . . . 23

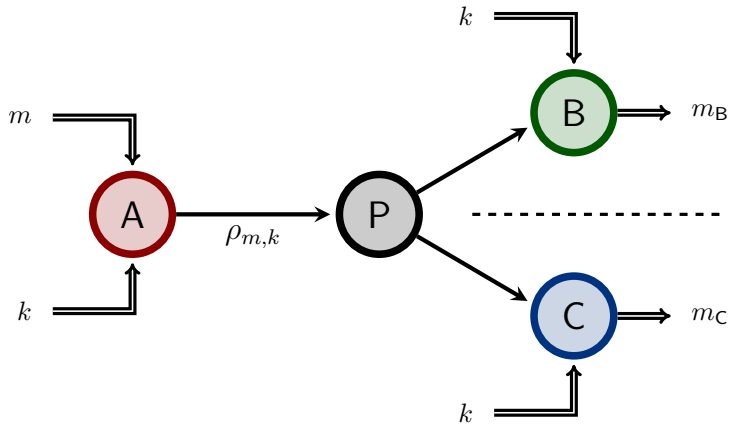


Figure 1. *No-Cloning Game for a 1-Bit Message.* Alice (A) encrypts a uniformly random message $m \in \{0,1\}$ using a classical key $k \in \{1,..,K\}$ into a quantum state $\rho_{m,k} \in \mathcal{B}(\mathcal{H}_A)$. She transmits it to a pirate (P) modeled by a CPTP map $\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B \otimes \mathcal{H}_C)$. Bob (B) and Charlie (C) are then given their respective registers $\mathcal{H}_B$ and $\mathcal{H}_C$, as well as a copy of the key k. They output m_B, $m_C \in \{0,1\}$, respectively, and *collaboratively win* if and only if $m_B = m_C = m$. *Uncloneable-indistinguishable security* holds if the winning probability is upper-bounded by $1/2 + \mathrm{negl}(\lambda)$ for some security parameter λ.

1 Introduction

Uncloneable encryption is an encryption scheme for classical messages into quantum ciphertexts that inherently protects the underlying plaintext from cloning, as defined by a security game that pits a triple of adversaries (P, B, C) against an honest sender A (see Figure 1). Clearly, such unclonability is unattainable with classical ciphertexts since P can send two copies of the classical ciphertext and, given the decryption key, B and C can decrypt in a straightforward way.

Originally proposed by Broadbent and Lord [BL20] who showed its achievability in the quantum random oracle model, (and under a less stringent definition called *uncloneable security*), uncloneable encryption has become an important building block for quantum cryptography, including for private-key quantum money [BL20], preventing storage attacks [BL20], quantum functional encryption [MM24], quantum copy-protection [AK21], quantum position verification [GALC25], and uncloneable decryption [GZ20, SW22, KT25].

Given the importance of uncloneable encryption, efforts have focused on its achievability under various models and definitions, including achievability in the quantum random oracle model (QROM) [BL20, AKL+22, AKL23], in an interactive version of the scenario [BC23b], in a device-independent variant with variable keys [KT25], assuming the existence of specific types of obfuscation [AB24, CHV24], and in a variant with quantum keys [AKY25].

Many open questions remain in the study of uncloneable cryptography, notably the achievability of a scheme that provides *uncloneable-indistinguishability* security in the sense originally defined in [BL20]: the security definition considers a game of the form of Figure 1, but where a message $m \in \{0,1\}^n$ is selected by the adversary, and the challenge that the adversaries B and C face is to identify if the original message m, or a fixed message 0^n, was encrypted, where the two cases happen with equal probability. In this scenario, limitations on possible schemes have been identified [MST21, AKL+22]. Notably, however, achievability in the standard model, even with computational assumptions, is wide open; for further discussion and a candidate scheme, see [CHV24].

At the heart of this intriguing open question is the simplest case, called the *uncloneable bit*, where $m \in \{0,1\}$ (see Figure 1), which, despite its simplicity, has remained unsolved in the plain model. Its importance is highlighted in [HKNY24], where it is shown that a scheme for an uncloneable bit can be transformed into a scheme that encrypts general messages and that satisfies

uncloneable-indistinguishability[1].

1.1 Results

Our work focuses on the achievability of an encryption scheme that realizes an *uncloneable bit* in the statistical model, thus without any computational or setup assumptions. However, given the apparent difficulty of achieving this task, we relax the security requirement, and we ask that the success probability of the adversaries be no more than $1/2 + f(\lambda)$, for some $f : \mathbb{R} \to \mathbb{R}$ such that $\lim_\lambda f(\lambda) = 0$ (weak security). This is a relaxation of the usual requirement that f be a negligible function (strong security).

Our contribution is a new candidate scheme for this relaxation of the uncloneable bit question. We prove weak security for some small security parameters and provide strong numerical evidence that it also holds asymptotically.

Candidate Scheme for an Uncloneable Bit. Our candidate scheme is based on a family of pairwise anti-commuting n-qubit Pauli strings, of the following form for n even:

$$X^{\otimes(i-1)} \otimes Y \otimes I^{\otimes(n-i)} \quad \text{and} \quad X^{\otimes(i-1)} \otimes Z \otimes I^{\otimes(n-i)}, \qquad i \in \{1, \dots, n\}\,. \tag{1}$$

Note that there are $2n$ such strings. When n is odd, we add to the above set $X^{\otimes n}$ and obtain $2n+1$ strings. We index these strings as Γ_k, and based on this, define the following candidate (see details in Section 3).

Definition (Candidate Scheme for an Uncloneable Bit)**.** Consider $\Gamma_1, ..., \Gamma_K$ Hermitian unitaries that anti-commute (*e.g.* the pairwise anti-commuting Pauli strings in eq. (1)), of dimension $d = 2^\lambda$, with $K = 2\lambda$ for even[2] λ. Sample uniformly at random a key $k \in \{1, \dots, K\}$. From this key k, encrypt a classical message $m \in \{0, 1\}$ into the following quantum state:

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

which is the normalized projector onto the eigenvalue $(\text{-}1)^m$ of Γ_k. For the decryption scheme of a quantum state $\rho_{m,k}$, measure it in the eigenbasis of Γ_k. The outcome is the decrypted message.

One can easily check the correctness of this protocol, *i.e.* decrypting an encrypted message recovers the initial message with full probability.

Our scheme can be seen as a generalization of the basic uncloneable encryption scheme [BL20] that uses as key $\theta \in \{0, 1\}$ and encodes a bit m as $H^\theta |m\rangle$. This encoding corresponds to the $K = 2$ case of our candidate. Already in the case $K = 2$, using the proof techniques from monogamy-of-entanglement games [TFKW13], the success probability of the adversary at the no-cloning game is $\frac{1}{2} + \frac{1}{2\sqrt{2}}$, which is consistent with the following conjecture (see Conjecture 1).

Conjecture. *Our candidate encryption scheme is weakly uncloneable-indistinguishable secure with the following upper-bound:*

$$\Pr\Big((\mathsf{P}, \mathsf{B}, \mathsf{C}) \textit{ win the no-cloning game}\Big) \leqslant \frac{1}{2} + \frac{1}{2\sqrt{K}}\,,$$

where K is the number of keys.

The contributions of this paper focus on this conjecture and are divided into several analytical and numerical results, as summarized in Figure 2. The source code for our numerical methods

[1] For conventional encryption, encrypting a message bitwise with a single-bit encryption scheme typically yields a secure encryption; however, such a construction is not secure in the context of uncloneable encryption.

[2] We only consider the case λ even here and let the reader see the complete definition of the scheme in Section 3.1.

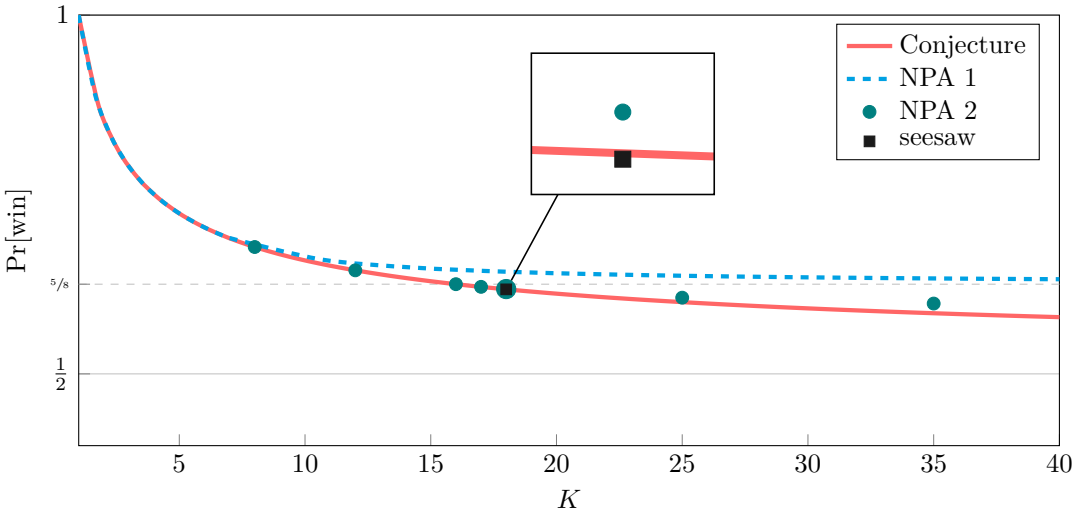


Figure 2. Upper-bounds on the winning probability in the no-cloning game involving three adversaries $(\mathsf{P}, \mathsf{B}, \mathsf{C})$ for our candidate scheme for Uncloneable Encryption with K keys. The solid line (red) is the conjectured upper-bound, the dashed line (cyan) corresponds to the upper-bound derived from NPA level 1, the circles (teal) are the numerical upper-bounds obtained from NPA level 2, and the square (black) is the numerical result obtained using the seesaw optimization method on $K = 18$.

is available on GitHub[3]. Our methods are mainly based on the Navascués-Pironio-Acín (NPA) hierarchy [NPA08] and Sum-of-Squares (SoS) decompositions [McC01, Hel02], which are standard primal/dual SDP algorithms to approximate the set of quantum (commuting) correlations. Those methods provide upper-bounds on the winning probability:

Result 1 (Cyan in Figure 2)**.** *The conjecture is confirmed for $K \leqslant 7$ using both an explicit Sum-of-Squares decomposition and an analytical level-1 NPA proof.*

Result 2 (Teal in Figure 2)**.** *The conjecture is numerically confirmed for $K \leqslant 17$ using a level-2 NPA optimisation*[4]*.*

Then, using the analytic solution of the first level of the NPA hierarchy and taking its limit in K, we also derive the following upper-bound:

Result 3 (Cyan in Figure 2)**.** *Asymptotically, the winning probability of our candidate scheme for the no-cloning game is upper-bounded by $5/8$.*

Additionally, we use an alternating optimization problem algorithm, known as seesaw methods, to obtain lower-bounds. We explore the case $K = 18$ and found no instances that violate the conjecture:

Result 4 (Black in Figure 2)**.** *For $K = 18$, no violation of the conjecture is found using seesaw methods.*

Finally, although we are unable to prove full uncloneable-indistinguishability, we prove that

[3] https://github.com/denis-rochette/Towards-Unconditional-Uncloneable-Encryption

[4] For larger K, we would need the next levels of the NPA hierarchy—computational limitations prevented us from extending the numerics.

conventional indistinguishability also holds, in a relaxed sense, for our candidate scheme (see Section 3.5).

1.2 Future Work

Our work introduces a candidate scheme supported by strong evidence, highlighting its significance in the field of unconditional uncloneable encryption. However, several important questions remain unresolved, which we outline below:

Question 1: Proving the Conjecture for Large K. In this paper, we provide an analytical proof for the conjecture when $K \leqslant 7$ and support it numerically for $K \leqslant 17$. Extending this proof to arbitrarily large values of K would be a significant advancement, as it would mark the first unconditional proof of uncloneable encryption in the plain model.

Question 2: Achieving Stronger Security. Our proposed protocol achieves a quadratic security rate while the original definition in [BL20] specifies a security with exponential decay in the security parameter. A key open challenge is to develop a protocol that achieves this stronger security.

1.3 Organization of the Paper

The remainder of this paper is organized as follows. Section 2 contains the necessary notation and preliminaries concerning states, measurements, and channels in quantum mechanics, as well as the formal definition of uncloneable encryption and its relation to monogamy-of-entanglement games. In Section 3, we present our scheme for uncloneable encryption and establish a conjecture regarding its uncloneable-indistinguishable security based on operator theory. Finally, in Section 4, we propose analytical proofs and numerical evidence of the conjecture in the first cases.

2 Preliminaries

We use $\mathbb{N}_+$ to represent the set of positive natural numbers $\mathbb{N} \setminus \{0\}$, and $[n]$ to denote the set $\{1, \dots, n\}$. The indicator function is written as $\mathbb{1}_{\{\cdot\}}$, and $\mathrm{negl}(\lambda)$ refers to a negligible function in $\lambda \in \mathbb{N}_+$ [5].

In this paper, all Hilbert spaces are considered to be finite-dimensional. Given a Hilbert space $\mathcal{H} \simeq \mathbb{C}^d$, we use $\mathcal{M}_d \simeq \mathcal{B}(\mathcal{H})$ for the set of matrices (or operators) acting on $\mathcal{H}$, and I_d for the identity matrix on this space. The trace on $\mathcal{H}$ is written as $\mathrm{Tr}[\cdot]$. An operator M is positive semi-definite if and only if it is Hermitian (*i.e.* $M^* = M$) with (real) non-negative eigenvalues. In this case, we write $M \succcurlyeq 0$. Given two Hermitian operators A and B, we write $A \succcurlyeq B$ if $A - B \succcurlyeq 0$. The norm on $\mathcal{H}$ is denoted by $\|\cdot\|$, and the operator norm on $\mathcal{M}_d$ by $\|\cdot\|_{\mathrm{op}}$. Given two operators A and B acting on $\mathcal{H}$, the notation $[A, B]$ represents the commutator $AB - BA$, and $\{A, B\}$ represents the anti-commutator $AB + BA$. The Frobenius inner product of two operators A and B acting on $\mathcal{H}$ is defined by $\langle A, B\rangle \coloneqq \mathrm{Tr}[A^*B]$.

A Hilbert space $\mathcal{H} \simeq \mathbb{C}^d$ is called a *quantum system*, and its density matrices (*i.e.* positive semi-definite unit-trace matrices) are the *quantum states*, forming the following set:

$$\mathcal{D}_d \coloneqq \left\{\rho \in \mathcal{M}_d \ : \ \mathrm{Tr}[\rho] = 1 \text{ and } \rho \succcurlyeq 0\right\}.$$

The set of density matrices $\mathcal{D}_d$ is convex, and its extreme points are precisely the unit-rank projectors $|\psi\rangle\langle\psi|$, for some unit vector $|\psi\rangle \in \mathcal{H}$, referred to as *pure quantum states*. On a composite system $\mathcal{H}^{\otimes n}$ with n parties, we write Tr_i for the *partial trace* on the Hilbert space corresponding to the i-th subsystem:

$$\mathrm{Tr}_i \coloneqq I_d \otimes \cdots \otimes I_d \otimes \underbrace{\mathrm{Tr}}_{i\text{-th}} \otimes I_d \otimes \cdots \otimes I_d \,.$$

[5] $\forall n \in \mathbb{N}, \exists N \in \mathbb{N}$ such that $\forall \lambda > N$ we have $\mathrm{negl}(\lambda) \leqslant \lambda^{-n}$ [KL07].

In the case of a composite system with different dimensions, we also use partial trace notation, indexed by the dimension to trace, *e.g.* on $\mathcal{H} \simeq \mathbb{C}^d \otimes \mathbb{C}^D$, the notation Tr_D stands for the partial trace on the second tensor factor. A *quantum channel* $\Phi : \mathcal{M}_d \to \mathcal{M}_D$ is a Completely Positive and Trace Preserving (CPTP) linear map. We use the notation Φ_i to denote the i-th marginal of the quantum channel: $\Phi_i \coloneqq \mathrm{Tr}_i \circ \Phi$. A Positive Operator-Valued Measure (POVM) on a Hilbert space $\mathcal{H} \simeq \mathbb{C}^d$ is a finite set of positive semi-definite operators $\{M_i\}$ that sum to the identity: $\sum_i M_i = I_d$. A Projection-Valued Measure (PVM) is a specific type of POVM where $\{M_i\}$ is a set of orthogonal projections.

In this paper, we use the standard *Pauli matrices*, which are Hermitian and unitary operators that serve as a basis for the space of 2×2 Hermitian matrices. They are defined as:

$$X \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y \coloneqq \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad I \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

2.1 Uncloneable Encryption

Uncloneable encryption, as introduced in [BL20], is a symmetric-key encryption scheme with *quantum* ciphertext to prevent unauthorized replication.

Definition 1 (Quantum Encryption of Classical Messages)**.** A *quantum encryption of classical messages* (QECM) is a triple of efficient quantum algorithms $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ such that:

- $\mathtt{Gen}(1^\lambda) \mapsto k$: takes a security parameter 1^λ as input, and outputs a classical secret key $k \in [K] \subseteq \{0,1\}^\lambda$.[6]
- $\mathtt{Enc}(m, k) \mapsto \rho$: takes a message $m \in \{0,1\}$ and a secret key $k \in [K] \subseteq \{0,1\}^\lambda$ as inputs, and outputs a quantum ciphertext $\rho \in \mathcal{B}(\mathcal{H})$.
- $\mathtt{Dec}(\rho, k) \mapsto m$: takes a ciphertext $\rho \in \mathcal{B}(\mathcal{H})$ and a secret key $k \in [K] \subseteq \{0,1\}^\lambda$ as inputs, and outputs a message $m \in \{0,1\}$.

The following definition requires that, for all keys that can be generated by the scheme, a valid ciphertext is always correctly decrypted, up to negligible probability.

Definition 2 (Correctness)**.** A scheme $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ is said to be *correct* if for any security parameter λ, for any secret key $k = \mathtt{Gen}(1^\lambda)$, and for any message m, we have

$$\Pr\Big[\mathtt{Dec}\big(\mathtt{Enc}(m,k),k\big) = m\Big] = 1 - \mathrm{negl}(\lambda)\,,$$

where $\mathrm{negl}(\lambda)$ is a *negligible function* of λ.

Now that we have a formal definition of the scheme and its correctness, we can define the security property called *uncloneable-indistinguishability*. This security property is formalized in terms of a no-cloning game for a 1-bit message (see Figure 1).

Definition 3 (No-Cloning Game)**.** Given an uncloneable encryption scheme $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ and a security parameter λ, the *no-cloning game* involving a challenger A and three adversaries $(\mathsf{P}, \mathsf{B}, \mathsf{C})$ is defined by the following procedure:

1. A challenger A generates a key $k \leftarrow \mathtt{Gen}(1^\lambda)$ and a message $m \in \{0,1\}$ uniformly at random, and sends the quantum state $\rho \leftarrow \mathtt{Enc}(m,k)$ to P.
2. The adversary P applies a CPTP map $\Phi : \mathcal{B}(\mathcal{H}_\mathsf{A}) \to \mathcal{B}(\mathcal{H}_\mathsf{B} \otimes \mathcal{H}_\mathsf{C})$ on the state ρ to obtain the bipartite state $\Phi(\rho)$, and sends to B and C their respective register.

[6] The notation "$1^\lambda = 11\cdots1$" means that the generation of the key $k \in [K]$ is efficient with respect to the security parameter λ.

3. The adversaries B and C receive the secret key k and measure their state using two POVMs $\{B_k\}$ and $\{C_k\}$, to output $m_\mathsf{B}, m_\mathsf{C} \in \{0,1\}$.

4. The adversaries $(\mathsf{P},\mathsf{B},\mathsf{C})$ win if $m = m_\mathsf{B} = m_\mathsf{C}$.

Remark 1. Since this work concerns the question of the *uncloneable bit*, we consider in Definition 3 a game with single-bit messages $m \in \{0,1\}$. See [BL20] for the more general case $m \in \{0,1\}^n$.

The uncloneable-indistinguishability security was introduced by Broadbent and Lord in [BL20], combining two other notions of security: uncloneable security, which they also introduced, and indistinguishable security [GM84, ABF+16]. In contrast to [BL20], we propose a stronger security definition, wherein adversaries are unbounded.

Definition 4 (Uncloneable-Indistinguishable Security)**.** An uncloneable encryption scheme satisfies *strong uncloneable-indistinguishable security* if for any security parameter λ and for any adversaries $(\mathsf{P},\mathsf{B},\mathsf{C})$ the no-cloning game from Definition 3 cannot succeed with probability more than $1/2 + \mathrm{negl}(\lambda)$. If instead the adversaries cannot succeed with probability more than $1/2 + f(\lambda)$ for some function $f : \mathbb{R} \to \mathbb{R}$ such that $\lim_\lambda f(\lambda) = 0$, we simply say that the scheme satisfies *weak uncloneable-indistinguishable security*.

Remark 2. As sketched in [BL20], uncloneable-indistinguishable security implies indistinguishable security in terms of a conventional encryption scheme [GM84, ABF+16]. For completeness, we provide a full proof of the indistinguishable security of our candidate scheme in Section 3.5.

2.2 Bound for Unconditional No-Cloning Game

By definition of the no-cloning game (see Definition 3), the winning probability of the three adversaries $(\mathsf{P},\mathsf{B},\mathsf{C})$ is equal to

$$\begin{aligned}\Pr[\mathrm{win}] &= \sup_{\substack{\Phi \\ B_{i|k}, C_{j|k}}} \mathop{\mathbb{E}}_{\substack{m\in\{0,1\} \\ k\leftarrow \mathtt{Gen}(1^\lambda)}} \sum_{i,j\in\{0,1\}} \mathbb{1}_{\{i=j=m\}} \mathrm{Tr}\big[\Phi(\rho_{m,k})(B_{i|k}\otimes C_{j|k})\big] \\ &= \sup_{\Phi,B,C} \mathop{\mathbb{E}}_{m,k} \mathrm{Tr}\big[\Phi(\rho_{m,k})(B_{m|k}\otimes C_{m|k})\big]\,,\end{aligned}$$

with $\rho_{m,k} \coloneqq \mathtt{Enc}(m,k)$, and where the expected values are taken with respect to the uniform measures, and the supremum is taken over all CPTP $\Phi : \mathcal{B}(\mathcal{H}_\mathsf{A}) \to \mathcal{B}(\mathcal{H}_\mathsf{B}\otimes\mathcal{H}_\mathsf{C})$ (for all finite-dimensional Hilbert spaces $\mathcal{H}_\mathsf{B}$ and $\mathcal{H}_\mathsf{C}$), and all families of POVM $\{B_{i|k}\}$ and $\{C_{j|k}\}$.

Given a CPTP map $\Phi : \mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^{d'})$, the Choi matrix [Wat18] $C_\Phi \in \mathcal{M}_d \otimes \mathcal{M}_{d'}$ is defined by

$$C_\Phi \coloneqq \sum_{i,j\in[d]} |i\rangle\!\langle j| \otimes \Phi\big(|i\rangle\!\langle j|\big)\,,$$

and satisfies the partial trace equality

$$\Phi(X) = \mathrm{Tr}_d\big[C_\Phi (X^\mathsf{T}\otimes I_{d'})\big]\,, \qquad \forall X \in \mathcal{M}_d\,, \tag{2}$$

and Choi's theorem [Cho75]:

$$\Phi \in \mathrm{CPTP} \quad\Longleftrightarrow\quad C_\Phi \succcurlyeq 0 \quad\text{and}\quad \mathrm{Tr}_{d'}[C_\Phi] = I_d. \tag{3}$$

Using the Choi matrix of the CPTP $\Phi : \mathcal{B}(\mathcal{H}_\mathsf{A}) \to \mathcal{B}(\mathcal{H}_\mathsf{B}\otimes\mathcal{H}_\mathsf{C})$, with $\mathcal{H}_\mathsf{A} \simeq \mathbb{C}^d$ and $\mathcal{H}_\mathsf{B}\otimes\mathcal{H}_\mathsf{C} \simeq \mathbb{C}^{d'}$, and the partial trace equality eq. (2), the winning probability of the no-cloning game becomes

$$\Pr[\mathrm{win}] = \sup_{C_\Phi,B,C} \mathop{\mathbb{E}}_{m,k} \mathrm{Tr}\big[C_\Phi(\rho_{m,k}^\mathsf{T}\otimes B_{m|k}\otimes C_{m|k})\big]\,,$$

where the supremum is now taken over all $C_\Phi \succcurlyeq 0$ such that $\mathrm{Tr}_{d'}[C_\Phi] = I_d$. This last condition can be relaxed to $\mathrm{Tr}[C_\Phi] = d$, giving the first upper-bound on the winning probability:

$$\begin{aligned}\Pr[\text{win}] &\leqslant \sup_{C_\Phi,B,C} \mathop{\mathbb{E}}_{m,k} \mathrm{Tr}\left[\tfrac{1}{d} \cdot C_\Phi(d \cdot \rho^{\mathsf{T}}_{m,k} \otimes B_{m|k} \otimes C_{m|k})\right] \\ &= \sup_{\sigma,B,C} \mathop{\mathbb{E}}_{m,k} \mathrm{Tr}\left[\sigma\,(d \cdot \rho^{\mathsf{T}}_{m,k} \otimes B_{m|k} \otimes C_{m|k})\right], \end{aligned} \tag{4}$$

where the first supremum is taken over all $C_\Phi \succcurlyeq 0$, and the last supremum is taken over all $\sigma \succcurlyeq 0$ such that $\mathrm{Tr}[\sigma] = 1$, *i.e.* a quantum state. The upper-bound eq. (4) is saturated on pure quantum states $|\psi\rangle\langle\psi|$, as pure quantum states form the extreme points of the convex set of quantum states, and the optimization is linear in σ. Hence

$$\Pr[\text{win}] \leqslant \sup_{\psi,B,C} \langle\psi| \mathop{\mathbb{E}}_{m,k}\left[d \cdot \rho^{\mathsf{T}}_{m,k} \otimes B_{m|k} \otimes C_{m|k}\right] |\psi\rangle \tag{5}$$

$$\leqslant \sup_{\psi,B,C} \left| \langle\psi| \mathop{\mathbb{E}}_{m,k}\left[d \cdot \rho^{\mathsf{T}}_{m,k} \otimes B_{m|k} \otimes C_{m|k}\right] |\psi\rangle \right| \tag{6}$$

$$= \sup_{B,C} \left\| \mathop{\mathbb{E}}_{m,k}\left[d \cdot \rho^{\mathsf{T}}_{m,k} \otimes B_{m|k} \otimes C_{m|k}\right] \right\|_{\mathrm{op}}, \tag{7}$$

where the first two suprema are taken over all $\|\psi\| = 1$ and the last equality holds because $d \cdot \rho^{\mathsf{T}}_{m,k} \otimes B_{m|k} \otimes C_{m|k}$ is a Hermitian operator.

By Naimark's theorem [Per90], we may always assume that the POVMs are in fact PVMs up to increasing the dimension. Moreover, any adversaries $(\mathsf{P}, \mathsf{B}, \mathsf{C})$ can be assumed to be *symmetric*, *i.e.* $\mathcal{H}_\mathsf{B} = \mathcal{H}_\mathsf{C}$ and $\{B_{i|k}\} = \{C_{j|k}\}$, by taking B's and C's spaces to be $\mathcal{H}_\mathsf{B} \oplus \mathcal{H}_\mathsf{C}$, the PVM operators to be $\{B_{i|k} \oplus C_{i|k}\}$,[7] and the CPTP map Φ that sends B's part of the output to the first component of the direct sum space and C's to the second component. Hence, the upper-bound eq. (7) becomes

$$\Pr[\text{win}] \leqslant \sup_{M} \left\| \mathop{\mathbb{E}}_{m,k}\left[d \cdot \rho^{\mathsf{T}}_{m,k} \otimes M_{m|k} \otimes M_{m|k}\right] \right\|_{\mathrm{op}}, \tag{8}$$

where the supremum is taken over all PVMs $\{M_{i|k}\}$.

2.3 Link with Monogamy-of-Entanglement Games

Limitations imposed by the *no-cloning theorem* [Wer98, KW99] are closely related to limitations due to *monogamy-of-entanglement* (MoE) [CKW00, KW04]. This explains the close relationship between no-cloning games and monogamy-of-entanglement games (see Figure 3), introduced in the foundational paper [TFKW13].

An MoE game involves three parties: a referee, denoted as Alice (A), and two cooperating players, Bob (B) and Charlie (C). The game proceeds as follows. Alice initially has a fixed family of positive operator-valued measures. Before the game's start, Bob and Charlie jointly agree upon a strategy, preparing a tripartite quantum state and sending the corresponding marginal state to referee Alice. Once the game begins, the players are space-like separated, meaning that any form of communication is no longer allowed. The referee Alice picks a POVM uniformly at random and performs a measurement on her quantum state to produce some classical outcome m_A. She publicly announces the POVM she used to Bob and Charlie. Their goal is then to independently recover m_A, by performing some measurements on their respective states, which result in classical outcomes m_B and m_C, respectively. Finally, the referee A declares that the players Bob and Charlie won the game if both of them recover Alice's outcome, *i.e.* if exactly $m_\mathsf{A} = m_\mathsf{B} = m_\mathsf{C}$.

When the POVMs fixed by the referee Alice are the ones of conjugate coding [Wie83], it is easy to show that the winning probability for the MoE game is at least $\frac{1}{2} + \frac{1}{2\sqrt{2}}$: the players Bob and Charlie share no entanglement, send to Alice the state $\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$ from the Breidbart basis, and always output $m_\mathsf{B} = m_\mathsf{C} = 0$, which is indeed equal to m_A with probability $(\cos\frac{\pi}{8})^2 = \frac{1}{2} + \frac{1}{2\sqrt{2}}$.[8]

[7] We do not consider the cases where $i \neq j$ because then the winning probability of the adversaries is zero.

[8] Alternatively, this can be seen as a consequence of an entropic uncertainty relation due to Deutsch [Deu83].

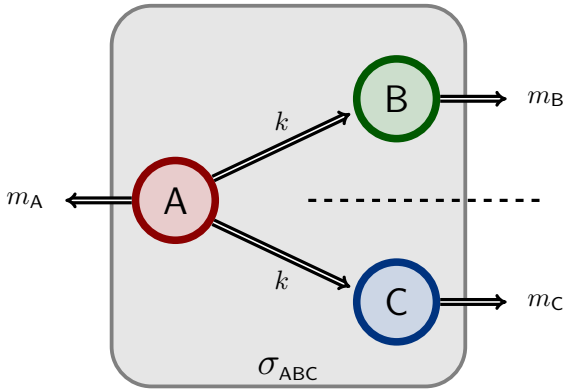


Figure 3. *Monogamy-of-Entanglement Game.* Alice (A), Bob (B), and Charlie (C) share a quantum state σ_{ABC}. Given a classical random key $k \in \{1, .., K\}$, Alice performs a measurement $\{A_{m|k}\}_m$ and obtains $m_A \in \{0, 1\}$. Using the same key k, the players Bob and Charlie perform respective measurements $\{B_{m|k}\}_m$ and $\{C_{m|k}\}_m$, and we say that they win the game if both of them recover the exact same message as Alice, *i.e.* if $m_A = m_B = m_C$.

Interestingly, this value is actually the optimal one, and if we repeat n times this game in parallel, then the optimal winning probability is precisely $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$ [TFKW13].

In the absence of MoE, the players in an MoE game would be able to perfectly win the game by considering a state maximally entangled between the referee (A) and the two players (B) and (C), *i.e.* a tripartite state ρ_{ABC} with reduced states

$$\rho_{AB} = \frac{1}{2}\sum_{ij} |ii\rangle\langle jj| \qquad \text{and} \qquad \rho_{AC} = \frac{1}{2}\sum_{ij} |ii\rangle\langle jj| \ .$$

The existence of such a state is precluded by the MoE principle, which stipulates that no quantum state can be maximally entangled with more than two parties simultaneously. This principle also implies the no-cloning principle which states that it is not possible, in general, to copy a quantum state. If this were possible, then a quantum channel $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H} \otimes \mathcal{H})$, with marginals $\Phi_1(\rho) = \rho$ and $\Phi_2(\rho) = \rho$ for all $\rho \in \mathcal{B}(\mathcal{H})$, would exist. But then its Choi matrix C_Φ is such that the marginals become

$$C_{\Phi_1} = \sum_{ij} |ii\rangle\langle jj| \qquad \text{and} \qquad C_{\Phi_2} = \sum_{ij} |ii\rangle\langle jj| \,,$$

that is, both proportional to a maximally entangled state, which is not possible due to the MoE and Choi's theorem eq. (3).

This relationship between MoE and no-cloning is reflected in the winning probability of MoE games and no-cloning games. The winning probability of the MoE game can be described as follows:

$$\Pr\left[\text{win}\right] \ = \ \sup_{\sigma,B,C} \frac{1}{K}\sum_{m,k} \mathrm{Tr}\left[\sigma \left(A_{m|k} \otimes B_{m|k} \otimes C_{m|k}\right)\right] , \tag{9}$$

where σ is a quantum state in $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, and the sets $\{A_{m|k}\}_k$, $\{B_{m|k}\}_k$, $\{C_{m|k}\}_k$ are POVMs on respectively $\mathcal{H}_A$, $\mathcal{H}_B$, $\mathcal{H}_C$. When $m \in \{0, 1\}$, this winning probability is precisely the expression we have in eq. (4) when $A_{m|k} = (d/2) \cdot \rho_{m,k}^{\mathsf{T}}$ is a POVM, *i.e.* when the normalization condition $\sum_m \rho_{m,k} = 2\, I_d/d$ holds for all k.

3 Candidate Scheme

In this section, we propose a new encryption scheme based on the Clifford algebra. In the next section, we show that it allows us to recover previously known results for $K = 2$, and we provide strong numerical evidence that this scheme achieves the uncloneable security for large K.

3.1 Clifford Algebra

For our uncloneable encryption scheme, we make use of the structure of Clifford algebra [Lou01, DL03], widely used in quantum information theory, in particular as a generalization of the Bloch sphere representation [Die06, WW08], in operator algebras theory [Pis03, BN18], and in non-local games [Slo11, Ost16]. This choice is motivated by the fact that the Clifford generators used below, were shown in [BN18] to give rise to maximally incompatible binary observables. Thus, the measurements associated with different keys are extremal from the viewpoint of joint measurability, making them natural candidates for an uncloneable encryption scheme, where security should arise from the impossibility of simultaneously reproducing such incompatible measurement outcomes.

For any integer $n \in \mathbb{N}_+$, the free real associative algebra generated by $\Gamma_1, \ldots, \Gamma_n$, and subject to the anti-commutation relations:

$$\{\Gamma_i, \Gamma_j\} \coloneqq \Gamma_i\Gamma_j + \Gamma_j\Gamma_i = 2\,\delta_{ij}\,\mathbb{1}\,,$$

is called the *Clifford algebra*, and denoted $\mathbf{CL}_n$. Any irreducible representation of the Clifford algebras $\mathbf{CL}_{2n}$ and $\mathbf{CL}_{2n+1}$ can be constructed explicitly by the following $2n+1$ Pauli string operators acting on $\mathbb{C}^{2^n}$, called the Jordan-Wigner transformation [JW93]:

$$\begin{aligned}
\sigma_{n,2i-1} &= X^{\otimes(i-1)} \otimes Y \otimes I^{\otimes(n-i)}, \quad i \in \{1, \ldots, n\}\,, \\
\sigma_{n,2i} &= X^{\otimes(i-1)} \otimes Z \otimes I^{\otimes(n-i)}, \quad i \in \{1, \ldots, n\}\,, \\
\sigma_{n,2n+1} &= X^{\otimes n}\,,
\end{aligned}$$

These operators are traceless, and as Hermitian unitaries, they have spectrum ± 1. Mapping the generators $\Gamma_1, \ldots, \Gamma_{2n}$ to $\sigma_{n,1}, \ldots, \sigma_{n,2n}$ gives the irreducible representation of the even Clifford algebra $\mathbf{CL}_{2n}$. Mapping the generators $\Gamma_1, \ldots, \Gamma_{2n+1}$ to $\sigma_{n,1}, \ldots, \sigma_{n,2n+1}$ or $\sigma_{n,1}, \ldots, -\sigma_{n,2n+1}$ gives the two inequivalent irreducible representations of the odd Clifford algebra $\mathbf{CL}_{2n+1}$.

An important property of the Clifford algebra is that $2n$ Hermitian anti-commuting operators $\Gamma_1, \ldots, \Gamma_{2n}$ can be view as orthogonal vectors, for the normalized Frobenius inner product, forming a basis for the $2n$-dimensional real vector space they span. Indeed, given $u, v \in \mathbb{R}^{2n}$ we have

$$\left\langle \sum_{i=1}^{2n} u_i\Gamma_i, \sum_{j=1}^{2n} v_j\Gamma_j \right\rangle = \frac{1}{2n}\left(\sum_{i=1}^{2n} u_i v_i \underbrace{\operatorname{Tr}\left(\Gamma_i^2\right)}_{=2n} + \sum_{\substack{i,j=1 \\ i<j}}^{2n} (u_i v_j - u_j v_i) \underbrace{\operatorname{Tr}\left(\Gamma_i\Gamma_j\right)}_{=0}\right) = \langle u, v\rangle\,.$$

In particular for a unit vector $v \in \mathbb{R}^{2n}$, the operator $\sum_{i=1}^{2n} v_i\Gamma_i$ is a Hermitian unitary. Using this property, given any vector $v \in \mathbb{R}^{2n}$, we have

$$\left\| \sum_{i=1}^{2n} v_i\Gamma_i \right\|_{\mathrm{op}} = \|v\|_2\,, \tag{10}$$

and taking the all-ones vector, we get $\left\|\sum_{i=1}^{2n} \Gamma_i\right\|_{\mathrm{op}} = \sqrt{2n}$.

3.2 Definition of the Scheme

We now define our candidate scheme for a weak uncloneable bit, using the Clifford algebra introduced in Section 3.1.

Definition 5 (Candidate Uncloneable Bit Encryption)**.** Let $\lambda \in \mathbb{N}_+$. We define our candidate uncloneable bit scheme. $\texttt{Gen}(1^\lambda)$ samples uniformly a key $k \in [K]$ with $K = 2\lambda$ (λ even) or $K = 2\lambda + 1$ (λ odd). The algorithms `Enc` and `Dec` are defined in Algorithm 1 and Algorithm 2, respectively. They use the irreducible representation of the generators $\Gamma_1, \ldots, \Gamma_K$ of a Clifford algebra (Section 3.1)[9], acting on $\mathbb{C}^d$ where $d = 2^\lambda$.

[9] When λ is odd, we choose $\sigma_{\lambda,1}, \ldots, \sigma_{\lambda,2\lambda+1}$, even if both irreducible representations form a valid scheme.

Algorithm 1: Encryption $\texttt{Enc}(m,k)$.	**Algorithm 2:** Decryption $\texttt{Dec}(\rho,k)$.
Input : A message $m \in \{0,1\}$ and a key $k \in [K]$.	**Input :** A state ρ acting on $\mathbb{C}^d$ and a key $k \in [K]$.
Output: A state $\rho_{m,k}$ acting on $\mathbb{C}^d$.	**Output:** A message $m \in \{0,1\}$.
1 Compute $\rho_{m,k} = \frac{2}{d}\frac{I_d+(-1)^m\Gamma_k}{2}$, the normalized projector onto the $(-1)^m$-eigenspace of Γ_k.	1 Measure ρ in the eigenbasis of Γ_k, with the PVM $\{\frac{1}{2}(I_d+(-1)^i\Gamma_k)\}_i$. Call m the outcome.
2 Output $\rho_{m,k}$.	2 Output m.

Remark 3. The correctness Definition 2 is immediate since the operators $\frac{I_d+\Gamma_k}{2}$ and $\frac{I_d-\Gamma_k}{2}$ are orthogonal. Thus the measurement of $\rho_{m,k}$ is

$$\operatorname{Tr}\left[\left(\frac{I_d+(-1)^i\Gamma_k}{2}\right)\rho_{m,k}\left(\frac{I_d+(-1)^i\Gamma_k}{2}\right)\right] = \begin{cases}1 & \text{if } i=m\,,\\ 0 & \text{otherwise}\,,\end{cases}$$

and $\Pr\Big[\texttt{Dec}\big(\texttt{Enc}(m,k),k\big)=m\Big]=1$.

When $K=2$, with $\Gamma_1 \coloneqq X$ and $\Gamma_2 \coloneqq Z$, then

$$\frac{I_d+(-1)^m\Gamma_1}{2} = H\,|m\rangle\langle m|\,H^* \qquad \text{and} \qquad \frac{I_d+(-1)^m\Gamma_2}{2} = |m\rangle\langle m|\,,$$

which is exactly the encryption used by the scheme defined in [BL20]. It should also be noted that in this case, the state $\rho_{m,k}$ is pure; however, it becomes mixed for larger K, as required by the impossibility results [MST21, AKL+22].

3.3 Conjecture

The upper-bound on the winning probability of the no-cloning game for three adversaries $(\mathsf{P},\mathsf{B},\mathsf{C})$ is given by eq. (8):

$$\Pr[\text{win}] \leqslant \sup_M \Big\| \mathop{\mathbb{E}}_{m,k}\big[d\cdot\rho_{m,k}^{\mathsf{T}}\otimes M_{m|k}\otimes M_{m|k}\big]\Big\|_{\text{op}}\,,$$

where the supremum is taken over all PVM $\{M_{i|k}\}$. For all the keys k, the PVM $\{M_{i|k}\}$ are binary measurement operators of dimension D. We can write

$$M_{i|k} = \frac{I_D+(-1)^iU_k}{2}\,,$$

for some Hermitian unitaries (observables) $U_k \coloneqq M_{0|k}-M_{1|k}$. Then the upper-bound eq. (8) for Clifford uncloneable encryption (Definition 5) is

$$\begin{aligned}
\Pr[\text{win}] &\leqslant \sup_{\{U_k\}}\left\| \mathop{\mathbb{E}}_{m,k}\left[d\cdot\frac{2}{d}\frac{I_d+(-1)^m\Gamma_k}{2}\otimes\frac{I_D+(-1)^mU_k}{2}\otimes\frac{I_D+(-1)^mU_k}{2}\right]\right\|_{\text{op}}\\
&\leqslant \sup_{\{U_k\}}\frac{1}{2K}\left\|\sum_{m,k} d\cdot\frac{2}{d}\frac{I_d+(-1)^m\Gamma_k}{2}\otimes\frac{I_D+(-1)^mU_k}{2}\otimes\frac{I_D+(-1)^mU_k}{2}\right\|_{\text{op}}\\
&\leqslant \sup_{\{U_k\}}\frac{1}{2K}\Bigg\|\frac{1}{4}\sum_{m,k}\Big(I_d\otimes I_D\otimes I_D\\
&\qquad +(-1)^m\left(\Gamma_k\otimes I_D\otimes I_D + I_d\otimes U_k\otimes I_D + I_d\otimes I_D\otimes U_k\right)\\
&\qquad +(-1)^{2m}\left(\Gamma_k\otimes U_k\otimes I_D + \Gamma_k\otimes I_D\otimes U_k + I_d\otimes U_k\otimes U_k\right)\\
&\qquad +(-1)^{3m}\,\Gamma_k\otimes U_k\otimes U_k\Big)\Bigg\|_{\text{op}}\\
&\leqslant \frac{1}{4}+\frac{1}{4K}\sup_{\{U_k\}}\Big\|\sum_k\Big(\Gamma_k\otimes(U_k\otimes I_D+I_D\otimes U_k)+I_d\otimes U_k\otimes U_k\Big)\Big\|_{\text{op}}\,,
\end{aligned}\tag{11}$$

where the supremum is taken over all Hermitian unitaries $U_k \in \mathcal{U}(\mathbb{C}^D)$.

A naive triangular inequality of the operator norm yields the trivial upper-bound $\Pr[\text{win}] \leqslant {}^1\!/_4 + {}^{3K}\!/_{4K} = 1$. Therefore, we need a finer upper-bound of this quantity, which we conjecture to be of the following form:

Conjecture 1. *Let $\Gamma_1, \dots, \Gamma_K$ be any pairwise anti-commuting Hermitian unitaries (Hermitian representation of some Clifford algebra) of dimension d. Then for all Hermitian unitaries $\{U_k\}$ of dimension D, the following upper-bound holds:*

$$\left\| \sum_{k\in[K]} \Big(\Gamma_k \otimes (U_k \otimes I_D + I_D \otimes U_k) + I_d \otimes U_k \otimes U_k \Big) \right\|_{\text{op}} \leqslant K + 2\sqrt{K}\,. \tag{12}$$

Remark. Under this conjecture, the upper-bound in eq. (11) gives $\frac{1}{2} + \frac{1}{2\sqrt{K}}$, with the asymptotic limit $\lim_{K\to\infty} \Pr[\text{win}] = {}^1\!/_2$ at a rate $O({}^1\!/_{\sqrt{K}})$, which would prove that the Clifford encryption scheme is weakly secure (see Definition 4).

3.4 Basic Properties

In this subsection, we prove basic properties related to our conjecture. First, we prove that the identity matrix saturates the bound of the conjecture, which means that if the wanted upper-bound holds, then it is tight (Theorem 1). Then we prove that the conjecture is true if the adversary's strategy is reduced to commuting operators U_k (Theorem 2) or if they only use product states (Theorem 4).

In what follows, we will refer to the family of operators involved in Conjecture 1 as:

$$W_K(U_1, \dots, U_K) \coloneqq \sum_{k\in[K]} \Big(\Gamma_k \otimes (U_k \otimes I_D + I_D \otimes U_k) + I_d \otimes U_k \otimes U_k \Big)\,. \tag{13}$$

We simply write $W \coloneqq W_K(U_1, \dots, U_K)$ if there are no ambiguities on $K \in \mathbb{N}_+$ and the Hermitian unitaries $U_1, \dots, U_K$.

Proposition 1 (Tight Upper-Bound)**.** *The supremum of $\|W_K\|_{\text{op}}$ is lower-bounded by $K + 2\sqrt{K}$, achieved by taking $U_k = I_D$ for all $k \in [K]$. As a consequence, the upper-bound in Conjecture 1 can only be tight.*

Proof. Combine the formulae $\|\sum_i \Gamma_i + I\|_{\text{op}} = \|\sum_i \Gamma_i\|_{\text{op}} + 1$, valid since the spectrum of $\sum_i \Gamma_i$ is symmetric [HKMS19], and eq. (10) to obtain the value $K + 2\sqrt{K}$. □

Remark 4 (Low Rank Operators Also Saturate the Bound)**.** Actually, the value $K + 2\sqrt{K}$ is also achieved by taking any $U_k \in \mathbb{C}^D$ with projector onto the 1-eigenspace of rank $r \leqslant \frac{D-1}{K}$. Indeed, write

$$U_k = 2\left(\sum_{i=1}^{r} |u_k^{(i)}\rangle\langle u_k^{(i)}| \right) - I_D\,,$$

for all $k \in [K]$ and for some quantum states $|u_k^{(i)}\rangle \in \mathbb{C}^D$ (or the zero vector). Using the condition $D \geqslant K\,r + 1$, there exists a quantum state $|u^\perp\rangle \in \mathbb{C}^D$ that is orthogonal to all the $|u_k^{(i)}\rangle$ for $i \in [r]$ and $k \in [K]$. Note that this vector satisfies $\langle u^\perp|U_k|u^\perp\rangle = 2(\sum_i 0) - 1 = -1$ for all k. It follows

that

$$\begin{aligned}
\|W_K\|_{\mathrm{op}} &= \sup_{\substack{|\psi\rangle\in\mathbb{C}^d\otimes\mathbb{C}^D\otimes\mathbb{C}^D \\ \||\psi\rangle\|=1}} \left|\langle\psi| \sum_k \left(\Gamma_k\otimes U_k\otimes I_D + \Gamma_k\otimes I_D\otimes U_k + I_d\otimes U_k\otimes U_k\right)|\psi\rangle\right| \\
&\geqslant \sup_{\substack{|a\rangle\in\mathbb{C}^d \\ \||a\rangle\|=1}} \left|\langle a\otimes u^\perp\otimes u^\perp| \sum_k \left(\Gamma_k\otimes(U_k\otimes I_D + I_D\otimes U_k) + I_d\otimes U_k\otimes U_k\right)|a\otimes u^\perp\otimes u^\perp\rangle\right| \\
&= \sup_{\substack{|a\rangle\in\mathbb{C}^d \\ \||a\rangle\|=1}} \left|2\langle a| \sum_k -\Gamma_k |a\rangle + K\right| \\
&= 2\left\|\sum_k -\Gamma_k\right\|_{\mathrm{op}} + K = 2\left\|\begin{bmatrix}-1\\ \vdots \\ -1\end{bmatrix}\right\|_2 + K = 2\sqrt{K} + K\,,
\end{aligned}$$

using the symmetry of the spectrum of $\sum_k \Gamma_k$ [HKMS19] in the third last equality and then using eq. (10) in the second last one. Hence the claimed result.

Proposition 2 (True for Commuting Operators)**.** *If the operators U_k commute, then Conjecture 1 holds.*

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

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

Then, using the triangular inequality, we obtain:

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

because $\left\|\sum_{k=1}^K \Gamma_k\otimes 1\otimes(\pm 1)\right\|_{\mathrm{op}} = \left\|\sum_{k=1}^K \Gamma_k\right\|_{\mathrm{op}} = \sqrt{K}$ using eq. (10). □

We give a connection between the operator norm of W and the supremum of $\langle\psi| W |\psi\rangle$:

Lemma 3 (Expression of the Operator Norm)**.** *For all $K \in \mathbb{N}_+$, we have the two following equalities:*

$$\sup_U \sup_{\|\psi\|=1} \langle\psi| W |\psi\rangle \overset{(1)}{=} \sup_U \sup_{\|\psi\|=1} |\langle\psi| W |\psi\rangle| \overset{(2)}{=} \sup_U \|W\|_{\mathrm{op}}\,,$$

where the suprema are taken over all Hermitian unitaries $U_k \in \mathcal{U}(\mathbb{C}^D)$.

Proof. Let $W' \coloneqq W + K\cdot I_d\otimes I_D\otimes I_D$, then we can write,

$$W' = \sum_k \left(\Gamma_k\otimes I_D\otimes I_D + I_d\otimes U_k\otimes I_D\right)\left(\Gamma_k\otimes I_D\otimes I_D + I_d\otimes I_D\otimes U_k\right).$$

Each Γ_k is a Hermitian unitary with a symmetric spectrum ± 1. There exist an invertible matrix H_k that can diagonalize Γ_k, *i.e.*

$$\Gamma_k = H_k \begin{pmatrix} -I_{d/2} & 0 \\ 0 & I_{d/2} \end{pmatrix} H_k^{-1}.$$

Thus, under those changes of basis, the operator W' is expressed as follows:

$$W' = \sum_k \tilde{H}_k \begin{pmatrix} (I-U_k)^{\otimes 2} & 0 \\ 0 & (I+U_k)^{\otimes 2} \end{pmatrix} \tilde{H}_k^{-1},$$

with $\tilde{H}_k \coloneqq H_k \otimes I_D \otimes I_D$. Since for all U_k, the inequalities $-I_D \preccurlyeq U_k \preccurlyeq I_D$ hold, the two operators $I + U_k$ and $I - U_k$ are both positive semi-definite, so is each term of the sum, and thus $W' \succcurlyeq 0$.

The first equality holds since,

$$\sup_{\|\psi\|=1} |\langle\psi| W |\psi\rangle| = \max\left\{ \sup_{\|\psi\|=1} \langle\psi| W |\psi\rangle , -\inf_{\|\psi\|=1} \langle\psi| W |\psi\rangle \right\},$$

but because $W' \succcurlyeq 0$, we have that $-\sup_U \inf_{\|\psi\|=1} \langle\psi| W |\psi\rangle = K$, and when all U_k are equal to I_D, we already know that $\sup_{\|\psi\|=1} \langle\psi| W |\psi\rangle = K + 2\sqrt{K}$ from Theorem 1.

Finally, the second equality is always true for Hermitian operators [Zim90, Lemma 3.2.4], and W is a Hermitian operator, as a sum of tensor products of Hermitian operators Γ_k and U_k. □

Hence, the three upper-bounds eqs. (5) to (7) of the winning probability of the no-cloning game for three adversaries $(\mathsf{P}, \mathsf{B}, \mathsf{C})$, are all equal, and Conjecture 1 can also be stated as the largest eigenvalue of the operator W.

From Theorem 3, see that an equivalent formulation of Conjecture 1 is:

$$\sup_U \sup_{\|\psi\|=1} \langle\psi| W |\psi\rangle \leqslant K + 2\sqrt{K},$$

where the quantum state $|\psi\rangle$ is taken in $\mathbb{C}^d \otimes \mathbb{C}^D \otimes \mathbb{C}^D$. We show that the conjecture holds in the restricted case where $|\psi\rangle$ is a product state between Alice and {Bob, Charlie}:

Proposition 4 (True for Product State)**.** *If the state is of the form* $|\psi\rangle = |\alpha_{\mathsf{A}}\rangle \otimes |\varphi_{\mathsf{BC}}\rangle$*, then:*

$$\sup_U \langle\psi| W |\psi\rangle \leqslant K + 2\sqrt{K}.$$

Proof. We have:

$$\begin{aligned}
&\sum_{k=1}^{K} \left\langle \alpha_{\mathsf{A}} \otimes \varphi_{\mathsf{BC}} \,\middle|\, \Big(\Gamma_k \otimes (U_k \otimes I_D + I_D \otimes U_k) + I_d \otimes U_k \otimes U_k\Big) \,\middle|\, \alpha_{\mathsf{A}} \otimes \varphi_{\mathsf{BC}} \right\rangle \\
&= \sum_{k=1}^{K} \left\langle \alpha_{\mathsf{A}} \,\middle|\, \Gamma_k \,\middle|\, \alpha_{\mathsf{A}} \right\rangle \underbrace{\left\langle \varphi_{BC} \,\middle|\, (U_k \otimes I_D + I_D \otimes U_k) \,\middle|\, \varphi_{BC} \right\rangle}_{=:c_k} \\
&\quad + \sum_{k=1}^{K} \left\langle \alpha_{\mathsf{A}} \otimes \varphi_{\mathsf{BC}} \,\middle|\, I_d \otimes U_k \otimes U_k \,\middle|\, \alpha_{\mathsf{A}} \otimes \varphi_{\mathsf{BC}} \right\rangle \\
&= \sum_{k=1}^{K} \left\langle \alpha_{\mathsf{A}} \,\middle|\, c_k\, \Gamma_k \,\middle|\, \alpha_{\mathsf{A}} \right\rangle + \sum_{k=1}^{K} \underbrace{\left\langle \alpha_{\mathsf{A}} \otimes \varphi_{\mathsf{BC}} \,\middle|\, I_d \otimes U_k \otimes U_k \,\middle|\, \alpha_{\mathsf{A}} \otimes \varphi_{\mathsf{BC}} \right\rangle}_{\leqslant 1} \\
&\leqslant \big\|(c_1, \ldots, c_K)\big\|_2 + K \\
&= 2\sqrt{K} + K,
\end{aligned}$$

using eq. (10) in the second last line. □

Remark 5. When $|\psi\rangle$ is a product state in all its tensors, *i.e.* when $|\psi\rangle = |\alpha_{\mathsf{A}} \otimes \beta_{\mathsf{B}} \otimes \gamma_{\mathsf{C}}\rangle$, then this result is equivalent to the one in Theorem 2.

3.5 Indistinguishability

Analogously to the two variants of uncloneable-indistinguishability security presented in Definition 4, namely those with a strong convergence rate and those with an arbitrary convergence rate, we can similarly define two corresponding notions of indistinguishability security.

The *strong indistinguishability security* requires that any adversary, upon receiving the encryption of a message m randomly chosen from a pair of messages, cannot predict the value of m with a

probability greater than negligibly close to $1/2$. If the adversary's probability of correctly predicting the encrypted message converges to $1/2$ at any arbitrary rate, we refer to this security notion as simply *indistinguishability security*.

In this section, we prove that our candidate scheme Definition 5 satisfies the latter indistinguishability security. Indeed, the success probability of such adversary is bounded by,

$$\Pr[\text{win}] \leqslant \sup_{\substack{\Phi \\ \{M_0,M_1\}}} \mathop{\mathbb{E}}_{\substack{m\in\{0,1\} \\ k\leftarrow \texttt{Gen}(1^\lambda)}} \operatorname{Tr}\left[\Phi(\rho_{m,k})M_m\right],$$

with $\rho_{m,k} \coloneqq \texttt{Enc}(m,k)$, and where the expected values are taken with respect to the uniform measures, and the supremum is taken over all CPTP map $\Phi : \mathcal{B}(\mathcal{H}_d) \to \mathcal{B}(\mathcal{H}_D)$ (for all finite-dimensional Hilbert spaces $\mathcal{H}_D$), and all binary POVM $\{M_0, M_1\}$. We now follow the same sequence of equations as presented in Section 2 to derive the result, which is outlined below:

$$\Pr[\text{win}] \leqslant \sup_M \left\| \mathop{\mathbb{E}}_{m,k} \left[d \cdot \rho_{m,k}^{\mathsf{T}} \otimes M_m \right] \right\|_{\text{op}},$$

where the supremum is taken over all binary POVM $\{M_0, M_1\}$. We proceed by adapting eq. (11), starting from the observable form $M_i = \frac{I_D + (-1)^i U}{2}$ for some Hermitian unitary U, to derive the following inequalities,

$$\begin{aligned}
\Pr[\text{win}] &\leqslant \sup_U \left\| \mathop{\mathbb{E}}_{m,k} \left[d \cdot \frac{2}{d} \frac{I_d + (-1)^m \Gamma_k}{2} \otimes \frac{I_D + (-1)^m U}{2} \right] \right\|_{\text{op}} \\
&\leqslant \sup_U \frac{1}{2K} \left\| \frac{1}{2} \sum_{m,k} \left(I_d \otimes I_D + (-1)^m \left(\Gamma_k \otimes I_D + I_d \otimes U \right) + (-1)^{2m} \Gamma_k \otimes U \right) \right\|_{\text{op}} \\
&\leqslant \frac{1}{2} + \frac{1}{2K} \sup_U \left\| \sum_k \Gamma_k \otimes U \right\|_{\text{op}},
\end{aligned}$$

where the supremum is taken over all Hermitian unitaries $U_k \in \mathcal{U}(\mathbb{C}^D)$. By applying the sub-multiplicative property of the operator norm (*i.e.* , $\|A \otimes B\|_{\text{op}} \leqslant \|A\|_{\text{op}} \cdot \|B\|_{\text{op}}$ for all A and B), along with the fact that the operator norm of a unitary is one, and the inequality $\left\|\sum_k \Gamma_k\right\|_{\text{op}} = \sqrt{K}$, we have the following upper-bound:

$$\Pr[\text{win}] \leqslant \frac{1}{2} + \frac{1}{2\sqrt{K}}.$$

This ensures a quadratic convergence rate for the indistinguishability security of our Clifford encryption scheme.

4 Analytical and Numerical Results for Conjecture 1

Although we have been unable to fully prove Conjecture 1, we present in this section several analytical and numerical results on the first values of $K \in \mathbb{N}$. Specifically, we prove the conjecture for $K \leqslant 7$ (Sections 4.1 and 4.2), provide numerical confirmation for $K \leqslant 17$ (Section 4.3), and present numerical evidence for $K = 18$ (Section 4.4). Additionally, we establish a weaker bound than the conjecture (Theorem 9), which holds for all $K \in \mathbb{N}$.

Inapplicability of the Triangular Inequality. As we saw in Section 3.1, a naive triangular inequality of the operator norm in eq. (11) yields a trivial upper-bound $\Pr[\text{win}] \leqslant 1/4 + 3K/4K = 1$. In light of the property of eq. (10), one might consider that a slightly more refined triangular inequality could be sufficient to address Conjecture 1, and that

$$\left\| \sum_{k\in[K]} \Gamma_k \otimes \left(U_k \otimes I_D + I_D \otimes U_k \right) \right\|_{\text{op}} + \left\| \sum_{k\in[K]} I_d \otimes U_k \otimes U_k \right\|_{\text{op}},$$

would be smaller than $K + 2\sqrt{K}$, but this is not true for $K > 2$. One should notice that $\left\|\sum_{k\in[K]} \Gamma_k \otimes U_k\right\|_{\text{op}} \leqslant K$, with equality by taking all $U_k = \Gamma_k$. With those U_k, the tensor products $U_k \otimes U_k$ are pairwise commuting and thus $\left\|\sum_{k\in[K]} I_d \otimes U_k \otimes U_k\right\|_{\text{op}} = K$, but the left-hand side of the triangular inequality $\left\|\sum_{k\in[K]} \Gamma_k \otimes (U_k \otimes I_D + I_D \otimes U_k)\right\|_{\text{op}}$ is in general larger than $2\sqrt{K}$, with first values:

$$2\sqrt{2},\ 2\sqrt{4},\ 2\sqrt{6},\ 2\sqrt{9},\ 2\sqrt{12},\ 2\sqrt{16},\ 2\sqrt{20},\ 2\sqrt{25},\ \ldots$$

In comparison, when all $U_k = \Gamma_k$, the complete operator norm $\left\|\sum_{k\in[K]} \Gamma_k \otimes (U_k \otimes I_D + I_D \otimes U_k) + I_d \otimes U_k \otimes U_k\right\|_{\text{op}}$ is smaller than $K + 2\sqrt{K}$, with first values:

$$4,\ 3,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ \ldots$$

4.1 Elementary Proofs for $K = 2$

We present two distinct preliminary proofs showing that Conjecture 1 is true for $K = 2$, a first one using the equivalence with the [BL20] scheme, and another one based on the Sum-of-Squares method. In Section 4.2, we will extend the second proof to larger values of K, with much more material involved. Note that a third proof can also be obtained by exploiting the anti-commutation of the two pairs of matrices in W_2 and the recent results in [HO21, dGHG23, XSW24, MH24] regarding uncertainty relations.

4.1.1 First Proof, with the BB84 MoE Game

As we saw in Section 3.1, for $K = 2$ our candidate scheme coincides with the scheme defined in [BL20], thus the upper-bound of the winning probability of the no-cloning game for three adversaries $(\mathsf{P}, \mathsf{B}, \mathsf{C})$ is the same as in [BL20], *i.e.* $\frac{1}{2} + \frac{1}{2\sqrt{2}}$. Thus, by Theorem 3,

$$\Pr[\text{win}] \leqslant \frac{1}{4} + \frac{1}{4K} \sup_U \left\|\sum_k \Big(\Gamma_k \otimes (U_k \otimes I_D + I_D \otimes U_k) + I_d \otimes U_k \otimes U_k\Big)\right\|_{\text{op}} = \frac{1}{2} + \frac{1}{2\sqrt{2}}\,,$$

which implies that $\|W_2\|_{\text{op}} \leqslant 2 + 2\sqrt{2}$ as claimed.

4.1.2 Second Proof, with Sum-of-Squares

From eq. (5), the upper-bound of the winning probability of the no-cloning game for three adversaries $(\mathsf{P}, \mathsf{B}, \mathsf{C})$ is

$$\Pr[\text{win}] \leqslant \sup_{\psi,B,C} \langle\psi| \mathop{\mathbb{E}}_{m,k} \left[d \cdot \rho_{m,k}^{\mathsf{T}} \otimes B_{m|k} \otimes C_{m|k}\right] |\psi\rangle\ ,$$

where the supremum is taken over all $\|\psi\| = 1$, all families of PVM $\{B_{i|k}\}$ and $\{C_{j|k}\}$, as well as their respective dimensions. Following the same steps as Section 3, we found

$$\Pr[\text{win}] \leqslant \frac{1}{4} + \frac{1}{4K} \sup_{\psi,B,C} \langle\psi| \sum_k \Big(\Gamma_k \otimes (B_k \otimes I_D + I_D \otimes C_k) + I_d \otimes B_k \otimes C_k\Big) |\psi\rangle\ , \tag{14}$$

where the supremum is now taken over all families of observables $\{B_k\}$ and $\{C_k\}$. Note that this time, we do not assume the adversaries $(\mathsf{P}, \mathsf{B}, \mathsf{C})$ to be symmetric, *i.e.* B and C may have different observables. The last part of the upper-bound eq. (14) can be stated as the optimization problem:

$$\begin{aligned} \sup_{\psi,B,C} \quad & \langle\psi| \sum_k \Big(\Gamma_k \otimes (B_k \otimes I_D + I_D \otimes C_k) + I_d \otimes B_k \otimes C_k\Big) |\psi\rangle\ , \\ \text{subject to} \quad & \cdot\ \|\psi\| = 1\,, \\ & \cdot\ B_i^* = B_i \quad \cdot\ C_i^* = C_i \quad \cdot\ B^2 = C^2 = I_D \quad \forall i\,. \end{aligned} \tag{15}$$

This problem can be relaxed through the use of what is called commuting operator strategies, in which the tensor product structure between Alice's and Bob's operators is replaced by the assumption that these operators commute:

$$\begin{aligned} \sup_{\psi,b,c} \quad & \langle\psi| \sum_k \Big(\Gamma_k \otimes (b_k + c_k) + I_d \otimes b_k \cdot c_k\Big) |\psi\rangle \ , \\ \text{subject to} \quad & \cdot \ \|\psi\| = 1 \, , \\ & \cdot \ b_i^* = b_i \quad \cdot \ c_i^* = c_i \quad \cdot \ b_i^2 = c_i^2 = I_D \quad \forall i \, , \\ & \cdot \ [b_i, c_j] = 0 \quad \forall i, j \, . \end{aligned} \tag{16}$$

An optimal value for the problem eq. (15) is immediately a lower-bound for the problem eq. (16) by taking $b_k \coloneqq B_k \otimes I_D$ and $c_k \coloneqq I_D \otimes C_k$. The question of the equality of the two optimization problems eqs. (15) and (16) (and in general of the tensor-based *versus* the commuting-based models) was a long-standing problem that was only recently refuted by [JNV+21]. However, in the case of finite-dimensional Hilbert spaces, the equality holds as an inductive consequence of Tsirelson's theorem [Tsi93, RXL26].

If the optimal value of the problem eq. (16) is $K + 2\sqrt{K}$, then the Hermitian operator

$$P_K \coloneqq (K + 2\sqrt{K}) \cdot I_d \otimes I_{D^2} - \sum_k \Big(\Gamma_k \otimes (b_k + c_k) + I_d \otimes b_k \cdot c_k\Big) \, , \tag{17}$$

must be positive semi-definite under the constraints of eq. (16). If we can find a family $\{H_i\}_i$ such that $P_k = \sum_i H_i^* H_i$, then the operator P_K would be guaranteed to be positive semi-definite, as a sum of positive semi-definite operators $H_i^* H_i$. If all H_i are also Hermitian, then we can write $P_K = \sum_i H_i^2$. This constitutes the fundamental principle of the Sum-of-Squares (SoS) decomposition technique, which is used to establish bounds on a variety of quantum correlations, including the CHSH Bell inequality [Bel64, CHSH69] and its associated Tsirelson bound [Cir80].

Let $P(\mathbf{X})$ be an Hermitian polynomial in non-commutative variables $\mathbf{X} = (X_i)_i$, then $P(\mathbf{X})$ is a positive semi-definite polynomial (*i.e.* $P(\mathbf{X}) \succcurlyeq 0$ for all evaluations of P on matrices $\mathbf{X}$) if and only if $P(\mathbf{X})$ is a Hermitian Sum-of-Squares [McC01, Hel02]:

$$P(\mathbf{X}) = \sum_i H_i(\mathbf{X})^* \, H_i(\mathbf{X}) \, .$$

This result can be used to maximize the operator norm of a non-commutative Hermitian polynomial. If the polynomial is constrained to an archimedean semi-algebraic set (a condition that is satisfied in our case), a hierarchy of converging upper-bounds can be obtained based on semi-definite optimization programs (SDP) [HM04]. The dual problem of those SDPs forms the Navascués-Pironio-Acín (NPA) hierarchy [NPA08] and correspond to the non-commutative variant of the Lasserre's hierarchy [Las01].

For $K = 2$ such SoS decomposition was already known [BC23a]:

$$P_2 = \frac{1}{2\sqrt{2}}\big(X \otimes b_1 + Z \otimes c_2 - \sqrt{2} \cdot I\big)^2 + \frac{1}{2\sqrt{2}}\big(X \otimes c_1 + Z \otimes b_2 - \sqrt{2} \cdot I\big)^2 + \frac{1}{2}\big(b_1 - c_1\big)^2 + \frac{1}{2}\big(b_2 - c_2\big)^2 \, ,$$

where we took $\Gamma_1 \coloneqq X$ and $\Gamma_2 \coloneqq Z$. This implies, using Theorem 3, that $\|W_2\|_{\text{op}} \leqslant 2 + 2\sqrt{2}$.

4.2 Proofs for $K \leqslant 7$ and Asymptotic Upper-Bound

We prove that Conjecture 1 is true for all $K \leqslant 7$ in two manners: first using a family of SoS decompositions, then based on its dual SDP problem, the NPA hierarchy.

4.2.1 First Proof, with Sum-of-Squares

We refer to Section 4.1.2 for intuition and background about the SoS method. Let $K \in \{2, \dots, 7\}$. The non-negativity certificate of P_K, defined in eq. (17), is given by the following SoS:

$$P_K \ = \ \frac{K - \sqrt{K}}{2K(K-1)} \sum_{i=1}^{K} \Big(Q_K + (\sqrt{K} + 1)\, \Gamma_i \otimes (c_i - b_i)\Big)^2 + \alpha_K \, Q_K^2 \, , \tag{18}$$

where:

$$Q_K := \sqrt{K}\, I \otimes I - \sum_{j=1}^{K} (\Gamma_j \otimes c_j) \qquad \text{and} \qquad \alpha_K := \frac{(3K-2)\sqrt{K} - K^2}{2K(K-1)}\,.$$

Notice that the coefficient α_K is positive for all $K \leqslant 7$, so eq. (18) is a valide SoS decomposition for $P_2, ..., P_7$, which validates Conjecture 1 for $K \leqslant 7$. However, for $K \geqslant 8$ the coefficient α_K is negative, so that the decomposition presented in eq. (18) no longer provides a valid non-negativity certificate. Note that it does not exclude the possibility of finding another SoS decomposition valid for larger values of K. It is also worth mentioning that the SoS decomposition given in eq. (18) can be readily symmetrized with respect to the variables b_i and c_i — the current formulation has been chosen for its simplicity.

4.2.2 Second Proof, with NPA Level-1, and Asymptotic Result

The NPA hierarchy is dual to the sum-of-squares (SoS) approach. At level n of the hierarchy, we keep track of only the relations on moments of order up to and including n of the operators. This gives rise to a SDP maximisation whose optimal value is precisely the value that can be certified by a SoS certificate where the squared terms have order n. For NPA level 1, we only consider the relations that are first order in the b_i and c_i.

To simplify the relations we work with in the NPA hierarchy, we first express the game value in terms of an anticommuting version of the scenario algebra. Then, at NPA level 1, we relax the optimisation to only depend on the first-order moments of the observables. This turns the problem into an SDP, which can be approximated efficiently. Making use of the symmetry of the problem allows us to drastically simplify the SDP we need to solve, allowing us to do it analytically. In Section 4.3, we pass to NPA level 2 and we proceed in the same way. There, we have to consider the second-order moments. We make use of analogous simplifications by symmetry to get a simpler problem; however, this problem becomes too complicated to solve analytically, so we solve it numerically to find the values.

We introduce two scenario algebras and prove that the optimal value of our conjecture is equivalent to the supremum of the operator norm of a new problem:

Definition 6 (Scenario Algebra)**.** The *scenario algebra* $\mathcal{A}(K)$ is the $*$-algebra generated by $b_1, c_1, \ldots, b_K, c_K$ such that $b_i^2 = c_i^2 = 1$, $b_i^* = b_i$, $c_i^* = c_i$, and $b_i c_j = c_j b_i$ for all $i, j \in [K]$.
The *anticommuting scenario algebra* $\mathcal{A}_{ac}(K)$ is the $*$-algebra generated by $\hat{b}_1, \hat{c}_1, \ldots, \hat{b}_K, \hat{c}_K$ such that $\hat{b}_i^2 = \hat{c}_i^2 = 1$, $\hat{b}_i^* = \hat{b}_i$, $\hat{c}_i^* = \hat{c}_i$, $\hat{b}_i\hat{c}_i = \hat{c}_i\hat{b}_i$ for all i, and $\hat{b}_i\hat{c}_j = -\hat{c}_j\hat{b}_i$ for all $i \neq j \in [K]$.

In our case, we can take, as a representation, $\Gamma_i \otimes B_i \otimes I$ for $\hat{b}_i$ and $\Gamma_i \otimes I \otimes C_i$ for $\hat{c}_i$. The game polynomial can be seen as an element $p_K \in \mathcal{M}_d \otimes \mathcal{A}(K)$, with $p_K = \sum_k \Big(\Gamma_k \otimes (b_k + c_k) + I \otimes b_k c_k\Big)$ so that the winning probability is $\frac{1}{4} + \frac{1}{4K} \sup_\pi \|(\mathrm{id} \otimes \pi)(p_K)\|$, where the supremum is over all finite-dimensional representations of $\mathcal{A}(K)$. First, we prove that the winning probabilities over $\mathcal{A}(K)$ and $\mathcal{A}_{ac}(K)$ coincide:

Proposition 5. *Let $\hat{p}_K = \sum_k (\hat{b}_k + \hat{c}_k + \hat{b}_k\hat{c}_k) \in \mathcal{A}_{ac}(K)$. Then,*

$$\sup_\pi \|(\mathrm{id} \otimes \pi)(p_K)\|_{\mathrm{op}} = \sup_{\hat{\pi}} \|\hat{\pi}(\hat{p}_K)\|_{\mathrm{op}}\,,$$

where the suprema are over finite-dimensional representations $\pi, \hat{\pi}$ of $\mathcal{A}(K)$, $\mathcal{A}_{ac}(K)$ respectively.

Proof. Let π be a finite-dimensional representation of $\mathcal{A}(K)$. Then, let $\hat{\pi}$ be the representation of $\mathcal{A}_{ac}(K)$ defined by $\hat{\pi}(\hat{b}_k) = \Gamma_k \otimes \pi(b_k)$ and $\hat{\pi}(\hat{c}_k) = \Gamma_k \otimes \pi(c_k)$. It is direct to see that this satisfies the relations of $\mathcal{A}_{ac}(K)$ and $(\mathrm{id} \otimes \pi)(p_K) = \hat{\pi}(\hat{p}_K)$, and hence that $\|(\mathrm{id} \otimes \pi)(p_K)\|_{\mathrm{op}} = \|\hat{\pi}(\hat{p}_K)\|_{\mathrm{op}}$. Taking suprema, we get $\sup_\pi \|(\mathrm{id} \otimes \pi)(p_K)\|_{\mathrm{op}} \leqslant \sup_{\hat{\pi}} \|\hat{\pi}(\hat{p}_K)\|_{\mathrm{op}}$.

For the other direction, let $\hat{\pi}$ be a finite-dimensional representation of $\mathcal{A}_{ac}(K)$. Then, define a representation π of $\mathcal{A}(K)$ by $\pi(b_k) = \Gamma_k^{\mathsf{T}} \otimes \hat{\pi}(\hat{b}_k)$ and $\pi(c_k) = \Gamma_k^{\mathsf{T}} \otimes \hat{\pi}(\hat{c}_k)$. As above,

it is direct to see that this satisfies the relations of $\mathcal{A}(K)$. Let $|\psi\rangle$ be a unit vector such that $\|\hat{\pi}(\hat{p}_K)\|_{\mathrm{op}} = |\langle\psi|\hat{\pi}(\hat{p}_K)\rangle\,\psi|$, and write $|\Psi_d\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ for the maximally entangled state. Then, $\langle \Psi_d | \Gamma_k \otimes \Gamma_k^{\mathsf{T}} \rangle\, \Psi_d = 1$, so

$$\begin{aligned}\|(\mathrm{id}\otimes\pi)(p_K)\|_{\mathrm{op}} &\geqslant \left|\langle \Psi_d \otimes \psi \,|\, \sum_k \left(\Gamma_k \otimes \Gamma_k^{\mathsf{T}} \otimes (\hat{\pi}(\hat{b}_k) + \hat{\pi}(\hat{c}_k)) + I_{d^2} \otimes \hat{\pi}(\hat{b}_k\hat{c}_k)\right) \,|\, \Psi_d \otimes \psi\rangle\right| \\ &= \left|\langle\psi|\hat{\pi}(\hat{p}_K)\rangle\,\psi\right| \;=\; \left\|\hat{\pi}(\hat{p}_K)\right\|_{\mathrm{op}},\end{aligned}$$

giving the inequality $\sup_\pi \|(\mathrm{id}\otimes\pi)(p_K)\|_{\mathrm{op}} \geqslant \sup_{\hat{\pi}} \|\hat{\pi}(\hat{p}_K)\|_{\mathrm{op}}$. □

Thus, the winning probability can be found via an optimization over representations of $\mathcal{A}_{ac}(K)$. Let the bias of a strategy be $4K\Pr[\text{win}] - K$. Then the optimal bias is $\beta_K = \sup_{\hat{\pi}} \|\hat{\pi}(\hat{p}_K)\|$ and it is the solution of the following optimization:

$$\begin{aligned}\sup_{\psi,b,c} \quad & \langle\psi| \sum_k \left(b_k + c_k + b_k \cdot c_k\right) |\psi\rangle \;, \\ \text{subject to} \quad & \cdot\ \|\psi\| = 1\,, \\ & \cdot\ b_i^* = b_i \quad \cdot\ c_i^* = c_i \quad \cdot\ b_i^2 = c_i^2 = I_D \quad \forall i\,, \\ & \cdot\ b_i c_i = c_i b_i \quad \forall i\,, \\ & \cdot\ b_i c_j = -c_j b_i \quad \forall i \neq j\,.\end{aligned}$$

By our conjecture, the value of the optimal bias should be $K + 2\sqrt{K}$. We consider the first level of the NPA hierarchy on this algebra [NPA08]. To do so, we write $|u_i\rangle = b_i\,|\psi\rangle$, and $|v_i\rangle = c_i\,|\psi\rangle$, and dilate the parameter spaces so that the only relations on these vectors are those that follow directly from the relations on the operators. For example, we have $\langle u_i|v_j\rangle = \langle\psi|b_ic_j\rangle\,\psi = -\langle\psi|c_jb_i\rangle\,\psi = -\langle v_j|u_i\rangle$ for all $i \neq j$. We have the level-1 NPA optimization:

$$\begin{aligned}\sup_{\psi,u,v} \quad & \sum_i \left(\langle\psi|u_i\rangle + \langle\psi|v_i\rangle + \langle u_i|v_i\rangle\right), \\ \text{subject to} \quad & \cdot\ \langle\psi|\psi\rangle = \langle u_i|u_i\rangle = \langle v_i|v_i\rangle = 1 \quad \forall\, i\,, \\ & \cdot\ \langle\psi|u_i\rangle = \langle u_i|\psi\rangle \quad \cdot\ \langle\psi|v_i\rangle = \langle v_i|\psi\rangle \quad \forall\, i\,, \\ & \cdot\ \langle u_i|v_i\rangle = \langle v_i|u_i\rangle \quad \forall\, i\,, \\ & \cdot\ \langle u_i|v_j\rangle = -\langle v_j|u_i\rangle \quad \forall\, i \neq j\,.\end{aligned} \tag{19}$$

Then, we use the Gram matrix G of the vectors $\left(|\psi\rangle, |u_1\rangle, \ldots, |u_K\rangle, |v_1\rangle, \ldots, |v_K\rangle\right)$ to reformulate the optimization problem:

$$G = \begin{pmatrix} \langle\psi|\psi\rangle & \langle\psi|u_1\rangle & \ldots & \langle\psi|u_K\rangle & \langle\psi|v_1\rangle & \ldots & \langle\psi|v_K\rangle \\ \langle u_1|\psi\rangle & \langle u_1|u_1\rangle & \ldots & \langle u_1|u_K\rangle & \langle u_1|v_1\rangle & \ldots & \langle u_1|v_K\rangle \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \langle u_K|\psi\rangle & \langle u_K|u_1\rangle & \ldots & \langle u_K|u_K\rangle & \langle u_K|v_1\rangle & \ldots & \langle u_K|v_K\rangle \\ \langle v_1|\psi\rangle & \langle v_1|u_1\rangle & \ldots & \langle v_1|u_K\rangle & \langle v_1|v_1\rangle & \ldots & \langle v_1|v_K\rangle \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \langle v_K|\psi\rangle & \langle v_K|u_1\rangle & \ldots & \langle v_K|u_K\rangle & \langle v_K|v_1\rangle & \ldots & \langle v_K|v_K\rangle \end{pmatrix}.$$

The first constraint in eq. (19) yields that the diagonal elements of G are all 1. Also, since G is positive semidefinite, the second and third constraints specify elements of G that are real; and the fourth constraint specifies elements of G that are imaginary. Therefore, taking:

$$H = \frac{1}{2}\begin{pmatrix} 0 & \langle 1_K| & \langle 1_K| \\ |1_K\rangle & 0 & I \\ |1_K\rangle & I & 0 \end{pmatrix},$$

where $|1_K\rangle \in \mathbb{C}^K$ is the column vector of ones, the optimization becomes:

$$\begin{aligned} \sup_G \quad & \mathrm{Tr}(HG)\,, \\ \text{subject to} \quad & \cdot\ G(\psi,\psi) = G(u_i,u_i) = G(v_i,v_i) = 1 \quad \forall\, i\,, \\ & \cdot\ G(\psi,u_i), G(\psi,v_i), G(u_i,v_i) \in \mathbb{R} \quad \forall\, i\,, \\ & \cdot\ G(u_i,v_j) \in i\mathbb{R} \quad \forall\, i \neq j\,, \\ & \cdot\ G \succcurlyeq 0\,. \end{aligned} \tag{20}$$

We can reduce this problem to only three variables:

Lemma 6. *The optimal value of the SDP eq. (20) is equal to the value of the optimization*

$$\begin{aligned} \sup_g \quad & 2Kg_1 + Kg_3\,, \\ \textit{subject to} \quad & \cdot \begin{pmatrix} 1 & g_1\langle 1_K| & g_1\langle 1_K| \\ g_1|1_K\rangle & I + g_2(|1_K\rangle\langle 1_K| - I) & g_3 I \\ g_1|1_K\rangle & g_3 I & I + g_2(|1_K\rangle\langle 1_K| - I) \end{pmatrix} \succcurlyeq 0\,, \\ & \cdot\ g_1, g_2, g_3 \in \mathbb{R}\,. \end{aligned}$$

Proof. The simplification exploits the symmetries of H, which can be used to induce symmetries on G. First, note that H has real components, and therefore G can be assumed to be real, yielding the optimization

$$\begin{aligned} \sup_G \quad & \mathrm{Tr}(HG)\,, \\ \text{subject to} \quad & \cdot\ G(\psi,\psi) = G(u_i,u_i) = G(v_i,v_i) = 1 \quad \forall i\,, \\ & \cdot\ G(u_i,v_j) = 0 \quad \forall\, i \neq j\,, \\ & \cdot\ G \succcurlyeq 0\,. \end{aligned}$$

Next, for any permutation $\sigma \in \mathfrak{S}_K$, the matrix H is invariant under the permutation of the indices $\big(u_i \mapsto u_{\sigma(i)}, v_j \mapsto v_{\sigma(j)}\big)$. Moreover, H is invariant under the permutation $\big(u_i \mapsto v_i, v_i \mapsto u_i\big)$. Thus, G can be supposed to be invariant under those permutations, and we can add the following constraints to the optimization: $G(\psi,u_i) = G(\psi,u_j) = G(\psi,v_i) = G(\psi,v_j) =: g_1$ and $G(u_i,v_i) = G(u_j,v_j) =: g_3$ for all i,j, and $G(u_i,u_j) = G(u_k,u_l) = G(v_i,v_j) = G(v_k,v_l) =: g_2$ for all $i \neq j$, $k \neq l$. These additional constraints take the SDP to the form given in the statement. □

By the previous lemma, we can find the optimal value by first finding the set of feasible points (g_1, g_2, g_3) explicitly, and then finding the optimum of the objective function $2Kg_1 + Kg_3$ over that set.

Lemma 7. *Let $A = \sum_i a_i |i\rangle\langle i|$ and $B = \sum_i b_i |i\rangle\langle i|$ be commuting Hermitian matrices. Then we have the eigendecomposition*

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix} = \sum_i \Big((a_i + b_i)\,|i+\rangle\langle i+| + (a_i - b_i)\,|i-\rangle\langle i-| \Big)\,,$$

where $|i+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} |i\rangle \\ |i\rangle \end{pmatrix}$ and $|i-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} |i\rangle \\ -|i\rangle \end{pmatrix}$.

Proof. We can express $\left(\begin{smallmatrix} A & B \\ B & A \end{smallmatrix}\right) = \sum_i \left(\begin{smallmatrix} a_i & b_i \\ b_i & a_i \end{smallmatrix}\right) \otimes |i\rangle\langle i|$. Now, $\left(\begin{smallmatrix} a_i & b_i \\ b_i & a_i \end{smallmatrix}\right) = (a_i + b_i)\,|+\rangle\langle +| + (a_i - b_i)\,|-\rangle\langle -|$, giving the result. □

Lemma 8. *Let $H = \sum_i \lambda_i |v_i\rangle\langle v_i|$ be a Hermitian matrix. Then the Hermitian matrix $\left(\begin{smallmatrix} 1 & \omega\langle v_1| \\ \omega|v_1\rangle & H \end{smallmatrix}\right)$ has eigenvalues λ_i for $i > 1$, and $\frac{1+\lambda_1}{2} \pm \sqrt{\left(\frac{1-\lambda_1}{2}\right)^2 + \omega^2}$.*

Proof. Noting that $\left(\begin{smallmatrix} 0 \\ |v_i\rangle \end{smallmatrix}\right)$ is an eigenvector with eigenvalue λ_i for all $i > 1$, the remaining two eigenvalues are the eigenvalues of $\left(\begin{smallmatrix} 1 & \omega \\ \omega & \lambda_1 \end{smallmatrix}\right)$, which are of the above form. □

Theorem 9. *The value of the first level of the NPA hierarchy for the Clifford uncloneable encryption MoE game is* $\frac{1}{2} + \frac{1}{2\sqrt{K}}$ *for* $K \leqslant 7$*, and* $\frac{5}{8} + \frac{1}{2(K-2)} - \frac{1}{4K}$ *for* $K > 7$*. In particular, we obtain the upper-bound of* $5/8 = 0.625$ *on the winning probability of the no-cloning game in the limit* $K \to \infty$*.*

Proof. First, we want to find the feasible points of the optimization in Theorem 6 by calculating the eigenvalues of the matrices G of that form. Using Theorem 7, we see that the eigenvalues of

$$\begin{pmatrix} I + g_2\,(|1_K\rangle\langle 1_K| - I) & g_3\, I \\ g_3\, I & I + g_2(|1_K\rangle\langle 1_K| - I) \end{pmatrix}$$

are $Kg_2+(1-g_2)+g_3$ with eigenvector $\frac{1}{\sqrt{2K}}\,|1_{2K}\rangle$, and $Kg_2+(1-g_2)-g_3$, $1-g_2+g_3$, $1-g_2-g_3$ with eigenvectors orthogonal to $\frac{1}{\sqrt{2K}}\,|1_{2K}\rangle$. Using Theorem 8, the eigenvalues of G are $Kg_2+(1-g_2)-g_3$, $1-g_2+g_3$, $1-g_2-g_3$ and $\frac{1}{2}(1+Kg_2+(1-g_2)+g_3) \pm \sqrt{\frac{1}{4}(1-(Kg_2+(1-g_2)+g_3))^2 + 2Kg_1^2}$. In order for this to be a feasible point of the SDP, all of these eigenvalues must be positive. This means that $1+(K-1)g_2 \geqslant g_3$, $1-g_2 \geqslant \pm g_3$, and $1+(K-1)g_2+g_3 \geqslant 2Kg_1^2$.

To find the optimal point, consider a new parametrisation $x = 1-g_2+g_3$, $y = 1-g_2-g_3$, $\lambda = 2g_1+g_3$. Then, $g_1 = \lambda/2-(x-y)/4$, $g_2 = 1-(x+y)/2$, $g_3 = (x-y)/2$ so the objective function becomes $K\lambda$ and the constraints become $x, y \geqslant 0$, $2 \geqslant x + \frac{K-2}{K}\,y$, and $\lambda^2 - (x-y)\lambda + \frac{(x-y)^2}{4} + \frac{K-2}{K}\,x + y - 2 \leqslant 0$, which is a degree-2 polynomial in λ. As λ is to be maximised, we get:

$$\lambda \;=\; \frac{x-y}{2} + \sqrt{2 - \frac{K-2}{K}\,x - y}\;.$$

Since λ decreases with y, it is maximised at $y = 0$, giving $x \in [0,2]$ and $\lambda = \frac{x}{2} + \sqrt{2 - \frac{K-2}{K}\,x}$. Its derivative is:

$$\frac{d\lambda}{dx} \;=\; \frac{1}{2} - \frac{K-2}{2K\sqrt{2 - \frac{K-2}{K}\,x}}\;,$$

which is 0 if and only if $x = \frac{2K}{K-2} - \frac{K-2}{K}$, and positive for smaller x. If $K \leqslant 7$, then this value of x is greater than 2, so λ is maximised at $x = 2$, giving $\lambda = 1 + \frac{2}{\sqrt{K}}$, and hence winning probability

$$w_1 \;=\; \frac{1}{4} + \frac{\lambda}{4} \;=\; \frac{1}{2} + \frac{1}{2\sqrt{K}}\;.$$

If $K \geqslant 8$, the maximum value is attained in the interval $[0,2]$ so the optimum $\lambda = \frac{K}{K-2} + \frac{K-2}{2K}$, and therefore the winning probability

$$w_1 \;=\; \frac{5}{8} + \frac{1}{2(K-2)} - \frac{1}{4K}\;.$$ □

4.3 Numerical Result with NPA Hierarchy Level 2 for $K \leqslant 17$

To get a better upper-bound on the game, we make use of a higher level of the NPA hierarchy. Here, we use level 2 of the NPA hierarchy, where we optimize over a Gram matrices indexed by quadratic terms in the generators of $\mathcal{A}_{ac}(K)$. Even using the symmetries of the problem, as in Theorem 6, this becomes a vastly more difficult optimization, and requires us to do it numerically. However, we observe the same behaviour as for NPA level 1: the optimal value of the SDP matches the conjectured value exactly, until a certain K, where it starts to diverge towards a higher limit than $1/2$. Here, the point of divergence is $K = 18$. We give some of the optimal values for the NPA level 1 and 2 optimizations in the table below, highlighting the points of divergence:

K	NPA level 1	NPA level 2	Conjecture
2	0.8536	0.8536	0.8536
4	0.7500	0.7500	0.7500
7	0.6890	0.6890	0.6890
8	0.6771	0.6768	0.6768
12	0.6542	0.6443	0.6443
16	0.6451	0.6250	0.6250
17	0.6436	0.6213	0.6213
18	0.6424	0.6182	0.6179
25	0.6367	0.6062	0.6000
35	0.6330	0.5980	0.5845

Note also that the NPA level 2 upper-bound of $w_2 = 0.5980$ for $K = 35$ is, to the best of our knowledge, the best known unconditional upper-bound on the security of an uncloneable encryption scheme.

To finish this section, we outline the construction of the SDP that allows us to find the NPA level 2 optimal values more efficiently. In particular, it allows us to reduce the number of free parameters from $1 + 3K^2$ to 18. First, the second level of the NPA hierarchy can be derived similarly to the first one by considering the optimization of the value over vectors $|u_i\rangle = b_i |\psi\rangle$, $|v_i\rangle = c_i |\psi\rangle$, $|u_i v_j\rangle = b_i c_j |\psi\rangle$ for all i, j, and $|u_i u_j\rangle = b_i b_j |\psi\rangle$, $|v_i v_j\rangle = c_i c_j |\psi\rangle$ for $i \neq j$ (noting that $|u_i u_i\rangle = |v_i v_i\rangle = |\psi\rangle$), and taking the relations on the vectors to be those that follow immediately from the relations on the operators. As for the first level, we may assume that the Gram matrix is real, and that it is invariant under the permutations of the indices $i \mapsto \sigma(i)$ and $u_i \leftrightarrow v_i$ as in Theorem 6. Then, this gives us that the optimization is over 18 independent parameters $g_1, \ldots, g_{18} \in \mathbb{R}$, where the inner products of the vectors satisfy

$$
\begin{aligned}
1 &= \langle\psi|\psi\rangle = \langle u_i|u_i\rangle = \langle v_i|v_i\rangle = \langle u_i v_i|u_i v_i\rangle = \langle u_i v_j|u_i v_j\rangle = \langle u_i u_j|u_i u_j\rangle = \langle v_i v_j|v_i v_j\rangle \\
0 &= \langle u_i|v_j\rangle = \langle\psi|u_i v_j\rangle = \langle u_i v_i|u_i u_j\rangle = \langle u_i v_i|u_j u_i\rangle = \langle u_i v_j|u_i u_k\rangle = \langle u_i v_j|u_k u_i\rangle \\
&= \langle u_i v_j|u_k u_l\rangle = \langle u_i v_i|v_i v_j\rangle = \langle u_i v_i|v_j v_i\rangle = \langle u_i v_j|v_k v_j\rangle = \langle u_i v_j|v_j v_k\rangle = \langle u_i v_j|v_k v_l\rangle \\
&= \langle u_i u_j|v_k v_i\rangle = \langle u_i u_j|v_j v_k\rangle \\
g_1 &= \langle\psi|u_i\rangle = \langle\psi|v_i\rangle = \langle u_i|u_i v_i\rangle = \langle v_i|u_i v_i\rangle = \langle u_i|u_i v_j\rangle = -\langle v_i|u_j v_i\rangle = \langle u_i|u_i u_j\rangle = \langle v_i|v_i v_j\rangle \\
g_2 &= \langle u_i|v_i\rangle = \langle\psi|u_i v_i\rangle = \langle u_i v_j|u_i u_j\rangle = -\langle u_i v_j|v_j v_i\rangle \\
g_3 &= \langle u_i|u_j\rangle = \langle v_i|v_j\rangle = \langle v_i v_j|v_i v_j\rangle = \langle u_i v_i|u_i v_j\rangle = -\langle u_i v_i|u_j v_i\rangle = \langle\psi|u_i u_j\rangle = \langle\psi|v_i v_j\rangle \\
&= \langle u_i v_j|u_i v_k\rangle = \langle u_i v_j|u_k v_j\rangle = \langle u_i u_j|u_i u_k\rangle = \langle v_i v_j|v_i v_k\rangle \\
g_4 &= \langle u_i|u_j v_j\rangle = -\langle u_i|u_j v_i\rangle = \langle v_i|u_j v_j\rangle = \langle v_i|u_i v_j\rangle = \langle v_i|u_i u_j\rangle = -\langle v_i|u_j u_i\rangle \\
&= \langle u_i|v_i v_j\rangle = -\langle u_i|v_j v_i\rangle \\
g_5 &= \langle u_i|u_j v_k\rangle = -\langle v_i|u_j v_k\rangle = \langle v_i|u_j u_k\rangle = \langle u_i|v_j v_k\rangle \\
g_6 &= \langle u_i v_i|u_j v_j\rangle = -\langle u_i u_j|v_j v_i\rangle \\
g_7 &= \langle u_i v_j|u_j v_i\rangle = -\langle u_i u_j|v_i v_j\rangle \\
g_8 &= \langle u_i v_j|u_k v_i\rangle = -\langle u_i u_j|v_i v_k\rangle = \langle u_i u_j|u_k v_k\rangle \\
g_9 &= \langle u_i v_j|u_k v_l\rangle = \langle u_i u_j|v_k v_l\rangle \\
g_{10} &= \langle u_i|u_j u_i\rangle = \langle v_i|v_j v_i\rangle \\
g_{11} &= \langle u_i|u_j u_k\rangle = \langle v_i|v_j v_k\rangle \\
g_{12} &= \langle u_i v_j|u_j u_i\rangle = -\langle u_i v_j|v_i v_j\rangle \\
g_{13} &= \langle u_i v_i|u_j u_k\rangle = \langle u_i v_j|u_k u_j\rangle = \langle u_i v_i|v_j v_k\rangle = -\langle u_i v_j|v_k v_i\rangle \\
g_{14} &= \langle u_i v_j|u_j u_k\rangle = -\langle u_i v_j|v_i v_k\rangle \\
g_{15} &= \langle u_i u_j|u_j u_i\rangle = \langle v_i v_j|v_j v_i\rangle \\
g_{16} &= \langle u_i u_j|u_k u_i\rangle = \langle v_i v_j|v_k v_i\rangle \\
g_{17} &= \langle u_i u_j|u_k u_j\rangle = \langle v_i v_j|v_k v_j\rangle \\
g_{18} &= \langle u_i u_j|u_k u_l\rangle = \langle v_i v_j|v_k v_l\rangle
\end{aligned}
$$

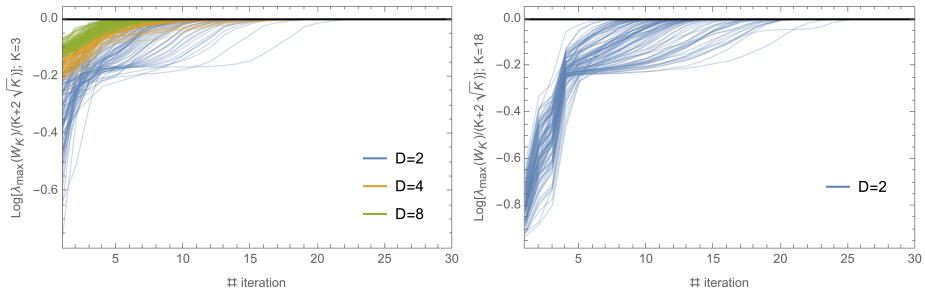


Figure 4. Optimizing the maximum eigenvalue of the operator W_K using a seesaw algorithm. Left panel: $K = 3$; right panel: $K = 18$. We consider different matrix sizes D and we run 100 instances of the algorithm (with random initializations) for each dimension, for $M = 10$ iterations of the three steps. The X axis tracks the intermediate step of the algorithm, ranging from 1 to $3M = 30$. The Y axis tracks the log-relative error $\log[\lambda_{\max}(W_K)/(K + 2\sqrt{K})]$. Note that all the curves are below 0, providing evidence towards Conjecture 1.

for all distinct $1 \leqslant i, j, k, l \leqslant K$. Then, the SDP simplifies to the form

$$\begin{aligned} \sup_{g} \quad & 2\,K\,g_1 + K\,g_2\,, \\ \text{subject to} \quad & \cdot\ G_0 + g_1\,G_1 + \ldots + g_{18}\,G_{18} \succcurlyeq 0\,, \\ & \cdot\ g_1, g_2, \ldots, g_{18} \in \mathbb{R}\,, \end{aligned}$$

where G_0 is the $1 + 3K^2$-dimensional matrix that has components 1 where the Gram matrix G is 1 and zeros elsewhere, G_1 is the matrix that has components ± 1 where G is $\pm g_1$, G_2 is the matrix that has components ± 1 where G is $\pm g_2$, and so on. We solve this SDP numerically to find the winning probabilities displayed in the second column of the above table.

4.4 Numerical Result with the Alternating Optimization Algorithm

We present in this subsection a heuristic algorithm for optimizing the largest eigenvalue of the operator

$$W_K = \sum_{k=1}^{K} \Big(\Gamma_k \otimes B_k \otimes I + \Gamma_k \otimes I \otimes C_k + I \otimes B_k \otimes C_k \Big)\,,$$

over self-adjoint contractions $B_1, C_1, \ldots, B_K, C_K$. We shall use the *alternating optimization* (or *seesaw*) method [BH02]. Note that our goal is to maximize a convex function over a convex set, *i.e.*

$$\max_{\substack{\|z\|=1 \\ \|B_k\|_{\mathrm{op}} \leqslant 1 \\ \|C_k\|_{\mathrm{op}} \leqslant 1}} \langle z | W_K | z \rangle\,,$$

hence our problem does not fall in the classical convex optimization framework.

Our algorithm optimizes iteratively over each of the variables z, $\{B_k\}_{k=1}^K$, and $\{C_k\}_{k=1}^K$ for a pre-determined number of iterations M. The variables z, B_k, C_k are initialized with random values (z uniform on the unit sphere of $\mathbb{C}^d \otimes \mathbb{C}^D \otimes \mathbb{C}^D$, and B_k, C_k i.i.d. with Haar-distributed eigenvectors and half of eigenvalues ± 1). We give below the details of each optimization step.

1. Optimizing z: compute the largest eigenvalue of the current operator P and assign to z the corresponding eigenvector.

2. Optimizing the contractions B: permute the first two tensors to rewrite the problem as

$$\langle z | \sum_{k=1}^{K} \Gamma_k \otimes I \otimes C_k | z \rangle + \max_{\|B_k\|_{\mathrm{op}} \leqslant 1} \langle z_{1 \leftrightarrow 2} | \sum_{k=1}^{K} B_k \otimes (\Gamma_k \otimes I + I \otimes C_k) | z_{1 \leftrightarrow 2} \rangle\,,$$

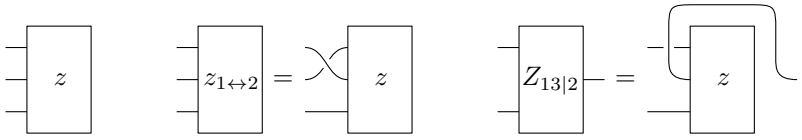


Figure 5. Graphical representations of the tensors z, $z_{1\leftrightarrow 2}$, and $Z_{13|2}$.

where $z_{1\leftrightarrow 2}$ is the 3-tensor z with the first two factors permuted. Clearly, the maximum above is equal to the sum of maxima over individual B_k's that we can further decompose as

$$\begin{aligned}
&\max_{\|B_k\|_{\mathrm{op}}\leqslant 1} \langle z_{1\leftrightarrow 2}|B_k \otimes (\Gamma_k \otimes I + I \otimes C_k)|z_{1\leftrightarrow 2}\rangle \\
&= \max_{\|B_k\|_{\mathrm{op}}\leqslant 1} \langle B_k, Z_{13|2}^*(\Gamma_k \otimes I + I \otimes C_k)Z_{13|2}\rangle \\
&= \|Z_{13|2}^*(\Gamma_k \otimes I + I \otimes C_k)Z_{13|2}\|_1 \,,
\end{aligned}$$

where $Z_{13|2} \in \mathcal{M}_{Dd\times D}$ is the reshaping of the 3-tensor $z_{1\leftrightarrow 2}$, see Figure 5. In the last equality above we have used the following fact:

$$\max_{\|B\|_{\mathrm{op}}\leqslant 1} \langle B, X\rangle = \|X\|_1 \,,$$

with the maximum being attained for

$$B_{\mathrm{opt}} = \sum_i \mathrm{sign}(\lambda_i)\, |x_i\rangle\langle x_i| \qquad \text{for} \qquad X = \sum_i \lambda_i\, |x_i\rangle\langle x_i| \,.$$

We apply this procedure for all the maximization problems corresponding to the B_k's and update the matrices B_k accordingly.

3. Optimizing the contractions C: similar procedure as above, up to tensor permutation.

We present in Figure 4 the results of numerical experiments in the case $K = 3$ and $K = 18$ for different matrix sizes D. The results we find agree with Conjecture 1.

Acknowledgements

The authors gratefully acknowledge Arthur Mehta for the many useful comments and support throughout the development of this work. We are also thankful to Sang-Jung Park for the insightful discussions and constructive feedback on the preliminary version of the manuscript. Special thanks go to Benoît Collins for his many enlightening discussions, as well as to Andreas Bluhm, Mariia Elovenkova, Aabhas Gulati, and Faedi Loulidi for their thoughtful comments and suggestions.

We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), MITACS grant FR113029, and of the ANR project ESQuisses, grant number ANR-20-CE47-0014-01. P.B. acknowledges the support of the Institute for Quantum Technologies in Occitanie. E.C. acknowledges the support of a CGS D scholarship from Canada's NSERC. C.P. acknowledges the support of the ANR project "Quantum Trajectories" grant no. ANR-20-CE40-0024-0. D.R. acknowledges the support of the Air Force Office of Scientific Research under award number FA9550-20-1-0375. This research was enabled in part by support provided by Compute Ontario and the Digital Research Alliance of Canada.

References

[AB24] P. Ananth and A. Behera. A modular approach to unclonable cryptography. In *Advances in Cryptology — CRYPTO 2024*, volume 7, pages 3–37, 2024. DOI: 10.1007/978-3-031-68394-7_1.

[ABF+16] G. Alagic, A. Broadbent, B. Fefferman, T. Gagliardoni, C. Schaffner, and M. St. Jules. Computational security of quantum encryption. In *Information Theoretic Security (ICITS 2016)*, pages 47–71, 2016. DOI: 10.1007/978-3-319-49175-2_3.

[AK21] P. Ananth and F. Kaleoglu. Unclonable encryption, revisited. In *Theory of Cryptography (TCC 2021)*, volume 1, pages 299–329, 2021. DOI: 10.1007/978-3-030-90459-3_11.

[AKL+22] P. Ananth, F. Kaleoglu, X. Li, Q. Liu, and M. Zhandry. On the feasibility of unclonable encryption, and more. In *Advances in Cryptology — CRYPTO 2022*, volume 2, pages 212–241, 2022. DOI: 10.1007/978-3-031-15979-4_8.

[AKL23] P. Ananth, F. Kaleoglu, and Q. Liu. Cloning games: A general framework for unclonable primitives. In *Advances in Cryptology — CRYPTO 2023*, volume 5, pages 66–98, 2023. DOI: 10.1007/978-3-031-38554-4_3.

[AKY25] P. Ananth, F. Kaleoglu, and H. Yuen. Simultaneous Haar indistinguishability with applications to unclonable cryptography. *16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, (7): 1–23, 2025. DOI: 10.4230/LIPIcs.ITCS.2025.7.

[BC23a] A. Broadbent and E. Culf. Rigidity for monogamy-of-entanglement games. In *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, pages 28:1–28:29, 2023. DOI: 10.4230/LIPIcs.ITCS.2023.28.

[BC23b] A. Broadbent and E. Culf. Uncloneable cryptographic primitives with interaction. E-print arXiv:2303.00048 [quant-ph], 2023. arXiv: 2303.00048.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics Physique Fizika*, 1(3): 195–200, 1964. DOI: 10.1103/PhysicsPhysiqueFizika.1.195.

[BH02] J. C. Bezdek and R. J. Hathaway. Some notes on alternating optimization. In *Advances in Soft Computing — AFSS 2002*, pages 288–300, 2002. DOI: 10.1007/3-540-45631-7_39.

[BL20] A. Broadbent and S. Lord. Uncloneable quantum encryption via oracles. In *15th Conference on the Theory of Quantum Computation, Communication, and Cryptography (TQC 2020)*, pages 4:1–4:22, 2020. DOI: 10.4230/LIPIcs.TQC.2020.4.

[BN18] A. Bluhm and I. Nechita. Joint measurability of quantum effects and the matrix diamond. *Journal of Mathematical Physics*, 59(11): 112202, 2018. DOI: 10.1063/1.5049125.

[Cho75] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3): 285–290, 1975. DOI: 10.1016/0024-3795(75)90075-0.

[CHSH69] J. F. Clauser, M. A. Horne., A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15): 880–884, 1969. DOI: 10.1103/PhysRevLett.23.880.

[CHV24] C. Chevalier, P. Hermouet, and Q.-H. Vu. Towards unclonable cryptography in the plain model. E-print arXiv:2311.16663 [quant-ph], 2024. arXiv: 2311.16663.

[Cir80] B. S. Cirel'son. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2): 93–100, 1980. DOI: 10.1007/BF00417500.

[CKW00] V. Coffman, J. Kundu, and W. K. Wootters. Distributed entanglement. *Physical Review A*, 61(5): 052306, 200. DOI: 10.1103/PhysRevA.61.052306.

[Deu83] D. Deutsch. Uncertainty in quantum measurements. *Physical Review Letters*, 50(9): 631–633, 1983. DOI: 10.1103/PhysRevLett.50.631.

[dGHG23] C. de Gois, K. Hansenne, and O. Gühne. Uncertainty relations from graph theory. *Physical Review A*, 107(6): 062211, 2023. DOI: 10.1103/PhysRevA.107.062211.

[Die06] K. Dietz. Generalized Bloch spheres for m-qubit states. *Journal of Physics A*, 39(6): 1433, 2006. DOI: 10.1088/0305-4470/39/6/016.

[DL03] C. Doran and A. Lasenby. *Geometric Algebra for Physicists*. Cambridge University Press, 2003. DOI: 10.1017/CBO9780511807497.

[GALC25] I. George, R. Allerstorfer, P. V. Lunel, and E. Chitambar. Orthogonality broadcasting and quantum position verification. *New Journal of Physics*, 27(5): 054511, 2025. DOI: 10.1088/1367-2630/add87c.

[GM84] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2): 270–299, 1984. DOI: 10.1016/0022-0000(84)90070-9.

[GZ20] M. Georgiou and M. Zhandry. Unclonable decryption keys. Cryptology ePrint Archive, Report 2020/877, 2020. Online: http://eprint.iacr.org/2020/877.

[Hel02] W. J. Helton. "Positive" noncommutative polynomials are sums of squares. *Annals of Mathematics*, 156(2): 675–694, 2002. DOI: 10.2307/3597203.

[HKMS19] J. W. Helton, I. Kelp, S. McCullough, and M. Schweighofer. Dilations, linear matrix inequalities, the matrix cube problem and beta distributions. *Memoirs of the American Mathematical Society*, 257(1232): 1–118, 2019. DOI: 10.1090/memo/1232.

[HKNY24] T. Hiroka, F. Kitagawa, R. Nishimaki, and T. Yamakawa. *Robust Combiners and Universal Constructions for Quantum Cryptography*, pages 126–158. 2024. DOI: 10.1007/978-3-031-78017-2_5.

[HM04] J. Helton and S. McCullough. A positivstellensatz for non-commutative polynomials. *Transactions of the American Mathematical Society*, 356(9): 3721–3737, 2004. DOI: 10.1090/S0002-9947-04-03433-6.

[HO21] M. B. Hastings and R. O'Donnell. Optimizing strongly interacting fermionic Hamiltonians. In *STOC 2022: Proceedings of the 54th ACM SIGACT Symposium on Theory of Computing*, pages 776–789, 2021. DOI: 10.1145/3519935.3519960.

[JNV+21] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen. MIP* = RE. *Communications of the ACM*, 64(11): 131–138, 2021. DOI: 10.1145/3485628.

[JW93] P. Jordan and E. P. Wigner. Über das Paulische Äquivalenzverbot. In *The Collected Works of Eugene Paul Wigner*, pages 109–129, 1993. DOI: 10.1007/978-3-662-02781-3_9.

[KL07] J. Katz and Y. Lindell. *Introduction to Modern Cryptography*. Chapman & Hall/CRC, 2007.

[KT25] S. Kundu and E. Y.-Z. Tan. Device-independent uncloneable encryption. *Quantum*, 9: 1582, 2025. DOI: 10.22331/q-2025-01-08-1582.

[KW99] M. Keyl and R. F. Werner. Optimal cloning of pure states, testing single clones. *Journal of Mathematical Physics*, 40(7): 3283–3299, 1999. DOI: 10.1063/1.532887.

[KW04] M. Koashi and A. Winter. Monogamy of quantum entanglement and other correlations. *Physical Review A*, 69(2): 022309, 2004. DOI: 10.1103/PhysRevA.69.022309.

[Las01] J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3): 796–817, 2001. DOI: 10.1137/S1052623400366802.

[Lou01] P. Lounesto. *Clifford Algebras and Spinors*. Cambridge University Press, 2nd edition, 2001. DOI: 10.1017/cbo9780511526022.

[McC01] S. McCullough. Factorization of operator-valued polynomials in several non-commuting variables. *Linear Algebra and its Applications*, 326(1): 193–203, 2001. DOI: 10.1016/S0024-3795(00)00285-8.

[MH24] M. B. Morán and F. Huber. Uncertainty relations from state polynomial optimization. *Physical Review Letters*, 132(20): 200202, 2024. DOI: 10.1103/PhysRevLett.132.200202.

[MM24] A. Mehta and A. Müller. Unclonable functional encryption. E-print arXiv:2410.06029 [quant-ph], 2024. arXiv: 2410.06029.

[MST21] C. Majenz, C. Schaffner, and M. Tahmasbi. Limitations on uncloneable encryption and simultaneous one-way-to-hiding. E-print arXiv:2103.14510 [quant-ph], 2021. arXiv: 2103.14510.

[NPA08] M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7): 073013, 2008. DOI: 10.1088/1367-2630/10/7/073013.

[Ost16] D. Ostrev. The structure of nearly-optimal quantum strategies for the non-local XOR games. *Quantum Information & Computation*, 16(13&14): 1191–1211, 2016. DOI: 10.26421/QIC16.13-14-6.

[Per90] A. Peres. Neumark's theorem and quantum inseparability. *Foundations of Physics*, 20(12): 1441–1453, 1990. DOI: 10.1007/BF01883517.

[Pis03] G. Pisier. *Introduction to Operator Space Theory*. Cambridge University Press, 2003. DOI: 10.1017/cbo9781107360235.

[RXL26] M.-O. Renou, X. Xu, and L. T. Ligthart. Two convergent NPA-like hierarchies for the quantum bilocal scenario. *Journal of Mathematical Physics*, 67(1), 2026. DOI: 10.1063/5.0211008.

[Slo11] W. Slofstra. Lower bounds on the entanglement needed to play XOR non-local games. *Journal of Mathematical Physics*, 52(10): 102202, 2011. DOI: 10.1063/1.3652924.

[SW22] O. Sattath and S. Wyborski. Uncloneable decryptors from quantum copy-protection. E-print arXiv:2203.05866 [quant-ph], 2022. arXiv: 2203.05866.

[TFKW13] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10): 103002, 2013. DOI: 10.1088/1367-2630/15/10/103002.

[Tsi93] B. S. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, 8: 329–345, 1993.

[Wat18] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. DOI: 10.1017/9781316848142.

[Wer98] R. F. Werner. Optimal cloning of pure states. *Physical Review A*, 58(3): 1827, 1998. DOI: 10.1103/PhysRevA.58.1827.

[Wie83] S. Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1): 78–88, 1983. DOI: 10.1145/1008908.1008920.

[WW08] S. Wehner and A. Winter. Higher entropic uncertainty relations for anti-commuting observables. *Journal of Mathematical Physics*, 49(6): 062105, 2008. DOI: 10.1063/1.2943685.

[XSW24] Z.-P. Xu, R. Schwonnek, and A. Winter. Bounding the joint numerical range of Pauli strings by graph parameters. *PRX Quantum*, 5(2): 020318, 2024. DOI: 10.1103/PRXQuantum.5.020318.

[Zim90] R. J. Zimmer. *Essential results of functional analysis*. University of Chicago Press, 1990.