# Cloning Games, Black Holes and Cryptography


Alexander Poremba[*] MIT

Seyoon Ragavan[†] MIT

Vinod Vaikuntanathan[‡] MIT



**Abstract**

The no-cloning principle has played a foundational role in quantum information and cryptography. Following a long-standing tradition of studying quantum mechanical phenomena through the lens of interactive games, Broadbent and Lord (TQC 2020) formalized *cloning games* in order to quantitatively capture no-cloning in the context of unclonable encryption schemes.

The conceptual contribution of this paper is the new, natural, notion of *Haar cloning games* together with two applications. In the area of black-hole physics, our game reveals that, in an idealized model of a black hole which features Haar random (or *pseudorandom*) scrambling dynamics, the information from infalling entangled qubits can only be recovered from either the interior or the exterior of the black hole—but never from both places at the same time. In the area of quantum cryptography, our game helps us construct succinct unclonable encryption schemes from the existence of *pseudorandom unitaries*, thereby, for the first time, bridging the gap between "MicroCrypt" and unclonable cryptography.

The technical contribution of this work is a tight analysis of Haar cloning games which requires us to overcome many long-standing barriers in our understanding of cloning games:

- *Are there cloning games which admit no non-trivial winning strategies*? Resolving this particular question turns out to be crucial for our application to black-hole physics. Existing work analyzing the $n$-qubit BB84 game and the subspace coset game only achieve the bounds of $2^{-0.228n}$ and $2^{-0.114n+o(n)}$, respectively, while the trivial adversarial strategy wins with probability $2^{-n}$.

  We show that the Haar cloning game is the *hardest* cloning game, by demonstrating a worst-case to average-case reduction for a large class of games which we refer to as oracular cloning games. We then show that the Haar cloning game admits *no non-trivial winning strategies*.

- *All existing works analyze $1 \mapsto 2$ cloning games; can we prove bounds on $t \mapsto t+1$ games for large $t$?* Such bounds are crucial in our application to unclonable cryptography. Unfortunately, the BB84 game is not even $2 \mapsto 3$ secure, and the subspace coset game is not $t \mapsto t+1$ secure for a polynomially large $t$. We show that the Haar cloning game is $t \mapsto t+1$ secure provided that $t = o(\log n / \log\log n)$, and we conjecture that this holds for $t$ that is polynomially large (in $n$).

Answering these questions provably requires us to go beyond existing methods (Tomamichel, Fehr, Kaniewski and Wehner, New Journal of Physics 2013). In particular, we show a new technique for analyzing cloning games with respect to binary phase states through the lens of binary *subtypes*, and combine it with novel bounds on the operator norms of block-wise tensor products of matrices.



[*]poremba@mit.edu
[†]sragavan@mit.edu
[‡]vinodv@mit.edu

# Contents

# 1 Introduction

*Quantum no-cloning* [WZ82] is a central property of quantum information. Roughly speaking, it says that no quantum procedure exists which can copy an unknown quantum state. This insight has even led to the design of new cryptographic primitives, starting with Wiesner's remarkable quantum money scheme [Wie83].

*Monogamy of entanglement* [Ter04] is another fundamental property of quantum information in which the no-cloning property manifests itself—it says that quantum correlations are "monogamous", and thus cannot be shared freely among multiple parties. For example, if Alice and Bob are maximally entangled and share an $n$-qubit Einstein-Podolsky-Rosen (EPR) pair [EPR35] of the form

$$|\mathsf{EPR}^n\rangle_{\mathsf{AB}} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle_{\mathsf{A}} \otimes |x\rangle_{\mathsf{B}}$$

then any third party, say Charlie, must be completely decoupled from them. Formally, for every tripartite quantum state $\rho_{\mathsf{ABC}} \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$ with the property that $\mathrm{Tr}_{\mathsf{C}}[\rho_{\mathsf{ABC}}] = \mathsf{EPR}^n_{\mathsf{AB}}$, where $\mathsf{EPR}^n_{\mathsf{AB}}$ is the density matrix which corresponds to the maximally entangled state, it must necessarily be the case that $\rho_{\mathsf{ABC}} = \mathsf{EPR}^n_{\mathsf{AB}} \otimes \sigma_{\mathsf{C}}$ for some residual state $\sigma_{\mathsf{C}}$.

Throughout history, the nature of quantum information has been fruitfully studied through the lens of *interactive games*. The celebrated works of Bell [Bel64] and those of Clauser, Horne, Shimony and Holt [CHSH69] initiated the study of so-called *non-local games*. Since then, many fundamental properties of quantum entanglement have been characterized in terms of optimal success probabilities of winning particular games [Mer90, Ara02, Har93, GHZ89, RUV12, TFKW13, JNV+21, KLVY23].

## 1.1 Games Galore: Monogamy Games and Cloning Games

**Monogamy of Entanglement Games.** Tomamichel, Fehr, Kaniewski and Wehner [TFKW13] introduced the notion of a *monogamy of entanglement game* in order to characterize entanglement monogamy using the language of non-local games. A monogamy of entanglement game $\mathsf{G}$ with respect to the question set $\Theta$, answer set $\mathcal{X}$ and measurement set $\{\mathbf{A}^\theta_x\}_{\theta \in \Theta, x \in \mathcal{X}}$ is an interactive game played by three players: a trusted referee called Alice, as well as two colluding and adversarial parties called Bob and Charlie.

1. (**Setup phase**) Bob and Charlie prepare a tripartite quantum state $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$. They send register $\mathsf{A}$ to Alice, and hold onto registers $\mathsf{B}$ and $\mathsf{C}$, respectively. Afterwards, they are no longer allowed to communicate for the remainder of the game.

2. (**Question phase**) Alice samples a random question $\theta \sim \Theta$, and then applies the corresponding measurement $\{\mathbf{A}^\theta_x\}_{x \in \mathcal{X}}$ to her register $\mathsf{A}$. Afterwards, Alice announces the question $\theta$ to both Bob and Charlie, and keeps the measurement outcome in $\mathcal{X}$ to herself.

3. (**Answer phase**) Bob and Charlie independently output a guess for Alice's outcome by applying the measurements $\{\mathbf{B}^\theta_x\}_{x \in \mathcal{X}}$ and $\{\mathbf{C}^\theta_x\}_{x \in \mathcal{X}}$ to their registers $\mathsf{B}$ and $\mathsf{C}$, respectively.

4. (**Outcome phase**) Bob and Charlie win if they both guess Alice's outcome correctly.

Here, we associate a particular *strategy* $\mathsf{S}$ employed by Bob and Charlie with the tuple consisting of the initial state $\rho$ and the positive operator-valued measurements $\{\mathbf{B}^\theta_x\}_{\theta \in \Theta, x \in \mathcal{X}}$ and $\{\mathbf{C}^\theta_x\}_{\theta \in \Theta, x \in \mathcal{X}}$. The *value* of a particular strategy $\mathsf{S}$ for the monogamy game $\mathsf{G}$ is defined as the average winning probability

$$\omega_{\mathsf{S}}(\mathsf{G}) := \mathop{\mathbb{E}}_{\theta \sim \Theta} \sum_{x \in \mathcal{X}} \mathrm{Tr}\left[(\mathbf{A}^\theta_x \otimes \mathbf{B}^\theta_x \otimes \mathbf{C}^\theta_x)\rho_{\mathsf{ABC}}\right].$$

We let $\omega(\mathsf{G})$ denote the maximal value of the game, i.e., the optimal winning probability over all strategies. An upper bound on the value of a monogamy game therefore limits the extent to which Bob and Charlie can simultaneously maintain a quantum correlation with Alice who holds a register outside of their view.

Tomamichel, Fehr, Kaniewski and Wehner [TFKW13] studied a particular monogamy of entanglement game $\mathsf{G}_{\mathrm{BB84}}$ that appears naturally in the context of quantum key distribution and the BB84 protocol [BB84]. Here, the game $\mathsf{G}_{\mathrm{BB84}}$ consists of question and answer sets $\Theta = \mathcal{X} = \{0,1\}^n$ and projective measurements $\{\mathbf{A}_x^\theta\}_{\theta,x\in\{0,1\}^n}$ with $\mathbf{A}_x^\theta = \mathsf{H}^\theta |x\rangle\langle x| \mathsf{H}^\theta$, where $\mathsf{H}$ denotes the Hadamard gate and $\mathsf{H}^\theta := \mathsf{H}^{\theta_1} \otimes \cdots \otimes \mathsf{H}^{\theta_n}$. Specifically, they showed that the optimal success probability of the game is given by

$$\omega(\mathsf{G}_{\mathrm{BB84}}) = \cos^2\left(\frac{\pi}{8}\right)^n \approx 2^{-0.228n}. \tag{1}$$

As an immediate application of the bound, [TFKW13] proved the security of a one-sided device independent quantum key-distribution protocol, as well as the soundness of a one-round position verification scheme.

Bounds on monogamy games, such as the one shown in [TFKW13], have since proven useful in many other areas of quantum cryptography, particularly in the area of unclonable cryptography. This has led to the development of unclonable encryption schemes [BL20], quantum copy-protection [Aar09, CMP22, CLLZ21, AKL$^+$22], unclonable decryption keys [GZ20], unclonable proofs [GMR23], and much more.

**Cloning Games.** The class of interactive games which are relevant for unclonable cryptography are known as *cloning games* [AKL23]. Broadly speaking, these games underlie the security of so-called *unclonable encryption* schemes which were first studied by Broadbent and Lord [BL20]. A general $1 \mapsto 2$ cloning game $\mathsf{G}_{1\mapsto 2}$ with respect to the question set $\Theta$, answer set $\mathcal{X}$, and ensemble of unitaries $\{U_\theta\}_{\theta\in\Theta}$ of dimension $|\mathcal{X}|$ is the following interactive game played by a trusted challenger, say Alice, as well as an adversary consisting of a cloner $\Phi$ and two additional players, say Bob and Charlie.

1. (**Setup phase**) Alice samples random $x \sim \mathcal{X}$ and $\theta \sim \Theta$, and sends $U_\theta |x\rangle_{\mathsf{A}}$ to the cloner $\Phi$.

   The cloner $\Phi$ splits the state into two registers $\mathsf{B}$ and $\mathsf{C}$, which he then forwards to Bob and Charlie, respectively. Afterwards, the players may no longer communicate for the rest of the game.

2. (**Question phase**) Bob and Charlie both receive the string $\theta$.

3. (**Answer phase**) Bob and Charlie independently output a guess for the element $x$.

4. (**Outcome phase**) Bob and Charlie win if they both guess $x$ correctly.

We illustrate the cloning game $\mathsf{G}_{1\mapsto 2}$ in Figure 1. A strategy $\mathsf{S}$ for the game $\mathsf{G}_{1\mapsto 2}$ consists of a cloning map $\Phi$ and a pair of positive operator-valued measurements $\mathcal{B} = \{\mathbf{B}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}$ and $\mathcal{C} = \{\mathbf{C}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}$. The *value*[1] of a particular strategy $\mathsf{S}$ for the cloning game $\mathsf{G}_{1\mapsto 2}$ is defined as the average winning probability

$$\omega_{\mathsf{S}}(\mathsf{G}_{1\mapsto 2}) = \mathop{\mathbb{E}}_{\theta\sim\Theta}\mathop{\mathbb{E}}_{x\sim\mathcal{X}} \mathrm{Tr}\left[\left(\mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta\right)\Phi_{\mathsf{A}\to\mathsf{BC}}(U_\theta |x\rangle\langle x|_{\mathsf{A}} U_\theta^\dagger)\right].$$

Similar to a monogamy of entanglement game, we use $\omega(\mathsf{G}_{1\mapsto 2})$ to denote the optimal winning probability over all joint strategies given by $\Phi$, $\mathcal{B}$ and $\mathcal{C}$. Note that there always exists a trivial strategy that succeeds with probability $1/|\mathcal{X}|$: the cloner $\Phi$ simply forwards the state $U_\theta |x\rangle$ to Bob, who can easily recover $x$ once $\theta$ becomes available, whereas Charlie simply guesses a random element in $\mathcal{X}$.

[1] We emphasize that an upper bound on the success probability of a cloning game implies something stronger than the conventional no-cloning theorem [WZ82]: if the cloner $\Phi$ can copy the state $U_\theta |x\rangle$, then $\Phi$ can certainly send the two copies to Bob and Charlie and ensure that they win the game. However, there may be other strategies for $\Phi$ that do not involve direct cloning but may nevertheless provide the players with enough information to simultaneously recover $x$ during the guessing phase.

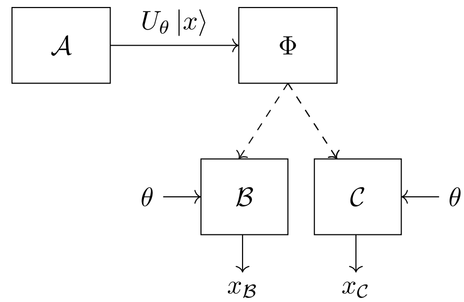


Figure 1: $1 \mapsto 2$ cloning game.

Although cloning games are syntactically quite different from monogamy games, they turn out to be closely related. Indeed, the paradigm introduced by Broadbent and Lord [BL20] implicitly[2] shows that the general $1 \mapsto 2$ cloning game in Figure 1 is in fact equivalent to a special class of monogamy games, where

- The tripartite state $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$ which is shared between Alice, Bob and Charlie is the result of applying a cloning channel $\Phi_{\mathsf{A}' \to \mathsf{BC}}$ to one half of an EPR pair, i.e.,

$$\rho_{\mathsf{ABC}} = (\mathbb{I}_{\mathsf{A}} \otimes \Phi_{\mathsf{A}' \to \mathsf{BC}})(|\mathsf{EPR}\rangle\langle\mathsf{EPR}|_{\mathsf{AA}'}).$$

- Alice's measurement $\{\mathbf{A}_x^\theta\}_{\theta \in \Theta, x \in \mathcal{X}}$ on register $\mathsf{A}$ is a projective rank-1 measurement of the form $\mathbf{A}_x^\theta = \bar{U}_\theta |x\rangle\langle x| \bar{U}_\theta^\dagger$, where $\bar{U}_\theta$ denotes the complex conjugate of $U_\theta$.

Therefore, the standard approach for deriving upper bounds on the value of cloning games is by analyzing the corresponding monogamy of entanglement game. To this day, the majority of unclonable cryptography is rooted in either $n$-qubit BB84 states with $U_\theta = \mathsf{H}^\theta$ [TFKW13, BL20] or subspace coset states over $\mathbb{F}_2^n$, where $U_\theta$ encodes a shift of a random $n/2$-dimensional subspace $A \subset \mathbb{F}_2^n$ [CLLZ21, CV22].

**Limitations on Cloning Games.** Despite their success in the field of unclonable cryptography, many fundamental gaps in our understanding of cloning games remain; in particular:

- **Optimal games:** Prior work on cloning games for $\mathcal{X} = \{0,1\}^n$ has shown the upper bounds $\cos^2\left(\frac{\pi}{8}\right)^n$ and $\sqrt{e}\cos\left(\frac{\pi}{8}\right)^n$ in the case of BB84 states [TFKW13] and subspace coset states [CV22], respectively. In contrast, a trivial strategy always succeeds with probability $2^{-n}$, and this holds for any cloning game. Are there *especially hard* cloning games which have asymptotically optimal bounds of the form $O(2^{-n})$? Closing this gap has important consequences, which we discuss in Section 2.2.

- **Quantum pseudorandomness:** A recent line of work [Kre21, AQY22, AGQY22, BCQ23] showed how to build quantum cryptography from *pseudorandom states and unitaries*, which are potentially weaker than than one-way functions [Kre21]. To this day, however, the worlds of quantum pseudorandomness and unclonable cryptography have been completely disconnected, as observed in [MPSY24, AMP24]. This begs the question: do pseudorandom unitaries give rise to interesting unclonable cryptographic primitives? The analysis of *Haar cloning games*, where $U_\theta$ is a *Haar* unitary (or, a unitary from a design), is far beyond the scope of existing techniques, as we explain in Section 2.1.

[2] We give a formal proof of this equivalence in Appendix A. At a high level, the statement follows from the ricochet property of EPR pairs, which allows Alice to "teleport" $U_\theta |x\rangle$ into the cloner's register by appropriately measuring her half of the EPR pair.

- **Applications beyond cryptography:** Can cloning games offer new insights in other scenarios where no-cloning and monogamy of entanglement play an important role, such as in black-hole physics? Recent works studied idealized models of black holes which rely on Haar random or pseudorandom unitary dynamics [HP07, KP23, EFL+24], which begs the question: can cloning games with Haar random unitaries help us understand how quantum information gets scrambled inside of a black hole?
- **Multi-copy security:** Can we extend $1 \mapsto 2$ cloning games towards $t \mapsto t+1$ cloning games? Here, the cloner $\Phi$ receives $t$ identical copies of the initial state, i.e., $(U_\theta |x\rangle)^{\otimes t}$, and there are $t+1$ players $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$ who simultaneously seek to recover $x$. This was posed as an open question in [MPSY24, AMP24], where the latter initiated the study of multi-copy security in the context of revocable quantum cryptography. Not only is prior work limited to $1 \mapsto 2$ cloning games, all existing unclonable cryptography becomes completely insecure if $t$ is allowed to grow polynomially [AMP24].

### 1.2 Our Work: Haar Cloning Games

In this work, we overcome many prior limitations in our understanding of cloning games; in particular, we make progress on all of the aforementioned questions. We give an overview of our contributions below.

**Oracular Cloning Games.** We significantly generalize the notion of a $1 \mapsto 2$ cloning game, and initiate the study of $t \mapsto t+1$ cloning games (see Section 6.2). Inspired by [AMP24], we also define a new relaxation of cloning games which we call *oracular cloning games*: rather than reveal the string $\theta$ in the clear as part of the guessing phase, we instead allow the players to query oracles for the unitary $U_\theta$ and its inverse $U_\theta^\dagger$. The main advantage behind this relaxation is that it allows us to consider *pseudorandom unitaries* in the context of cloning games. Thanks to this model, we can invoke the security of pseudorandom unitaries and analyze *Haar cloning games* instead; note that this switch is generally not possible in the standard notion of a cloning game (since in this case the secret key $\theta$ will eventually be disclosed to the adversaries).

**Worst-Case to Average-Case Reductions.** Motivated by the question of whether $1 \mapsto 2$ cloning games with asymptotically optimal bounds exist, we ask: which cloning game is the "hardest" of all? Our first technical contribution is a *worst-case to average-case reduction* for $t \mapsto t+1$ cloning games; we argue that a Haar cloning game instantiated with a Haar random (or pseudorandom) unitary is *at least as hard* as any other cloning game. At a high level, our proof exploits the invariance of the Haar measure over the unitary group. Thanks to this observation, we can indirectly analyze cloning games which are instantiated using a pseudorandom unitary or a unitary design—we simply pass to another cloning game that is technically easier to analyze. We give a proof of our worst-case to average-case reduction in Section 6.3.

**New Techniques for Cloning Games with Binary Phase States.** Because all existing constructions for $1 \mapsto 2$ cloning games fail in the $t \mapsto t+1$ setting [AMP24], this forces us to seek out new candidates beyond BB84 states and subspace coset states. One natural candidate is to consider pseudorandom unitaries $U_\theta$, where $\theta$ describes the key. However, because such cloning games appear difficult to analyze directly, we instead focus on *binary phase states* as a alternative candidate for $t \mapsto t+1$ cloning games—thanks to our worst-case to average-case reduction, such an analysis suffices. Specifically, we study states of the form

$$|\psi_x^f\rangle = 2^{-n/2} \sum_{y \in \{0,1\}^n} (-1)^{f(y)+\langle x,y\rangle} |y\rangle .$$

In other words, we let $|\psi_x^f\rangle = U_\theta |x\rangle$, where $U_\theta := \mathsf{U}_f \mathsf{H}^{\otimes n}$ and where $\mathsf{U}_f$ is a diagonal phase operator for a Boolean function $f : \{0,1\}^n \to \{0,1\}$ which is of the form

$$\mathsf{U}_f = \sum_{y \in \{0,1\}^n} (-1)^{f(y)} |y\rangle\langle y| \,.$$

Similar binary phase states have been considered in the context of quantum pseudorandomness [JLS18, BS19, Col23], and have been shown to be computationally indistinguishable from a Haar random state (even with a polynomial number of copies). Our contributions for analyzing binary phase states are two-fold:

- We show that existing techniques are fundamentally insufficient for showing asymptotically optimal bounds of the form $O(2^{-n})$, even in the $1 \mapsto 2$ setting. In Section 7.2, we analyze a corresponding binary phase monogamy game using standard techniques which are rooted in [TFKW13]. We prove a bound of the form $\widetilde{O}(2^{-n/2})$ for a particular class of functions $f$, which significantly improves on prior bounds but is far from the desired bound of $O(2^{-n})$. We show that this is an inherent limitation of the [TFKW13] technique; as we show in Section 7.3, we cannot hope to prove a better upper bound than this for *any* monogamy game of the desired form using their techniques.

- We develop fundamentally new techniques for analyzing binary phase states in the $t \mapsto t+1$ oracular cloning game setting. Thanks to these techniques, we can show the *first* asymptotically optimal bound $O(2^{-n})$, provided[3] that $t = o(\log n / \log\log n)$ and that all players only make one query to $\mathsf{U}_f$. Thanks to this restriction, it suffices to analyze simple *binary phase twirls* of the form

$$\mathop{\mathbb{E}}_f \operatorname{Tr}\left[\mathsf{U}_f^{\otimes 2t+1}\, \Xi\, \mathsf{U}_f^{\otimes 2t+1} \rho\right],$$

  for some Hermitian operator $\Xi$ and state $\rho$ that we unpack in Section 9.1. Expressions of this form have previously been studied in terms of *binary types*, such as in [AGQY22]. However, in our setting, binary types do not appear to have sufficient structure to obtain the kinds of spectral bounds we would need to bound the above expression. To get around this barrier, we introduce a refinement of binary types which we refer to as *binary subtypes*. These are much more structured and combinatorial in nature, and essentially reduce the task of bounding the above expression to analyzing the operator norms of block-wise tensor products of matrices. We go more into detail in Section 2.1 and Section 8.

**Resolving Central Questions.** To demonstrate the full potential of our new insights into cloning games, we give two applications of our techniques which help resolve fundamental open questions in the field.

- **Black Hole Cloning Games:** In Section 4, we analyze a new three-player game which is designed to capture monogamy and no-cloning in the context of evaporating black holes (see Fig. 2). Our results offer new quantitative insights into the *black hole information paradox* [Haw76, Pre92, HP07] and suggest that, in an idealized model of a black hole which features Haar random (or pseudorandom) scrambling dynamics, the information from infalling entangled qubits can only be recovered from either the interior or the exterior of the black hole—but never from both places at the same time.

- **Unclonable Cryptography in "MicroCrypt":** In Section 5, we give an affirmative answer to an open question which was recently posed in [MPSY24]; namely: do interesting unclonable cryptographic primitives exist, even in a world in which $\mathsf{P} = \mathsf{NP}$? We construct succinct unclonable encryption schemes from the existence of pseudorandom unitaries; thereby, for the first time, bridging the gap between the worlds of quantum pseudorandomness and unclonable cryptography.

[3] With that said, we remark that this construction could very well be secure even for $t$ that is polynomially large in $n$.

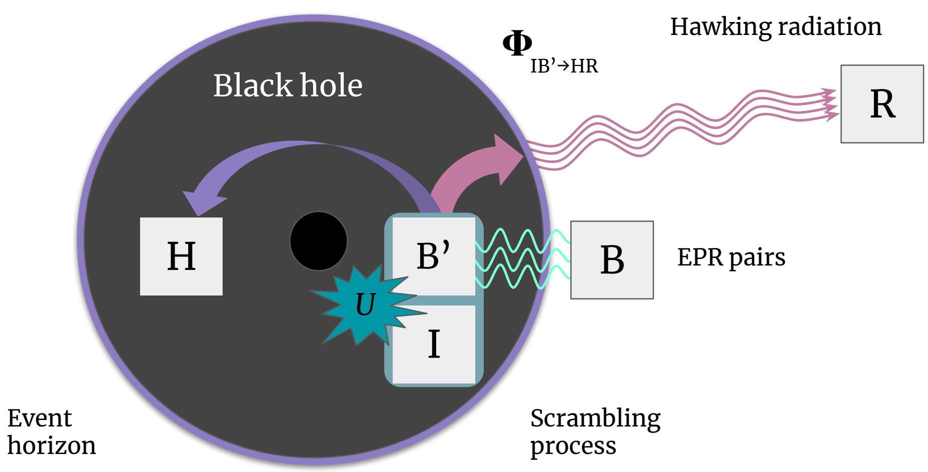


Figure 2: **Black Hole Cloning Game**. Entangled particles emerge near the boundary and form a $k$-qubit EPR pair $|\mathsf{EPR}\rangle_{\mathsf{B}'\mathsf{B}}$, of which register $\mathsf{B}'$ falls inside of the black hole, and register $\mathsf{B}$ is given to Alice. The interior of the black hole, modeled as $|0^{n-k}\rangle_{\mathsf{I}}$, together with the $k$ infalling qubits in register $\mathsf{B}'$, undergo a *scrambling process*. Here, the internal dynamics of the black hole are described a random $n$-qubit unitary time-evolution operator $U$ which gets applied to registers $\mathsf{B}'\mathsf{I}$. A quantum channel $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$ processes the internal qubits into two registers: a register $\mathsf{H}$ corresponding to the qubits within the event horizon, and a register $\mathsf{R}$ corresponding to the emitted Hawking radiation. Charlie (who falls inside of the black hole) receives register $\mathsf{H}$, whereas Bob (who is a distant observer) receives register $\mathsf{R}$. The two observers are allowed to have some knowledge of the internal dynamics $U$, and thus receive oracles for $U$ and $U^\dagger$. Finally, Alice measures $\mathsf{B}$, and Bob and Charlie win if they simultaneously guess her outcome correctly.

In the remainder of the introduction, we give an overview for each of our main applications. First, in Section 1.3, we discuss our contributions to black-hole physics. Then, in Section 1.4, we discuss our contributions to quantum cryptography. Next, in Section 2, we give a detailed technical overview.

### 1.3 Application: Black Hole Cloning Games

What happens when entangled particles fall into a black hole? Does the information get destroyed, or is it effectively conserved and eventually radiates out in some scrambled form? This question has puzzled physicists for many decades. The endeavour of trying to reconcile the predictions of quantum mechanics and general relativity has led to the famous *black hole information paradox* [Haw76, Pre92].

In this section, we first provide some relevant context on the black hole information paradox, and then give an overview of how we revisit the problem using the language of cloning games.

**Black-Hole Radiation Decoding.** In his seminal work, Hawking [Haw76] made the remarkable prediction that black holes are not completely black—they slowly emit what is now known as *Hawking radiation* at a rate per unit time which scales like $\sim n^{-1/2}$, where $n$ denotes the number of qubits or internal degrees of freedom of the black hole. This means that it would take time $\sim n^{3/2}$ for the black hole to radiate away a signficant fraction of its qubits [Bek72]. Hayden and Preskill [HP07] proposed a thought experiment that illustrates the black-hole information loss problem: Suppose that Alice throws $k$ qubits into a black hole, which are maximally entangled with a second register in her possession. For simplicity, we assume that the black hole initially consists of $n - k$ qubits. After a long period of time, another distant observer, say Bob, uses the intercepted Hawking radiation (say, in the form of photons) which he has collected in the meantime, feeds it into his quantum computer and applies an appropriate computation that will decode Alice's quantum state. In principle, Bob only needs $k$ many qubits of Hawking radiation to perform such a decoding. Hayden and Preskill asked: how long would Bob have to wait before he finally starts to observe correlations between the outgoing Hawking radiation and the entangled infalling matter near the boundary? To answer this question, they made the following crucial assumption: black holes are extremely strong and efficient *information scramblers*—their internal dynamics can be modeled as a more or less *random* unitary time-evolution. This view has since been widely adopted as an idealized model of black holes [AMPS13, HH13, KP23, EFL$^+$24] and has also led to the so-called *fast scrambling conjecture* [SS08, Sho18].

Because genuine *Haar random* dynamics are known to have exponential quantum circuit complexity with overwhelming probability [Kni00], Hayden and Preskill instead opted for a weaker notion of Haar randomness; namely, that of a *unitary* 2*-design*. They showed that after slightly more than half of the black hole has evaporated (sometimes called the *Page time*), Bob finally starts to observe correlations between Alice's infalling qubits and the outgoing radiation. This led them to conclude that black holes act as *information mirrors*: while Alice's information remains concealed up until the half-way point, it then starts to emerge fairly quickly in the form of scrambled Hawking radiation.

**Do Black Holes Clone Information?** While the Hayden-Preskill thought experiment [HP07] suggests that the information which is thrown into a black hole is conserved (and ultimately comes out in the form of scrambled Hawking radiation), it does beg the question: what would an infalling observer, say Charlie, see as he falls towards the singularity (rather than intercept radiation from the outside). From Charlie's perspective, Alice's qubits fall towards the singularity and never leave. But from Bob's perspective, who stays outside of the event horizon, the qubits eventually come out in the form of scrambled Hawking radiation. This seems to lead us to the conclusion that there are two identical copies of Alice's qubits, thereby violating the *principle of quantum no-cloning* [WZ82]. This begs the question: are black holes quantum cloning machines? In an attempt to resolve such paradoxes, Susskind, Thorlacius and Uglum [STU93], as well as 't-Hooft ['t 85], proposed the notion of *black hole complementarity*—it states that the two supposed copies of Alice's qubits are not really *distinct*; rather, they represent two complementary ways of viewing the *same* quantum system. Concretely, black hole complementarity rests on the following three postulates [STU93]:

1. The entire process—from the formation to the evaporation of the black hole—can be described within the context of standard quantum theory. In particular, the evolution of the black hole can be thought of as a unitary quantum channel which takes as input the set of qubits belonging to the interior of the black hole—together with Alice's infalling qubits—and converts them into a global pure state of which a subsystem constitutes the outgoing Hawking radiation, as viewed by a distant observer.

2. Outside of the black hole's event horizon, physics can be described to a good approximation by a set of semi-classical field equations that are consistent with Hawking's predictions [Haw76].

3. A black hole is a quantum system with discrete energy levels, as viewed by a distant observer.

When taken together, the three postulates above assert that standard quantum theory, semi-classical general relativity and statistical thermodynamics are all valid as a foundation for the study of black hole evolution. Importantly, these postulates alone appear to suffice at preventing any single observer from ever witnessing an actual violation of no-cloning in a physically meaningful scenario [STU93, HP07].

A series of works [AMPS13, HH13, Aar16, Bra23] have since explored yet another related paradox—the *Firewall Paradox*—which has put black hole complementarity into doubt, and has led to the belief that black-hole radiation decoding must be *computationally intractable* as a way of avoiding paradoxes. Subsequent work by Brakerski [Bra23] draws an even more explicit connection to quantum cryptography and views this observation as a physical justification for the existence of secure quantum cryptography itself. The computational complexity of black-hole radiation decoding has since also been solidified as a central quantum information-processing task within the framework of *unitary complexity* [BEM$^+$23].

To this day, however, the black hole information paradox remains—for the most part—unresolved, and is still an on-going research area.

**This Work: Revisiting the Black Hole Information Paradox.** We seek to extend our existing understanding of the black hole information paradox in two ways. The first is that we would like to provide a new and *quantitative* characterization of cloning and entanglement monogamy which arises in the context of evaporating black holes. Many seminal works [CHSH69, TFKW13] have quantified and enhanced our understanding of physical principles (e.g., the nature of entanglement) through the formulation and analysis of certain interactive games; our first goal is to do the same for the black hole information paradox:

*Question One: Can we give a quantitative bound on the extent to which two observers—one falling inside of a black hole, and another intercepting its Hawking radiation from a distance—can simultaneously recover information from infalling entangled qubits?*

Ideally, such a statement would be proven under assumptions that are consistent with the postulates of black hole complementarity [STU93, 't 85]. While most prior works on black-hole radiation decoding focus on the perspective of an outside observer [HP07, AMPS13, HH13, Bra23], a more recent work has also found it useful to take considerations from the black hole interior into account [AEH$^+$22].

As it turns out, however, such an information-theoretic analysis seems to lie way beyond the scope of existing techniques. (We refer the reader to Section 2.1 for a discussion of the fundamental limitations of existing techniques.) This is mainly due to the fact that black holes are to be modeled as information scramblers that feature Haar random (or pseudorandom [KP23, EFL$^+$24]) dynamics.

Secondly, we aim to revisit prior attempts for how to model the decoder's knowledge of the internal dynamics of the black hole. In the highly influential Hayden-Preskill thought experiment [HP07], the authors assume that the decoder (say, Bob) holds a quantum memory that is maximally entangled with the qubits in the interior of the black hole. In other words, Bob is an extremely powerful observer that has complete control over the black hole and its resulting radiation. As noted by Hayden and Preskill, we would ideally like a more realistic model that captures Bob's knowledge of the black hole dynamics without giving him direct control over the black hole, which begs the question:

*Question Two: Are there alternative—and perhaps more reasonable—models that capture the fact that the decoder has knowledge of the internal dynamics of the black hole?*

We believe that an affirmative answer to these questions could offer new and valuable insights into the black-hole information paradox.

**Our Approach.** To address *Question One*, we cast the black-hole information paradox into the form of a cloning game. At the beginning of the game, Alice throws her entangled qubits into the black hole. Later, at the end of the game, two spatially separated "adversaries" called Bob and Charlie will attempt to decode Alice's state—either as an *outside observer* with access to the emitted Hawking radiation (say, Bob), or as an *infalling observer* who has access to the black hole's internal qubits (say, Charlie). Moreover, in line with prior works [HP07, HH13, KP23, EFL$^+$24], we model the black hole's internal evolution in between as a "scrambling process" which is the result of some random unitary time-evolution $U$, followed by a quantum channel $\Phi$ that processes the internal qubits into two systems: one corresponding to the qubits within the event horizon of the black hole, and another corresponding to the emitted Hawking radiation. While $\Phi$ is typically assumed to be a unitary channel, we do not enforce any additional restrictions beyond the fact that it is a completely-positive and trace-preserving map. As in a conventional monogamy of entanglement game, it is crucial that Bob and Charlie do not communicate while the decoding phase is taking place, which also consistent with our modeling assumption that Charlie falls towards the singularity of the black hole, whereas Bob remains a distant outside observer.

To address *Question Two*, we grant the adversaries Bob and Charlie *oracle access* to the internal scrambling dynamics $U$, as well as its inverse $U^\dagger$. Additionally, we assume that Bob and Charlie have a complete description of the physical process $\Phi$ that results in the outgoing radiation. While Bob (and also Charlie) no longer has the ability to exercise direct control the black hole dynamics (as in the Hayden-Preskill model), he does have the power (via the oracle for $U^\dagger$) to essentially "unscramble" the black hole's time evolution at will. Here, the oracle access to the unitaries $U, U^\dagger$ is meant to reflect the possibility that Bob and Charlie are powerful observers who have obtained some knowledge on the physical equations and parameters governing the black hole's evolution (see Figure 3 for a circuit representation of Bob's and Charlie's strategy).

Our modeling assumptions behind our black hole cloning game appear entirely consistent with the postulates of black hole complementarity [STU93, 't 85]; in the sense that all components of our black hole cloning game are modeled according to the existing understanding of physics and Hawking radiation:

- we model the entire process of black hole evolution as a (possibly unitary) quantum channel which takes as input the set of qubits belonging to the interior—together with Alice's infalling qubits—and converts them into a global (possibly pure) state of which a subsystem constitutes outgoing radiation;

- we assume that Hawking radiation is a valid phenomenon—it enables Bob to intercept outgoing radiation in the form of qubits that he can process on his quantum computer. Meanwhile, Charlie is simply a free falling observer that encounters nothing unique or strange when passing the event horizon; and

- we assume that Bob and Charlie have knowledge of the internal dynamics of the black hole, say as the result of statistical mechanical and thermodynamic considerations—in analogy to how deciphering the contents of a burning book is possible, at least in principle, by observing its smoke and ashes.[4]

Therefore, we believe that black hole cloning games offer a reasonable characterization of quantum cloning in the context of evaporating black holes. In Section 1.5, we discuss further improvements to our modeling assumptions which could potentially make our game even more realistic from a physical perspective.

**Defining Black Hole Cloning Games.** With the above in mind, we now sketch our formulation of the black hole information paradox as a particular cloning game (see Section 4 for a formal definition).

We consider the following interactive game $\mathsf{G}_{\mathrm{BH}}$ (as illustrated in Figure 2) between a trusted party called Alice and two colluding and adversarial parties called Bob and Charlie.

[4] This analogy was also used in the work of Hayden and Preskill [HP07].

1. (**Setup phase**) A tripartite quantum state $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{I}} \otimes \mathcal{H}_{\mathsf{B}'} \otimes \mathcal{H}_{\mathsf{B}})$ is prepared, where
$$\rho = \Big( |0^{n-k}\rangle\langle 0^{n-k}|_{\mathsf{I}} \otimes |\mathsf{EPR}^k\rangle\langle \mathsf{EPR}^k|_{\mathsf{B}'\mathsf{B}} \Big).$$
Here, $k$ denotes the number of qubits in the registers $\mathsf{B}$ and $\mathsf{B}'$. Next, Alice receives register $\mathsf{B}$.

2. (**Time-evolution phase**) An $n$-qubit scrambling unitary $U \sim \nu$ is selected uniformly at random from an ensemble $\nu = \{U_\theta\}_{\theta\in\Theta}$, and the internal registers of the black hole evolve according to the unitary quantum channel $\big(U \cdot U^\dagger\big)_{\mathsf{IB}'\to\mathsf{IB}'}$ which is applied to registers $\mathsf{IB}'$ of the state $\rho$. Afterwards, a (not necessarily unitary) quantum channel $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$ is applied to $\mathsf{IB}'$ and produces registers $\mathsf{H}$ and $\mathsf{R}$ (This should be thought of as the black hole's final internal state and Hawking radiation, respectively).

3. (**Guessing phase**) Charlie and Bob receive the registers $\mathsf{H}$ and $\mathsf{R}$, respectively.[5] They also receive oracles for both $U$ and $U^\dagger$, but may no longer communicate. They independently perform the oracle-aided measurements $\{\mathbf{H}_x^{U,U^\dagger}\}_{x\in\{0,1\}^k}$ and $\{\mathbf{R}_x^{U,U^\dagger}\}_{x\in\{0,1\}^k}$ and each output a $k$-bit string.

4. (**Outcome phase**) Alice measures $\mathsf{B}$ is measured in the computational basis, resulting in $x \in \{0,1\}^k$. Charlie and Bob win if they both guessed $x$ correctly.

Here, we associate with $\mathsf{S}$ a particular strategy which is specified by Charlie's and Bob's measurements. The value of a particular strategy $\mathsf{S}$ for the game $\mathsf{G}_{\text{BH}}$ is defined as the average winning probability
$$\omega_{\mathsf{S}}(\mathsf{G}_{\text{BH}}) := \mathop{\mathbb{E}}_{U\sim\nu}\Bigg\{ \sum_{x\in\{0,1\}^k} \mathrm{Tr}\Bigg[ \Big(\mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \otimes |x\rangle\langle x|_{\mathsf{B}}\Big) \Big(\Phi_{\mathsf{IB}'\to\mathsf{HR}} \otimes \mathbb{I}_{\mathsf{B}}\Big) \\ \Big(\big(U \cdot U^\dagger\big)_{\mathsf{IB}'\to\mathsf{IB}'} \otimes \mathbb{I}_{\mathsf{B}}\Big) \Big( |0^{n-k}\rangle\langle 0^{n-k}|_{\mathsf{I}} \otimes |\mathsf{EPR}^k\rangle\langle \mathsf{EPR}^k|_{\mathsf{B}'\mathsf{B}} \Big)\Bigg]\Bigg\}.$$

Moreover, we denote by $\omega(\mathsf{G}_{\text{BH}})$ the maximal value of the game, i.e., the optimal winning probability over all possible strategies employed by Bob and Charlie. Let us remark that the tripartite state $\rho$ is not adversarially prepared by Bob and Charlie (unlike in typical monogamy games [TFKW13]); rather, it is generated by an external process (say, nature) over which the players have no control. While this is also true of the $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$ cloning channel in practice, our bounds will hold even if $\Phi$ is chosen *adversarially* by Bob and Charlie.

In Theorem 4.4, we prove the following result without any restrictions on the choice of channel $\Phi$ but where, for technical reasons (which we unpack in detail in Section 2.2), we let $\nu$ be a unitary 3-design and assume that Bob and Charlie employ single-query strategies only. We visualize what Bob and Charlie's strategies might look like in Figure 3, and we mention further potential improvements in Section 1.5.

**Theorem 1.1** (Informal, see Theorem 4.4 for formal statement)**.** *Let $n, k \in \mathbb{N}$ be integers with $n \geq k$ and let $\nu = \{U_\theta\}_{\theta\in\Theta}$ be an $n$-qubit unitary 3-design. Then, for any quantum channel $\Phi$ (of appropriate dimensions), the maximal single-query value of the black hole cloning game $\mathsf{G}_{BH}$ (as illustrated in Figure 2) with respect to $\nu$ and $\Phi$ is at most*
$$\sup_{\textit{strategies } \mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}_{BH}) \;=\; O(2^{-k})\,,$$
*where the supremum ranges over all oracle-aided strategies $\mathsf{S}$ employed by Bob and Charlie that only make a single oracle query (to either $U_\theta$ or $U_\theta^\dagger$), for any given $\theta$.*

[5] Here, we allow both Charlie and Bob to have any number of auxiliary registers. In our scenario, we imagine that Charlie jumps into the black hole with additional qubits of his choice, and that Bob has access to registers outside of the black hole. This is essentially without loss of generality—we can always absorb additional reference systems by re-defining the channel $\Phi$.

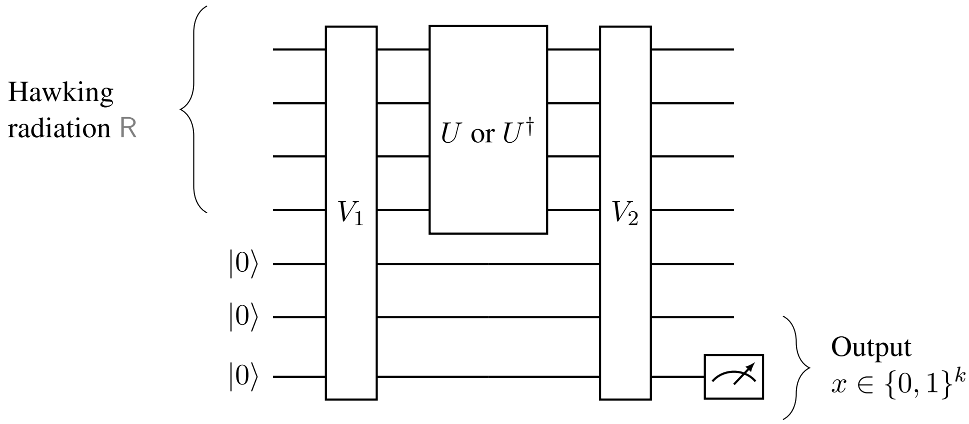


Figure 3: Visualization of Bob's quantum computation in our black hole cloning game. He takes the intercepted Hawking radiation in register $\mathsf{R}$ as input, adds any number of ancilla qubits (in the $|0\rangle$ state) of his choosing, and applies an initial unitary $V_1$ to the entire system. He then makes one oracle query to either $U$ or $U^\dagger$, where $U$ is the black hole's scrambling unitary. Finally, he applies an additional unitary $V_2$ then measures the last $k$ qubits to produce his guess $x \in \{0,1\}^k$. The diagram for Charlie's strategy would be similar, except the input would consist of the black hole's internal qubits in register $\mathsf{H}$.

**Implications to Black-Hole Physics.** Theorem 1.1 yields the first quantitative bound on the extent to which two observers, Bob and Charlie, can simultaneously recover information from $k$ infalling entangled qubits that emerge near the boundary of a black hole. In fact, our bound of $O(2^{-k})$ is also optimal (up to constant factors), since there always exists a particular Hawking radiation channel $\Phi$ together with a trivial strategy $\mathsf{S}$ that attains it: we can consider a variant of the black hole cloning game where $\Phi$ is the channel that converts the entirety of all the qubits inside of the black hole into radiation (i.e., acting as the identity), which would allow Bob to perfectly recover the information from Alice's system by simply applying the inverse of the scrambling unitary. Now Charlie can guess randomly and succeed with probability $2^{-k}$.

We believe that our bound has several interesting implications. First, it suggests that the moment Bob has produced a register which is nearly maximally correlated with Alice's infalling qubits, then any additional qubits that lie within the black hole's event horizon (i.e., in Charlie's system), must be almost completely uncorrelated from them. Second, such a strong decoupling result is achieved for *any* choice of Hawking radiation channel $\Phi$—it arises precisely because of the strong scrambling properties of the unitary 3-design itself. By contrast, the same would not be true for a *classical* model of black-hole scrambling [HP07], say in the form of a random reversible circuit or a random permutation[6]. Despite the fact that a random permutation is already exponentially complex (i.e., requires exponential-sized circuits with overwhelming probability), it is simply not *scrambling enough* to allow for a similar decoupling to hold. In summary, our results suggest that, in an idealized model of a black hole which features Haar random (or pseudorandom) scrambling dynamics, the information from infalling entangled qubits can only be recovered from either the interior or the exterior of the black hole, though never from both places at the same time.

[6]Interestingly, one could interpret the one-round variant of the *sponge construction* which underlies the international hash standard SHA-3 [BDPA11, CP24, CPZ24] as a classical model of black hole scrambling, where the scrambling unitary is given by a random permutation and the Hawking radiation channel is an erasure channel that selects a subset of the final output bits.

### 1.4 Application: Unclonable Cryptography in "MicroCrypt"

In this section, we describe our applications to quantum cryptography; specifically, for how to construct succinct unclonable encryption schemes from the existence of *pseudorandom unitaries*. This allows us to fully bridge the gap between the world of quantum pseudorandomness and unclonable cryptography.

**Unclonable Cryptography.** Cloning games have played a foundational role in the field of *unclonable cryptography*—a branch of quantum cryptography that capitalizes on quantum no-cloning [WZ82] to achieve guarantees of "unclonable security" which are completely impossible classically. These include uclonable encryption [BL20, AKL23, KT23, AKY24], encryption with unclonable decryption keys [GZ20], unclonable commitments and proofs [GMR23], quantum copy-protection [AKL$^+$22, CMP22], and unclonable quantum advice [BKL23]. Most of these constructions rely at minimum on the existence of post-quantum one-way functions, placing unclonable cryptography in "Post-Quantum MiniCrypt" [Imp95].[7]

**Quantum Cryptography in "MicroCrypt".** Meanwhile, another line of work [JLS18, BS19, MPSY24, MH24, BHHP24] has introduced and constructed notions of *pseudorandom quantum states and unitaries*. These are implied by the existence of post-quantum one-way functions; however, the reverse implication is not known. In fact, recent work [Kre21, AIK22, KQST23] has provided evidence that such an implication is unlikely to exist. This has led to the development of new and *inherently quantum* assumptions [BHHP24, PQS24]. As a result, the quantum cryptographic landscape includes yet another world, sometimes referred to as "MicroCrypt", which is potentially even weaker than that of MiniCrypt.

Moreover, pseudorandom states have proven to be powerful cryptographic tools in quantum cryptography, implying commitments [MY22] and oblivious transfer [BCKM21, GLSV21], and more. The fact that such powerful primitives live in MicroCrypt begs the following question:

*Does unclonable cryptography exist in MicroCrypt?*

In fact, the authors of [MPSY24] explicitly asked whether pseudorandom unitaries (which have eluded major cryptographic application so far) imply the existence of unclonable cryptographic primitives.

**Multi-Copy Unclonable Cryptography.** Previous works on unclonable cryptography have exclusively focused exclusively on the case of $1 \mapsto 2$ cloning games, e.g. in the case of unclonable encryption [BL20], the adversarial cloner is given only one copy of a ciphertext state and aims to provide two receivers, say Bob and Charlie, with sufficient information to later recover the plaintext message.

These cryptographic primitives could naturally be extended to $t \mapsto t+1$ security: in the case of unclonable encryption, the cloner receives $t$ identical copies of a ciphertext state and aims to provide $t+1$ receivers with enough information to later recover the plaintext message. This begs the following question:

*Can we construct $t \mapsto t+1$ unclonable cryptography from well-founded assumptions?*

This would resolve a question which was recenly left open in [AMP24], who asked whether the desirable property of multi-copy security is within reach in unclonable cryptography more generally.

[7] The work by [BL20] does imply an information-theoretic construction of unclonable encryption based on BB84 states; however, this lacks succinctness as the size of the encryption and decryption keys scales with the message length $n$ rather than just the security parameter $\lambda$.

**Our Results.** In this work, we make progress towards these foundational questions, and give an affirmative answer to both of them. Our main result of this section is the following:

**Theorem 1.2** (Informal, see Theorems 5.4 and 5.5 for formal statements)**.** *We show the following statements:*

1. *Assuming the existence of pseudorandom unitaries, there exists a deterministic unclonable encryption scheme with succinct keys which satisfies oracular $1 \mapsto 2$ search security (i.e., the adversaries are computationally bounded and only given oracle access to encryption and decryption functionality).*

2. *If the message space is $\mathcal{X} = \{0,1\}^n$ and we fix $t = o(\log n/\log\log n)$ then, assuming the existence of post-quantum pseudorandom functions, there exists a deterministic unclonable encryption scheme with succinct keys satisfies oracular $t \mapsto t+1$ search security,* ***provided*** *that the adversaries are computationally bounded and can only make* ***a single oracle query*** *to either the encryption or decryption functionality.*

**Remark 1.** *Although we only prove security for $t = o(\log n/\log\log n)$, we remark that our construction is plausibly secure for $t$ that is an arbitrary polynomial in $n$ (unlike previous constructions based on BB84 states [BL20] and coset states [CLLZ21]).*

Our proof of the first result uses a worst-case to average-case reduction for cloning games, which can be thought of as an additional cryptographic application of pseudorandom unitaries[8] which was previously not known. Our proof of the second result uses our machinery for analyzing cloning games based on binary phase states, which we unpack further in Section 2. We visualize the landscape of some unclonable cryptographic primitives relative to the worlds of MicroCrypt, Post-Quantum Minicrypt, and Post-Quantum Obfustopia in Figure 4.

### 1.5 Open Questions

Any improvement to our analysis of cloning games would immediately yield applications to either or both of the black hole and unclonable encryption settings. We list some of these questions here:

1. Can the security of the underlying $1 \mapsto 2$ oracular cloning game (i.e., as in Construction 3) be proven even if Bob and Charlie can adaptively make *any* polynomial number of queries to the encoding underlying unitary and its inverse?

   This would immediately imply the security of our black hole cloning game against *arbitrary* Bob and Charlie strategies, when instantiated with a pseudorandom unitary (PRU) rather than a unitary design. Due to their highly efficient (and yet strong) scrambling properties, pseudorandom unitaries are believed to be an excellent theoretical model of black hole dynamics [KP23, EFL+24].

2. More tantalizingly, can this security be shown if the PRU secret key $\theta$ is given to Bob and Charlie in the clear, rather than in the form of an oracle? This still plausibly satisfies unclonable security, but is highly counterintuitive; the PRU security guarantee does not say anything about what could happen in a game where the secret key $\theta$ is eventually leaked.

   In our black hole cloning game, this would allow us to prove much stronger quantitative statements, even in the scenario in which Bob and Charlie have *complete* knowledge of the internal scrambling dynamics of the black hole.

[8] To the best of our knowledge, the use of pseudorandom unitaries in the context of efficient worst-case to average-case reductions has not previously appeared.

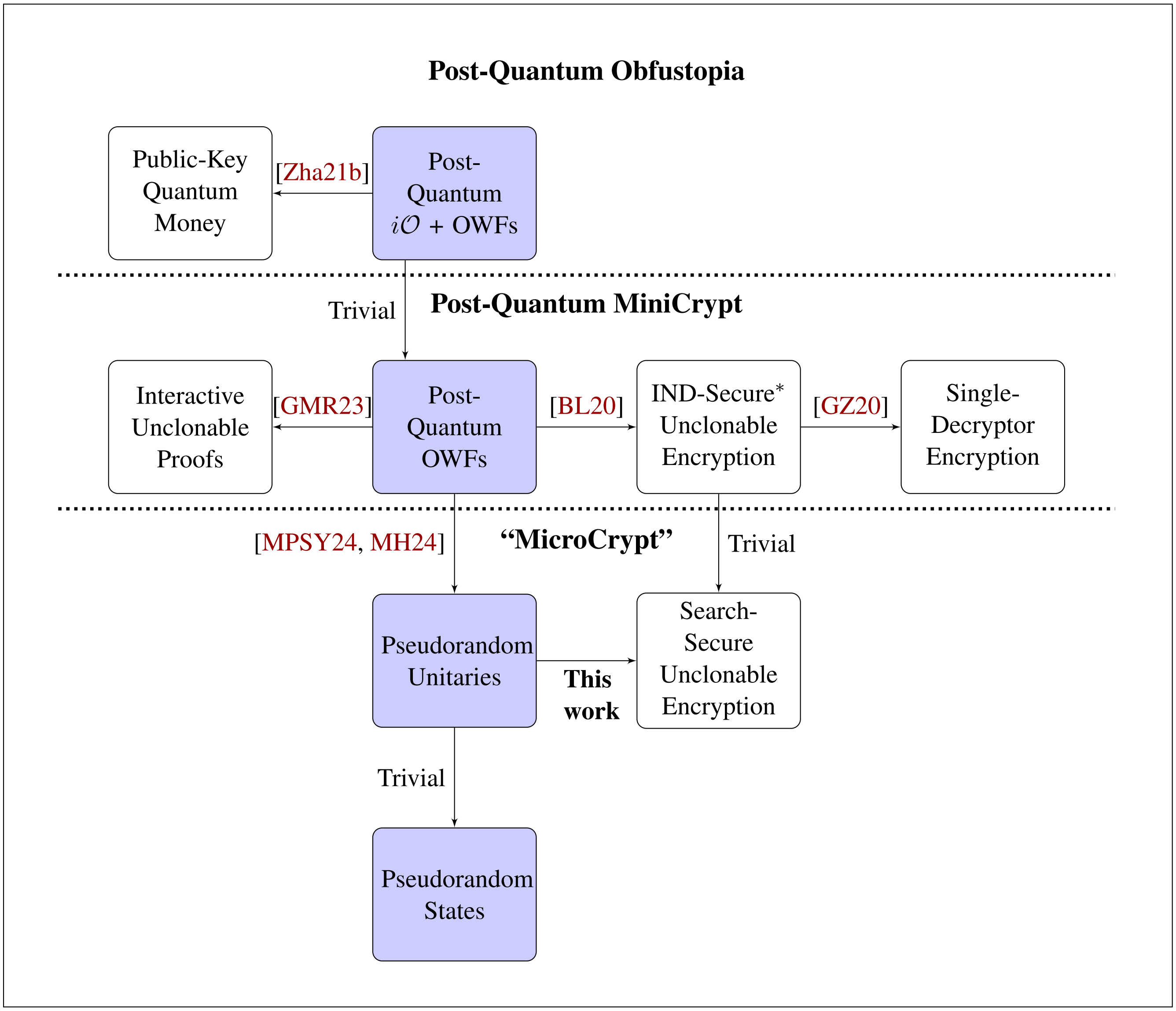


Figure 4: A visualization of some primitives in unclonable cryptography and the assumptions that are known to imply them (we focus here on primitives that are relatively well-understood and related to monogamy of entanglement games). We segment these assumptions into three worlds, loosely following [Imp95]: Obfustopia, MiniCrypt, and MicroCrypt. MicroCrypt is a world where we only assume the existence of pseudorandom states and unitaries, which could plausibly hold even if $\mathsf{P} = \mathsf{NP}$ [KQST23]. Powerful cryptographic primitives such as bit commitments [MY22] and oblivious transfer [BCKM21, GLSV21] have been shown to exist in MicroCrypt; however, prior to our work, it was not known how to instantiate any unclonable cryptography *with succinct keys* in MicroCrypt. Our work takes a first step in this direction by showing that pseudorandom unitaries imply search-secure succinct unclonable encryption in an oracle model.
(*We note for clarity that the existing results on indistinguishability-secure unclonable encryption all come with some kind of caveat e.g. existing in an oracle model and requiring that the adversaries are disentangled [BL20], or requiring quantum decryption keys [AKY24].)

3. Can we make our modeling assumptions in our definition of black hole cloning games in Section 4 more physically realistic? For example, can we model the (initial) internal qubits of the black hole as a more general quantum state (potentially even entangled with the exterior) rather than as the all-zero state $|0^{n-k}\rangle$? What if the scrambling dynamics do not just affect internal qubits, but also external qubits? And lastly, what if the scrambling dynamics is in the form of a Haar random isometry?

4. Can we use the language of interactive games to offer new quantitative insights into information scrambling in other chaotic quantum systems, besides black holes?

5. Can we achieve any of the above stronger security guarantees for $t \mapsto t+1$ cloning games? Or as a starting point: can we prove security against players $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$ that are free to make multiple *non-adaptive* queries to $U_\theta, U_\theta^\dagger$?

As far as applications to unclonable cryptography go, the following questions naturally arise:

1. What other unclonable cryptography primitives can be instantiated in MicroCrypt?

2. Can we obtain unclonable encryption with the stronger notion of indistinguishability security that we usually require of encryption schemes? (Our notion of unclonable security takes the form of "search security".) This is an important but difficult problem that recent works have made some progress on [BL20, KT23, AKL23, AKY24].

3. Which unclonable cryptography primitives have natural, constructible, and applicable $t \mapsto t+1$ analogues, besides unclonable encryption?

**Organization of the Paper.** In Section 2, we provide an overview of our techniques with pointers to the corresponding technical sections. We then present some preliminaries in Section 3. In Section 4, we formally define black hole cloning games and provide a proof using our technical results on cloning games in later sections to prove an upper bound on the value of the black hole cloning game. In Section 5, we define the notion of succinct unclonable encryption schemes and show that it exists in an oracle model, assuming the existence of pseudorandom unitaries. We also provide a first result towards establishing multi-copy security of the same scheme. In Section 6, we formally define monogamy of entanglement games and cloning games, and prove a worst-case to average-case reduction for cloning games. We then revisit existing techniques for analyzing monogamy games in Section 7, and establish that they will not suffice for our black hole application. Finally, in Sections 8 and 9, we introduce our novel notion of subtypes and apply this to prove the desired monogamy bound.

**Acknowledgements.** The authors would like to thank Aditya Nema, Aparna Gupte, Aram Harrow, Fermi Ma, Henry Yuen, Jiahui Liu, John Bostanci, Jonas Haferkamp, Jonathan Lu, Joseph Carolan, Lisa Yang, Makrand Sinha, Netta Engelhardt, Peter Shor, Prabhanjan Ananth, Ran Canetti, Saachi Mutreja, Soonwon Choi, Thomas Vidick, Tony Metger, William Kretschmer, and Yael Tauman Kalai for useful discussions. AP is supported by the National Science Foundation (NSF) under Grant No. CCF-1729369. SR and VV are supported by DARPA under Agreement No. HR00112020023, NSF CNS-2154149 and a Simons Investigator Award. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Government or DARPA.

## 2 Technical Overview

This technical overview is structured as follows:

1. In Section 2.1, we review the existing techniques for analyzing cloning games, explain their limitations, and then outline our techniques for circumventing these issues.

2. In Section 2.2, we explain the application of our results to black hole physics, in particular highlighting the necessity of obtaining an asymptotically optimal $O(2^{-n})$ cloning bound.

3. In Section 2.3, we discuss the application of our results to unclonable cryptography: first in terms of obtaining it from "MicroCrypt" (assumptions that are believed to be weaker than one-way functions), and secondly in terms of obtaining multi-copy secure unclonable encryption.

### 2.1 Sections 6-9: Analyzing Cloning Games

For simplicity, we will focus for most of this technical overview on $1 \mapsto 2$ cloning games, and we will consider the case where the players Bob and Charlie are each allowed only one query to either $U_\theta$ or $U_\theta^\dagger$. One can think of $U_\theta$ as being Haar random for now; we will specify the right pseudorandom object to instantiate this as we go along.

**Lemma 9.1 and Appendix A: Analyzing an Equivalent Special Monogamy Game.** As sketched in Section 1.1, we can analyze cloning games by equivalently recasting them as a special type of monogamy game. In a cloning game, Alice sends the cloner $\Phi$ the state $U_\theta |x\rangle$. Instead, we could imagine that Alice and $\Phi$ share several EPR pairs, and later on in the game (even after the cloning phase) Alice can apply a measurement $\left\{ \mathbf{A}_x^\theta := \bar{U}_\theta |x\rangle\langle x| \bar{U}_\theta^\dagger \right\}_{x \in \{0,1\}^n}$ on her side to induce the state $U_\theta |x\rangle$ on the cloner's side. This yields a monogamy of entanglement game with the following two restrictions:

- As already mentioned, Alice's measurements $\mathbf{A}_x^\theta$ must take the form $\bar{U}_\theta |x\rangle\langle x| \bar{U}_\theta^\dagger$.
- The tripartite state $\rho$ shared by Alice, Bob, and Charlie is the *Choi state* of the cloning channel $\Phi$. Concretely, we must have the special form

$$\rho_{\mathsf{ABC}} = (\mathbb{I}_{\mathsf{A}} \otimes \Phi_{\mathsf{A}' \to \mathsf{BC}})(|\mathsf{EPR}\rangle\langle\mathsf{EPR}|_{\mathsf{AA}'}). \tag{2}$$

This equivalence was first observed and used by [BL20] and follows from the ricochet property of EPR pairs, which we formally state in Section 3.1. The technical benefit of doing this is that it enables us to get a handle on the cloning channel $\Phi$ by absorbing it into the state shared by the players in the equivalent monogamy game. Now we can focus on Bob and Charlie's measurements, which can be handled using spectral bounds as first observed by [TFKW13]. As we will see, our work builds a different suite of techniques for spectral bounds that are useful for monogamy games.

**Section 6.3: Worst-Case to Average-Case Reduction for Cloning Games.** Our task has now been reduced to analyzing the value of a particular type of monogamy game where the unitary $U_\theta$ is sampled from the Haar measure on the unitary group $\mathrm{U}(d)$, for $d = 2^n$. Analyzing this game directly boils down to proving spectral bounds on the *mixed Haar twirl* of a certain operator $\Xi$; informally, expressions of the form:

$$\left\| \mathop{\mathbb{E}}_{U \sim \mathrm{U}(d)} \left[ \left( U \otimes U \otimes \bar{U} \right) \Xi \left( U \otimes U \otimes \bar{U} \right)^{\dagger} \right] \right\|_{\infty}.$$

Expressions of this form have been studied by [EW01, GO23, GBO23] using *mixed Schur-Weyl duality*, but their techniques appear to be very unwieldy in our setting. Instead, we take a two-step approach which is based on the following insight: cloning games instantiated with a Haar (pseudo)random unitary are, in some sense, *strictly harder for the adversaries to win* than any other cloning game.

This suggests the following approach:

1. Argue that for *any* distribution $\mathfrak{D}$ supported on $\mathrm{U}(d)$, we have:

$$\sup_{\text{strategies } \mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}; U \sim \mathrm{U}(d)) \leq \sup_{\text{strategies } \mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}; U \sim \mathfrak{D}). \tag{3}$$

2. Find a convenient distribution $\mathcal{D}$ such that we can more easily show that

$$\sup_{\text{strategies } \mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}; U \sim \mathfrak{D}) \leq O(2^{-n}),$$

perhaps by passing first to an equivalent monogamy game as stated earlier.

We prove the worst-case-to-average-case reduction captured in Item 1 in Section 6.3. The high-level idea is to use Haar invariance; we can convert samples $U \sim \mathfrak{D}$ to samples $W \sim \mathrm{U}(d)$ by simply sampling $V \sim \mathrm{U}(d)$ and defining $W := VU$. So given several copies of a state $U |\psi\rangle$ with $U$ sampled from $\mathfrak{D}$, we can simply sample $V$ to be Haar random and apply $V$ to $U |\psi\rangle$.

Instantiating this requires being able to sample $V$ that appears Haar random, together with a classical description of it. There are two regimes of interest to us:

- In the query-bounded setting (as is the case for our black hole cloning game), this can be achieved using *mixed unitary designs*, which we formally define in Section 3.2. We also show that the more standard notion of a unitary $t$-design (studied and constructed in [Haf22, MPSY24, SHH24]) will also work as a mixed unitary design without modification.
- In the unbounded-query setting, where the adversaries can adaptively make any polynomial number of queries, this can be achieved using *pseudorandom unitaries*, which were constructed by [MPSY24, MH24]. We formally define these in Section 3.3. In this case, we will obtain Equation (3) but incur an additive $\mathsf{negl}(\lambda)$ security loss on the RHS.

It now remains to address Item 2, which we do by analyzing the corresponding monogamy games. The key challenge is to find *any* monogamy game with $\mathcal{X} = \{0,1\}^n$ and value $O(2^{-n})$, subject to the restrictions stated at the beginning of Section 2.1, and we additionally restrict Bob and Charlie to make a single oracle query to $U_\theta$ or $U_\theta^\dagger$ (for technical reasons). We first revisit existing techniques and explain why they are insufficient for this goal, then introduce our new techniques for achieving this.

**Starting Point: [TFKW13].** In order to analyze the BB84 monogamy game, the work by [TFKW13] uses two beautiful ideas:

1. The value of a particular monogamy game can be bounded *independently* of the state $\rho_{\mathsf{ABC}}$ shared by the 3 players, noting that $\rho_{\mathsf{ABC}}$ is PSD and has trace 1.

$$\begin{aligned}\omega(\mathsf{G}) &= \mathop{\mathbb{E}}_{\theta\sim\Theta}\sum_{x\in\mathcal{X}} \operatorname{Tr}\left[(\mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta)\rho_{\mathsf{ABC}}\right] \\ &= \operatorname{Tr}\left[\left(\mathop{\mathbb{E}}_{\theta\sim\Theta}\sum_{x\in\mathcal{X}} \mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta\right)\rho_{\mathsf{ABC}}\right] \\ &\le \left\|\mathop{\mathbb{E}}_{\theta\sim\Theta}\sum_{x\in\mathcal{X}} \mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta\right\|_\infty .\end{aligned}$$

This reduces the task of bounding the value of a monogamy game to bounding an operator norm.

2. This operator norm can in turn be bounded just in terms of *pairwise overlaps* between the $\mathbf{A}_x^\theta$'s, which the designer of the game is free to choose. As we state in Theorem 7.1, the authors of [TFKW13] show that

$$\left\|\mathop{\mathbb{E}}_{\theta\sim\Theta}\sum_{x\in\mathcal{X}} \mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta\right\|_\infty \le \frac{1}{|\Theta|} + \frac{|\Theta|-1}{|\Theta|}\cdot \max_{\substack{\theta,\theta'\in\Theta\\ \theta\neq\theta'}} \max_{x,x'\in\mathcal{X}} \left\|\mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'}\right\|_\infty .$$

We refer the reader to Theorem 7.1 for a formal statement.

In the BB84 monogamy game where $\Theta = \mathcal{X} = \{0,1\}$ and $\mathbf{A}_x^\theta = \mathsf{H}^\theta |x\rangle\langle x| \mathsf{H}^\theta$, it is straightforward to see that $\left\|\mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'}\right\|_\infty = \frac{1}{\sqrt{2}}$, and hence $\omega(\mathsf{G}_{\text{BB84}}) \le \frac{1}{2} + \frac{1}{2\sqrt{2}}$. The work by [TFKW13] also extends this to "parallel-repeated" BB84 games with $|\Theta| = |\mathcal{X}| = \{0,1\}^n$ (see Theorem 6.4) for a formal definition, and show that

$$\omega(\mathsf{G}_{\text{BB84}}^{\otimes n}) \le \cos^2\left(\frac{\pi}{8}\right)^n \approx 2^{-0.228n}.$$

Hence we have an $n$-bit monogamy game with value $\le 2^{-0.228n}$. In fact, this is tight; [TFKW13] exhibits a simple strategy achieving this bound. However, for our black hole application, we require a tight bound (up to constant factors) of $O(2^{-n})$. We explain how we do this in the forthcoming paragraphs.

**Section 7: Better Bounds from Binary Phase States.** The security of the BB84 monogamy game is fundamentally limited, both in terms of the value of the $1 \mapsto 2$ monogamy game (which we just saw), and its multi-copy security (which we will discuss in Section 2.3). To improve on this, we instead consider *binary phase states*. For any function $f : \{0,1\}^n \to \{0,1\}$ from some function family $\mathfrak{F}$, we define

$$\mathsf{U}_f = \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle\langle x| ,$$

and consider the monogamy game defined by $\mathcal{X} = \{0,1\}^n$, $\Theta = \mathfrak{F}$, and

$$\mathbf{A}_x^f = \mathsf{U}_f \mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n} \mathsf{U}_f .$$

In other words, $\mathbf{A}_x^f$ is a projector onto the state

$$|\psi_x^f\rangle := \mathsf{U}_f \mathsf{H}^{\otimes n} |x\rangle = 2^{-n/2} \sum_{y\in\{0,1\}^n} (-1)^{f(y)+\langle x,y\rangle} |y\rangle ,$$

and our proposed distribution $\mathfrak{D}$ over unitaries is obtained by first sampling $f$ from some function family $\mathfrak{F}$ and outputting $\mathsf{U}_f \mathsf{H}^{\otimes n}$.

The state $|\psi_0^f\rangle$, where $\mathfrak{F}$ is a post-quantum pseudorandom function (PRF) family [Zha21a], has previously been considered by [JLS18, BS19] as a construction of a *pseudorandom state*, owing to its multi-copy security. We include additional information about the answer $x$ in the phase as a means of "encrypting" $x$ within this state. Intuitively, these states enjoy better security than BB84 states due to the fact that for any $f$, the basis $\left\{|\psi_x^f\rangle : x \in \{0,1\}^n\right\}$ is highly entangled across the $n$ qubits. In the BB84 case, the measurement basis is entirely disentangled across the $n$ qubits, and this hurts security. In fact, [AK21] describes a generic attack on cloning games where the measurement basis is entirely disentangled across qubits.

As a first step, in Section 7.2 we analyze this binary phase monogamy game instantiated with $\mathfrak{F}$ being a PRF family, using the aforementioned techniques by [TFKW13]. We show a bound on this monogamy game of essentially $\widetilde{O}(2^{-n/2})$, which is better than the BB84 case but still not the desired $O(2^{-n})$. This is in fact an inherent limitation of the [TFKW13] technique; as we show in Section 7.3, we cannot hope to prove a better upper bound than this for *any* monogamy game of the desired form using their techniques.

**Sections 8 and 9.1-9.3: Binary Types and Extending Them to Subtypes.** In order to attain the desired bound of $O(2^{-n})$, we will hence need to turn to new techniques. As a first attempt, let us try to retain Item 1 of the [TFKW13] technique and find alternative ways to bound the operator norm of interest. In order to get a better handle on the projectors $\mathbf{B}_x^f$ and $\mathbf{C}_x^f$, we will now *restrict* Bob and Charlie by giving them *one oracle query* to $\mathsf{U}_f$ (which is its own inverse), rather than actually revealing $f$. With these constraints, we can model Bob and Charlie's projectors as follows:

$$\mathbf{B}_x^f = \mathsf{U}_f \mathbf{P}^\dagger |x\rangle\langle x| \mathbf{P} \mathsf{U}_f;$$
$$\mathbf{C}_x^f = \mathsf{U}_f \mathbf{Q}^\dagger |x\rangle\langle x| \mathbf{Q} \mathsf{U}_f,$$

for unitaries $\mathbf{P}, \mathbf{Q}$. (In reality, we later also allow Bob and Charlie additional ancillary workspace qubits; we define this generalization in Definition 6.8. Moreover, we assume without loss of generality that Bob and Charlie do not perform any preprocessing before making their query to $\mathsf{U}_f$, by absorbing this preprocessing into the cloning channel $\Phi$ that constructs their initial states.) Although this is quite restrictive, notice that a single query to $\mathsf{U}_f$ is actually sufficient if we only wanted one player (Bob, say) to recover $x$ from $|\psi_x^f\rangle = \mathsf{U}_f \mathsf{H}^{\otimes n} |x\rangle$. The operator we now need to bound the $\ell_\infty$ norm of has the following form:

$$\begin{aligned}
&\mathop{\mathbb{E}}_{f \sim \mathfrak{F}}\left[\sum_{x \in \{0,1\}^n} \mathbf{A}_x^f \otimes \mathbf{B}_x^f \otimes \mathbf{C}_x^f\right] \\
&= \mathop{\mathbb{E}}_{f \sim \mathfrak{F}}\left[\mathsf{U}_f^{\otimes 3} \underbrace{\left(\sum_{x \in \{0,1\}^n} \left(\mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n}\right) \otimes \left(\mathbf{P}^\dagger |x\rangle\langle x| \mathbf{P}\right) \otimes \left(\mathbf{Q}^\dagger |x\rangle\langle x| \mathbf{Q}\right)\right)}_{=:\Xi} \mathsf{U}_f^{\otimes 3}\right].
\end{aligned}$$

Let us assume from now that $\mathfrak{F}$ is the family of *all* functions from $\{0,1\}^n \to \{0,1\}$ (we can make this switch provided $\mathfrak{F}$ is 6-wise uniform). In this case, this expression is known as a *binary phase twirl* applied to the operator $\Xi$, and this object is well-understood [JLS18, BS19, AGQY22] in terms of *binary types*, which were recently used by [AGQY22]. We present these definitions in Section 8.3. In the simple case above, a binary type $\boldsymbol{\lambda}$ is specified by a subset $T_{\boldsymbol{\lambda}} \subseteq \{0,1\}^n$ with $|T_{\boldsymbol{\lambda}}| \in \{1,3\}$. We say that a vector

$\mathbf{x} \in [2^n]^3$ *matches* $\boldsymbol{\lambda}$ if every string in $T_{\boldsymbol{\lambda}}$ appears an odd number of times in $\mathbf{x}$, while every string outside $T_{\boldsymbol{\lambda}}$ appears an even number of times in $\mathbf{x}$. Then, it can be shown that:

$$\mathop{\mathbb{E}}_{f \sim \mathfrak{F}} \left[ \mathsf{U}_f^{\otimes 3} \Xi \mathsf{U}_f^{\otimes 3} \right] = \sum_{\boldsymbol{\lambda}} \Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}} \,, \qquad \text{where} \qquad \Pi_{\boldsymbol{\lambda}} := \sum_{\mathbf{x} \in [2^n]^3 \text{ matches } \boldsymbol{\lambda}} |\mathbf{x}\rangle\langle\mathbf{x}|$$

is the projector onto vectors matching $\boldsymbol{\lambda}$. The projectors $\{\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}}\}$ are mutually orthogonal, so it suffices to bound $\|\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}}\|_\infty$ for each type $\boldsymbol{\lambda}$.

To the best of our knowledge, it appears difficult to directly bound these operator norms. Informally, the reason is that the combinatorial structure arising from a type $\boldsymbol{\lambda}$ entangles registers together; if we consider the type defined by $T_{\boldsymbol{\lambda}} = \{x^*\}$ for some string $x^*$, then strings of the form $(x^*, y, y)$, $(y, x^*, y)$, or $(x^*, y, y)$ would all match $\boldsymbol{\lambda}$. It would be much cleaner if we could just analyze strings from one of these categories at a time.

This is exactly what we do, and we formalize this using a novel notion of *subtypes* (defined formally in Section 8.2). Informally, a subtype would capture all strings matching just one of the above categories e.g. $\{(y, x^*, y)\}_{y \in \{0,1\}^n}$. We denote subtypes by $\boldsymbol{\mu}$ and their corresponding subtype projectors by $\Pi_{\boldsymbol{\mu}}$. In Section 8.2.2, we show that to bound $\|\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}}\|_\infty$ for a type $\boldsymbol{\lambda}$, it suffices to bound $\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\|_\infty$ for a *subtype* $\boldsymbol{\mu}$. This added structure allows us to prove better spectral bounds, which we present in Section 9.3.

It turns out that this technique allows us to prove the desired bound of $O(2^{-n})$ for $1 \mapsto 2$ cloning games, albeit with the restriction that Bob and Charlie can only make one query each to $\mathsf{U}_f$. At a very high level, the "product structure" of subtypes enables us to leverage a simple but novel spectral bound on the column-wise tensor product of several matrices, which we present in Lemma 3.22.

**Sections 9.4 and 9.5: Towards Multi-Copy Security.** One could also define a "$t \mapsto t+1$" cloning game, where the cloner receives the $t$-copy state $(U_\theta |x\rangle)^{\otimes t}$, and there are now $t+1$ players $\mathcal{P}_1, \ldots, \mathcal{P}_{t+1}$ with respective registers $\mathsf{P}_1, \ldots, \mathsf{P}_{t+1}$ who need to all simultaneously guess $x$, given a single query to an oracle for $U_\theta, U_\theta^\dagger$. (In other words, the setting we have considered so far is when $t = 1$.) In this setting, the operator we want to bound is

$$2^{n(t-1)} \sum_{x \in \{0,1\}^n} \left[ (\mathbf{A}_x)^{\otimes t} \otimes \bigotimes_{i=1}^{t+1} \mathbf{P}_{i,x} \right].$$

(We include the $2^{n(t-1)}$ factor to compensate for the fact that these measurements are incomplete; we are post-selecting on Alice's $t$ measurements all yielding the same outcome; see Lemma 9.1 for a formal derivation.) In this setting, we note that previous candidate constructions used for cloning games based on BB84 or coset states [BL20, AKL+22] are *provably insecure* if $t$ is allowed to be an arbitrary polynomial:

- BB84 states can be broken even when $t = 2$; the adversary can measure one copy in the standard basis and the other copy in the Hadamard basis, and send the results of all measurements to the three receivers $P_1, P_2, P_3$.

  Once the BB84 bases $\theta \in \{0,1\}^n$ have been revealed, the receivers can all reconstruct the message $x$.

- Coset states of dimension $d \leq n$ can be broken with $t = O(d)$ copies; the adversary can simply measure all the copies in the standard basis to recover a classical description of the subspace, then send this to the three players.

In contrast, binary phase states are secure for an arbitrary number of polynomial copies, so one might plausibly hope for unclonable $t \mapsto t+1$ security for any (polynomially bounded) $t$. In other words, we would ideally like to show the following (see Section 9.1 for a derivation):

$$\|\Pi_{\boldsymbol{\lambda}}\Xi\Pi_{\boldsymbol{\lambda}}\|_\infty = 2^{n(t-1)} \cdot \left\|\Pi_{\boldsymbol{\lambda}} \left[\sum_{x\in\{0,1\}^n} \left(\mathsf{H}^{\otimes n}\,|x\rangle\langle x|\,\mathsf{H}^{\otimes n}\right)^{\otimes t} \otimes \bigotimes_{i=1}^{t+1} \left(\mathbf{P}_i^\dagger\,|x\rangle\langle x|\,\mathbf{P}_i\right)\right] \Pi_{\boldsymbol{\lambda}}\right\|_\infty \le O_t(2^{-n}).$$

Surprisingly, this is *false* even for $t=2$; we provide a counterexample showing this in Section 9.5. We finally outline how we manage to circumvent this problem in a restricted setting, as an additional contribution and stepping stone towards the goal of $t \mapsto t+1$ unclonable cryptography. The restriction we impose on the $t+1$ players is analogous to the restriction we imposed on Bob and Charlie in the black hole setting: each player can be an arbitrary quantum algorithm that makes a single query to the phase oracle $\mathsf{U}_f$.

We note that our construction is plausibly secure when $t$ is an arbitrary polynomial in the security parameter and the players are completely unrestricted; however, we are currently only able to prove security in this restricted setting.

**Specializing to Cloning Games.** The issue is the loss incurred by using Item 1 of the [TFKW13] technique to dispose of the shared state $\rho_{\mathsf{A},\mathsf{P}_{1\to t+1}}$. This step is tight if $\rho_{\mathsf{A},\mathsf{P}_{1\to t+1}}$ can be an arbitrary mixed state as in a monogamy game. **However, in the special case of cloning games, $\rho_{\mathsf{A},\mathsf{P}_{1\to t+1}}$ is not arbitrary!** In our case, the shared state will be the result of applying some channel to the right half of $tn$ EPR pairs. This can be seen from Equation (2) (appropriately generalized to the multi-copy setting). In other words, if we apply a partial trace to remove the $\mathsf{P}_{1\to t+1}$ registers, the residual state on $\mathsf{A}$ should be proportional to $\mathbb{I}_{2^n\times 2^n}$.

This structure may seem mild, but it turns out to be enough to complete our analysis; we present this in Section 9.4. At a high level, we show that for any subtype $\boldsymbol{\mu}$ such that $\Xi$ places high weight on the image of $\Pi_{\boldsymbol{\mu}}$, the shared state $\rho_{\mathsf{A},\mathsf{P}_{1\to t+1}}$ must place *low* weight on the image of $\Pi_{\boldsymbol{\mu}}$. These effects roughly cancel each other out, and thus we are able to prove a bound of $O_t(2^{-n})$, provided that the $t+1$ players only make a single query to either $U_\theta$ or $U_\theta^\dagger$.

**Section 3.4: Spectral Bounds on Blockwise Tensor Products.** In the special case that the $t+1$ players do not have any ancilla qubits and can only apply unitaries, the subtype formalism together with Lemma 3.22 and a simple technical observation suffice to prove the desired bound. This simple technical observation is that if we have three matrices $\mathbf{A},\mathbf{B},\mathbf{C} \in \mathbb{C}^{d\times d}$ such that $\mathbf{A},\mathbf{B}$ are unitary and all entries of $\mathbf{C}$ have magnitude $\le 1$, then the entrywise product of $\mathbf{A},\mathbf{B},\mathbf{C}$ has operator norm $\le 1$. This can be shown by using well-known bounds relating the operator norm of a matrix to the $\ell_1$ norms of its rows and columns (see Lemmas 3.15 and 3.16).

However, this is unreasonably restrictive. In order to accommodate the possibility of the $t+1$ players using ancilla qubits, we require a stronger version of this observation that allows $\mathbf{A},\mathbf{B}$ to be $d\times d$ *block matrices* (i.e. they each comprise $d^2$ blocks). For example, when $d=2$ we would need to show that

$$\left\|\begin{bmatrix} c_{1,1}\mathbf{A}_{1,1}\otimes\mathbf{B}_{1,1} & c_{1,2}\mathbf{A}_{1,2}\otimes\mathbf{B}_{1,2} \\ c_{2,1}\mathbf{A}_{2,1}\otimes\mathbf{B}_{2,1} & c_{2,2}\mathbf{A}_{2,2}\otimes\mathbf{B}_{2,2}\end{bmatrix}\right\|_\infty \le 1,$$

provided that $\begin{bmatrix}\mathbf{A}_{1,1} & \mathbf{A}_{1,2}\\ \mathbf{A}_{2,1} & \mathbf{A}_{2,2}\end{bmatrix}, \begin{bmatrix}\mathbf{B}_{1,1} & \mathbf{B}_{1,2}\\ \mathbf{B}_{2,1} & \mathbf{B}_{2,2}\end{bmatrix}$ are unitary and $|c_{i,j}| \le 1$ for all $i,j$. Proving this turns out to be much more technically challenging, although elementary; we present this result and its proof in Theorem 3.19. Given that this theorem is a purely linear algebraic statement unrelated to monogamy games, we are hopeful that it might be useful elsewhere in quantum information and even in other areas.

Our techniques to obtain better bounds than [TFKW13] for $t \mapsto t+1$ cloning games (including when $t=1$) thus require a complete overhaul of their framework, albeit at the expense of restricting the $t+1$ players to make a single query to a decryption oracle, and restricting attention to cloning games rather than arbitrary monogamy games. We note however that the vast majority of monogamy games encountered in physics and cryptography are of a form that can be equivalently formulated as cloning games.

### 2.2 Section 4: Application to Black-Hole Physics

As one application of our techniques, we study the notion of a *black hole cloning game*—a three-player non-local game which is designed to capture the unclonability of quantum information in the context of evaporating black holes. We show an asymptotically tight upper bound on the success probability of a particular variant of the game.

While our notion of a black hole cloning game is syntactically different from the cloning and monogamy games studied by [TFKW13, BL20], we believe it nevertheless captures unclonability in a similar spirit. Given the similarity between our black hole cloning game and the games studied in [TFKW13, BL20], this begs the question of whether one can indeed interpret one as an instance of the other. We show that the analysis of black hole cloning games is inextricably linked to the existence of standard monogamy games which have asymptotically optimal bounds of the form $O(2^{-n})$—well beyond the pre-existing upper bound of $2^{-0.228n}$ in Equation (1).

The bulk of our work in Section 4 is to show that the maximal value $\omega(\mathsf{G}_{\text{BH}})$ can always be related to the maximal value of a related (but standard) cloning game $\mathsf{G}_{\text{clone}}$. Specifically, we show that the game $\mathsf{G}_{\text{BH}}$ emerges as a special case of $\mathsf{G}_{\text{clone}}$ in which we post-select on the event that Alice's sampled message $y$ takes the form $y = x||0^{n-k}$, for some $x \in \{0,1\}^k$. Because this event occurs with probability $2^{-n+k}$, this allows us to deduce that

$$\sup_{\text{strategies } \mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}_{\text{clone}}) \geq 2^{-n+k} \cdot \omega(\mathsf{G}_{\text{BH}}).$$

Therefore, in order to obtain an asymptotically optimal bound of the form $\omega(\mathsf{G}_{\text{BH}}) = O(2^{-k})$, it suffices to show that the related monogamy game $\mathsf{G}_{\text{clone}}$ has a maximal value of $\sup_{\text{strategies } \mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}_{\text{clone}}) = O(2^{-n})$. **Crucially, we require an $O(2^{-n})$ bound; a bound of the form $O(2^{-cn})$ for any $c < 1$ is insufficient.** This would yield $\omega(\mathsf{G}_{\text{BH}}) \leq 2^{-k} \cdot 2^{n(1-c)}$, which is a completely trivial bound if we assume $n \gg k$ (which is likely since presumably the black hole is a much larger system than the set of qubits Alice throws inside).

Thus in order to analyze $\mathsf{G}_{\text{BH}}$, we need to prove a $O(2^{-n})$ bound on the corresponding $1 \mapsto 2$ cloning game. As explained in Section 2.1, our work is the first to do this (albeit in a restricted query setting). This completes our overview of our analysis of the black hole cloning game, and the proof of Theorem 4.4.

### 2.3 Section 5: Application to Unclonable Cryptography

As another application of our techniques for analyzing cloning games, we study the notion of *succinct unclonable encryption*, and show that it is implied by the existence of pseudorandom unitaries, thus providing the first connection between the worlds of quantum pseudorandomness and unclonable cryptography.

**Unclonable Encryption from Pseudorandom Unitaries.** Our first contribution towards connecting unclonable cryptography and quantum pseudorandomness is encapsulated in Theorem 5.4, where we show that the existence of pseudorandom unitaries is sufficient to instantiate search-secure succinct unclonable encryption in an oracle setting. To do this, we use the same worst-case to average-case reduction that we outlined in Section 2.1 and will flesh out in Section 6.3. For the distribution $\mathfrak{D}$, we simply use the BB84 cloning game and the analysis by [TFKW13, BL20] i.e. we sample $\theta \leftarrow \{0,1\}^n$ and output the unitary $\mathsf{H}^\theta$. While this gives us a security bound of $2^{-0.228n} + \mathsf{negl}(\lambda)$ rather than the ideal $O(2^{-n}) + \mathsf{negl}(\lambda)$, this is not a crucial difference for this application (unlike in the black hole setting); moreover, the analysis of the BB84 cloning game has the advantage that it does not need to restrict Bob's and Charlie's strategies.

**Towards Multi-Copy Unclonable Encryption.** We also consider the natural extension of unclonable encryption to the multi-copy setting: the cloner now receives $t$ copies of the ciphertext state $(U_\theta |x\rangle)^{\otimes t}$, and must then forward some information to $t+1$ players who will later be given oracle access to encryption and decryption functionality. To the best of our knowledge, our work is the first to consider this notion of multi-copy security, and we are optimistic that this notion might be naturally applicable to other primitives in unclonable cryptography.

Using our analysis of $t \mapsto t+1$ cloning games presented in Section 2.1, we are able to construct search-secure succinct $t \mapsto t+1$ unclonable encryption in the restricted setting where $t = o(\log n / \log\log n)$ and the adversaries may only make one query to encryption/decryption oracles (but are otherwise computationally unbounded). We provide a formal statement in Theorem 5.5.

We emphasize that our construction is the first that could even be plausibly secure in the setting where $t$ can be an a priori unbounded polynomial in $\lambda, n$ and the $t+1$ players are given the secret key $\theta$ in the clear. While our results are far from this ideal goal, we view our techniques as providing a stepping stone towards an ideal security result for unclonable encryption. We are also optimistic that our results and techniques might be adaptable to other problems in unclonable cryptography.

# 3 Preliminaries

## 3.1 Quantum Computation

For a comprehensive background, we refer to [NC16]. We denote a finite-dimensional complex Hilbert space by $\mathcal{H}$, and we use subscripts to distinguish between different systems (or registers). For example, we let $\mathcal{H}_\mathsf{A}$ be the Hilbert space corresponding to a system $\mathsf{A}$. The tensor product of two Hilbert spaces $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$ is another Hilbert space denoted by $\mathcal{H}_\mathsf{AB} = \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$. The Euclidean norm of a vector $|\psi\rangle \in \mathcal{H}$ over the finite-dimensional complex Hilbert space $\mathcal{H}$ is denoted as $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$. Let $\mathrm{L}(\mathcal{H})$ denote the set of linear operators over $\mathcal{H}$. A quantum system over the 2-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^2$ is called a *qubit*. For $n \in \mathbb{N}$, we refer to quantum registers over the Hilbert space $\mathcal{H} = \left(\mathbb{C}^2\right)^{\otimes n}$ as $n$-qubit states. We use the word *quantum state* to refer to both pure states (unit vectors $|\psi\rangle \in \mathcal{H}$) and density matrices $\rho \in \mathcal{D}(\mathcal{H})$, where we use the notation $\mathcal{D}(\mathcal{H})$ to refer to the space of positive semidefinite matrices of unit trace acting on $\mathcal{H}$. The *trace distance* of two density matrices $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ is given by

$$\mathsf{TD}(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1.$$

A quantum channel $\Phi : \mathrm{L}(\mathcal{H}_\mathsf{A}) \to \mathrm{L}(\mathcal{H}_\mathsf{B})$ is a linear map between linear operators over the Hilbert spaces $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$. Oftentimes, we use the compact notation $\Phi_{\mathsf{A}\to\mathsf{B}}$ to denote a quantum channel between $\mathrm{L}(\mathcal{H}_\mathsf{A})$ and $\mathrm{L}(\mathcal{H}_\mathsf{B})$. We say that a channel $\Phi$ is *completely positive* if, for a reference system $\mathsf{R}$ of arbitrary size, the induced map $\mathbb{I}_\mathsf{R} \otimes \Phi$ is positive, and we call it *trace-preserving* if $\mathrm{Tr}[\Phi(X)] = \mathrm{Tr}[X]$, for all $X \in \mathrm{L}(\mathcal{H})$. A quantum channel that is both completely positive and trace-preserving is called a quantum $\mathsf{CPTP}$ channel. A *unitary* $U : \mathrm{L}(\mathcal{H}_\mathsf{A}) \to \mathrm{L}(\mathcal{H}_\mathsf{A})$ is a special case of a quantum channel that satisfies $U^\dagger U = UU^\dagger = \mathbb{I}_\mathsf{A}$. When $U$ acts on a density matrix $\rho$, it maps $\rho \mapsto U\rho U^\dagger$, and we will denote this channel by $U \cdot U^\dagger$.

Whenever $d = 2^n$, we refer to the group of unitaries acting on $n$ qubits as $\mathrm{U}(d)$. An isometry is a linear map $V : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ with $\dim(\mathcal{H}_{\mathsf{B}}) \geq \dim(\mathcal{H}_{\mathsf{A}})$ and $V^\dagger V = \mathbb{I}_{\mathsf{A}}$. A *projector* $\Pi$ is a Hermitian operator such that $\Pi^2 = \Pi$, and a *projective measurement* is a collection of projectors $\{\Pi_i\}_i$ such that $\sum_i \Pi_i = \mathbb{I}$. A positive-operator valued measure ($\mathsf{POVM}$) is a set of Hermitian positive semidefinite operators $\{M_i\}$ acting on a Hilbert space $\mathcal{H}$ such that $\sum_i M_i = \mathbb{I}$.

Given a bipartite state $\rho_{\mathsf{AB}}$, the *partial trace* $\mathrm{Tr}_{\mathsf{B}}$ captures the residual state of the system on just the $\mathsf{A}$ register. $\mathrm{Tr}_{\mathsf{B}}$ is thus defined as a linear map from $\mathrm{L}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{A}})$ that maps $R \otimes S \mapsto \mathrm{Tr}\,[S] \cdot R$. Given a multipartite operator $X \in \mathrm{L}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$, the *partial transpose* applies a transpose to only some of these systems. For example, the partial transpose $X \mapsto X^{\top_{\mathsf{B}}}$ with respect to the second system is defined as a linear map satisfying $X_1 \otimes X_2 \otimes X_3 \mapsto X_1 \otimes X_2^\top \otimes X_3$. We can also define a $\mathsf{SWAP}$ operator that acts on say registers $\mathsf{A}$ and $\mathsf{C}$; this is a linear map that will map $X_1 \otimes X_2 \otimes X_3 \mapsto X_3 \otimes X_2 \otimes X_1$.

**Operators.** Define the following unitary operators:

- Phase oracle: For $f : \{0,1\}^n \to \{0,1\}$ we let
$$\mathsf{U}_f = \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle\langle x| \,.$$
- Multi-bit Pauli operator: For $m \in \{0,1\}^n$, let
$$\mathsf{Z}^m = \sum_{x \in \{0,1\}^n} (-1)^{\langle x, m\rangle} |x\rangle\langle x| \,.$$
- Hadamard: The $n$-qubit Hadamard operator is defined by
$$\mathsf{H}^{\otimes n} = 2^{-n/2} \sum_{x,y \in \{0,1\}^n} (-1)^{\langle x, y\rangle} |x\rangle\langle y| \,.$$

**Choi-Jamiołkowski isomorphism.** Let $\mathcal{H}_{\mathsf{A}}$ be a $d$-dimensional Hilbert space with an orthonormal basis denoted by $\{|1\rangle, \dots, |d\rangle\}$. Let $|\Omega\rangle = \sum_{i\in[d]} |i\rangle \otimes |i\rangle$ be the vectorization of the identity $\mathbb{I}_d = \sum_{i\in[d]} |i\rangle\langle i|$. Then, the Choi-Jamiołkowski isomorphism $J(\Phi) \in \mathrm{L}(\mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{A}'})$ with respect to a linear map of the form $\Phi : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ is defined as
$$J(\Phi) = (\Phi_{\mathsf{A}\to\mathsf{B}} \otimes \mathbb{I}_{\mathsf{A}'})(|\Omega\rangle\langle\Omega|) = \sum_{i,j\in[d]} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j| \,.$$

We use the following well known fact.

**Lemma 3.1.** *Let $\Phi : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ be a linear map. Then, for any $|\psi\rangle \in \mathrm{S}(\mathcal{H}_{\mathsf{A}})$ and $|\phi\rangle \in \mathrm{S}(\mathcal{H}_{\mathsf{B}})$,*
$$\langle\phi|\, \Phi(|\psi\rangle\langle\psi|)\, |\phi\rangle = \langle\phi| \otimes \langle\bar{\psi}|\, J(\Phi)\, |\phi\rangle \otimes |\bar{\psi}\rangle \;,$$
*where the complex conjugation is taken with respect to the computational basis. Equivalently, we have:*
$$\mathrm{Tr}\left[|\phi\rangle\langle\phi|\, \Phi(|\psi\rangle\langle\psi|)\right] = \mathrm{Tr}\left[\left(|\phi\rangle\langle\phi| \otimes |\bar{\psi}\rangle\langle\bar{\psi}|\right) J(\Phi)\right] .$$

By linearity, we immediately obtain the following corollary:

**Corollary 3.2.** *Let $\Phi : \mathrm{L}(\mathcal{H}_{\mathsf{A}}) \to \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ be any linear map. Then, for any Hermitian operators $\mathbf{P} \in \mathrm{L}(\mathcal{H}_{\mathsf{B}})$ and $\mathbf{Q} \in \mathrm{L}(\mathcal{H}_{\mathsf{A}})$, it holds that*
$$\mathrm{Tr}\left[\mathbf{P}\Phi(\mathbf{Q})\right] = \mathrm{Tr}\left[\left(\mathbf{P} \otimes \bar{\mathbf{Q}}\right) J(\Phi)\right] .$$

### 3.2 Mixed Unitary Designs

In this section, we formally define the *Haar measure* [Sim95] and define a new and more general version of a *mixed* unitary $t$-design which also allows for inverses with respect to the adjoint of the unitary.

**Definition 3.3** (Haar measure)**.** *Let $d \in \mathbb{N}$ denote the dimension. The Haar measure $\mu_H$ is the unique left and right unitarily-invariant measure over the unitary group $\mathrm{U}(d)$; that is, for every (possibly matrix-valued) integrable function $f$ with domain $\mathrm{L}(\mathbb{C}^d)$ and every unitary $V \in \mathrm{U}(d)$,*

$$\int_{\mathrm{U}(d)} f(U)\, \mathrm{d}_{\mu_H} U = \int_{\mathrm{U}(d)} f(U \cdot V)\, \mathrm{d}_{\mu_H} U = \int_{\mathrm{U}(d)} f(V \cdot U)\, \mathrm{d}_{\mu_H} U.$$

*For brevity, we oftentimes denote the expectation of $f$ over the Haar measure by*

$$\mathop{\mathbb{E}}_{U \sim \mathrm{U}(d)}[f(U)] = \int_{\mathrm{U}(d)} f(U)\, \mathrm{d}_{\mu_H} U.$$

**Vectorization Formalism.** For a linear operator $\mathbf{\Lambda} \in \mathrm{L}(\mathbb{C}^d)$, we consider the corresponding vectorization map $\mathrm{vec} : \mathrm{L}(\mathbb{C}^d) \to (\mathbb{C}^d)^{\otimes 2}$ which is defined as follows:

$$\mathbf{\Lambda} = \sum_{i,j \in [d]} \Lambda_{(i,j)} |i\rangle\langle j| \quad \mapsto \quad \mathrm{vec}(\mathbf{\Lambda}) := |\mathbf{\Lambda}\rangle\!\rangle = \sum_{i,j \in [d]} \Lambda_{(i,j)} |i\rangle \otimes |j\rangle .$$

We are also going to use the so-called ABC-rule [Mel24]: for any linear operators $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathrm{L}(\mathbb{C}^d)$,

$$|\mathbf{ABC}\rangle\!\rangle = (\mathbf{A} \otimes \mathbf{C}^{\intercal})\, |\mathbf{B}\rangle\!\rangle.$$

**Non-Adaptive Mixed Unitary Designs.** In this section, we introduce a generalization of the standard notion of a unitary $t$-design which also accounts for inverse queries (to the adjoint of the unitary). We exclusively consider exact designs; in particular, exact unitary 3-designs via the Clifford group [Web16].

**Definition 3.4** (Mixed-Adjoint Moment Operator)**.** *Let $\nu$ be an ensemble of unitary operators over $\mathbb{C}^d$. Then, we define the mixed-adjoint $(p, q)$-moment operator $\mathcal{M}^{(p,q)}_{\nu,\mathsf{adj}} : \mathrm{L}(\mathbb{C}^d) \to \mathrm{L}(\mathbb{C}^d)$ by*

$$\mathcal{M}^{(p,q)}_{\nu,\mathsf{adj}}(\mathbf{O}) := \mathop{\mathbb{E}}_{U \sim \nu}\left[(U^{\otimes p} \otimes (U^{\dagger})^{\otimes q})\mathbf{O}(U^{\otimes p} \otimes (U^{\dagger})^{\otimes q})^{\dagger}\right]$$

*for a linear operator $\mathbf{O} \in \mathrm{L}((\mathbb{C}^d)^{\otimes (p+q)})$. Similarly, we let $\mathcal{M}^{(p,q)}_{\mathrm{U}(d),\mathsf{adj}}$ denote the mixed-adjoint $(p, q)$-moment operator with respect to the Haar measure over the unitary group $\mathcal{U}_d$.*

**Definition 3.5** (Non-Adaptive Mixed Unitary $(p, q)$-Design)**.** *Let $\nu$ be an ensemble of unitary operators over $\mathbb{C}^d$. Then, $\nu$ is a (non-adaptive) unitary $(p, q)$-design if, for every $\mathbf{O} \in \mathrm{L}((\mathbb{C}^d)^{\otimes (p+q)})$,*

$$\mathop{\mathbb{E}}_{U \sim \nu}\left[(U^{\otimes p} \otimes (U^{\dagger})^{\otimes q})\mathbf{O}(U^{\otimes p} \otimes (U^{\dagger})^{\otimes q})^{\dagger}\right] = \mathop{\mathbb{E}}_{U \sim \mathrm{U}(d)}\left[(U^{\otimes p} \otimes (U^{\dagger})^{\otimes q})\mathbf{O}(U^{\otimes p} \otimes (U^{\dagger})^{\otimes q})^{\dagger}\right].$$

Note that a unitary $t$-design is a special case of the above definition.

**Definition 3.6** (Non-Adaptive Unitary $t$-Design)**.** *Let $\nu$ be an ensemble of unitary operators over $\mathbb{C}^d$. Then, $\nu$ is a (non-adaptive) unitary $t$-design if it is a (non-adaptive) unitary $(t, q)$-design for $q = 0$.*

We show the following equivalence in terms of the vectorized mixed moment operator.

**Lemma 3.7.** *A unitary ensemble $\nu$ over $\mathbb{C}^d$ is a (non-adaptive) unitary $(p,q)$-design if and only if*

$$\mathop{\mathbb{E}}_{U\sim\nu}\left[U^{\otimes p}\otimes(U^{\dagger})^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes(U^{\intercal})^{\otimes q}\right]=\mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}\left[U^{\otimes p}\otimes(U^{\dagger})^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes(U^{\intercal})^{\otimes q}\right].$$

*Proof.* Suppose that $\nu$ is a unitary $(p,q)$-design. Then, for all $\mathbf{O}\in\mathrm{L}((\mathbb{C}^d)^{\otimes(p+q)})$, it holds that

$$\mathcal{M}^{(p,q)}_{\nu,\mathsf{adj}}(\mathbf{O})=\mathcal{M}^{(p,q)}_{\mathrm{U}(d),\mathsf{adj}}(\mathbf{O}).$$

By applying the vectorization $\mathrm{vec}:\mathrm{L}((\mathbb{C}^d)^{\otimes(p+q)})\to((\mathbb{C}^d)^{\otimes(p+q)})^{\otimes 2}$ on both sides, we get

$$|\mathcal{M}^{(p,q)}_{\nu,\mathsf{adj}}(\mathbf{O})\rangle\!\rangle=|\mathcal{M}^{(p,q)}_{\mathrm{U}(d),\mathsf{adj}}(\mathbf{O})\rangle\!\rangle.$$

By linearity and the $ABC$-rule for $\mathrm{vec}(\cdot)$, this is equivalent to

$$\mathop{\mathbb{E}}_{U\sim\nu}\left[U^{\otimes p}\otimes(U^{\dagger})^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes(U^{\intercal})^{\otimes q}\right]|\mathbf{O}\rangle\!\rangle=\mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}\left[U^{\otimes p}\otimes(U^{\dagger})^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes(U^{\intercal})^{\otimes q}\right]|\mathbf{O}\rangle\!\rangle.$$

Because $\mathrm{vec}(\cdot)$ is a bijection between $\mathrm{L}((\mathbb{C}^d)^{\otimes(p+q)})$ and $((\mathbb{C}^d)^{\otimes(p+q)})^{\otimes 2}$, the operators above must be identical on the entire vector space $((\mathbb{C}^d)^{\otimes(p+q)})^{\otimes 2}$. The converse statement can be shown analogously. ☐

**Lemma 3.8.** *A unitary $t$-design $\nu$ is a mixed unitary $(p,q)$-design for any $p,q$ with $t=p+q$.*

*Proof.* Let $t=p+q$. According to Theorem 3.7, it suffices to show that $\nu$ satisfies

$$\mathop{\mathbb{E}}_{U\sim\nu}\left[U^{\otimes p}\otimes(U^{\dagger})^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes(U^{\intercal})^{\otimes q}\right]=\mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}\left[U^{\otimes p}\otimes(U^{\dagger})^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes(U^{\intercal})^{\otimes q}\right].$$

By inserting the partial transpose with respect to the 2nd and 4th system, this is equivalent to

$$\mathop{\mathbb{E}}_{U\sim\nu}\left[U^{\otimes p}\otimes\bar{U}^{\otimes q}\otimes\bar{U}^{\otimes q}\otimes U^{\otimes p}\right]^{\intercal_{2,4}}=\mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}\left[U^{\otimes p}\otimes\bar{U}^{\otimes q}\otimes\bar{U}^{\otimes q}\otimes U^{\otimes p}\right]^{\intercal_{2,4}}.$$

After inserting a $\mathsf{SWAP}$ between the 2nd and 4th system via $\mathbb{F}_{2,4}$, it is also equivalent to showing that

$$\left[\mathbb{F}^{\dagger}_{2,4}\mathop{\mathbb{E}}_{U\sim\nu}\left[U^{\otimes p}\otimes U^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes\bar{U}^{\otimes q}\right]\mathbb{F}_{2,4}\right]^{\intercal_{2,4}}=\left[\mathbb{F}^{\dagger}_{2,4}\mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}\left[U^{\otimes p}\otimes U^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes\bar{U}^{\otimes q}\right]\mathbb{F}_{2,4}\right]^{\intercal_{2,4}}.$$

By assumption, $\nu$ is a unitary $t$-design for $t=p+q$, and hence it holds that

$$\mathop{\mathbb{E}}_{U\sim\nu}\left[U^{\otimes p}\otimes U^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes\bar{U}^{\otimes q}\right]=\mathop{\mathbb{E}}_{U\sim\mathrm{U}(d)}\left[U^{\otimes p}\otimes U^{\otimes q}\otimes\bar{U}^{\otimes p}\otimes\bar{U}^{\otimes q}\right]$$

which yields the desired equality from before. ☐

**Adaptive Mixed Unitary Designs.** In this section, we generalize the notion of mixed unitary designs to algorithms which may query a unitary (and possibly its inverse) adaptively, rather than in parallel.

**Definition 3.9** (Adaptive Mixed Unitary $(p, q)$-Design)**.** *Let $\nu$ be an ensemble of unitary operators over $\mathbb{C}^d$. Then, $\nu$ is an adaptive unitary $(p, q)$-design if, for every single-bit output (possibly adaptive) quantum algorithm $\mathcal{A}$ making at most $p$ many queries to a unitary and $q$ many queries to its adjoint,*

$$\Pr\left[1 \leftarrow \mathcal{A}^{U,U^\dagger}(1^{\lceil \log d \rceil}) \,:\, U \sim \nu\right] = \Pr\left[1 \leftarrow \mathcal{A}^{U,U^\dagger}(1^{\lceil \log d \rceil}) \,:\, U \sim \mathrm{U}(d)\right].$$

*We say that $\nu$ is an adaptive mixed unitary $t$-design if the property above holds for any adaptive quantum query algorithm $\mathcal{A}$ which submits no more than $t$ queries to either $U$ or $U^\dagger$.*

We now show that an (exact) non-adaptive mixed unitary $t$-design is automatically also an (exact) adaptive mixed unitary $t$-design. In the approximate case, this conversion incurs an exponential blow-up.

**Theorem 3.10.** *Any exact non-adaptive unitary $t$-design is also an exact adaptive mixed unitary $t$-design.*

*Proof.* Let $\nu$ be a non-adaptive unitary $t$-design over $\mathbb{C}^d$. Suppose that $\mathcal{A}^{U,U^\dagger}(1^{\lceil \log d \rceil})$ is an adaptive $t$-query quantum algorithm that makes $p$ many queries to $U$ and $q$ queries to $U^\dagger$, for $U \in \mathrm{U}(d)$ and $t = p + q$.

The idea is to use a standard gate teleportation approach, similar to [AMR19, Kre21]. Concretely, we can argue that, for any $U \in \mathrm{U}(d)$, there exists a non-adaptive algorithm $\mathcal{B}^{U,U^\dagger}(1^{\lceil \log d \rceil})$ that makes $p$ many parallel queries to $U$ and $q$ many parallel queries to $U^\dagger$ such that

$$\Pr\left[1 \leftarrow \mathcal{A}^{U,U^\dagger}(1^{\lceil \log d \rceil})\right] = d^{2(p+q)} \Pr\left[1 \leftarrow \mathcal{B}^{U,U^\dagger}(1^{\lceil \log d \rceil})\right].$$

This essentially follows from [Kre21, Lemma 23], since the non-adaptive query algorithm has access to both $U$ and $U^\dagger$. Because $\nu$ is a non-adaptive unitary $t$-design, we know from Theorem 3.8 that $\nu$ is also mixed unitary $(p, q)$-design. Putting everything together, we get that

$$\begin{aligned}\Pr\left[1 \leftarrow \mathcal{A}^{U,U^\dagger}(1^{\lceil \log d \rceil}) \,:\, U \sim \nu\right] &= d^{2(p+q)} \Pr\left[1 \leftarrow \mathcal{B}^{U,U^\dagger}(1^{\lceil \log d \rceil}) \,:\, U \sim \nu\right] \\ &= d^{2(p+q)} \Pr\left[1 \leftarrow \mathcal{B}^{U,U^\dagger}(1^{\lceil \log d \rceil}) \,:\, U \sim \mathrm{U}(d)\right] \\ &= \Pr\left[1 \leftarrow \mathcal{A}^{U,U^\dagger}(1^{\lceil \log d \rceil}) \,:\, U \sim \mathrm{U}(d)\right].\end{aligned}$$

This proves the claim. □

### 3.3 Pseudorandom Unitaries

Pseudorandom unitaries are ensembles of unitary operators that look indistinguishable from Haar random unitaries for all computationally bounded observers. These ensembles of unitaries have been first proposed in [JLS18], and have only very recently been constructed assuming the existence of post-quantum one-way functions [MPSY24, MH24]. We give a formal definition below.

**Definition 3.11** (Pseudorandom Unitary)**.** *Let $\lambda$ be the security parameter, $n := n(\lambda) \in \mathbb{N}$ be some polynomial, and $d = 2^n$. An infinite sequence $\mathfrak{U} = \{\mathfrak{U}_n\}_{n \in \mathbb{N}}$ of $n$-qubit unitary ensembles $\mathfrak{U}_n = \{U_{\theta,n}\}_{\theta \in \{0,1\}^\lambda}$ is a pseudorandom unitary if it satisfies the following conditions:*

- ***(Efficient computation)*** *For all $\lambda, n$, there exists a polynomial-time quantum algorithm $\mathcal{Q}$ such that for all keys $\theta \in \{0,1\}^\lambda$, and any $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, it holds that*

$$\mathcal{Q}(\theta, |\psi\rangle) = U_{\theta,n} |\psi\rangle \ .$$

- ***(Pseudorandomness)*** *The unitary $U_{\theta,n}$, for a random key $\theta \sim \{0,1\}^\lambda$, is computationally indistinguishable from a Haar random unitary $U \sim \mathrm{U}(d)$. In other words, for any QPT algorithm $\mathcal{A}$, it holds that*

$$\left| \Pr_{\theta \sim \{0,1\}^\lambda}[\mathcal{A}^{U_{\theta,n},U_{\theta,n}^\dagger}(1^\lambda, 1^n) = 1] - \Pr_{U \sim \mathrm{U}(d)}[\mathcal{A}^{U_{\theta,n},U_{\theta,n}^\dagger}(1^\lambda, 1^n) = 1] \right| \leq \mathsf{negl}(\lambda)\,.$$

**Remark 2.** *We note that this definition of pseudorandom unitary is quite strong; the adversary $\mathcal{A}$ is free to make its queries adaptively, and moreover it is allowed to query both $U$ and $U^\dagger$, in analogy to strong pseudorandom permutations. This notion was constructed in recent work by Ma and Huang [MH24].*

### 3.4 Operator Norm Bounds

In this section, we lay out some tools for bounding the operator norm $\|\mathbf{A}\|_\infty$ of operators $A \in \mathbb{C}^{d\times d}$. For matrices $\mathbf{A}, \mathbf{B}$ of the same dimensions, we use $\mathbf{A} \circ \mathbf{B}$ to denote their entrywise product.

**Lemma 3.12** (Well-known)**.** *For any matrix $\mathbf{A} \in \mathbb{C}^{d_1 \times d_2}$, we have*

$$\|\mathbf{A}\|_\infty = \sqrt{\lambda_{\max}(\mathbf{A}^\dagger \mathbf{A})} = \sqrt{\lambda_{\max}(\mathbf{A}\mathbf{A}^\dagger)} = \max\left\{\|\mathbf{A}x\|_2 : \|x\|_2 = 1\right\}.$$

*Moreover, if $\mathbf{A}$ has rank $\leq 1$, then we have $\lambda_{\max}(\mathbf{A}^\dagger\mathbf{A}) = \mathrm{Tr}\left[\mathbf{A}^\dagger\mathbf{A}\right]$.*

**Lemma 3.13** (Well-known)**.** *For any pair of matrices $\mathbf{A} \in \mathbb{C}^{d_1\times d_2}$ and $\mathbf{A}' \in \mathbb{C}^{d_1'\times d_2'}$ such that $\mathbf{A}'$ is a submatrix of $\mathbf{A}$, we have $\|\mathbf{A}'\|_\infty \leq \|\mathbf{A}\|_\infty$.*

**Lemma 3.14** (Well-known)**.** *For $\mathbf{A} \in \mathbb{C}^{d_1\times d_2}$ and $\mathbf{B} \in \mathbb{C}^{d_3\times d_4}$, we have $\|\mathbf{A} \otimes \mathbf{B}\|_\infty = \|\mathbf{A}\|_\infty \cdot \|\mathbf{B}\|_\infty$.*

**Lemma 3.15.** *Let $\mathbf{A}_1, \ldots, \mathbf{A}_k \in \mathbb{C}^{d\times d}$ be unitary matrices with $k \geq 2$. Then, the rows and columns of $\mathbf{C} = \mathbf{A}_1 \circ \ldots \circ \mathbf{A}_k$ all have $\ell_1$ norm $\leq 1$.*

*Proof.* In the case of rows, we have:

$$\begin{aligned}
\sum_{j=1}^d |C_{i,j}| &= \sum_{j=1}^d |A_{1;(i,j)}| \cdot \ldots \cdot |A_{k;(i,j)}| \\
&\leq \sum_{j=1}^d |A_{1;(i,j)}| \cdot |A_{2;(i,j)}| \text{ (all entries of a unitary are } \leq 1) \\
&\leq \sqrt{\left(\sum_{j=1}^d |A_{1;(i,j)}|^2\right) \cdot \left(\sum_{j=1}^d |A_{2;(i,j)}|^2\right)} \text{ (Cauchy-Schwarz)} \\
&= 1.
\end{aligned}$$

The case of columns is analogous. ∎

**Lemma 3.16.** *Let $\mathbf{C} \in \mathbb{C}^{d_1 \times d_2}$ be such that the $\ell_1$ norm of each row is $\leq a$ and the $\ell_1$ norm of each column is $\leq b$. Then $\|\mathbf{C}\|_\infty \leq \sqrt{ab}$.*

*Proof.* For any row $i$ of $\mathbf{C}^\dagger \mathbf{C} \in \mathbb{C}^{d_2 \times d_2}$, we have:

$$\begin{aligned}\sum_{j=1}^{d_2} |(\mathbf{C}^\dagger \mathbf{C})_{i,j}| &= \sum_{j=1}^{d_2} |\sum_{k=1}^{d_1} C^\dagger_{i,k} C_{k,j}| \\ &\leq \sum_{j=1}^{d_2} \sum_{k=1}^{d_1} |C_{k,i}||C_{k,j}| \\ &\leq a \cdot \sum_{k=1}^{d} |C_{k,i}| \\ &\leq ab.\end{aligned}$$

Since the maximum eigenvalue of a square matrix is at most the maximum $\ell_1$ norm of its rows, we have $\left\|\mathbf{C}^\dagger \mathbf{C}\right\|_\infty \leq ab \Rightarrow \|\mathbf{C}\|_\infty \leq \sqrt{ab}$. $\square$

We also define and state some simple properties of matrix inner products:

**Definition 3.17.** *For matrices $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{d_1 \times d_2}$, define the inner product*

$$\langle \mathbf{A}, \mathbf{B} \rangle = \sum_{i \in [d_1], j \in [d_2]} \overline{A_{i,j}} \cdot B_{i,j} = \operatorname{Tr}\left[\mathbf{A}^\dagger \mathbf{B}\right].$$

*We also define the Frobenius norm $\|\mathbf{A}\|_F = \sqrt{\langle \mathbf{A}, \mathbf{A} \rangle}$.*

**Lemma 3.18.** *For matrices $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{d \times d}$, we have:*

- *(Cauchy-Schwarz) $|\langle \mathbf{A}, \mathbf{B} \rangle| \leq \|\mathbf{A}\|_F \cdot \|\mathbf{B}\|_F$.*
- *(Well-known) If $\mathbf{A}$ is Hermitian and $\mathbf{B}$ is Hermitian PSD, then we have $|\langle \mathbf{A}, \mathbf{B} \rangle| \leq \|\mathbf{A}\|_\infty \cdot \operatorname{Tr}[\mathbf{B}]$.*

### 3.4.1 Blockwise Tensor Products

This section is devoted to stating and proving Theorem 3.19, which will serve as our central linear algebraic workhorse. We will make some comments about this theorem and its proof at the end of this section. We will then present some straightforward consequences of this theorem in Section 3.4.2, which we will use directly when analyzing $t \mapsto t+1$ cloning games.

**Theorem 3.19.** *Let $R, C$ be positive integers. Let $r_1, r_2, \ldots, r_R, r'_1, r'_2, \ldots, r'_R, c_1, \ldots, c_C, c'_1, \ldots, c'_C$ be positive integers. For each $i \in [R], k \in [C]$, let $\mathbf{A}_{i,k} \in \mathbb{C}^{r_i \times c_k}$ and $\mathbf{B}_{i,k} \in \mathbb{C}^{r'_i \times c'_k}$ be matrices. Additionally, for each $i \in [R], k \in [C]$, let $\gamma_{i,k} \in \mathbb{C}$ be a scalar of magnitude at most 1, i.e. $|\gamma_{i,k}| \leq 1$.*

*Define the following block matrices:*

$$\mathbf{A} := \begin{bmatrix} \mathbf{A}_{1,1} & \ldots & \mathbf{A}_{1,C} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{R,1} & \ldots & \mathbf{A}_{R,C} \end{bmatrix} \in \mathbb{C}^{(r_1 + \ldots + r_R) \times (c_1 + \ldots + c_C)}$$

$$\mathbf{B} := \begin{bmatrix} \mathbf{B}_{1,1} & \dots & \mathbf{B}_{1,C} \\ \vdots & \ddots & \vdots \\ \mathbf{B}_{R,1} & \dots & \mathbf{B}_{R,C} \end{bmatrix} \in \mathbb{C}^{(r'_1+\ldots+r'_R)\times(c'_1+\ldots+c'_C)}$$

$$\mathbf{M} := \begin{bmatrix} \gamma_{1,1}\mathbf{A}_{1,1}\otimes\mathbf{B}_{1,1} & \dots & \gamma_{1,C}\mathbf{A}_{1,C}\otimes\mathbf{B}_{1,C} \\ \vdots & \ddots & \vdots \\ \gamma_{R,1}\mathbf{A}_{R,1}\otimes\mathbf{B}_{R,1} & \dots & \gamma_{R,C}\mathbf{A}_{R,C}\otimes\mathbf{B}_{R,C} \end{bmatrix} \in \mathbb{C}^{(r_1r'_1+\ldots+r_Rr'_R)\times(c_1c'_1+\ldots+c_Cc'_C)}.$$

*Suppose both of the following conditions hold:*

1. $\|\mathbf{A}\|_\infty \le 1$.
2. *Each block column of* $\mathbf{B}$ *has operator norm* $\le 1$ *i.e. for all* $k \in [C]$, *we have*

$$\left\| \begin{bmatrix} \mathbf{B}_{1,k} \\ \vdots \\ \mathbf{B}_{R,k} \end{bmatrix} \right\|_\infty \le 1.$$

*Then, it holds that* $\|\mathbf{M}\|_\infty \le 1$.

**High-level proof idea.** The main idea is as follows: it suffices to show that for any unit vectors $x, y$ of the right dimensions that $|x^\dagger \mathbf{M} y| \le 1$. As a function of $B$, $x^\dagger \mathbf{M} y$ is linear. We can hence express this as the inner product of $\mathbf{B}$ with some other matrix. It turns out that this matrix has a simple form; reformulating the problem in these terms will allow us to use the standard bounds stated in Lemma 3.18.

**Notation.** We begin by setting up some notation. If we have a sequence of matrices $\{\mathbf{A}_I : I \in \mathcal{I}\}$ indexed by $I$ with rows and columns indexed by $r \in \mathcal{R}$ and $c \in \mathcal{C}$, we use $(\mathbf{A}_I)_{r;c}$ to denote the entry in row $r$ and column $c$ of matrix $\mathbf{A}_I$.

Now let us define $\widetilde{\mathbf{B}}$ as follows, and let $\mathbf{B}'$ be its entrywise conjugate:

$$\widetilde{\mathbf{B}} := \begin{bmatrix} \widetilde{\mathbf{B}_{1,1}} & \dots & \widetilde{\mathbf{B}_{1,C}} \\ \vdots & \ddots & \vdots \\ \widetilde{\mathbf{B}_{R,1}} & \dots & \widetilde{\mathbf{B}_{R,C}} \end{bmatrix} = \begin{bmatrix} \gamma_{1,1}\mathbf{B}_{1,1} & \dots & \gamma_{1,C}\mathbf{B}_{1,C} \\ \vdots & \ddots & \vdots \\ \gamma_{R,1}\mathbf{B}_{R,1} & \dots & \gamma_{R,C}\mathbf{B}_{R,C} \end{bmatrix} \in \mathbb{C}^{(r'_1+\ldots+r'_R)\times(c'_1+\ldots+c'_C)}.$$

As outlined earlier, it suffices to show for any unit vectors $x \in \mathbb{C}^{r_1r'_1+\ldots+r_Rr'_R}$ and $y \in \mathbb{C}^{c_1c'_1+\ldots+c_Cc'_C}$ that $|x^\dagger \mathbf{M} y| \le 1$. We index the entries of $x$ by an index $i \in [R]$ and then values $j \in [r_i]$ and $j' \in [r'_i]$. We similarly index the entries of $y$ by $(k, l, l')$. We can also apply this same indexing to the rows and columns of $\mathbf{M}$. Thus for $i \in [R]$ and $k \in [C]$, we can define $\mathbf{M}_{i,k} \in \mathbb{C}^{r_ir'_i \times c_kc'_k}$ by $\mathbf{M}_{i,k} = \gamma_{i,k}\mathbf{A}_{i,k} \otimes \mathbf{B}_{i,k}$ (i.e. this is one block of $\mathbf{M}$).

For each $i \in [R]$, let $\mathbf{X}_i \in \mathbb{C}^{r_i \times r'_i}$ be defined by $(\mathbf{X}_i)_{j;j'} = x_{(i,j,j')}$. Similarly define $\mathbf{Y}_k \in \mathbb{C}^{c_k \times c'_k}$ for each $k \in [C]$. We also defined the following matrices:

$$\mathbf{X} := \begin{bmatrix} \mathbf{X}_1 & 0 & \dots & 0 \\ 0 & \mathbf{X}_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \mathbf{X}_R \end{bmatrix} \in \mathbb{C}^{(r_1+\ldots+r_R)\times(r'_1+\ldots+r'_R)}$$

$$\mathbf{Y} := \begin{bmatrix} \mathbf{Y}_1 & 0 & \dots & 0 \\ 0 & \mathbf{Y}_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \mathbf{Y}_C \end{bmatrix} \in \mathbb{C}^{(c_1+\ldots+c_C)\times(c'_1+\ldots+c'_C)}.$$

It is straightforward to see that $\|\mathbf{X}\|_F = \|\mathbf{Y}\|_F = 1$, since the nonzero entries in $\mathbf{X}$ are exactly the same as in $x$, and similarly for $Y$ and $y$.

Finally, over $\mathbb{C}_{c'_1+\ldots+c'_C}$, for each $k \in [C]$ define the projector $\Pi'_k$ to be onto the natural $c'_k$ coordinates (more precisely, all coordinates $z$ such that $c'_1 + \ldots + c'_{k-1} < z \leq c'_1 + \ldots + c'_k$. Note then that the block-diagonal structure of $Y$ implies that:

$$\mathbf{Y}^\dagger \mathbf{Y} = \sum_{k\in[C]} \Pi'_k \mathbf{Y}^\dagger \mathbf{Y} \Pi'_k. \tag{4}$$

**Rewriting $x^\dagger \mathbf{M}\, y$ as a linear function of $\mathbf{B}'$.** We now show that $x^\dagger \mathbf{M}\, y$ can be written as a linear function of $B'$. This is captured in the following lemma:

**Lemma 3.20.** *We have*

$$x^\dagger\, \mathbf{M}\, y = \mathrm{Tr}\left[\mathbf{X}^\dagger \mathbf{A} \mathbf{Y} (\mathbf{B}')^\dagger\right].$$

*Proof.* We proceed as follows:

$$\begin{aligned}
x^\dagger \mathbf{M}\, y &= \sum_{i\in[R],k\in[C]} \; \sum_{j\in[r_i],j'\in[r'_i],l\in[c_k],l'\in[c'_k]} \overline{x_{(i,j,j')}}\, (\mathbf{M}_{i,k})_{(j,j');(l,l')}\, y_{(k,l,l')} \\
&= \sum_{i\in[R],k\in[C]} \; \sum_{j\in[r_i],j'\in[r'_i],l\in[c_k],l'\in[c'_k]} \overline{x_{(i,j,j')}} \left(\mathbf{A}_{i,k} \otimes \widetilde{\mathbf{B}_{i,k}}\right)_{(j,j');(l,l')} y_{(k,l,l')} \\
&= \sum_{i\in[R],k\in[C]} \; \sum_{j\in[r_i],j'\in[r'_i],l\in[c_k],l'\in[c'_k]} \overline{x_{(i,j,j')}}\, (\mathbf{A}_{i,k})_{j;l} \left(\widetilde{\mathbf{B}}_{i,k}\right)_{j';l'} y_{(k,l,l')} \\
&= \sum_{i\in[R],k\in[C]} \; \sum_{j'\in[r'_i],l'\in[c'_k]} \left(\widetilde{\mathbf{B}}_{i,k}\right)_{j';l'} \cdot \left( \sum_{j\in[r_i],l\in[c_k]} \overline{x_{(i,j,j')}}\, (\mathbf{A}_{i,k})_{j;l}\, y_{(k,l,l')} \right) \\
&= \sum_{i\in[R],k\in[C]} \; \sum_{j'\in[r'_i],l'\in[c'_k]} \left(\widetilde{\mathbf{B}}_{i,k}\right)_{j';l'} \cdot \left( \sum_{j\in[r_i],l\in[c_k]} \overline{(\mathbf{X}_i)_{j;j'}}\, (\mathbf{A}_{i,k})_{j;l}\, (\mathbf{Y}_k)_{l;l'} \right) \\
&= \sum_{i\in[R],k\in[C]} \; \sum_{j'\in[r'_i],l'\in[c'_k]} \left(\widetilde{\mathbf{B}}_{i,k}\right)_{j';l'} \cdot \left( \sum_{j\in[r_i],l\in[c_k]} \left(\mathbf{X}_i^\dagger\right)_{j';j} (\mathbf{A}_{i,k})_{j;l}\, (\mathbf{Y}_k)_{l;l'} \right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i\in[R],k\in[C]} \sum_{j'\in[r_i'],l'\in[c_k']} \left(\widetilde{\mathbf{B}}_{i,k}\right)_{j';l'} \cdot \left(\mathbf{X}_i^\dagger \mathbf{A}_{i,k} \mathbf{Y}_k\right)_{j';l'} \\
&= \sum_{i\in[R],k\in[C]} \sum_{j'\in[r_i'],l'\in[c_k']} \widetilde{\mathbf{B}}_{(i,j');(k,l')} \cdot (\mathbf{X}^\dagger \mathbf{A}\mathbf{Y})_{(i,j');(k,l')} \\
&= \langle \mathbf{B}', \mathbf{X}^\dagger \mathbf{A}\mathbf{Y}\rangle \;=\; \mathrm{Tr}\left[(\mathbf{B}')^\dagger \mathbf{X}^\dagger \mathbf{A}\mathbf{Y}\right] \;=\; \mathrm{Tr}\left[\mathbf{X}^\dagger \mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right].
\end{aligned}
$$

□

**Bounding the operator norm of $B'\Pi_k'$.** Our second ingredient will be the following straightforward observation:

**Lemma 3.21.** *For any $k \in [C]$, we have $\|\mathbf{B}'\Pi_k'\|_\infty \le 1$.*

*Proof.* After removing zero columns, $\mathbf{B}'\Pi_k'$ is just the following block matrix:

$$
\begin{bmatrix} \overline{\gamma_{1,k}}\,\overline{\mathbf{B}_{1,k}} \\ \vdots \\ \overline{\gamma_{R,k}}\,\overline{\mathbf{B}_{R,k}} \end{bmatrix}.
$$

This is the result of taking $\begin{bmatrix} \mathbf{B}_{1,k} \\ \vdots \\ \mathbf{B}_{R,k} \end{bmatrix}$, multiplying each row by a scalar of magnitude $\le 1$, then conjugating all entries. The latter two operations do not increase operator norm, and we are assuming that the starting matrix has operator norm $\le 1$. The conclusion follows. □

**Completing the proof.** We are now ready to complete the proof of Theorem 3.19; this will follow from the standard inequalities stated in Lemma 3.18, in addition to using the block-diagonal structure of $Y$ (as in Equation (4)).

*Proof of Theorem 3.19.* Starting from Lemma 3.20, we have:

$$
\begin{aligned}
|x^\dagger \mathbf{M}\, y| &= \left|\mathrm{Tr}\left[\mathbf{X}^\dagger \mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right]\right| \\
&\le \|\mathbf{X}\|_F \cdot \left\|\mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right\|_F \quad \text{(Lemma 3.18)} \\
&= \left\|\mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right\|_F .
\end{aligned}
$$

Continuing from here, we have:

$$
\begin{aligned}
\left\|\mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right\|_F^2 &= \mathrm{Tr}\left[\mathbf{B}'\mathbf{Y}^\dagger \mathbf{A}^\dagger \mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger\right] \\
&= \mathrm{Tr}\left[\mathbf{A}^\dagger \mathbf{A}\mathbf{Y}(\mathbf{B}')^\dagger \mathbf{B}'\mathbf{Y}^\dagger\right] \\
&\le \mathrm{Tr}\left[\mathbf{Y}(\mathbf{B}')^\dagger \mathbf{B}'\mathbf{Y}^\dagger\right] \quad \text{(Lemma 3.18; } \|\mathbf{A}\|_\infty \le 1\text{)} \\
&= \mathrm{Tr}\left[\mathbf{Y}^\dagger \mathbf{Y}(\mathbf{B}')^\dagger \mathbf{B}'\right]
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{k\in[C]} \operatorname{Tr}\left[\Pi'_k \mathbf{Y}^\dagger \mathbf{Y} \Pi'_k (\mathbf{B}')^\dagger \mathbf{B}'\right] \text{ (Equation (4))} \\
&= \sum_{k\in[C]} \operatorname{Tr}\left[\left(\Pi'_k \mathbf{Y}^\dagger \mathbf{Y} \Pi'_k\right)\left(\Pi'_k (\mathbf{B}')^\dagger \mathbf{B}' \Pi'_k\right)\right] \\
&\leq \sum_{k\in[C]} \operatorname{Tr}\left[\Pi'_k \mathbf{Y}^\dagger \mathbf{Y} \Pi'_k\right] \cdot \left\|\Pi'_k (\mathbf{B}')^\dagger \mathbf{B}' \Pi'_k\right\|_\infty \text{ (Lemma 3.18)} \\
&\leq \sum_{k\in[C]} \operatorname{Tr}\left[\Pi'_k \mathbf{Y}^\dagger \mathbf{Y} \Pi'_k\right] \text{ (Lemma 3.21)} \\
&= \sum_{k\in[C]} \operatorname{Tr}\left[\Pi'_k \mathbf{Y}^\dagger \mathbf{Y}\right] \\
&= \operatorname{Tr}\left[\mathbf{Y}^\dagger \mathbf{Y}\right] \\
&= \|\mathbf{Y}\|_F^2 \\
&= 1,
\end{aligned}
$$

thus completing the proof of the theorem. □

**Discussion.** Given the simplicity of the statement of Theorem 3.19, one might wonder why our proof is so involved. Here, we present some justification that this theorem is actually quite strong, and discuss some obstacles to more intuitive proof strategies. First, we note that our theorem captures some simple special cases:

- When $R = C = 1$, this is immediate from Lemma 3.14.
- When $\gamma_{i,k} = 1$ for all $i, k$ (or more generally $\gamma_{i,k}$ is constant) and $\|\mathbf{B}\|_\infty \leq 1$, this can be shown by noting that the matrix $\mathbf{M}$ would be a submatrix of $\mathbf{A} \otimes \mathbf{B}$, and then appealing to Lemma 3.14. (We rigorously argue this fact as part of the proof of Lemma 3.23.)

  However, this argument completely breaks down if $\gamma_{i,k}$ is allowed to vary between blocks.
- When $r_i = r'_i = c_k = c'_k = 1$ for all $i, k$, this boils down to bounding the operator norm of any complex $R \times C$ matrix with the entry in row $i$ and column $k$ having magnitude equal to $|A_{i;k} B_{i;k}|$ (noting that in this setting $A_{i;k}, B_{i;k}$ are scalars). This is not straightforward but still easier to handle; one can argue by Cauchy-Schwarz that the rows and columns of such a matrix must have $\ell_1$ norm $\leq 1$, and it is well-known that such a matrix must have operator norm $\leq 1$ (see Lemmas 3.15 and 3.16 for details).

  This argument also breaks down as soon as the block matrices $A_{i,k}, B_{i,k}$ are not just scalars; the $\ell_1$ norms of the rows and columns of $M$ will end up growing polynomially in $\max(r_1, \ldots, r_R, r'_1, \ldots, r'_R, c_1, \ldots, c_C, c'_1, \ldots, c'_C)$ in the worst case. (Jumping ahead, in the setting of oracular cloning games, this would yield a bound that degrades exponentially in the number of ancilla qubits that each adversary is allowed to use, which is of course undesirable.)

One could imagine "interpolating" between these two techniques by considering the operator norm of each block of $\mathbf{M}$ individually, and using this to obtain a bound on $\|\mathbf{M}\|_\infty$. Perhaps surprisingly, this is also *provably* insufficient. Suppose $R = C = n$ for some $n$, and $r_i = r'_i = c_k = c'_k = n$ for all $i, k$. Then let us take $\mathbf{A}, \mathbf{B}$ to be $n^2 \times n^2$ permutation matrices with exactly one 1 in each block. Now we will have $\|\mathbf{A}_{i,k}\|_\infty = \|\mathbf{B}_{i,k}\|_\infty = 1 \Rightarrow \|\mathbf{A}_{i,k} \otimes \mathbf{B}_{i,k}\|_\infty = 1$ for all $i, k$. However, there exist $n \times n$ block matrices (i.e. containing $n^2$ blocks in total) with each block having operator norm 1, but where the overall matrix has operator norm growing with $n$; one such example is the $n \times n$ all 1's matrix (appropriately padded with zero rows and columns to obtain the right dimensions). This counterexample implies that just considering the operator norm of each block of $\mathbf{M}$ is too lossy.

Thus Theorem 3.19 is quite strong and there are natural barriers to proof strategies that might feel more simple and intuitive. The proof we have presented is the simplest one that we are aware of.

### 3.4.2 Consequences

We now state some corollaries of Theorem 3.19 that we will later directly apply when bounding the operator norms relevant to cloning games in Section 9.3.

**Lemma 3.22.** *Let $\mathbf{A}_1, \ldots, \mathbf{A}_k$ be block matrices of $d$ columns. More formally, for each $i \in [k]$ set*

$$\mathbf{A}_i = \begin{bmatrix} \mathbf{A}_{i,1} & \ldots & \mathbf{A}_{i,d} \end{bmatrix},$$

*for some block matrices $\mathbf{A}_{i,1}, \ldots, \mathbf{A}_{i,d}$ that have the same number of rows but not necessarily the same number of columns. (Note that we do not require $\mathbf{A}_{i,1}$ and $\mathbf{A}_{j,1}$ to have the same number of rows when $i \neq j$.) Assume the following preconditions:*

1. *For all $i \in [k]$ and $j \in [d]$, we have $\|\mathbf{A}_{i,j}\|_\infty \leq 1$; and*
2. *There exists some $i \in [k]$ such that $\|\mathbf{A}_i\|_\infty \leq 1$.*

*Let*

$$\mathbf{A} = \begin{bmatrix} \bigotimes_{i=1}^k \mathbf{A}_{i,1} & \bigotimes_{i=1}^k \mathbf{A}_{i,2} & \ldots & \bigotimes_{i=1}^k \mathbf{A}_{i,d} \end{bmatrix}$$

*be defined as a "block column-wise tensor product" of $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_d$. Then $\|\mathbf{A}\|_\infty \leq 1$.*

*Proof.* Firstly, if $k = 1$ then we will have $\mathbf{A} = \mathbf{A}_1$ so the conclusion will follow from the second precondition. From now on, assume that $k \geq 2$. Also, by symmetry, let us assume without loss of generality that $\|\mathbf{A}_1\|_\infty \leq 1$.

Now define the matrix $\mathbf{M}$ as follows:

$$\mathbf{M} = \begin{bmatrix} \bigotimes_{i=2}^k \mathbf{A}_{i,1} & \bigotimes_{i=2}^k \mathbf{A}_{i,2} & \ldots & \bigotimes_{i=2}^k \mathbf{A}_{i,d} \end{bmatrix}.$$

Notice that, for each $j \in [d]$, the $j$th block column of $\mathbf{M}$ has operator norm equal to $\prod_{i=1}^k \|\mathbf{A}_{i,j}\|_\infty \leq 1$. Since we also have $\|\mathbf{A}_1\|_\infty \leq 1$, we can apply Theorem 3.19 to $\mathbf{A}_1$ and $\mathbf{M}$ (with $R = 1$, $C = d$, and $\gamma_{i,j} = 1$ for all $i, j$) to immediately obtain that $\|A\|_\infty \leq 1$, as desired. $\square$

**Lemma 3.23.** *Let $R, C$ be positive integers. Let $r_1, \ldots, r_R, c_1, \ldots, c_C$ be positive integers. Fix some integer $d \geq 2$. For each $t \in [d], i \in [R], k \in [C]$, let $\mathbf{A}_{t,i,k} \in \mathbb{C}^{r_i \times c_k}$ be a matrix. Additionally, for each $i \in [R], k \in [C]$, let $\gamma_{i,k} \in \mathbb{C}$ be a scalar of magnitude at most 1 i.e. $|\gamma_{i,k}| \leq 1$. Then define the following block matrices:*

$$\mathbf{A}_t := \begin{bmatrix} \mathbf{A}_{t,1,1} & \ldots & \mathbf{A}_{t,1,C} \\ \vdots & \ddots & \vdots \\ \mathbf{A}_{t,R,1} & \ldots & \mathbf{A}_{t,R,C} \end{bmatrix} \in \mathbb{C}^{(r_1 + \ldots + r_R) \times (c_1 + \ldots + c_C)}, \text{ for each } t \in [d]$$

$$\mathbf{M} := \begin{bmatrix} \gamma_{1,1} \bigotimes_{t=1}^{d} \mathbf{A}_{t,1,1} & \dots & \gamma_{1,C} \bigotimes_{t=1}^{d} \mathbf{A}_{t,1,C} \\ \vdots & \ddots & \vdots \\ \gamma_{R,1} \bigotimes_{t=1}^{d} \mathbf{A}_{t,R,1} & \dots & \gamma_{R,C} \bigotimes_{t=1}^{d} \mathbf{A}_{t,R,C} \end{bmatrix} \in \mathbb{C}^{(r_1^d + \ldots + r_R^d) \times (c_1^d + \ldots + c_C^d)}.$$

*Suppose that for all $t \in [d]$, we have $\|\mathbf{A}_t\|_\infty \leq 1$. Then $\|\mathbf{M}\|_\infty \leq 1$. (Note that the $d = 2$ case is immediate from Theorem 3.19.)*

*Proof.* Define the matrix

$$\mathbf{B} = \begin{bmatrix} \bigotimes_{t=2}^{d} \mathbf{A}_{t,1,1} & \dots & \bigotimes_{t=2}^{d} \mathbf{A}_{t,1,C} \\ \vdots & \ddots & \vdots \\ \bigotimes_{t=2}^{d} \mathbf{A}_{t,R,1} & \dots & \bigotimes_{t=2}^{d} \mathbf{A}_{t,R,C} \end{bmatrix} \in \mathbb{C}^{(r_1^{d-1} + \ldots + r_R^{d-1}) \times (c_1^{d-1} + \ldots + c_C^{d-1})}.$$

We claim that $\mathbf{B}$ is a submatrix of $\mathbf{A}_2 \otimes \ldots \otimes \mathbf{A}_d$. This is intuitive, but nevertheless we justify this rigorously before completing the proof. To this end, let us index each row of each $A_t$ by an index $i \in [R]$ together with an index $\alpha \in [i]$. Similarly, we can index each column by an index $k \in [C]$ together with $\beta \in [k]$. We can hence index rows of $\mathbf{A}_2 \otimes \ldots \otimes \mathbf{A}_d$ by $(i_2, \ldots, i_t, \alpha_2, \ldots, \alpha_d)$ and similarly the columns by $(k_2, \ldots, k_d, \beta_2, \ldots, \beta_d)$; so that:

$$(\mathbf{A}_2 \otimes \ldots \otimes \mathbf{A}_d)_{(i_2,\ldots,i_d,\alpha_2,\ldots,\alpha_d);(k_2,\ldots,k_d,\beta_2,\ldots,\beta_d)} = \prod_{t=2}^{d} (\mathbf{A}_{t,i_t,k_t})_{\alpha_t;\beta_t}.$$

On the other hand, we can index the rows of $\mathbf{B}$ by one index $i \in [R]$ and indices $\alpha_2, \ldots, \alpha_d \in [i]$, and similarly the columns by $k, \beta_2, \ldots, \beta_d$, so that:

$$B_{(i,\alpha_2,\ldots,\alpha_d);(k,\beta_2,\ldots,\beta_d)} = \prod_{t=2}^{d} (\mathbf{A}_{t,i,k})_{\alpha_t;\beta_t}.$$

It is now clear that $\mathbf{B}$ can be obtained by restricting $\mathbf{A}_2 \otimes \ldots \otimes \mathbf{A}_d$ to rows where $i_2 = \ldots = i_d$ and columns where $k_2 = \ldots = k_d$. This establishes our claim.

We now complete the proof as follows. By Lemma 3.13, our claim implies that

$$\|\mathbf{B}\|_\infty \leq \prod_{t=2}^{d} \|\mathbf{A}_t\|_\infty \leq 1.$$

The conclusion now follows by applying Theorem 3.19 to $\mathbf{A}_1$ and $\mathbf{B}$ for the choices of $R, C$, and scalars $\gamma_{i,k}$. This proves the claim. ☐

# 4 Black Hole Cloning Games

Hayden and Preskill [HP07] put forward the idea that the dynamics of a black hole are well-described by a random unitary time-evolution operator, e.g., via a *unitary design*. Does such a scrambling process limit the extent to which two observers (say, one of which falls inside of the black hole and another remains a distant observer) can simultaneously decode infalling entangled qubits near the boundary of the black hole? In this section, we seek to give a quantitative answer to this question. We formally state and discuss our model for this problem in terms of *black hole cloning games* in Section 4.1, and then turn to proving a bound on the value of black hole cloning games in Section 4.2.

### 4.1 Definition

Inspired by the monogamy game of Tomamichel, Fehr, Kaniewski and Wehner [TFKW13], we formalize the notion of a *black hole cloning game* as follows:

**Definition 4.1** (Black Hole Cloning Game)**.** *A black hole cloning game is specified by a tuple of the form* $\mathsf{G}_{BH} = (\mathcal{H}_{\mathsf{I}}, \mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_{\mathsf{H}}, \mathcal{H}_{\mathsf{R}}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$ *and consists of the following elements:*

- *A finite dimensional Hilbert space* $\mathcal{H}_{\mathsf{I}}$ *associated with the internal degrees of the freedom of the black hole; in particular, where* $\mathcal{H}_{\mathsf{I}}$ *contains the* $(n-k)$*-qubit initial state of the black hole;*
- *A pair of isomorphic finite dimensional Hilbert spaces* $\mathcal{H}_{\mathsf{B}}$ *and* $\mathcal{H}_{\mathsf{B}'}$ *which are associated with* $k$*-qubit* EPR *pairs that emerge near the boundary of the black hole;*
- *A finite dimensional Hilbert space* $\mathcal{H}_{\mathsf{H}}$ *associated with the final state of the black hole that comprises all of the qubits within its event horizon;*
- *A finite dimensional Hilbert space* $\mathcal{H}_{\mathsf{R}}$ *associated with the emitted Hawking radiation;*
- *A finite set of indices* $\Theta$ *over the set of all possible scrambling unitaries;*
- *A finite ensemble of scrambling unitaries* $\{U_\theta^\dagger\}_{\theta\in\Theta}$ *indexed by* $\Theta$ *which is associated with the internal time-evolution of the black hole within its event horizon;*
- *A completely positive and trace-preserving channel* $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$ *associated with the physical process that maps the internal registers* $\mathsf{IB}'$ *of the black hole into a final internal register* $\mathsf{H}$ *and a register* $\mathsf{R}$ *associated with the emitted Hawking radiation.*

**Definition 4.2** (Quantum Strategy)**.** *A quantum strategy* $\mathsf{S} = (\{\mathbf{H}_x^{U_\theta, U_\theta^\dagger}\}_{\theta\in\Theta, x\in\{0,1\}^k}, \{\mathbf{R}_x^{U_\theta, U_\theta^\dagger}\}_{\theta\in\Theta, x\in\{0,1\}^k})$ *for a black hole cloning game* $\mathsf{G}_{BH} = (\mathcal{H}_{\mathsf{I}}, \mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_{\mathsf{H}}, \mathcal{H}_{\mathsf{R}}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$ *consists of*

- *An ensemble of oracle-aided positive operator-valued measurements*
$$\left\{\mathbf{H}_x^{U_\theta, U_\theta^\dagger}\right\}_{\theta\in\Theta, x\in\{0,1\}^k}$$
*which are to be performed on Charlie's system* $\mathcal{H}_{\mathsf{H}}$*.*
- *An ensemble of oracle-aided positive operator-valued measurements*
$$\left\{\mathbf{R}_x^{U_\theta, U_\theta^\dagger}\right\}_{\theta\in\Theta, x\in\{0,1\}^k}$$
*which are to be performed on Bob's system* $\mathcal{H}_{\mathsf{R}}$*.*

Next, we define the value of a black hole cloning game, which can be thought of as the maximal winning probability over all admissible strategies.

**Game 1** (Black Hole Cloning Game)**.**
*A black hole cloning game* $\mathsf{G}_{BH} = (\mathcal{H}_{\mathsf{I}}, \mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_{\mathsf{H}}, \mathcal{H}_{\mathsf{R}}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$ *for a quantum strategy* $\mathsf{S} = (\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k}, \{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k})$ *is the following game between a trusted referee called Alice and two colluding and adversarial parties Bob and Charlie.*

1. *(**Setup phase**) A tripartite quantum state* $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{I}} \otimes \mathcal{H}_{\mathsf{B}'} \otimes \mathcal{H}_{\mathsf{B}})$ *is prepared, where*
$$\rho = \Big( |0^{n-k}\rangle\langle 0^{n-k}|_{\mathsf{I}} \otimes |\mathsf{EPR}^k\rangle\langle \mathsf{EPR}^k|_{\mathsf{B}'\mathsf{B}} \Big).$$
*Here,* $k$ *denotes the number of qubits in the registers* $\mathsf{B}$ *and* $\mathsf{B}'$*. Next, Alice receives register* $\mathsf{B}$*.*

2. *(**Time-evolution phase**) A random scrambling unitary* $U_\theta$ *is selected, where* $\theta \sim \Theta$ *is chosen uniformly at random, and the internal registers of the black hole evolve according to the unital quantum channel* $\big(U_\theta \cdot U_\theta^\dagger\big)_{\mathsf{IB}'\to\mathsf{IB}'}$ *which is applied to registers* $\mathsf{IB}'$ *of the state* $\rho$*.*
*Afterwards, the channel* $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$ *is applied to registers* $\mathsf{IB}'$ *and produces registers* $\mathsf{HR}$*.*

3. *(**Guessing phase**) Charlie and Bob receive the registers* $\mathsf{H}$ *and* $\mathsf{R}$*, respectively. They also receive oracles for both* $U_\theta$ *and* $U_\theta^\dagger$*, but may no longer communicate. They independently perform the measurements* $\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\}_{x\in\mathcal{X}}$ *and* $\{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\}_{x\in\mathcal{X}}$ *and output a* $k$*-bit string.*

4. *(**Outcome phase**) Alice measures* $\mathsf{B}$ *is measured in the computational basis, resulting in an outcome* $x \in \{0,1\}^k$*. Charlie and Bob win if they both guessed* $x$ *correctly.*

Figure 5: A black hole cloning game.

**Definition 4.3** (Value of a Black Hole Cloning Game)**.** *Consider a black hole cloning game of the form* $\mathsf{G}_{BH} = (\mathcal{H}_{\mathsf{I}}, \mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_{\mathsf{H}}, \mathcal{H}_{\mathsf{R}}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$*. Then, the winning probability of a quantum strategy* $\mathsf{S} = (\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k}, \{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k})$ *for* $\mathsf{G}_{BH}$ *is defined by the quantity*

$$\omega_{\mathsf{S}}(\mathsf{G}_{BH}) := \mathop{\mathbb{E}}_{\theta\sim\Theta}\Bigg\{ \sum_{x\in\{0,1\}^k} \mathrm{Tr}\Bigg[ \Big( \mathbf{H}_x^{U_\theta,U_\theta^\dagger} \otimes \mathbf{R}_x^{U_\theta,U_\theta^\dagger} \otimes |x\rangle\langle x|_{\mathsf{B}} \Big) \Big( \Phi_{\mathsf{IB}'\to\mathsf{HR}} \otimes \mathbb{I}_{\mathsf{B}} \Big)$$
$$\Big( \big(U_\theta \cdot U_\theta^\dagger\big)_{\mathsf{IB}'\to\mathsf{IB}'} \otimes \mathbb{I}_{\mathsf{B}} \Big) \Big( |0^{n-k}\rangle\langle 0^{n-k}|_{\mathsf{I}} \otimes |\mathsf{EPR}^k\rangle\langle \mathsf{EPR}^k|_{\mathsf{B}'\mathsf{B}} \Big) \Bigg] \Bigg\}.$$

*Moreover, we define the value of the monogamy game* $\mathsf{G}_{BH}$ *as the optimal winning probability*

$$\omega(\mathsf{G}_{BH}) := \sup_{\mathsf{S}=\left(\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\},\{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\}\right)} \omega_{\mathsf{S}}(\mathsf{G}_{BH}).$$

We refer the reader to Section 1.3 for a discussion of our modeling assumptions in formulating the black hole information paradox as a cloning game.

## 4.2 Bounds On the Value of a Black Hole Cloning Game

In this section, we bound the maximal value $\omega(\mathsf{G}_{\text{BH}}) = \sup_{\mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}_{\text{BH}})$ of a particular black hole cloning game $\mathsf{G}_{\text{BH}}$ for a unitary 3-design $\{U_\theta\}_{\theta\in\Theta}$ and where we restrict the set of oracle-aided strategies

$$\mathsf{S} = \left(\{\mathbf{H}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k}, \{\mathbf{R}_x^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\{0,1\}^k}\right)$$

such that Charlie and Bob only make a single oracle query (to either $U_\theta$ or $U_\theta^\dagger$), for any given $\theta \in \Theta$.

Let us first give a brief overview of the idea behind our proof. We refer the reader to our technical overview (Section 2) and the associated technical sections for details on each of these steps.

**Overview of the proof.** To obtain a bound, we consider a sequence of *hybrid games*:

- $\mathsf{G}_{\text{BH}}$: This is a black hole cloning game of the form

$$\mathsf{G}_{\text{BH}} = (\mathcal{H}_{\mathsf{I}}, \mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_{\mathsf{H}}, \mathcal{H}_{\mathsf{R}}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$$

  where $\nu = \{U_\theta\}_{\theta\in\Theta}$ is an $n$-qubit unitary 3-design and $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$ is an arbitrary CPTP map.

- $\mathsf{G}_{\text{MOE}}$: This is a (regular) monogamy of entanglement game (as in Section 6.1), where

$$\mathsf{G}_{\text{MOE}} = (\mathcal{H}_{\mathsf{A}}, \Theta, \{0,1\}^n, \{\mathbf{A}_y^\theta\}_{\theta\in\Theta,x\in\{0,1\}^n})$$

  where Alice performs a set of projective measurements $\{\mathbf{A}_y^\theta\}_{\theta\in\Theta,\, y\in\{0,1\}^n}$ acting on the Hilbert space $\mathcal{H}_{\mathsf{A}} = (\mathbb{C}^2)^{\otimes n}$, for some rank-1 projectors $\mathbf{A}_y^\theta = \bar{U}_\theta \left|y\right\rangle\!\left\langle y\right| \bar{U}_\theta^\dagger$.

- $\mathsf{G}_{1\mapsto 2}$: This is a $1 \mapsto 2$ oracular cloning game (as in Section 6.2), where

$$\mathsf{G}_{1\mapsto 2} = (1, \mathcal{H}_{\mathsf{A}}, \Theta, \{0,1\}^n, \{U_\theta\}_{\theta\in\Theta}).$$

- $\mathsf{G}_{\mathfrak{F},1}$: This is a different $1 \mapsto 2$ oracular cloning game (as in Section 6.2), where

$$\mathsf{G}_{\mathfrak{F},1} = (1, \mathcal{H}_{\mathsf{A}}, \{0,1\}^\lambda, \{0,1\}^n, \{\mathsf{U}_{f_\theta}\mathsf{H}^{\otimes n}\}_{\theta\in\{0,1\}^\lambda}).$$

  and $\mathfrak{F} = \{f_\theta : \{0,1\}^n \to \{0,1\}\}_{\theta\in\Theta}$ is a family of 6-wise uniform functions.

First, we show that the game $\mathsf{G}_{\text{BH}}$ emerges as a special case of $\mathsf{G}_{\text{MOE}}$ in which we post-select on the event that Alice measures $\{\mathbf{A}_y^\theta\}_{\theta\in\Theta,\, y\in\{0,1\}^n}$ and obtains the outcome $y = x||0^{n-k}$, for some $x \in \{0,1\}^k$. Informally, because this event occurs with probability $2^{-n+k}$, we can deduce that that:

$$\sup_{\hat{\mathsf{S}}}\, \omega_{\hat{\mathsf{S}}}(\mathsf{G}_{\text{MOE}}) \,\geq\, 2^{-n+k} \cdot \sup_{\mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}_{\text{BH}}),$$

where we maximize over the choice of strategies $\hat{\mathsf{S}}$ selected by Bob and Charlie which consist of a tripartite state $\rho$, where $\rho$ is the normalized *Choi state* of the quantum channel $\Phi$, and where Bob and Charlie perform oracle aided measurements with single-query access to $U_\theta$ and $U_\theta^\dagger$) on an enlarged Hilbert space. Therefore, in order to obtain an asymptotically optimal bound of the form $\omega(\mathsf{G}_{\text{BH}}) = O(2^{-k})$, it suffices to show that the related monogamy game $\mathsf{G}_{\text{MOE}}$ has a maximal value of $\sup_{\hat{\mathsf{S}}} \omega_{\hat{\mathsf{S}}}(\mathsf{G}_{\text{MOE}}) = O(2^{-n})$.

Second, we relate the game $\mathsf{G}_{\text{MOE}}$ to the $1 \mapsto 2$ cloning game $\mathsf{G}_{1\mapsto 2}$. Here, we use the general result in Theorem A.1 which allows us to relate this particular class of monogamy games to cloning games. As a result, we find that $\sup_{\hat{\mathsf{S}}} \omega_{\hat{\mathsf{S}}}(\mathsf{G}_{\text{MOE}}) = \sup_{\mathsf{S}'} \omega_{\mathsf{S}'}(\mathsf{G}_{1\mapsto 2})$, where $\mathsf{S}'$ ranges over the set of analogous oracular cloning strategies, but which involve $\Phi$ as a cloning channel.

Third, we use the insight from our worst-case to average-case reduction in Theorem 6.12 in order to argue that the $\mathsf{G}_{1\mapsto 2}$ is at least as hard as the cloning game $\mathsf{G}_{\mathfrak{F},1}$. In particular, we observe that the winning probabilities satisfy $\sup_{\hat{\mathsf{S}}'} \omega_{\hat{\mathsf{S}}'}(\mathsf{G}_{1\mapsto 2}) \leq \sup_{\mathsf{S}'} \omega_{\mathsf{S}'}(\mathsf{G}_{\mathfrak{F},1})$, where the set of strategies $\hat{\mathsf{S}}'$ remains the same.

Finally, we invoke Theorem 9.12 which gives an explicit bound on the game $\mathsf{G}_{\mathfrak{F},1}$. Specifically, we prove that $\sup_{\mathsf{S}'} \omega_{\mathsf{S}'}(\mathsf{G}_{\mathfrak{F},1}) \leq O(2^{-n})$, if $\mathfrak{F}$ is a family of 6-wise uniform functions.

Putting everything together, we then obtain the aforementioned asymptotically optimal bound of the form $\omega(\mathsf{G}_{\text{BH}}) = O(2^{-k})$ on the black hole cloning game $\mathsf{G}_{\text{BH}}$. Let us now state our main theorem.

**Theorem 4.4.** *Let $n, k \in \mathbb{N}$ be integers such that $n \geq k$ and let $\nu = \{U_\theta\}_{\theta\in\Theta}$ be a unitary 3-design on $n$-qubits. Then, for any quantum channel $\Phi_{\mathsf{IB}'\to\mathsf{HR}}$, the maximal single-query value of the black hole cloning game $\mathsf{G}_{BH} = (\mathcal{H}_\mathsf{I}, \mathcal{H}_\mathsf{B}, \mathcal{H}_{\mathsf{B}'}, \mathcal{H}_\mathsf{H}, \mathcal{H}_\mathsf{R}, \Theta, \{U_\theta\}_{\theta\in\Theta}, \Phi_{\mathsf{IB}'\to\mathsf{HR}})$ is at most*

$$\sup_{\mathsf{S}} \omega_{\mathsf{S}}(\mathsf{G}_{BH}) \;=\; O(2^{-k}),$$

*where the supremum ranges over all oracle-aided strategies*

$$\mathsf{S} = \left(\{\mathbf{H}_x^{U_\theta, U_\theta^\dagger}\}_{\theta\in\Theta, x\in\{0,1\}^k}, \{\mathbf{R}_x^{U_\theta, U_\theta^\dagger}\}_{\theta\in\Theta, x\in\{0,1\}^k}\right)$$

*that only make a single oracle query (to either $U_\theta$ or $U_\theta^\dagger$), for any given $\theta \in \Theta$.*

*Proof.* Let $\mathsf{S}$ be any single-query strategy. For convenience, we also assume there exists an auxiliary register $\mathsf{E}$ (say, the exterior of the black hole) which is initialized to $|0^{n-k}\rangle_\mathsf{E}$ and not touched by any of the processes in the black hole cloning game. This is without loss of generality, since it can always be absorbed into $\Phi$ by re-defining the quantum channel appropriately. Then, it follows that:

$$\begin{aligned}
\omega_{\mathsf{S}}(\mathsf{G}_{\text{BH}}) &= \mathop{\mathbb{E}}_{U\sim\nu}\Bigg\{\sum_{x\in\{0,1\}^k} \mathrm{Tr}\Bigg[\left(\mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \otimes |x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}}\right)\left(\Phi_{\mathsf{IB}'\to\mathsf{HR}} \otimes \mathbb{I}_{\mathsf{BE}}\right) \\
&\qquad \left((U\cdot U^\dagger)_{\mathsf{IB}'\to\mathsf{IB}'} \otimes \mathbb{I}_{\mathsf{BE}}\right)\left(|0^{n-k}\rangle\langle 0^{n-k}|_\mathsf{I} \otimes |\mathsf{EPR}^k\rangle\langle\mathsf{EPR}^k|_{\mathsf{B}'\mathsf{B}} \otimes |0^{n-k}\rangle\langle 0^{n-k}|_\mathsf{E}\right)\Bigg]\Bigg\} \\
&= 2^{n-k} \mathop{\mathbb{E}}_{U\sim\nu}\Bigg\{\sum_{x\in\{0,1\}^k} \mathrm{Tr}\Bigg[\left(\mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \otimes |x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}}\right)\left(\Phi_{\mathsf{IB}'\to\mathsf{HR}} \otimes \mathbb{I}_{\mathsf{BE}}\right) \\
&\qquad \left((U\cdot U^\dagger)_{\mathsf{IB}'\to\mathsf{IB}'} \otimes \mathbb{I}_{\mathsf{BE}}\right)\left(|\mathsf{EPR}^n\rangle\langle\mathsf{EPR}^n|_{\mathsf{IB}'\mathsf{BE}}\right)\Bigg]\Bigg\}.
\end{aligned}$$

The above step holds because in the second line the projector $|0^{n-k}\rangle\langle 0^{n-k}|_\mathsf{E}$ will act on one half of the EPR pair $|\mathsf{EPR}^{n-k}\rangle\langle\mathsf{EPR}^{n-k}|_{\mathsf{IE}}$, thus collapsing it to $|0^{n-k}\rangle\langle 0^{n-k}|_\mathsf{I} \otimes |0^{n-k}\rangle\langle 0^{n-k}|_\mathsf{E}$ and pulling out a factor of $2^{k-n}$.

We continue by using the ricochet property of EPR pairs (formally, Corollary 3.2) to pull $U, U^\dagger$ "out" of the cloning channel to obtain something that will look more like a monogamy game. First, consider the channel $\Psi_{\mathsf{IB}'\to\mathsf{HR}}$ defined as $\Phi \circ (U \cdot U^\dagger)$ (here, $\circ$ denotes composition). Applying Corollary 3.2 to the channel $\Psi$ yields the following:

$$2^{n-k} \mathop{\mathbb{E}}_{U\sim\nu}\Bigg\{\sum_{x\in\{0,1\}^k} \mathrm{Tr}\Bigg[\left(\mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \otimes |x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}}\right)\left(\Phi_{\mathsf{IB}'\to\mathsf{HR}} \otimes \mathbb{I}_{\mathsf{BE}}\right)$$

$$\left( \left( U \cdot U^\dagger \right)_{\mathsf{IB'} \to \mathsf{IB'}} \otimes \mathbb{I}_{\mathsf{BE}} \right) \left( |\mathsf{EPR}^n\rangle\langle\mathsf{EPR}^n|_{\mathsf{IB'BE}} \right) \Bigg] \Bigg\}$$

$$= 2^{-k} \mathop{\mathbb{E}}_{U \sim \nu} \left\{ \sum_{x \in \{0,1\}^k} \mathrm{Tr} \left[ \left( \mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \otimes |x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}} \right) J(\Psi) \right] \right\}$$

$$= 2^{-k} \mathop{\mathbb{E}}_{U \sim \nu} \left\{ \sum_{x \in \{0,1\}^k} \mathrm{Tr} \left[ \left( \mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \right) \Psi(|x0^{n-k}\rangle\langle x0^{n-k}|) \right] \right\}$$

$$= 2^{-k} \mathop{\mathbb{E}}_{U \sim \nu} \left\{ \sum_{x \in \{0,1\}^k} \mathrm{Tr} \left[ \left( \mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \right) \Phi(U |x0^{n-k}\rangle\langle x0^{n-k}| U^\dagger) \right] \right\}.$$

Next, we apply Corollary 3.2 once more, this time to the channel $\Phi$:

$$2^{-k} \mathop{\mathbb{E}}_{U \sim \nu} \left\{ \sum_{x \in \{0,1\}^k} \mathrm{Tr} \left[ \left( \mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \right) \Phi(U |x0^{n-k}\rangle\langle x0^{n-k}| U^\dagger) \right] \right\}$$

$$= 2^{-k} \mathop{\mathbb{E}}_{U \sim \nu} \left\{ \sum_{x \in \{0,1\}^k} \mathrm{Tr} \left[ \left( \mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \otimes \bar{U} |x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}} \bar{U}^\dagger \right) J(\Phi) \right] \right\}$$

$$= 2^{n-k} \mathop{\mathbb{E}}_{U \sim \nu} \left\{ \sum_{x \in \{0,1\}^k} \mathrm{Tr} \Bigg[ \left( \mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \otimes \bar{U} |x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}} \bar{U}^\dagger \right) \right.$$

$$\left( \Phi_{\mathsf{IB'} \to \mathsf{HR}} \otimes \mathbb{I}_{\mathsf{BE}} \right) \left( |\mathsf{EPR}^n\rangle\langle\mathsf{EPR}^n|_{\mathsf{IB'BE}} \right) \Bigg] \Bigg\}.$$

For the remainder of the proof, we will bound the final quantity in the expression above; specifically, by relating it to the value of a related monogamy of entanglement game. To this end, we now observe that

$$\mathop{\mathbb{E}}_{U \sim \nu} \left\{ \sum_{x \in \{0,1\}^k} \mathrm{Tr} \Bigg[ \left( \mathbf{H}_x^{U,U^\dagger} \otimes \mathbf{R}_x^{U,U^\dagger} \otimes \bar{U} |x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}} \bar{U}^\dagger \right) \right.$$

$$\left( \Phi_{\mathsf{IB'} \to \mathsf{HR}} \otimes \mathbb{I}_{\mathsf{BE}} \right) \left( |\mathsf{EPR}^n\rangle\langle\mathsf{EPR}^n|_{\mathsf{IB'BE}} \right) \Bigg] \Bigg\}$$

$$= \mathop{\mathbb{E}}_{U \sim \nu} \left\{ \sum_{x \in \{0,1\}^k} \mathrm{Tr} \Bigg[ \left( \tilde{\mathbf{H}}_{x||0^{n-k}}^{U,U^\dagger} \otimes \tilde{\mathbf{R}}_{x||0^{n-k}}^{U,U^\dagger} \otimes \bar{U} |x0^{n-k}\rangle\langle x0^{n-k}|_{\mathsf{BE}} \bar{U}^\dagger \right) \right.$$

$$\left( \Phi_{\mathsf{IB'} \to \mathsf{HR}} \otimes \mathbb{I}_{\mathsf{BE}} \right) \left( |\mathsf{EPR}^n\rangle\langle\mathsf{EPR}^n|_{\mathsf{IB'BE}} \right) \Bigg] \Bigg\}$$

$$\leq \sup_{\tilde{\mathsf{S}} = \left( \{\hat{\mathbf{H}}_y^{U,U^\dagger}\}, \{\hat{\mathbf{R}}_y^{U,U^\dagger}\} \right)} \mathop{\mathbb{E}}_{U \sim \nu} \left\{ \sum_{y \in \{0,1\}^n} \mathrm{Tr} \Bigg[ \left( \hat{\mathbf{H}}_y^{U,U^\dagger} \otimes \hat{\mathbf{R}}_y^{U,U^\dagger} \otimes \bar{U} |y\rangle\langle y|_{\mathsf{BE}} \bar{U}^\dagger \right) \right.$$

$$\left( \Phi_{\mathsf{IB'} \to \mathsf{HR}} \otimes \mathbb{I}_{\mathsf{BE}} \right) \left( |\mathsf{EPR}^n\rangle\langle\mathsf{EPR}^n|_{\mathsf{IB'BE}} \right) \Bigg] \Bigg\}. \tag{5}$$

We have now transitioned successfully to $\mathsf{G}_{\text{MOE}}$. Because the bound in Equation (5) applies to any single-query strategy $\mathsf{S}$, we can therefore complete the proof by bounding the black hole cloning game as follows:

$$
\begin{aligned}
\omega(\mathsf{G}_{\text{BH}}) &= \sup_{\mathsf{S}=\left(\{\mathbf{H}_x^{U,U^\dagger}\},\{\mathbf{R}_x^{U,U^\dagger}\}\right)} \omega_{\mathsf{S}}(\mathsf{G}_{\text{BH}}) \\
&\leq 2^{n-k} \sup_{\hat{\mathsf{S}}=\left(\mathcal{H}_{\mathsf{H}},\mathcal{H}_{\mathsf{R}},\rho_{\mathsf{AHR}},\{\hat{\mathbf{H}}_y^{U,U^\dagger}\},\{\hat{\mathbf{R}}_y^{U,U^\dagger}\}\right)} \omega_{\hat{\mathsf{S}}}(\mathsf{G}_{\text{MOE}}) && \text{(by Equation (5))} \\
&= 2^{n-k} \sup_{\mathsf{S}'=\left(\mathcal{H}_{\mathsf{H}}\otimes\mathcal{H}_{\mathsf{R}},\Phi_{\mathsf{IB}'\to\mathsf{HR}},\{\hat{\mathbf{H}}_y^{U,U^\dagger}\},\{\hat{\mathbf{R}}_y^{U,U^\dagger}\}\right)} \omega_{\mathsf{S}'}(\mathsf{G}_{1\mapsto 2}) && \text{(Theorem A.1)} \\
&\leq 2^{n-k} \sup_{\mathsf{S}'=\left(\mathcal{H}_{\mathsf{H}}\otimes\mathcal{H}_{\mathsf{R}},\Phi_{\mathsf{IB}'\to\mathsf{HR}},\{\hat{\mathbf{H}}_y^{U,U^\dagger}\},\{\hat{\mathbf{R}}_y^{U,U^\dagger}\}\right)} \omega_{\mathsf{S}'}(\mathsf{G}_{\mathfrak{F},1}) && \text{(Theorem 6.12)} \\
&\leq 2^{n-k}\cdot O(2^{-n}) \;=\; O(2^{-k}). && \text{(Theorem 9.12)}
\end{aligned}
$$

□

# 5 Succinct Unclonable Encryption

In this section, we formally define succinct unclonable encryption, loosely following the terminology introduced by Broadbent and Lord [BL20]. We will use $\theta \in \{0,1\}^\lambda$ (rather than $k$, which we are already using in Section 4 to denote the number of EPR pairs in a black hole monogamy game) to denote the secret key.

## 5.1 Definitions

**Definition 5.1** (Succinct Unclonable Encryption)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter and let $n := n(\lambda)$ be some polynomial in $\lambda$. A **succinct** unclonable encryption scheme* (sUE) *is a tuple* (KeyGen, Enc, Dec) *consisting of the following QPT algorithms:*

- $\mathsf{KeyGen}(1^\lambda, 1^n)$ : *takes as input $1^\lambda, 1^n$ and outputs $\theta \in \{0,1\}^\lambda$.*
- $\mathsf{Enc}(\theta \in \{0,1\}^\lambda, x \in \{0,1\}^n)$ : *on input $(\theta, x)$, it outputs a pure ciphertext state $|\psi_x^\theta\rangle$. **We require** $\mathsf{Enc}(\theta, x)$ **to deterministically output** $U_\theta |x\rangle$**, for some unitary** $U_{\theta,n} \in \mathcal{U}(2^n)$**. Thus the ciphertext state must also comprise $n$ qubits.***
- $\mathsf{Dec}(1^n, \theta \in \{0,1\}^\lambda, \rho)$*: on input $\theta$ and a quantum state $\rho$, it outputs $x' \in \{0,1\}^n$.*

*We require the following correctness property: for any $\lambda, n$, it holds that*

$$\Pr\left[\mathsf{Dec}\left(1^n, \theta, |\psi_x^\theta\rangle\langle\psi_x^\theta|\right) = x \;:\; \begin{smallmatrix}\theta\leftarrow\mathsf{KeyGen}(1^\lambda,1^n)\\ |\psi_x^\theta\rangle\leftarrow\mathsf{Enc}(\theta,x)\end{smallmatrix}\right] = 1.$$

*Succinctness is implicit in our requirement that the key length only depends on $\lambda$ rather than $n$.*

**Definition 5.2** ($t \mapsto t+1$ sUE security)**.** *Let* (KeyGen, Enc, Dec) *be a* sUE *scheme, and $t \in \mathbb{N}$ a positive integer. Consider the following experiment between a challenger and an adversary $(\Phi, \mathcal{P}_1, \ldots, \mathcal{P}_{t+1})$ consisting of a cloner $\Phi$ and $t+1$ players $\mathcal{P}_1, \ldots \mathcal{P}_{t+1}$ who are not allowed to communicate:*

1. *The challenger runs $\theta \leftarrow \mathsf{KeyGen}(1^\lambda, 1^n)$. Next, the challenger samples $x \leftarrow \{0,1\}^n$ and runs $\mathsf{Enc}(\theta, x)$ to obtain the ciphertext $|\psi_x^\theta\rangle$, and sends $t$ copies $|\psi_x^\theta\rangle^{\otimes t}$ of the state to the cloner $\Phi$.*

2. *The cloner $\Phi$ applies any quantum channel to $|\psi_x^\theta\rangle^{\otimes t}$ in registers $\mathsf{A}_1 \dots \mathsf{A}_t$ and then splits the resulting state into $t+1$ registers $\mathsf{B}_1, \dots, \mathsf{B}_{t+1}$. Finally, $\Phi$ sends $\mathsf{B}_i$ to player $\mathcal{P}_i$.*

3. *The players $\mathcal{P}_1, \dots, \mathcal{P}_{t+1}$ receive $\theta$ and output their guesses for $x$, and win if they all guess correctly.*

*We say that* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *satisfies statistical (respectively, computational) $t \mapsto t+1$ and $\epsilon(t, \lambda, n)$-*$\mathsf{sUE}$ *security if, for any computationally unbounded (respectively, computationally bounded) adversary $(\Phi, \mathcal{P}_1, \dots, \mathcal{P}_{t+1})$, where each $\mathcal{P}_i$ is an ensemble of positive-operator valued measurements $\{\mathbf{P}_{i,x}^\theta\}_{x,\theta}$,*

$$\mathop{\mathbb{E}}_{(x,\theta)\sim\mathsf{KeyGen}(1^n)} \mathrm{Tr}\left[\left(\mathbf{P}_{1,x}^\theta \otimes \dots \otimes \mathbf{P}_{t+1,x}^\theta\right) \Phi_{\mathsf{A}_1\dots\mathsf{A}_t \to \mathsf{B}_1 \dots \mathsf{B}_{t+1}} \left(|\psi_x^\theta\rangle\langle\psi_x^\theta|_{\mathsf{A}_1\dots\mathsf{A}_t}^{\otimes t}\right)\right] \leq O\left(\epsilon(t, \lambda, n)\right).$$

The $1 \mapsto 2$ $\mathsf{sUE}$ security experiment is visualized in Figure 6. In the following definition, we also define an *oracular* version of this security experiment.

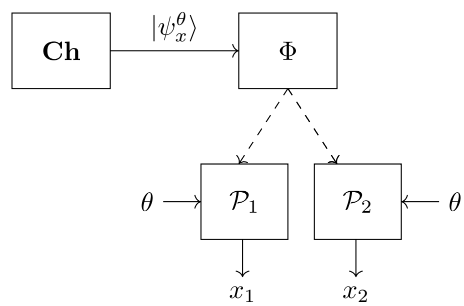


Figure 6: The $1 \mapsto 2$ $\mathsf{sUE}$ experiment. A cloner $\Phi$ splits a state $|\psi_x^\theta\rangle$ prepared by the challenger **Ch** into two parts, one is sent to $\mathcal{P}_1$ and one is sent to $\mathcal{P}_2$. Given $\theta$, $\mathcal{P}_1$ and $\mathcal{P}_2$ then output their guesses $x_1$ and $x_2$ for $x$.

**Definition 5.3** ($t \mapsto t+1$ oracular $\mathsf{sUE}$ security)**.** *We say that* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *satisfies statistical (respectively, computational) $t \mapsto t+1$ $\epsilon$-*$\mathsf{sUE}$ *oracular security under the same conditions as Definition 5.2, with the following modification: in the final phase, the players $\mathcal{P}_1, \dots \mathcal{P}_{t+1}$ do not receive $\theta$ directly. Instead, they receive query access to the unitary $U_{\theta,n}$ computing* $\mathsf{Enc}(\theta, \cdot)$ *as well as its inverse $U_{\theta,n}^\dagger$.*

*We say that* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *satisfies the weaker notion of $(\epsilon, q)$-*$\mathsf{sUE}$ *oracular security if each of the players may only make a total of $\leq q$ queries to $U_{\theta,n}$ and $U_{\theta,n}^\dagger$.*

**Remark 3.** *We make some remarks about these definitions:*

- *Our reason for focusing on* $\mathsf{UE}$ *schemes with* deterministic unitary *encryption is in order to be able to naturally instantiate the oracular security setting.*

- *Even if we only allow each player only* one *query, the oracular* $\mathsf{sUE}$ *security setting is still quite expressive. In particular, it would be sufficient for recovering $x$ from $|\psi_x^\theta\rangle$, and thus there is still a trivial strategy that succeeds with probability $2^{-n}$: the cloner forwards their copies to the first $t$ players, and nothing to player $t+1$. The first $t$ players can decrypt and output $x$, and player $t+1$ will simply guess randomly.*

**Remark 4.** *At first glance, in the $t = 1$ case this notion may already appear to have been achieved by the construction by Broadbent and Lord [BL20], which achieves a security bound of $\epsilon(\lambda, n) = \frac{9}{2^n} + \left(\cos^2 \frac{\pi}{8}\right)^\lambda$. At a high level, they compose a $\lambda$-bit BB84 cloning game as in [TFKW13] with a PRF-based one-time pad. However, their construction has two aspects which we would like to improve on:*

- *Their construction assumes the existence of post-quantum pseudorandom functions. We would like to instantiate a* sUE *scheme assuming the milder notions of pseudorandom quantum states or unitaries.*
- *Their encryption is randomized. The natural deterministic analogue of this would be the BB84-based encryption scheme without the PRF, which has security $\left(\cos^2 \frac{\pi}{8}\right)^n$ but is no longer succinct as this would use keys of length $n$.*

*We note that a common shortcoming of both the work by [BL20] and our work is the reliance on oracles for proving security.*

**Remark 5.** *We emphasize that our work is the first to consider $t \mapsto t+1$ cloning games for $t > 1$: not only is prior work limited to $1 \mapsto 2$ cloning games, all existing unclonable cryptography (based on BB84 states or coset states) becomes completely insecure if $t$ is allowed to grow polynomially [AMP24].*

*While we are only able to prove security for $t = o(\log n / \log\log n)$ (see Theorem 5.5), we reiterate that our construction could very well be secure for $t$ that is an arbitrary polynomial in $n$ (unlike previous constructions based on BB84 states [BL20] and coset states [CLLZ21]).*

### 5.2 Constructions

**Construction 1.** *Let $\mathfrak{U} = \{\mathfrak{U}_n\}_{n\in\mathbb{N}}$ be some ensemble of unitaries (we will specify what $\mathfrak{U}$ should be later). Recall that $\mathfrak{U}_n = \{U_{\theta,n}\}_{\theta\in\{0,1\}^\lambda}$. Our construction proceeds as follows:*

- $\mathsf{KeyGen}(1^\lambda, 1^n)$*: sample and output uniformly random $\theta \in \{0,1\}^\lambda$.*
- $\mathsf{Enc}(\theta, x)$*: output $U_{\theta,n} |x\rangle$.*
- $\mathsf{Dec}(1^n, \theta, \rho)$*. First apply the unitary channel $U_{\theta,n}^\dagger \cdot U_{\theta,n}$ to obtain the state $U_{\theta,n}^\dagger \rho U_{\theta,n}$. Now measure in the standard basis and output the result.*

Correctness is clear, so we now prove security in two different settings. First, we show $1 \mapsto 2$ security assuming the existence of pseudorandom unitaries, thus placing unclonable encryption in MicroCrypt:

**Theorem 5.4.** *If $\mathfrak{U}$ is a pseudorandom unitary (as defined in Definition 3.11), then the* sUE *scheme specified in Construction 1 satisfies computational $1 \mapsto 2$ $\epsilon$-*sUE *oracular security, where $\epsilon = \mathsf{negl}(\lambda) + \left(\cos^2 \frac{\pi}{8}\right)^n$.*

*Proof.* We consider a series of hybrid games:

- $\mathsf{Hyb}_0$: This is the $1 \mapsto 2$ oracular sUE security game, as defined in Definition 5.3.
- $\mathsf{Hyb}_1$: In step 1 of the sUE security game, the challenger also only has oracle access to $U_{\theta,n}, U_{\theta,n}^\dagger$. To generate the ciphertext state $|\psi_x^\theta\rangle$, they query the oracle for $U_{\theta,n}$ on input $|x\rangle$.
- $\mathsf{Hyb}_2$: Now, the unitary $U$ is sampled as follows: sample a string $b \leftarrow \{0,1\}^n$ uniformly at random, and output $\mathsf{H}^b$ (which applies a Hadamard at every position where the corresponding entry of $b$ is 1).

For $i = 0, 1, 2$, let $\omega(\mathsf{Hyb}_i)$ denote the probability of the players winning the security game in $\mathsf{Hyb}_i$. Then we observe the following:

- $\omega(\mathsf{Hyb}_0) = \omega(\mathsf{Hyb}_1)$, as these two are functionally equivalent.
- $|\omega(\mathsf{Hyb}_1) - \omega(\mathsf{Hyb}_2)| \leq \mathsf{negl}(\lambda)$ by the worst-case to average-case reduction in Section 6.3.
- $\omega(\mathsf{Hyb}_2) \leq \cos^2\left(\frac{\pi}{8}\right)^n$: this is exactly the BB84 security game. This security bound essentially follows from analysis by [TFKW13], and was formally shown in [BL20, Corollary 2].

The conclusion follows. $\square$

Secondly, we show assuming the existence of post-quantum one-way functions that Construction 1 can be instantiated to satisfy multi-copy security against query-bounded adversaries:

**Theorem 5.5.** *For any $\lambda, n$, let $n' = n - \omega(\log \lambda)$ and consider $t$ such that*

$$t \leq O\left(\frac{\log n'}{\log \log n'}\right) \Leftrightarrow \exp(\exp(O(t \log t))) \leq 2^{n'} = 2^n \cdot \mathsf{negl}(\lambda).$$

*Let $\left\{f_{\theta,n} : \theta \in \{0,1\}^\lambda\right\}$ be a post-quantum pseudorandom function family from $\{0,1\}^n \to \{0,1\}$. Then we define $\mathfrak{U}$ by*

$$U_{\theta,n} = \mathsf{U}_{f_{\theta,n}} \mathsf{H}^{\otimes n}.$$

*Then the $\mathsf{sUE}$ scheme specified in Construction 1 satisfies computational $t \mapsto t+1$ $(\epsilon, 1)$-$\mathsf{sUE}$ oracular security, where*

$$\epsilon = \exp(\exp(O(t \log t))) \cdot 2^{-n} + \mathsf{negl}(\lambda) = \mathsf{negl}(\lambda).$$

*Proof.* We first pass from a pseudorandom function $f_{\theta,n}$ to a truly random function $f$ at the expense of an additive $\mathsf{negl}(\lambda)$ security loss. A random function is $(4t+2)$-wise uniform, so we can then finish using Lemma 6.11 and Theorem 9.18. $\square$

# 6 Monogamy of Entanglement and Oracular Cloning Games

In this section, we formally define monogamy of entanglement games, as well as the closely related notion of (oracular) cloning games. In Section 6.3, we show a worst-case to average-case reduction for oracular cloning games.

Later, we will revisit existing techniques to analyze monogamy games in Section 7 and present new techniques to obtain improved bounds on cloning games in particular in Sections 8 and 9.

## 6.1 Monogamy of Entanglement Games

A monogamy of entanglement game [TFKW13] is an interactive game which is played by three players: a trusted referee called Alice, and two colluding and adversarial parties Bob and Charlie.

**Definition 6.1** (Monogamy of Entanglement Game). *A monogamy of entanglement (MOE) game is specified by a tuple $\mathsf{G} = (\mathcal{H}_\mathsf{A}, \Theta, \mathcal{X}, \{\mathbf{A}_x^\theta\}_{\theta \in \Theta, x \in \mathcal{X}})$ which consists of the following elements:*

- *A finite dimensional Hilbert space $\mathcal{H}_\mathsf{A}$ corresponding to a register $\mathsf{A}$ that Alice holds;*

**Game 2** (Monogamy of Entanglement Game)**.**
*A monogamy of entanglement game* $\mathsf{G} = (\mathcal{H}_{\mathsf{A}}, \Theta, \mathcal{X}, \{\mathbf{A}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}})$ *for a quantum strategy* $\mathsf{S} = (\mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{C}}, \rho_{\mathsf{ABC}}, \{\mathbf{B}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}}, \{\mathbf{C}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}})$ *is the following game between a trusted referee (called Alice) and two collaborating players (called Bob and Charlie):*

1. *(**Setup phase**) Bob and Charlie prepare a tripartite quantum state* $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$*. They send register* $\mathsf{A}$ *to Alice, and hold onto registers* $\mathsf{B}$ *and* $\mathsf{C}$*, respectively. Afterwards, they are no longer allowed to communicate for the remainder of the game.*

2. *(**Question phase**) Alice first samples a uniformly random question* $\theta \sim \Theta$*, and then applies the corresponding measurement* $\{\mathbf{A}_x^\theta\}_{x\in\mathcal{X}}$ *to her register* $\mathsf{A}$*. Afterwards, Alice announces the question* $\theta$ *to both Bob and Charlie.*

3. *(**Answer phase**) Bob and Charlie independently output a guess for Alice's outcome by applying the measurements* $\{\mathbf{B}_x^\theta\}_{x\in\mathcal{X}}$ *and* $\{\mathbf{C}_x^\theta\}_{x\in\mathcal{X}}$ *to their registers* $\mathsf{B}$ *and* $\mathsf{C}$*, respectively.*

4. *(**Outcome phase**) Bob and Charlie win if they both guess Alice's outcome correctly.*

Figure 7: A monogamy of entanglement game.

- *A finite set* $\Theta$ *corresponding to the set of possible questions;*
- *A finite set* $\mathcal{X}$ *corresponding to the set of all possible answers;*
- *A set of positive operator-valued measurements* $\left\{\mathbf{A}_x^\theta\right\}_{\theta\in\Theta, x\in\mathcal{X}}$ *to be performed on Alice's system.*

**Definition 6.2** (Quantum Strategy)**.** *A quantum strategy* $\mathsf{S} = (\mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{C}}, \rho_{\mathsf{ABC}}, \{\mathbf{B}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}}, \{\mathbf{C}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}})$ *for a monogamy of entanglement game* $\mathsf{G} = (\mathcal{H}_{\mathsf{A}}, \Theta, \mathcal{X}, \{\mathbf{A}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}})$ *consists of*

- *A finite dimensional Hilbert space* $\mathcal{H}_{\mathsf{B}}$ *corresponding to a register* $\mathsf{B}$ *that Bob holds;*
- *A finite dimensional Hilbert space* $\mathcal{H}_{\mathsf{C}}$ *corresponding to a register* $\mathsf{C}$ *that Charlie holds;*
- *A tripartite quantum state* $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$*;*
- *A set of positive operator-valued measurements* $\left\{\mathbf{B}_x^\theta\right\}_{\theta\in\Theta, x\in\mathcal{X}}$ *to be performed on Bob's system.*
- *A set of positive operator-valued measurements* $\left\{\mathbf{C}_x^\theta\right\}_{\theta\in\Theta, x\in\mathcal{X}}$ *to be performed on Charlie's system.*

**Definition 6.3** (Value of a Monogamy Game)**.** *Let* $\mathsf{G} = (\mathcal{H}_{\mathsf{A}}, \Theta, \mathcal{X}, \{\mathbf{A}_x^\theta\}_{\theta\in\Theta, x\in\Sigma})$ *be monogamy game. Then, the winning probability of a quantum strategy* $\mathsf{S} = (\mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{C}}, \rho_{\mathsf{ABC}}, \{\mathbf{B}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}}, \{\mathbf{C}_x^\theta\}_{\theta\in\Theta, x\in\mathcal{X}})$ *for the particular monogamy game* $\mathsf{G}$ *is defined by the quantity*

$$\omega_{\mathsf{S}}(\mathsf{G}) := \mathop{\mathbb{E}}_{\theta\sim\Theta} \sum_{x\in\mathcal{X}} \mathrm{Tr}\left[(\mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta)\rho_{\mathsf{ABC}}\right].$$

*Moreover, we define the value of the monogamy game* $\mathsf{G}$ *as the optimal winning probability*

$$\omega(\mathsf{G}) := \sup_{\mathsf{S}=(\mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{C}}, \rho_{\mathsf{ABC}}, \{\mathbf{B}_x^\theta\}, \{\mathbf{C}_x^\theta\})} \omega_{\mathsf{S}}(\mathsf{G}).$$

**Remark 6.** *As noted in [TFKW13], a standard purification argument and Neumark's dilation theorem show that we can assume without loss of generality that all POVMs are projective. We will assume this going forward.*

**Definition 6.4** (Parallel-Repeated Monogamy Game)**.** *Let $r \in \mathbb{N}$ be a parameter. For any monogamy game $\mathsf{G} = (\mathcal{H}_{\mathsf{A}}, \Theta, \mathcal{X}, \{\mathbf{A}_x^\theta\}_{\theta \in \Theta, x \in \mathcal{X}})$, we define the $r$-*fold parallel-repeated monogamy game* $\mathsf{G}^{\times r}$ as follows:*

- *The Hilbert space for Alice's register will be $\mathcal{H}_{\mathsf{A}}^{\otimes r}$.*
- *The set of questions will now be $\Theta^r$.*
- *The set of answers will be $\mathcal{X}^r$.*
- *For any $(x_1, \ldots, x_r) \in \mathcal{X}^r$ and $(\theta_1, \ldots, \theta_r) \in \Theta^r$, we define Alice's measurement to be*

$$\mathbf{A}_{(x_1,\ldots,x_r)}^{(\theta_1,\ldots,\theta_r)} = \bigotimes_{i=1}^{r} \mathbf{A}_{x_i}^{\theta_i}.$$

*Informally, Alice will carry out $r$ parallel measurements and Bob and Charlie succeed if they successfully guess the outcomes of all $r$ measurements.*

**Example** (BB84 Monogamy Game)**.** *As a simple example, the following monogamy game is known as the "BB84 monogamy game":*

- *The Hilbert space $\mathcal{H}_{\mathsf{A}}$ is $\mathbb{C}^2$.*
- *The sets of questions $\Theta$ and answers $\mathcal{X}$ are both $\{0, 1\}$.*
- *For any $x, \theta \in \{0, 1\}$, we have*

$$\mathbf{A}_x^\theta = \mathsf{H}^\theta \left|x\right\rangle\!\left\langle x\right| \mathsf{H}^\theta.$$

**Remark 7.** *We note that any MOE game admits a trivial strategy with success probabiliy $1/|\mathcal{X}|$. Bob and Charlie could set up the state $\rho_{\mathsf{ABC}}$ so that Bob and Alice are maximally entangled. This would enable Bob to always guess $x$ correctly, and now Charlie can guess randomly. (He cannot do better as in this case he must be completely decoupled from Alice and Bob.)*

## 6.2 Oracular Cloning Games

The monogamy of entanglement games which we encounter in physics and cryptography often deal with some restrictions on the types of strategies that can be employed.

Motivated by this, in this section, we introduce the notion of a $t \mapsto t+1$ *cloning game*. In the case when $t = 1$, this notion turns out to be a special case of a monogamy of entanglement game in Section 6.1, with the following additional restrictions:

- The tripartite state $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$ which is shared between Alice, Bob and Charlie is the result of applying a cloning channel $\Phi_{\mathsf{A}' \to \mathsf{BC}}$ to one half of an EPR pair, i.e.,

$$\rho_{\mathsf{ABC}} = (\mathbb{I}_{\mathsf{A}} \otimes \Phi_{\mathsf{A}' \to \mathsf{BC}})(\left|\mathsf{EPR}\right\rangle\!\left\langle \mathsf{EPR}\right|_{\mathsf{AA}'}).$$

  In other words, $\rho_{\mathsf{ABC}}$ is the normalized Choi state of some channel $\Phi_{\mathsf{A}' \to \mathsf{BC}}$.

- Alice's measurement $\{\mathbf{A}_x^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}$ on register $\mathsf{A}$ is a projective measurement of the form
$$\mathbf{A}_x^\theta = \bar{U}_\theta |x\rangle\langle x| \bar{U}_\theta^\dagger ,$$
for some family of unitary operators $\{U_\theta\}_{\theta\in\Theta}$ acting on $\mathcal{H}_\mathsf{A}$.
- (If we are in the oracular setting) Bob and Charlie's measurements can only depend on oracle queries to $U_\theta$ and $U_\theta^\dagger$, rather than directly on $\theta$.

We give a proof of this equivalence in Lemma A.1. We remark, however, that for $t \geq 2$, the notion of a $t \mapsto t+1$ cloning game includes $t+1$ colluding parties and thus starts to become incomparable to a monogamy of entanglement game in Section 6.1.

Let us now give a formal definition of a $t \mapsto t+1$ cloning game.

**Definition 6.5** ((Oracular) Cloning Game)**.** *Let $t \in \mathbb{N}$ be an integer. A $t \mapsto t+1$ (oracular) cloning game* ((O)CG) *is a tuple $\mathsf{G}_{t\mapsto t+1} = (t, \mathcal{H}_{\mathsf{A}^\mathsf{t}}, \Theta, \mathcal{X}, \{U_\theta\}_{\theta\in\Theta})$ which consists of the following elements:*

- *A finite dimensional Hilbert space $\mathcal{H}_{\mathsf{A}^\mathsf{t}}$ consisting of registers $\mathsf{A}^\mathsf{t} := \mathsf{A}_1 \cdots \mathsf{A}_\mathsf{t}$ given to the cloner;*
- *A finite set $\Theta$ corresponding to the set of possible questions;*
- *A finite set $\mathcal{X}$ corresponding to the set of all possible answers;*
- *A finite ensemble of unitary operators $\{U_\theta\}_{\theta\in\Theta}$ acting on the $\mathsf{A}$ systems.*

**Definition 6.6** (Quantum Strategy for Cloning Games)**.** *Let $t \in \mathbb{N}$ and let $\mathsf{G}_{t\mapsto t+1} = (t, \mathcal{H}_{\mathsf{A}^\mathsf{t}}, \Theta, \mathcal{X}, \{U_\theta\}_{\theta\in\Theta})$ be a cloning game. A quantum strategy $\mathsf{S} = (\mathcal{H}_{\mathsf{B}^{\mathsf{t}+1}}, \Phi_{\mathsf{A}^\mathsf{t}\to\mathsf{B}^{\mathsf{t}+1}}, \{\mathbf{P}_{1,x}^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}, \ldots, \{\mathbf{P}_{t+1,x}^\theta\}_{\theta\in\Theta,x\in\mathcal{X}})$ for the game $\mathsf{G}_{t\mapsto t+1}$ is characterized by the following elements:*

- *A finite dimensional Hilbert space $\mathcal{H}_{\mathsf{B}^{\mathsf{t}+1}}$ consisting of registers $\mathsf{B}^{\mathsf{t}+1} := \mathsf{B}_1 \cdots \mathsf{B}_{\mathsf{t}+1}$ which are held by the $k+1$ many players in the game;*
- *A completely positive and trace-preserving channel $\Phi_{\mathsf{A}^\mathsf{t}\to\mathsf{B}^{\mathsf{t}+1}}$ performed by the cloner;*
- *A sequence of measurements $\{\mathbf{P}_{1,x}^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}, \ldots, \{\mathbf{P}_{t+1,x}^\theta\}_{\theta\in\Theta,x\in\mathcal{X}}$ which are to be performed by the $t+1$ players on the registers $\mathsf{B}_1, \cdots, \mathsf{B}_{\mathsf{t}+1}$, respectively.*

**Definition 6.7** (Quantum Strategy for **Oracular** Cloning Games)**.** *A quantum strategy for an **oracular** cloning game is the same as a quantum strategy for a cloning game, with the following crucial restriction: the measurements by the $t+1$ players will now be* oracle-aided. *We denote these as*
$$\left\{\mathbf{P}_{1,x}^{U_\theta,U_\theta^\dagger}\right\}_{\theta\in\Theta,x\in\mathcal{X}}, \ldots, \left\{\mathbf{P}_{t+1,x}^{U_\theta,U_\theta^\dagger}\right\}_{\theta\in\Theta,x\in\mathcal{X}}.$$

*Informally, an oracular cloning game is one where the players are only given oracle access to $U_\theta, U_\theta^\dagger$, whereas in Definition 6.6 the players are given the question $\theta$ in the clear.*

**Definition 6.8** (**Restricted** Quantum Strategy for Oracular Cloning Games)**.** *Assume $\mathcal{X} = \{0,1\}^n$. Then a **restricted** quantum strategy for an oracular cloning game further restricts the players in the following way. For each $i \in [t+1]$, player $\mathcal{P}_i$ must output their guess $x \in \{0,1\}^n$ after applying some quantum algorithm that makes **at most one query** to either $U_\theta$ or $U_\theta^\dagger$.*

*We let $\mathcal{S}_{\mathrm{rest}}$ denote the collection of restricted quantum strategies $\mathsf{S}$ for the oracular cloning game $\mathsf{G}$.*

We first observe that we can impose some structure on the $t+1$ players' strategies without loss of generality; this will make our analysis easier:

**Lemma 6.9.** *Without loss of generality, a restricted quantum strategy for* $\mathsf{G}$ *may be taken to the have the following much more restricted structure: Each player* $\mathcal{P}_i$ *will hold a register* $\mathsf{B_i}$ *that splits into the following registers:*

- *A query register* $\mathsf{C_i}$ *of* $n$ *qubits;*
- *An ancilla register* $\mathsf{D_i}$ *of* $a$ *qubits (we allow* $a$ *to be arbitrary, but assume WLOG that it is the same for all the players); and*
- *A classical control bit* $b_i$ *from the cloning channel* $\Phi$*, which we store in a single-qubit register* $\mathsf{E_i}$ *for formality's sake.*

*The player* $\mathcal{P}_i$ *will then proceed as follows:*

1. *They first make* ***exactly one query*** *to either* $U_\theta$ *or* $U_\theta^\dagger$*, which will be applied to the* $\mathsf{C_i}$ *register. Which of these unitaries they query will be controlled by* $b_i$*.*
2. *They can then apply a unitary* $Q_i$ *of their choice to their entire system* $\mathsf{B_i}$*. (We assume without loss of generality that the same unitary* $Q_i$ *is applied regardless of the value of the control bit* $b_i$*; the cloner could simply include a copy of the control bit in register* $\mathsf{D}_i$ *as well, which* $Q_i$ *acts on.)*
3. *They now measure the* $n$ *qubits in the* $\mathsf{C_i}$ *register to obtain a string* $x \in \{0,1\}^n$*.*
4. *They output* $x$*.*

*Formally: for every* $i \in [t+1]$ *and* $x \in \{0,1\}^n$*, player* $\mathcal{P}_i$*'s projector has the form:*

$$\begin{aligned}\mathbf{P}_{i,x}^{U_\theta, U_\theta^\dagger} &= \Big[(U_\theta^\dagger \otimes \mathbb{I}_{\mathsf{D}_i}) Q_i^\dagger (|x\rangle\langle x| \otimes \mathbb{I}_{D_i}) Q_i (U_\theta \otimes \mathbb{I}_{\mathsf{D_i}})\Big] \otimes |0\rangle\langle 0|_{\mathsf{E_i}} \\ &+ \Big[(U_\theta \otimes \mathbb{I}_{\mathsf{D}_i}) Q_i^\dagger (|x\rangle\langle x| \otimes \mathbb{I}_{D_i}) Q_i (U_\theta^\dagger \otimes \mathbb{I}_{\mathsf{D_i}})\Big] \otimes |1\rangle\langle 1|_{\mathsf{E_i}}\,.\end{aligned}$$

*Proof.* Any preprocessing that player $\mathcal{P}_i$ might carry out before their query can be absorbed into the cloning channel $\Phi$, including the decision about which of $U_\theta, U_\theta^\dagger$ to query, which we represent in the control bit $b_i$. (If the player does not want to query either, we can just treat $\mathsf{C_i}$ as dummy qubits and make a query there.)

The conclusion now follows from the Stinespring and Neumark dilation theorems [NC16]. □

**Remark 8.** *Some comments are in order about Definition 6.8:*

- *The cloner* $\Phi$ *remains entirely unrestricted; they can apply an arbitrary quantum channel to* $(U_\theta\,|x\rangle)^{\otimes t}$*.*
- *While quite restrictive, this model is still sufficiently expressive to admit a trivial strategy (akin to that in Remark 7) that succeeds with probability* $2^{-n} = 1/\mathcal{X}$ *(even when* $a = 0$*). The cloner* $\Phi$ *will simply forward their copies of* $U_\theta\,|x\rangle$ *to players* $\mathcal{P}_1, \ldots, \mathcal{P}_t$*. For* $i \leq t$*, player* $\mathcal{P}_i$ *will make a query to* $U_\theta^\dagger$ *to obtain the state* $|x\rangle$*, which they can then measure and output. Player* $\mathcal{P}_{t+1}$ *will guess randomly.*

**Definition 6.10** (Value of a (Oracular) Cloning Game)**.** *Let $t \in \mathbb{N}$. The winning probability of a quantum strategy $\mathsf{S} = (\mathcal{H}_{\mathsf{B}^{t+1}}, \Phi_{\mathsf{A}^t \to \mathsf{B}^{t+1}}, \{\mathbf{P}_{1,x}^{U_\theta, U_\theta^\dagger}\}_{\theta\in\Theta, x\in\mathcal{X}}, \ldots, \{\mathbf{P}_{t+1,x}^{U_\theta, U_\theta^\dagger}\}_{\theta\in\Theta, x\in\mathcal{X}})$ for a particular $t \mapsto t+1$ oracular cloning game $\mathsf{G}_{t\mapsto t+1} = (t, \mathcal{H}_{\mathsf{A}^t}, \Theta, \mathcal{X}, \{U_\theta\}_{\theta\in\Theta})$ is defined by the quantity*

$$\omega_{\mathsf{S}}(\mathsf{G}_{t\mapsto t+1}) := \mathop{\mathbb{E}}_{\theta\sim\Theta} \mathop{\mathbb{E}}_{x\sim\mathcal{X}} \operatorname{Tr}\left[\left(\mathbf{P}_{1,x}^{U_\theta, U_\theta^\dagger} \otimes \ldots \otimes \mathbf{P}_{t+1,x}^{U_\theta, U_\theta^\dagger}\right) \Phi_{\mathsf{A}^t \to \mathsf{B}^{t+1}} \left((U_\theta \left|x\right\rangle\!\left\langle x\right| U_\theta^\dagger)_{\mathsf{A}^t}^{\otimes t}\right)\right].$$

*Moreover, we define the value of the oracular cloning game $\mathsf{G}$ as the optimal winning probability*

$$\omega(\mathsf{G}_{t\mapsto t+1}) := \sup_{\mathsf{S}=(\mathcal{H}_{\mathsf{B}^{t+1}}, \Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}, \{\mathbf{P}_{1,x}\}, \ldots, \{\mathbf{P}_{t+1,x}\})} \omega_{\mathsf{S}}(\mathsf{G}_{t\mapsto t+1}).$$

*We analogously define the value of a cloning game $\mathsf{G}$, using the measurements $\left\{\mathbf{P}_{i,x}^\theta\right\}$ instead.*

We also make the straightforward observation that cloning games are closely related to $\mathsf{sUE}$ schemes:

**Lemma 6.11.** *Consider a cloning game with t players, $\mathcal{X} = \{0,1\}^n$, and $\Theta = \{0,1\}^\lambda$. Then all of the following hold:*

- *If the corresponding cloning game has value $\leq \epsilon$ with computationally unbounded (respectively, computationally bounded) $(\Phi, \mathcal{P}_1, \ldots, \mathcal{P}_{t+1})$, then there exists a $\mathsf{sUE}$ scheme satisfying statistical (respectively, computational) $t \mapsto t+1$ $\epsilon$-$\mathsf{sUE}$ security.*
- *If the corresponding* oracular *cloning game has value $\leq \epsilon$ with computationally unbounded (respectively, computationally bounded) $(\Phi, \mathcal{P}_1, \ldots, \mathcal{P}_{t+1})$, then there exists a $\mathsf{sUE}$ scheme satisfying (statistical, respectively computational) $t \mapsto t+1$ $(\epsilon, \infty)$-$\mathsf{sUE}$* oracular *security.*
- *If in the corresponding oracular cloning game, any computationally unbounded (respectively, computationally bounded)* restricted *strategy $(\Phi, \mathcal{P}_1, \ldots, \mathcal{P}_{t+1})$ has value $\leq \epsilon$, then there exists a $\mathsf{sUE}$ scheme satisfying (statistical, respectively computational) $t \mapsto t+1$ $(\epsilon, 1)$-$\mathsf{sUE}$ oracular security.*

*Proof.* In all cases, the construction proceeds as follows: we will take $\mathsf{Enc}(\theta, x) = U_\theta \left|x\right\rangle$, and $\mathsf{Dec}$ will apply $U_\theta^\dagger$ and measure in the standard basis. The conclusions are now straightforward to verify. ☐

## 6.3 Worst-Case to Average-Case Reduction

In this section, we show that $t \mapsto t+1$ oracular cloning games admit a worst-case to average-case reduction: even the hardest games which are specified by some worst-case unitary $U_w$ can be won by a strategy for the average-case version of the game that involves a Haar-like unitary $U_a$ from an appropriate unitary design, or alternatively from a pseudorandom unitary ensemble.

**Theorem 6.12** (Worst-Case to Average-Case Reduction)**.** *Let $n, t \in \mathbb{N}$ and let $\nu = \{U_a\}_{a\in\Theta}$ be an ensemble of $n$-qubit unitaries to be specified later. Suppose there exists a quantum strategy*

$$\mathsf{S}^{\mathsf{avg}} = (\mathcal{H}_{\mathsf{B}^{t+1}}, \Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}, \{\mathbf{P}_{1,x}^{U_a, U_a^\dagger}\}_{a\in\Theta,\, x\in\{0,1\}^n}, \ldots, \{\mathbf{P}_{t+1,x}^{U_a, U_a^\dagger}\}_{a\in\Theta,\, x\in\{0,1\}^n})$$

*for the average-case $t \mapsto t+1$ oracular cloning game $\mathsf{G}_{t\mapsto t+1}^{\mathsf{avg}} = (t, \mathcal{H}_{\mathsf{A}^t}, \Theta, \{0,1\}^n, \{U_a\}_{a\in\Theta})$, where the $t+1$ players make no more than a total of q many oracle queries to either $U_a$ or $U_a^\dagger$ combined, and*

$$\omega_{\mathsf{S}^{\mathsf{avg}}}(\mathsf{G}_{t\mapsto t+1}^{\mathsf{avg}}) = \epsilon.$$

**Game 3** (Oracular Cloning Game)**.**
*A $t \mapsto t+1$ oracular cloning game $\mathsf{G}_{t\mapsto t+1} = (k, \mathcal{H}_{\mathsf{A}^t}, \Theta, \mathcal{X}, \{U_\theta\}_{\theta\in\Theta})$ for a quantum strategy of the form $\mathsf{S} = (\mathcal{H}_{\mathsf{B}^{t+1}}, \Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}, \{\mathbf{P}_{1,x}^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\mathcal{X}}, \dots, \{\mathbf{P}_{t+1,x}^{U_\theta,U_\theta^\dagger}\}_{\theta\in\Theta,x\in\mathcal{X}})$ is the following game between a trusted challenger, a cloner and $t+1$ many players:*

1. *(**Setup phase**) The challenger samples a random $x \sim \mathcal{X}$ and a random $\theta \sim \Theta$, and sends the state $(U_\theta |x\rangle)^{\otimes t}$ consisting of registers $\mathsf{A}^t := \mathsf{A}_1 \cdots \mathsf{A}_t$ to the cloner.*

   *The cloner applies the channel $\Phi_{\mathsf{A}^t\to\mathsf{B}^{t+1}}$ to $(U_\theta |x\rangle)^{\otimes t}$ and sends the resulting registers $\mathsf{B}^{t+1} = \mathsf{B}_1 \cdots \mathsf{B}_{t+1}$ to the $t+1$ many players, respectively. Afterwards, the players may no longer communicate with each other for the remainder of the game.*
2. *(**Question phase**) Each of the players receives oracles for both $U_\theta$ and $U_\theta^\dagger$.*
3. *(**Answer phase**) The players independently output a guess for the element $x$ by applying the measurements $\{\mathbf{P}_{1,x}^{U_\theta,U_\theta^\dagger}\}_{x\in\mathcal{X}}, \dots, \{\mathbf{P}_{t+1,x}^{U_\theta,U_\theta^\dagger}\}_{x\in\mathcal{X}}$ to their registers, respectively.*
4. *(**Outcome phase**) The players win if they all guess $x$ correctly.*

Figure 8: A $t \mapsto t+1$ oracular cloning game. A regular cloning game is defined analogously, except the measurements are now $\mathbf{P}_{i,x}^{\theta}$ and free to depend on $\theta$ in any way. Informally, in a standard cloning game $\theta$ is revealed to the $t+1$ players in the clear, while in the oracular cloning game the players are only given oracle access to $U_\theta$ and $U_\theta^\dagger$.

*Then, there exists a quantum strategy (in which the $t+1$ many players make the same number of queries)*

$$\mathsf{S}^{\mathsf{wst}} = (\mathcal{H}_{\tilde{\mathsf{B}}^{t+1}}, \tilde{\Phi}_{\mathsf{A}^t\to\tilde{\mathsf{B}}^{t+1}}, \{\tilde{\mathbf{P}}_{1,x}^{V_w,V_w^\dagger}\}_{x\in\{0,1\}^n}, \dots, \{\tilde{\mathbf{P}}_{t+1,x}^{V_w,V_w^\dagger}\}_{x\in\{0,1\}^n})$$

*for any $t \mapsto t+1$ oracular cloning game $\mathsf{G}_{t\mapsto t+1}^{\mathsf{wst}} = (t, \mathcal{H}_{\mathsf{A}^t}, \Theta', \{0,1\}^n, \{V_w\}_{w\in\Theta'})$ in the worst-case (i.e., for any adversarially chosen ensemble of $n$-qubit unitaries $\{V_w\}_{w\in\Theta'}$), such that:*

- *If $\nu$ is an exact unitary $r$-design, for $r = t+q$ and $q \in \mathbb{N}$: we will have*

$$\omega_{\mathsf{S}^{\mathsf{wst}}}(\mathsf{G}_{t\mapsto t+1}^{\mathsf{wst}}) = \epsilon.$$

- *If $\nu$ is a pseudorandom unitary family with security parameter $\lambda$, and the adversaries $(\Phi, \mathcal{P}_1, \dots, \mathcal{P}_{t+1})$ are computationally bounded: we will have*

$$\omega_{\mathsf{S}^{\mathsf{wst}}}(\mathsf{G}_{t\mapsto t+1}^{\mathsf{wst}}) \geq \epsilon - \mathsf{negl}(\lambda).$$

*Proof.* Let $\mathsf{G}_{t\mapsto t+1}^{\mathsf{wst}} = (t, \mathcal{H}_{\mathsf{A}^t}, \Theta', \{0,1\}^n, \{V_w\}_{w\in\Theta'})$ be a worst-case $t \mapsto t+1$ oracular cloning game for ensemble of unitaries $\{V_w\}$. Consider the quantum strategy $\mathsf{S}^{\mathsf{wst}}$ for the game $\mathsf{G}_{t\mapsto t+1}^{\mathsf{wst}}$ which internally uses $\mathsf{S}^{\mathsf{avg}}$ and proceeds as follows:

- (Cloning Channel:) on input $(V_w |x\rangle)^{\otimes t}$ in register $\mathsf{A}^t$, the channel $\tilde{\Phi}_{\mathsf{A}^t\to\tilde{\mathsf{B}}^{t+1}}$ proceeds as follows:
  1. Sample a uniformly random unitary $U_a \sim \nu$ from the unitary ensemble $\nu$.

2. Apply $U_a$ to each copy of $V_w |x\rangle$, resulting in a state $(U_a V_w |x\rangle)^{\otimes t}$ in register $\mathsf{A}^t$.
3. Run $\Phi_{\mathsf{A^t \to B^{t+1}}}$ on $(U_a V_w |x\rangle)^{\otimes t}$, and let $\mathsf{B^{t+1}} = \mathsf{B_1} \cdots \mathsf{B_{t+1}}$ denote the resulting registers.
4. Output $\tilde{\mathsf{B}}^{\mathsf{t+1}} := \tilde{\mathsf{B}}_1 \cdots \tilde{\mathsf{B}}_{\mathsf{t+1}}$, where $\tilde{\mathsf{B}}_\mathsf{i}$ consists of $\mathsf{B_i}$ together with $\mathsf{B}'_\mathsf{i} = |a\rangle\langle a|$, for $i \in [t+1]$.

- ($i$-th Player:) On input $\tilde{\mathsf{B}}_\mathsf{i}$, the measurement $\{\tilde{\mathbf{P}}_{i,x}^{V_w, V_w^\dagger}\}_{x \in \{0,1\}^n}$ proceeds as follows:
  1. Parse $\tilde{\mathsf{B}}_\mathsf{i}$ as $\mathsf{B_i B'_i}$. Measure $\mathsf{B}'_\mathsf{i}$ to obtain the string $a$.
  2. Run the oracle-aided measurement $\{\mathbf{P}_{i,x}^{U,U^\dagger}\}_{x \in \{0,1\}^n}$ with respect to $U := U_a V_w$ in such a way that, whenever one of the $q$-many oracle queries to $U$ or $U^\dagger$ is submitted:
     - If the query is to $U$: the query is first submitted to the available oracle $V_w$, then the unitary $U_a$ is applied to the resulting outcome.
     - If the query is to $U^\dagger$: the unitary $U_a^\dagger$ is applied, and the resulting outcome submitted to the available oracle $V_w^\dagger$.

Let us now analyze the success probability $\omega_{\mathsf{S^{wst}}}(\mathsf{G}^{\mathsf{wst}}_{t \mapsto t+1})$ of the strategy $\mathsf{S^{wst}}$. We first address the case where $\nu$ is an exact unitary $r$-design. Recall from Theorem 3.10 that any exact (non-adaptive) unitary $r$-design is also an exact adaptive $r$-design. Therefore, using that $\nu$ is an adaptive unitary $r$-design, for $r = t+q$, as well as the right-invariance of the Haar measure over the unitary group $\mathrm{U}(2^n)$, we get:

$$
\begin{aligned}
&\underset{\substack{x \sim \{0,1\}^n \\ w \sim \Theta'}}{\mathbb{E}} \operatorname{Tr}\left[\left(\tilde{\mathbf{P}}_{1,x}^{V_w,V_w^\dagger} \otimes \ldots \otimes \tilde{\mathbf{P}}_{t+1,x}^{V_w,V_w^\dagger}\right) \tilde{\Phi}_{\mathsf{A^t \to \tilde{B}^{t+1}}}\left((V_w |x\rangle\langle x| V_w^\dagger)^{\otimes t}_{\mathsf{A^t}}\right)\right] \\
&= \underset{U_a \sim \nu}{\mathbb{E}} \underset{\substack{x \sim \{0,1\}^n \\ w \sim \Theta'}}{\mathbb{E}} \operatorname{Tr}\left[\left(\mathbf{P}_{1,x}^{U_aV_w,(U_aV_w)^\dagger} \otimes \ldots \otimes \mathbf{P}_{t+1,x}^{U_aV_w,(U_aV_w)^\dagger}\right) \Phi_{\mathsf{A^t \to B^{t+1}}}\left((U_aV_w |x\rangle\langle x| (U_aV_w)^\dagger)^{\otimes t}_{\mathsf{A^t}}\right)\right] \\
&= \underset{W \sim \mathrm{U}(2^n)}{\mathbb{E}} \underset{\substack{x \sim \{0,1\}^n \\ w \sim \Theta'}}{\mathbb{E}} \operatorname{Tr}\left[\left(\mathbf{P}_{1,x}^{WU_w,(WU_w)^\dagger} \otimes \ldots \otimes \mathbf{P}_{t+1,x}^{WU_w,(WU_w)^\dagger}\right) \Phi_{\mathsf{A^t \to B^{t+1}}}\left((WV_w |x\rangle\langle x| (WV_w)^\dagger)^{\otimes t}_{\mathsf{A^t}}\right)\right] \\
&= \underset{U \sim \mathrm{U}(2^n)}{\mathbb{E}} \underset{x \sim \{0,1\}^n}{\mathbb{E}} \operatorname{Tr}\left[\left(\mathbf{P}_{1,x}^{U,U^\dagger} \otimes \ldots \otimes \mathbf{P}_{t+1,x}^{U,U^\dagger}\right) \Phi_{\mathsf{A^t \to B^{t+1}}}\left((U |x\rangle\langle x| U^\dagger)^{\otimes t}_{\mathsf{A^t}}\right)\right] \\
&= \underset{U_a \sim \nu}{\mathbb{E}} \underset{x \sim \{0,1\}^n}{\mathbb{E}} \operatorname{Tr}\left[\left(\mathbf{P}_{1,x}^{U_a,U_a^\dagger} \otimes \ldots \otimes \mathbf{P}_{t+1,x}^{U_a,U_a^\dagger}\right) \Phi_{\mathsf{A^t \to B^{t+1}}}\left((U_a |x\rangle\langle x| U_a^\dagger)^{\otimes t}_{\mathsf{A^t}}\right)\right].
\end{aligned}
$$

Therefore, we get that $\omega_{\mathsf{S^{wst}}}(\mathsf{G}^{\mathsf{wst}}_{t \mapsto t+1}) = \omega_{\mathsf{S^{avg}}}(\mathsf{G}^{\mathsf{avg}}_{t \mapsto t+1}) = \epsilon$, which proves the claim. In the case that $\nu$ is a PRU family and the adversary is computationally bounded, we can apply essentially the same calculation, but we will incur a potential additive loss of $\mathsf{negl}(\lambda)$ when passing from $U_a$ to the Haar measure. (Note that we can appeal to PRU security because the strategy $\mathsf{S^{wst}}$ can be simulated using only oracle access to $U_a, U_a^\dagger$.) □

# 7 Analyzing Monogamy Games Using Existing Techniques

In this section, we revisit the existing techniques laid out by [TFKW13] for upper bounding the value of monogamy games (and hence cloning games in particular). In Section 7.2, we use their framework to construct monogamy games with $\mathcal{X} = \{0,1\}^n$ with an improved upper bound of essentially $O(2^{-n/2})$. Finally, in Section 7.3, we show formally that these techniques cannot be used to establish significantly better bounds for a monogamy game.

### 7.1 Worst-Case Overlap Analysis

The main pre-existing tool for bounding the value of a monogamy game is a spectral bound due to [TFKW13]. We summarize their technique and main result here. For a particular strategy $\mathsf{S}$, they define the projector

$$\Pi^{\theta}_{\mathsf{ABC}} := \sum_{x \in \mathcal{X}} \mathbf{A}^{\theta}_{x} \otimes \mathbf{B}^{\theta}_{x} \otimes \mathbf{C}^{\theta}_{x}.$$

Then note that we have:

$$\begin{aligned} \omega_{\mathsf{S}}(\mathsf{G}) &= \mathop{\mathbb{E}}_{\theta \sim \Theta} \left[ \mathrm{Tr} \left[ \Pi^{\theta}_{\mathsf{ABC}} \rho_{\mathsf{ABC}} \right] \right] \\ &\leq \left\| \mathop{\mathbb{E}}_{\theta \sim \Theta} \left[ \Pi^{\theta}_{\mathsf{ABC}} \right] \right\|_{\infty}, \end{aligned}$$

since $\rho_{\mathsf{ABC}}$ has trace 1 (by Lemma 3.18). To bound this, they show the following result:

**Theorem 7.1** (Essentially [TFKW13], Theorem 4)**.** *We have*

$$\left\| \mathop{\mathbb{E}}_{\theta \sim \Theta} \left[ \Pi^{\theta}_{\mathsf{ABC}} \right] \right\|_{\infty} \leq \frac{1}{|\Theta|} + \frac{|\Theta| - 1}{|\Theta|} \cdot \max_{\substack{\theta, \theta' \in \Theta \\ \theta \neq \theta'}} \max_{x, x' \in \mathcal{X}} \left\| \sqrt{\mathbf{A}^{\theta}_{x}} \sqrt{\mathbf{A}^{\theta'}_{x'}} \right\|_{\infty}.$$

Using this theorem, they are able to show that the BB84 monogamy game has value $\frac{1}{2} + \frac{1}{2\sqrt{2}}$. Moreover, they show that the $n$-fold parallel repetition of the BB84 monogamy game has value $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$. The remainder of this section is organized as follows:

1. In Section 7.2, we will provide a different monogamy game with $\mathcal{X} = \{0,1\}^n$ that has value $\leq 2^{-n/2+o(n)}$, assuming the existence of sub-exponentially *classically* secure PRFs.

2. In Section 7.3, we will show that this is essentially the best bound that we could hope to show using Theorem 7.1.

   In order to bypass this limitation and obtain monogamy bounds of $O(2^{-n})$, we will later restrict attention to *oracular cloning games* (defined in Section 6.2) and analyze these with a completely different technique based on subtypes in Section 9.

### 7.2 Monogamy Games with Salted Phase States

In this section, we restrict attention to monogamy games such that $\mathbf{A}^{\theta}_{x} = \mathsf{V}_{\theta} |x\rangle\langle x| \mathsf{V}^{\dagger}_{\theta}$ for some $|\mathcal{X}| \times |\mathcal{X}|$ unitary $\mathsf{V}_{\theta}$. In this case, we have the following observation:

**Lemma 7.2.** *For any $x, x' \in \mathcal{X}$ and $\theta, \theta' \in \Theta$, we have*

$$\left\| \sqrt{\mathbf{A}^{\theta}_{x}} \sqrt{\mathbf{A}^{\theta'}_{x'}} \right\|_{\infty} = \left\| \mathbf{A}^{\theta}_{x} \mathbf{A}^{\theta'}_{x'} \right\|_{\infty} = \left| \langle x | \mathsf{V}^{\dagger}_{\theta} \mathsf{V}_{\theta'} | x' \rangle \right|.$$

*Proof.* Note firstly that the $\ell_\infty$ norm of any rank 1 Hermitian PSD matrix is equal to its trace (see Lemma 3.12). Bearing this in mind, we have:

$$\left\| \mathbf{A}^{\theta}_{x} \mathbf{A}^{\theta'}_{x'} \right\|^2_{\infty} = \left\| \mathbf{A}^{\theta}_{x} \mathbf{A}^{\theta'}_{x'} \mathbf{A}^{\theta' \dagger}_{x'} \mathbf{A}^{\theta \dagger}_{x} \right\|_{\infty}$$

$$
\begin{aligned}
&= \left\| \mathsf{V}_\theta \left|x\right\rangle\!\left\langle x\right| \mathsf{V}_\theta^\dagger \cdot \mathsf{V}_{\theta'} \left|x'\right\rangle\!\left\langle x'\right| \mathsf{V}_{\theta'}^\dagger \cdot \mathsf{V}_{\theta'} \left|x'\right\rangle\!\left\langle x'\right| \mathsf{V}_{\theta'}^\dagger \cdot \mathsf{V}_\theta \left|x\right\rangle\!\left\langle x\right| \mathsf{V}_\theta^\dagger \right\|_\infty \\
&= \mathrm{Tr}\left[ \mathsf{V}_\theta \left|x\right\rangle\!\left\langle x\right| \mathsf{V}_\theta^\dagger \cdot \mathsf{V}_{\theta'} \left|x'\right\rangle\!\left\langle x'\right| \mathsf{V}_{\theta'}^\dagger \cdot \mathsf{V}_{\theta'} \left|x'\right\rangle\!\left\langle x'\right| \mathsf{V}_{\theta'}^\dagger \cdot \mathsf{V}_\theta \left|x\right\rangle\!\left\langle x\right| \mathsf{V}_\theta^\dagger \right] \\
&= \left| \langle x | \mathsf{V}_\theta^\dagger \mathsf{V}_{\theta'} | x' \rangle \right|^2 \cdot \mathrm{Tr}\left[ \mathsf{V}_\theta \left|x\right\rangle \left\langle x'\right| \mathsf{V}_{\theta'}^\dagger \cdot \mathsf{V}_{\theta'} \left|x'\right\rangle \left\langle x\right| \mathsf{V}_\theta^\dagger \right] \\
&= \left| \langle x | \mathsf{V}_\theta^\dagger \mathsf{V}_{\theta'} | x' \rangle \right|^2,
\end{aligned}
$$

which implies the conclusion. □

We now describe our PRF-based construction. We stress that we only require the PRF to be secure against classical adversaries, and we do not assume that Bob and Charlie are computationally bounded. The reasons for this will become clear later, and are summarized in Remark 11.

**Construction 2.** *Let $\mathfrak{F} = \left\{F_k : \{0,1\}^{m+n} \to \{0,1\}\right\}_{k \in \{0,1\}^\lambda}$ be a PRF family. (Here, $m := m(\lambda)$ and $n := n(\lambda)$ should be thought of as small polynomials in the security parameter $\lambda$ e.g. $\lambda^{0.1}$.) For any $k \in \{0,1\}^\lambda$ and $\theta \in \{0,1\}^m$, define the "salted" function $f_{k,s} : \{0,1\}^n \to \{0,1\}$ by $f_{k,\theta}(x) = F_k(\theta||x)$.*

*Then for any $k \in \{0,1\}^\lambda$, we define the monogamy game $\mathsf{G}_{\mathfrak{F},k}$ as follows:*

- *The Hilbert space $\mathcal{H}_{\mathsf{A}}$ is $\mathcal{C}^{2^n}$.*
- *The set of questions $\Theta$ is $\{0,1\}^m$.*
- *The set of answers $\mathcal{X}$ is $\{0,1\}^n$.*
- *For any $\theta \in \{0,1\}^m$ and $x \in \{0,1\}^n$, we define the following:*

$$
\begin{aligned}
\mathsf{V}_\theta &= \mathsf{U}_{f_{k,\theta}} \mathsf{H}^{\otimes n}, \text{ and} \\
\mathbf{A}_x^\theta &= \mathsf{V}_\theta \left|x\right\rangle\!\left\langle x\right| \mathsf{V}_\theta^\dagger,
\end{aligned}
$$

  *where $\mathsf{U}_{f_{k,\theta}}$ is the phase unitary defined in Section 8.3.*

**Remark 9.** *Our use of PRF security is already quite unconventional; the PRF key $k$ should be thought of here as a public parameter that is known to all parties (including Bob and Charlie) before the monogamy game commences.*

**Remark 10.** *At first glance, this "salting" construction appears unnatural; it would be much more natural to consider a PRF family $\{F_k : \{0,1\}^n \to \{0,1\}\}_{k \in \{0,1\}^\lambda}$, set $\Theta = \{0,1\}^\lambda$, and set $\mathsf{V}_\theta = \mathsf{U}_{F_\theta} \mathsf{H}^{\otimes n}$ (where $\theta \in \{0,1\}^\lambda$ is the PRF key).*

*The problem with this is that we will be analyzing this construction using Theorem 7.1, which considers the* worst-case *overlap across different $\theta, \theta' \in \{0,1\}^\lambda$, while PRF security would only give us a "with high probability" guarantee with respect to $\theta$, which is insufficient for us.*

*To remedy this, we salt the PRF so that the "with high probability" guarantee is absorbed into the setup phase of the construction. In other words, this can be thought of as a "randomized monogamy game" (where the new randomization occurs during the setup phase). We can now obtain the desired worst-case overlap bounds using simple concentration bounds, as we will see next.*

Our starting point to analyze Construction 2 is the following lemma:

**Lemma 7.3** (Essentially [O'D21], Exercise 5.8)**.** *Let $F : \{0,1\}^{m+n} \to \{-1,1\}$ be a random function. For any $s \in \{0,1\}^m$, define $f_s : \{0,1\}^n \to \{-1,1\}$ by $f_s(u) = F(s,u)$. Then with probability $1 - O(2^{-n})$ over the randomness of $F$, we have*

$$\max_{r \neq s} \max_{w \in \{0,1\}^n} \left| \mathbb{E}_u \left[ (-1)^{\langle w,u \rangle} f_r(u) f_s(u) \right] \right| \leq 2 \cdot 2^{-n/2} \sqrt{m+n}.$$

*Proof.* We will first argue for any fixed $r, s, w$ then take a union bound at the end. If we let $G(u) = f_r(u) f_s(u) = F(r,u)F(s,u)$, it is clear that $G$ is itself a random function from $\{0,1\}^n \to \{-1,1\}$ (noting that we get independence because $r \neq s$). Hence we just want to bound

$$\left| \mathbb{E}_u \left[ (-1)^{\langle w,u \rangle} G(u) \right] \right|.$$

For each $u$, $(-1)^{\langle w,u \rangle} G(u)$ is an independent and uniformly random sample from $\{-1,1\}$, so this quantity can be bounded with a straightforward Chernoff bound. Indeed, Hoeffding's inequality tells us that:

$$\begin{aligned} \Pr\left[ \left| \mathbb{E}_u \left[ (-1)^{\langle w,u \rangle} G(u) \right] \right| > 2 \cdot 2^{-n/2} \sqrt{m+n} \right] &\leq 2 \exp\left( \frac{-4 \cdot 2^n \cdot (m+n)}{2^{n+1}} \right) \\ &= 2 \exp(-2(m+n)). \end{aligned}$$

Taking a union bound over $2^m$ choices of $r$, $2^m$ choices of $s$, and $2^n$ choices of $w$ implies that:

$$\begin{aligned} \Pr\left[ \max_{r \neq s} \max_{w \in \{0,1\}^n} \left| \mathbb{E}_u \left[ (-1)^{\langle w,u \rangle} G(u) \right] \right| > 2 \cdot 2^{-n/2} \sqrt{m+n} \right] &\leq 2^{2m+n} \cdot 2 \exp(-2(m+n)) \\ &= O(2^{-n}). \end{aligned}$$

□

**Corollary 7.4.** *Assume that the PRF family $\mathfrak{F}$ is $(2^{m+n}, \epsilon(\lambda))$-classically secure i.e. a classical distinguisher that runs in time $\mathsf{poly}(2^{m+n})$ can only distinguish a function sampled from $\mathfrak{F}$ from a truly random function with advantage $\leq \epsilon(\lambda)$. Then with probability $1 - O(2^{-n}) - \epsilon(\lambda)$ over the randomness of $k \leftarrow \{0,1\}^\lambda$, we have*

$$\max_{r \neq s} \max_{w \in \{0,1\}^n} \left| \mathbb{E}_u \left[ (-1)^{\langle w,u \rangle + f_{k,r}(u) + f_{k,s}(u)} \right] \right| \leq 2 \cdot 2^{-n/2} \sqrt{m+n}.$$

*Proof.* Consider the following PRF distinguisher given oracle access to some function $F$: it simply iterates over all $r, s, w, u$ and computes

$$\max_{r \neq s} \max_{w \in \{0,1\}^n} \left| \mathbb{E}_u \left[ (-1)^{\langle w,u \rangle + F(r,u) + F(s,u)} \right] \right|,$$

and outputs 1 if the result is $> 2 \cdot 2^{-n/2} \sqrt{m+n}$. This distinguisher runs in time $\mathsf{poly}(2^{m+n})$. By Lemma 7.3, it outputs 1 given a random function with probability at most $O(2^{-n})$ (noting that the outputs of $F$ are in $\{0,1\}$, so the outputs of $(-1)^{F(\cdot)}$ are in $\{-1,1\}$ as in Lemma 7.3). Hence by PRF security, it outputs 1 given a function sampled from $\mathfrak{F}$ with probability at most $O(2^{-n}) + \epsilon(\lambda)$. The conclusion follows. □

Note that a PRF with this security guarantee can be instantiated assuming sub-exponentially secure PRFs since $\lambda$ is a large polynomial in $m+n$. With this corollary, we can prove an upper bound on the value of our monogamy game:

**Theorem 7.5.** *Assume (as in Corollary 7.4) that the PRF family $\mathfrak{F}$ is $(2^{m+n}, \epsilon(\lambda))$-classically secure i.e. a classical distinguisher that runs in time $\mathsf{poly}(2^{m+n})$ can only distinguish a function sampled from $\mathfrak{F}$ from a truly random function with advantage $\leq \epsilon(\lambda)$. Then with probability $1-O(2^{-n})-\epsilon(\lambda)$ over the randomness of $k \leftarrow \{0,1\}^\lambda$, we have:*

$$\omega(\mathsf{G}_{\mathfrak{F},k}) \leq O(2^{-m} + 2^{-n/2}\sqrt{m+n}).$$

*Proof.* By Theorem 7.1 and the analysis preceding it, we have:

$$\omega(\mathsf{G}_{\mathfrak{F},k}) \leq 2^{-m} + (1-2^{-m}) \cdot \max_{\substack{\theta,\theta' \in \{0,1\}^m \\ \theta \neq \theta'}} \max_{x,x' \in \{0,1\}^n} \left\| \sqrt{\mathbf{A}_x^\theta} \sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_\infty .$$

Hence it suffices to show that

$$\max_{\substack{\theta,\theta' \in \{0,1\}^m \\ \theta \neq \theta'}} \max_{x,x' \in \{0,1\}^n} \left\| \sqrt{\mathbf{A}_x^\theta} \sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_\infty \leq O(2^{-n/2}\sqrt{m+n}).$$

Indeed, we have:

$$\begin{aligned}
\left\| \sqrt{\mathbf{A}_x^\theta} \sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_\infty &= \left| \langle x | \mathsf{V}_\theta^\dagger \mathsf{V}_{\theta'} | x' \rangle \right| \text{ (Lemma 7.2)} \\
&= \left| \langle x | \mathsf{H}^{\otimes n} \mathsf{U}_{f_{k,\theta}} \mathsf{U}_{f_{k,\theta'}} \mathsf{H}^{\otimes n} | x' \rangle \right| \\
&= \frac{1}{2^n} \left| \sum_{y,y' \in \{0,1\}^n} (-1)^{\langle x,y \rangle + \langle x',y' \rangle} \langle y | \mathsf{U}_{f_{k,\theta}} \mathsf{U}_{f_{k,\theta'}} | y' \rangle \right| \\
&= \frac{1}{2^n} \left| \sum_{y,y' \in \{0,1\}^n} (-1)^{\langle x,y \rangle + \langle x',y' \rangle + f_{k,\theta}(y) + f_{k,\theta'}(y')} \langle y | y' \rangle \right| \\
&= \left| \mathop{\mathbb{E}}_{y \leftarrow \{0,1\}^n} \left[ (-1)^{\langle x+x',y \rangle + f_{k,\theta}(y) + f_{k,\theta'}(y)} \right] \right| \\
\Rightarrow \max_{\substack{\theta,\theta' \in \{0,1\}^m \\ \theta \neq \theta'}} \max_{x,x' \in \{0,1\}^n} \left\| \sqrt{\mathbf{A}_x^\theta} \sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_\infty &= \max_{\substack{\theta,\theta' \in \{0,1\}^m \\ \theta \neq \theta'}} \max_{x,x' \in \{0,1\}^n} \left| \mathop{\mathbb{E}}_{y \leftarrow \{0,1\}^n} \left[ (-1)^{\langle x+x',y \rangle + f_{k,\theta}(y) + f_{k,\theta'}(y)} \right] \right| \\
&\leq O(2^{-n/2}\sqrt{m+n}),
\end{aligned}$$

with probability at least $1 - O(2^{-n}) - \epsilon(\lambda)$ over the randomness of $k$ by Corollary 7.4 (noting that we can consolidate the $\max$ over $x$ and $x'$ into a single $\max$ over $w := x + x'$). □

**Remark 11.** *Our use of PRF security is only to prove the concentration bound in Corollary 7.4, and hence we only need security against classical adversaries. Once we have this bound, we are applying Theorem 7.5 which holds against computationally unbounded Bob and Charlie. Therefore, although our construction is based on a cryptographic assumption, it is secure even against computationally unbounded adversaries Bob and Charlie.*

### 7.3 Limitations of [TFKW13]

Here, we show that the framework laid out by [TFKW13] of using Theorem 7.1 to bound monogamy games cannot prove a better bound than $1/\sqrt{|\mathcal{X}|}$ (see the statement of Theorem 7.1).

**Lemma 7.6.** *If $|\Theta| \geq 2$, then we have*

$$\max_{\substack{\theta,\theta'\in\Theta \\ \theta\neq\theta'}} \max_{x,x'\in\mathcal{X}} \left\| \sqrt{\mathbf{A}_x^{\theta}}\sqrt{\mathbf{A}_{x'}^{\theta'}} \right\|_\infty = \max_{\substack{\theta,\theta'\in\Theta \\ \theta\neq\theta'}} \max_{x,x'\in\mathcal{X}} \left\| \mathbf{A}_x^{\theta}\mathbf{A}_{x'}^{\theta'} \right\|_\infty \geq \frac{1}{\sqrt{|\mathcal{X}|}}.$$

*Proof.* The first equality follows since the measurements are projective, so $\sqrt{A_x^\theta} = A_x^\theta$. Now for any distinct $\theta, \theta' \in \Theta$, we will show that

$$\max_{x,x'\in\mathcal{X}} \left\| \mathbf{A}_x^{\theta}\mathbf{A}_{x'}^{\theta'} \right\|_\infty \geq \frac{1}{\sqrt{|\mathcal{X}|}}.$$

Indeed, fix any $x' \in \mathcal{X}$ such that $\mathbf{A}_{x'}^{\theta'}$ is nonzero (such $x'$ exists since $\sum_{x'} \mathbf{A}_{x'}^{\theta'} = \mathbb{I}$) and consider an arbitrary state $|\psi\rangle$ in the image of $\mathbf{A}_{x'}^{\theta'}$. Then we have:

$$\begin{aligned} |\psi\rangle &= \sum_{x\in\mathcal{X}} \mathbf{A}_x^{\theta} |\psi\rangle \\ &= \sum_{x\in\mathcal{X}} \mathbf{A}_x^{\theta}\mathbf{A}_{x'}^{\theta'} |\psi\rangle \\ \Rightarrow 1 &= \left\| \sum_{x\in\mathcal{X}} \mathbf{A}_x^{\theta}\mathbf{A}_{x'}^{\theta'} |\psi\rangle \right\|_2^2. \end{aligned}$$

For each $x \in \mathcal{X}$, let $|\psi_x\rangle = \mathbf{A}_x^{\theta}\mathbf{A}_{x'}^{\theta'} |\psi\rangle$, where $|\psi_x\rangle$ may not be normalized. Note for any $x \neq y$ that $\langle\psi_x|\psi_y\rangle = \langle\psi|\mathbf{A}_{x'}^{\theta'}\mathbf{A}_x^{\theta}\mathbf{A}_y^{\theta}\mathbf{A}_{x'}^{\theta'}|\psi\rangle = 0$, since $\mathbf{A}_x^{\theta}\mathbf{A}_y^{\theta} = 0$. Hence the $|\psi_x\rangle$'s are mutually orthogonal, implying that:

$$\begin{aligned} 1 &= \left\| \sum_{x\in\mathcal{X}} |\psi_x\rangle \right\|_2^2 \\ &= \sum_{x\in\mathcal{X}} \| |\psi_x\rangle \|_2^2. \end{aligned}$$

Hence there exists $x \in \mathcal{X}$ such that $\| |\psi_x\rangle \|_2^2 \geq 1/|\mathcal{X}| \Rightarrow \| |\psi_x\rangle \|_2 \geq 1/\sqrt{|\mathcal{X}|}$. For this $x$, we have:

$$\begin{aligned} \frac{1}{\sqrt{|\mathcal{X}|}} &\leq \| |\psi_x\rangle \|_2 \\ &= \left\| \mathbf{A}_x^{\theta}\mathbf{A}_{x'}^{\theta'} |\psi\rangle \right\|_2 \\ &\leq \left\| \mathbf{A}_x^{\theta}\mathbf{A}_{x'}^{\theta'} \right\|_\infty, \end{aligned}$$

as desired. ∎

# 8 Types and Subtypes

In order to improve on the limitations of the [TFKW13] framework for bounding the value of monogamy games, we essentially restrict attention to oracular cloning games, and restrict each player to only make one query. This allows us to analyze this game using the language of *binary phase twirls* (defined and analyzed in Section 8.3). To effectively capture the effect of binary phase twirls on an operator, we revisit the formalism of *types* introduced by [AGQY22] in Section 8.1 and extend this to *subtypes* in Section 8.2. Later, in Section 9, we will leverage these tools to analyze our construction using binary phase states and prove monogamy bounds of $O_t(2^{-n})$.

## 8.1 Binary Types

Let $N, M \in \mathbb{N}$ and $r \in \mathbb{N}$. For a vector $\mathbf{x} = (x_1, \ldots, x_r) \in [N]^r$ and an ancilla input $y \in [M]$, we denote by $\mathsf{Type}(\mathbf{x}, y) \in [0 : r]^N$ the so-called *type vector* in which the $i$-th entry corresponds to the number of occurrences of $i \in [N]$ in $\mathbf{x}$. Note that the ancillary information $y$ is just representing some auxiliary input that we do not consider when evaluating Type. We denote by $\mathsf{BinType}(\mathbf{x}, y) \in \{0,1\}^N$ the *binary type vector* in which the $i$-th entry corresponds to the parity of the number of occurrences of $i \in [N]$ in $\mathbf{x}$. In other words, we let

$$\mathsf{BinType}(\mathbf{x}, y) = \mathsf{Type}(\mathbf{x}, y) \pmod 2.$$

We note that our definition of Type and BinType is a natural extension of the standard definition in the literature (which does not consider auxiliary input); in particular, when $M = 0$ and $y$ is the empty string, our definitions and the standard definitions coincide.

**BinType decomposition.** When working with the vector space $\mathcal{H} = (\mathbb{C}^N)^{\otimes r} \otimes \mathbb{C}^M$, we use the following BinType decomposition into orthogonal subspaces $V_{\boldsymbol{\lambda}}$ indexed by binary types $\boldsymbol{\lambda} \in \{0,1\}^N$ such that

$$(\mathbb{C}^N)^{\otimes r} \otimes \mathbb{C}^M \cong \bigoplus_{\boldsymbol{\lambda}} V_{\boldsymbol{\lambda}}\,,$$

where each subspace $V_{\boldsymbol{\lambda}} \subseteq \mathcal{H}$ corresponds to vectors with a particular binary type $\boldsymbol{\lambda}$, i.e.,

$$V_{\boldsymbol{\lambda}} = \mathrm{span}_{\mathbb{C}}\{|v_1, \ldots, v_r, w\rangle \,:\, \mathsf{BinType}((v_1, \ldots, v_r), w) = \boldsymbol{\lambda}\}.$$

## 8.2 Subtypes

### 8.2.1 Definitions and Combinatorial Properties

While BinType is very simple to define, it comes with an "entangled"[9] combinatorial structure that is difficult to work with. As a simple example, consider the case where $r = 3, M = 0$, and the binary type $\boldsymbol{\lambda}$ is $(1, 0, 0, \ldots, 0)$. There are a few different ways for a vector in $[N]^3$ to attain this BinType: the vector could be of the form $(0, x, x)$ for any $x \in [N]$ or any permutation of this, and moreover these collections of vectors will overlap on $(0, 0, 0)$.

Instead of working with the BinType directly, it is more natural and convenient to address each of these different collections of vectors separately. Within each of these collections, there is now a very clean combinatorial structure that we will be able to exploit.

To formalize the above intuition, we will work with the notion of *subtypes*. As in Section 8.1, let $N, M, r$ be positive integer parameters:

[9] This comment is qualitative, and does not relate in any way to quantum entanglement.

**Definition 8.1.** *A* subtype *of a given type $\boldsymbol{\lambda} = (c_1, \ldots, c_N) \in \{0,1\}^N$ is a string $\boldsymbol{\mu}$ of length $r$. Each entry of $\boldsymbol{\mu}$ is either an integer $i \in [N]$ such that $\boldsymbol{\lambda}_i = 1$, or a* variable symbol *$x_i$ for some index $i$. We have the following constraints:*

- *For each $i \in [N]$ such that $\boldsymbol{\lambda}_i = 1$, $i$ should appear an odd number of times in $\boldsymbol{\mu}$.*
- *For any $i$ such that $x_i$ appears at least once in $\boldsymbol{\mu}$, the first $i$ distinct variable symbols that appear in $\boldsymbol{\mu}$ are $x_1, x_2, \ldots, x_i$ in that order.*
- *Each variable symbol $x_i$ appears an even number of times in $\boldsymbol{\mu}$.*

**Definition 8.2.** *For a vector $(\mathbf{x}, y) \in [N]^r \times [M]$, define its* query restriction *to be $\mathbf{x} \in [N]^r$. (Informally, the query restriction discards any auxiliary information.)*

**Definition 8.3.** *We say a vector $(\mathbf{x}, y) \in [N]^r \times [M]$ matches a subtype $\boldsymbol{\mu}$ if there exist assignments of values in $[N]$ to the variable symbols in $\boldsymbol{\mu}$ to yield the query restriction $\mathbf{x}$ of $(\mathbf{x}, y)$.*

*For a subtype $\boldsymbol{\mu}$, we define $S_{\boldsymbol{\mu}} \subseteq [N]^r \times [M]$ to be the set of vectors $(\mathbf{x}, y)$ that match $\boldsymbol{\mu}$, and let $\Pi_{\boldsymbol{\mu}}$ denote the projection onto standard basis vectors in $S_{\boldsymbol{\mu}}$.*

**Definition 8.4.** *For any subtype $\boldsymbol{\mu}$ with variable symbols $x_1, \ldots, x_k$ and some specific values $y_1, \ldots, y_k \in [N]$ and $z \in [M]$, define $\mathsf{Reconstruct}(\boldsymbol{\mu}, (y_1, \ldots, y_k), z)$ to be the vector in $[N]^r \times [M]$ obtained by taking $\boldsymbol{\mu}$ and replacing the variable symbol $x_i$ with $y_i$ for each $i$, then finally appending $z$.*

At this point, we make some straightforward observations. Firstly, membership of a vector $(\mathbf{x}, y)$ in a subtype $\boldsymbol{\mu}$ or a type $\boldsymbol{\lambda}$ depends only on its query restriction. Also, any vector $(\mathbf{x}, y)$ that matches a subtype $\boldsymbol{\mu}$ of a type $\boldsymbol{\lambda}$ must have type $\boldsymbol{\lambda}$. This is due to the parity constraints in Definition 8.1. Conversely, for any vector $(\mathbf{x}, y)$ of type $\boldsymbol{\lambda}$, there is at least one subtype $\boldsymbol{\mu}$ of $\boldsymbol{\lambda}$ that $(\mathbf{x}, y)$ matches: we can take $\mathbf{x}$, leave entries $i$ such that $\boldsymbol{\lambda}_i = 1$ as they are, and replace all other distinct values by variable symbols $x_1, x_2, \ldots$. This suggests that an inclusion-exclusion counting argument will allow us to relate the collection of vectors in a given $\mathsf{BinType}$ to the collection of vectors in a given subtype. To do this, we need the following straightforward observation:

**Lemma 8.5.** *For any two subtypes $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2$ of the same type $\boldsymbol{\lambda}$, either there exists a subtype $\boldsymbol{\mu}_3$ of $\boldsymbol{\lambda}$ such that $S_{\boldsymbol{\mu}_1} \cap S_{\boldsymbol{\mu}_2} = S_{\boldsymbol{\mu}_3}$, or $S_{\boldsymbol{\mu}_1} \cap S_{\boldsymbol{\mu}_2} = \emptyset$.*

*Proof.* Firstly, if there is an entry where $\boldsymbol{\mu}_1$ and $\boldsymbol{\mu}_2$ have differing values $i \in [N]$, then the intersection is clearly empty. From now on, we assume this is not the case.

Let $\mathbf{x}$ be a candidate vector in $S_{\boldsymbol{\mu}_1} \cap S_{\boldsymbol{\mu}_2}$, and let $\mathbf{x}'$ be its query restriction. We label the variable symbols in $\boldsymbol{\mu}_1$ as $x_1, x_2, \ldots, x_k$ and in $\boldsymbol{\mu}_2$ as $y_1, y_2, \ldots, y_l$. Then equating for each entry of $\mathbf{x}'$ yields some restriction on the $x_i$'s and $y_i$'s. We have already addressed entries where both entries are constants in $[N]$ in the above paragraph. To reason about the remaining constraints, consider a tripartite graph $G$ with repeated edges allowed, where the vertex set is $[N] \cup \{x_1, \ldots, x_k\} \cup \{y_1, \ldots, y_l\}$. For each entry, we draw an edge between the two values that it requires to be equal.

Now we can consider the connected components of $G$. If there are distinct $i, j \in [N]$ such that $i, j$ belong to the same connected component, then this implies that $S_{\boldsymbol{\mu}_1} \cap S_{\boldsymbol{\mu}_2} = \emptyset$. So now assume this is not the case. Then each connected component of $G$ can be labeled either by a value $i \in [N]$ if it has a vertex $i$ in the first part, or a variable symbol $z_j$ for some $j$ if it has no such vertex. Then we define the subtype $\boldsymbol{\mu}_3$ as follows: in entries where both $\boldsymbol{\mu}_1$ and $\boldsymbol{\mu}_2$ are the same constant value in $[N]$, $\boldsymbol{\mu}_3$ will just match this value. Each other entry corresponds to some edge in $G$; let the corresponding entry in $\boldsymbol{\mu}_3$ be the label of that edge's connected component in $G$. We first check parity constraints:

- For each $i \in [N]$ such that $\boldsymbol{\lambda}_i = 1$, we need to check that the constant $i$ appears an odd number of times in $\boldsymbol{\mu}_3$. The number of times $i$ appears will be the number of entries $A$ where $\boldsymbol{\mu}_1$ and $\boldsymbol{\mu}_2$ are both $i$, plus the number of edges in the connected component containing $i$. The latter term splits further into the $B$ edges where one endpoint is an $x_i$ vertex, and the $C$ edges where one endpoint is $i$ and one endpoint is a $y_i$ vertex. Our goal is to show that $A + B + C$ is odd.

  To see this, note that $A+C$ is the total number of times that $i$ appears in $\boldsymbol{\mu}_1$, hence it is odd. Secondly, $B$ is even since each $x_i$ vertex must have even degree (its degree is the number of times it appears in $\boldsymbol{\mu}_1$). The claim follows.

- For each variable symbol $z_j$, we need to check that it appears an even number of times. This is equal to the number of edges in the corresponding connected component, noting that it only comprises $x_i$ and $y_i$ vertices. This must be even because each $x_i$ vertex has even degree.

Finally, the constraint about the labeling of the variable symbols can be ensured by just relabeling the variable symbols in $\boldsymbol{\mu}_3$. Therefore $\boldsymbol{\mu}_3$ is a valid subtype of $\boldsymbol{\lambda}$, and it is clear that we have $S_{\boldsymbol{\mu}_3} = S_{\boldsymbol{\mu}_1} \cap S_{\boldsymbol{\mu}_2}$. The conclusion follows. ☐

**Lemma 8.6.** *Any type $\boldsymbol{\lambda}$ has at most $(2r)^r$ subtypes.*

*Proof.* Consider a subtype $\boldsymbol{\mu}$ of $\boldsymbol{\lambda}$. Any entry in the string defining $\boldsymbol{\mu}$ must be one of the following:

- A fixed integer $i \in [N]$ such that $\boldsymbol{\lambda}_i = 1$. There are at most $r$ such integers.

- A variable symbol $x_i$, where $i \leq r$.

$\boldsymbol{\mu}$ has $r$ entries, so the conclusion follows. ☐

### 8.2.2 Relating Subtype Projectors to Type Projectors

It turns out that our main technical task to prove bounds on monogamy games in Section 9 is to bound expressions of the form

$$\mathrm{Tr}\left[\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}} \rho\right],$$

where $\rho$ is some quantum mixed state in $\mathrm{S}((\mathbb{C}^N)^{\otimes r} \otimes \mathbb{C}^M)$, $\Xi$ is some PSD operator, and $\boldsymbol{\lambda}$ is a $\mathsf{BinType}$. Here, we will use the combinatorial machinery we just introduced in Section 8.2.1 to reduce this to bounding expressions of the form

$$\mathrm{Tr}\left[\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}} \rho\right],$$

where $\boldsymbol{\mu}$ is now a subtype. Our starting point is the following lemma:

**Lemma 8.7.** *For any type $\boldsymbol{\lambda}$, there exist constants $\gamma_{\boldsymbol{\lambda},\boldsymbol{\mu}} \in \mathbb{Z}$ for each subtype $\boldsymbol{\mu}$ of $\boldsymbol{\lambda}$ such that*

$$\Pi_{\boldsymbol{\lambda}} = \sum_{\boldsymbol{\mu}} \gamma_{\boldsymbol{\lambda},\boldsymbol{\mu}} \Pi_{\boldsymbol{\mu}}.$$

*Moreover, we have $|\gamma_{\boldsymbol{\lambda},\boldsymbol{\mu}}| \leq 2^{(2r)^r}$ for all $\boldsymbol{\lambda}, \boldsymbol{\mu}$.*

*Proof.* By the inclusion-exclusion principle, we have the following decomposition into subtypes $\boldsymbol{\mu}$ of $\boldsymbol{\lambda}$:

$$
\begin{aligned}
\Pi_{\boldsymbol{\lambda}} &= \sum_{x \text{ matching } \boldsymbol{\lambda}} |x\rangle\langle x| \\
&= \sum_{x \text{ matching at least one } \boldsymbol{\mu}} |x\rangle\langle x| \\
&= \sum_{\boldsymbol{\mu}} \left( \sum_{x \in S_{\boldsymbol{\mu}}} |x\rangle\langle x| \right) - \sum_{\boldsymbol{\mu}_1 < \boldsymbol{\mu}_2} \left( \sum_{x \in S_{\boldsymbol{\mu}_1} \cap S_{\boldsymbol{\mu}_2}} |x\rangle\langle x| \right) + \sum_{\boldsymbol{\mu}_1 < \boldsymbol{\mu}_2 < \boldsymbol{\mu}_3} \left( \sum_{x \in S_{\boldsymbol{\mu}_1} \cap S_{\boldsymbol{\mu}_2} \cap S_{\boldsymbol{\mu}_3}} |x\rangle\langle x| \right) - \dots .
\end{aligned}
$$

By Lemma 8.5, each term in parentheses is either 0 or a projector onto some subtype of $\boldsymbol{\lambda}$. Hence we can collect like terms to write $\Pi_{\boldsymbol{\lambda}}$ as a linear combination of the $\Pi_{\boldsymbol{\mu}}$'s. The coefficient $\gamma_{\boldsymbol{\lambda},\boldsymbol{\mu}}$ in front of $\Pi_{\boldsymbol{\mu}}$ is at most the total number of times that $\Pi_{\boldsymbol{\mu}}$ appears in the above expression, which is trivially at most the number of subcollections of the collection of subtypes of $\boldsymbol{\lambda}$. By Lemma 8.6, there are at most $(2r)^r$ subtypes of $\boldsymbol{\lambda}$, which implies the desired bound. □

Finally, we completely reduce our problem to working with subtypes instead of types via the following lemma:

**Lemma 8.8.** *For any PSD matrix $A$ and type $\boldsymbol{\lambda}$, we have*

$$
\Pi_\lambda A \Pi_\lambda \leq (2r)^r \cdot 2^{2(2r)^r} \cdot \left( \sum_{\boldsymbol{\mu} \text{ subtype of } \boldsymbol{\lambda}} \Pi_{\boldsymbol{\mu}} A \Pi_{\boldsymbol{\mu}} \right),
$$

*with respect to the PSD ordering.*

*Proof.* By linearity, it suffices to prove the result when $A$ is a rank 1 projector $|\phi\rangle\langle\phi|$. Then we have for any state $|\Phi\rangle$ that:

$$
\begin{aligned}
\langle \Phi | \Pi_{\boldsymbol{\lambda}} A \Pi_{\boldsymbol{\lambda}} | \Phi \rangle &= | \langle \Phi | \Pi_{\boldsymbol{\lambda}} | \phi \rangle |^2 \\
&= \left| \sum_{\boldsymbol{\mu}} \gamma_{\boldsymbol{\lambda},\boldsymbol{\mu}} \langle \Phi | \Pi_{\boldsymbol{\mu}} | \phi \rangle \right|^2 \quad \text{(Lemma 8.7)} \\
&\leq \left( \sum_{\boldsymbol{\mu}} \gamma_{\boldsymbol{\lambda},\boldsymbol{\mu}}^2 \right) \cdot \left( \sum_{\boldsymbol{\mu}} | \langle \Phi | \Pi_{\boldsymbol{\mu}} | \phi \rangle |^2 \right) \quad \text{(Cauchy-Schwarz)} \\
&\leq (2r)^r \cdot 2^{2(2r)^r} \cdot \sum_{\boldsymbol{\mu}} \langle \Phi | \Pi_{\boldsymbol{\mu}} A \Pi_{\boldsymbol{\mu}} | \Phi \rangle ,
\end{aligned}
$$

which implies the desired bound. In the final step, we have used Lemma 8.7 to bound each $\gamma_{\boldsymbol{\lambda},\boldsymbol{\mu}}$ along with Lemma 8.6 to bound the number of subtypes being summed over.

□

## 8.3 Phase Twirling

For a binary function $f : [N] \to \{0, 1\}$, we let $\mathsf{U}_f$ define the phase unitary

$$
\mathsf{U}_f = \sum_{x \in [N]} (-1)^{f(x)} |x\rangle\langle x| .
$$

Using the $\mathsf{BinType}$ decomposition, we can show the following identity for the $r$-wise twirl with $\mathsf{U}_f$:

**Lemma 8.9.** *Let $O \in L(\mathcal{H})$ be a linear operator acting on the vector space $\mathcal{H} = (\mathbb{C}^N)^{\otimes r} \otimes \mathbb{C}^M$. Then,*

$$\mathop{\mathbb{E}}_{f \sim \mathcal{F}_n} \left[ \left( \mathsf{U}_f^{\otimes r} \otimes \mathbb{I} \right) O \left( \mathsf{U}_f^{\otimes r} \otimes \mathbb{I} \right) \right] = \sum_{\boldsymbol{\lambda} \in \{0,1\}^N} \Pi_{\boldsymbol{\lambda}} O \Pi_{\boldsymbol{\lambda}} \,,$$

*where $\Pi_{\boldsymbol{\lambda}}$ projects onto $V_{\boldsymbol{\lambda}} = \mathrm{span}_{\mathbb{C}}\{|x_1, \ldots, x_r, v\rangle \in (\mathbb{C}^N)^{\otimes r} \otimes \mathbb{C}^M \,:\, \mathsf{BinType}((x_1, \ldots, x_r), v) = \boldsymbol{\lambda}\}$.*

*Proof.* Expanding $O$ in the standard basis and using the linearity of expectation, we get

$$\begin{aligned}
&\mathop{\mathbb{E}}_{f \sim \mathcal{F}_n} \left[ \left( \mathsf{U}_f^{\otimes r} \otimes \mathbb{I} \right) O \left( \mathsf{U}_f^{\otimes r} \otimes \mathbb{I} \right) \right] \\
&= \sum_{\substack{\mathbf{x}, \mathbf{y} \in [N]^r \\ v, w \in [M]}} O_{(\mathbf{x}, v);(\mathbf{y}, w)} \mathop{\mathbb{E}}_{f \sim \mathcal{F}_n} \left[ \mathsf{U}_f^{\otimes r} |\mathbf{x}\rangle\langle\mathbf{y}| \, \mathsf{U}_f^{\otimes r} \otimes |v\rangle\langle w| \right] \\
&= \sum_{\substack{\mathbf{x}, \mathbf{y} \in [N]^r \\ v, w \in [M]}} O_{(\mathbf{x}, v);(\mathbf{y}, w)} \mathop{\mathbb{E}}_{f \sim \mathcal{F}_n} \left[ (-1)^{f(x_1) + \ldots + f(x_r) + f(y_1) + \ldots + f(y_r)} \right] |\mathbf{x}\rangle\langle\mathbf{y}| \otimes |v\rangle\langle w| \\
&= \sum_{\substack{\mathbf{x}, \mathbf{y} \in [N]^r \\ v, w \in [M] \\ \mathsf{BinType}(\mathbf{x}, v) = \mathsf{BinType}(\mathbf{y}, w)}} O_{(\mathbf{x}, v);(\mathbf{y}, w)} \, |\mathbf{x}, v\rangle\langle\mathbf{y}, w| \;=\; \sum_{\boldsymbol{\lambda} \in \{0,1\}^N} \Pi_{\boldsymbol{\lambda}} O \Pi_{\boldsymbol{\lambda}}.
\end{aligned}$$

□

# 9 Construction from Binary Phase States

In this section, we prove upper bounds on the value of restricted oracular cloning games (defined in Definition 6.8). The remainder of this section is organized as follows:

1. In Section 9.1, we formally state our binary phase construction and prove some preliminary lemmas.
2. In Section 9.2, we expand out the relevant operators and states in terms of *subtypes* (defined in Section 8.2).
3. In Section 9.3, we prove spectral bounds on the operator norms of the relevant operators, and show that these quickly yield our desired bounds on the value of $1 \mapsto 2$ oracular cloning games.
4. In Section 9.4, we provide some additional tools for handling $t \mapsto t+1$ cloning games when $t > 1$, and then put everything together to prove our desired bounds in the restricted oracular cloning setting.
5. For completeness, in Section 9.5, we provide an example showing that generic techniques for bounding monogamy games will not suffice in this setting, justifying our use of the specific structure of oracular cloning games.

## 9.1 Setup and Notation

We begin by presenting our construction. Note the qualitative similarity of this construction with Construction 2; both rely centrally on binary phase states.

**Construction 3.** *Let $\mathfrak{F} = \{f_\theta : \{0,1\}^n \to \{0,1\}\}_{\theta\in\Theta}$ be a family of functions parametrized by elements $\Theta = \{0,1\}^\lambda$. Consider the following $t \mapsto t+1$ oracular cloning game (as defined in Definition 6.5) $\mathsf{G}_{\mathfrak{F},t}$ with question set $\Theta$ and answer set $\mathcal{X} := \{0,1\}^n$. For any $\theta$, we will take the unitary $U_\theta$ to be $\mathsf{U}_{f_\theta}\mathsf{H}^{\otimes n}$. (Here, $\mathsf{U}_{f_\theta}$ is the phase oracle for $f_\theta$ as defined in Section 3.1.) In other words, for any $x \in \{0,1\}^n$, we have*

$$U_\theta |x\rangle = 2^{-n/2} \sum_{u\in\{0,1\}^n} (-1)^{f_\theta(u)\oplus\langle x,u\rangle} |u\rangle .$$

**Remark 12.** *We are being intentionally vague about the choice of function family $\mathfrak{F}$. One could imagine instantiating it with a post-quantum PRF family, to obtain a construction that is plausibly secure against arbitrary polynomial-time adversaries in the oracular cloning game.*

*Since we only prove oracular security in the case where $t = O(1)$ and each player can make $q = 1$ query in total, we will instead instantiate $\mathfrak{F}$ as an $O(1)$-wise uniform function family, which is statistically indistinguishable from the family of all functions from $\{0,1\}^n \to \{0,1\}$ in this query bounded game. We will reiterate this formally when establishing our final theorems in Section 9.4.*

We will consider restricted quantum strategies (defined in Definition 6.8). Recall that we use $\mathcal{S}_{\text{rest}}$ to denote the collection of all such strategies. We now make a crucial observation:

**Remark 13.** *Since $U_\theta^\dagger = \mathsf{H}^{\otimes n}\mathsf{U}_{f_\theta}$ and each player $\mathcal{P}_i$ is given a control bit in register $\mathsf{E_i}$ dictating whether they will query $U_\theta$ or $U_\theta^\dagger$, we can assume without loss of generality that each player simply makes one non-adaptive query to $\mathsf{U}_{f_\theta}$ as their first step. (In the event that the player is querying $U_\theta = \mathsf{U}_{f_\theta}\mathsf{H}^{\otimes n}$, they would technically need to query $\mathsf{H}^{\otimes n}$ first. We can get around this by absorbing this query to $\mathsf{H}^{\otimes n}$ into the cloning channel $\Phi$.)*

Recall from Definition 6.8 that each player's register $\mathsf{B_i}$ splits into a query register $\mathsf{C_i}$, an ancilla register $\mathsf{D_i}$, and a control qubit register $\mathsf{E_i}$. Recalling the setup in Definition 6.8 together with Lemma 6.9 and Remark 13, we can write

$$\mathbf{P}_{i,x}^{U_\theta,U_\theta^\dagger} = (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D_iE_i}})Q_i^\dagger(|x\rangle\langle x| \otimes \mathbb{I}_{\mathsf{D_iE_i}})Q_i(\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D_iE_i}}),$$

for some unitaries $Q_1, \ldots, Q_{t+1}$ such that $Q_i$ acts on all the three registers $\mathsf{C_iD_iE_i}$.

With this in mind, we now switch from a cloning-based formulation to an entanglement-based formulation. At a high level, the point of this is to use the ricochet property of EPR pairs (formally, Lemma 3.1) to express the value of the cloning game as a phase twirl with respect to $\mathfrak{F}$. The below lemma closely follows the proof of Lemma A.1; indeed, when $t = 1$ the proofs are nearly identical.

**Lemma 9.1.** *For $\mathsf{S} \in \mathcal{S}_{\text{rest}}$ as specified above, define the shared state*

$$\rho_{\mathsf{B}_{1:t+1}\mathsf{A}'_{1:t}} := (\Phi_{\mathsf{A}_1\ldots\mathsf{A}_t\to\mathsf{B}_1\ldots\mathsf{B}_{t+1}} \otimes \mathbb{I}_{\mathsf{A}'_{1:t}}) \left(|\mathsf{EPR}^n\rangle\langle\mathsf{EPR}^n|^{\otimes t}\right).$$

*Then we have:*

$$\begin{aligned}\omega_{\mathsf{S}}(\mathsf{G}) =& 2^{n(t-1)} \cdot \mathop{\mathbb{E}}_{\theta} \sum_{x\in\{0,1\}^n} \mathrm{Tr}\Bigg[\Bigg(\Big(\bigotimes_{i\in[t+1]} (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D_iE_i}})Q_i^\dagger(|x\rangle\langle x| \otimes \mathbb{I}_{\mathsf{D_iE_i}})Q_i(\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D_iE_i}})\Big) \\ &\otimes \left(\mathsf{U}_{f_\theta}\mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n}\mathsf{U}_{f_\theta}\right)^{\otimes t}_{\mathsf{A}'_{1:t}}\Bigg)\rho\Bigg].\end{aligned}$$

*Proof.* Let $J(\Phi) \in \mathrm{L}(\mathcal{H}_{\mathsf{B}_{1:t+1}} \otimes \mathcal{H}_{\mathsf{A}'_{1:t}})$ denote the Choi-Jamiołkowski isomorphism of the cloning map $\Phi_{\mathsf{A}_{1:t} \to \mathsf{B}_{1:t+1}}$. Recall that

$$J(\Phi) = 2^{nt} \cdot (\Phi_{\mathsf{A}_1 \dots \mathsf{A}_t \to \mathsf{B}_1 \dots \mathsf{B}_{t+1}} \otimes \mathbb{I}_{\mathsf{A}'_{1:t}}) \left( |\mathsf{EPR}^n\rangle\langle \mathsf{EPR}^n|^{\otimes t} \right) = 2^{nt} \rho.$$

Now using Lemma 3.1, we have:

$$\begin{aligned}
\omega_{\mathsf{S}}(\mathsf{G}) =& \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{x \sim \{0,1\}^n} \mathrm{Tr} \left[ \left( \mathbf{P}_{1,x}^{\mathsf{U}_{f_\theta}} \otimes \dots \otimes \mathbf{P}_{t+1,x}^{\mathsf{U}_{f_\theta}} \right) \Phi_{\mathsf{A}_1 \dots \mathsf{A}_t \to \mathsf{B}_1 \dots \mathsf{B}_{t+1}} \left( (\mathsf{U}_{f_\theta} \mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n} \mathsf{U}_{f_\theta})^{\otimes t}_{\mathsf{A}_1 \dots \mathsf{A}_t} \right) \right] \\
=& \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{x \sim \{0,1\}^n} \mathrm{Tr} \left[ \left( \mathbf{P}_{1,x}^{\mathsf{U}_{f_\theta}} \otimes \dots \otimes \mathbf{P}_{t+1,x}^{\mathsf{U}_{f_\theta}} \otimes \left( \mathsf{U}_{f_\theta} \mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n} \mathsf{U}_{f_\theta} \right)^{\otimes t}_{\mathsf{A}'_{1:t}} \right) J(\Phi)_{\mathsf{B}_{1:t+1} \mathsf{A}'_{1:t}} \right] \\
=& \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{x \sim \{0,1\}^n} \mathrm{Tr} \Bigg[ \Bigg( \Big( \bigotimes_{i \in [t+1]} (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D_i E_i}}) Q_i^\dagger (|x\rangle\langle x| \otimes \mathbb{I}_{\mathsf{D_i E_i}}) Q_i (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D_i E_i}}) \Big) \\
& \otimes \left( \mathsf{U}_{f_\theta} \mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n} \mathsf{U}_{f_\theta} \right)^{\otimes t}_{\mathsf{A}'_{1:t}} \Bigg) J(\Phi)_{\mathsf{B}_{1:t+1} \mathsf{A}'_{1:t}} \Bigg] \\
=& 2^{nt} \cdot \mathop{\mathbb{E}}_{\theta} \mathop{\mathbb{E}}_{x \sim \{0,1\}^n} \mathrm{Tr} \Bigg[ \Bigg( \Big( \bigotimes_{i \in [t+1]} (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D_i E_i}}) Q_i^\dagger (|x\rangle\langle x| \otimes \mathbb{I}_{\mathsf{D_i E_i}}) Q_i (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D_i E_i}}) \Big) \\
& \otimes \left( \mathsf{U}_{f_\theta} \mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n} \mathsf{U}_{f_\theta} \right)^{\otimes t}_{\mathsf{A}'_{1:t}} \Bigg) \rho \Bigg] \\
=& 2^{n(t-1)} \cdot \mathop{\mathbb{E}}_{\theta} \sum_{x \in \{0,1\}^n} \mathrm{Tr} \Bigg[ \Bigg( \Big( \bigotimes_{i \in [t+1]} (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D_i E_i}}) Q_i^\dagger (|x\rangle\langle x| \otimes \mathbb{I}_{\mathsf{D_i E_i}}) Q_i (\mathsf{U}_{f_\theta} \otimes \mathbb{I}_{\mathsf{D_i E_i}}) \Big) \\
& \otimes \left( \mathsf{U}_{f_\theta} \mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n} \mathsf{U}_{f_\theta} \right)^{\otimes t}_{\mathsf{A}'_{1:t}} \Bigg) \rho \Bigg].
\end{aligned}$$

□

Now let $\rho$ be the Choi state as defined in Lemma 9.1, and define the projector

$$\Xi = \sum_{x \in \{0,1\}^n} \left( \left( \bigotimes_{i \in [t+1]} Q_i^\dagger \left( |x\rangle\langle x|_{\mathsf{C_i}} \otimes \mathbb{I}_{\mathsf{D_i E_i}} \right) Q_i \right) \otimes \left( \mathsf{H}^{\otimes n} |x\rangle\langle x| \mathsf{H}^{\otimes n} \right)^{\otimes t}_{\mathsf{A}'_{1:t}} \right). \tag{6}$$

Let $d = 2^n$, $r = 2t+1$, $d' = 2^{a+1}$, and $r' = t+1$. Recall that $(\mathbb{C}^d)^{\otimes r} \otimes (\mathbb{C}^{d'})^{\otimes r'} \cong \bigoplus_{\boldsymbol{\lambda}} V_{\boldsymbol{\lambda}}$ decomposes into a collection of subspaces corresponding to binary type vectors $\boldsymbol{\lambda} \in \{0,1\}^d$. Here, $(\mathbb{C}^{d'})^{\otimes r'}$ serves as an auxiliary register; in terms of the notation in Section 8.1, we are taking $N = d$ and $M = d'^{r'}$ (in other words, we are packing all the players' ancillary registers into one auxiliary input).

Moreover, we assume going forward that $\mathfrak{F}$ is a $(4t+2)$-wise uniform family of functions from $\{0,1\}^n \to \{0,1\}$. As noted in Remark 12, this is statistically indistinguishable from instantiating $\mathfrak{F}$ as the family of all functions from $\{0,1\}^n \to \{0,1\}$, since the expression in Lemma 9.1 has degree $4t+2$ in $\mathsf{U}_{f_\theta}$.

Then using Lemma 9.1 and then Lemma 8.9, we get:

$$\omega_{\mathsf{S}}(\mathsf{G}) = 2^{n(t-1)} \mathrm{Tr} \left[ \mathop{\mathbb{E}}_{f} \left[ \left( \mathsf{U}_f^{\otimes r} \otimes \mathbb{I}_{\mathsf{D}_{1:t+1}} \right) \Xi \left( \mathsf{U}_f^{\otimes r} \otimes \mathbb{I}_{\mathsf{D}_{1:t+1}} \right) \right] \rho \right]$$

$$= 2^{n(t-1)} \sum_{\boldsymbol{\lambda} \in \{0,1\}^d} \operatorname{Tr}\left[\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}} \rho\right], \tag{7}$$

where $\Pi_{\boldsymbol{\lambda}}$ is the projector onto the subspace of $(\mathbb{C}^d)^{\otimes r} \otimes (\mathbb{C}^{d'})^{\otimes(t+1)}$ given by

$$V_{\boldsymbol{\lambda}} = \operatorname{span}_{\mathbb{C}}\{|(v_1, \ldots, v_r, a_1, \ldots, a_{t+1})\rangle \ : \ \mathsf{BinType}(v_1, \ldots, v_r, a_1, \ldots, a_{t+1}) = \boldsymbol{\lambda}\}.$$

We now state some simple high-level bounds on $\omega(\mathsf{G})$ in terms of *subtypes* $\boldsymbol{\mu}$:

**Lemma 9.2.** *We have*

$$\omega(\mathsf{G}) \leq \exp(\exp(O(t \log t))) \cdot 2^{n(t-1)} \cdot \max_{\textit{subtypes } \boldsymbol{\mu}} \left\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\right\|_\infty.$$

*Proof.* Continuing from Equation (7), we have:

$$\begin{aligned}
\omega(\mathsf{G}) &= 2^{n(t-1)} \cdot \sum_{\boldsymbol{\lambda} \in \{0,1\}^d} \operatorname{Tr}\left[\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}} \cdot \Pi_{\boldsymbol{\lambda}} \rho\right] \\
&\leq 2^{n(t-1)} \cdot \sum_{\boldsymbol{\lambda} \in \{0,1\}^d} \left(\operatorname{Tr}\left[\Pi_{\boldsymbol{\lambda}} \rho\right] \cdot \left\|\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}}\right\|_\infty\right) \\
&\leq 2^{n(t-1)} \cdot \left(\sum_{\boldsymbol{\lambda} \in \{0,1\}^d} \operatorname{Tr}\left[\Pi_{\boldsymbol{\lambda}} \rho\right]\right) \cdot \max_{\boldsymbol{\lambda} \in \{0,1\}^d} \left\|\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}}\right\|_\infty \\
&= 2^{n(t-1)} \cdot \max_{\boldsymbol{\lambda} \in \{0,1\}^d} \left\|\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}}\right\|_\infty.
\end{aligned}$$

We can now use Lemma 8.8 to pass further to subtypes $\boldsymbol{\mu}$ at the expense of an $\exp(\exp(O(t \log t)))$ multiplicative loss:

$$\begin{aligned}
\omega(\mathsf{G}) &\leq \exp(\exp(O(t \log t))) \cdot 2^{n(t-1)} \cdot \max_{\boldsymbol{\lambda} \in \{0,1\}^d} \left(\sum_{\boldsymbol{\mu} \text{ subtype of } \boldsymbol{\lambda}} \left\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\right\|_\infty\right) \\
&\leq \exp(\exp(O(t \log t))) \cdot 2^{n(t-1)} \cdot \max_{\boldsymbol{\mu}} \left\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\right\|_\infty \ \text{(Lemma 8.6)}.
\end{aligned}$$

□

Much like the techniques by [TFKW13], Lemma 9.2 has the attractive feature that it does not depend on the Choi state $\rho$. This is sufficient when $t = 1$, but *provably* insufficient for any $t \geq 2$ (as we will show in Section 9.5). To handle $t > 1$, we must additionally consider the state $\rho$, and we capture this in the following lemma:

**Lemma 9.3.** *We have*

$$\omega(\mathsf{G}) \leq \exp(\exp(O(t \log t))) \cdot 2^{n(t-1)} \cdot \sum_{\boldsymbol{\mu}} \operatorname{Tr}\left[\Pi_{\boldsymbol{\mu}} \rho\right] \cdot \left\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\right\|_\infty.$$

*Proof.* We will again start with Equation (7), but instead pass to subtypes immediately using Lemma 8.8:

$$\begin{aligned}
\omega(\mathsf{G}) &\leq \exp(\exp(O(t \log t))) \cdot 2^{n(t-1)} \cdot \operatorname{Tr}\left[\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}} \rho\right] \\
&= \exp(\exp(O(t \log t))) \cdot 2^{n(t-1)} \cdot \operatorname{Tr}\left[\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}} \cdot \Pi_{\boldsymbol{\mu}} \rho\right] \\
&\leq \exp(\exp(O(t \log t))) \cdot 2^{n(t-1)} \cdot \sum_{\boldsymbol{\mu}} \operatorname{Tr}\left[\Pi_{\boldsymbol{\mu}} \rho\right] \cdot \left\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\right\|_\infty.
\end{aligned}$$

□

## 9.2 Expanding out $\Xi$ using Subtypes

We now set up some additional notation. For each $i \in [t+1]$ and $j_1, j_2 \in [d]$ and $l_1, l_2 \in [d']$, we let $Q^\dagger_{i,(j_1,l_1);(j_2,l_2)}$ denote the entry in the $(j_1, l_1)$-th row and $(j_2, l_2)$-th column of the unitary $Q_i^\dagger$. To keep track of the ancillary indices in registers $\mathsf{D}_{1:t+1}$, we will introduce the values $z_1, \ldots, z_{t+1} \in [d']$ and denote $\mathbf{z} = (z_1, \ldots, z_{t+1})$ for brevity. We can now write the projector $\Xi$ in Equation (6) as:

$$\Xi = \sum_{\substack{x \in \{0,1\}^n \\ z_1,\ldots,z_{t+1} \in \{0,1\}^a}} |\Xi^{x,\mathbf{z}}\rangle\langle\Xi^{x,\mathbf{z}}| \,, \text{ where}$$

$$\begin{aligned}
|\Xi^{x,\mathbf{z}}\rangle &= Q_1^\dagger \left(|x\rangle \otimes |z_1\rangle\right) \otimes \cdots \otimes Q_{t+1}^\dagger \left(|x\rangle \otimes |z_{t+1}\rangle\right) \otimes \left(\mathsf{H}^{\otimes n} |x\rangle\right)^{\otimes t} \\
&= 2^{-nt/2} \sum_{\substack{v_1,\ldots,v_r \in [d] \\ w_1,\ldots,w_{t+1} \in [d']}} \left( (-1)^{\langle v_{t+2} + \cdots + v_r, x\rangle} \prod_{i=1}^{t+1} Q^\dagger_{i,(v_i,w_i);(x,z_i)} \right) |v_1, \ldots, v_r\rangle \otimes |w_1, \ldots, w_{t+1}\rangle \,.
\end{aligned}$$

We now begin unpacking the operator $\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}$, using the formalism of subtypes introduced in Section 8.2. Recall that we have:

$$\begin{aligned}
\Xi &= \sum_{\substack{x \in \{0,1\}^n \\ z_1,\ldots,z_{t+1} \in \{0,1\}^a}} |\Xi^{x,\mathbf{z}}\rangle\langle\Xi^{x,\mathbf{z}}| \\
\Rightarrow \Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}} &= \sum_{\substack{x \in \{0,1\}^n \\ z_1,\ldots,z_{t+1} \in \{0,1\}^a}} \Pi_{\boldsymbol{\mu}} |\Xi^{x,\mathbf{z}}\rangle\langle\Xi^{x,\mathbf{z}}| \Pi_{\boldsymbol{\mu}}.
\end{aligned}$$

Therefore we can define a matrix $\mathbf{A} \in \mathbb{C}^{d_1 \times d_2}$, where $d_1 = 2^{rn+(t+1)a}$ is the dimension of $|\Xi^{x,\mathbf{z}}\rangle$ and $d_2 = 2^{n+(t+1)a}$ is the number of possible values of $x, \mathbf{z}$. The columns of $\mathbf{A}$ are indexed by $x, \mathbf{z}$ and the corresponding column is exactly $\Pi_{\boldsymbol{\mu}} |\Xi^{x,\mathbf{z}}\rangle$. Then we have $\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}} = \mathbf{A}\mathbf{A}^\dagger \Rightarrow \|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\|_\infty = \|\mathbf{A}\|_\infty^2$.

Recall also that we have:

$$|\Xi^{x,\mathbf{z}}\rangle = 2^{-nt/2} \sum_{\substack{v_1,\ldots,v_r \in [d] \\ w_1,\ldots,w_{t+1} \in [d']}} \left( (-1)^{\langle v_{t+2} + \cdots + v_r, x\rangle} \prod_{i=1}^{t+1} Q^\dagger_{i,(v_i,w_i);(x,z_i)} \right) |v_1, \ldots, v_r\rangle \otimes |w_1, \ldots, w_{t+1}\rangle \,.$$

Therefore, once we project onto the subspace corresponding to the subtype $\boldsymbol{\mu}$, we get the state

$$\Pi_{\boldsymbol{\mu}} |\Xi^{x,\mathbf{z}}\rangle = 2^{-nt/2} \sum_{\substack{v_1,\ldots,v_r \in [d] \\ w_1,\ldots,w_{t+1} \in [d'] \\ (\mathbf{v},\mathbf{w}) \in S_{\boldsymbol{\mu}}}} \left( (-1)^{\langle v_{t+2} + \cdots + v_r, x\rangle} \prod_{i=1}^{t+1} Q^\dagger_{i,(v_i,w_i);(x,z_i)} \right) |v_1, \ldots, v_r\rangle \otimes |w_1, \ldots, w_{t+1}\rangle \,. \tag{8}$$

Now note that any row of $\mathbf{A}$ that does not correspond to a standard basis vector in $S_{\boldsymbol{\mu}}$ will be 0. We can discard all such rows without affecting the operator norm of $A$. We can therefore re-index the rows of $\mathbf{A}$ by the variable symbols $x_1, \ldots, x_l$ of $\boldsymbol{\mu}$ and the ancilla indices $w_1, \ldots, w_{t+1}$, so that $\mathbf{A}$ is effectively a $2^{nl+a(t+1)} \times 2^{n+a(t+1)}$ matrix.

With this setup in mind, we introduce a couple more definitions that will help us complete our analysis:

**Definition 9.4.** *Let $\ell \in [0, t]$ be an integer parameter (typically we will work with $\ell = t$). Let $\boldsymbol{\mu}$ be a subtype of $(\mathbb{C}^d)^{\otimes(t+1+\ell)} \otimes (\mathbb{C}^{d'})^{\otimes r'}$ with variable symbols $x_1, \ldots, x_l$. Then, define the matrix*

$$\mathbf{B} := \mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})$$

*with dimensions $2^{nl+a(t+1)} \times 2^{n+a(t+1)}$ as follows:*

*Its rows are indexed by $y_1, \ldots, y_l \in [d]$ and $w_1, \ldots, w_{t+1} \in [d']$. Its columns are indexed by $x \in [d]$ and $z_1, \ldots, z_{t+1} \in [d']$. For any such indices, take*

$$(v_1, \ldots, v_{t+1+\ell}, w_1, \ldots, w_{t+1}) = \mathsf{Reconstruct}(\boldsymbol{\mu}, (y_1, \ldots, y_l), (w_1, \ldots, w_{t+1})) \in [d]^{t+1+\ell} \times [d']^{t+1}.$$

*(The function* Reconstruct *is defined in Definition 8.4.) Then we define the entry*

$$\mathbf{B}_{(y_1,\ldots,y_l,w_1,\ldots,w_{t+1});(x,z_1,\ldots,z_{t+1})} = (-1)^{\langle v_{t+2}+\ldots+v_{t+1+\ell}, x\rangle} \prod_{i=1}^{t+1} Q^{\dagger}_{i,(v_i,w_i);(x,z_i)}. \tag{9}$$

We remark that when $\ell = t$, this definition coincides with the matrix $2^{nt/2}A$. The reason we generalize to $\ell < t$ is for technical reasons; there could be variable symbols that only appear in the "phase entries" $v_{t+2}, \ldots, v_{t+1+\ell}$, in which case they appear an even number of times and do not have any effect on the value of that entry in the matrix $B$. These variable symbols artificially blow up the operator norm of $B$ and will need to be dealt with separately. To capture this, we have the following notion:

**Definition 9.5.** *For a subtype $\boldsymbol{\mu}$ with respect to $(\mathbb{C}^d)^{\otimes(t+1+\ell)} \otimes (\mathbb{C}^{d'})^{\otimes r'}$ and variable symbol $x_i$, we say $x_i$ is a* free variable symbol *of $\boldsymbol{\mu}$ if it only appears in entries $t+2, t+3, \ldots, t+1+\ell$ of $\boldsymbol{\mu}$. (Informally, a free variable symbol is one that only appears in the phase.)*

## 9.3 Bounding $\|\mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})\|_\infty$

In this section, we provide estimates on the operator norm of $\mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})$. We first begin with a lemma that allows us to dispose of free variable symbols:

**Lemma 9.6.** *Suppose $\boldsymbol{\mu}$ is a subtype with respect to $(\mathbb{C}^d)^{\otimes(2t+1)} \otimes (\mathbb{C}^{d'})^{\otimes r'}$, and suppose it has $b$ free variable symbols that appear in a total of $p$ positions in indices $k+2, k+3, \ldots, 2k+1$.*

*Then define $\ell := t - p$, and $\boldsymbol{\mu}'$ to be the subtype with respect to $(\mathbb{C}^d)^{\otimes(t+1+\ell)} \otimes (\mathbb{C}^{d'})^{\otimes r'}$ obtained by taking $\boldsymbol{\mu}$ and removing all free variable symbols. Then we have*

$$\|\mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})\|_\infty = 2^{nb/2} \left\|\mathbf{B}_{\boldsymbol{\mu}'}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})\right\|_\infty.$$

*Proof.* For brevity, write $\mathbf{B} = \mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})$ and $\mathbf{B}' = \mathbf{B}_{\boldsymbol{\mu}'}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{t+1})$. Let the variable symbols of $\boldsymbol{\mu}$ be $y_1, \ldots, y_l$, so that its free variable symbols are $y_{l-b+1}, \ldots, y_l$. Note that $\boldsymbol{\mu}'$ will have $l - b$ variable symbols, none of which are free variable symbols. Now since each free variable symbol appears an even number of times in the phase, we have for any indices that

$$B_{(y_1,\ldots,y_l,w_1,\ldots,w_{t+1});(x,z_1,\ldots,z_{t+1})} = B'_{(y_1,\ldots,y_{l-b},w_1,\ldots,w_{t+1});(x,z_1,\ldots,z_{t+1})}.$$

In other words, the matrix $\mathbf{B}$ is obtained by vertically stacking $2^{nb}$ copies of $\mathbf{B}'$ (up to a permutation of rows). Put another way, $\mathbf{B}$ is equal to $B'$ tensored with a column vector consisting of $2^{nb}$ 1's. It follows by

Lemma 3.14 that:

$$\|\mathbf{B}\|_\infty = \|\mathbf{B}'\|_\infty \cdot \left\| \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \right\|_\infty = 2^{nb/2} \|\mathbf{B}'\|_\infty .$$

□

For most of the remainder of this section, we focus on subtypes $\boldsymbol{\mu}$ that do not have any free variable symbols. We first set up some more notation. At a high level, the idea is to cluster the terms being multiplied in Equation (9) according to which of the variable symbols they depend on. This allows us to write $B$ as a block column-wise tensor product of several much simpler block matrices, and then we will appeal to Lemma 3.22.

To this end, let $\boldsymbol{\mu}$ have variable symbols $x_1, \ldots, x_l$. For each for $i \in [l]$, let $I_i = \{j \in [t+1+\ell] : \boldsymbol{\mu}_j = x_i\}$ and $J = \{j \in [t+1+\ell] : \boldsymbol{\mu}_j \text{ is fixed}\}$. Note that $[t+1+\ell]$ is the disjoint union of $I_1, I_2, \ldots, I_l, J$. Also, for convenience we will make the following abuse of notation: for any integer $h$, subset $I \subseteq [h]$, and vector $\mathbf{b}$ with $h$ entries, we use $\mathbf{b}_I$ to denote the sub-vector of length $|I|$ obtained by taking only the indices in $I$ from $\mathbf{b}$. With this in mind, for each $i \in [l]$ define the following matrix $\mathbf{M}_i$ of dimensions $2^{n+a(|I_i|\cap[t+1])} \times 2^{n+a(|I_i|\cap[t+1])}$:

$$M_{i,(y_i,\mathbf{w}_{I_i\cap[t+1]});(x,\mathbf{z}_{I_i\cap[t+1]})} = \prod_{j\in I_i\cap[t+2,t+1+\ell]} (-1)^{\langle y_i, x\rangle} \cdot \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(y_i,w_j);(x,z_j)}.$$

Additionally, define the following matrix $\mathbf{T}$ of dimensions $2^{a(|J|\cap[t+1])} \times 2^{n+a(|J|\cap[t+1])}$:

$$\mathbf{T}_{\mathbf{w}_{J\cap[t+1]};(x,\mathbf{z}_{J\cap[t+1]})} = \prod_{j\in J\cap[t+2,t+1+\ell]} (-1)^{\langle \boldsymbol{\mu}_j, x\rangle} \cdot \prod_{j\in J\cap[t+1]} Q^\dagger_{j,(\boldsymbol{\mu}_j,w_j);(x,z_j)}.$$

It is clear by inspection that $\mathbf{B}_{\boldsymbol{\mu}}$ is the result of applying the block column-wise tensoring operation described in Lemma 3.22 to $\mathbf{M}_1, \ldots, \mathbf{M}_l, \mathbf{T}$. Here, the block columns are indexed by $x$. We will proceed by applying this lemma to these matrices. We thus need to check that the preconditions of the lemma apply, which we do in the next few lemmas:

**Lemma 9.7.** *For any $x^* \in [2^n]$, consider the matrix $\mathbf{T}_{x^*}$ obtained by restricting $\mathbf{T}$ to columns where $x = x^*$. Then $\|\mathbf{T}_{x^*}\|_\infty \leq 1$. Moreover, if $J \cap [t+1]$ is nonempty, then we have $\|\mathbf{T}\|_\infty \leq 1$.*

*Proof.* We have:

$$T_{\mathbf{w}_{J\cap[t+1]};(x,\mathbf{z}_{J\cap[t+1]})} = \prod_{j\in J\cap[t+2,t+1+\ell]} (-1)^{\langle \boldsymbol{\mu}_j, x\rangle} \cdot \prod_{j\in J\cap[t+1]} Q^\dagger_{j,(\boldsymbol{\mu}_j,w_j);(x,z_j)}.$$

Now consider the matrix $T'$ with the same dimensions as $T$ defined by:

$$T'_{\mathbf{w}_{J\cap[t+1]};(x,\mathbf{z}_{J\cap[t+1]})} = \prod_{j\in J\cap[t+1]} Q^\dagger_{j,(\boldsymbol{\mu}_j,w_j);(x,z_j)}.$$

Since $\boldsymbol{\mu}_j$ is fixed for $j \in J$, $\mathbf{T}'$ can be obtained from $\mathbf{T}$ by just flipping the signs of some columns. This preserves the operator norm (this can be seen from Lemma 3.12 for example), so we have $\|\mathbf{T}'\|_\infty = \|\mathbf{T}\|_\infty$. It also follows analogously that $\|\mathbf{T}'_{x^*}\|_\infty = \|\mathbf{T}_{x^*}\|_\infty$, where we analogously define $\mathbf{T}'_{x^*}$ as the result of restricting $\mathbf{T}'$ to columns where $x = x^*$. At this point, we split into two cases:

- If $J \cap [t+1]$ is nonempty, we claim that $\mathbf{T}'$ is a submatrix of $\mathbf{Q} := \bigotimes_{j \in J \cap [t+1]} Q_j^\dagger$. Indeed, we can index the rows of $\mathbf{Q}$ by $(\mathbf{a}, \mathbf{b})$ and the columns by $(\mathbf{c}, \mathbf{d})$, and write

  $$Q_{(\mathbf{a},\mathbf{b});(\mathbf{c},\mathbf{d})} = \prod_{j \in J \cap [t+1]} Q^\dagger_{j,(a_j,b_j);(c_j,d_j)}.$$

  Then $\mathbf{T}'$ is the submatrix of $\mathbf{Q}$ obtained by restricting to rows $(\mathbf{a}, \mathbf{b})$ such that $a_j = \boldsymbol{\mu}_j$ for all $j \in J \cap [t+1]$ and columns $(\mathbf{c}, \mathbf{d})$ such that $c_{j_1} = c_{j_2}$ for any $j_1, j_2 \in J \cap [t+1]$.

  Since the operator norm of a unitary matrix is 1 and there is at least one unitary matrix in this tensor product, it follows from Lemmas 3.13 and 3.14 that $\|\mathbf{T}'\|_\infty \leq 1 \Rightarrow \|\mathbf{T}\|_\infty \leq 1$. Then, it also follows that $\|\mathbf{T}_{x^*}\|_\infty \leq 1$ by Lemma 3.13.

- If $J \cap [t+1]$ is empty then $T'$ is really just a vector of $2^n$ many 1's. Hence $T'_{x^*}$ is just the scalar 1, which trivially has operator norm $\leq 1$.

□

**Lemma 9.8.** *Assume $\boldsymbol{\mu}$ does not have free variable symbols. For any $x^* \in [2^n]$ and $i \in [l]$, consider the matrix $\mathbf{M}_{i,x^*}$ obtained by restricting $M_i$ to columns where $x = x^*$. Then $\|\mathbf{M}_{i,x^*}\|_\infty \leq 1$.*

*Proof.* We have:

$$\mathbf{M}_{i,(y_i,\mathbf{w}_{I_i \cap [t+1]});(x^*,\mathbf{z}_{I_i \cap [t+1]})} = \prod_{j \in I_i \cap [t+2, t+1+\ell]} (-1)^{\langle y_i, x^* \rangle} \cdot \prod_{j \in I_i \cap [t+1]} Q^\dagger_{j,(y_i,w_j);(x^*,z_j)}.$$

We can now define another matrix $\mathbf{M}'_{i,x^*}$ with the same dimensions as $\mathbf{M}_{i,x^*}$ defined by:

$$\mathbf{M}'_{(i,x^*),(y_i,\mathbf{w}_{I_i \cap [t+1]});\mathbf{z}_{I_i \cap [t+1]}} = \prod_{j \in I_i \cap [t+1]} Q^\dagger_{j,(y_i,w_j);(x^*,z_j)}.$$

Since we are fixing $x^*$, $\mathbf{M}'_{i,x^*}$ can be obtained from $\mathbf{M}_{i,x^*}$ by just flipping the signs of some rows. It follows that $\left\|\mathbf{M}'_{i,x^*}\right\|_\infty = \|\mathbf{M}_{i,x^*}\|_\infty$. Now to finish, we argue that $\mathbf{M}'_{i,x^*}$ is a submatrix of $\mathbf{Q} := \bigotimes_{j \in I_i \cap [t+1]} \mathbf{Q}_j^\dagger$. Note that $I_i \cap [t+1]$ must be non-empty as otherwise $x_i$ would be a free variable symbol. Given this, this claim would imply the conclusion by Lemmas 3.13 and 3.14.

To see this claim, note that we can index the rows of $\mathbf{Q}$ by $(\mathbf{a}, \mathbf{b})$ and the columns by $(\mathbf{c}, \mathbf{d})$, and write:

$$Q_{(\mathbf{a},\mathbf{b});(\mathbf{c},\mathbf{d})} = \prod_{j \in I_i \cap [t+1]} Q^\dagger_{j,(a_j,b_j);(c_j,d_j)}.$$

Then $\mathbf{M}'_{i,x^*}$ is the submatrix of $\mathbf{Q}$ obtained by restricting to rows $(\mathbf{a}, \mathbf{b})$ where $a_{j_1} = a_{j_2}$ for any $j_1, j_2 \in I_i \cap [t+1]$ and columns $(\mathbf{c}, \mathbf{d})$ where $c_j = x^*$ for all $j \in I_i \cap [t+1]$. This completes the proof of the lemma. □

**Lemma 9.9.** *Assume $\boldsymbol{\mu}$ does not have free variable symbols. Consider some $i \in [l]$ such that the integer $|I_i \cap [t+2, t+1+\ell]|$ is even. Then, it holds that $\|\mathbf{M}_i\|_\infty \leq 1$.*

*Proof.*

$$M_{i,(y_i,\mathbf{w}_{I_i\cap[t+1]});(x,\mathbf{z}_{I_i\cap[t+1]})} = \prod_{j\in I_i\cap[t+2,t+1+\ell]} (-1)^{\langle y_i,x\rangle} \cdot \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(y_i,w_j);(x,z_j)}$$
$$= \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(y_i,w_j);(x,z_j)},$$

since there are an even number of identical terms being multiplied together in the first product. In this case, we just argue that $\mathbf{M}_i$ is a submatrix of $\mathbf{Q} := \bigotimes_{j\in I_i\cap[t+1]} \mathbf{Q}_j^\dagger$. This is a non-empty tensor product since otherwise $x_i$ would be a free variable symbol. Given this, this claim would imply the conclusion by Lemmas 3.13 and 3.14.

To see this claim, we once again index the rows of $\mathbf{Q}$ by $(\mathbf{a},\mathbf{b})$ and the columns by $(\mathbf{c},\mathbf{d})$, and write:

$$Q_{(\mathbf{a},\mathbf{b});(\mathbf{c},\mathbf{d})} = \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(a_j,b_j);(c_j,d_j)}.$$

Then, $\mathbf{M}_i$ is the submatrix of $\mathbf{Q}$ obtained by restricting to rows $(\mathbf{a},\mathbf{b})$ such that $a_{j_1} = a_{j_2}$ for any $j_1, j_2 \in I_i \cap [t+1]$ and columns $(\mathbf{c},\mathbf{d})$ such that $c_{j_1} = c_{j_2}$ for any $j_1, j_2 \in I_i \cap [t+1]$. This completes the proof of the lemma. □

Our final technical lemma handles the case where a variable symbol appears multiple times among $v_1, \ldots, v_{t+1}$:

**Lemma 9.10.** *Consider some $i \in [l]$ be such that $|I_i \cap [t+1]| \geq 2$ (we are assuming that such $i$ exists; this may not always be the case). Then*

$$\|\mathbf{M}_i\|_\infty \leq 1.$$

*Proof.* Firstly, if $|I_i \cap [t+1]|$ is even, then by the parity constraints (the variable symbol $x_i$ should appear an even number of times in $\boldsymbol{\mu}$), we must also have that $|I_i \cap [t+2, t+1+\ell]|$ is even. In this case, the conclusion would follow from Lemma 9.9. Hence from now on we assume that $|I_i \cap [t+1]|$ is odd. We hence have:

$$\mathbf{M}_{i,(y_i,\mathbf{w}_{I_i\cap[t+1]});(x,\mathbf{z}_{I_i\cap[t+1]})} = \prod_{j\in I_i\cap[t+2,t+1+\ell]} (-1)^{\langle y_i,x\rangle} \cdot \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(y_i,w_j);(x,z_j)}$$
$$= (-1)^{\langle y_i,x\rangle} \cdot \prod_{j\in I_i\cap[t+1]} Q^\dagger_{j,(y_i,w_j);(x,z_j)}.$$

The conclusion now follows by applying Lemma 3.23 with the following inputs:

- We will take $R = C = 2^n$, and $d = |I_i \cap [t+1]| \geq 2$. (In fact, $d \geq 3$ since $|I_i \cap [t+1]|$ is odd, but this will not matter for us.)
- The matrices will be $\left\{\mathbf{Q}_j^\dagger \in \mathbb{C}^{2^{n+a}\times 2^{n+a}}\right\}_{j\in I_i\cap[t+1]}$. Accordingly, we will have

  $$r_1 = \ldots = r_R = c_1 = \ldots = c_C = d'.$$

  These matrices are unitary so they have operator norm exactly 1.

- For each $y_i, x \in \{0,1\}^n$, the scalar $\gamma_{y_i,x}$ will be $(-1)^{\langle y_i, x\rangle}$, which clearly has magnitude 1.

$\square$

Finally, we can put these lemmas together to prove the bounds that we want:

**Lemma 9.11.** *Suppose $\boldsymbol{\mu}$ is a subtype with respect to $(\mathbb{C}^d)^{\otimes 2t+1} \otimes (\mathbb{C}^{d'})^{r'}$ with $b$ free variable symbols. Then we have $\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\|_\infty \leq 2^{-nt+nb}$.*

*Moreover, when $t = 1$, we must have $b = 0$ and hence $\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\|_\infty \leq 2^{-n}$.*

*Proof.* We first address the final claim about the $t = 1$ case. Indeed, a subtype with respect to $(\mathbb{C}^d)^{\otimes 2t+1} \otimes (\mathbb{C}^{d'})^{\otimes t+1} = (\mathbb{C}^d)^{\otimes 3} \otimes (\mathbb{C}^{d'})^{\otimes 2}$ cannot have free variable symbols. Definition 9.5 states that a free variable symbol of $\boldsymbol{\mu}$ could only appear in entry 3 of $\boldsymbol{\mu}$. But a free variable symbol must appear an even number of times (as specified by Definition 8.1), so in fact it cannot appear at all. Now let us turn to proving the desired bound.

Now let $\boldsymbol{\mu}'$ be defined as in the statement of Lemma 9.6 i.e. it is $\boldsymbol{\mu}$ but with free variable symbols removed. Then we would like to show:

$$\begin{aligned}
\|\Pi_{\boldsymbol{\mu}} \Xi \Pi_{\boldsymbol{\mu}}\|_\infty &\leq 2^{-nt+nb} \\
\Leftrightarrow \|\mathbf{A}\|_\infty^2 &\leq 2^{-nt+nb} \\
\Leftrightarrow \|\mathbf{B}_{\boldsymbol{\mu}}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{k+1})\|_\infty^2 &\leq 2^{nb} \\
\Leftrightarrow \left\|\mathbf{B}_{\boldsymbol{\mu}'}(\mathbf{Q}_1, \ldots, \mathbf{Q}_{k+1})\right\|_\infty &\leq 1. \text{ (Lemma 9.6)}
\end{aligned}$$

Let $\boldsymbol{\mu}'$ have $l$ variable symbols. As hinted at earlier, we will bound this by applying Lemma 3.22 to the matrices $\mathbf{M}_1, \ldots, \mathbf{M}_l$ and $\mathbf{T}$ defined with respect to $\boldsymbol{\mu}'$. The first precondition follows from Lemmas 9.7 and 9.8. To check the second precondition, we need only show that $\min(\|\mathbf{M}_1\|_\infty, \ldots, \|\mathbf{M}_l\|_\infty, \|\mathbf{T}\|_\infty) \leq 1$. For this, we have some light casework:

1. If at least one of $\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_{t+1}$ is fixed, then $J \cap [t+1]$ is nonempty, so it follows that $\|T\|_\infty \leq 1$ by Lemma 9.7.

2. Otherwise, all of $\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_{t+1}$ must be variable symbols. However, every variable symbol must appear at least twice and we only have $2t+1$ entries in total, so the total number of variable symbols must be $\leq t$. Therefore by the pigeonhole principle, some two of $\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_{t+1}$ are the same variable symbol i.e. there exists $i \in [l]$ such that $|I_i \cap [t+1]| \geq 2$. In this case, Lemma 9.10 tells us that $\|\mathbf{M}_i\|_\infty \leq 1$.

$\square$

### 9.3.1 Completing the $t = 1$ Case

In this section, we address the case of restricted strategies for $1 \mapsto 2$ oracular cloning games. This will of course be implied by our subsequent analysis in Section 9.4, but we present this case separately to emphasize that the $t = 1$ case can be finished off very easily in comparison to the $t > 1$ case.

**Theorem 9.12.** *Let $\mathfrak{F}$ be a $4t+2 = 6$-wise uniform family of functions from $\{0,1\}^n \to \{0,1\}$. Then for all $n$, we have*

$$\sup_{\mathsf{S} \in \mathcal{S}_{\text{rest}}} \omega_{\mathsf{S}}(\mathsf{G}_{\mathfrak{F},1}) \leq O(2^{-n}).$$

*Proof.* By Lemma 9.2, it suffices to show that for any subtype $\boldsymbol{\mu}$ we have $\|\Pi_{\boldsymbol{\mu}}\Xi\Pi_{\boldsymbol{\mu}}\|_\infty \leq O(2^{-n})$. This follows from Lemma 9.11, thus proving the theorem. $\square$

**Remark 14.** *Since the above proof relies on Lemma 9.2 rather than Lemma 9.3, it does not rely on the particular structure of the Choi state $\rho$ shared by the players. In other words, it really shows an upper bound on the value of a certain "oracular monogamy game".*

*In the forthcoming sections, to handle the case where $t > 1$, we will need to take the specific structure of the Choi state $\rho$ into account. (See Section 9.5 for a counterexample showing that this is necessary.)*

## 9.4 The $t > 1$ Case

### 9.4.1 Combinatorial Lemmas about Free Variable Symbols

In the case where $t > 1$, free variable symbols could exist, and as indicated by Lemma 9.11, they can blow up the operator norms we care about. To mitigate this, we establish some simple lemmas about free variable symbols:

**Definition 9.13.** *For any $l \in [t]$, define the projector $\Gamma_l$ over $(\mathbb{C}^d)^{\otimes r} \otimes (\mathbb{C}^{d'})^{\otimes(t+1)}$ as the projector onto*

$$W_l := \mathrm{span}_{\mathbb{C}}\{|(v_1, \ldots, v_r, a_1, \ldots, a_{t+1})\rangle \ : \ \textit{exactly } l \textit{ distinct values among } v_{t+2}, \ldots, v_r\}.$$

**Lemma 9.14.** *We have*

$$\sum_{b \leq t/2} \sum_{\boldsymbol{\mu} \text{ with } b \text{ free variable symbols}} 2^{nb}\Pi_{\boldsymbol{\mu}} \leq \exp(O(t \log t)) \cdot \sum_{l \leq t} 2^{n(t-l)}\Gamma_l,$$

*with respect to the PSD ordering.*

*Proof.* Note that the LHS and RHS are both diagonal in the standard basis. Hence it suffices to show for any $\mathbf{x} = (v_1, \ldots, v_r, a_1, \ldots, a_{t+1})$ that:

$$\sum_{b \leq t/2} \sum_{\boldsymbol{\mu} \text{ with } b \text{ free variable symbols}} 2^{nb} \langle \mathbf{x}|\Pi_{\boldsymbol{\mu}}|\mathbf{x}\rangle \leq \exp(O(t \log t)) \cdot \sum_{l \leq t} 2^{n(t-l)} \langle \mathbf{x}|\Gamma_l|\mathbf{x}\rangle \,.$$

Let $l^*$ be the number of distinct values among $v_{t+2}, \ldots, v_r$, then the RHS is $\exp(O(t \log t)) \cdot 2^{n(t-l^*)}$. On the other hand, the LHS is equal to:

$$\sum_{b \leq t/2} \sum_{\substack{\boldsymbol{\mu} \text{ with } b \text{ free variable symbols} \\ \mathbf{x} \in S_{\boldsymbol{\mu}}}} 2^{nb}.$$

Now consider any subtype $\boldsymbol{\mu}$ with $b$ free variable symbols such that $\mathbf{x} \in S_{\boldsymbol{\mu}}$. Each of its $b$ free variable symbols must appear at least twice among $v_{t+2}, \ldots, v_r$ due to the parity constraint, which implies that we must have $l^* \leq t - b \Leftrightarrow b \leq t - l^*$. Hence every term in the above sum is at most $2^{n(t-l^*)}$. Moreover, by Lemma 8.6, there are at most $\exp(O(t \log t))$ subtypes $\boldsymbol{\mu}$ with $\mathbf{x} \in S_{\boldsymbol{\mu}}$, so there are at most $\exp(O(t \log t))$ terms in the above sum. It follows that the LHS is at most $\exp(O(t \log t)) \cdot 2^{n(t-l^*)}$, which is exactly the RHS, as desired. $\square$

We make one more observation:

**Lemma 9.15.** *The number of tuples $(x_1, \ldots, x_t) \in [2^n]^t$ with $l$ distinct values is at most $\exp(t \log t) \cdot 2^{nl}$.*

*Proof.* There are at most $2^{nl}$ ways to choose the $l$ distinct values. Then there are $l^t \leq t^t = \exp(t \log t)$ ways to assign a value to each individual $x_i$. The conclusion follows. $\square$

Next, we present the only specific property of the shared state $\rho$ that we need. In the following, we partition the Hilbert space $(\mathbb{C}^d)^{\otimes r} \otimes (\mathbb{C}^{d'})^{\otimes t+1}$ as the tensor product of Hilbert spaces on the following systems:

- $\mathsf{R}_1$: this consists of the values $(v_{t+2}, \ldots, v_r)$. Thus $\mathcal{H}_{\mathsf{R}_1} \cong (\mathbb{C}^d)^{\otimes t}$.
- $\mathsf{R}_2$: all other values i.e. $(v_1, \ldots, v_{t+1}, a_1, \ldots, a_{t+1})$. Thus $\mathcal{H}_{\mathsf{R}_2} \cong (\mathbb{C}^d)^{\otimes t+1} \otimes (\mathbb{C}^{d'})^{\otimes t+1}$.

**Lemma 9.16.** *We have*

$$\mathrm{Tr}_{\mathsf{R}_2}[\rho] = 2^{-nt} \cdot \mathbb{I}_{\mathsf{R}_1}.$$

*Informally, if we take $\rho$ and trace out the system $\mathsf{R}_2$, we are left with a maximally mixed state.*

*Proof.* We have by definition that:

$$\begin{aligned}
\rho &= (\mathbb{I}_{\mathsf{R}_1} \otimes \Phi_{\mathsf{R}_2}) \left( |\mathsf{EPR}\rangle\langle\mathsf{EPR}|^{\otimes nt}_{\mathsf{R}_1,\mathsf{R}_2} \right) \\
&= 2^{-nt} \cdot \sum_{\mathbf{x},\mathbf{y} \in [2^n]^t} (\mathbb{I}_{\mathsf{R}_1} \otimes \Phi) \left( |\mathbf{x}\rangle\langle\mathbf{y}|_{\mathsf{R}_1} \otimes |\mathbf{x}\rangle\langle\mathbf{y}|_{\mathsf{R}_2} \right) \\
&= 2^{-nt} \cdot \sum_{\mathbf{x},\mathbf{y} \in [2^n]^t} |\mathbf{x}\rangle\langle\mathbf{y}|_{\mathsf{R}_1} \otimes \Phi(|\mathbf{x}\rangle\langle\mathbf{y}|)_{\mathsf{R}_2} \\
\Rightarrow \mathrm{Tr}_{\mathsf{R}_2}[\rho] &= 2^{-nt} \cdot \sum_{\mathbf{x},\mathbf{y} \in [2^n]^t} |\mathbf{x}\rangle\langle\mathbf{y}|_{\mathsf{R}_1} \cdot \mathrm{Tr}\left[\Phi(|\mathbf{x}\rangle\langle\mathbf{y}|)_{\mathsf{R}_2}\right] \\
&= 2^{-nt} \cdot \sum_{\mathbf{x} \in [2^n]^t} |\mathbf{x}\rangle\langle\mathbf{x}|_{\mathsf{R}_1},
\end{aligned}$$

which implies the conclusion. In the last step, we are using the fact that $\Phi$ is trace-preserving. $\square$

Finally, we put these two together to show the following:

**Lemma 9.17.** *For any integer $l \in [1, t]$, we have*

$$\mathrm{Tr}[\Gamma_l \rho] \leq \exp(t \log t) \cdot 2^{-nt+nl}.$$

*Proof.* We can clearly write

$$\Gamma_l = \Gamma'_{l,\mathsf{R}_1} \otimes \mathbb{I}_{\mathsf{R}_2},$$

where $\Gamma'_l$ is the projector onto standard basis vectors $|v_{t+2}, \ldots, v_r\rangle$ with exactly $l$ distinct values. We hence have:

$$\begin{aligned}
\mathrm{Tr}[\Gamma_l \rho] &= \mathrm{Tr}\left[\left(\Gamma'_{l,\mathsf{R}_1} \otimes \mathbb{I}_{\mathsf{R}_2}\right) \rho\right] \\
&= \mathrm{Tr}\left[\Gamma'_{l,\mathsf{R}_1} (\mathrm{Tr}_{\mathsf{R}_2} \rho)\right] \\
&= 2^{-nt} \cdot \mathrm{Tr}\left[\Gamma'_{l,\mathsf{R}_1}\right] \text{ (Lemma 9.16)} \\
&\leq \exp(t \log t) \cdot 2^{-nt+nl},
\end{aligned}$$

where in the last step we are using the fact that $\Gamma'_{l,\mathsf{R}_1}$ is a projector together with Lemma 9.15. $\square$

### 9.4.2 Putting Everything Together

In this section, we complete our treatment of the case of $t \mapsto t+1$ cloning games for $t > 1$. Our bounds here are once again independent of the number of ancilla qubits $a$ used by each player.

**Theorem 9.18.** *Let $\mathfrak{F}$ be a $(4t+2)$-wise uniform family of functions from $\{0,1\}^n \to \{0,1\}$. Then for all $n$, we have*

$$\sup_{\mathsf{S} \in \mathcal{S}_{\text{rest}}} \omega_{\mathsf{S}}(\mathsf{G}_{\mathfrak{F},t}) \le \exp(\exp(O(t \log t))) \cdot 2^{-n}.$$

*Proof.* For any strategy $\mathsf{S} \in \mathcal{S}_{\text{rest}}$, we have:

$$\begin{aligned}
\omega_{\mathsf{S}}(\mathsf{G}) &\le \exp(\exp(O(t\log t))) \cdot 2^{n(t-1)} \cdot \sum_{\boldsymbol{\mu}} \mathrm{Tr}\left[\Pi_{\boldsymbol{\mu}}\rho\right] \cdot \|\Pi_{\boldsymbol{\mu}}\,\Xi\,\Pi_{\boldsymbol{\mu}}\|_\infty \text{ (Lemma 9.3)} \\
&\le \exp(\exp(O(t\log t))) \cdot 2^{n(t-1)} \cdot \sum_{b \le t/2} \sum_{\boldsymbol{\mu} \text{ with } b \text{ free variable symbols}} 2^{-nt+nb} \cdot \mathrm{Tr}\left[\Pi_{\boldsymbol{\mu}}\rho\right] \text{ (Lemma 9.11)} \\
&\le \exp(\exp(O(t\log t))) \cdot 2^{-n} \cdot \sum_{l \le t} 2^{n(t-l)} \cdot \mathrm{Tr}\left[\Gamma_l \rho\right] \text{ (Lemma 9.14)} \\
&\le \exp(\exp(O(t\log t))) \cdot 2^{-n} \cdot \sum_{l \le t} 2^{n(t-l)} \cdot 2^{-nt+nl} \text{ (Lemma 9.17)} \\
&\le \exp(\exp(O(t\log t))) \cdot 2^{-n},
\end{aligned}$$

as desired. □

## 9.5 Limitations of Bounding the Operator Norm Directly

Recall that our high-level strategy was to bound:

$$2^{n(t-1)} \cdot \sum_{\boldsymbol{\lambda} \in \{0,1\}^d} \mathrm{Tr}\left[\Pi_{\boldsymbol{\lambda}}\Xi\Pi_{\boldsymbol{\lambda}}\rho\right] \le O_t(2^{n(t-1)}) \cdot \sum_{\boldsymbol{\mu}} \mathrm{Tr}\left[\Pi_{\boldsymbol{\mu}}\rho\right] \cdot \|\Pi_{\boldsymbol{\mu}}\Xi\Pi_{\boldsymbol{\mu}}\|_\infty .$$

One could instead attempt to emulate the [TFKW13] technique and ignore the state $\rho$ entirely, which would instead yield the following bound:

$$2^{n(t-1)} \cdot \sum_{\boldsymbol{\lambda} \in \{0,1\}^d} \mathrm{Tr}\left[\Pi_{\boldsymbol{\lambda}}\Xi\Pi_{\boldsymbol{\lambda}}\rho\right] \le 2^{n(t-1)} \cdot \left\| \sum_{\boldsymbol{\lambda} \in \{0,1\}^d} \Pi_{\boldsymbol{\lambda}}\Xi\Pi_{\boldsymbol{\lambda}} \right\|_\infty .$$

In fact, as noted in Remark 14, the analysis in Section 9.3.1 implies that this technique would suffice in the case where $t = 1$ and we are interested in $1 \mapsto 2$ security. However, in this section we will show by counterexample that this technique is insufficient for $t > 1$ (even if the players are only allowed one query and do not have any ancilla qubits). At a high level, this is due to the possibility of free variable symbols in subtypes (see Definition 9.5). We got around this in Section 9.4 by arguing that in subtypes $\boldsymbol{\mu}$ such that $\|\Pi_{\boldsymbol{\mu}}\Xi\Pi_{\boldsymbol{\mu}}\|_\infty$, the state $\rho$ does not place much weight on the image of $\Pi_{\boldsymbol{\mu}}$. In other words, we are crucially relying on the fact that the shared state $\rho$ must have a specific structure, as dictated by Lemma 9.16. The aim of this section is to prove that this more careful approach is *necessary*.

**Lemma 9.19.** *For simplicity, suppose $t > 1$ is even and $a = 0$ (i.e. the players do not have ancilla qubits). We also assume the players are still restricted to making only one query to $\mathsf{U}_f$. Then we have*

$$\left\| \sum_{\boldsymbol{\lambda} \in \{0,1\}^d} \Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}} \right\|_\infty \geq 2^{-nt/2}.$$

*Proof.* Since the projectors $\{\Pi_{\boldsymbol{\lambda}}\}$ are mutually orthogonal, we have

$$\left\| \sum_{\boldsymbol{\lambda} \in \{0,1\}^d} \Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}} \right\|_\infty = \max_{\boldsymbol{\lambda} \in \{0,1\}^d} \left\| \Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}} \right\|_\infty .$$

For each $i \in [t+1]$, set $Q_i = \mathbb{I}$. For each $x \in \{0,1\}^n$, we hence have:

$$|\Xi^x\rangle = |x\rangle^{\otimes(t+1)} \otimes (H^{\otimes n} |x\rangle)^{\otimes t}.$$

Now consider the following pure state (we could equivalently consider the density operator $\sigma := |\Psi\rangle\langle\Psi|$ and calculate $\operatorname{Tr}[\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}} \sigma]$):

$$|\Psi\rangle = \frac{1}{2^{nt/4}} \sum_{v_1, \ldots, v_{t/2} \in \{0,1\}^n} |0^n\rangle^{\otimes(t+1)} \otimes |v_1\rangle^{\otimes 2} \otimes |v_2\rangle^{\otimes 2} \otimes \ldots \otimes |v_{t/2}\rangle^{\otimes 2} .$$

Note that $|\Psi\rangle$ is entirely supported in the image of $\Pi_{\boldsymbol{\lambda}}$ where $\boldsymbol{\lambda} = (1, 0, 0, \ldots, 0)$. (Intuitively, we choose $|\Psi\rangle$ to be uniform over a subtype $\boldsymbol{\mu}$ of $\boldsymbol{\lambda}$ that has the maximum number $t/2$ of free variable symbols.) Then we have:

$$\begin{aligned}
\langle\Psi|\Pi_{\boldsymbol{\lambda}} \Xi \Pi_{\boldsymbol{\lambda}}|\Psi\rangle &= \langle\Psi|\Xi|\Psi\rangle \\
&= \sum_{x \in \{0,1\}^n} \langle\Psi|\Xi^x\rangle \langle\Xi^x|\Psi\rangle \\
&= \sum_{x \in \{0,1\}^n} |\langle\Psi|\Xi^x\rangle|^2 \\
&= \left|\langle\Psi|\Xi^{0^n}\rangle\right|^2 \\
&= \frac{1}{2^{nt/2}} \sum_{v_1, v_2, \ldots, v_{t/2} \in \{0,1\}^n} \left| \langle v_1|H^{\otimes n}|x\rangle^2 \cdot \ldots \cdot \langle v_{t/2}|H^{\otimes n}|x\rangle^2 \right| \\
&= \frac{1}{2^{nt/2}} \sum_{v_1, v_2, \ldots, v_{t/2} \in \{0,1\}^n} 2^{-nt/2} \\
&= 2^{-nt/2},
\end{aligned}$$

which implies the conclusion.

We remark that when $t$ is odd we can similarly show a bound of $2^{n(-1-t)/2}$ by taking

$$|\Psi\rangle = \frac{1}{2^{n(t-1)/4}} \sum_{v_1, \ldots, v_{(t-1)/2} \in \{0,1\}^n} |0^n\rangle^{\otimes(t+2)} \otimes |v_1\rangle^{\otimes 2} \otimes \ldots \otimes |v_{(t-1)/2}\rangle^{\otimes 2} .$$

$\square$

## References


[Aar09] Scott Aaronson. Quantum copy-protection and quantum money. In *2009 24th Annual IEEE Conference on Computational Complexity*, page 229–242. IEEE, July 2009. 2

[Aar16] Scott Aaronson. The complexity of quantum states and transformations: From quantum money to black holes, 2016. 8

[AEH+22] Chris Akers, Netta Engelhardt, Daniel Harlow, Geoff Penington, and Shreya Vardhan. The black hole interior from non-isometric codes and complexity, 2022. 8

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In Eike Kiltz and Vinod Vaikuntanathan, editors, *Theory of Cryptography - 20th International Conference, TCC 2022, Chicago, IL, USA, November 7-10, 2022, Proceedings, Part I*, volume 13747 of *Lecture Notes in Computer Science*, pages 237–265. Springer, 2022. 3, 5, 19, 57

[AIK22] Scott Aaronson, DeVon Ingram, and William Kretschmer. The acrobatics of BQP. In Shachar Lovett, editor, *37th Computational Complexity Conference, CCC 2022, July 20-23, 2022, Philadelphia, PA, USA*, volume 234 of *LIPIcs*, pages 20:1–20:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. 12

[AK21] Prabhanjan Ananth and Fatih Kaleoglu. Unclonable encryption, revisited. In Kobbi Nissim and Brent Waters, editors, *Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part I*, volume 13042 of *Lecture Notes in Computer Science*, pages 299–329. Springer, 2021. 19

[AKL+22] Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. On the feasibility of unclonable encryption, and more. In *Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II*, page 212–241, Berlin, Heidelberg, 2022. Springer-Verlag. 2, 12, 20

[AKL23] Prabhanjan Ananth, Fatih Kaleoglu, and Qipeng Liu. Cloning games: A general framework for unclonable primitives. In *Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part V*, page 66–98, Berlin, Heidelberg, 2023. Springer-Verlag. 2, 12, 15

[AKY24] Prabhanjan Ananth, Fatih Kaleoglu, and Henry Yuen. Simultaneous Haar indistinguishability with applications to unclonable cryptography. *CoRR*, abs/2405.10274, 2024. 12, 14, 15

[AMP24] Prabhanjan Ananth, Saachi Mutreja, and Alexander Poremba. Revocable encryption, programs, and more: The case of multi-copy security, 2024. 3, 4, 12, 43

[AMPS13] Ahmed Almheiri, Donald Marolf, Joseph Polchinski, and James Sully. Black holes: complementarity or firewalls? *Journal of High Energy Physics*, 2013(2), February 2013. 7, 8

[AMR19] Gorjan Alagic, Christian Majenz, and Alexander Russell. Efficient simulation of random states and random unitaries. Cryptology ePrint Archive, Paper 2019/1204, 2019. 27

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 208–236, Cham, 2022. Springer Nature Switzerland. 3

[Ara02] P. K. Aravind. Bell's theorem without inequalities and only two distant observers, 2002. 1

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984. 2

[BCKM21] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 467–496. Springer, 2021. 12, 14

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the Computational Hardness Needed for Quantum Cryptography. In Yael Tauman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:21, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. 3

[BDPA11] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. The keccak sha-3 submission. Submission to NIST (Round 3), 2011. 11

[Bek72] J. D. Bekenstein. Black holes and the second law. *Lett. Nuovo Cim.*, 4:737–740, 1972. 7

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1:195–200, November 1964. 1

[BEM$^+$23] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary complexity and the uhlmann transformation problem, 2023. 8

[BHHP24] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. Efficient quantum pseudorandomness from hamiltonian phase states, 2024. 12

[BKL23] Anne Broadbent, Martti Karvonen, and Sébastien Lord. Uncloneable quantum advice, 2023. 12

[BL20] Anne Broadbent and Sébastien Lord. Uncloneable Quantum Encryption via Oracles. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:22, Dagstuhl, Germany, 2020. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. 2, 3, 12, 13, 14, 15, 16, 20, 22, 23, 41, 43, 44

[Bra23] Zvika Brakerski. Black-hole radiation decoding is quantum cryptography. In *Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part V*, page 37–65, Berlin, Heidelberg, 2023. Springer-Verlag. 8

[BS19] Zvika Brakerski and Omri Shmueli. (pseudo) random quantum states with binary phase, 2019. 5, 12, 19

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, October 1969. 1, 8

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 556–584, Cham, 2021. Springer International Publishing. 2, 3, 13, 43

[CMP22] Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model, 2022. 2, 12

[Col23] Andrea Coladangelo. Quantum trapdoor functions from classical one-way functions. Cryptology ePrint Archive, Paper 2023/282, 2023. 5

[CP24] Joseph Carolan and Alexander Poremba. Quantum one-wayness of the single-round sponge with invertible permutations. In *Advances in Cryptology – CRYPTO 2024: 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2024, Proceedings, Part VI*, page 218–252, Berlin, Heidelberg, 2024. Springer-Verlag. 11

[CPZ24] Joseph Carolan, Alexander Poremba, and Mark Zhandry. (quantum) indifferentiability and precomputation, 2024. 11

[CV22] Eric Culf and Thomas Vidick. A monogamy-of-entanglement game for subspace coset states. *Quantum*, 6:791, September 2022. 3

[EFL+24] Netta Engelhardt, Asmund Folkestad, Adam Levine, Evita Verheijden, and Lisa Yang. Cryptographic censorship, 2024. 4, 7, 8, 9, 13

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935. 1

[EW01] T. Eggeling and R. F. Werner. Separability properties of tripartite states with $u \bigotimes u \bigotimes u$ symmetry. *Phys. Rev. A*, 63:042111, Mar 2001. 17

[GBO23] Dmitry Grinko, Adam Burchardt, and Maris Ozols. Gelfand-tsetlin basis for partially transposed permutations, with applications to quantum information, 2023. 17

[GHZ89] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. *Going Beyond Bell's Theorem*, pages 69–72. Springer Netherlands, Dordrecht, 1989. 1

[GLSV21] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 531–561. Springer, 2021. 12, 14

[GMR23] Vipul Goyal, Giulio Malavolta, and Justin Raizes. Unclonable commitments and proofs. Cryptology ePrint Archive, Paper 2023/1538, 2023. 2, 12, 14

[GO23] Dmitry Grinko and Maris Ozols. Linear programming with unitary-equivariant constraints, 2023. 17

[GZ20] Marios Georgiou and Mark Zhandry. Unclonable decryption keys. Cryptology ePrint Archive, Paper 2020/877, 2020. 2, 12, 14

[Haf22] Jonas Haferkamp. Random quantum circuits are approximate unitary t-designs in depth o(nt5+o(1)). *Quantum*, 6:795, 2022. 17

[Har93] Lucien Hardy. Nonlocality for two particles without inequalities for almost all entangled states. *Phys. Rev. Lett.*, 71:1665–1668, September 1993. 1

[Haw76] S. W. Hawking. Breakdown of predictability in gravitational collapse. *Phys. Rev. D*, 14:2460–2473, November 1976. 5, 6, 7

[HH13] Daniel Harlow and Patrick Hayden. Quantum computation vs. firewalls. *Journal of High Energy Physics*, 2013(6), June 2013. 7, 8, 9

[HP07] Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 2007(09):120, September 2007. 4, 5, 7, 8, 9, 11, 35

[Imp95] R. Impagliazzo. A personal view of average-case complexity. In *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*, pages 134–147, 1995. 12, 14

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. Cryptology ePrint Archive, Paper 2018/544, 2018. `https://eprint.iacr.org/2018/544`. 5, 12, 19, 27

[JNV+21] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP* = RE. *Commun. ACM*, 64(11):131–138, October 2021. 1

[KLVY23] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 1617–1628, New York, NY, USA, 2023. Association for Computing Machinery. 1

[Kni00] E. Knill. Approximation by quantum circuits. August 2000. 7

[KP23] Isaac H. Kim and John Preskill. Complementarity and the unitarity of the black hole S-matrix. *Journal of High Energy Physics*, 2023(2), February 2023. 4, 7, 8, 9, 13

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 1589–1602. ACM, 2023. 12, 14

[Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. In Min-Hsiu Hsieh, editor, *16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference*, volume 197 of *LIPIcs*, pages 2:1–2:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. 3, 12, 27

[KT23] Srijita Kundu and Ernest Y. Z. Tan. Device-independent uncloneable encryption, 2023. 12, 15

[Mel24] Antonio Anna Mele. Introduction to Haar Measure Tools in Quantum Information: A Beginner's Tutorial. *Quantum*, 8:1340, May 2024. 25

[Mer90] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65:3373–3376, December 1990. 1

[MH24] Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. Cryptology ePrint Archive, Paper 2024/1652, 2024. 12, 14, 17, 27, 28

[MPSY24] Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries. *CoRR*, abs/2404.12647, 2024. 3, 4, 5, 12, 14, 17, 27

[MY22] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part I*, volume 13507 of *Lecture Notes in Computer Science*, pages 269–295. Springer, 2022. 12, 14

[NC16] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary edition)*. Cambridge University Press, 2016. 23, 48

[O'D21] Ryan O'Donnell. Analysis of boolean functions. *CoRR*, abs/2105.10386, 2021. 54

[PQS24] Alexander Poremba, Yihui Quek, and Peter Shor. The learning stabilizers with noise problem, 2024. 12

[Pre92] John Preskill. Do black holes destroy information? In *International Symposium on Black holes, Membranes, Wormholes and Superstrings*, January 1992. 5, 6

[RUV12] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games, 2012. 1

[SHH24] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. Random unitaries in extremely low depth. *CoRR*, abs/2407.07754, 2024. 17

[Sho18] Peter W. Shor. Scrambling time and causal structure of the photon sphere of a Schwarzschild black hole, 2018. 7

[Sim95] Barry Simon. Representations of finite and compact groups. 1995. 25

[SS08] Yasuhiro Sekino and L. Susskind. Fast scramblers. *Journal of High Energy Physics*, 2008(10):065, October 2008. 7

[STU93] Leonard Susskind, Lárus Thorlacius, and John Uglum. The stretched horizon and black hole complementarity. *Phys. Rev. D*, 48:3743–3761, October 1993. 7, 8, 9

['t 85] Gerard 't Hooft. On the quantum structure of a black hole. *Nuclear Physics B*, 256:727–745, 1985. 7, 8, 9

[Ter04] B. M. Terhal. Is entanglement monogamous? *IBM Journal of Research and Development*, 48(1):71–78, 2004. 1

[TFKW13] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, October 2013. i, 1, 2, 3, 5, 8, 10, 16, 17, 18, 19, 21, 22, 23, 36, 43, 44, 46, 51, 52, 56, 57, 64, 73

[Web16] Zak Webb. The clifford group forms a unitary 3-design, 2016. 25

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. 1

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982. 1, 2, 7, 12

[Zha21a] Mark Zhandry. How to construct quantum random functions. *J. ACM*, 68(5), August 2021. 19

[Zha21b] Mark Zhandry. Quantum lightning never strikes the same state twice. or: Quantum money from cryptographic assumptions. *J. Cryptol.*, 34(1):6, 2021. 14


# A Monogamy of Entanglement Games and $1 \mapsto 2$ Cloning Games

In this section, we show that $1 \mapsto 2$ cloning games are in fact equivalent to a particular variant of a monogamy of entanglement game from Section 6.1, where

- The tripartite state $\rho \in \mathcal{D}(\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}})$ which is shared between Alice, Bob and Charlie is the result of applying a cloning channel $\Phi_{\mathsf{A}' \to \mathsf{BC}}$ to one half of an EPR pair, i.e.,

$$\rho_{\mathsf{ABC}} = (\mathbb{I}_{\mathsf{A}} \otimes \Phi_{\mathsf{A}' \to \mathsf{BC}})(|\mathsf{EPR}\rangle\langle\mathsf{EPR}|_{\mathsf{AA}'}).$$

  In other words, $\rho_{\mathsf{ABC}}$ is the normalized Choi state of some channel $\Phi_{\mathsf{A}' \to \mathsf{BC}}$.

- Alice's measurement $\{\mathbf{A}_x^\theta\}_{\theta \in \Theta, x \in \mathcal{X}}$ on register $\mathsf{A}$ is a projective measurement of the form

$$\mathbf{A}_x^\theta = \bar{U}_\theta \, |x\rangle\langle x| \, \bar{U}_\theta^\dagger \,,$$

  for some family of unitary operators $\{U_\theta\}_{\theta \in \Theta}$ acting on $\mathcal{H}_{\mathsf{A}}$.

- (If we are in the oracular setting) Bob and Charlie's measurements can only depend on oracle queries to $U_\theta$ and $U_\theta^\dagger$, rather than directly on $\theta$.

We now prove a formal equivalence between the two notions.

**Lemma A.1.** *Let $\mathsf{G}_{1\mapsto 2} = (1, \mathcal{H}_{\mathsf{A}}, \Theta, \mathcal{X}, \{U_\theta\}_{\theta \in \Theta})$ be a $1 \mapsto 2$ cloning game, for some family of unitary operators $\{U_\theta\}_{\theta \in \Theta}$ acting on the Hilbert space $\mathcal{H}_{\mathsf{A}}$. Then, the winning probability of a particular strategy $\mathsf{S} = (\mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}}, \Phi_{\mathsf{A} \to \mathsf{BC}}, \{\mathbf{P}_{1,x}^\theta\}_{\theta \in \Theta, x \in \mathcal{X}}, \{\mathbf{P}_{2,x}^\theta\}_{\theta \in \Theta, x \in \mathcal{X}})$ (possibly in the oracular setting) with*

$$\omega_{\mathsf{S}}(\mathsf{G}_{1\mapsto 2}) = \mathop{\mathbb{E}}_{\theta \sim \Theta} \mathop{\mathbb{E}}_{x \sim \mathcal{X}} \mathrm{Tr}\left[\left(\mathbf{P}_{1,x}^\theta \otimes \mathbf{P}_{2,x}^\theta\right) \Phi_{\mathsf{A} \to \mathsf{BC}}(U_\theta \, |x\rangle\langle x|_{\mathsf{A}} \, U_\theta^\dagger)\right].$$

*is exactly equal to the winning probability*

$$\omega_{\tilde{\mathsf{S}}}(\mathsf{G}) = \mathop{\mathbb{E}}_{\theta\sim\Theta} \sum_{x\in\mathcal{X}} \mathrm{Tr}\left[\left(\mathbf{P}^{\theta}_{1,x} \otimes \mathbf{P}^{\theta}_{2,x} \otimes (\bar{U}_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} \bar{U}^{\dagger}_{\theta})\right) \rho_{\mathsf{BCA}}\right].$$

*of a quantum strategy* $\tilde{\mathsf{S}} = (\mathcal{H}_{\mathsf{B}}, \mathcal{H}_{\mathsf{C}}, \rho_{\mathsf{BCA}}, \{\mathbf{P}^{\theta}_{1,x}\}_{\theta\in\Theta,x\in\mathcal{X}}, \{\mathbf{P}^{\theta}_{2,x}\}_{\theta\in\Theta,x\in\mathcal{X}})$ *(possibly in the oracular setting) of a monogamy entanglement game* $\mathsf{G} = (\mathcal{H}_{\mathsf{A}}, \Theta, \mathcal{X}, \{\bar{U}_\theta \left|x\right\rangle\!\left\langle x\right| \bar{U}^{\dagger}_{\theta}\}_{\theta\in\Theta,x\in\mathcal{X}})$*, where*

$$\rho_{\mathsf{BCA}} = (\Phi_{\mathsf{A}'\to\mathsf{BC}} \otimes \mathbb{I}_{\mathsf{A}}) \left|\mathsf{EPR}\right\rangle\!\left\langle\mathsf{EPR}\right|_{\mathsf{A}'\mathsf{A}}.$$

*Here,* $\left|\mathsf{EPR}\right\rangle_{\mathsf{AA}'}$ *denotes* $\frac{1}{\sqrt{|\mathcal{X}|}}\sum_{x\in\mathcal{X}} \left|x\right\rangle_{\mathsf{A}} \otimes \left|x\right\rangle_{\mathsf{A}'}$. *(We swap the* $\mathsf{A}$ *and* $\mathsf{BC}$ *registers in the formulation of the relevant monogamy game for the purposes of syntactic compliance with Corollary 3.2 in our proof.)*

*Proof.* Recall that Corollary 3.2 implies that, for any projector $\mathbf{P} \in L(\mathcal{H}_{\mathsf{BC}})$,

$$\mathrm{Tr}\left[\mathbf{P}_{\mathsf{BC}}\Phi_{\mathsf{A}'\to\mathsf{BC}}(U_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} U^{\dagger}_{\theta})\right] = \mathrm{Tr}\left[\left(\mathbf{P} \otimes \bar{U}_\theta \left|x\right\rangle\!\left\langle x\right| \bar{U}^{\dagger}_{\theta}\right) J(\Phi)\right],$$

where $J(\Phi) \in \mathrm{L}(\mathcal{H}_{\mathsf{B}} \otimes \mathcal{H}_{\mathsf{C}} \otimes \mathcal{H}_{\mathsf{A}})$ is the Choi-Jamiołkowski isomorphism of $\Phi$. Therefore:

$$\begin{aligned}
\omega_{\mathsf{S}}(\mathsf{G}_{1\mapsto 2}) &= \mathop{\mathbb{E}}_{\theta\sim\Theta} \mathop{\mathbb{E}}_{x\sim\mathcal{X}} \mathrm{Tr}\left[\left(\mathbf{P}^{\theta}_{1,x} \otimes \mathbf{P}^{\theta}_{2,x}\right) \Phi_{\mathsf{A}\to\mathsf{BC}}(U_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} U^{\dagger}_{\theta})\right] \\
&= \mathop{\mathbb{E}}_{\theta\sim\Theta} \mathop{\mathbb{E}}_{x\sim\mathcal{X}} \mathrm{Tr}\left[\left(\mathbf{P}^{\theta}_{1,x} \otimes \mathbf{P}^{\theta}_{2,x} \otimes (\bar{U}_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} \bar{U}^{\dagger}_{\theta})\right) J(\Phi)\right] \\
&= \mathop{\mathbb{E}}_{\theta\sim\Theta} \sum_{x\sim\mathcal{X}} \mathrm{Tr}\left[\left(\mathbf{P}^{\theta}_{1,x} \otimes \mathbf{P}^{\theta}_{2,x} \otimes (\bar{U}_\theta \left|x\right\rangle\!\left\langle x\right|_{\mathsf{A}} \bar{U}^{\dagger}_{\theta})\right) \rho_{\mathsf{BCA}}\right] \;=\; \omega_{\tilde{\mathsf{S}}}(\mathsf{G}),
\end{aligned}$$

where we define $\rho_{\mathsf{BCA}} = (\Phi_{\mathsf{A}'\to\mathsf{BC}} \otimes \mathbb{I}_{\mathsf{A}}) \left|\mathsf{EPR}\right\rangle\!\left\langle\mathsf{EPR}\right|_{\mathsf{A}'\mathsf{A}}$. The final step holds because of the identity $J(\Phi) = |\mathcal{X}| \cdot \rho_{\mathsf{BCA}}$ (see the definitions preceding Lemma 3.1). This proves the claim. $\square$