


# Cloning Games, Black Holes and Cryptography

Alexander Poremba ✉ 🏠 

Department of Computer Science and Department of Physics, Boston University, MA, USA

Seyoon Ragavan ✉ 🏠 

Department of Computer Science, MIT, Cambridge, MA, USA

Vinod Vaikuntanathan ✉ 🏠 

Department of Computer Science, MIT, Cambridge, MA, USA

---

## Abstract

In this work, we introduce a new toolkit for analyzing *cloning games*, a notion that captures stronger and more quantitative versions of the celebrated quantum no-cloning theorem. This framework allows us to analyze a new cloning game based on *binary phase states*. Our results provide evidence that these games may be able to overcome important limitations of previous candidates based on BB84 states and subspace coset states: in a model where the adversaries are restricted to making a single oracle query, we show that the binary phase variant is  $t$ -copy secure when  $t = o(n/\log n)$ . Moreover, for constant  $t$ , we obtain the *first* optimal bounds of  $O(2^{-n})$ , asymptotically matching the value attained by a trivial adversarial strategy. We also show a worst-case to average-case reduction which allows us to show the same quantitative results for the new and natural notion of *Haar cloning games*.

Our analytic toolkit, which we believe will find further applications, is based on binary subtypes and uses novel bounds on the operator norms of block-wise tensor products of matrices. To illustrate the effectiveness of these new techniques, we present two applications: first, in black-hole physics, where our asymptotically optimal bound offers quantitative insights into information scrambling in idealized models of black holes; and second, in unclonable cryptography, where we (a) construct succinct unclonable encryption schemes from the existence of pseudorandom unitaries, and (b) propose and provide evidence for the security of multi-copy unclonable encryption schemes.

**2012 ACM Subject Classification** Theory of computation → Cryptographic primitives

**Keywords and phrases** Unclonable cryptography, quantum pseudorandomness, black hole physics

**Digital Object Identifier** 10.4230/LIPIcs.ITCS.2026.109

**Related Version** *Full Version*: <https://arxiv.org/abs/2411.04730>

**Funding** *Alexander Poremba*: Supported by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Co-design Center for Quantum Advantage (C2QA) under contract number DE-SC0012704.

*Seyoon Ragavan*: Supported by an Akamai Presidential Fellowship, the grants of the third author, and the Defense Advanced Research Projects Agency (DARPA) under Contract No. HR0011-25-C-0300. Partially supported by Jane Street.

*Vinod Vaikuntanathan*: 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.

**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.



© Alexander Poremba, Seyoon Ragavan, and Vinod Vaikuntanathan;  
licensed under Creative Commons License CC-BY 4.0

17th Innovations in Theoretical Computer Science Conference (ITCS 2026).

Editor: Shubhangi Saraf; Article No. 109; pp. 109:1–109:21

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

## 1 Introduction

*Quantum no-cloning* [59] is one of the most fundamental properties of quantum information. Roughly speaking, it states that no quantum procedure can create an exact copy of an arbitrary unknown quantum state. The principle of no-cloning has profound implications in quantum information processing [13, 15, 50, 26] and has even inspired entirely new cryptographic primitives, starting with Wiesner’s remarkable quantum money scheme [58] and many subsequent primitives which are collectively known as *unclonable cryptography* [51]; these include unclonable quantum encryption [19, 6, 42, 7], encryption with unclonable decryption keys [31, 9], quantum copy-protection [5, 25, 24], unclonable commitments and proofs [32], and many more.

These cryptographic applications require one to prove unclonability guarantees that are much stronger than those implied by the no-cloning theorem, or even stronger variants stating that an unknown quantum state cannot be approximately copied to high fidelity [20, 47]. Take the example of *unclonable encryption*, where a classical message is encrypted into a quantum state, which an adversarial cloner  $\Phi$  then operates on arbitrarily and forwards to two isolated adversaries  $\mathcal{B}$  and  $\mathcal{C}$ . Later, the decryption key is revealed and  $\mathcal{B}$  and  $\mathcal{C}$  attempt to recover the original message; they win if they both succeed. The adversaries will certainly succeed if  $\Phi$  can clone a ciphertext state, but  $\Phi$  could also conceivably succeed by generating two completely different states that merely reveal enough information to later decrypt. The no-cloning theorem and even its approximate variants can only rule out the first type of attack.

### 1.1 Cloning Games

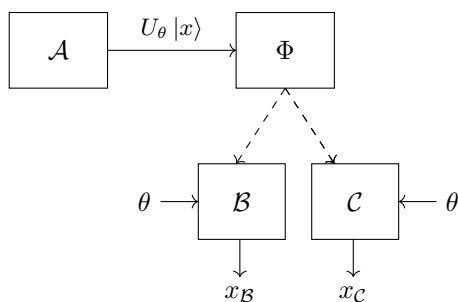
Following a long-standing tradition of studying quantum mechanical phenomena through the lens of interactive games [45, 33, 49, 56, 39], the field of unclonable cryptography today relies on abstract *cloning games* [6] as a means of capturing the desired strong unclonability guarantees. These types of games first emerged in the context of unclonable encryption schemes [19] but the general framework<sup>1</sup> also applies to many other fundamental unclonable primitives, such as copy-protection, single-decryptor encryption, quantum money, and more [6].

A basic  $1 \mapsto 2$  cloning game  $G_{1 \mapsto 2}$  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  $U_\theta |x\rangle_A$  to the cloner  $\Phi$ .  
The cloner  $\Phi$  splits the state into two registers  $B$  and  $C$ , 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.

---

<sup>1</sup> We note that our notion of a basic cloning game is slightly more specific than the general framework studied in [6]; we discuss these differences in more detail in Remark 8 of the full version.



■ **Figure 1** A basic  $1 \mapsto 2$  cloning game.

We illustrate the cloning game  $G_{1 \mapsto 2}$  in Figure 1. Formally, a strategy  $S$  for the game  $G_{1 \mapsto 2}$  consists of a cloning map  $\Phi$  and 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* of a particular strategy  $S$  for the cloning game  $G_{1 \mapsto 2}$  is defined as the average winning probability

$$\omega_S(G_{1 \mapsto 2}) = \mathbb{E}_{\theta \sim \Theta} \mathbb{E}_{x \sim \mathcal{X}} \text{Tr} \left[ (\mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta) \Phi_{A \rightarrow BC}(U_\theta |x\rangle \langle x|_A U_\theta^\dagger) \right].$$

Here,  $\omega(G_{1 \mapsto 2})$  denotes the optimal winning probability over all strategies specified by  $\Phi$ ,  $\mathcal{B}$  and  $\mathcal{C}$ . Note that there exists a trivial strategy that succeeds with probability  $1/|\mathcal{X}|$ : the cloner  $\Phi$  simply forwards  $U_\theta |x\rangle$  to Bob, who can easily recover  $x$  once  $\theta$  becomes available, whereas Charlie simply guesses at random.

► **Remark 1 (Cloning games capture much stronger forms of no-cloning).** At first glance, it appears that establishing an upper bound on the winning probability of Bob and Charlie just boils down to the no-cloning theorem [59] or perhaps its approximate variant [20]. Indeed, if the cloner  $\Phi$  can copy the state  $U_\theta |x\rangle$ , then  $\Phi$  can certainly also send the two copies to Bob and Charlie and ensure that they win the game. However, there could be other strategies which do not involve direct cloning but may nevertheless provide the players with enough information to win the game.<sup>2</sup> In fact, the only property of  $U_\theta |x\rangle$  that  $\Phi$  needs to clone are the measurement statistics with respect to the unknown basis specified by  $\theta$  (or more weakly, just  $x$  itself). As it turns out, this stronger notion of unclonability is required for most applications in unclonable cryptography [51], and is significantly more challenging to prove.

To this day, the majority of unclonable cryptography is rooted in either  $n$ -qubit BB84 states where  $U_\theta = H^\theta$  [56, 19] or subspace coset states over  $\mathbb{F}_2^n$ , where  $U_\theta$  encodes a shift of a random  $n/2$ -dimensional subspace  $A \subset \mathbb{F}_2^n$  [24, 27, 52]. In both cases, the optimal winning probability for the corresponding cloning game decays exponentially in the number of qubits [19, 27, 52].

## 1.2 Our Contributions

Despite extensive study and multiple successful applications in unclonable cryptography, several important gaps in our understanding of cloning games remain. Our contributions to this effect are several fold:

<sup>2</sup> We provide an example of such a game and strategy at the beginning of Section 2.1.

1. We show that existing techniques for analyzing cloning games are severely limited; in particular, they prevent us from making progress on many fundamental open questions in the field. We formally expose these limitations with counterexamples and concrete, quantitative proofs.
2. We study new cloning games and develop a suite of techniques for analyzing them; these techniques allow us to circumvent some of the limitations of previous approaches (in some cases, at the expense of restricting Bob’s and Charlie’s access to  $\theta$  down to only a single query to  $U_\theta$  or  $U_\theta^\dagger$ ).
3. Finally, we present two applications of our results which have previously been out of reach; one in the area of *black hole physics* and one in the field of *unclonable cryptography*. Both of these applications provably require us to overcome several technical barriers which are inherent in prior work.

We now discuss each of these contributions in more detail.

### Exposing Limitations on Cloning Games

Our first contribution is to expose several important gaps in our understanding of cloning games; more importantly, we also show that existing techniques for analyzing cloning games appear fundamentally insufficient at addressing them. We list some of these gaps below:

1. **Optimal games:** Prior work on cloning games over  $\mathcal{X} = \{0, 1\}^n$  has shown the upper bounds of  $\cos^2(\frac{\pi}{8})^n$  and  $2^{-n/4}$  in the case of BB84 states [56] and subspace coset states [27, 52], 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 admit no non-trivial strategies and have asymptotically optimal bounds of the form  $O(2^{-n})$ ? Closing this gap is not merely an intellectual and aesthetic curiosity; it has important consequences for an application of cloning games to black hole physics which we introduce and study in our work. We outline this application in Section 1.3 of the full version.

Not only are all known cloning games far from optimal, we prove that existing techniques can at best only produce upper bounds of the form  $2^{-n/2}$ . We discuss this limitation in detail in Section 2.1.

2. **Unclonable encryption in MicroCrypt:** A number of recent works [41, 10, 3, 17] showed how to build quantum cryptography from *pseudorandom states and unitaries*, which exist in “MicroCrypt” and are potentially even weaker than one-way functions [41]. To this day, however, the worlds of unclonable cryptography and MicroCrypt have been somewhat disconnected<sup>3</sup>, as was recently observed in [46, 8]. Do pseudorandom unitaries, which have so far eluded major cryptographic application, give rise to interesting unclonable cryptography?

The analysis of *Haar cloning games*, where  $U_\theta$  is a *Haar* unitary (or, a unitary sampled from a unitary design), seems far beyond the scope of existing techniques, as we explain in Sections 2.1 and 2.2.

3. **Multi-copy games:** Can we extend  $1 \mapsto 2$  cloning games to  $t \mapsto t + 1$  cloning games, where the cloner  $\Phi$  receives  $t$  many copies  $(U_\theta |x\rangle)^{\otimes t}$  and where  $t + 1$  players  $\mathcal{P}_1, \dots, \mathcal{P}_{t+1}$  simultaneously seek to recover  $x$ ? Although multi-copy variants of no-cloning have been

---

<sup>3</sup> This is with the notable exception of private-key quantum money, which is implied by pseudorandom states [38].

studied before [57], these are far from sufficient to understand multi-copy cloning games, as we previously noted in Remark 1. The natural notion of multi-copy games was raised as an open problem in [46, 8], where the latter initiated the study of multi-copy security in the context of revocable cryptography.

Not only is prior work limited to  $1 \mapsto 2$  cloning games, all existing unclonable cryptography is based on *highly learnable* classes of states and becomes **completely insecure** if  $t$  is allowed to grow polynomially in the number of qubits; this is in stark contrast with most quantum states which require exponentially many copies to be learned, as the literature on quantum tomography suggests [11]. We discuss the limitations of current approaches in Section 2.1 and provide strong evidence that existing techniques seem fundamentally insufficient for analyzing multi-copy games more generally.

We remark that prior works [43, 21] studied a variant of multi-copy security in the context of quantum copy-protection and unclonable decryption, where each “copy” of the program or key is an i.i.d. *mixed* state, and thus effectively an independent sample rather than an identical copy of a *pure state*. While this setting allows one to generically reduce notions of multi-copy security to  $1 \mapsto 2$  security (using a “quantum pigeonhole argument”), it fails to capture the natural – and significantly more *quantum* – notion of identical pure state copies; in particular, the same techniques do not carry over in this setting. The pure state notion of unclonability is clearly more desirable in practice; not only does it allow one to send copies of the *same* exact state to multiple recipients without compromising security, many identical copies also allow the recipients to approximately *reflect* around the state [54], thereby offering an additional “public verification feature” which is unavailable for mixed states, and which has found many use-cases in unclonable cryptography [12, 8].

4. **Applications beyond cryptography:** While cloning games appear quite fundamental, their use case has so far been limited to 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 [37, 40, 30], which raises the question: can cloning games with Haar random unitaries help us understand how information gets scrambled inside of a black hole?

An application to black hole physics once again seems to require new insights into *Haar cloning games* which, as mentioned before, are currently out of reach. We refer to Sections 2.1 and 2.2.

Given these inherent limitations on cloning games, it seems that fundamentally new techniques are needed in order to advance the field. This is where our next contribution comes in.

## A New Suite of Techniques for Analyzing Cloning Games

Our approach towards overcoming both limitations 1 and 3 is to focus on entirely new cloning games altogether. Inspired by the recent literature on pseudorandom quantum states [38, 18, 23], we study a cloning game based on *binary phase states*. The pseudorandomness of these states makes them excellent candidates for multi-copy unclonability [57], in the sense of a traditional no-cloning theorem. In order to extend this to a stronger cloning game bound as discussed in Remark 1, we take the existing formalism of binary types [3] and extend it to a new notion of binary *subtypes*, proving new standalone spectral bounds along the way. For technical reasons, our results only apply to a restricted model: rather than receiving the

string  $\theta$  in the clear, each player receives oracle access and is allowed to make a single query to either  $U_\theta$  or  $U_\theta^\dagger$ . While this constitutes a weaker model, it already implies something much stronger than a conventional  $t \mapsto t + 1$  no-cloning bound.<sup>4</sup>

Ultimately, we prove the following theorem (see Section 2.3 for more details):

► **Theorem 2** (Informal, see Theorem 5.15 of the full version for a formal statement). *Let  $n, t \in \mathbb{N}$ . Then, the one-query  $t \mapsto t + 1$  binary phase cloning game  $\mathsf{G}_{t \mapsto t+1}$  over  $\mathcal{X} = \{0, 1\}^n$ , where each of the players is allowed to make one oracle query, has a value of  $\omega(\mathsf{G}_{t \mapsto t+1}) \leq \exp(O(t \log t)) \cdot 2^{-n}$ .*

For constant  $t$ , this is asymptotically optimal and thus overcomes limitation 1. For  $t = o(n/\log n)$ , this is still negligible in  $n$  and thus makes significant progress towards overcoming limitation 3. However, we believe that this construction is plausibly secure when  $t$  is *any* polynomial in  $n$  (unlike previous constructions based on BB84 [56, 19] and coset states [24, 27, 52]), and view our results as providing evidence towards this conjecture. Our justification for the plausible security of this construction is the fact that binary phase states are pseudorandom [38, 18] and hence multi-copy unclonable [57]. We discuss our binary phase state construction more in Section 2.3.

Secondly, we study the new and natural notion of a *Haar cloning game*. Here, the unitary  $U_\theta$  is sampled according to the *Haar measure* and the players receive oracle access to  $U_\theta$  and  $U_\theta^\dagger$ . We show that the Haar cloning game is the *hardest* cloning game by exhibiting a *worst-case to average-case reduction*; this allows us to use an upper bound on the value of *any* cloning game, including our binary phase state game, in order to bound the value of the Haar cloning game. As a consequence, we additionally obtain the following:

► **Corollary 3** (Informal). *Let  $n, t \in \mathbb{N}$ . As a consequence of our worst-case to average-case reduction (Theorem 7.5 of the full version), we can show the following bounds on the Haar cloning game:*

- *In the single-copy setting, the Haar game  $\mathsf{G}_{1 \mapsto 2}$  has a value of  $\omega(\mathsf{G}_{1 \mapsto 2}) \leq (\cos^2(\pi/8))^n \approx 2^{-0.228n}$ .  
(Here, the players are free to make **arbitrarily many adaptive queries** to  $U_\theta$  or  $U_\theta^\dagger$ .)*
- *In the multi-copy setting, the Haar game  $\mathsf{G}_{t \mapsto t+1}$  has a value of  $\omega(\mathsf{G}_{t \mapsto t+1}) \leq \exp(O(t \log t)) \cdot 2^{-n}$ . (Here, the players are restricted to making **only a single query** to  $U_\theta$  or  $U_\theta^\dagger$ .)*

We will see next that Haar cloning games are central to the applications previously listed in items 2 and 4. We will discuss Haar cloning games and our worst-case to average-case reduction more in Section 2.2.

## Opening Up New Applications

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. We will see that these applications crucially require us to overcome the aforementioned limitations 1 and 3 in the existing constructions and analyses of cloning games.

---

<sup>4</sup> As we explain in Remark 1 and Remark 7 of the full version, approximate  $t \mapsto t + 1$  no-cloning emerges as a special case of our one-query cloning game, whereby each player makes a single query to  $U_\theta^\dagger$  and immediately measures in the computational basis (with no post-processing whatsoever). In this case, the value of the cloning game is precisely equal to the maximum *average* cloning fidelity for  $t \mapsto t + 1$ .

- **Black Hole Cloning Games.** In Section 8 of the full version, we analyze a new three-player game which is designed to capture cloning and entanglement monogamy in the context of evaporating black holes. Our results offer new quantitative insights into the *black hole information paradox* [36, 48, 37] and suggest that, in an idealized model of a black hole which features Haar random (or pseudorandom) scrambling dynamics, the information from infalling qubits can only be recovered from either the interior or the exterior of the black hole, but never from both places at once – even in the presence of powerful observers which can make a single query to the scrambling unitary or its inverse. At a technical level, this requires us to essentially show a bound of  $O(2^{-n})$  for the  $1 \mapsto 2$  Haar cloning game; **even an exponentially small bound of  $O(2^{-cn})$  for  $c < 1$  will not suffice.** We thus crucially need to overcome the aforementioned limitation 1, and we also need to make use of the aforementioned worst-case to average-case reduction. We discuss this application at a high level in Section 1.3 of the full version, taking care to provide context on relevant prior work in black hole physics.
- **Unclonable Encryption: “MicroCrypt” and the Multi-Copy Setting.** In Section 9 of the full version, we give an affirmative answer to an open question which was recently posed in [46]; namely: do interesting unclonable cryptographic primitives – other than private-key quantum money which is implied by pseudorandom states [38] – exist, even in a world in which  $P = NP$ ? We construct succinct unclonable encryption schemes from the existence of pseudorandom unitaries; thereby continuing to close the gap between the worlds of MicroCrypt and unclonable cryptography. A crucial ingredient for this result is the aforementioned worst-case to average-case reduction.

Secondly, we propose a candidate multi-copy unclonable encryption scheme based on the aforementioned binary phase cloning game. We view Theorem 2 as evidence and a first step towards proving its security in the stronger setting where  $t$  can be an a priori unbounded polynomial in  $n$  and the players are free to make polynomially many queries to the encryption and decryption functionality (or even more strongly, are given the secret key  $\theta$  in the clear). Considering the pseudorandomness of the binary phase states that we use as ciphertexts, we believe this stronger security guarantee to be plausible. Obtaining multi-copy security clearly requires us to overcome limitation 3.

We discuss these applications to unclonable cryptography in some more detail in Section 1.4 of the full version.

We now turn to a detailed overview of our techniques.

## 2 Technical Overview

This technical overview is organized as follows:

- In Section 2.1, we discuss previous constructions [19, 24] and explain the limitations of these constructions and the underlying techniques [56, 27, 52] in both the multi-copy and single-copy settings.
- In Section 2.2, we discuss a natural construction using Haar random unitaries, the obstacles to directly analyzing this construction, and our worst-case to average-case reduction as a means of indirectly studying this construction.
- In Section 2.3, we present our construction based on binary phase states (previously put forth by [38, 18] as a quantum pseudorandom state), and our new tools for analyzing this. Our tools significantly extend the previous notion of *binary types* introduced by [3] for analyzing binary phase states.

We remark at the outset that, when considering cloning games, we will consider a few different models for how the players (Bob and Charlie) access  $\theta$ :

- *Strong cloning games*: Bob and Charlie are given  $\theta$  in the clear;
- *Oracular cloning games*: Bob and Charlie are given oracle access to  $U_\theta$  and  $U_\theta^\dagger$ , and are free to make an a priori unbounded polynomial number of queries.
- *Bounded-query-oracular cloning games*: Bob and Charlie are given some a priori bound  $q$  on the number of queries they can adaptively make.

We note that, even when  $q = 1$ , this model is still quite expressive; as noted in Remark 7 of the full version, it captures conventional and approximate  $t \mapsto t + 1$  no-cloning bounds as a special case.

We will also sometimes consider Bob and Charlie who are required to run in quantum polynomial time.

## 2.1 Previous Techniques and Their Limitations

Let us now dive a little deeper into the shortcomings of our current understanding of cloning games. Here, it is instructive to start with limitation 3; namely, that of multi-copy games.

### Multi-Copy Insecurity of BB84 and Coset States

One can extend cloning games as defined in Figure 1 to *multi-copy* cloning games: in this variant, the cloner  $\Phi$  receives  $t$  copies i.e. the state  $(U_\theta |x\rangle)^{\otimes t}$ . In the place of Bob and Charlie, there are now  $t + 1$  players  $\mathcal{P}_1, \dots, \mathcal{P}_{t+1}$  who wish to all simultaneously guess  $x$ . It is easy to see that this game becomes provably easier for the adversaries as  $t$  increases.

In the case of BB84 states, where  $U_\theta |x\rangle = H^\theta |x\rangle$ , we claim that the adversaries can win with probability 1 for any  $t \geq 2$ . The attack is simple:  $\Phi$  will measure one copy in the standard basis and one copy in the Hadamard basis, and forward these results to all players. Upon receiving  $\theta$ , the players can mix-and-match these results to recover  $x$ . The intuitive issue here is that the measurement basis is entirely disentangled across qubits; in fact, [4] describes a generic attack on cloning games with this disentangled structure.

The case of coset states [24, 27, 52] is similar, albeit only after  $t$  becomes larger than  $n$ . Here, we will interpret the basis  $\theta$  as a subspace  $A \subseteq \mathbb{F}_2^n$  of dimension  $n/2$ , and the input  $x \in \{0, 1\}^n$  as a pair of cosets  $s + A, s' + A^\perp$ . Then the cloner will receive copies of the state

$$|A_{s,s'}\rangle = \frac{1}{2^{n/4}} \sum_{a \in A} (-1)^{\langle a, s' \rangle} |a + s\rangle.$$

The cloner can measure half the copies in the standard basis and half the copies in the Hadamard basis, and forward these results to all players. Upon receiving  $A$ , they can all identify the cosets  $s + A$  and  $s' + A^\perp$  with high probability.

As stated, the above attacks only apply in the strong cloning setting. However, the situation is more grim for a very simple reason: *these families of states are both learnable given poly(n) copies*, whereas most states require exponentially many copies to become learnable, as the state of the art in quantum tomography [11] suggests. Hence, the cloner  $\Phi$  can simply learn a classical description of the state and subsequently forward both the basis  $\theta$  and the message  $x$  to the  $t + 1$  players; the players do not even require the challenger to send them  $\theta$ . In other words, these attacks even hold in the bounded-query-oracular model with  $q = 0$  or  $q = 1$ . Nevertheless, our technical starting point, which we discuss next, is the toolkit used by previous works to analyze cloning games in the single copy ( $t = 1$ ) case. We will pin down where exactly it fails to work in the multi-copy case and remedy these problems. To provide the necessary background, we begin by introducing the notion of a monogamy of entanglement game.

## Monogamy of Entanglement Games

We now take a brief detour and discuss the concept of *monogamy of entanglement games*; we will see shortly that they are closely related to cloning games. Monogamy of entanglement games were introduced by Tomamichel, Fehr, Kaniewski and Wehner [56] in order to characterize entanglement monogamy [55] using the language of non-local games. Informally, quantum correlations are “monogamous”, and thus cannot be shared freely among multiple parties.

A monogamy of entanglement (MOE) game  $G$  with respect to the question set  $\Theta$ , answer set  $\mathcal{X}$  and measurement set  $\{\mathbf{A}_x^\theta\}_{\theta \in \Theta, x \in \mathcal{X}}$  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  $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ . They send register A to Alice, and hold onto registers B and 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  $\{\mathbf{A}_x^\theta\}_{x \in \mathcal{X}}$  to her register 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  $\{\mathbf{B}_x^\theta\}_{x \in \mathcal{X}}$  and  $\{\mathbf{C}_x^\theta\}_{x \in \mathcal{X}}$  to their registers B and C, respectively.
4. (**Outcome phase**) Bob and Charlie win if they both guess Alice’s outcome correctly.

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

$$\omega_S(G) := \mathbb{E}_{\theta \sim \Theta} \sum_{x \in \mathcal{X}} \text{Tr}[(\mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta) \rho_{ABC}].$$

We let  $\omega(G)$  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. *We emphasize that, in general monogamy of entanglement games, the shared state  $\rho$  is completely arbitrary and adversarially chosen by Bob and Charlie; as we will see, this is the main way in which cloning games deviate from the monogamy of entanglement setting.*

## Appendix A of the Full Version: Connecting Cloning and Monogamy Games

The standard tool for analyzing cloning games is to recast them as a special type of monogamy game. Together with the techniques laid out by [56] for analyzing monogamy games, this has found numerous applications in unclonable cryptography, including unclonable encryption [19], quantum copy-protection [1, 25, 24, 5], unclonable decryption keys [31], and unclonable proofs [32].

We now explain this connection between cloning and MOE games. 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, where  $\bar{U}$  denotes the complex conjugate of  $U$ . This yields a monogamy of entanglement game with the following two restrictions:

## 109:10 Cloning Games, Black Holes and Cryptography

- 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

$$\rho_{ABC} = (\mathbb{I}_A \otimes \Phi_{A' \rightarrow BC})(|\text{EPR}\rangle\langle \text{EPR}|_{AA'}). \quad (1)$$

In words,  $\rho$  can be adversarially chosen subject to the constraint that its marginal state on Alice’s system is maximally mixed.

This equivalence, which we formally show in Lemma A.1 of the full version, was first observed in the context of BB84 states by Broadbent and Lord [19]. On a high level, the statement is a consequence of the *ricochet property* of EPR pairs, which we formally state in Section 2.1 of the full version. 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, as we will see, can be handled using spectral bounds as first observed by [56].

Although the equivalence observed by [19] is in the single-copy setting, it turns out that this idea readily generalizes to the multi-copy setting, as we show in Lemma A.2 of the full version. The differences are as follows:

- In the cloning game, Alice and the cloner  $\Phi$  now share  $nt$  EPR pairs, and Alice will measure each of the  $t$  copies in the basis specified by  $\left\{ \bar{U}_\theta |x\rangle\langle x| \bar{U}_\theta^\dagger \right\}_{x \in \{0,1\}^n}$ .
- In the equivalent monogamy-like<sup>5</sup> game, we only say that the adversaries win if Alice’s  $t$  measurements and the  $t + 1$  players’ outputs are all equal to the same string  $x$ . In other words, we need to essentially post-select on Alice’s measured string  $x \in \{0,1\}^n$  being the same for each of the  $t$  copies, which means the value of this monogamy-like game is immediately upper bounded by  $2^{-n(t-1)}$ .

Because of this post-selection, what we end up with is an equality of the following form:

$$\omega(\mathbf{G}_{\text{cloning}}) = 2^{n(t-1)} \cdot \omega(\mathbf{G}_{\text{monogamy-like}}). \quad (2)$$

Note that when  $t = 1$ , the  $2^{n(t-1)}$  term is 1 and we recover the equivalence used by [19]. Our goal is hence to upper bound the value of  $\mathbf{G}_{\text{monogamy-like}}$  by  $2^{-n(t-1)} \cdot \text{negl}(n)$ , ideally even  $O(2^{-nt})$ .

### Section 6 of the Full Version: TFKW13 and its Limitations

The work by Tomamichel, Fehr, Kaniewski and Wehner [56] analyzes MOE games and later focuses on the BB84 case (i.e.  $U_\theta = H^\theta$ ) and uses two beautiful ideas, which for simplicity we state in the single-copy setting:

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

$$\mathbb{E}_{\theta \sim \Theta} \sum_{x \in \mathcal{X}} \text{Tr} [(\mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta) \rho_{ABC}] \leq \left\| \mathbb{E}_{\theta \sim \Theta} \sum_{x \in \mathcal{X}} \mathbf{A}_x^\theta \otimes \mathbf{B}_x^\theta \otimes \mathbf{C}_x^\theta \right\|_\infty.$$

<sup>5</sup> We say “monogamy-like” because monogamy-of-entanglement games traditionally involve just three parties [56].

This reduces the task of bounding the value of a monogamy game to bounding an operator norm. In general monogamy games as formulated by [56], the shared state  $\rho_{ABC}$  is adversarially chosen so this step is tight. However, we will see soon that this step is too lossy when restricting attention to the special monogamy-like games that are equivalent to cloning games.

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 restate in Theorem 6.1 of the full version, the authors of [56] show that

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

We refer the reader to Theorem 6.1 of the full version for a formal statement.

In the BB84 monogamy game where  $\Theta = \mathcal{X} = \{0, 1\}$  and  $\mathbf{A}_x^\theta = \mathbf{H}^\theta |x\rangle\langle x| \mathbf{H}^\theta$ , it is straightforward to see that  $\left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} \right\|_\infty = \frac{1}{\sqrt{2}}$ , and hence  $\omega(\mathbf{G}_{\text{BB84}}) \leq \frac{1}{2} + \frac{1}{2\sqrt{2}}$ . The work by [56] also extends this to “parallel-repeated” BB84 games with  $|\Theta| = |\mathcal{X}| = \{0, 1\}^n$  (see Theorem 3.4 of the full version for a formal definition), and show that

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

Hence the BB84 monogamy game has value  $\leq 2^{-0.228n}$ , and in fact this is tight; [56] exhibits a simple strategy achieving this bound. Similar techniques were used by [27] and improved upon by [52] to analyze subspace coset states, ultimately proving an upper bound of  $O(2^{-n/4})$ ; it is not known whether or not this is tight.<sup>6</sup> However, the techniques laid out by [56] *provably* do not suffice for our applications:

- In the multi-copy case, recall from Equation (2) that we need to prove a bound on  $\mathbf{G}_{\text{monogamy-like}}$  of  $\ll 2^{-n(t-1)}$ . Item 1 of the [56] methodology proposes to ignore the structure of the state shared by Alice and  $\mathcal{P}_1, \dots, \mathcal{P}_{t+1}$ , in order to reduce our task to bounding an operator norm.

This is likely too lossy in our setting, as evidenced by the following simple counterexample (assume  $t > 1$  is even for simplicity) that holds against any cloning game where the unitaries  $U_\theta$  have real entries. Alice will hold  $tn/2$  EPR pairs (which are unentangled from the states held by  $\mathcal{P}_1, \dots, \mathcal{P}_{t+1}$ ). The  $t+1$  players will each deterministically output  $0^n$  as their guess (note that once again this strategy does not depend at all on  $\theta$ ). The winning probability is now just the probability that Alice measures 0 on each of her  $tn/2$  EPR pairs (in whatever basis she samples), which is  $2^{-nt/2} \geq 2^{-n(t-1)}$ . We formalize this counterexample in Section 6.1 of the full version.

We note that this does not rule out the possibility of the [56] technique being adaptable to the multi-copy setting for a construction that uses unitaries with complex entries. However, the pre-existing constructions based on BB84 states or coset states – as well as our main construction based on binary phase states (which we sketch in Section 2.3) – only use unitaries with real entries. Thus we still view our result as a bound against the adaptability of existing construction and techniques to the multi-copy setting.

<sup>6</sup> Previous work [53] proved an upper bound of  $O(2^{-n/2})$  in a setting where the cloner  $\Phi$  is restricted to splitting the state as is into two equal-sized halves, sending one to Bob and the other to Charlie. We cite  $O(2^{-n/4})$  as the state of the art, as we are interested in games where the cloner  $\Phi$  is unrestricted.

- Even in the single-copy case, there is another inherent limitation that arises from using Item 2 of the [56] methodology: the maximal pairwise overlap  $\max_{\theta \neq \theta'} \left\| \mathbf{A}_x^\theta \mathbf{A}_{x'}^{\theta'} \right\|_\infty$  is provably at least  $2^{-n/2}$  for any monogamy game, as we show in Section 6.2 of the full version. For completeness, we also show in Section 6.3 of the full version that our binary phase state construction (which we will discuss more in Section 2.3) essentially attains this maximum pairwise overlap.

However, we would ideally like to prove a tight bound (up to constant factors) of  $O(2^{-n})$ . This is not just a matter of aesthetic taste; this is actually crucial for our application to black hole physics, as we explain in Section 1.3 of the full version.

We next turn our attention to our construction and our new techniques for analyzing it, which make progress towards overcoming both of these barriers.

## 2.2 Section 7 of the Full Version: Haar Cloning Games and Worst-Case to Average-Case Reductions

Given our previous observations on the multi-copy insecurity of BB84 and coset states, it is clear that we need to look for entirely new constructions. Ideally, such a candidate ensemble of states would also remain *unlearnable* in the presence of an arbitrary polynomial amount of identical copies. A natural idea is to consider Haar random states, which Werner [57] showed to be multi-copy unclonable. This suggests the following very natural approach: Alice will take  $\{U_\theta : \theta \in \Theta\}$ <sup>7</sup> to be a Haar random ensemble and send the cloner  $(U_\theta |x\rangle)^{\otimes t}$ . We call this the  $t \mapsto t+1$  *Haar cloning game*. However, existing techniques for analyzing the Haar measure, which we outline below, appear severely limited for our purposes:

- Prior works [46, 22, 2] often rely on representation-theoretic techniques. In our setting, we would roughly need to prove spectral bounds on the *mixed Haar twirl* of a certain operator  $\Xi$ ; informally, in the  $1 \mapsto 2$  case, these amount to expressions of the form:

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

General expressions of this form have been studied by [29, 35, 34] using the machinery of *mixed Schur-Weyl duality*, but their techniques appear to be very unwieldy in our more complicated setting with multiple non-communicating parties.

- The recent breakthrough result by Ma and Huang [44] uses a technically involved purification argument [44] that once again does not seem to adapt easily to the multi-party setting.
- Finally, the recent beautiful work by Bhattacharya and Culf [16] analyzes the Haar measure in the single-copy case using a modular application of the one-shot decoupling theorem [28], but in the process only establishes a cloning bound of  $\tilde{O}(1/n)$ , whereas we would like a bound that is  $O(2^{-n})$  or at the very least exponentially small in  $n$ .

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 to win* than any other cloning game. We prove this via a *worst-case to average-case reduction* which, at a high level, follows from Haar invariance and some additional new insights into *mixed* unitary designs, which we explain in more detail below.

<sup>7</sup> The Haar random ensemble is infinite so this is not well-defined; this technicality can be circumvented by using a higher order unitary design or a pseudorandom unitary [46, 44] in its place.

Our observation immediately suggests the following approach for analyzing a Haar cloning game:

1. Argue that for *any* distribution  $\mathfrak{D}$  supported on  $U(2^n)$ , we have:

$$\sup_{\text{strategies } S} \omega_S(\mathbb{G}; U \sim U(2^n)) \leq \sup_{\text{strategies } S} \omega_S(\mathbb{G}; U \sim \mathfrak{D}). \quad (3)$$

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

$$\sup_{\text{strategies } S} \omega_S(\mathbb{G}; U \sim \mathcal{D}) \leq O(2^{-n}),$$

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

We prove the aforementioned *worst-case-to-average-case reduction* which is captured in Item 1 in Section 7 of the full version. To instantiate this argument, we need to be able to sample  $V$  that appears Haar random, together with a classical description of it. This can be done using either a *mixed unitary design* (in the bounded-query-oracular setting) or a pseudorandom unitary [46, 44] (in the oracular setting with computationally bounded players). We formally define mixed unitary designs in Section 7.1 of the full version, and – as a bonus – we also prove that the standard notion of an exact unitary  $t$ -design will also work as a mixed unitary design without modification. To the best of our knowledge, this was not previously observed in the literature, and we hope that this contribution might be of independent interest. We leave the task of adapting this reduction to the strong cloning game setting – that is, where a description of the unitary is revealed to the players in the clear rather than embedded in an oracle – as a direction for future work.

It now remains to address Item 2 i.e. find some other cloning game that we can more easily show an upper bound of  $O(2^{-n})$  for. We address this next.

### 2.3 Sections 4 and 5 of the Full Version: Construction and Analysis from Binary Phase States

#### Our Construction Inspired by Quantum Pseudorandom States

We begin from a simple starting point: in Section 2.2, we suggested having Alice send a Haar random state  $U_\theta |x\rangle$  to the cloner. Instead, what if Alice were to send a *pseudorandom* state [38, 18]? These are also multi-copy unclonable by a trivial hybrid argument combined with Werner’s result [57] in the Haar case. The advantage of working with binary phase states is that we have much simpler constructions that, as we will see, are easier to analyze.

It was shown by [38, 18] that if  $\mathfrak{F}$  is a family of post-quantum pseudorandom functions [61]  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , then the *binary phase state*

$$|\psi^f\rangle := 2^{-n/2} \sum_{y \in \{0, 1\}^n} (-1)^{f(y)} |y\rangle$$

is pseudorandom. To use this in a cloning game, we follow the approach in [23] in order to encode  $x \in \{0, 1\}^n$  into this state, which we do by taking:

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

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

is a phase oracle for  $f$ . In other words, we are proposing to define a cloning game with  $\Theta = \mathfrak{F}$  and  $U_\theta = U_f H^{\otimes n}$ . Thus in the equivalent monogamy game, Alice’s projectors will be defined by

$$\mathbf{A}_x^f := U_f H^{\otimes n} |x\rangle\langle x| H^{\otimes n} U_f.$$

The question is now how one should go about analyzing this game. As mentioned in Section 2.1, the usual [56] methodology for analyzing cloning games is firstly limited to the single-copy setting, and secondly even in this setting can only prove a bound of  $2^{-n/2}$ . For completeness, we show in Section 6.3 of the full version that plugging our binary phase construction into [56] “saturates” this technique and yields a single-copy cloning bound of  $\tilde{O}(2^{-n/2})$ , which is stronger than the previous results on BB84 [56, 19] and coset [24, 27, 52] states.

### Compressed Oracles and Binary Types

The techniques discussed up to this point draw on the machinery of [56] and thus suffice to establish cloning bounds even in the setting where a classical description of the measurement basis  $\theta$  (in the binary phase case, the function  $f$ ) is sent to all players  $\mathcal{P}_1, \dots, \mathcal{P}_{t+1}$  in the clear. To our knowledge, the only other technique that works in this strong regime is the decoupling technique by [16]. However, as we explained in Sections 2.1 and 2.2, both of these techniques run into limitations with respect to the multi-copy setting and/or attaining an optimal bound of  $O(2^{-n})$ .

We hence propose to migrate to the oracular setting, where each player can make oracle queries to  $U_f$ , but is not given a description of  $f$  in the clear. Note that this still suffices to recover  $x$  from  $U_f H^{\otimes n} |x\rangle$ . In fact, we only need one query: a single query to  $U_f$  would leave us with  $H^{\otimes n} |x\rangle$ , and now measuring in the Hadamard basis yields  $x$ . We explain this in the case of general cloning games in Remark 7 of the full version.

We now want to reason about algorithms that make oracle queries to  $U_f$  for a random (or pseudorandom) function  $f$ . The natural candidate technique for such a task is Zhandry’s compressed oracle technique [60]. The crucial idea is to purify the cloning game by adding a register that stores the function  $f$ . One can then argue that queries to  $U_f$  for a random  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  can be simulated as follows:

- We will add a purifying “database” register to the system that we initialize to  $|\emptyset\rangle$ . In general, it will store some subset  $S \subseteq \{0, 1\}^n$ .
- If the algorithm wishes to query the string  $y \in \{0, 1\}^n$ , simply update  $|S\rangle \leftarrow |S \oplus \{y\}\rangle$  (note that if  $y$  is in  $S$  before the query, this will remove  $y$  from  $S$ .)

Let us see how this technique would play out in our setting. Alice and  $\mathcal{P}_1, \dots, \mathcal{P}_{t+1}$  all share some global state, and act as follows:

- Alice queries each of her  $t$   $n$ -qubit states, then applies a Hadamard to each copy. Her local transformation can be written as  $\bigotimes_{i=1}^t \left( \sum_{y_i \in \{0, 1\}^n} H^{\otimes n} |y_i\rangle\langle y_i| \right)$ , and she will XOR  $\{y_1\} \oplus \dots \oplus \{y_t\}$  into the database register.
- For each  $i \in [t + 1]$ , let the adversary  $\mathcal{P}_i$  make  $q$  adaptive queries represented by unitaries  $V_{i,1}, \dots, V_{i,q}$ . Their local transformation can be written as a sum of terms of the form

$$V_{i,q} |z_{i,q}\rangle\langle z_{i,q}| V_{i,q-1} |z_{i,q-1}\rangle\langle z_{i,q-1}| \dots V_{i,1} |z_{i,1}\rangle\langle z_{i,1}|,$$

and they will XOR  $\{z_{i,1}\} \oplus \dots \oplus \{z_{i,q}\}$  into the database register.

In summary, the database register will contain the set:

$$\bigoplus_{i=1}^t \{y_i\} \oplus \bigoplus_{i=1}^{t+1} \bigoplus_{j=1}^q \{z_{i,j}\}. \quad (4)$$

At this point, it is unclear how to proceed, for the following simple conceptual reason: the utility of Zhandry’s compressed oracle technique [60] lies in the fact that it connects the algorithm’s success probability with the contents of the database register in some way. For example, when reproving the [14] lower bound showing the optimality of Grover search, Zhandry shows that the success probability of the algorithm is essentially upper bounded by the probability of a solution  $x$  to the search problem appearing in the database register. However, there is no analogous notion in our setting, because we are considering a problem with *inherently quantum inputs*; a successful adversary likely needs to query  $U_f$  on every input in superposition.

Instead, we will deviate from Zhandry’s compressed oracle formalism by simply tracing out (or equivalently, measuring) the database register. This effectively conditions our superposition on the collection of strings that are listed an odd number of times in Equation (4). This is exactly the notion of *binary types* introduced by [3]. In order to get a better handle on the binary type’s combinatorial structure, we will restrict each of the  $t + 1$  players to only make *one oracle query* to  $U_f$ ; as explained in Remark 7 of the full version, this is still sufficiently expressive to admit a trivial strategy attaining value  $2^{-n}$ .

In this case, a binary type  $\lambda$  is specified by a subset  $T_\lambda \subseteq [2^n]$  with  $|T_\lambda| \leq 2t + 1$ . For  $\mathbf{x} \in [2^n]^{2t+1}$ , we say that  $\text{BinType}(\mathbf{x}) = \lambda$ , or equivalently that  $\mathbf{x}$  *matches*  $\lambda$ , if every string in  $T_\lambda$  appears an odd number of times in  $\mathbf{x}$ , while every string outside  $T_\lambda$  appears an even number of times in  $\mathbf{x}$ . Thus, if Alice and the players jointly hold a standard basis state  $|\mathbf{x}\rangle$ , a simultaneous query to  $U_f$  by all parties will write  $\text{BinType}(\mathbf{x})$  into the database register. Finally, we let  $\Pi_\lambda$  denote the projector onto standard basis vectors  $\mathbf{x}$  that match  $\lambda$ . We provide more precise definitions and properties of binary types in Section 4.2 of the full version. We now model each player’s projector as follows:

$$\mathbf{P}_{i,x}^f = U_f V_i^\dagger |x\rangle\langle x| V_i U_f,$$

for unitaries  $Q_i$ .<sup>8</sup> This simplification together with the aforementioned binary type formalism allows us to succinctly characterize the value of the cloning game: if we define

$$\Xi := \sum_{x \in \{0,1\}^n} \left[ \left( \mathbb{H}^{\otimes n} |x\rangle\langle x| \mathbb{H}^{\otimes n} \right)^{\otimes t} \otimes \bigotimes_{i=1}^{t+1} \left( V_i^\dagger |x\rangle\langle x| V_i \right) \right], \text{ then}$$

$$\omega(\mathsf{G}) = \sum_{\lambda} \text{Tr} [\Pi_\lambda \Xi \Pi_\lambda \rho],$$

where  $\rho$  is the shared state from the monogamy-like game that we introduced in Section 2.1. We face two challenges in bounding expressions of this form. We state them below and then describe how we address these challenges:

1. The [56] paradigm of discarding the tripartite state  $\rho$  and simply bounding this expression by  $\max_{\lambda} \|\Pi_\lambda \Xi \Pi_\lambda\|_\infty$ <sup>9</sup> is provably too lossy, as we explained in Section 2.1.
2. Even if it were somehow sufficient to bound  $\|\Pi_\lambda \Xi \Pi_\lambda\|_\infty$  for each  $\lambda$ , to the best of our knowledge, it appears difficult to directly establish such a bound. Informally, the reason is that the combinatorial structure arising from a type  $\lambda$  entangles registers together; if we consider the  $t = 1$  case and the type defined by  $T_\lambda = \{x^*\}$  for some string  $x^*$ , then strings of the form  $(x^*, y, y)$ ,  $(y, x^*, y)$ , or  $(x^*, y, y)$  would all match  $\lambda$ . It would be much cleaner if we could just analyze strings from one of these categories at a time.

<sup>8</sup> In reality, we later also allow these players additional ancillary workspace qubits; we define this generalization in Definition 3.8 of the full version. Moreover, we assume without loss of generality that the players do not perform any preprocessing before making their query to  $U_f$ , by absorbing this preprocessing into the cloning channel  $\Phi$  that constructs their initial states.

<sup>9</sup> This bound holds by noting that the projectors  $\Pi_\lambda \Xi \Pi_\lambda$  are mutually orthogonal.

**Idea 1 (Section 5.4 of the Full Version): Staring at the Shared State**

To address Item 1, we take a closer look at the structure of the shared state  $\rho$ . It is the result of applying some (adversarially chosen) channel to the right half of  $tn$  EPR pairs. This can be seen from Equation (1) (appropriately generalized to the multi-copy setting). In other words, if we apply a partial trace to remove the  $P_{1 \rightarrow t+1}$  registers of the  $t+1$  players, the residual state on Alice's register  $A$  will always 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 Sections 5.4 and 5.5 of the full version. This is perhaps not surprising; in the counterexample we presented in Section 2.1 showing that just bounding the operator norm would be insufficient, Alice's local state was very far from maximally mixed. In fact, it was a pure state consisting of  $t/2$  EPR qudit pairs.

At a high level, our analysis to use this structure of  $\rho$  proceeds by showing that for any type  $\lambda$  such that  $\Pi_\lambda \Xi \Pi_\lambda$  has high operator norm, the shared state  $\rho$  must place *low* weight on the image of  $\Pi_\lambda$ . These effects roughly cancel each other out.

**Idea 2 (Sections 4.3 and 5.3 of the Full Version): From Types to Subtypes**

We now turn to the issue stated in Item 2. Continuing with the  $t=1$  example, reasoning about  $\lambda$  directly requires simultaneously handling three categories of strings:  $(x^*, y, y)$ ,  $(y, x^*, y)$ , or  $(x^*, y, y)$ . Instead, we simplify matters by focusing on just one of these categories at a time – we call such a category a *subtype*, a novel notion we define formally in Section 4.3 of the full version. We denote subtypes by  $\mu$  and their corresponding subtype projectors by  $\Pi_\mu$ . In Section 4.3.2 of the full version, we show that instead of bounding  $\|\Pi_\lambda \Xi \Pi_\lambda\|_\infty$  for a type  $\lambda$ , it suffices to bound  $\|\Pi_\mu \Xi \Pi_\mu\|_\infty$  for a *subtype*  $\mu$ . This added structure allows us to prove better spectral bounds, which we present in Section 5.3 of the full version.

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  $U_f$ . 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 2.18 of the full version.

**Technical Tool (Section 2.4 of the Full Version): Spectral Bounds on Blockwise Tensor Products**

In order to prove spectral bounds on the norm of  $\Pi_\mu \Xi \Pi_\mu$  for any subtype  $\mu$ , and accommodate the possibility of the  $t+1$  players using ancilla qubits, we require a novel bound on the norm of a blockwise tensor product of  $d \times d$  block matrices. As a simple example, the  $d=2$  case is the following: we need to show that

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

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  $|c_{i,j}| \leq 1$  for all  $i, j$ . Proving this turns out to be rather technically challenging; we present this result and its proof in Theorem 2.15 of the full version. We also discuss at the end of Section 2.4.1 of the full version why existing techniques fail to prove the general result we need. 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.

Putting these ideas together, we manage to prove a multi-copy cloning bound of  $O_t(2^{-n})$ , overcoming the limitations of previous techniques explained in 2.1 with a complete overhaul of the technical framework laid out by [56], albeit at the expense of restricting the  $t + 1$  players to make a single oracle query to  $U_f$ .

### 3 Open Questions

#### Cloning Games in General

We first list some open questions related to cloning games in general; these 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 1 of the full version) be proven even if the two players (say, 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 [40, 30].

2. More tantalizingly, can this security be shown if the measurement basis  $\theta$  (either a PRU or PRF secret key, depending on whether we are considering the PRU or binary phase construction) is given to Bob and Charlie in the clear, rather than in the form of an oracle? This still plausibly satisfies unclonable security (as demonstrated by [56, 19, 27, 52] for BB84 and coset state cloning games), but is highly counterintuitive; the PRU/PRF security guarantees do 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.

3. 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  $\mathcal{P}_1, \dots, \mathcal{P}_{t+1}$  that are free to make multiple *non-adaptive* queries to  $U_\theta, U_\theta^\dagger$ ?

#### Applications to Black Hole Physics and Beyond

Here, we list some questions specific to our black hole application:

1. Can we make our modeling assumptions in our definition of black hole cloning games in Section 8 of the full version 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?
2. Can we use the language of interactive games to offer new quantitative insights into information scrambling in other chaotic quantum systems, besides black holes?

### Applications to Unclonable Cryptography

Finally, we present some questions specific to our applications to unclonable cryptography:

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”, which as we argue in Section 1.4 of the full version offers a plausible but not yet proven path towards indistinguishable security.) This is an important but difficult problem that recent works have made some progress on [19, 42, 6, 7].
3. Which unclonable cryptography primitives have natural, constructible, and applicable  $t \mapsto t + 1$  analogues, besides unclonable encryption?

---

### References

- 1 Scott Aaronson. Quantum copy-protection and quantum money. In *2009 24th Annual IEEE Conference on Computational Complexity*, pages 229–242. IEEE, July 2009. doi:10.1109/ccc.2009.42.
- 2 Rene Allerstorfer, Matthias Christandl, Dmitry Grinko, Ion Nechita, Maris Ozols, Denis Rochette, and Philip Verduyn Lunel. Monogamy of highly symmetric states, 2024. arXiv:2309.16655.
- 3 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. doi:10.1007/978-3-031-22318-1\_9.
- 4 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. doi:10.1007/978-3-030-90459-3\_11.
- 5 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*, pages 212–241, Berlin, Heidelberg, 2022. Springer-Verlag. doi:10.1007/978-3-031-15979-4\_8.
- 6 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*, pages 66–98, Berlin, Heidelberg, 2023. Springer-Verlag. doi:10.1007/978-3-031-38554-4\_3.
- 7 Prabhanjan Ananth, Fatih Kaleoglu, and Henry Yuen. Simultaneous Haar indistinguishability with applications to unclonable cryptography. *CoRR*, abs/2405.10274, 2024. doi:10.48550/arXiv.2405.10274.
- 8 Prabhanjan Ananth, Saachi Mutreja, and Alexander Poremba. Revocable encryption, programs, and more: The case of multi-copy security, 2024. doi:10.48550/arXiv.2410.13163.
- 9 Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. *Cryptology ePrint Archive*, Paper 2023/325, 2023. URL: <https://eprint.iacr.org/2023/325>.
- 10 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. doi:10.1007/978-3-031-15802-5\_8.

- 11 K Banaszek, Marcus Cramer, and D Gross. Focus on quantum tomography. *New Journal of Physics*, 15:5020–, December 2013. doi:10.1088/1367-2630/15/12/125020.
- 12 Amit Behera and Or Sattath. Almost public quantum coins, 2024. arXiv:2002.12438.
- 13 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.
- 14 Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997. doi:10.1137/S0097539796300933.
- 15 Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993. doi:10.1103/PhysRevLett.70.1895.
- 16 Archishna Bhattacharyya and Eric Culf. Uncloneable encryption from decoupling, 2025. arXiv:2503.19125.
- 17 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. doi:10.4230/LIPIcs.ITCS.2023.24.
- 18 Zvika Brakerski and Omri Shmueli. (pseudo) random quantum states with binary phase, 2019. arXiv:1906.10611.
- 19 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. doi:10.4230/LIPIcs.TQC.2020.4.
- 20 V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54(3):1844–1852, September 1996. doi:10.1103/physreva.54.1844.
- 21 Alper Çakan and Vipul Goyal. Unclonable cryptography with unbounded collusions and impossibility of hyperefficient shadow tomography. In Elette Boyle and Mohammad Mahmoody, editors, *Theory of Cryptography*, pages 225–256, Cham, 2025. Springer Nature Switzerland.
- 22 Chi-Fang Chen, Jordan Docter, Michelle Xu, Adam Bouland, Fernando G.S.L. Brandão, and Patrick Hayden. Efficient unitary designs from random sums and permutations. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 476–484. IEEE, October 2024. doi:10.1109/focs61266.2024.00037.
- 23 Andrea Coladangelo. Quantum trapdoor functions from classical one-way functions. Cryptology ePrint Archive, Paper 2023/282, 2023. URL: <https://eprint.iacr.org/2023/282>.
- 24 Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to uncloneable cryptography. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 556–584, Cham, 2021. Springer International Publishing. doi:10.1007/978-3-030-84242-0\_20.
- 25 Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model, 2022. arXiv:2009.13865.
- 26 Patrick J. Coles, Mario Berta, Marco Tomamichel, and Stephanie Wehner. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.*, 89:015002, February 2017. doi:10.1103/RevModPhys.89.015002.
- 27 Eric Culf and Thomas Vidick. A monogamy-of-entanglement game for subspace coset states. *Quantum*, 6:791, September 2022. doi:10.22331/q-2022-09-01-791.

- 28 Frédéric Dupuis, Mario Berta, Jürg Wullschlegler, and Renato Renner. One-shot decoupling. *Communications in Mathematical Physics*, 328(1):251–284, May 2014. doi:10.1007/s00220-014-1990-4.
- 29 T. Eggeling and R. F. Werner. Separability properties of tripartite states with  $u \otimes u \otimes u$  symmetry. *Phys. Rev. A*, 63:042111, March 2001. doi:10.1103/PhysRevA.63.042111.
- 30 Netta Engelhardt, Asmund Folkestad, Adam Levine, Evita Verheijden, and Lisa Yang. Cryptographic censorship, 2024. arXiv:2402.03425.
- 31 Marios Georgiou and Mark Zhandry. Unclonable decryption keys. Cryptology ePrint Archive, Paper 2020/877, 2020. URL: <https://eprint.iacr.org/2020/877>.
- 32 Vipul Goyal, Giulio Malavolta, and Justin Raizes. Unclonable commitments and proofs. Cryptology ePrint Archive, Paper 2023/1538, 2023. URL: <https://eprint.iacr.org/2023/1538>.
- 33 Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Going beyond Bell’s theorem. In Menas Kafatos, editor, *Bell’s Theorem, Quantum Theory and Conceptions of the Universe*, pages 69–72. Springer Netherlands, Dordrecht, 1989. doi:10.1007/978-94-017-0849-4\_10.
- 34 Dmitry Grinko, Adam Burchardt, and Maris Ozols. Gelfand-tsetlin basis for partially transposed permutations, with applications to quantum information, 2023. arXiv:2310.02252.
- 35 Dmitry Grinko and Maris Ozols. Linear programming with unitary-equivariant constraints, 2023. arXiv:2207.05713.
- 36 S. W. Hawking. Breakdown of predictability in gravitational collapse. *Phys. Rev. D*, 14:2460–2473, November 1976. doi:10.1103/PhysRevD.14.2460.
- 37 Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 2007(09):120, September 2007. doi:10.1088/1126-6708/2007/09/120.
- 38 Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. Cryptology ePrint Archive, Paper 2018/544, 2018. URL: <https://eprint.iacr.org/2018/544>.
- 39 Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP\* = RE. *Commun. ACM*, 64(11):131–138, 2021. doi:10.1145/3485628.
- 40 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. doi:10.1007/jhep02(2023)233.
- 41 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. doi:10.4230/LIPICs.TQC.2021.2.
- 42 Srijita Kundu and Ernest Y. Z. Tan. Device-independent uncloneable encryption, 2023. arXiv:2210.01058.
- 43 Jiahui Liu, Qipeng Liu, Luowen Qian, and Mark Zhandry. Collusion resistant copy-protection for watermarkable functionalities. 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 294–323. Springer, 2022. doi:10.1007/978-3-031-22318-1\_11.
- 44 Fermi Ma and Hsin-Yuan Huang. How to construct random unitaries. Cryptology ePrint Archive, Paper 2024/1652, 2024. URL: <https://eprint.iacr.org/2024/1652>.
- 45 N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65:3373–3376, December 1990. doi:10.1103/PhysRevLett.65.3373.
- 46 Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024*, pages 485–492. IEEE, 2024. doi:10.1109/FOCS61266.2024.00038.

- 47 Abel Molina, Thomas Vidick, and John Watrous. Optimal counterfeiting attacks and generalizations for Wiesner's quantum money. In Kazuo Iwama, Yasuhito Kawano, and Mio Murao, editors, *Theory of Quantum Computation, Communication, and Cryptography*, pages 45–64, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.
- 48 John Preskill. Do black holes destroy information? In *International Symposium on Black holes, Membranes, Wormholes and Superstrings*, January 1992. [arXiv:hep-th/9209058](https://arxiv.org/abs/hep-th/9209058).
- 49 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. [arXiv:1209.0448](https://arxiv.org/abs/1209.0448).
- 50 Marco Roncaglia. On the conservation of information in quantum physics. *Foundations of Physics*, 49:1278–1286, 2019. [doi:10.1007/s10701-019-00304-9](https://doi.org/10.1007/s10701-019-00304-9).
- 51 Or Sattath. Uncloneable cryptography, 2022. [doi:10.48550/arXiv.2210.14265](https://doi.org/10.48550/arXiv.2210.14265).
- 52 Michael Schlegel and Emina Soljanin. Winning rates of  $(n, k)$  quantum coset monogamy games. *arXiv preprint arXiv:2501.17736*, 2025. [doi:10.48550/arXiv.2501.17736](https://doi.org/10.48550/arXiv.2501.17736).
- 53 Michael Schlegel, Emina Soljanin, and Nicolas Swanson. Optimal strategies for winning certain coset-guessing quantum games. *arXiv preprint arXiv:2410.08160*, 2024. [doi:10.48550/arXiv.2410.08160](https://doi.org/10.48550/arXiv.2410.08160).
- 54 Eddie Schoute, Dmitry Grinko, Yigit Subasi, and Tyler Volkoff. Quantum programmable reflections, 2024. [arXiv:2411.03648](https://arxiv.org/abs/2411.03648).
- 55 B. M. Terhal. Is entanglement monogamous? *IBM Journal of Research and Development*, 48(1):71–78, 2004. [doi:10.1147/rd.481.0071](https://doi.org/10.1147/rd.481.0071).
- 56 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. [doi:10.1088/1367-2630/15/10/103002](https://doi.org/10.1088/1367-2630/15/10/103002).
- 57 R. F. Werner. Optimal cloning of pure states. *Phys. Rev. A*, 58:1827–1832, September 1998. [doi:10.1103/PhysRevA.58.1827](https://doi.org/10.1103/PhysRevA.58.1827).
- 58 Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. [doi:10.1145/1008908.1008920](https://doi.org/10.1145/1008908.1008920).
- 59 W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982. [doi:10.1038/299802a0](https://doi.org/10.1038/299802a0).
- 60 Mark Zhandry. How to record quantum queries, and applications to quantum indistinguishability. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 239–268. Springer, 2019. [doi:10.1007/978-3-030-26951-7\\_9](https://doi.org/10.1007/978-3-030-26951-7_9).
- 61 Mark Zhandry. How to construct quantum random functions. *J. ACM*, 68(5), 2021. [doi:10.1145/3450745](https://doi.org/10.1145/3450745).