A Computational Separation Between Quantum No-Cloning and No-Telegraphing

Barak Nehoran
Princeton University, NJ, USA

Mark Zhandry
NTT Research, Sunnyvale, CA, USA

Abstract

Two of the fundamental no-go theorems of quantum information are the no-cloning theorem (that it is impossible to make copies of general quantum states) and the no-teleportation theorem (the prohibition on telegraphing, or sending quantum states over classical channels without pre-shared entanglement). They are known to be equivalent, in the sense that a collection of quantum states is telegraphable if and only if it is clonable.

Our main result suggests that this is not the case when computational efficiency is considered. We give a collection of quantum states and quantum oracles relative to which these states are efficiently clonable but *not* efficiently telegraphable. Given that the opposite scenario is impossible (states that can be telegraphed can always trivially be cloned), this gives the most complete quantum oracle separation possible between these two important no-go properties.

We additionally study the complexity class clonableQMA, a subset of QMA whose witnesses are efficiently clonable. As a consequence of our main result, we give a quantum oracle separation between clonableQMA and the class QCMA, whose witnesses are restricted to classical strings. We also propose a candidate oracle-free promise problem separating these classes. We finally demonstrate an application of clonable-but-not-telegraphable states to cryptography, by showing how such states can be used to protect against key exfiltration.

2012 ACM Subject Classification Theory of computation → Quantum query complexity; Theory of computation → Oracles and decision trees; Theory of computation → Complexity classes; Theory of computation → Cryptographic primitives; Theory of computation → Quantum complexity theory

Keywords and phrases Cloning, telegraphing, no-cloning theorem, oracle separations

Digital Object Identifier 10.4230/LIPIcs.ITCS.2024.82

Related Version *Full Version*: https://arxiv.org/abs/2302.01858 [29]

1 Introduction

One of the defining features of quantum information is the no-cloning theorem: that it is impossible to copy a general quantum state [30, 34, 16]. Another fundamental no-go theorem is the no-teleportation theorem: that it is impossible (without any pre-shared entanglement) to send quantum information over a classical channel [33]. Because of the potential confusion with the very possible task of quantum teleportation [14], we prefer to use the term *telegraphing* to refer to this latter task.

These two no-go theorems are well-understood to be *equivalent*, in the following sense: given a set of quantum states $S = \{|\psi_1\rangle, |\psi_2\rangle, \cdots\}$, then states in S can be perfectly cloned if and only if they can be perfectly telegraphed, both clonability and telegraphability being equivalent to the states in S being orthogonal. Here, S being cloned means there is a process mapping $|\psi_i\rangle$ to two copies of $|\psi_i\rangle$. S being telegraphed means there is a deconstruction process which maps $|\psi_i\rangle$ into classical information c_i, and a reconstruction process that maps c_i back to $|\psi_i\rangle$.

Introducing Computational Constraints

The above discussion is information-theoretic. Here, we ask: *what happens when computational constraints are considered*? We consider a set S to be computationally clonable if there is a *polynomial-time* quantum algorithm that solves the cloning task on S. Likewise, we consider S to be computationally telegraphable if there is both a polynomial-time deconstruction and corresponding polynomial-time reconstruction procedure for S.

We observe the trivial relationship that computational telegraphing implies computational cloning: by running reconstruction twice on the deconstructed classical information c_i, one obtains two copies of $|\psi_i\rangle$, therefore cloning. This process is only twice as slow as the original telegraphing procedure, and is therefore efficient if telegraphing is efficient. However, the converse is a priori unclear: if a state can be cloned efficiently, it is not clear if there is an efficient process to deconstruct the state into a classical c_i and also an efficient process to turn c_i back into the quantum state.

1.1 Our Results

In this work, we provide evidence that no-cloning and no-telegraphing are *not* equivalent properties in the computationally bounded setting. Our main theorem is:

▶ **Theorem 1** (Informal presentation of Theorem 17)**.** *There exists a quantum oracle $\mathcal{O}$ and a set of quantum states S such that S can be efficiently cloned relative to $\mathcal{O}$, but there is no efficient telegraphing procedure relative to $\mathcal{O}$. Even more, there is no telegraphing procedure where the reconstruction is efficient, even if we allow deconstruction to be unbounded.*

In other words, while no-cloning implies no-telegraphing, the converse is not true, at least relative to a quantum oracle.

Counter-intuitively, we prove this theorem by starting from a certain set of orthogonal but computationally *unclonable* states (related to those used by [5]). By the trivial relationship that telegraphing implies clonability, we observe that these states cannot be efficiently telegraphed either. But of course, while these states can be cloned inefficiently (as they are all orthogonal), we need them to be clonable efficiently. We therefore augment the setup with a quantum oracle that performs this cloning in a single query. The main technical difficulty is that we need to show that despite adding this cloning oracle, telegraphing remains inefficient. We do this through a multistep process, gradually converting any supposed telegraphing scheme that uses this oracle into a telegraphing scheme that does not, reaching a contradiction.

An interesting consequence of our proof is that the no-telegraphing property holds, *even if the sender is allowed to be inefficient*. The only party that needs to be efficient to achieve a separation is the receiver.

We additionally bring to light certain applications of clonable-but-untelegraphable states to both complexity theory and cryptography.

1.1.1 Complexity Theory

An important open problem in quantum complexity theory is the question of whether quantum states are more powerful than classical strings as proofs (or witnesses) for efficient quantum computation. This is the question of whether the class QMA of problems which have efficiently verifiable quantum proofs is contained in the class QCMA of problems where a classical proof suffices [4]. A number of recent works [3, 18, 28, 23] have endeavored to give increasingly strong oracle separations between the two classes. We take a slightly different approach, inspired by clonable-but-untelegraphable states. We define a class clonableQMA

of problems which have quantum proofs that are *efficiently clonable*. It is easy to see that QCMA $\subseteq$ clonableQMA $\subseteq$ QMA, and we argue that clonableQMA is not likely equal to either of the other two. Specifically, we use the clonable-but-untelegraphable states of Theorem 1 to show a quantum oracle separation with QCMA:

▶ **Theorem 2** (Informal). *There exists a unitary quantum oracle $\mathcal{O}$ such that* clonableQMA$^{\mathcal{O}}$ *is not contained in* QCMA$^{\mathcal{O}}$.

We also give a candidate *oracle-free* promise problem separating these classes, and we show that any such problem would immediately yield clonable-but-untelegraphable quantum states. Finally, we argue that it is unlikely that QMA is contained in clonableQMA, as it would mean that every QMA-complete problem would have efficiently clonable witnesses and act as a barrier against the existence of public-key quantum money. For details on these complexity theoretic applications, see the full version of this paper [29].

1.1.2 Cryptography

While no-cloning has seen significant attention in cryptography (e.g. [1, 2, 7, 15]), no-telegraphing has so far received little-to-no attention. We give a proof-of-concept application of clonable-but-untelegraphable states to protecting against key exfiltration. See Section 1.2.1 below for a more expansive discussion of the result. This motivates the use of no-telegraphing as an useful cryptographic tool.

1.2 Motivation

The importance of the interplay between quantum information and computational complexity is becoming increasingly clear. For example, computational complexity played a crucial role in Harlow and Hayden's resolution to the black hole Firewall Paradox [22].

This interplay is also fundamentally important for many cryptographic applications. For example, despite certain information-theoretically secure quantum protocols [13], most cryptographic tasks still require computational constraints even when using quantum information [26, 25]. Nevertheless, combining quantum information with computational constraints opens up numerous possibilities, from minimizing computational assumptions [20, 8] to classically-impossible applications [1].

The previous examples show that scenarios with quantum information can be fundamentally altered by the presence of computational considerations. It is therefore important to develop a broad understanding of quantum information in the computationally bounded setting. This includes the famous no-go theorems of quantum information. Numerous prior works have studied no-cloning in the computational setting (see references in Section 1.3). However, the computational difficulty of telegraphing has, to the best of our knowledge, not been previously studied. As our work shows, the equivalence of two of the most important quantum no-go theorems no longer holds in the computationally bounded setting, giving a very different picture and allowing for new possibilities that do not exist in the information-theoretic setting.

1.2.1 Cryptographic Applications

Besides addressing fundamental questions, we also explore potential cryptographic applications of our separation.

Concretely, consider the following key exfiltration scenario: a server contains a cryptographic key, say, for decrypting messages. An attacker remotely compromises the server, and then attempts to exfiltrate the key, sending it from the compromised server to the attacker's computer.

A classical approach to mitigate this problem is *big key cryptography* [11, 10, 27], where the secret decryption key is made inconveniently large. This may make it impossible for the attacker to exfiltrate the key (perhaps there are bandwidth constraints on outgoing messages from the server) or at least makes it easier to detect the exfiltration (the large communication of the key may be easily detected). Unfortunately, such large keys are also inconvenient for the honest server, as now the server needs significant storage for each key (perhaps the server is storing keys for many different users). Moreover, decrypting using the key may be problematic, since the server will have to compute on a large key, which at least requires reading it from storage. If the server is decrypting many messages simultaneously using parallelism, then each process would presumably need to separately load the entire key from memory.

A quantum proposal would be to have decryption keys be quantum states. It is still reasonable to consider such a setting where all communication is classical: after all, the messages being encrypted and decrypted may just be classical. The server could therefore force all outgoing communication to be classical by measuring it. This would prevent the remote adversary from exfiltrating the key, by the non-telegraphability of the key.

Since telegraphing trivially implies cloning, we note that any classical program which has been quantum copy protected [1] will be immune from classical exfiltration. Copy protection for decryption keys was first considered by [19], and was constructed from indistinguishability obfuscation by [15], along with copy protection for pseudorandom functions and signatures.

However, using copy protection comes with its own limitations. Indeed, suppose the server is decrypting a large volume of incoming communication under a single decryption key. Classically, the server could divide the communication across several processors, with each decrypting in parallel. Unfortunately, this requires giving each processor a copy of the key. While trivial classically, the whole point of copy protection is to prevent copying. In fact, [6] consider exactly the task of preventing the use of parallelism via copy protection. The server could simply store numerous copies of each copy-protected key, but it would have to store these keys forever, even when the server is sitting idle or processing other tasks. This could be a major burden on the server. It also requires security to hold given multiple copies of the program, a non-trivial extension to single-copy security [24].

Instead, we imagine a protocol where the quantum keys *are* copy-able, but remain impossible to telegraph. This would protect against exfiltration, while allowing the server to only store a single copy of the key for long-term use. Then, if the incoming communication load ever becomes large, it can copy the key and spread the copies amongst several quantum processors that process the communication in parallel. After the load subsides and processors would return to being idle, the copies of the key can simply be discarded.

Assuming states that can be cloned but not telegraphed, we show how to realize an encryption scheme with the above features:

▶ **Theorem 3** (Informal). *Assume the existence of clonable-but-untelegraphable states which can be efficiently sampled. Additionally assume the existence of* extractable witness encryption for QMA. *Then there exists public key encryption with quantum secret keys that can be cloned but not exfiltrated.*

For the necessary witness encryption, we could use [9] as a candidate. Note that the states we construct relative to an oracle in Theorem 1 are efficiently sampleable. However, witness encryption requires non-black box use of the QMA language, meaning it cannot be applied to query-aided languages like that implied by Theorem 1. However, any standard-model realization of clonable-but-non-exfiltrateable states would suffice, and our Theorem 1 gives some evidence that such states exist. For details on the cryptographic applications, see the full version of this paper [29].

This is just one potential application of no-telegraphing that does not follow immediately from no-cloning. Our hope is that this work will motivate further study of no-telegraphing in cryptography.

1.2.2 On Oracles

Our separation between no-cloning and no-telegraphing requires oracles. Given the current state of complexity theory and the fact that these no-go properties are equivalent for computationally unbounded adversaries, we cannot hope to achieve unconditional separations between them in the standard model. As such, either computational assumptions or a relativized separation (that is, oracles) are required.

For cryptographic applications such as Theorem 3, certainly a standard-model construction from computational assumptions would be needed. On the other hand, by using oracles, we are able to give an unconditional separation, independent of what assumptions may or may not hold. While such a relativized separation does not necessarily rule out a standard-model equivalence, it shows a fundamental barrier to such an equivalence. Indeed, an immediate corollary of Theorem 1 is:

▶ **Corollary 4.** *There is no black box reduction showing the equivalence of cloning and telegraphing in the computational setting.*

We also note that our oracles as stated are sampled from a distribution, rather than being fixed oracles. This is typical of the cryptographic black-box separation literature. In the setting of uniform adversaries, a routine argument allows us to turn this into a fixed oracle relative to which the separations hold. We do this explicitly in the proof of Theorem 2 to get a separation relative to a fixed unitary oracle, and we further note that this directly implies such a separation between cloning and telegraphing as well.

1.3 Other Related Work

Cloning in the complexity-theoretic setting has been extensively studied during the last decade, in the context of public key quantum money [1, 17, 2, 37, 32] and copy protection [1, 7, 15].

A recent development in quantum money has been quantum money with *classical* communication [31, 6, 32]. This can be seen as a complement to our separation, giving a setting where a quantum state *is* telegraphable, but not clonable. In order to overcome the trivial telegraphing-implies-cloning result, however, these works move to *interactive* telegraphing, involving two or more messages between sender and receiver. Moreover, telegraphing happens in only a weak sense: the receiver does not get the original quantum state. Instead, the sender's quantum money state is actually irreversibly destroyed, but in the process the receiver is able to create a single new quantum money state.

1.4 Technical Overview

Let f be a random function with codomain much smaller than domain. Our clonable-but-not-telegraphable states will be the the superpositions over pre-images of f:

$$|\psi_z\rangle = \frac{1}{\sqrt{|f^{-1}(z)|}} \sum_{x|f(x)=z} |x\rangle$$

where $f^{-1}(z) := \{x|f(x) = z\}$ is the set of preimages of z in f.

As of now, the $|\psi_z\rangle$ are easily shown to be *un*clonable: if one could create two copies of $|\psi_z\rangle$, then measuring each would give two pre-images x_1, x_2 such that $f(x_1) = z = f(x_2)$. Since f has a small codomain, there are exponentially many x in the support of $|\psi_z\rangle$, and therefore $x_1 \neq x_2$ with overwhelming probability. Thus we obtain a collision for f, which is known to be intractable for query-bounded algorithms to random oracles, even ones with small codomains [36].

That the $|\psi_z\rangle$ are unclonable seems to be counterproductive for our aims. But it allows us to also readily prove that the $|\psi_z\rangle$ are also un-telegraphable: if one could telegraph $|\psi_z\rangle$, it means one can generate a classical a_z such that from a_z it is possible to reconstruct $|\psi_z\rangle$. But by running reconstruction multiple times, one obtains multiple copies of $|\psi_z\rangle$, contradicting no-cloning. This is not exactly how we prove un-telegraphability, but provides an intuition for why it should be true.

Now that we have an untelegraphable set of states, we make them clonable by adding a cloning oracle, which very roughly maps $|\psi_z\rangle \mapsto |\psi_z\rangle|\psi_z\rangle$ for all valid states $|\psi_z\rangle$ and does nothing on states that are not uniform superpositions of pre-images. This clearly makes the $|\psi_z\rangle$ clonable. The challenge is then to prove that telegraphing is still impossible, even given this cloning oracle. This is proved through a sequence of stages:

- **Stage 1.** Here, we remove the cloning oracle, and just consider the oracle f. We show that, with arbitrary classical advice a_z of polynomially-bounded size dependent on z (which could have been constructed in an arbitrary inefficient manner), it is impossible for a query-bounded algorithm to reconstruct $|\psi_z\rangle$. This is proved by showing that such a reconstruction procedure could be used to contradict known lower bounds on the hardness of finding K collisions [21].
  The above shows that even if we give the *sender* the cloning oracle, then telegraphing is still impossible for a query-bounded receiver, as long as the receiver does not have access to the cloning oracle. Indeed, the hypothetical output of such a sender would be an a_z contradicting the above.
- **Stage 2.** Here, we upgrade the receiver to have a limited cloning oracle that only clones a single $|\psi_z\rangle$, namely the unique state $|\psi_z\rangle$ that the receiver is trying to reconstruct.
  The intuition is that such a limited cloning oracle is of no use, since in order to query it on a useful input, the receiver needs to have $|\psi_z\rangle$ in the first place. We make this formal using a careful analysis.
- **Stage 3.** Finally, we give the receiver the full cloning oracle. We show that if there is such a query-bounded receiver that can successfully reconstruct, then we can compile it into a query-bounded receiver for Stage 2, reaching a contradiction.
  This is the most technically challenging part of our proof. The rough idea is that the Stage 2 receiver will simulate a set of imposter oracles, where it forwards queries relating to z to its own z-only cloning oracle, and all other queries it handles for itself. This simulation is not perfect, and care is required to prove that the simulation still allows for successful reconstruction.

Putting these together, we prove Theorem 1, that there cannot exist *any* telegraphing scheme for the set of $|\psi_z\rangle$ with a query-bounded receiver (regardless of whether the sender is query bounded).

▶ Remark 5. The above description requires two oracles, a classical random oracle (queryable in superposition) and the cloning oracle. We first note that superposition access to a random oracle is in particular unitary, so the classical random oracle is also a unitary. Second, we can view these two oracles as a single quantum oracle, which operates on two sets of registers, applying one oracle to one register and the other oracle to the other. For the single combined

oracle to be equivalent to the two individual oracles, we only need that the individual oracles have efficiently constructible fixed points. This is true of both the oracles we use. Thus, we obtain a separation relative to a single oracle sampled from an appropriate distribution.

2 Preliminaries

2.1 Query Magnitudes and Modifying Oracles

When working with quantum oracle algorithms, it is often useful to be able to bound the effect that replacing one oracle with another can have on the result of the computation. To this end, we recall the following definition and two theorems due to Bennett, Bernstein, Brassard, and Vazirani [12]:

▶ **Theorem 6** (Theorem 3.1 from [12]). *If two unit-length superpositions are within Euclidean distance ε then observing the two superpositions gives samples from distributions which are within total variation distance at most 4ε.*

▶ **Definition 7** (Definition 3.2 from [12]). *Let $|\phi_i\rangle$ be the superposition of M^A on input x at time i. We denote by $q_y(|\phi_i\rangle)$ the sum of squared magnitudes in $|\phi_i\rangle$ of configurations of M which are querying the oracle on string y. We refer to $q_y(|\phi_i\rangle)$ as the query magnitude of y in $|\phi_i\rangle$.*

▶ **Theorem 8** (Theorem 3.3 from [12]). *Let $|\phi_i\rangle$ be the superposition of M^A on input x at time i. Let $\varepsilon > 0$. Let $F \subseteq [0, T-1] \times \Sigma^*$ be a set of time-strings pairs such that $\sum_{(i,y)\in F} q_y(|\phi_i\rangle) \leq \frac{\varepsilon^2}{T}$. Now suppose the answer to each query $(i, y) \in F$ is modified to some arbitrary fixed $a_{i,y}$ (these answers need not be consistent with an oracle). Let $|\phi'_i\rangle$ be the time i superposition of M on input x with oracle A modified as stated above. Then $\big||\phi_T\rangle - |\phi'_T\rangle\big| \leq \varepsilon$.*

2.2 Measuring an approximation of a state

The following lemma is useful if we expect to have a pure quantum state $|\psi\rangle$, but instead, we only have an approximate version of it, ρ, which may in general be a mixed state. We want that any measurement on $|\psi\rangle$ can be approximately performed on ρ instead.

▶ **Lemma 9** (Measuring an approximation of a state). *Let $|\psi\rangle \in \mathcal{H}$ be a pure state, let Π be a measurement operator for the binary projective measurement $\{\Pi, \mathbb{I} - \Pi\}$ on $\mathcal{H}$, and let $\rho \in \mathcal{D}(\mathcal{H})$ be a mixed state such that*

1. $\langle\psi|\,\rho\,|\psi\rangle \geq p_1$
2. $\langle\psi|\,\Pi\,|\psi\rangle \geq p_2$

Then $\mathsf{tr}(\Pi\rho) \geq p_1 p_2 - 2\sqrt{(1-p_1)(1-p_2)}$.

This means that if ρ is very close to $|\psi\rangle\langle\psi|$, and the measurement given by Π succeeds with good probability on $|\psi\rangle$, then the same measurement also succeeds on ρ, though with appropriately smaller probability. For a proof of Lemma 9, see the full version of this paper [29].

3 Fundamental Tasks and Their No-go Properties

3.1 Schemes of Quantum States

We introduce the following syntax for a scheme of quantum states. A scheme is the basic structure on which the quantum no-go properties may or may not apply. In other words, some schemes may be clonable, for instance, while other schemes may not. Schemes consist primarily of a collection of quantum states, but they can also specify the collection of oracles which may be used, as well as a distribution for sampling from those states.

▶ **Definition 10** (Scheme). *In the context of quantum no-go properties, a* ***scheme****, $(S, \mathcal{D}, \mathcal{O})$, is an indexed collection of quantum states $S = \{|\psi_i\rangle\}_{i\in\mathcal{Z}}$ over an index set $\mathcal{Z}$ (which we call the set of labels), a distribution $\mathcal{D}$ over the labels, and a collection $\mathcal{O}$ of any quantum oracles that may be used.*

Whenever either the distribution or the oracles are irrelevant or otherwise clear from context, we will drop them from the notation and write $(S, \mathcal{O})$, $(S, \mathcal{D})$, or simply S. Note that the distribution $\mathcal{D}$, which allows sampling from the collection of states, is only important for defining average-case security of the scheme, and $\mathcal{O}$ is only necessary when considering oracle algorithms.

Under a certain scheme $(S, \mathcal{D}, \mathcal{O})$, *verification* of an unknown quantum state $|\phi\rangle$ for a label z is the measurement of whether $|\phi\rangle$ passes for the intended state $|\psi_z\rangle$, which succeeds with probability $p = |\langle\psi_z|\phi\rangle|^2$. When we say that an algorithm succeeds in passing verification with some probability p, we mean that verification succeeds with that probability over the randomness of the algorithm's output as well as the randomness of the sampling from $\mathcal{D}$ and that of the verification measurement. That is, if the algorithm is randomized and outputs a mixed state ρ_z when label z is drawn, then we say that it succeeds at verification for z with probability $p = \mathbb{E}_{z\leftarrow\mathcal{D}}\langle\psi_z|\rho_z|\psi_z\rangle$. This is the expected fidelity of the states produced by the algorithm with the intended state. Whenever an algorithm is tasked with passing verification for a label z, we call z the target label and we call $|\psi_z\rangle$ the target state.

3.2 Cloning and Telegraphing

We now formally define the tasks of cloning and telegraphing.

▶ **Definition 11** (Cloning). *A scheme S is said to be η-****worst case clonable*** *if there exists a quantum algorithm $\mathsf{Clone}(|\psi\rangle)$ such that for every label $z \in \mathcal{Z}$, when given $|\psi_z\rangle$, its corresponding quantum state in S, returns a quantum state $|\phi\rangle$ on two registers that, with probability at least η, passes verification for z on both registers simultaneously. That is, $\left|\left(\ \langle\psi_z| \otimes \langle\psi_z|\ \right)|\phi\rangle\right|^2 \geq \eta$.*

*$(S, \mathcal{D})$ is said to be η-****average case clonable*** *if there exists a quantum algorithm $\mathsf{Clone}(|\psi\rangle)$ that succeeds at the cloning task with probability η when z is sampled from the distribution $\mathcal{D}$.*

▶ **Definition 12** (Telegraphing). *A scheme S is said to be η-****worst case telegraphable*** *if there exists a pair of quantum algorithms $\mathsf{Send}(|\psi\rangle) \to c$ and $\mathsf{Receive}(c) \to |\phi\rangle$ where c is a classical string, such that for every label $z \in \mathcal{Z}$, when given $|\psi_z\rangle$, its corresponding quantum state in S, $|\phi\rangle := \mathsf{Receive}(\mathsf{Send}(|\psi_z\rangle))$ passes verification for z with probability at least η.*

*$(S, \mathcal{D})$ is said to be η-****average case telegraphable*** *if there exists a pair of quantum algorithms $\mathsf{Send}(|\psi\rangle) \to c$ and $\mathsf{Receive}(c) \to |\phi\rangle$ that succeed at the telegraphing task with probability η when z is sampled from the distribution $\mathcal{D}$.*

Note that quantum teleportation is the process by which a quantum state can be transmitted through a classical channel by the use of pre-shared quantum entanglement [14]. Telegraphing can thus be viewed as describing a quantum teleportation protocol without the use of entanglement: Send converts the quantum state $|\psi_z\rangle$ to a classical description c, which Receive then converts back into $|\psi_z\rangle$, or an approximation thereof. This is why the no-go theorem of the telegraphing task for general quantum states is often referred to as the *no-teleportation theorem*, a name first coined by the originator of the theorem [33]. This terminology can be confusing, however, since teleportation *is* in fact always possible when the sending and receiving parties are allowed to start out with an additional entangled quantum state. To sidestep this confusion, throughout this paper we instead use the term *telegraphing* for the unentangled no-go task. Here, and throughout this paper, any pair of algorithms attempting to achieve the telegraphing task are attempting to do so without the use of pre-shared entanglement.

3.3 Information Theoretic No-go Theorems

We now state a version of the (information theoretic) no-go theorems for these two tasks. The No-Cloning Theorem was first proved by three independent papers [30, 34, 16], but the version we present here is due to [35]. The No-Telegraphing Theorem (originally called the No-Teleportation Theorem), a corollary of the No-Cloning Theorem, is due to [33]. We present the two theorems here together to emphasize the direct connection between them.

▶ **Theorem 13** (No-Cloning Theorem and No-Telegraphing Theorem). *Let $\mathcal{H}$ be a Hilbert space, and let $S = \{|\psi_i\rangle\}_{i\in[k]}$ be a collection of pure quantum states on this Hilbert space. The following are equivalent:*

1. *S can be perfectly cloned*
2. *S can be perfectly telegraphed*
3. *S is a collection of orthogonal states, with duplication $(\forall i, j\ |\langle\psi_i|\psi_j\rangle|^2$ is either 0 or $1)$*

The proof of cases 1 and 3 is due to [35] and the addition of case 2 is due to [33]. Theorem 13 demonstrates that a general collection of quantum states cannot be cloned or telegraphed, but all orthogonal collections can.

3.4 Computational No-go Properties

We now define the efficient versions of the no-go tasks of cloning and telegraphing, and their associated computational no-go properties.

Computational Restrictions. We call the algorithms Clone, Send, and Receive the adversaries for their respective tasks. Specifying the class of algorithms from which the adversaries may originate allows us to further parameterize the definitions of these no-go tasks by computational complexity.

For instance, if the adversaries are required to be computationally efficient (polynomial-time) quantum algorithms, we say that the scheme is *efficiently* or *computationally* clonable (or unclonable, telegraphable, etc.). If the scheme includes oracles and the adversaries are quantum oracle algorithms that make a polynomial number of oracle queries, that is, query-efficient algorithms, then we say that the scheme is clonable (unclonable, telegraphable, etc.) by efficient oracle algorithms or query-efficient algorithms. The one thing to note is that for telegraphing by efficient oracle algorithms, we require as an additional restriction that the classical message c be of polynomial length. We often use the words "computational" and "efficient" as a catch-all for both computationally efficient and query-efficient algorithms,

and we use more specific terminology whenever it is necessary to differentiate between them. If the adversaries are not bounded in any way, we say that the scheme is *statistically* or *information-theoretically* clonable (unclonable, telegraphable, etc.).

Success Probability. We say that a scheme is η-*unclonable* or η-*untelegraphable* (in either the worst case or in the average case) if no quantum algorithm succeeds at the corresponding task with probability greater than η. We will often just drop the parameter η and simply say that a scheme is unclonable (or untelegraphable) if it is η-unclonable (respectively η-untelegraphable) for every non-negligible probability η (non-negligible in the length of the input, in qubits). We say that a scheme is perfectly clonable (or telegraphable) if it is clonable (respectively, telegraphable) with probability 1.

Telegraphing Implies Cloning. We now give the trivial direction of the relationship between computational cloning and computational telegraphing: that telegraphing implies cloning. This implication and its proof are certainly not a new result, even in the context of computational efficiency. However, both directions of the relationship have too often been taken for granted despite one direction not always holding. We therefore give a formal proof for the direction that *does* still hold in the context of efficient algorithms, both for completeness, as well as to contrast its simplicity with the relative complexity of the supposed converse.

▶ **Theorem 14** (Telegraphing Implies Cloning). *Any scheme that is $(1-\varepsilon)$-computationally telegraphable is also $(1-2\varepsilon)$-computationally clonable. Note that this applies to both computationally efficient and query-efficient algorithms as well as to both worst case and average case versions of these properties.*

Proof. We prove this for computationally efficient algorithms, and in the worst case, since the other cases are nearly identical to this one.

Let S be a scheme that is $(1-\varepsilon)$-telegraphable in the worst case by computationally efficient adversaries. That is, there exist efficient quantum algorithms $\mathsf{Send}(|\psi\rangle) \to c$ and $\mathsf{Receive}(c) \to |\phi\rangle$ such that for all $|\psi_z\rangle \in S$, $|\phi\rangle := \mathsf{Receive}(\mathsf{Send}(|\psi_z\rangle))$ passes verification for z with probability at least $1-\varepsilon$.

Without loss of generality, we assume that Send always outputs *some* message to send to $\mathsf{Receive}$. This is because it can always output an arbitrary/random message, which is no worse than outputting nothing. That is, on input $|\psi_i\rangle$, $\sum_{c\in\{0,1\}^*} \Pr[\mathsf{Send} \text{ outputs } c] = 1$.

The probably of successfully telegraphing is

$$p_{\text{successful telegraphing}} = \sum_c \Pr[\mathsf{Send} \text{ outputs } c] \Pr[\mathsf{Receive} \text{ succeeds on } c] > 1-\varepsilon$$

where the probabilities are taken over the internal randomness and measurements of the algorithms as well as over the randomness of verification.

So, if we run Send once on $|\psi_i\rangle$ to get message c and then run $\mathsf{Receive}$ twice on the same c, we get that the probability of successfully getting two copies of $|\psi_i\rangle$ is

$$\begin{aligned} p_{\text{successful cloning}} &= \sum_c \Pr[\mathsf{Send} \text{ outputs } c]\big(\Pr[\mathsf{Receive} \text{ succeeds on } c]\big)^2 \\ &\geq \left(\sum_c \Pr[\mathsf{Send} \text{ outputs } c] \Pr[\mathsf{Receive} \text{ succeeds on } c]\right)^2 \\ &\geq (1-\varepsilon)^2 = 1-2\varepsilon+\varepsilon^2 > 1-2\varepsilon \end{aligned}$$

Thus S is also $(1-2\varepsilon)$-clonable in the worst case, in time that is at most twice what it took to telegraph. ◀

Our main result, which we show in Section 4, is that the converse to this theorem does not hold, at least with respect to efficient oracle algorithms.

3.5 Reconstruction

Our central aim is to separate efficient cloning from efficient telegraphing. However, in order to do so, we find it convenient to introduce an additional third task, which we call *reconstruction*.

▶ **Definition 15** (Reconstruction). *A scheme S is said to be η-**worst case reconstructible** if there exists a quantum algorithm $\mathsf{Reconstruct}(a) \to |\phi\rangle$ such that for every label $z \in \mathcal{Z}$, there exists an instance-dependent advice string[1] a_z such that $|\phi\rangle := \mathsf{Reconstruct}(a_z)$ passes verification for z with probability at least η.*

*$(S, \mathcal{D})$ is said to be η-**average case reconstructible** if there exists a quantum algorithm $\mathsf{Reconstruct}(a) \to |\phi\rangle$ that succeeds at the reconstruction task with probability η when z is sampled from the distribution $\mathcal{D}$.*

The different parameterized versions of reconstruction are defined analogously to those of cloning and telegraphing. As with the classical message in the case of telegraphing, for reconstruction by efficient oracle algorithms, we require as an additional restriction that the advice string a_z be of polynomial length.

Reconstruction can be viewed in one way as a subtask of telegraphing, where we focus our attention only on the receiving end of the telegraphing, or in another way as a telegraphing protocol in which the sender is all-powerful and can implement a (potentially even nonphysical) function from $|\psi_z\rangle$ to a_z. (This function is in fact performing the task of what we call *deconstruction*, which we do not define here, but which can be roughly described as assigning a uniquely identifying label to every state in S.) Following this line of thought, we can observe another trivial implication: between telegraphing and reconstruction.

▶ **Theorem 16** (Telegraphing Implies Reconstruction). *Any scheme that is η-computationally telegraphable is also η-computationally reconstructible. Note that, as before, this applies to both computationally efficient and query-efficient algorithms as well as to both worst case and average case versions of these properties.*

Proof. The proof here is even simpler than that of Theorem 14. As we did in that proof, we prove this theorem only for computationally efficient algorithms, and in the worst case, since the other cases are much the same. Let S be a scheme that is η-telegraphable in the worst case by computationally efficient adversaries. That is, there exist efficient quantum algorithms $\mathsf{Send}(|\psi\rangle) \to c$ and $\mathsf{Receive}(c) \to |\phi\rangle$ such that for all $|\psi_z\rangle \in S$, $|\phi\rangle := \mathsf{Receive}(\mathsf{Send}(|\psi_z\rangle))$ passes verification for z with probability at least η.

For every $|\psi_z\rangle \in S$, $\mathsf{Send}(|\psi_z\rangle)$ produces an output c_z that comes from some distribution over classical strings. There must be at least one string c_z^* in its support for which $\mathsf{Receive}(c_z^*)$ succeeds with probability at least η (otherwise, $\mathsf{Receive}(c_z)$ has success probability less than η for all c_z, and so the telegraphing could not have succeeded with probability η). Thus, for each $z \in \mathcal{Z}$, let $a_z := c_z^*$ and let $\mathsf{Receive}$ be the reconstruction adversary, which we have just shown will succeed on input a_z with probability at least η for all $z \in \mathcal{Z}$. ◀

[1] Note that classical tasks become trivial when an adversary is given trusted advice that is *instance-dependent*, as opposed to depending only on the input length. However, the same is not the case for quantum tasks. A quantum task such as that of preparing a quantum state may still be non-trivial, even when given trusted classical advice that depends on each instance.

The direct consequence of Theorem 16 is that in order to show that a scheme is not telegraphable, it suffices to show that it is not reconstructible. In other words, in order to prove our separation between computational cloning and computational telegraphing, it suffices to show a scheme that can be computationally cloned but *not computationally reconstructed*. Reframing our aim in such a way simplifies the analysis because now we only have to deal with a single adversary in both situations (cloning and reconstruction), as opposed to two interacting adversaries for telegraphing. Furthermore, by doing so, we in fact end up showing a stronger separation.

4 Cloning without Telegraphability

We now come to the main theorem of the paper.

▶ **Theorem 17.** *There exists a scheme, relative to a quantum oracle, that on the one hand, can be perfectly cloned by an efficient quantum oracle algorithm in the worst case, but that on the other hand cannot be telegraphed by a pair of efficient quantum oracle algorithms with any non-negligible probability, even in the average case.*

As mentioned before, we in fact prove the following stronger theorem, which, as a consequence of Theorem 16, implies Theorem 17:

▶ **Theorem 18.** *There exists a scheme, relative to a quantum oracle, that on the one hand, can be perfectly cloned by an efficient quantum oracle algorithm in the worst case, but that on the other hand cannot be* ***reconstructed*** *by an efficient quantum oracle algorithm with any non-negligible probability, even in the average case.*[2]

The rest of Section 4 contains the proof of Theorem 18. In Section 4.1, we define the scheme, Scheme 23, and show that it is perfectly clonable. In Section 4.2, we prove that the scheme cannot be efficiently reconstructed.

The form of our scheme is based on a set of states introduced by [5] which take a uniform superposition over the preimages of a random oracle. These states cannot be cloned by query-efficient algorithms, so by Theorem 14 this directly implies that they are untelegraphable.[3] We want a scheme that is untelegraphable despite being clonable, so we add a cloning oracle, a quantum oracle that clones only this set of states. The main technical challenge is to show that access to this cloning oracle does not allow the adversaries to telegraph.

We start by showing that with just the random oracle, the states are not reconstructible, via a reduction from the problem of finding multi-collisions in the random oracle. We then show that allowing cloning for the target state cannot be detected by the adversary. We finally simulate the rest of the cloning oracle by replacing the random oracle with an impostor for which we know how to clone.

4.1 The Scheme

Before we give the scheme, we first give a few definitions that are useful both for defining the scheme and for the proof of its unreconstructibility.

[2] Note importantly that the fact that these quantum states cannot be efficiently reconstructed does not preclude them from appearing naturally and being used in efficient quantum computation, since they may nevertheless be efficiently *samplable*. That is, there may be an efficient way to sample from the set of states without being able to reconstruct any particular one of them on command. In fact, this is exactly the case for our scheme.

[3] Note, however, that this does not imply that they are unreconstructable. Nevertheless, we show that this is the case in Proposition 24.

We first define a cloning oracle for orthonormal sets. This is an oracle that successfully clones a specific subset of basis states for a given basis.

▶ **Definition 19** (Cloning oracle for a set). *Let $\mathcal{H}$ be a Hilbert space and let $S = \{|\psi_i\rangle\}_{i\in[k]}$ be an orthonormal subset of $\mathcal{H}$. Augment $\mathcal{H}$ with a special symbol $\perp$ outside the support of $\mathcal{H}$. That is, $|\perp\rangle$ is orthogonal to all of $\mathcal{H}$.*

*A **cloning oracle** $\mathcal{C}_S$ on set $S = \{|\psi_i\rangle\}_{i\in[k]}$ is a quantum oracle that, for all $i \leq k$ sends $|\psi_i\rangle|\perp\rangle$ to $|\psi_i\rangle|\psi_i\rangle$ and $|\psi_i\rangle|\psi_i\rangle$ to $|\psi_i\rangle|\perp\rangle$. For all other orthogonal states, it applies the identity. That is, when the second register is $|\perp\rangle$, it clones any state in S and leaves all other orthogonal states unmodified.*

▶ **Definition 20** (Preimage superposition state). *Let $f : \{0,1\}^m \to \{0,1\}^n$. A **preimage superposition state** for image $z \in \{0,1\}^n$ in function f is the quantum state that is the uniform positive superposition of preimages of z in f:*

$$|\psi_z\rangle = \frac{1}{\sqrt{|f^{-1}(z)|}} \sum_{x|f(x)=z} |x\rangle$$

where $f^{-1}(z) := \{x|f(x) = z\}$ is the set of preimages of z in f.

▶ **Definition 21** (Preimage superposition set). *Let $f : \{0,1\}^m \to \{0,1\}^n$. A **preimage superposition set for** f, S_f, is the set of preimage superposition states for all images in the range of f.*

$$S_f := \left\{ \frac{1}{\sqrt{|f^{-1}(z)|}} \sum_{x|f(x)=z} |x\rangle \;\middle|\; z \in \{0,1\}^n \right\}$$

▶ **Definition 22** (Cloning oracle relative to a function). *Let $f : \{0,1\}^m \to \{0,1\}^n$. A **cloning oracle relative to** f, $\mathcal{C}_f$, is a cloning oracle for the preimage superposition set, S_f, of f.*

We now give the formal definition of the scheme:

▶ **Scheme 23.** *Let $H : \{0,1\}^m \to \{0,1\}^n$ be a random oracle, where $m \geq 2n$ (but bounded by a polynomial in n). Let $\mathcal{C}_H$ be the cloning oracle relative to H. The scheme consists of the following:*

- *The collection of oracles is $\mathcal{O} := \{H, \mathcal{C}_H\}$.*
- *The set of states is $S := S_H$, the preimage superposition set for H.*
- *The distribution, $\mathcal{D}$, samples the image of a random domain element of H. That is, it returns $z \leftarrow H(x)$ for a uniformly random $x \in \{0,1\}^m$.*

It is clear that the scheme presented here is perfectly clonable in the worst case by an efficient quantum oracle algorithm. Specifically, the cloning oracle, $\mathcal{C}_H$, provides that capability, and in a single oracle query. Therefore, it remains to show that no efficient quantum oracle algorithm can reconstruct it. This is the main technical challenge of our proof and takes up the remaining part of Section 4.[4]

[4] As is evident from Scheme 23, we prove Theorems 17 and 18 relative to a quantum oracle (or rather, a pair of quantum oracles) sampled from a probability distribution rather than a fixed quantum oracle. However, as mentioned in the introduction to the paper, this is not a weakness, as a straightforward transformation allows fixing the randomness at the cost of the proof becoming non-constructive. For details, refer to the full version of the paper [29].

4.2 Proof of Unreconstructibility

We wish to prove that Scheme 23 cannot be efficiently reconstructed by efficient quantum oracle algorithms in the average case. We prove this in a sequence of three stages, beginning with a simplified version of the scheme without a cloning oracle, then moving to one with an oracle that can only clone a single state, and finally to the full scheme with the full cloning oracle.

4.2.1 With No Cloning Oracle

In the first stage, we consider an adversary, R, which is a quantum oracle algorithm with advice. R is given a polynomial length advice string a_z, and is allowed a polynomial number of queries to the random oracle. It is tasked with producing a state that passes verification for z, namely the positive uniform superposition over all the preimages of z in the random oracle. Note that this first version does not yet have access to a cloning oracle of any sort.

▶ **Proposition 24.** *Let R be a quantum oracle algorithm that is given a classical advice string $a_z \in \{0,1\}^\ell$ for some polynomial ℓ in n, and makes q queries to the random oracle, where q is a polynomial in n. For $z \in \{0,1\}^n$ drawn uniformly at random, R cannot output a quantum state that passes verification for z with probability that is non-negligible in n.*[5]

Proof. The main idea is that if R were able to produce the target state $|\psi_z\rangle$ with non-negligible probability, then it can also do so without the advice by guessing the advice string, albeit with significantly lower probability. Measuring $|\psi_z\rangle$ then gives a random preimage of the random oracle, and we can do this multiple times to produce several preimages of the same image z, producing a multi-collision for the random oracle, which is harder to do than this method would give.

We now give the proof. Suppose, for the sake of contradiction, that R, when given advice string a_z, makes q queries to the random oracle and then produces the mixed state ρ_z which passes verification for z with non-negligible probability η (that is, $\langle\psi_z|\,\rho_z\,|\psi_z\rangle \geq \eta$). We use R to produce a large number of disjoint collisions of the oracle.

Let $H^{-1}(z)$ be the set of preimages of z in H. We have that with high probability, $|H^{-1}(z)| \geq \Omega(2^{m-n})$. Let $\Gamma \subset H^{-1}(z)$ be an arbitrary polynomial sized subset of $H^{-1}(z)$, and let Π be the binary projective measurement that projects onto the preimages of z that are not in Γ, that is, onto the computational basis states $H^{-1}(z) \setminus \Gamma$. We have that $\langle\psi_z|\,\Pi\,|\psi_z\rangle \geq 1-\epsilon$ for $\epsilon = \frac{|\Gamma|}{|H^{-1}(z)|} \in \mathsf{negl}(n)$. Given that $\langle\psi_z|\,\rho_z\,|\psi_z\rangle \geq \eta$, we apply Lemma 9 to get that $\mathsf{tr}(\Pi\rho_i) \geq \eta(1-\epsilon) - 2\sqrt{\epsilon(1-\eta)} \geq \frac{1}{2}\eta$ for sufficiently large n. In other words, for any polynomial sized subset of preimages, and for sufficiently large n, we have that measuring ρ_z will with non-negligible probability give a preimage of z outside that subset.

Let k be a sufficiently large polynomial in n, for instance let $k = 2n(\ell+1)$ (note that ℓ is itself a positive integer bounded by a polynomial in n). We run R repeatedly (on the same target label z and advice a_z) a total of $8k/\eta$ times and measure the outcome in the computational basis, with the goal of producing at least $2k$ unique preimages of z. By a Chernoff bound, this then succeeds with constant probability $\Omega(1)$: that is, if X is the number of valid unique preimages, $\Pr\left[X \leq \frac{1}{2}(4k)\right] \leq e^{-4k/8} = e^{-n(\ell+1)} \leq 1/2$. Finally,

[5] Note that the advice string, a_z, may in general contain *any* information, including, for instance, any details about the set of preimages of z in H, or any other useful information about the task. We show here that no polynomial amount of classical information *of any kind* will allow R to faithfully reconstruct the state.

because every pair of unique preimages is a collision, this gives k disjoint collisions of the random oracle. That is, this process therefore produces k disjoint collisions with constant probability $\Omega(1)$.

Now, if this process succeeds given the advice $a_z \in \{0,1\}^\ell$, then it can also succeed without being given advice, though with a much lower probability, by guessing the advice string with probability $2^{-\ell}$, for an overall success probability of at least $\Omega(2^{-\ell})$.

To recap, this gives an quantum oracle algorithm for producing k disjoint collisions of a random oracle which makes $t = 8kq/\eta$ oracle queries and succeeds with probability at least $\Omega(2^{-\ell})$.

On the other hand, we recall the following theorem from Hamoudi and Magniez [21]:

▶ **Theorem 25** (Theorem 4.6 from [21]). *The success probability of finding K disjoint collisions in a random function $f : [M] \to [N]$ is at most $O(T^3/(K^2N))^{K/2} + 2^{-K}$ for any algorithm making T quantum queries to f and any $1 \leq K \leq N/8$.*

Applying the bound from the above Theorem 25 with $T = 8kq/\eta$, $K = k$, $M = 2^m$ and $N = 2^n$, the success probability for this task must be at most

$$O\left(\frac{T^3}{K^2N}\right)^{K/2} + 2^{-K} = O\left(\frac{(8kq/\eta)^3}{k^2 2^n}\right)^{k/2} + 2^{-k} = O\left(\frac{kq^3}{\eta^3 2^n}\right)^{k/2} + 2^{-k}$$
$$\leq 2^{-\Omega(k)} \leq 2^{-\Omega(n(\ell+1))}$$

There therefore exists a sufficiently large n, for which this is a contradiction. This completes the proof of Proposition 24. ◀

4.2.2 With a Limited Cloning Oracle

In the second stage, we allow R access to a limited cloning oracle which can clone only the target state.

▶ **Definition 26.** *Let z be a label and $|\psi_z\rangle$ the corresponding quantum state from the scheme. A **z-cloning oracle**, $\mathcal{C}_z$, is a cloning oracle for the singleton set $\{|\psi_z\rangle\}$.*

▶ **Proposition 27.** *Let R be a quantum oracle algorithm that is given a classical advice string $a_z \in \{0,1\}^\ell$ for some polynomial ℓ in n, and makes q queries (where q is a polynomial in n) to the random oracle **as well as a z-cloning oracle**. Let R' be a run of R where queries to the z-cloning oracle are instead returned unmodified (or equivalently, passed to a dummy oracle which acts as the identity). Then the total variation distance between the outcomes of the two runs is negligible in n.*

Proof. The idea is that since the z-cloning oracle and the dummy oracle differ only on the basis states where the first register is $|\psi_z\rangle$, if R puts low query weight on those basis states, then swapping between the oracles can only make minimal difference.

We now give the proof. Consider an adversary R which, when given advice string a_z, makes k queries to the random oracle and q queries to the z-cloning oracle. Let R' be a quantum oracle algorithm which simulates a run of R in which the z-cloning oracle is replaced by a dummy oracle (an oracle which acts as the identity on all states) by ignoring all of the z-cloning oracle queries (equivalent to performing the identity on each one).

For each $t \in [q]$, let R'_t be a version of R' in which the simulation is stopped prematurely at cloning query number t and which then outputs the first register of the query input. Let ρ'_t be the reduced density matrix of the outputted state. Because the runs of R' and R'_t

are identical up until R'_t stops and outputs cloning query number t, ρ'_t is also the reduced state of the first query register when R' requests query number t. Let $\eta'_t := \langle\psi_z|\rho'_t|\psi_z\rangle$ be the probability that ρ'_t would pass verification for z. As above, since each R'_t is a quantum oracle algorithm with advice that satisfies the conditions of Proposition 24, all the η'_t must be negligible in n.

Choose a basis $\{|\chi_i\rangle\}_{i\in[0,\dim(\mathcal{H})]}$ for $\mathcal{H}' := \mathcal{H} \oplus |\perp\rangle$ as in Definition 19, that includes $|\chi_0\rangle := |\perp\rangle$ and $|\chi_z\rangle := |\psi_z\rangle$ as two basis elements. Let D be a unitary from this basis into the computational basis that sends $|\psi_z\rangle|\perp\rangle$ to $|z\rangle|0\rangle$ and $|\psi_z\rangle|\psi_z\rangle$ to $|z\rangle|1\rangle$ and which arbitrarily assigns all other orthogonal states to computational basis states. (For example, let $B = \sum_i |i\rangle\langle\chi_i|$, let $C = \sum_{ij\notin\{(z,1),(z,z)\}} |i\rangle|j\rangle\langle i|\langle j| + |z\rangle|1\rangle\langle z|\langle z| + |z\rangle|z\rangle\langle z|\langle 1|$, and let $D = C\cdot(B\otimes B)$.)

In this basis, both the z-cloning oracle and the dummy oracle can be expressed as applications of binary classical functions on all but the last bit. The z-cloning oracle becomes an application of the classical indicator function for the string $(z, 0^{m-1})$: $f_{=z}(x) = \begin{cases} 1 & x = (z, 0^{m-1}) \\ 0 & \text{otherwise} \end{cases}$, and the dummy cloning oracle becomes an application of the all-zero function $f_\emptyset(x) = 0$. Let $\mathcal{O}_{=z}$ be the unitary application of the indicator function, $f_{=z}(x)$ above, which XORs the result into the last bit. Then the z-cloning oracle can be expressed as $\mathcal{C}_z = D^\dagger\mathcal{O}_{=z}D$, and the dummy oracle can be expressed as $\mathcal{C}_\emptyset = D^\dagger\mathcal{O}_{\text{identity}}D = D^\dagger ID = I$.

The algorithms R, R', and $\{R'_t\}_{t\in[q]}$ can therefore be reformulated as quantum oracle algorithms that direct cloning queries to the classical oracles $\mathcal{O}_{=z}$ in the case of R, or $\mathcal{O}_{\text{identity}}$ in the case of R' and $\{R'_t\}_{t\in[q]}$. That is, before they make a cloning query, they apply the change of basis D into the computational basis. They then query $\mathcal{O}_{=z}$ or $\mathcal{O}_{\text{identity}}$, and then apply the change of basis $D^\dagger$ back to the original basis. Call the versions of R, R', and $\{R'_t\}_{t\in[q]}$ in this new basis $\mathcal{R}$, $\mathcal{R}'$, and $\{\mathcal{R}'_t\}_{t\in[q]}$.

Note that the only difference between $\mathcal{R}$ and $\mathcal{R}'$ is that cloning queries to $\mathcal{O}_{=z}$ in $\mathcal{R}$ are redirected to $\mathcal{O}_{\text{identity}}$ in $\mathcal{R}'$. Furthermore, $\mathcal{O}_{=z}$ and $\mathcal{O}_{\text{identity}}$ only differ on inputs where the first register is $|z\rangle$.

We now therefore compute the query magnitude of cloning queries of $\mathcal{R}'$ on $|z\rangle$. The state of the first register of cloning query number t of $\mathcal{R}'$ to $\mathcal{O}_{\text{identity}}$ is given by $B\rho'_tB^\dagger = \sum_{i,j} |i\rangle\langle\chi_i|\,\rho'_t\,|\chi_j\rangle\langle j|$. The query magnitude on $|z\rangle$ is then $\langle z|\left(\sum_{i,j}|i\rangle\langle\chi_i|\,\rho'_t\,|\chi_j\rangle\langle j|\right)|z\rangle = \langle\chi_z|\rho'_t|\chi_z\rangle = \langle\psi_z|\rho'_t|\psi_z\rangle = \eta'_t$.

We now apply Theorem 8 on the set $F := \{(i,y) \mid i\in[q], y = z\}$ and $\varepsilon := \sqrt{T\sum_{t=1}^T \eta'_t}$, with $T := q$. The sum of the query magnitudes of $\mathcal{R}'$ on F is then $\sum_{t=1}^T \eta'_t \le \frac{\varepsilon^2}{T}$. Let $|\phi\rangle$ and $|\phi'\rangle$ be the states outputted by $\mathcal{R}$ and $\mathcal{R}'$ respectively (and therefore also by R and R' respectively). Since $\mathcal{R}$ is identical to $\mathcal{R}'$, with the only difference being that the cloning oracle queries are modified on the set F, then by Theorem 8, $\big||\phi\rangle - |\phi'\rangle\big| \le \varepsilon$. By Theorem 6, then, the total variation distance between runs of R and R' is therefore at most $4\varepsilon = 4\sqrt{q\sum_{t=1}^q \eta'_t}$, which is negligible, since all the η'_t are negligible and q is a polynomial. ◀

▶ **Corollary 28.** *Let R be a quantum oracle algorithm that is given a classical advice string $a_z \in \{0,1\}^\ell$ for some polynomial ℓ in n, and makes q queries (where q is a polynomial in n) to the random oracle **as well as a z-cloning oracle**. For $z \in \{0,1\}^n$ drawn uniformly at random, R cannot output a quantum state that passes verification for z with probability that is non-negligible in n.*

Proof. Suppose that R, when given advice string a_z, makes k queries to the random oracle and q queries to the z-cloning oracle, and then produces a state ρ_z which passes verification for z with probability η. As in Proposition 27, let R' be a run of R in which queries to the

z-cloning oracle are returned unmodified. R' is then a quantum oracle algorithm with advice that satisfies the conditions of Proposition 24, so it must have negligible success probability η'. By Proposition 27, the total variation distance between runs of R and R' is negligible in n so η is at most negligibly larger than η', and thus negligible as well. ◀

4.2.3 With the Full Cloning Oracle

In the third stage, we finally allow R access to the full cloning oracle, which clones all valid states of the scheme while doing nothing for invalid states.

▶ **Proposition 29.** *Let R be a quantum oracle algorithm that is given a classical advice string $a_z \in \{0,1\}^\ell$ for some polynomial ℓ in n, and makes q queries (where q is a polynomial in n) to the random oracle **and a full cloning oracle** for the set of valid states. For $z \in \{0,1\}^n$ drawn uniformly at random, R cannot output a quantum state that passes verification for z with probability that is non-negligible in n.*

Proof. Note that in showing this, we are demonstrating that the ability to clone other valid states does not help it produce the target state. The idea is use R to produce a new adversary R' which queries just the z-cloning oracle with comparable success. Ideally we would take a z-cloning oracle and simply simulate the rest of the cloning oracle (for states other than the target state) by using the random oracle. However, such a simulation would require a large number of queries to the random oracle and thus be highly inefficient. We get around this issue by creating an imposter random oracle and simulating cloning queries relative to it rather than relative to the original random oracle. We must show first that the impostor random oracle is indistinguishable from the original random oracle, and second that it is possible to approximately simulate cloning queries to the impostor oracle.

We now give the proof. Consider an adversary R which, when given advice string a_z, makes q queries to the random oracle and the full cloning oracle, and then with probability η produces a state $|\psi_z\rangle$ which passes verification for z. We use R to produce a similar algorithm, R', which only makes cloning queries to the z-cloning oracle, and which must succeed with comparable probability. We produce R' as follows:

We first sample a private random function, $H_{\text{private}} : \{0,1\}^m \to \{0,1\}^n \setminus \{z\}$, which has a limited codomain such that it does not output z. That is, for each input, independently choose a uniformly random element of $\{0,1\}^n \setminus \{z\}$.

We then create an impostor random oracle, $H_{\text{impostor}} : \{0,1\}^m \to \{0,1\}^n$, by combining the original and private random oracles in the following way:

$$H_{\text{impostor}}(x) = \begin{cases} z & H(x) = z \\ H_{\text{private}}(x) & \text{otherwise} \end{cases}$$

That is, on query input x, if x is a preimage of z in H, it passes the query to the original random oracle, producing z, but otherwise passes it to the newly sampled private random oracle.

We also create a cloning oracle relative to this impostor random oracle, $\mathcal{C}_{\text{impostor}}$. This *impostor cloning oracle* clones the states that are valid for the impostor random oracle, which will in general be different than the set of valid states of the original random oracle. We claim that the impostor oracles perfectly mimic the originals.

▷ Claim 30. The joint distribution of target image z and the impostor random oracle H_{impostor} is identical to that of z and H. That is, H_{impostor} is distributed as a uniform random oracle conditioned on z being one of its images.

Proof. To show this, we begin giving an equivalent lazy method of sampling the random oracle H, along with sampling the target image z.

First, we choose a random element $x^* \in \{0,1\}^m$ in the domain of H. We then randomly choose $z \in \{0,1\}^n$ as both its image in H and as the target image. Then, for each of the remaining elements of the domain of H, sample a random image from its range.

We now describe a similar method for lazily sampling the impostor random oracle H_{impostor}, along with the target image z.

As before, we choose a random element $x^* \in \{0,1\}^m$ in the domain, and a random image $z \in \{0,1\}^n$ as both its image in H_{impostor} and as the target image. For each remaining element, x, of the domain, we first sample a random image y. If $y \neq z$, resample an independent sample y' from $\{0,1\}^n \setminus \{z\}$ to be the image of x. Since, conditioned on $y \neq z$, y is uniform on $\{0,1\}^n \setminus \{z\}$, and so is y', the resampled image y' is identically distributed to the original y. The extra resampling performed to sample H_{impostor} thus has no effect on the distribution, so this process produces a distribution identical to the one above for sampling H and z. ◁

As a consequence, no quantum oracle algorithm can tell the difference between query access to the original oracles H and $\mathcal{C}_H$, and query access to the impostor oracles H_{impostor} and $\mathcal{C}_{\text{impostor}}$. That is, an algorithm R'' which simulates R and redirects its oracle queries to the impostor oracles will succeed with the same probability η.

This completes the first part, showing that the impostor oracles are perfect replacements for the original oracles. It now remains to show that the impostor oracles can be simulated efficiently in terms of the number of queries to the original random oracle H and a z-cloning oracle $\mathcal{C}_z$.

Note that implementing $\mathcal{C}_{\text{impostor}}$ using H and $\mathcal{C}_z$ may be query inefficient. We therefore create a new efficient impostor cloning oracle $\widehat{\mathcal{C}}_{\text{impostor}}$, which for each query only makes a constant number of queries to H and $\mathcal{C}_z$, but which nevertheless performs nearly as well as the inefficient $\mathcal{C}_{\text{impostor}}$.

We would like to define $\widehat{\mathcal{C}}_{\text{impostor}}$ by saying that it acts on computational basis states approximately as

$$\widehat{\mathcal{C}}_{\text{impostor}}|x\rangle|y\rangle = \begin{cases} \mathcal{C}_z|x\rangle|y\rangle & H(x) = z \\ \mathcal{C}_{\text{private}}|x\rangle|y\rangle & \text{otherwise} \end{cases}$$

However, in reality, this is not unitary, since the resulting states will not be exactly orthogonal. We instead define it with an additional ancilla qubit as follows:

Define the following two unitaries acting on an ancilla qubit $|b\rangle$ as well as the two input registers (of the cloning oracle).

$$\mathcal{U}_1|b\rangle|x\rangle|y\rangle = \begin{cases} |b \oplus 1\rangle|x\rangle|y\rangle & H(x) = z \\ |b\rangle|x\rangle|y\rangle & \text{otherwise} \end{cases}$$

$$\mathcal{U}_2|b\rangle|x\rangle|y\rangle = \begin{cases} |b\rangle \otimes \mathcal{C}_z|x\rangle|y\rangle & b = 1 \\ |b\rangle \otimes \mathcal{C}_{\text{impostor}}|x\rangle|y\rangle & \text{otherwise} \end{cases}$$

The action of $\mathcal{C}_{\text{impostor}}$ with an extra ancilla qubit can be expressed as $I \otimes \mathcal{C}_{\text{impostor}}\,|0\rangle\,|x\rangle\,|y\rangle = \mathcal{U}_1\mathcal{U}_2\mathcal{U}_1\,|0\rangle\,|x\rangle\,|y\rangle$. That is, after applying $\mathcal{U}_1$, then $\mathcal{U}_2$ acts as $I \otimes \mathcal{C}_{\text{impostor}}$ because whenever $H(x) = z$, then $\mathcal{C}_z|x\rangle|y\rangle = \mathcal{C}_H|x\rangle|y\rangle = \mathcal{C}_{\text{impostor}}|x\rangle|y\rangle$. Furthermore, for any $x \in \{0,1\}^m$, the support of the state $\mathcal{C}_{\text{impostor}}|x\rangle|y\rangle$ is only on computational basis states $|x'\rangle|y'\rangle$ such that $H(x') = z \Leftrightarrow H(x) = z$, which implies that the second application of $\mathcal{U}_1$ properly uncomputes its own action on the ancilla qubit.

We now define a modified version of $\mathcal{U}_2$, but which makes no use of $\mathcal{C}_{\text{impostor}}$, and instead uses $\mathcal{C}_{\text{private}}$, the cloning oracle relative to H_{private}:

$$\widehat{\mathcal{U}}_2|b\rangle|x\rangle|y\rangle = \begin{cases} |b\rangle \otimes \mathcal{C}_z|x\rangle|y\rangle & b = 1 \\ |b\rangle \otimes \mathcal{C}_{\text{private}}|x\rangle|y\rangle & \text{otherwise} \end{cases}$$

We thus define $\widehat{\mathcal{C}}_{\text{impostor}} = \mathcal{U}_1\widehat{\mathcal{U}}_2\mathcal{U}_1$, which we note makes two queries to H and one query[6] to $\mathcal{C}_z$ on each application (note that $\mathcal{C}_{\text{private}}$ uses no oracle queries as it can be simulated directly using the private random function H_{private}). It remains to show that, when the ancilla qubit is initialized to $|0\rangle$, $\widehat{\mathcal{C}}_{\text{impostor}}$ cannot be distinguished from $I \otimes \mathcal{C}_{\text{impostor}}$. That is, we show that it is a good efficient approximation for $\mathcal{C}_{\text{impostor}}$.

We observe that the actions of $I \otimes \mathcal{C}_{\text{impostor}}$ and $\widehat{\mathcal{C}}_{\text{impostor}}$ differ only in whether they apply $\mathcal{C}_{\text{impostor}}$ or $\mathcal{C}_{\text{private}}$ (in $\mathcal{U}_2$ and $\widehat{\mathcal{U}}_2$ respectively) on the two non-ancilla registers, and only on basis states for which the first of those registers is not a preimage of z. In fact they differ only by a change of basis between a basis that includes the preimage superposition set of H_{private} and one that includes the preimage superposition set of H_{impostor}.

Taking a closer look at H_{impostor} and H_{private}, the only difference between the functions is that the domain elements that are preimages of the target image z in H_{impostor} are reassigned to another random image in H_{private}. Moreover, since the difference we observe in this setting is only for domain elements that do not map to z in H (and thus in H_{impostor}), we can set aside z in the analysis and focus on the other images.

Let $|\psi_i\rangle$ and $|\widehat{\psi}_i\rangle$ be the respective preimage superposition states of H_{impostor} and H_{private} for image $i \in \{0,1\}^n \setminus \{z\}$. Let $\theta_i := \cos^{-1}\left(\langle\psi_i|\widehat{\psi}_i\rangle\right)$ be the small angle between them. Further, let $|\psi_{z\to i}\rangle$ be the equal positive superposition over any preimages of the target image, z, in H_{impostor} that were reassigned to image i in H_{private}. Then we can write $|\widehat{\psi}_i\rangle = \cos(\theta_i)|\psi_i\rangle + \sin(\theta_i)|\psi_{z\to i}\rangle$.

Note that for all $i \neq j$, $\langle\psi_i|\widehat{\psi}_j\rangle = \cos(\theta_j)\langle\psi_i|\psi_j\rangle + \sin(\theta_j)\langle\psi_i|\psi_{z\to j}\rangle = 0$ because the supports of the states (that is, their sets of preimages) are disjoint (where note again that we exclude the target image z here). And of course, each of the preimage superposition sets is orthogonal within the set: $\langle\psi_i|\psi_j\rangle = \langle\widehat{\psi}_i|\widehat{\psi}_j\rangle = 0 \quad \forall i \neq j$.

We can therefore partition the Hilbert space into $2^n - 1$ orthogonal planes, each of which is spanned by a $|\psi_i\rangle$ and its corresponding $|\widehat{\psi}_i\rangle$ (or $|\psi_{z\to i}\rangle$), as well as a remaining space orthogonal to all those planes. With this perspective, the change of basis that differentiates between $\mathcal{C}_{\text{impostor}}$ and $\widehat{\mathcal{C}}_{\text{impostor}}$ can be described as a small rotation of angle θ_i in each of these planes and the identity in the remaining space.

$$\begin{aligned}\mathcal{U}_3 := I &- \sum_i \left(|\psi_i\rangle\langle\psi_i| + |\psi_{z\to i}\rangle\langle\psi_{z\to i}|\right) \\ &+ \sum_i \left(\cos(\theta_i)|\psi_i\rangle + \sin(\theta_i)|\psi_{z\to i}\rangle\right)\langle\psi_i| + \left(-\sin(\theta_i)|\psi_i\rangle + \cos(\theta_i)|\psi_{z\to i}\rangle\right)\langle\psi_{z\to i}|\end{aligned}$$

Then,

$$I \otimes \mathcal{C}_{\text{impostor}}\,|0\rangle\,|x\rangle\,|y\rangle = \mathcal{U}_1\mathcal{U}_2\mathcal{U}_1\,|0\rangle\,|x\rangle\,|y\rangle \quad \text{and} \quad \widehat{\mathcal{C}}_{\text{impostor}} = \mathcal{U}_1(\mathcal{U}_3^\dagger \otimes \mathcal{U}_3^\dagger)\mathcal{U}_2(\mathcal{U}_3 \otimes \mathcal{U}_3)\mathcal{U}_1$$

[6] Note that it is straightforward to implement a controlled version of $\mathcal{C}_z$ using a single query to $\mathcal{C}_z$, as it is for any oracle for which a fixed state, on which it acts as the identity, is known. In this case, the fixed state is $|\perp\rangle|\perp\rangle$. To do so, we prepare the state $|\perp\rangle|\perp\rangle$ in an ancilla register. We then apply a 0-controlled SWAP gate between this register and the input register on which $\mathcal{C}_z$ acts, once before and then then once again after applying $\mathcal{C}_z$. If the control is a 0, then the fixed state $|\perp\rangle|\perp\rangle$ is swapped in, neutralizing the application of the oracle. If the control is a 1, then nothing is swapped and the oracle acts as expected.

It therefore suffices to show that $\mathcal{U}_3$ cannot be distinguished from the identity except with negligible advantage. Specifically, we want to show that the eigenvalues of $I - \mathcal{U}_3$ are all negligible. That's because if the magnitudes of all the eigenvalues of $I - \mathcal{U}_3$ are bounded from above by a negligible function ε, then given any quantum state $|\phi\rangle$ before the application of $\mathcal{U}_3$ or I, and any subsequent transformation, we have that the resulting Euclidean distance is $\big\||\phi\rangle - \mathcal{U}_3|\phi\rangle\big\| = \big\|(I - \mathcal{U}_3)|\phi\rangle\big\| \leq \varepsilon$, and thus by Theorem 6, when replacing I with $\mathcal{U}_3$, the probability of success can change by at most 4ε.

Since $I - \mathcal{U}_3$ acts independently on and maintains the $2^n - 1$ orthogonal planes, it suffices to look at each plane individually. Specifically, its non-zero eigenvalues come in pairs of magnitude

$$|\lambda_i| = |1 - e^{\pm \mathbf{i}\theta_i}| = |1 - \cos(\theta_i) \mp \mathbf{i}\sin(\theta_i)| = \sqrt{(1 - \cos(\theta_i))^2 + \sin^2(\theta_i)}$$
$$= \sqrt{2(1 - \cos(\theta_i))} = \sqrt{2\left(1 - \langle\psi_i|\widehat{\psi_i}\rangle\right)}$$

In order to further break this down, let k_i be the number of preimages of i in H_{impostor} and let $k_{z\to i}$ be the number of preimages of the target image, z, in H_{impostor} that were reassigned to image i in H_{private}. We evaluate the inner product as

$$\langle\psi_i|\widehat{\psi_i}\rangle = \left(\frac{1}{\sqrt{k_i}} \sum_{x|H_{\text{impostor}}(x)=i} \langle x|\right)\left(\frac{1}{\sqrt{k_i + k_{z\to i}}} \sum_{x|H_{\text{private}}(x)=i} |x\rangle\right)$$
$$= \sqrt{\frac{k_i}{k_i + k_{z\to i}}} = \sqrt{1 - \frac{k_{z\to i}}{k_i + k_{z\to i}}} \geq 1 - \frac{k_{z\to i}}{k_i + k_{z\to i}}$$

which gives

$$|\lambda_i| = \sqrt{2\left(1 - \langle\psi_i|\widehat{\psi_i}\rangle\right)} \leq \sqrt{\frac{2k_{z\to i}}{k_i + k_{z\to i}}}$$

The following claim frames this bound in terms of n.

▷ Claim 31. With overwhelming probability in the choice of H and H_{private}, for all $i \in \{0,1\}^n \setminus \{z\}$, we have that

$$\frac{k_{z\to i}}{k_i + k_{z\to i}} \leq 72n \cdot 2^{-n}$$

Proof. We show that the following all happen with overwhelming probability:

a) for all $i \in \{0,1\}^n \setminus \{z\}$, $\quad k_i > \frac{1}{2} \cdot 2^{m-n}$

b) $\frac{1}{2} \cdot 2^{m-n} < k_z < 3 \cdot 2^{m-n}$

c) for all $i \in \{0,1\}^n \setminus \{z\}$, $\quad k_{z\to i} < 36n \cdot 2^{m-2n}$

First we show that with overwhelming probability, for all $i \in \{0,1\}^n \setminus \{z\}$, $\quad k_i > \frac{1}{2} \cdot 2^{m-n}$. The expected number of preimages of any image i is $\mathbb{E}[k_i] = 2^{m-n}$. By a Chernoff bound, $P[k_i \leq \frac{1}{2}(2^{m-n})] \leq e^{-\frac{1}{8}\cdot 2^{m-n}}$ for any particular image i. By a union bound over the $2^n - 1$ images, the probability that for any i, $k_i \leq \frac{1}{2}(2^{m-n})$, is at most $2^n \cdot e^{-\frac{1}{8}\cdot 2^{m-n}} \leq e^{-(\frac{1}{8}\cdot 2^{m-n} - n)}$, which is negligible in n as we have that $m \geq 2n$.

We next bound the number of preimages of the target image z. Specifically, we show that $\frac{1}{2} \cdot 2^{m-n} < k_z < 3 \cdot 2^{m-n}$. The lower bound is identical to the one above for the other k_i's. The upper bound is given by another Chernoff bound as $P[k_z \geq 3(2^{m-n})] \leq e^{-2^{m-n}}$, which is likewise negligible in n.

Finally, we bound the number of preimages of z in H_{impostor} that can be mapped to any one i in H_{impostor}. Specifically, we show that for all $i \in \{0,1\}^n \setminus \{z\}$, $\quad k_{z\to i} < 36n \cdot 2^{m-2n}$. Since we just showed that with overwhelming probability, z has at least $\frac{1}{2} \cdot 2^{m-n}$ and at most $3 \cdot 2^{m-n}$ preimages, the expected number of these preimages distributed to each of the $2^n - 1$ other images is bounded by $\frac{1}{2} \cdot 2^{m-2n} < \mathbb{E}[k_{z\to i}] < 6 \cdot 2^{m-2n}$. By a Chernoff bound, $P[k_{z\to i} \geq 6n(6 \cdot 2^{m-2n})] \leq e^{-\frac{25n^2}{2+5n} \cdot \frac{1}{2} \cdot 2^{m-2n}} \leq e^{-\frac{3}{2}n \cdot 2^{m-2n}}$ for any particular image i. As before, by a union bound over the $2^n - 1$ images, the probability that for any i, $k_{z\to i} \geq 36n \cdot 2^{m-2n}$ is at most $2^n \cdot e^{-\frac{3}{2}n \cdot 2^{m-2n}} \leq e^{-(\frac{3}{2}n \cdot 2^{m-2n} - n)}$ which is negligible in n as $m \geq 2n$.

Putting these three things together, by a union bound over the three above events, with all but a negligible probability in n, for all i,

$$\frac{k_{z\to i}}{k_i + k_{z\to i}} \leq \frac{36n \cdot 2^{m-2n}}{\frac{1}{2} \cdot 2^{m-n}} = 72n \cdot 2^{-n} \qquad \lhd$$

We therefore get an upper bound of $\varepsilon := 12\sqrt{n} \cdot 2^{-n/2}$ on the eigenvalues of $I - \mathcal{U}_3$, which is negligible in n, and therefore, as shown above, an upper bound of 4ε on the change in success probability incurred by replacing I with $\mathcal{U}_3$.

We now use a standard hybrid argument over the at most $4q$ locations where $\mathcal{U}_3$ might appear. We start with R'', for which all such locations have the identity, and for which the success probability is the original success probability of R, namely η. One at a time, we insert a $\mathcal{U}_3$ at each location, each time incurring a loss of at most 4ε in the success probability. With all $4q$ applications of $\mathcal{U}_3$, we therefore get a success probability η' of at least $\eta - 16q\varepsilon - \gamma$ (where γ is an additional negligible loss from the negligible chance that the sampled H and H_{private} are not covered by Claim 31).

We therefore construct R' in this way as a quantum oracle algorithm with advice with query access to the original random oracle H and a z-cloning oracle $\mathcal{C}_z$. It simulates R and redirects its oracles queries: Whenever R makes a random oracle query, it redirects the query to its own simulated H_{impostor}, which makes at most a single query to H. Whenever R makes a cloning oracle query, it redirects the query to its $\widehat{\mathcal{C}}_{\text{impostor}}$, which makes at most one query to $\mathcal{C}_z$ and two to H. R' thus satisfies the conditions of Corollary 28, so its success probability $\eta' \geq \eta - 16q\varepsilon - \gamma$ must be negligible. Therefore, η, the success probability of R, must be negligible, thus completing the proof of Proposition 29, and as a consequence, completing the proof of our main theorems, Theorem 18 and Theorem 17. ◀

References

1. Scott Aaronson. Quantum copy-protection and quantum money. *Proceedings of the Annual IEEE Conference on Computational Complexity*, October 2011.
2. Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing*, STOC '12, pages 41–60, New York, NY, USA, 2012. Association for Computing Machinery.
3. Scott Aaronson and Greg Kuperberg. Quantum versus classical proofs and advice. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 115–128. IEEE, 2007.
4. Dorit Aharonov and Tomer Naveh. Quantum NP - a survey, 2002. `arXiv:quant-ph/0210077`.
5. A. Ambainis, A. Rosmanis, and D. Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *2014 IEEE 55th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 474–483, Los Alamitos, CA, USA, October 2014. IEEE Computer Society.

6 Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2020, pages 255–268, New York, NY, USA, 2020. Association for Computing Machinery.

7 Prabhanjan Ananth and Rolando L. La Placa. Secure software leasing. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 501–530, Cham, 2021. Springer International Publishing.

8 James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In *Advances in Cryptology – CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part I*, pages 467–496, Berlin, Heidelberg, 2021. Springer-Verlag.

9 James Bartusek and Giulio Malavolta. Indistinguishability obfuscation of null quantum circuits and applications. In *ITCS 2022*, 2022.

10 Mihir Bellare and Wei Dai. Defending against key exfiltration: Efficiency improvements for big-key cryptography via large-alphabet subkey prediction. In Bhavani Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 923–940. ACM, 2017.

11 Mihir Bellare, Daniel Kane, and Phillip Rogaway. Big-key symmetric encryption: Resisting key exfiltration. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*, pages 373–402, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

12 Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997. doi:10.1137/S0097539796300933.

13 Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984*, 1984.

14 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. *Phys. Rev. Lett.*, 70:1895–1899, March 1993. doi:10.1103/PhysRevLett.70.1895.

15 Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 556–584. Springer, Heidelberg, August 2021.

16 D. Dieks. Communication by EPR devices. *Phys. Lett. A*, 1982.

17 Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, and Peter Shor. Quantum money from knots. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ITCS '12, pages 276–289, New York, NY, USA, 2012. Association for Computing Machinery.

18 Bill Fefferman and Shelby Kimmel. Quantum vs. classical proofs and subset verification. In *43rd International Symposium on Mathematical Foundations of Computer Science*, page 1, 2018.

19 Marios Georgiou and Mark Zhandry. Unclonable decryption keys. Cryptology ePrint Archive, Paper 2020/877, 2020. URL: https://eprint.iacr.org/2020/877.

20 Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in MiniQCrypt. In *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*, pages 531–561, Berlin, Heidelberg, 2021. Springer-Verlag.

21 Yassine Hamoudi and Frédéric Magniez. Quantum time-space tradeoff for finding multiple collision pairs. *ACM Trans. Comput. Theory*, 15(1-2):1–22, 2023. doi:10.1145/3589986.

22 Daniel Harlow and Patrick Hayden. Quantum computation vs. firewalls. *Journal of High Energy Physics*, 2013, January 2013.

23 Xingjian Li, Qipeng Liu, Angelos Pelecanos, and Takashi Yamakawa. Classical vs quantum advice under classically-accessible oracle, 2023. arXiv:2303.04298.

24 Jiahui Liu, Qipeng Liu, Luowen Qian, and Mark Zhandry. Collusion resistant copy-protection for watermarkable functionalities. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 294–323. Springer, Heidelberg, November 2022.

25 Hoi-Kwong Lo and H. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78, August 1998.

26 Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78, May 1996.

27 Tal Moran and Daniel Wichs. Incompressible encodings. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020*, pages 494–523, Cham, 2020. Springer International Publishing.

28 Anand Natarajan and Chinmay Nirkhe. A distribution testing oracle separation between QMA and QCMA, 2023. arXiv:2210.15380.

29 Barak Nehoran and Mark Zhandry. A computational separation between quantum no-cloning and no-telegraphing, 2023. arXiv:2302.01858.

30 James L. Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1970.

31 Roy Radian and Or Sattath. Semi-quantum money. *J. Cryptol.*, 35(2):8, 2022. doi:10.1007/S00145-021-09418-8.

32 Omri Shmueli. Public-key quantum money with a classical bank. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2022, pages 790–803, New York, NY, USA, 2022. Association for Computing Machinery.

33 R. F. Werner. Optimal cloning of pure states. *Physical Review A*, 58(3):1827–1832, September 1998. doi:10.1103/physreva.58.1827.

34 William K. Wootters and Wojciech Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

35 Horace P. Yuen. Amplification of quantum states and noiseless photon amplifiers. *Physics Letters A*, 113(8):405–407, 1986. doi:10.1016/0375-9601(86)90660-2.

36 Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Info. Comput.*, 15(7-8):557–567, May 2015.

37 Mark Zhandry. Quantum lightning never strikes the same state twice. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 408–438, Cham, 2019. Springer International Publishing.