Simultaneous Haar Indistinguishability with Applications to Unclonable Cryptography

Prabhanjan Ananth
University of California, Santa Barbara, CA, USA

Fatih Kaleoglu
University of California, Santa Barbara, CA, USA

Henry Yuen
Columbia University, New York, NY, USA

Abstract

We study a novel question about nonlocal quantum state discrimination: how well can non-communicating – but entangled – players distinguish between different distributions over quantum states? We call this task *simultaneous state indistinguishability*. Our main technical result is to show that the players cannot distinguish between each player receiving independently-chosen Haar random states versus all players receiving the same Haar random state.

We show that this question has implications to unclonable cryptography, which leverages the no-cloning principle to build cryptographic primitives that are classically impossible to achieve. Understanding the feasibility of unclonable encryption, one of the key unclonable primitives, satisfying indistinguishability security in the plain model has been a major open question in the area. So far, the existing constructions of unclonable encryption are either in the quantum random oracle model or are based on new conjectures.

We leverage our main result to present the first construction of unclonable encryption satisfying indistinguishability security, with quantum decryption keys, in the plain model. We also show other implications to single-decryptor encryption and leakage-resilient secret sharing. These applications present evidence that simultaneous Haar indistinguishability could be useful in quantum cryptography.

2012 ACM Subject Classification Theory of computation → Cryptographic protocols; Theory of computation → Quantum information theory

Keywords and phrases Quantum, Haar, unclonable encryption

Digital Object Identifier 10.4230/LIPIcs.ITCS.2025.7

Related Version This paper is based on the following technical report:
Full Version: `https://arxiv.org/abs/2405.10274` [8]

Funding *Prabhanjan Ananth*: the National Science Foundation Grant No. 2329938.
Fatih Kaleoglu: the National Science Foundation Grant No. 2329938.
Henry Yuen: AFOSR awards FA9550-21-1-0040 and FA9550-23-1-0363, NSF CAREER award CCF-2144219, NSF award CCF-2329939, and the Sloan Foundation.

Acknowledgements The authors would like to thank Ludovico Lami for answering many questions related to non-local state discrimination.

1 Introduction

Quantum state discrimination [40] is a foundational concept with applications to quantum information theory, learning theory and cryptography. In a state discrimination task, a party receives ρ_x from an ensemble $\{\rho_x\}_{x \in \mathcal{X}}$ and has to determine which state it received. A compelling variant of this problem is concerned with the multi-party setting where there are two or more parties and each party receives a disjoint subset of qubits of ρ_x. This multi-party variant of state discrimination has also garnered interest from quantum information-theorists

16th Innovations in Theoretical Computer Science Conference (ITCS 2025).
Editor: Raghu Meka; Article No. 7; pp. 7:1–7:23
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

focused on the LOCC (local operations and classical communication) model and quantum data hiding [50, 14, 29, 25]. Understanding the multi-party state discrimination problem in turn sheds light on the difficulty of simulating global measurements using local measurements [52].

An important aspect to consider when formulating the multi-party state discrimination problem is the resources shared between the different parties. If we allow the parties to share entanglement and also communicate with each other then this is equivalent to the original state discrimination task (against a single party) due to teleportation. Thus, in order for the multi-party setting to be distinct from the single-party setting, we need to disallow either shared entanglement or classical communication. This results in two different settings:

- Parties without shared entanglement: In this setting, the parties are allowed to communicate using classical channels but they cannot share entanglement. The extensive research on quantum data hiding and LOCC [29, 32, 39, 46, 51, 15, 23, 24, 25, 36, 48] are mainly concerned with this setting.
- Parties with shared entanglement: In this setting, the parties are allowed to share entanglement but they cannot communicate. On the contrary, this setting is relatively unexplored with the notable exception being the recent works of [45, 30]. There are good reasons to study multi-party state discrimination with shared entanglement. Firstly, it can be viewed as a subclass of semi-quantum games [18], which are non-local games with quantum questions and classical answers. Secondly, it has connections to unclonable cryptography [54, 1], an emerging area in quantum cryptography, as discussed in [45].

Our Work. We focus on the setting when the parties share entanglement but are not allowed to communicate. We introduce a new concept called *simultaneous state indistinguishability* (SSI). In the two-party version of the problem, we have two parties (say, Bob and Charlie) who receive as input one of two bipartite states $\{\rho_0, \rho_1\}$ and they are supposed to distinguish. The first half of ρ_b is given to Bob and the second half is given to Charlie for $b \in \{0, 1\}$.

We say that ρ_0 and ρ_1 are *ϵ-simultaneous state indistinguishable* if the probability that Bob and Charlie can simultaneously distinguish is at most ϵ. That is, $d_{\mathsf{TV}}(x, x') \leq \epsilon$, where $d_{\mathsf{TV}}(\cdot, \cdot)$ denotes the total variation distance, $x = (x_B, x_C) \leftarrow (\text{Bob, Charlie})(\rho_0)$ denotes the random variable corresponding to the joint outputs of Bob and Charlie given input ρ_0, and similarly $x' = (x'_B, x'_C) \leftarrow (\text{Bob, Charlie})(\rho_1)$ denotes the random variable corresponding to their joint outputs when given input ρ_1.

This is related to a recent concept introduced by [45] who considered the unpredictability (search) version of this problem whereas we are interested in indistinguishability. Looking ahead, for applications, it turns out that the indistinguishability notion is more amenable to carrying out proofs (e.g. in the security of unclonable encryption) compared to the unpredictability definition considered by [45]. This is largely due to the fact that our notion is more compatible with the hybrid technique.

An interesting special case of simultaneous-state-indistinguishability is when Bob and Charlie either receive copies of the same state $|\psi\rangle$ drawn from some distribution $\mathcal{D}$ or receive i.i.d. samples from $\mathcal{D}$, i.e.

$$\rho_0 = \mathop{\mathbb{E}}_{|\psi\rangle \sim \mathcal{D}} \psi^{\otimes t} \otimes \psi^{\otimes t} \quad \text{vs.} \quad \rho_1 = \mathop{\mathbb{E}}_{|\psi_B\rangle, |\psi_C\rangle \sim \mathcal{D}} \psi_B{}^{\otimes t} \otimes \psi_C^{\otimes t}.$$

Observe that if Bob and Charlie were allowed to make global entangled measurements then they can indeed distinguish by performing swap tests. However, it is not clear these two situations are distinguishable using local measurements, even with preshared entanglement between Bob and Charlie.

We study simultaneous state indistinguishability in the case that each party receives (copies of) a state drawn from the *Haar measure.*[1] Specifically, we consider the following definition:

> **(d,t,ε)-Simultaneous Haar Indistinguishability**: We say that (d,t,ε)-simultaneous Haar indistinguishability holds if any two non-communicating and entangled adversaries Bob and Charlie can distinguish the following distributions with probability at most ε:
>
> - Bob and Charlie each receive t copies of $|\psi\rangle$, where $|\psi\rangle$ is a d-dimensional Haar state,
> - Bob receives t copies of $|\psi_B\rangle$ and Charlie receives t copies of $|\psi_C\rangle$, where $|\psi_B\rangle, |\psi_C\rangle$ are i.i.d d-dimensional Haar states.

In the default setting, both Bob and Charlie each output 1 bit. We also consider the setting when they output multiple bits.

Variants of this problem have been studied in different contexts before. Independently, two works, namely, Harrow [38] and Chen, Cotler, Huang and Li [22] showed (for the case when $t = 1$) that Bob and Charlie fail, except with probability negligible in the dimension d, in the above distinguishing experiment as long as they don't share any entanglement. In fact, Harrow's result proves something stronger: the indistinguishability holds even if the two parties exchange classical information (i.e., LOCC setting). Both works discuss the applications of this problem to well studied topics such as multiparty data hiding, local purity testing and separations between quantum and classical memory. Neither of the works [38, 22] addresses the setting when Bob and Charlie can share an arbitrary amount of entanglement.

1.1 Our Results

1.1.1 Main Result

We show the following:

▶ **Theorem 1** (Informal). *For any $d, t \in \mathbb{N}$, (d,t,ε)-Simultaneous Haar indistinguishability holds for $\varepsilon = O\left(\frac{t^2}{\sqrt{d}}\right)$.*

Our result complements the works of [38, 22] by showing that it is not possible to distinguish i.i.d versus identical Haar states either using the entanglement resource or using classical communication.

In the case when $t = 1$, we show that $(d,1,\epsilon)$-simultaneous Haar indistinguishability does not hold for $\epsilon = O\left(\frac{1}{d}\right)$, which suggests that the above bound cannot be improved significantly. Perhaps surprisingly, our attack even holds in the setting when Bob and Charlie do not share any entanglement. This further indicates that for the problem of simultaneous Haar indistinguishability, the gap between the optimal success probabilities in the entangled and the unentangled cases is small.

1.1.2 Applications

Besides being a natural problem, simultaneous Haar indistinguishability has applications to unclonable cryptography [54, 1, 55, 17, 9, 28, 27, 19]. This is an area of quantum cryptography that leverages the no-cloning principle of quantum mechanics to design cryptographic notions for tasks that are impossible to achieve classically.

[1] The Haar measure over states is the unique measure where for all fixed unitaries U, if $|\psi\rangle$ is Haar-distributed then so is $U|\psi\rangle$.

Unclonable Encryption: Unclonable encryption is an encryption scheme with quantum ciphertexts that are unclonable. It was first introduced by Broadbent and Lord [17] and is now considered a fundamental notion in unclonable cryptography. There are two security notions of unclonable encryption, namely search and indistinguishability security, studied in the literature. The search security stipulates that any cloning adversary[2] after receiving a ciphertext of randomly chosen message m should not be able to guess m except with probability negligible in $|m|$. In the challenge phase, the cloning adversary receives as input (k, k), where k is the decryption key. The indistinguishability security imposes a stronger guarantee that any cloning adversary after receiving encryption of m_b, for a randomly chosen bit b and adversarially chosen message pair (m_0, m_1), cannot predict b except with probability negligibly close to $\frac{1}{2}$.

While we have long known that search security is feasible [17], establishing indistinguishability security has remained an important and intriguing open problem. Unclonable encryption satisfying indistinguishability is achievable in the quantum random oracle model [6, 7] or in the plain model (i.e., without oracles) based on new unproven conjectures [3]. Various generic transformations are also known that convert one-time unclonable encryption to the public-key variant [5] or those that convert unclonable encryption for one-bit messages to multi-bit messages [41]. Given that unclonable-indistinguishable encryption has interesting applications to copy-protection [5, 26], it is important we completely settle its feasibility in the plain model. Perhaps embarassingly, we do not how to establish feasibility in the plain model even under strong assumptions such as indistinguishability obfuscation [10, 31]!

We consider the notion of unclonable encryption, where the decryption keys are allowed to be quantum keys. This only affects the challenge phase of the security experiment, where the cloning adversary now receives as input many copies[3] of the quantum decryption key.

We show the following:

▶ **Theorem 2** (Informal). *There is an unclonable encryption scheme, with quantum decryption keys, satisfying indistinguishability security in the plain model.*

Ours is the first work to show that unclonable-indistinguishable encryption exists in the plain model albeit with quantum decryption keys. Our relaxation (i.e. decryption keys being quantum states) is not only natural and interesting, it also respects the essence of unclonable encryption. For a detailed perspective on the above result, we refer the reader to the full version. We leave open the problem of achieving unclonable encryption with *classical* decryption keys to future works; we note that the prior works only mentioned the open problem of constructing unclonable encryption in the plain model without explicitly mentioning the need for classical decryption keys.

Moving Beyond Quantum Decryption Keys: A potential approach to transform this scheme into another scheme where the decryption keys are binary strings is to generate the decryption key to be an obfuscation of the setup algorithm that produces decryption keys. It is an intriguing problem to formalize the requirements of the underlying quantum obfuscation scheme. At the bare minimum, we require that the quantum obfuscation scheme satisfies the property that the obfuscated program can be represented as a binary string. While

[2] A cloning adversary is a tri-partite adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$. $\mathcal{A}$ receives as input an unclonable state and produces a bipartite state given to $\mathcal{B}$ and $\mathcal{C}$ who are not allowed to communicate. Then, in the challenge phase, the cloning adversary receives as input $(\mathsf{ch}_{\mathcal{B}}, \mathsf{ch}_{\mathcal{C}})$ and then gives $\mathsf{ch}_{\mathcal{B}}$ to $\mathcal{B}$ and $\mathsf{ch}_{\mathcal{C}}$ to $\mathcal{C}$. Finally, $\mathcal{B}$ and $\mathcal{C}$ output their respective answers. Refer to [7] for an abstract modeling of unclonable security notions.

[3] We consider a security notion where the adversary receives at most t copies of the quantum decryption key and t is fixed ahead of time.

achieving quantum obfuscation has been a difficult open problem [16, 12, 11], obfuscating special classes of quantum algorithms (those that capture the setup algorithm of Theorem 2) could be relatively more tractable.

Our scheme supports one-bit messages and is one-time secure. It is an interesting future direction to extend the works of [5] and [41] to generically achieve unclonable encryption with quantum decryption keys in the public-key setting and for longer messages.

Single-Decryptor Encryption: Single-decryptor encryption [33] is a sister notion of unclonable encryption, where instead of requiring the ciphertexts to be unclonable, we instead require the decryption keys to be unclonable. Constructions of single-decryptor encryption in different settings are known from a variety of assumptions [33, 27, 7, 43]. There are two important security notions considered in the literature. In the *independent* setting, in the challenge phase, the cloning adversary gets two independently generated ciphertexts while in the *identical* setting, it gets copies of the same ciphertext. All the known constructions of single-decryptor encryption [27, 7, 43] are in the independent setting and specifically, there are no known constructions in the identical setting. This should not be surprising in light of [33] who showed the equivalence between single-decryptor encryption with identical ciphertexts and unclonable encryption, which suggests the difficulty in achieving the identical ciphertext setting.

We prove the following.

▶ **Theorem 3** (Informal). *There is a single-decryptor encryption scheme, with quantum ciphertexts, satisfying identical indistinguishability security.*

Ours is the first work to demonstrate the feasibility of single-decryptor encryption in the identical-challenge setting, albeit with quantum ciphertexts.

In addition to its applications to unclonable cryptography, simultaneous Haar indistinguishability can be used to construct leakage-resilient secret sharing.

Leakage-Resilient Secret Sharing: Leakage-resilient cryptography [42] is an area of cryptography that is concerned with the goal of building cryptographic primitives that are resilient to side-channel attacks. We are interested in designing secret sharing schemes that are leakage resilient. In a leakage-resilient secret sharing scheme, a leakage function is applied on each share and we require the guarantee that all the leakages put together are not sufficient enough to compromise the security of the secret sharing scheme. Leakage-resilient secret sharing is a well studied topic [35, 53, 2, 21, 13] with applications to leakage-resilient secure multi-party computation [13].

We consider a notion of leakage-resilient secret sharing, where we allow the parties holding the shares to be entangled with each other. We now require the guarantee that security should still hold even if each share is individually leaked. Moreover, we consider a relaxed requirement where the shares are allowed to be quantum. Just like the works in the classical setting, we consider the bounded leakage model. That is, if the number of qubits of each share is m then we allow for some $\lfloor \frac{c}{n} \rfloor$ fraction of bits of leakage from each share, where c is some constant and n is the number of parties[4].

We show the following:

▶ **Theorem 4** (Informal). *There is a 2-out-n leakage-resilient secret sharing scheme with the following properties: (a) the shares are quantum, (b) the number of bits of leakage on each share is $\lfloor \frac{c \cdot m}{n} \rfloor$, where c is some constant and the size of each share is m qubits, and (c) the parties can share arbitrary amount of entanglement.*

[4] We set $m \gg n$.

In fact, our construction satisfies a stronger security guarantee where the adversary can receive $p(n)$ number of copies of its share, where $p(\cdot)$ is an arbitrary polynomial.

A recent interesting work by [20] also considers leakage-resilient secret sharing schemes with quantum shares. However, there are notable differences. Firstly, they consider the setting when there can be unbounded amount of classical[5] bits of leakage from each quantum share whereas we consider bounded leakage. On the other hand, we allow the parties to be entangled whereas they mainly focus on the LOCC setting. In fact, they show that it is not possible to achieve unbounded amount of leakage in the shared entanglement setting even with two parties; this is the reason we focus on the setting of bounded leakage. However, there seems to be a large gap between the amount of leakage leveraged in the impossibility result in [20][6] and the leakage that we tolerate in our feasibility result. It is an interesting problem to close the gap. Finally, we allow each party to get arbitrary polynomially many copies of its share whereas [20] doesn't satisfy this guarantee.

Paper Organization. We give a technical overview in Section 1.3. In Section 2 we formally define simultaneous state indistinguishability and give basic facts about it. In Section 3, we show SSI for Haar states. In Section 4 we show cryptographic applications of our result. For a full list of preliminaries and a list of missing proofs, please refer to the full version of the paper.

1.2 Subsequent Work

Studying the simultaneous Haar indistinguishabiliy problem could have further implications beyond unclonable cryptography. Indeed, inspired by our work, a recent subsequent work [4] studied a dual problem of simultaneous Haar indistinguishabiliy problem where two parties can communicate using classical channels but cannot share entanglement. They showed similar bounds and demonstrated applications to proving black-box separations in quantum cryptography. The combination of our results implies an interesting fact: entanglement and classical communication are resources that are individually insufficient to non-locally distinguish independent vs. identical Haar states, whereas together they suffice (indeed trivialize the problem) due to quantum teleportation. Exploring the relationship between the resources of entanglement and classical communication for different non-local tasks is an interesting research direction.

1.3 Technical Overview

1.3.1 Simultaneous Haar Indistinguishability

We formally define the notion of simultaneous state indistinguishability (SSI), of which simultaneous Haar indistinguishability is a special case. We consider a non-local distinguisher $(\text{Bob}, \text{Charlie}, \rho)$ where Bob and Charlie are spatially separated quantum parties who share an entangled state ρ. Given two distributions $\mathcal{D}_1, \mathcal{D}_2$ over bipartite states, we can write the distinguishing advantage of $(\text{Bob}, \text{Charlie}, \rho)$ as $d_{\mathsf{TV}}(x, x')$, where $x = (x_B, x_C)$ is the random variable corresponding to the output of Bob and Charlie when they get as input $\rho \otimes \psi$ where $|\psi\rangle$ is sampled from $\mathcal{D}_1$. Here, x_B refers to Bob's output and x_C refers to Charlie's output. Similarly, $x' = (x'_B, x'_C)$ is the random variable corresponding to Bob and Charlie's outputs when they receive $\rho \otimes \psi'$ where $|\psi'\rangle$ is sampled from $\mathcal{D}_2$.

[5] They also consider bounded quantum leakage in addition to the classical leakage.
[6] Their impossibility result seems to require $O(2^m)$ bits of total leakage from all the parties.

For fixed $\mathcal{D}_1, \mathcal{D}_2$ we can ask the question: *What is the maximal distinguishing advantage if Bob and Charlie are restricted to output n classical bits?*. We first limit our attention to a special case of this problem such that $n = 1$ as well as:

1. $\mathcal{D}_1$ outputs two identical Haar random states $|\psi\rangle \otimes |\psi\rangle$.
2. $\mathcal{D}_2$ outputs two independent Haar random states $|\psi_B\rangle \otimes |\psi_C\rangle$.

In both $\mathcal{D}_1$ and $\mathcal{D}_2$, the first half of the state will be given to Bob and the second half will be given to Charlie. Note that if we restrict our attention to Bob (or Charlie) alone, then the two cases are perfectly indistinguishable. Therefore, Bob and Charlie need to work collectively in order to achieve a non-trivial distinguishing advantage.

For now assume that the pre-shared entanglement consists of some arbitrary number (r) of EPR pairs, denoted by $|\mathsf{EPR}\rangle^{\otimes r}$. Let M and N be the measurements (formally POVM elements) applied by Bob and Charlie, respectively. It is without loss of generality to assume that M and N are projective. In this case, we can write the distinguishing advantage of Bob and Charlie as

$$\mathsf{Tr}\left[(M \otimes N)\left\{\mathsf{EPR}^{\otimes r} \otimes \left(\mathop{\mathbb{E}}_{|\psi\rangle} \psi \otimes \psi - \mathop{\mathbb{E}}_{\psi_B, \psi_C} \psi_B \otimes \psi_C\right)\right\}\right].$$

The second expectation equals the maximally mixed state $(\mathsf{id} \otimes \mathsf{id})/d^2$, where d is the dimension of the Haar random states. The first expectation equals the maximally mixed state over the symmetric subspace[7], which is $O(1/d)$ close to $(\mathsf{id} \otimes \mathsf{id} + F)/d^2$, where F is the operator that swaps two registers. Hence, we can approximate the advantage as

$$\frac{1}{d^2}\mathsf{Tr}\left[(M \otimes N)\left\{\mathsf{EPR}^{\otimes r} \otimes F\right\}\right].$$

We examine this expression in terms of tensor network diagrams[8] [49]. Up to normalization, the effect of the EPR pairs (followed by trace) is to connect the entangled registers of M and N in reverse (i.e. after partially transposing one of the projectors), whereas the effect of F (followed by trace) is to connect the registers of M and N containing the Haar states. Overall, we observe that the expression above equals

$$\frac{1}{2^r d^2}\mathsf{Tr}\left[M \cdot N^{\top_P}\right], \tag{1}$$

where $\top_P$ denotes the partial transpose operation. Notice that this is the Hilber-Schmidt inner-product of M and $N^{\top_P}$, hence by Cauchy-Schwarz we can bound it by

$$\frac{1}{2^r d^2}\|M\|_2 \cdot \left\|N^{\top_P}\right\|_2 = \frac{1}{2^r d^2}\|M\|_2 \cdot \|N\|_2 \leq \frac{1}{2^r d^2}\sqrt{2^r d} \cdot \sqrt{2^r d} = \frac{1}{d},$$

where we used the fact that $\|M\|_2^2$ equals the rank of M. Together with the previous approximation error we had, this gives us a bound of $O(1/d)$.

This bound is in fact tight, which can be seen by a simple attack where Bob and Charlie measure and output the first qubit of their input state. Moreover, this attack is unentangled, leading to the interesting conclusion that entangled attacks are no more powerful than unentangled attacks.

[7] See [37] for an introduction to the symmetric subspace.
[8] See [47] for an introduction to tensor network diagrams.

The Case of Many Copies. Now we generalize our argument to the case when Bob and Charlie each get t copies of their input. Similar to the $t = 1$ case, we can write the projection onto the symmetric subspace over t registers as

$$\Pi^t = \frac{1}{t!} \sum_{\sigma \in S_t} P_\sigma,$$

where P_σ is a register-wise permutation operator. Using this identity for Bob's and Charlie's registers alike, the independent case yields a sum of terms of the form $P_{\sigma_B} \otimes P_{\sigma_C}$. On the other hand, the identical case will give us a sum of P_σ for $\sigma \in S_{2t}$. We can match the coefficients up to $O(t^2/d)$ error, and thus we can approximate the advantage as

$$\frac{1}{d^{2t}} \mathsf{Tr}\left[(M \otimes N) \left\{ \mathsf{EPR}^{\otimes r} \otimes \sum_{\sigma \in S_{2t}^*} P_\sigma \right\} \right],$$

where S_{2t}^* is the set of permutations over $2t$ registers that cannot be expressed as a product of two permutations over t registers. A natural idea would be to bound this expression separately for each P_σ, but it would yield a factor of $\mathsf{poly}(t!)$ which blows up very fast. Our idea instead is to group permutations based on how far they are from a product permutation. In more detail, we define $S_{2t}^{(s)}$ as the set of permutations σ which obeys the identity

$$P_\sigma = (P_{\sigma_1} \otimes P_{\sigma_2}) \, P_{\sigma_s} \, (P_{\sigma_3} \otimes P_{\sigma_4})$$

for some permutations $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ over t registers, where σ_s is a fixed permutation that swaps t of Bob's registers with t of Charlie's registers. Indeed, $S_{2t}^{(s)}$ is the set of permutations σ that make s *swaps* across Bob's and Charlie's registers. Moreover, by a combinatorial argument, we can compute the average of P_σ by averaging the identity above over $\sigma_1, \sigma_2, \sigma_3, \sigma_4$, so that

$$\sum_{\sigma \in S_{2t}^{(s)}} P_\sigma = C_s \left(\Pi_B^t \otimes \Pi_C^t \right) P_{\sigma_s} \left(\Pi_B^t \otimes \Pi_C^t \right),$$

where C_s is a constant that depends on s, t, and Π_B^t, Π_C^t are projections onto the symmetric subspace over Bob's and Charlie's t registers, respectively. Using the generalization of Equation (1) we show that

$$\frac{1}{d^{2t}} \mathsf{Tr}\left[(M \otimes N) \left\{ \mathsf{EPR}^{\otimes r} \otimes \sum_{\sigma \in S_{2t}^{(s)}} P_\sigma \right\} \right] \leq \binom{t}{s}^2 s! d^{-s},$$

and summing this over $s = 1, 2, \ldots, t$ gives us a bound of $O(t^2/d)$. Keep in mind that $s = 0$ is excluded from the sum because it corresponds to product permutations.

The Case of General Entanglement. Now suppose the entangled state $|\Omega\rangle$ shared between Bob and Charlie is arbitrary. Intuitively, we don't expect this relaxation to help the adversary a lot since the number of EPR pairs above was unbounded, yet it requires a proof to show this. Recall that $|\Omega\rangle$ can be written as

$$|\Omega\rangle = \sum_i \sqrt{\lambda_i} \, |u_i\rangle \, |v_i\rangle$$

for some choice of bases $(u_i), (v_i)$ for the registers of Bob and Charlie, known as the *Schmidt decomposition*. An equivalent way to write this is[9]

$$|\Omega\rangle = (\sigma^{1/2} \otimes V)\,|\mathsf{EPR}^{\otimes r}\rangle$$

for some density matrix σ, unitary V, and integer r. The unitary V can be safely ignored by changing the basis of Charlie's projection N. Using the cyclicity of trace we can absorb $\sigma^{1/2}$ in M and get a similar expression for the distinguishing advantage as the maximally entangled state, where M is replaced with $(\sigma^{1/2} \otimes \mathsf{id})M(\sigma^{1/2} \otimes \mathsf{id})/2^r$, with d' being the dimension of Bob's share of the entangled state. Following the same analysis as the EPR case results in a bound that scales with $\sqrt{d'}$. In order to get a bound that does not depend on the amount of entanglement we perform a more refined and involved analysis coupled with a more careful application of Cauchy-Schwarz, which yields a bound of $O(t^2/\sqrt{d})$ on the distinguishing advantage. An interesting open question is whether the gap between the EPR and non-EPR cases is inherent.

1.3.2 Applications

Unclonable Encryption. The search (weak) security of unclonable encryption (UE) was known since its formal introduction [17], yet strong (CPA-style/indistinguishability) security has been an open problem. There are fundamental reasons why this problem has been difficult, including the following:

1. Because the adversary learns the secret key in the challenge phase of the unclonable security experiment, it is hard to leverage traditional cryptographic tools – wherein revealing the secret key tantamounts to the compromise of security – in the construction of unclonable encryption.
2. There is a lack of straightforward equivalence between unpredictability and indistinguishability in the unclonability setting. The former is used to define CPA-style security and is not transitive, hence unfriendly to hybrid arguments.
3. Due to the simultaneous nature of the security experiment, extraction techniques that work for a single party often fail against two or more entangled parties.

To elaborate on the third bullet further, one can hope to deploy classical techniques for search-to-decision reductions in this setting. For instance, it has been shown that random oracles can be used to go from weak security to strong security in UE [6, 7]. In the plain model, a common classical tool is the Goldreich-Levin extraction technique [34], using which one can try the following folklore construction of UE:

1. The key consists of (k, r), where k is a key for a weakly secure UE scheme and $r \in \{0,1\}^n$ is a random string.
2. To encrypt a single-bit message $m \in \{0,1\}$, sample a random message $x \in \{0,1\}^n$, then output encryption of x using k, as well as $\langle r, x\rangle \oplus m$.
3. To decrypt, first use k to recover x using the decryption procedure of the weakly secure UE scheme and then recover m.

To prove unclonable security of this construction, one needs the *identical-challenge* version of simultaneous Goldreich-Levin, where Bob and Charlie will get the same r as challenge. This is unknown even though the independent-challenge version is known [44, 7].

[9] Here we are implicitly assuming that the dimensions of Bob and Charlie's registers both equal the same power of 2. This is merely for convenience and does not affect the analysis.

Our main insight is to make the string r in the key come in superposition, i.e. from a quantum state $\sum \alpha_r |r\rangle$. Intuitively, if Bob and Charlie were to measure r in the computational basis, then they would effectively receive independent values of r, meaning that we can hope to use independent-challenge Goldreich-Levin. Accordingly, we look for a state $\sum \alpha_r |r\rangle$ such that (1) Bob and Charlie cannot simultaneously distinguish whether or not this state has been measured in the computational basis, and (2) the computational basis measurement results in a uniform value of r.

Perhaps the most natural candidate for this task is to pick a Haar random state. This allows us to apply our simultaneous Haar indistinguishability result. Nonetheless, there still remain some technical challenges in the application of this concept. To begin with, we need to adapt the construction slightly to incorporate the newly acquired quantumness of r. Our solution is as follows:

1. The key is partially quantum:
   - The (classical) *encryption key* consists of $(k, x, \widetilde{b})$, where x is a random message and $\widetilde{b} \in \{0,1\}$ is a single-bit one-time-pad.
   - The (quantum) *decryption key* consists of k and a state $\sum \alpha_r |r\rangle |\langle r, x\rangle \oplus \widetilde{b}\rangle$, where $\sum \alpha_r |r\rangle$ is a Haar random state.
2. To encrypt a single-bit message $m \in \{0,1\}$, output encryption of x using k, as well as $\widetilde{b} \oplus m$.
3. To decrypt, first use k to recover x, then coherently recover $\widetilde{b}$ followed by m.

Using the simultaneous Haar indistinguishability, we can show that our construction is secure via the hybrid method. Note that we can do this because our notion of simultaneous-state-indistinguishability is strong enough that it is amenable to the use of hybrids.

In more detail, we reach an indistinguishable hybrid experiment where the Bob and Charlie get keys which use independently generated Haar random states. Equivalently, Bob gets $(r, \langle r, x\rangle \oplus \widetilde{b})$ and Charlie gets $(r', \langle r', x\rangle \oplus \widetilde{b})$ for independent r, r'.

Next, we move to a hybrid which is the weak security (i.e. search security) experiment of the underlying unclonable encryption scheme, so that Bob and Charlie need to output x each given the key k. Unfortunately, even though r and r' are independent in the previous hybrid, independent-challenge simultaneous Goldreich-Levin [44, 7] is insufficient due to the correlation between the bits $b = \langle r, x\rangle \oplus \widetilde{b}$ and $b' = \langle r', x\rangle \oplus \widetilde{b}$, namely $b \oplus b' = \langle r, x\rangle \oplus \langle r', x\rangle$. To overcome this issue, we prove exactly what we need, which we call *correlated simultaneous quantum Goldreich-Levin*[10] [11] (Lemma 30), which can be summarized as follows:

> Correlated Goldreich-Levin: Suppose that Bob is given input (r, b) and Charlie is given input (r', b'), where r, r' are independent strings and b, b' are uniform bits satisfying the correlation $b \oplus b' = \langle r, x\rangle \oplus \langle r', x\rangle$. If (Bob, Charlie) can output $(\langle r, x\rangle, \langle r', x\rangle)$ with probability $1/2 + 1/\mathsf{poly}$, then there is an extractor $(\text{ExtBob}, \text{ExtCharlie})$ that extracts (x, x) from (Bob, Charlie) with probability $1/\mathsf{poly}$.

To prove this lemma we first tackle the correlation between b and b'. Consider $\widetilde{\text{Bob}}$ who takes as input r, samples b himself uniformly, and runs Bob on input (r, b) to obtain b_B; similarly consider $\widetilde{\text{Charlie}}$ who takes r' as input, samples b' and runs Charlie on input (r', b') to obtain b_C. Now that the input bits b, b' are uncorrelated, $(\widetilde{\text{Bob}}, \widetilde{\text{Charlie}})$, who output (b_B, b_C), are expected to have worse success probability than (Bob, Charlie). However, we can in turn relax the success criterion for $(\widetilde{\text{Bob}}, \widetilde{\text{Charlie}})$ to merely output bits (b_B, b_C) that

[10] As a side note, this lemma resolves an open question in [44], implying that their construction achieves a more desirable notion of security.

[11] Previously, the work of [3] explicitly stated the correlated Goldreich-Levin problem over large finite fields as a conjecture.

satisfy $b_B \oplus b_C = \langle r, x\rangle \oplus \langle r', x\rangle$ in order to counteract this lack of correlation. In other words, now $(\widetilde{\text{Bob}}, \widetilde{\text{Charlie}})$ are additionally allowed to be *both incorrect*. Indeed, we show that the success probability of $(\widetilde{\text{Bob}}, \widetilde{\text{Charlie}})$ in this case is at least that of (Bob, Charlie), i.e. $1/2 + 1/\mathsf{poly}$. To show this fact, we define E as the event that $b \oplus b' = \langle r, x\rangle \oplus \langle r', x\rangle$. Conditioned on E, Bob and Charlie will output $(\langle r, x\rangle, \langle r', x\rangle)$ with probability $1/2 + 1/\mathsf{poly}$ by our assumption. In addition, the event E is independent of Bob's (or Charlie's) marginal output due to the fact that the players' correlation satisfies no-signalling. To see this, notice that the bits b and b' can each independently control the event E. We utilize this important observation to show the desired result. Another way to interpret this reduction is as follows: the correlation that (Bob, Charlie) require in order to output $(\langle r, x\rangle, \langle r', x\rangle)$ appears as a correlation in the output of $(\widetilde{\text{Bob}}, \widetilde{\text{Charlie}})$, who take uncorrelated bits as input.

After this reduction, it seems that we still cannot use the original independent-challenge simultaneous Goldreich-Levin because of the relaxed success criterion above. Luckily, by examining the proof of [7] we see that this condition is sufficient without additional work for the existence of (ExtBob, ExtCharlie) who can extract (x, x) simultaneously.

Many-Copy Security. For t-copy security, where Bob and Charlie get t copies of the decryption key in the unclonable security experiment, we need t to be at most linear in n, for otherwise Bob and Charlie can learn x using Gaussian elimination. In the proof, we similarly reach a hybrid where the Haar random states given to Bob and Charlie are independent. Then, we need an extra step where we switch to a hybrid in which Bob gets as input $(r_i, \langle r_i, x\rangle \oplus \widetilde{b})$ for independent samples $r_1, \ldots, r_t$ (instead of $(r_1, \ldots, r_t)$ being generated from t copies of a Haar random state) and similarly Charlie gets $(r'_i, \langle r'_i, x\rangle \oplus \widetilde{b})$ for independently generated $r'_1, \ldots, r'_t$. We show that the success probability of Bob and Charlie does not decrease from this change. To show this, we argue that that given $(r_i, \langle r_i, x\rangle \oplus \widetilde{b})$ Bob can prepare

$$\left(\sum_r \alpha_r \left|r\right\rangle \left|\langle r, x\rangle \oplus \widetilde{b}\right\rangle\right)^{\otimes t}$$

where $\left|\varphi\right\rangle = \sum_r \alpha_r \left|r\right\rangle$ is a Haar random state. In the expression above, $\left|r\right\rangle$ corresponds to the register that holds Goldreich-Levin samples, which are generated from t copies of a Haar random state rather than t independent samples. Recall that $\varphi^{\otimes t}$ can be written as a random vector in the *type basis*. Using this fact, Bob can coherently apply a random permutation $\sigma \in S_t$ to the values $\left|r_i, \langle r_i, x\rangle \oplus \widetilde{b}\right\rangle$, after which he can uncompute the permutation σ. We can argue similarly for Charlie, since their inputs originate from independent Haar distributions. This argument in fact requires the strings r_i to be distinct, which fortunately holds with high probability by the birthday bound.

Note that the input above given to Bob can be thought of as $(r, \langle r, x\rangle \oplus \widetilde{b})$ alongside $t - 1$ random samples of $(r_i, \langle r_i, x\rangle)$. In the final step, we apply our correlated Goldreich-Levin result in the presence of this extra information to reach the search security experiment for the weakly secure UE scheme. In this experiment, the extra information can be guessed by Bob and Charlie, hence if t is bounded by a linear function of n the security still holds.

Single-Decryptor Encryption. Single-decryptor encryption is a primitive that closely resembles unclonable encryption. It is an encryption scheme in which the decryption key is unclonable. In the security experiment, Alice tries to clone a quantum decryption key and split it between Bob and Charlie, who then try to decrypt a ciphertext they receive using their shares of the key. Depending on the correlation of these ciphertexts, one can define *identical-challenge* or *independent-challenge* security. We adapt our construction of unclonable encryption with quantum decryption keys to construct single-decryptor encryption with quantum ciphertexts. Our construction can be summarized as follows:

1. The encryption key consists of a key k as well as a random message x for a weakly secure UE scheme. The quantum decryption key contains k and encryption of x using k.
2. To encrypt a one-bit message m, output k as well as $\sum \alpha_r \left|r\right\rangle \left|\langle r, x\rangle \oplus m\right\rangle$, where $\sum \alpha_r \left|r\right\rangle$ is a Haar random state.
3. To decrypt, first recover x and then coherently compute m.

We can show that this construction is secure if Bob and Charlie are given t copies of the same ciphertext for $t = O(|x|)$. The proof is nearly identical to the security proof of our UE construction above. For more clear exposition, in the technical sections we first present our construction of single-decryptor encryption (Section 4.1), followed by that of unclonable encryption (Section 4.2).

Classical-Leakage-Resilient Secret-Sharing. As another application of simultaneous Haar indistinguishability, we construct a 2-out-of-n quantum secret-sharing scheme for a single-bit classical message. The construction is as follows:

1. The shares of bit $b = 0$ are identical Haar random states $\left|\psi\right\rangle$ and the shares of $b = 1$ are independent Haar random states $\left|\psi_i\right\rangle$. In addition, we give t copies of their share to all parties $1, 2, \ldots, n$.
2. Any two parties i, j can recover the message by applying t SWAP tests between their secrets. If $m = 0$, then all the tests will succeed. On the other hand, if $m = 1$, then with high probability the independent Haar random states held by i and j will be almost orthogonal, therefore the number of SWAP tests that pass will be concentrated near $t/2$ by a Chernoff bound.

Formally, we show that m remains hidden in the presence of ℓ-bits of classical leakage from each party. This amounts to showing a many-party and many-bit generalization of simultaneous Haar indistinguishability (SHI), that is, either all parties get (copies of) the same Haar random state or they get (copies of) independent Haar random states. Firstly, we go from 1-bit SHI to ℓ-bit SHI for 2 parties. This can be achieved by a union bound, which incurs a multiplicative loss of $2^{2\ell}$ in security. And then we show an equivalence between SHI in the cases of (1) 2 parties each getting $O(nt)$ copies and (2) $O(n)$ parties each getting t copies. This can be seen as distributing a fixed number of Haar random states among more parties. In the proof we use $O(\log n)$ hybrids, doubling the number of parties at each hybrid. We show by an additional hybrid argument that we incur a multiplicative loss of $O(1)$ at each step, hence a multiplicative loss of $O(n)$ in total after $O(\log n)$ steps. Putting everything together, we show that we can allow $\ell = O(\log d/n)$ bits of leakage from each party, where $\log d$ is the number of qubits of each copy of a share. The number of copies (t) given to each party can be an arbitrary polynomial, which lets us amplify the correctness of the scheme. An interesting open question is to get rid of the exponential dependence on the number of bits leaked (ℓn), which would imply that our construction tolerates unbounded polynomial leakage.

1.4 Notation

We write $\log := \log_e$ to denote the natural logarithm. We write $[n] := \{1, \ldots, n\}$. We use the notation $\langle \cdot, \cdot \rangle : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ to denote the inner product over $\mathbb{F}_2^n$, i.e. for classical strings $x, y \in \{0,1\}^n$ we have $\langle x, y\rangle := \sum_{i=1}^n x_i y_i \pmod 2$. We denote the set of d-dimensional pure quantum states by $\mathcal{S}(\mathbb{C}^d) := \left\{\left|\psi\right\rangle \in \mathbb{C}^d \ : \ \langle\psi|\psi\rangle = 1\right\}$. We sometimes write $\psi := |\psi\rangle\langle\psi|$ for simplicity. For a complex matrix (or operator) A, we write $A^\top$ to denote its transpose and $\overline{A}$ to denote its entry-wise complex conjugation, both with respect to the computational basis. $d_{\mathsf{TV}}(x, x')$ denotes the total-variation distance between random variables x, x'.

2 Simultaneous State Indistinguishability

Terminology. Below, $\mathcal{D}$ represents a probability distribution over pure states. Particularly, we will consider bipartite pure states $|\psi\rangle_{BC}$ and non-local adversaries $\mathcal{A} = (\mathcal{B}, \mathcal{C}, \rho_{BC})$ as distinguishers, where the B register will be given to $\mathcal{B}$ and the C register will be given to $\mathcal{C}$.

2.1 Definitions

▶ Remark 5. A distribution $\mathcal{D}$ has a unique representation as a quantum mixed state $\rho_{\mathcal{D}}$, whereas a quantum mixed state can represent many distributions. Accordingly, we can apply our results to mixed states ρ for which we can find an appropriate distribution $\mathcal{D}'$ that satisfies $\rho_{\mathcal{D}'} = \rho$.

▶ **Definition 6** (Simultaneous State Indistinguishability). *We say that two distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ are* ε-simultaneous state indistinguishable *(ε-SSI) against a non-local adversary $\mathcal{A} = (\mathcal{B}, \mathcal{C}, \rho_{BC})$ if the following holds for every pair of bits b_1, b_2:*

$$\left| \mathsf{Pr}\left[(b_1, b_2) \leftarrow \mathcal{A}(\psi_{BC}) \ : \ |\psi\rangle_{BC} \leftarrow \mathcal{D}_1\right] - \mathsf{Pr}\left[(b_1, b_2) \leftarrow \mathcal{A}(\psi_{BC}) \ : \ |\psi\rangle_{BC} \leftarrow \mathcal{D}_2\right] \right| \leq \varepsilon$$

Here, $\mathcal{B}$ gets the register B of ψ and $\mathcal{C}$ gets the register C.

Of interest to us is the case when $\mathcal{D}_1 = \mathcal{D}^{\mathsf{id}}$ and $\mathcal{D}_2 = \mathcal{D}^{\mathsf{ind}}$, where we define $\mathcal{D}^{\mathsf{id}}$ and $\mathcal{D}^{\mathsf{ind}}$ as follows[12]:

($\mathcal{D}^{\mathsf{id}}$) : Sample $|\psi\rangle \leftarrow \mathcal{D}$ and output $(|\psi\rangle_B \otimes |\psi\rangle_C)$

($\mathcal{D}^{\mathsf{ind}}$) : Sample $|\psi\rangle, |\psi'\rangle \leftarrow \mathcal{D}$ and output $(|\psi\rangle_B \otimes |\psi'\rangle_C)$, i.e. $\mathcal{D}^{\mathsf{ind}} = \mathcal{D} \times \mathcal{D}$.

In this case, we refer to the above notion as $(\varepsilon, \mathcal{D})$-simultaneous state indistinguishability ($(\varepsilon, \mathcal{D})$-SSI). Note that up to a constant factor this is equivalent to the output distributions of $\mathcal{A}$ with respect to $\mathcal{D}_1, \mathcal{D}_2$ having total variation distance ε. Also note that we can fix the bits b_1, b_2 without loss of generality.

▶ **Definition 7** ($(\varepsilon, \mathcal{D})$-SSI). *We say that* $(\varepsilon, \mathcal{D})$-SSI) *holds if $\mathcal{D}^{\mathsf{id}}$ and $\mathcal{D}^{\mathsf{ind}}$ defined above are ε-SSI against all non-local adversaries $(\mathcal{B}, \mathcal{C}, \rho)$.*

▶ Remark 8. When it is clear from the context, we omit the mention of the registers B and C.

2.1.1 SSI as a metric

This notion defines a metric over bipartite states, namely $T_{SSI}(\rho_0, \rho_1)$ is the smallest value of ε such that ρ_0 and ρ_1 are ε simultaneously indistinguishable. Equivalently,

$$T_{SSI}(\rho_0, \rho_1) := \sup_{(\mathcal{B}, \mathcal{C}, \rho)} \left| \Pr\left[(1,1) \leftarrow (\mathcal{B} \otimes \mathcal{C})(\rho \otimes \rho_0)\right] - \Pr\left[(1,1) \leftarrow (\mathcal{B} \otimes \mathcal{C})(\rho \otimes \rho_1)\right] \right|. \quad (2)$$

It is easy to see that this is a valid metric[13].

Since any binary measurement is a linear combination of projective measurements by the Spectral Theorem, we have the following fact.

[12] Here id stands for *identical* and ind stands for *independent*.

[13] Technically, a pseudometric since two different states may have distance 0.

▶ **Lemma 9.** *$T_{SSI}(\cdot,\cdot)$ can be equivalently defined by restricting $\mathcal{B},\mathcal{C}$ to be projective measurements.*

2.1.2 Extending to Many-Bit Output

We can extend the definition of SSI such that the non-local adversary can output many bits in each register. We then require that the total variation distance between the collective outputs of $\mathcal{B}$ and $\mathcal{C}$ for the two distributions is small.

▶ **Definition 10** (($\varepsilon, \mathcal{D}, n$)-SSI)**.** *We say that $(\varepsilon, \mathcal{D}, n)$-SSI holds if for any nonlocal adversary $\mathcal{A} = (\mathcal{B}, \mathcal{C}, \rho)$ and any $S \subseteq \{0,1\}^n \times \{0,1\}^n$ we have*

$$\left|\Pr\left[(x_1, x_2) \in S \ : \ \substack{|\psi\rangle \leftarrow \mathcal{D} \\ (x_1,x_2) \leftarrow \mathcal{A}(\psi\otimes\psi)}\right] - \Pr\left[(x_1, x_2) \in S \ : \ \substack{|\psi\rangle,|\psi'\rangle \leftarrow \mathcal{D} \\ (x_1,x_2) \leftarrow \mathcal{A}(\psi\otimes\psi')}\right]\right| \leq \varepsilon$$

Note that $(\varepsilon, \mathcal{D}, 2)$-SSI and $(\varepsilon, \mathcal{D})$-SSI are equivalent up to a constant factor on ε. There is a straightforward relation between $(\varepsilon, \mathcal{D})$-SSI and $(\varepsilon, \mathcal{D}, n)$-SSI using the union bound, which we formally state below.

▶ **Lemma 11.** *Suppose $(\varepsilon, \mathcal{D})$-SSI holds, then $(2^{2n-1}\varepsilon, \mathcal{D}, n)$-SSI holds for all $n \in \mathbb{N}$.*

Proof. For any non-local adversary $\mathcal{A} = (\mathcal{B}, \mathcal{C}, \rho)$ and any $y, y' \in \{0,1\}^n$, we have

$$|\Pr[(y, y') \leftarrow \mathcal{A}(\psi \otimes \psi) \ : \ |\psi\rangle \leftarrow \mathcal{D}] - \Pr[(y, y') \leftarrow \mathcal{A}(\psi \otimes \psi') \ : \ |\psi\rangle, |\psi'\rangle \leftarrow \mathcal{D}]| \leq \varepsilon$$

by $(\varepsilon, \mathcal{D})$-SSI. This is because $\mathcal{B}$ ($\mathcal{C}$) can associate y (respectively, y') with 0 and every other string with 1. By summing over all y, y' and dividing by 2 we get the desired result. ◀

2.1.3 Extending to Many Copies

For a distribution $\mathcal{D}$, denote by $\mathcal{D}^t$ the distribution that samples $|\psi\rangle \leftarrow \mathcal{D}$ and outputs $|\psi\rangle^{\otimes t}$. Then, we can consider $(\varepsilon, \mathcal{D}^t)$-SSI or $(\varepsilon, \mathcal{D}^t, n)$-SSI as extensions where $\mathcal{B}$ and $\mathcal{C}$ each get t copies of their respective inputs.

2.1.4 Extending to Many Parties

We can consider as the distinguisher a q-party non-local adversary $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_q, \rho_{A_1 \cdots A_q})$. By giving every party t copies of a quantum state generated either identically or independently we can generalize Definition 10:

▶ **Definition 12** (($\varepsilon, \mathcal{D}, n$)-SSI against q Parties)**.** *We say that $(\varepsilon, \mathcal{D}, n)$-SSI holds* against q parties *if for any q-party nonlocal adversary $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_q, \rho_{A_1 \cdots A_q})$ and any $S \subseteq \{0,1\}^{nq}$ we have*

$$\left|\Pr\left[(x_1, \ldots, x_q) \in S \ : \ \substack{|\psi\rangle \leftarrow \mathcal{D} \\ (x_1,\ldots,x_q) \leftarrow \mathcal{A}(\psi_{A_1}\otimes\cdots\otimes\psi_{A_q})}\right] \right.$$
$$\left. - \Pr\left[(x_1, \ldots, x_q) \in S \ : \ \substack{|\psi_1\rangle,\ldots,|\psi_q\rangle \leftarrow \mathcal{D} \\ (x_1,\ldots,x_q) \leftarrow \mathcal{A}((\psi_1)_{A_1}\otimes\ldots\otimes(\psi_q)_{A_q})}\right]\right| \leq \varepsilon$$

In general, SSI against many parties is weaker than regular SSI with the same number of copies and the same total output length, which we state formally below.

▶ **Lemma 13.** *Suppose that $(\varepsilon, \mathcal{D}^{qt}, qn)$-SSI holds (against 2 parties), then $(2q\varepsilon, \mathcal{D}^t, n)$-SSI holds against q parties.*

Combining Lemmas 11 and 13 yields the following corollary:

▶ **Corollary 14.** *Suppose that $(\varepsilon, \mathcal{D}^{qt})$-SSI holds, then $(2^{2qn}q\varepsilon, \mathcal{D}^t, n)$-SSI holds against q parties.*

2.2 Distinguishing Bell-States

In this section, we use the Bell basis over a 2-qubit system as a warm-up example to demonstrate some facts about simultaneous state indistinguishability. By the Bell basis we mean

$$\left\{\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right), \frac{1}{\sqrt{2}}\left(|00\rangle-|11\rangle\right), \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle+|{-}{-}\rangle\right), \frac{1}{\sqrt{2}}\left(|{+}{+}\rangle-|{-}{-}\rangle\right)\right\}.$$

Note that the Bell basis is symmetric for the purposes of this section, meaning any fact we show about a pair of Bell states will also apply to any other pair of Bell states. We start off by demonstrating that the non-local distance $T_{SSI}(\cdot,\cdot)$ can be strictly less than LOCC distance. Recall that two orthogonal Bell states can be perfectly distinguished using LOCC measurements.

▶ **Lemma 15** (Comparison to LOCC). *Let $|\Phi^+\rangle, |\Phi^-\rangle$ be orthogonal Bell states. Then,* $T_{SSI}\left(|\Phi^+\rangle\!\langle\Phi^+|, |\Phi^-\rangle\!\langle\Phi^-|\right) = 1/2$.

Proof. It suffices to consider projective $\mathcal{B}, \mathcal{C}$. After that, the only non-trivial case is when they both are rank-1 projections, in which case it is easy to show

$$\mathsf{Tr}\left((\mathcal{B}\otimes\mathcal{C})\left(|\Phi^+\rangle\!\langle\Phi^+| - |\Phi^-\rangle\!\langle\Phi^-|\right)\right) \le \mathsf{Tr}\left((\mathcal{B}\otimes\mathcal{C})\,|\Phi^+\rangle\!\langle\Phi^+|\right) \le 1/2. \qquad ◀$$

Next, we show that a non-local distinguisher with an arbitrary number of EPR pairs is no more powerful than unentangled distinguishers for the same problem.

▶ **Lemma 16** (Entanglement has no effect). *Let $|\Phi^+\rangle, |\Phi^-\rangle$ be orthogonal Bell states and let $|\mathsf{EPR}_n\rangle$ denote n EPR pairs. Then,* $T_{SSI}\left(|\Phi^+\rangle\!\langle\Phi^+| \otimes |\mathsf{EPR}_n\rangle\!\langle\mathsf{EPR}_n|, |\Phi^-\rangle\!\langle\Phi^-| \otimes |\mathsf{EPR}_n\rangle\!\langle\mathsf{EPR}_n|\right) = 1/2$.

2.3 Impossibility Results about SSI

There are many distributions that are simultaneously distinguishable. We give some examples below by identifying $\mathcal{D}$ for which $(\varepsilon, \mathcal{D})$-SSI does not hold for small ε.

▷ Claim 17. Suppose $\mathcal{D}$ is a (classical) distribution on $\{0,1\}^n$ such that $\mathsf{Pr}[y_1 \neq y_2 : y_1, y_2 \leftarrow \mathcal{D}] \ge c$, for some $c = c(n)$. Then, $(\varepsilon, \mathcal{D})$-simultaneous state indistinguishability does not hold for any $\varepsilon < c/2n$.

▷ Claim 18. Let $m, n \in \mathbb{N}$ and $m \ge n$. Let $C \in \mathcal{L}(\mathbb{C}^{2^n}, \mathbb{C}^{2^m})$ be a Clifford circuit. That is, C appends $m-n$ qubits initialized to zeros to its input and applies a sequence of Clifford gates. Define $\mathcal{D}_1$ as follows: sample $r \xleftarrow{\$} \{0,1\}^{n-1}$ and then output $|\psi_r\rangle_{BC} = C\,|r||0\rangle$. Define $\mathcal{D}_2$ as follows: sample $r \xleftarrow{\$} \{0,1\}^{n-1}$ and then output $|\psi_r\rangle_{BC} = C\,|r||1\rangle$. Then, the distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ are ε-simultaneous state distinguishable for all $\varepsilon < \frac{1}{2}$.

3 Simultaneous Haar Indistinguishability

We show that SSI can be instantiated using Haar random states.

3.1 Single-Copy Case

▶ **Theorem 19** (Simultaneous Haar Indistinguishability (SHI)). *$(\varepsilon, \mathcal{H}_{2^n})$-simultaneous state indistinguishability holds for $\varepsilon = O(1/2^{n/2})$.*

▶ Remark 20. The entangled state held by $\mathcal{A}$ above can have arbitrary dimension. In particular, the proof shows that an arbitrary number of EPR pairs has no asymptotic advantage in distinguishing identical vs. independent Haar states, for the advantage is $O(1/d)$ in both cases.

3.2 Generalization to Many Copies

We generalize Theorem 19 to show indistinguishability when the non-local distinguisher is given many copies of the input state. The proof has the same overall structure, but requires some additional ideas. We start by listing a useful lemma.

▶ **Lemma 21.** *Let $S_{2t}^{(s)} \subset S_{2t}$ be the set of permutations σ over $[2t]$ such that*

$$|\{i \in [t] \ : \ \sigma(i) \notin [t]\}| = s.$$

Define P_σ as the permutation operator over registers $X_1 \dots X_t Y_1 \dots Y_t$, where we match $[t]$ with $X_1 \dots X_t$ and $[2t] \setminus [t]$ with $Y_1 \dots Y_t$. Then,

$$\sum_{\sigma \in S_{2t}^{(s)}} P_\sigma = (t!)^2 \binom{t}{s}^2 \left(\Pi_{\mathsf{Sym}}(X_1 \dots X_t) \otimes \Pi_{\mathsf{Sym}}(Y_1 \dots Y_t)\right) P_{\sigma_s} \left(\Pi_{\mathsf{Sym}}(X_1 \dots X_t) \otimes \Pi_{\mathsf{Sym}}(Y_1 \dots Y_t)\right),$$

where $\sigma_s \in S_{2t}^{(s)}$ is the permutation that swaps i with $t+i$ for $i \in [s]$.

▶ **Theorem 22** (t-Copy Simultaneous Haar Indistinguishability (SHI))**.** *Let $\varepsilon = o(1)$ and $t = \varepsilon 2^{n/4}$. Let $\mathcal{H}_{2^n}^t$ be the distribution defined by sampling t copies of a state from $\mathcal{H}_{2^n}$. Then, $(O(\varepsilon^2), \mathcal{H}_{2^n}^t)$-simultaneous state indistinguishability holds.*

4 Applications

We present applications of simultaneous Haar indistinguishability (Section 3) to single-decryptor encryption (Section 4.1) and unclonable encryption (Section 4.2). Ordinarily, single-decryptor encryption is defined with classical ciphertexts and quantum decryption keys, whereas unclonable encryption is defined using quantum ciphertexts and classical encryption/decryption keys. We achieve relaxed notions of both primitives above: namely, we additionally allow quantum ciphertexts in single-decryptor encryption and quantum decryption keys in unclonable encryption.

In Section 4.3, we show how to construct leakage-resilient quantum secret sharing of classical messages, which additionally guarantees security against an eavesdropper that learns classical leakage of all the shares.

4.1 Single-Decryptor Encryption with Quantum Cipertexts

4.1.1 Definitions

We adopt the definition of single-decryptor encryption by [33] to the setting where the ciphertexts can be quantum.

▶ **Definition 23** (Single-Decryptor Encryption)**.** *A* single-decryptor encryption *(SDE) scheme is a tuple of QPT algorithms* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$*:*

- $\mathsf{Gen}(1^\lambda)$ *takes as input a security paramter. It outputs a classical encryption key* ek *and a one-time quantum decryption key* |🔑⟩*.*
- $\mathsf{Enc}(\mathsf{ek}, m)$ *takes as input an encryption key* ek*, and a classical message m. It outputs a quantum ciphertext* $|\mathsf{CT}\rangle$*. We require that* Enc *is pseudo-deterministic.*
- Dec(|🔑⟩, $|\mathsf{CT}\rangle$) *takes as input a quantum decryption key* |🔑⟩*, a quantum ciphertext* $|\mathsf{CT}\rangle$ *and outputs a classical message m.*

▶ **Definition 24** (Correctness). *A SDE scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *with quantum ciphertexts is* correct *if for any security parameter* λ *and any message* m *we have*

$$\Pr\left[m' = m \ : \ \substack{(\mathsf{ek}, |\text{🔑}\rangle) \leftarrow \mathsf{Gen}(1^\lambda) \\ |\mathsf{CT}\rangle \leftarrow \mathsf{Enc}(\mathsf{ek}, m) \\ m' \leftarrow \mathsf{Dec}(|\text{🔑}\rangle, |\mathsf{CT}\rangle)} \right] \geq 1 - \mathsf{negl}(\lambda).$$

Before defining security, we introduce a notation $\mathsf{Enc}^T(\mathsf{ek}, m)$, which means sampling randomness r and running $\mathsf{Enc}(\mathsf{ek}, m; r)$ for T times.

▶ **Definition 25** (Security of SDE). *An SDE scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is called* (information-theoretically) secure against identical ciphertexts *if for any cloning adversary* $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ *and any pair of messages* (m_0, m_1) *we have*

$$\Pr\left[b_{\mathcal{B}} = b_{\mathcal{C}} = b \ : \ \substack{(\mathsf{ek}, |\text{🔑}\rangle) \leftarrow \mathsf{Gen}(1^\lambda) \\ \rho_{BC} \leftarrow \mathcal{A}(|\text{🔑}\rangle) \\ b \xleftarrow{\$} \{0,1\}, \quad |\mathsf{CT}\rangle^{\otimes 2} \leftarrow \mathsf{Enc}^2(\mathsf{ek}, m_b) \\ b_{\mathcal{B}} \leftarrow \mathcal{B}(|\mathsf{CT}\rangle, \rho_B), \quad b_{\mathcal{C}} \leftarrow \mathcal{C}(|\mathsf{CT}\rangle, \rho_C)} \right] \leq \frac{1}{2} + \mathsf{negl}(\lambda),$$

where ρ_E *denotes the* E *register of the bipartite state* ρ_{BC} *for* $E \in \{B, C\}$*.*

▶ Remark 26 (Identical Ciphertexts). In Definition 25 we consider security against identical ciphertexts. One can similarly define security against ciphertexts that are independently generated. This alternate definition was achieved in the plain model by [7], and it only requires independent-challenge Goldreich-Levin.

▶ Remark 27. Note that Definition 25 need not be physical for an arbitrary scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ without the requirement that Enc is pseudo-deterministic due to the fact that $|\mathsf{CT}\rangle$ may be unclonable even for the encryptor. Nonetheless, our construction satisfies this condition, with the classical randomness of Enc being used for sampling a Haar random state.

Below, we consider a stronger security definition where many copies of the quantum ciphertext are given to the adversary. This matches the case of classical ciphertext more closely, since classical ciphertexts can be cloned arbitrarily. Another implication of this stronger definition is that security holds against adversaries who can clone the quantum ciphertexts.

▶ **Definition 28** (t-Copy Security of SDE). *An SDE scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is called* (information-theoretically) t-copy secure against identical ciphertexts *if for any cloning adversary* $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ *and any pair of messages* (m_0, m_1) *we have*

$$\Pr\left[b_{\mathcal{B}} = b_{\mathcal{C}} = b \ : \ \substack{(\mathsf{ek}, |\text{🔑}\rangle) \leftarrow \mathsf{Gen}(1^\lambda) \\ \rho_{BC} \leftarrow \mathcal{A}(|\text{🔑}\rangle) \\ b \xleftarrow{\$} \{0,1\}, \quad |\mathsf{CT}\rangle^{\otimes 2t} \leftarrow \mathsf{Enc}^{2t}(\mathsf{ek}, m_b) \\ b_{\mathcal{B}} \leftarrow \mathcal{B}(|\mathsf{CT}\rangle^{\otimes t}, \rho_B), \quad b_{\mathcal{C}} \leftarrow \mathcal{C}(|\mathsf{CT}\rangle^{\otimes t}, \rho_C)} \right] \leq \frac{1}{2} + \mathsf{negl}(\lambda),$$

where ρ_E *denotes the* E *register of the bipartite state* ρ_{BC} *for* $E \in \{B, C\}$*.*

4.1.2 Construction

Let $(\mathsf{Gen}_{\mathsf{UE}}, \mathsf{Enc}_{\mathsf{UE}}, \mathsf{Dec}_{\mathsf{UE}})$ be a one-time unclonable encryption scheme with C^n-weak unclonable security and message space $\mathcal{M} \subseteq \{0,1\}^n$, with $n = \mathsf{poly}(\lambda)$, where $C \in (1/2, 1)$ is a constant. Let $\mathcal{D} = \mathcal{H}_{2^n}$, so that:

1. $(\varepsilon, \mathcal{D}^t)$-SSI holds for some $\varepsilon = \mathsf{negl}(\lambda)$ by Theorem 22 as long as $t^2/2^{n/2}$ is negligible.
2. $\mathbb{E}_{|\psi\rangle \leftarrow \mathcal{D}} |\psi\rangle\langle\psi| = \mathsf{id}_{2^n}$.

We construct SDE for single-bit messages ($m \in \{0,1\}$) secure against identical ciphertexts as follows:

- $\mathsf{Gen}(1^\lambda)$ samples a random message $x \xleftarrow{\$} \mathcal{M}$ and a key $k \leftarrow \mathsf{Gen}_{\mathsf{UE}}(1^\lambda)$. It computes $|\psi\rangle \leftarrow \mathsf{Enc}_{\mathsf{UE}}(k, x)$. It outputs an encryption key $\mathsf{ek} = (k, x)$ and a decryption key $|$🔑$\rangle = |\psi\rangle$.
- $\mathsf{Enc}(\mathsf{ek}, m)$ samples $|\varphi\rangle = \sum_y \alpha_y |y\rangle \leftarrow \mathcal{D}$. It parses $\mathsf{ek} = (k, x)$ and computes the state $|\phi\rangle = \sum_y \alpha_y |y\rangle |\langle y, x\rangle \oplus m\rangle$. It outputs a quantum ciphertext $|\mathsf{CT}\rangle = (k, |\phi\rangle)$. Note that Enc is pseudo-deterministic given that it can sample from $\mathcal{D}$ using classical randomness.
- $\mathsf{Dec}(|$🔑$\rangle, |\mathsf{CT}\rangle)$ parses $|\mathsf{CT}\rangle = (k, |\phi\rangle)$. It computes $x \leftarrow \mathsf{Dec}_{\mathsf{UE}}(k, |\phi\rangle)$. It computes $U_x |\psi\rangle$ and measures the second register to obtain m, where U_x is the unitary defined as $U_x |y\rangle |z\rangle = |y\rangle |z \oplus \langle y, x\rangle\rangle$. It outputs m.

▶ Remark 29. Since t is bounded (see Theorem 34), we can use a $2t$-state design to instantiate the Haar random state used in the construction. We can similarly use a $2t$-state design to instantiate our construction of unclonable encryption in Section 4.2.

From the correctness of $(\mathsf{Gen}_{\mathsf{UE}}, \mathsf{Enc}_{\mathsf{UE}}, \mathsf{Dec}_{\mathsf{UE}})$, it follows that Dec recovers m (with probability negligibly close to 1) from $|\mathsf{CT}\rangle$, where $|\mathsf{CT}\rangle$ is an encryption of m.

4.1.3 Security Proof

We first show a lemma that is needed in our security proof:

▶ **Lemma 30** (Simultaneous Quantum Goldreich-Levin with Correlated Input). *Let $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ be a cloning adversary that given*[14] *$(\rho, (\sigma, (y_{\mathcal{B}}, b_{\mathcal{B}}), (y_{\mathcal{C}}, b_{\mathcal{C}})))$, where $y_{\mathcal{B}}, y_{\mathcal{C}} \in \{0,1\}^n$ are i.i.d. uniform strings and $b_{\mathcal{B}}, b_{\mathcal{C}} \in \{0,1\}$ are random bits satisfying $b_{\mathcal{B}} \oplus b_{\mathcal{C}} = \langle y_{\mathcal{B}}, x\rangle \oplus \langle y_{\mathcal{C}}, x\rangle$, can output $(\langle y_{\mathcal{B}}, x\rangle, \langle y_{\mathcal{C}}, x\rangle)$ with probability at least $1/2 + \varepsilon$. Then, there is an extractor $(\mathcal{A}', \mathcal{B}', \mathcal{C}')$ that given input (ρ, σ) outputs (x, x) (running $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ as a subprotocol) with probability* $\mathsf{poly}(\varepsilon)$*.*

▶ Remark 31. Lemma 30 proves a special case of the simultaneous inner product conjecture postulated in [3]. Roughly speaking, the simultaneous inner product conjecture states that if a set of bipartite states $\{\rho_x\}_{x \in \{0,1\}^n}$ is such that any non-local adversary $(\mathcal{B}, \mathcal{C})$ given ρ_x, where $x \xleftarrow{\$} \{0,1\}^n$, cannot recover x (except with negligible probability) then $\mathcal{B}$ and $\mathcal{C}$ cannot distinguish Goldreich-Levin samples versus uniform samples (except with negligible advantage). The conjecture is parameterized by the distribution of the samples and also by the algebraic field associated with the samples. Lemma 30 shows that the conjecture is true for a correlated distribution of samples and when the field in question is $\mathbb{F}_2$.

▶ Remark 32. Lemma 30 resolves an important technical issue we will face in our unclonable security proof, similar to the one faced by [44][15]. Namely, $\mathcal{B}$ and $\mathcal{C}$ seem to get additional information about the hidden values $\langle y_{\mathcal{B}}, x\rangle, \langle y_{\mathcal{C}}, x\rangle$ by holding secret shares of their XOR value. Above we show that this is in fact not the case, i.e. the adversary does not get additional power from these shares. In [44], the authors utilized alternative security definitions to overcome this issue.

▶ **Theorem 33.** $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *above is secure against identical ciphertexts.*

***t*-Copy Security.** We show that our construction remains secure if up to $O(n)$ copies of the quantum ciphertext is given to the adversary in the unclonable security experiment.

[14] Here ρ is given to $\mathcal{A}$ and then a bipartite state σ is given to $\mathcal{B}$, $\mathcal{C}$ in the challenge phase.

[15] See Remark 7 (pp. 53) in [44].

▶ **Theorem 34.** *Let $c > 0$ be a constant and $t \leq (\log_2(1/\sqrt{C}) - c)n)$, then* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *above is t-copy secure against identical ciphertexts.*

By instantiating $(\mathsf{Gen}_{\mathsf{UE}}, \mathsf{Enc}_{\mathsf{UE}}, \mathsf{Dec}_{\mathsf{UE}})$ with the construction of [17], we can set $C = 0.86$ and thus $t = n/10$. Therefore, by setting $n = 10t$ we get the following corollary:

▶ **Corollary 35.** *For any $t = \mathsf{poly}(\lambda)$, there exists a single-decryptor encryption scheme with quantum ciphertexts t-copy secure against identical ciphertexts (Definition 28) in the plain model.*

▶ Remark 36 (Bounded Number of Copies). Our construction is not t-copy secure against identical ciphertexts if t is an unbounded polynomial due to a simple attack that measures each copy of the ciphertext in the computational basis. Every measurement (except the first) will give a random linear constraint on the bits of x, hence a linear number of copies on average suffice to solve for x entirely. Nonetheless, we can set n accordingly for any fixed polynomial t.

4.2 Unclonable Encryption with Quantum Keys

Using our ideas in Section 4.1, we construct unclonable encryption with quantum keys in the plain model. Besides allowing the decryption key to be quantum, we do not relax the syntax of unclonable encryption. In particular, we achieve identical-challenge security with quantum challenges. Due to its similarity with Section 4.1, we leave the details of this section for the full version.

4.3 Secret Sharing

Definition. Below we formally define a quantum secret sharing scheme for a single-bit message $m \in \{0, 1\}$, which is secure against an eavesdropper if only classical strings are leaked from the quantum shares.

▶ **Definition 37** (2-out-of-n Classical-Leakage-Resilient Quantum Secret Sharing). *Let $n = \mathsf{poly}(\lambda)$. A* 2-out-of-$n$ classical-leakage-resilient quantum secret sharing scheme *is a tuple of algorithms* $(\mathsf{Share}, \mathsf{Rec})$ *with the following syntax:*

- $\mathsf{Share}(1^\lambda, m)$ *takes as input a security parameter and a message $m \in \{0, 1\}$; it outputs a product state $|\psi_m\rangle = \bigotimes_{i=1}^n |\psi_m^i\rangle$ over registers $S_1, S_2, \ldots, S_n$ with* $\mathsf{poly}(\lambda)$ *qubits each.*
- $\mathsf{Rec}(i, j, \psi^i, \psi^j)$ *takes as input two indices $i, j \in [n]$ and quantum shares $|\psi^i\rangle, |\psi^j\rangle$ over registers S_i, S_j. It outputs a message $m \in \{0, 1\}$.*

It satisfies the following properties:

1. **δ-Correctness:** *For all $m \in \{0, 1\}, \lambda \in \mathbb{N}, (i, j) \in [n] \times [n]$ we have*

$$\Pr\left[m \leftarrow \mathsf{Rec}(i, j, \psi_m^i, \psi_m^j) \;:\; |\psi\rangle = \bigotimes_{i=1}^n |\psi_m^i\rangle \leftarrow \mathsf{Share}(1^\lambda, m)\right] \geq \delta.$$

2. **Perfect Secrecy:** *For all $i \in [n]$, we have*

$$\mathop{\mathbb{E}}_{|\psi_0\rangle \leftarrow \mathsf{Share}(1^\lambda, 0)} |\psi_0^i\rangle\langle\psi_0^i| = \mathop{\mathbb{E}}_{|\psi_1\rangle \leftarrow \mathsf{Share}(1^\lambda, 1)} |\psi_1^i\rangle\langle\psi_1^i|.$$

3. **ℓ-bit ε Classical-Leakage-Resilience:** *For any quantum algorithms* $\mathsf{Leak}_1, \dots, \mathsf{Leak}_n$ *that output ℓ classical bits, any n-partite state ρ, and any distinguisher $\mathcal{A}$, we have*

$$\left| \Pr\left[1 \leftarrow \mathcal{A}(y_1, \dots, y_n) \ : \ \substack{\psi_0 \leftarrow \mathsf{Share}(1^\lambda, 0) \\ y_i \leftarrow \mathsf{Leak}_i(\psi_0^i, \rho_i),\ i \in [n]}\right] \right.$$
$$\left. - \Pr\left[1 \leftarrow \mathcal{A}(y_1, \dots, y_n) \ : \ \substack{\psi_1 \leftarrow \mathsf{Share}(1^\lambda, 1) \\ y_i \leftarrow \mathsf{Leak}_i(\psi_1^i, \rho_i),\ i \in [n]}\right] \right| \leq \varepsilon,$$

where ρ_i is the i-th register of ρ.

▶ Remark 38. Note that we consider the perfect secrecy and the classical leakage resilience properties separately. It is natural to ask if it is possible to combine the two properties into a stronger property that guarantees security even against adversaries who in addition to receiving one of the shares, also receives as input classical leakage on the rest of the shares. Unfortunately, this stronger property cannot be satisfied due to a simple attack via quantum teleportation. Thus, we need to consider these two properties separately.

▶ Remark 39. The above notion can be generalized in many ways. Firstly, for simplicity, we define the shares to be pure states and we could consider a general notion where the shares could be entangled with each other. Secondly, we can consider sharing schemes guaranteeing security against different adversarial access structures.

4.3.1 Construction

We will construct the primitive above using the Haar distribution $\mathcal{D} = \mathcal{H}_d$ for $d = 2^{4\ell+\lambda}$. This satisfies $(\varepsilon, \mathcal{D}^t, \ell)$-SSI for $\varepsilon = \mathsf{negl}(\lambda)$ by Corollary 14 and Theorem 22. $\mathcal{H}_d$ can in turn be instantiated using a nt-design. We will pick $\omega(\log \lambda) \leq t \leq \mathsf{poly}(\lambda)$, so that the construction is efficient.

- $\mathsf{Share}(1^\lambda, m)$: Set $d = 2^{4n\ell+\lambda}$ and $\mathcal{D} = \mathcal{H}_d$. If $m = 0$, it samples nt copies of $|\psi\rangle \leftarrow \mathcal{D}$ and outputs $|\psi\rangle_{S_1}^{\otimes t} \otimes \dots \otimes |\psi\rangle_{S_n}^{\otimes t}$. If $m = 1$, it independently samples t copies of $|\psi_i\rangle \leftarrow \mathcal{D}$ for $i \in [n]$ and outputs $|\psi_1\rangle_{S_1}^{\otimes t} \otimes \dots \otimes |\psi_n\rangle_{S_n}^{\otimes t}$.
- $\mathsf{Rec}(i, j, |\varphi\rangle_{S_i}, |\varphi'\rangle_{S_j})$: It parses $S_i = S_i^{(1)} \dots S_i^{(t)}$ and $S_j = S_j^{(1)} \dots S_i^{(t)}$ as t registers. It applies a SWAP test to the registers $S_i^{(k)}$ and $S_j^{(k)}$ for $k \in [t]$. It outputs 0 if at least $\lfloor 3t/4 \rfloor$ of the SWAP tests succeed and outputs 1 otherwise.

4.3.2 Correctness and Secrecy

The construction above has δ-correctness for $\delta \geq 1 - \mathsf{negl}(\lambda)$. Note that for $m = 0$ each SWAP test will succeed with probability 1, so Rec will always output the correct message. If $m = 1$ on the other hand, each SWAP test will succeed with probability negligibly close to $1/2$, so by a Chernoff bound Rec will output 0 with only negligible probability since $t = \omega(\log \lambda)$.

Perfect secrecy is trivial given that each share is distributed according to $\mathcal{D}$.

4.3.3 Classical Leakage Resilience

By Corollary 14 and Theorem 22, the total variation distance between the output distributions of any ℓ-bit leakage functions $\mathsf{Leak}_1, \dots, \mathsf{Leak}_n$ with respect to shares of $m = 0$ and $m = 1$ is at most

$$O\left(\frac{2^{2n\ell} n^3 t^2}{\sqrt{d}}\right) = O\left(\frac{n^3 t^2}{2^{\lambda/2}}\right) \leq \mathsf{negl}(\lambda).$$

References

1 Scott Aaronson. Quantum copy-protection and quantum money. In *2009 24th Annual IEEE Conference on Computational Complexity*, pages 229–242. IEEE, 2009. doi:10.1109/CCC.2009.42.

2 Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, Joao Ribeiro, and Mark Simkin. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39*, pages 510–539. Springer, 2019. doi:10.1007/978-3-030-26951-7_18.

3 Prabhanjan Ananth and Amit Behera. A modular approach to unclonable cryptography. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024*, pages 3–37, Cham, 2024. Springer Nature Switzerland. doi:10.1007/978-3-031-68394-7_1.

4 Prabhanjan Ananth, Aditya Gulati, and Yao-Ting Lin. Cryptography in the common haar state model: Feasibility results and separations. In Elette Boyle and Mohammad Mahmoody, editors, *Theory of Cryptography*, pages 94–125, Cham, 2025. Springer Nature Switzerland.

5 Prabhanjan Ananth and Fatih Kaleoglu. Unclonable encryption, revisited. In *Theory of Cryptography Conference*, pages 299–329. Springer, 2021. doi:10.1007/978-3-030-90459-3_11.

6 Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. On the feasibility of unclonable encryption, and more. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 212–241, Cham, 2022. Springer Nature Switzerland. doi:10.1007/978-3-031-15979-4_8.

7 Prabhanjan Ananth, Fatih Kaleoglu, and Qipeng Liu. Cloning games: A general framework for unclonable primitives. In *CRYPTO*, 2023.

8 Prabhanjan Ananth, Fatih Kaleoglu, and Henry Yuen. Simultaneous haar indistinguishability with applications to unclonable cryptography, 2024. arXiv:2405.10274, doi:10.48550/arXiv.2405.10274.

9 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. doi:10.1007/978-3-030-77886-6_17.

10 Boaz Barak, Oded Goldreich, Rusell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im) possibility of obfuscating programs. In *Annual international cryptology conference*, pages 1–18. Springer, 2001. doi:10.1007/3-540-44647-8_1.

11 James Bartusek, Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Obfuscation of pseudo-deterministic quantum circuits. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1567–1578, 2023. doi:10.1145/3564246.3585179.

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

13 Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. *Journal of Cryptology*, 34:1–65, 2021.

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. *Physical review letters*, 70(13):1895, 1993.

15 Charles H Bennett, David P DiVincenzo, Christopher A Fuchs, Tal Mor, Eric Rains, Peter W Shor, John A Smolin, and William K Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59(2):1070, 1999.

16 Anne Broadbent and Raza Ali Kazmi. Constructions for quantum indistinguishability obfuscation. In *International Conference on Cryptology and Information Security in Latin America*, pages 24–43. Springer, 2021. doi:10.1007/978-3-030-88238-9_2.

17 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.

18 Francesco Buscemi. All entangled quantum states are nonlocal. *Physical review letters*, 108(20):200401, 2012.

19 Alper Çakan and Vipul Goyal. Unclonable cryptography with unbounded collusions. *Cryptology ePrint Archive*, 2023.

20 Alper Cakan, Vipul Goyal, Chen-Da Liu-Zhang, and João Ribeiro. Unbounded leakage-resilience and intrusion-detection in a quantum world. *Cryptology ePrint Archive*, 2023.

21 Eshan Chattopadhyay, Jesse Goodman, Vipul Goyal, Ashutosh Kumar, Xin Li, Raghu Meka, and David Zuckerman. Extractors and secret sharing against bounded collusion protocols. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1226–1242. IEEE, 2020. doi:10.1109/FOCS46700.2020.00117.

22 Sitan Chen, Jordan Cotler, Hsin-Yuan Huang, and Jerry Li. Exponential separations between learning with and without quantum memory. In *FOCS*, 2021.

23 Andrew M Childs, Debbie Leung, Laura Mančinska, and Maris Ozols. A framework for bounding nonlocality of state discrimination. *Communications in Mathematical Physics*, 323:1121–1153, 2013.

24 Eric Chitambar and Min-Hsiu Hsieh. Asymptotic state discrimination and a strict hierarchy in distinguishability norms. *Journal of Mathematical Physics*, 55(11), 2014.

25 Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about locc (but were afraid to ask). *Communications in Mathematical Physics*, 328:303–326, 2014.

26 Andrea Coladangelo and Sam Gunn. How to use quantum indistinguishability obfuscation. In *STOC*, 2024.

27 Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden cosets and applications to unclonable cryptography. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology – CRYPTO 2021*, pages 556–584, Cham, 2021. Springer International Publishing. doi:10.1007/978-3-030-84242-0_20.

28 Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model. *Quantum*, 8:1330, May 2024. doi:10.22331/q-2024-05-02-1330.

29 David P DiVincenzo, Debbie W Leung, and Barbara M Terhal. Quantum data hiding. *IEEE Transactions on Information Theory*, 48(3):580–598, 2002. doi:10.1109/18.985948.

30 Llorenç Escolà-Farràs, Jaròn Has, Maris Ozols, Christian Schaffner, and Mehrdad Tahmasbi. Parallel repetition of local simultaneous state discrimination. *arXiv preprint arXiv:2211.06456*, 2022.

31 Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. *SIAM Journal on Computing*, 45(3):882–929, 2016. doi:10.1137/14095772X.

32 Julio Gea-Banacloche. Hiding messages in quantum data. *Journal of Mathematical Physics*, 43(9):4531–4536, 2002.

33 Marios Georgiou and Mark Zhandry. Unclonable decryption keys. *IACR Cryptol. ePrint Arch.*, 2020:877, 2020. URL: https://eprint.iacr.org/2020/877.

34 O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, STOC '89, pages 25–32, New York, NY, USA, 1989. Association for Computing Machinery. doi:10.1145/73007.73010.

35 Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 685–698, 2018. doi:10.1145/3188745.3188872.

36 Saronath Halder, Manik Banik, Sristy Agrawal, and Somshubhro Bandyopadhyay. Strong quantum nonlocality without entanglement. *Physical review letters*, 122(4):040403, 2019.

37 Aram W. Harrow. The church of the symmetric subspace, 2013. arXiv:1308.6595.

38 Aram W. Harrow. Approximate orthogonality of permutation operators, with application to quantum information, 2023. arXiv:2309.00715.

39 Patrick Hayden, Debbie Leung, and Graeme Smith. Multiparty data hiding of quantum information. *Physical Review A*, 71(6):062339, 2005.

40 Carl W Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1:231–252, 1969.

41 Taiga Hiroka, Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Robust combiners and universal constructions for quantum cryptography. *arXiv preprint arXiv:2311.09487*, 2023.

42 Yael Tauman Kalai and Leonid Reyzin. A survey of leakage-resilient cryptography. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 727–794. Association for Computing Machinery, 2019. doi:10.1145/3335741.3335768.

43 Fuyuki Kitagawa and Ryo Nishimaki. One-out-of-many unclonable cryptography: Definitions, constructions, and more. In *Theory of Cryptography Conference*, pages 246–275. Springer, 2023. doi:10.1007/978-3-031-48624-1_10.

44 Srijita Kundu and Ernest Y. Z. Tan. Device-independent uncloneable encryption, 2022. doi:10.48550/arXiv.2210.01058.

45 Christian Majenz, Maris Ozols, Christian Schaffner, and Mehrdad Tahmasbi. Local simultaneous state discrimination, 2021. arXiv:2111.01209.

46 William Matthews, Stephanie Wehner, and Andreas Winter. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. *Communications in Mathematical Physics*, 291:813–843, 2009.

47 Antonio Anna Mele. Introduction to haar measure tools in quantum information: A beginner's tutorial, 2024. arXiv:2307.08956.

48 Michael Nathanson. Distinguishing bipartitite orthogonal states using locc: Best and worst cases. *Journal of Mathematical Physics*, 46(6), 2005.

49 Roger Penrose. Applications of negative dimensional tensors. *Welsh, D., Ed., Combinatorial Mathematics and Its Applications*, pages 221–244, 1971.

50 Asher Peres and William K Wootters. Optimal detection of quantum information. *Physical Review Letters*, 66(9):1119, 1991.

51 Marco Piani, Varun Narasimhachar, and John Calsamiglia. Quantumness of correlations, quantumness of ensembles and quantum data hiding. *New Journal of Physics*, 16(11):113001, 2014.

52 Robert Raussendorf and Tzu-Chieh Wei. Quantum computation by local measurement. *Annual Review of Condensed Matter Physics*, 3(Volume 3, 2012):239–261, 2012. doi:10.1146/annurev-conmatphys-020911-125041.

53 Akshayaram Srinivasan and Prashant Nalini Vasudevan. Leakage resilient secret sharing and applications. In *Annual International Cryptology Conference*, pages 480–509. Springer, 2019. doi:10.1007/978-3-030-26951-7_17.

54 Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983. doi:10.1145/1008908.1008920.

55 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. doi:10.1007/978-3-030-17659-4_14.