Unclonable Secret Sharing

Prabhanjan Ananth[1(✉)], Vipul Goyal[2], Jiahui Liu[3], and Qipeng Liu[4]

[1] University of California, Santa Barbara, Santa Barbara, USA
prabhanjan@cs.ucsb.edu
[2] NTT Research, Carnegie Mellon University, Pittsburgh, USA
vipul@cmu.edu
[3] Massachusetts Institute of Technology, Cambridge, USA
[4] University of California, San Diego, San Diego, USA

Abstract. Unclonable cryptography utilizes the principles of quantum mechanics to addresses cryptographic tasks that are impossible classically. We introduce a novel unclonable primitive in the context of secret sharing, called unclonable secret sharing (USS). In a USS scheme, there are n shareholders, each holding a share of a classical secret represented as a quantum state. They can recover the secret once all parties (or at least t parties) come together with their shares. Importantly, it should be infeasible to copy their own shares and send the copies to two non-communicating parties, enabling both of them to recover the secret.

Our work initiates a formal investigation into the realm of unclonable secret sharing, shedding light on its implications, constructions, and inherent limitations.

- **Connections**: We explore the connections between USS and other quantum cryptographic primitives such as unclonable encryption and position verification, showing the difficulties to achieve USS in different scenarios.
- **Limited Entanglement**: In the case where the adversarial shareholders do not share any entanglement or limited entanglement, we demonstrate information-theoretic constructions for USS.
- **Large Entanglement**: If we allow the adversarial shareholders to have unbounded entanglement resources (and unbounded computation), we prove that unclonable secret sharing is impossible. On the other hand, in the quantum random oracle model where the adversary can only make a bounded polynomial number of queries, we show a construction secure even with unbounded entanglement.
  Furthermore, even when these adversaries possess only a polynomial amount of entanglement resources, we establish that any unclonable secret sharing scheme with a reconstruction function implementable using Cliffords and logarithmically many T-gates is also unattainable.

1 Introduction

Alice is looking for storage for her sensitive data. She decides to hire multiple independent cloud providers and secret shares her data across them. Later

K.-M. Chung and Y. Sasaki (Eds.): ASIACRYPT 2024, LNCS 15492, pp. 129–157, 2025.
https://doi.org/10.1007/978-981-96-0947-5_5

on, Alice retrieves these shares and reconstructs the data. Everything went as planned. However: what if the cloud providers keep a copy and sell shares of her data to her competitor, Bob? How can Alice make sure that once she retrieves her data, no one else can?

This is clearly impossible in the classical setting. The cloud providers can always keep a copy of the share locally and later, if Bob comes along, sell that copy to Bob. Nonetheless, this problem has been recently studied in the classical setting by a recent work of Goyal, Song, and Srinivasan [GSS21] who introduced the notion of traceable secret sharing (TSS). In TSS, if (a subset of) the cloud providers sell their shares to Bob, they cannot avoid leaving a cryptographic proof of fraud with Bob. Moreover, this cryptographic proof could not have been generated by Alice. Hence, (assuming Bob cooperates with Alice), Alice can sue the cloud providers in court and recover damages. Thus, TSS only acts as a deterrent and indeed, cannot stop the cloud providers from copying the secret.

However, in the quantum setting, the existence of no cloning theorem offers the tantalizing possibility that perhaps one may be able to build an "unclonable secret sharing" (USS) scheme. Very informally, the most basic version of a USS can be described as follows:

- Alice (the dealer) has a classical secret $m \in \{0,1\}^*$. She hires n cloud providers $\mathcal{P}_1, \ldots, \mathcal{P}_n$.
- Alice computes shares $(\rho_1, \cdots, \rho_n)$, which is an n-partite state, from m and sends the share ρ_i to the party $\mathcal{P}_i$ (note that Alice does not need to store any information like a cryptography key on her own).
- Given $(\rho_1, \cdots, \rho_n)$, it is easy to recover m. But given any strict subset of the shares, no information about m can be deduced (i.e., it is an n-out-of-n secret sharing scheme).
- The most important is the unclonability. For every $i \in [n]$, the party $\mathcal{P}_i$ computes a bipartite state $\sigma_{\mathbf{X}_i\mathbf{Y}_i}$. It sends the register $\mathbf{X}_i$ to Bob and $\mathbf{Y}_i$ to Charlie. Assuming that the message m was randomly chosen to be either m_0 or m_1 (where (m_0, m_1) is chosen adversarially), the probability that both Bob and Charlie can guess the correct message must be upper bounded by a quantity negligibly close to $\frac{1}{2}$.

In other words, the parties $\mathcal{P}_1, \ldots, \mathcal{P}_n$ must be unable to locally clone their shares such that both sets of shares allow for reconstruction. Indeed, as we mentioned, this is the most basic version of USS. Even this basic setting has a practical significance: the servers which store Alice's shares may not intentionally communicate her shares with each other, because they belong to companies with conflict of interest; but a malicious Bob may still buy a copy of Alice's share from each of them.

One can consider more general settings where, e.g., we are interested in threshold (i.e., t-out-of-n) USS or, where a subset of the n parties might collude in attempting to clone their shares. One can also consider the setting where the parties $\mathcal{P}_1, \ldots, \mathcal{P}_n$ share some entanglement (allowing them to use quantum teleportation).

Unclonable cryptography leverages the power of quantum information and empowers one to achieve primitives which are clearly impossible in classical cryptography. While a lot of efforts have been made towards various unclonable cryptographic primitives including but not limited to quantum money [BB20, AC12, Zha17, Shm22, LMZ23], copy-protection [Aar09, CLLZ21, AL20], tokenized signatures [BS16, CLLZ21, Shm22] and unclonable encryption (UE) [Got02, BL20, AK21, AKL+22, AKL23], the question of unclonable secret sharing had not been studied prior to our work. Secret sharing is one of the most fundamental primitives in cryptography and as such, we believe that studying unclonable secret sharing is an important step towards laying the foundation of unclonable cryptography. Our contribution lies in initiating a systematic study of USS.

Connection to Unclonable Encryption. The classical counterparts of unclonable encryption and (2-out-of-2) unclonable secret sharing are very similar. For instance, both one-time pad encryption and 2-out-of-2 secret sharing rely on the same ideas in the classical setting. One may wonder if UE and USS share similar a relation. UE resembles standard encryption with one additional property: now ciphertext is unclonable, meaning no one can duplicate a ciphertext into two parts such that both parts can be used separately to recover the original plaintext. At first glance, it might seem like UE directly implies a 2-out-of-2 USS. To secret share m, the dealer (Alice) would generate a secret key sk, and compute ciphertext ρ_{ct}, which encrypts the classical message m. One of the shares will be ρ_{ct} while the other will be sk. Since ρ_{ct} is unclonable, this may prevent two successful reconstructions of the original message.

However, the above intuition does not work if the two parties in (2-out-of-2) USS share entanglement. In UE, the ciphertext ρ_{ct} is a split into two components and sent to Alice and Bob. Later on, the secret key sk is sent (without any modification) to both Alice and Bob. However, in USS, the secret key sk corresponds to the second share and might also be split into two register such that one is sent to Alice and the other to Bob. This split could be done using a quantum register which is entangled with the quantum register used to split the cipher text ρ_{ct}. It is unclear if such an attack can be reduced to the UE setting, where there is no analog of such an entangled register. In fact, we show the opposite. We show that in some settings, USS implies UE, thus showing that USS could be a stronger primitive.

Connection to Instantaneous Non-local Computation. It turns out that the positive results on instantaneous non-local computation imply negative results on USS in specific settings. The problem of instantaneous non-local computation [Vai03, BK11, Spe15, IH08, GC19] is the following: Dave and Eve would like to compute a unitary U on a state $\rho_{\mathbf{XY}}$, where Dave has the register $\mathbf{X}$ and Eve has the register $\mathbf{Y}$. They need to do so by just exchanging one message simultaneously with each other. Non-local computation has connections to the theory of quantum gravity, as demonstrated in some recent works [May19, May22]. Suppose there is a unitary U for which non-local computation is possible then this rules out a certain class of unclonable secret sharing schemes. Specifically, it disallows certain reconstruction procedures that are functionally equivalent to U. In more detail, consider a USS scheme that is defined as follows: on input a message m, it produces shares on two registers $\mathbf{X}$ and $\mathbf{Y}$. The reconstruction procedure[1] takes as input the shares and outputs m in both registers $\mathbf{X}$ and $\mathbf{Y}$. Any non-local computation protocol for such a reconstruction procedure would violate the security of the USS scheme. Investigating both positive and negative results of USS schemes could shed more light on the feasibility of non-local computation. In this work, we adapt and generalize techniques used in the literature on non-local computation to obtain impossibility results for USS.

USS also has connections to position verification, a well-studied notion in quantum cryptography that has connections to problems in fundamental physics. We discuss this in the next section.

1.1 Our Results

In this work, our primary emphasis will be on n-out-of-n unclonable secret sharing schemes as even though they are the simplest, they give rise to numerous intriguing questions. Our results are twofold, as below.

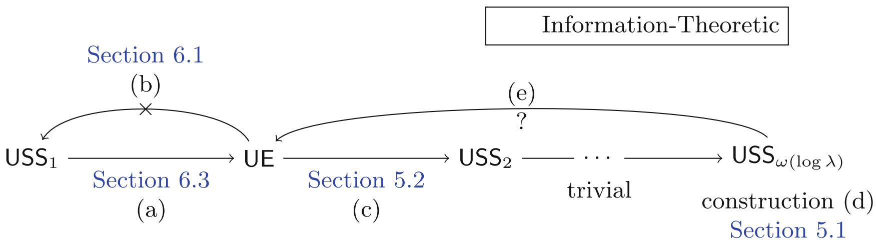

Fig. 1. Relations between USS and UE in the information-theoretic regime.

Results on Information-Theoretic USS. We first examine the connections between USS and UE and constructions of UE in the information-theoretic regime. The first part of our results can be summarized by Fig. 1. In the figure, USS_1 stands for information-theoretic USS, secure against adversarial parties sharing *unbounded* amount of entanglement; we will explain why we call it USS_1 later on. We first show that, even if we restrict adversaries in USS_1 to have a polynomial amount of entanglement, it implies UE.

[1] In general, a reconstruction procedure need not output a copy of the secret twice but using CNOT gates, we can easily transform any reconstruction procedure into one that outputs two copies of the secret.

Theorem 1 (direction (a) in Fig. 1, Sect. 6.3). *Information-theoretic USS that is secure against adversarial parties $\mathcal{P}$ sharing* polynomial *amount of entanglement implies UE.*

This leads us to ponder whether USS_1 and UE share equivalence, like their classical counterparts do. Perhaps surprisingly, we show that this connection is unlike to hold. We prove that USS_1 does not exist in the information-theoretic setting. Since there is no obvious evidence to refute UE in the IT setting and many candidates were proposed toward information-theoretic UE, our impossibility stands in sharp contrast to UE.

Theorem 2 (direction (b) in Fig. 1, Sect. 6.1). *Information-theoretic USS that is secure against adversarial parties $\mathcal{P}$ sharing* unbounded *amount of entanglement with each other, does not exist.*

Facing the above impossibility, it seems like USS in the IT regime comes to a dead end. To overcome the infeasibility result, we investigate USS against adversarial parties with specific entanglement configurations. We consider the case where every pair of $\mathcal{P}_i$ and $\mathcal{P}_j$ either shares unbounded entanglement or shares no entanglement. In this case, we can define an entanglement graph, of which an edge (i, j) corresponds to entanglement between $\mathcal{P}_i$ and $\mathcal{P}_j$. Then, we propose the natural generalization and define USS_d for any $d > 1$:

USS_d: Information-theoretic USS, secure against adversarial parties sharing entanglement whose entanglement graph has at least d connected components.

The above definition captures the case that there are d groups of parties; there is unlimited entanglement between parties in the same group and no entanglement between parties in different groups. This notation is not only for overcoming the barrier, but also has practical interest: parties from different groups are geographically separated or have conflict of interest, maintaining entanglement between them is either too expensive or impossible. Note that the characterization of entanglement is only for adversarial parties, whereas honest execution of the scheme does not need any pre-shared entanglement. We also like to note that aforementioned USS_1 is also captured by the above definition when $d = 1$.

It is easy to see that the existence of USS_d implies USS_{d+1} for any $d \geq 1$, as having less entanglement makes attacking more difficult. However, since USS_1 is impossible, can we construct USS_d for some d? We complete the picture of USS and UE by presenting the following two theorems.

Theorem 3 (direction (c) in Fig. 1, Sect. 5.2). UE *implies* USS_2 *in the information-theoretic setting. As a corollary, it implies* USS_d *for any* $d > 1$ *in the IT setting.*

Theorem 4 (construction (d) in Fig. 1, Sect. 5.1). USS_d *exists for every* $d = \omega(\log \lambda)$ *in the information-theoretic setting, where* λ *is the security parameter.*

Along with Theorem 4, we proved a special XOR lemma of the well-known monogamy-of-entanglement property for BB84 states [BB20, TFKW13], when the splitting adversary is limited to tensor strategies. More precisely, we only consider cloning strategies that apply channels on each individual qubit, but never jointly on two or more qubits. Given a BB84 state, let $p(n)$ be the probability of the optimal tensor cloning strategy, that later two non-communicating parties recover the parity simultaneously. $p(1) = 1/2 + 1/2\sqrt{2}$ was proved in [TFKW13]. In this work, we show that $p(n) = 1/2 + \exp(-\Omega(n))$, which demonstrates a XOR hardness amplification for tensor strategies. We believe the proof of the theorem will be of independent interest, as a more general version of the theorem (that applies to any cloning strategies) will imply UE in the IT setting, resolving an open question on unclonable encryption since [BL20].

These two theorems establish a clear distinction between USS_1 and USS_d for all d greater than 1. Furthermore, the latter theorem illustrates that as the value of d becomes sufficiently large, it becomes feasible to achieve USS_d within the IT setting. Consequently, it implies that, at the very least, certain objectives outlined in Fig. 1 can be constructed.

Lastly, as the final arrow in Fig. 1, does USS_2 or $\mathsf{USS}_{\omega(\log\lambda)}$ implies UE?

Remark 1 (direction (e) in Fig. 1). We do not have an answer yet. Nonetheless, we assert that either USS_d does not imply UE, or establishing this implication is as challenging as constructing UE. The latter assertion arises from our existing knowledge of $\mathsf{USS}_{\omega(\log\lambda)}$—demonstrating such an implication should, in turn, furnish us with a means to construct UE within the IT framework.

Results on Computational USS. In this computational regime, adversarial parties are computationally bounded; this in turn implies that the amount of pre-shared entanglement is also computationally bounded. Unlike the comprehensive picture presented in Fig. 1, our understanding here is more intricate. Specifically, as demonstrated in Fig. 2, the feasibility or infeasibility hinges on factors such as the computational complexity of USS schemes and the actual quantity of shared entanglement among malicious parties.

Similar to the IT setting, the implication of USS_1 and UE still works (direction (a) in Fig. 2). What is new here is that we present one impossibility result and one infeasibility result on USS_1.

Theorem 5 (Informal, impossibility (f) in Fig. 2, Sect. 6.2). *USS whose reconstruction function has only d T gates, can be attacked with adversarial parties sharing $O(2^d)$ qubits of pre-shared entanglement.*

Therefore, when the reconstruction has low T complexity, say $d = \log\lambda$, then such USS does not exist even in the computational regime. Next, we present a construction, in sharp contrast to the impossibility above. Quantum random oracle [BDF+11], models the perfect (and unrealizable) cryptographic hash function. As it should behave as a truly random function, it can not have a small number of T gates.

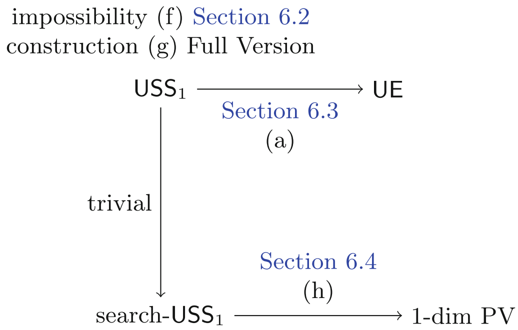

Fig. 2. Relations between USS and UE in the computational regime.

Theorem 6 (construction (g) in Fig. 2, Full Version). *USS that is secure against query-efficient adversarial parties sharing an arbitrary amount of pre-shared entanglement*[2]*, exists in the quantum random oracle model (QROM).*

As quantum random oracle is not realizable in general, we wonder whether USS_1 can be constructed in the plain model. To the end, we show that USS_1 implies a cryptographic primitive called 1-dimensional position verification that is secure against parties sharing any polynomial amount of entanglement. Position verification represents an actively explored research area. Despite all the ongoing efforts, the development of a construction for position verification within the standard model remains elusive. This underscores the formidable challenge of devising USS_1, when relying on computational assumptions.

Theorem 7 (direction (h) in Fig. 2, Sect. 6.4). *USS that is secure against adversarial parties having pre-shared entanglement, implies* 1*-dimensional position verification that is secure against parties sharing the same amount of pre-shared entanglement.*

1.2 Other Related Works

On Secret Sharing of Quantum States. Our work focuses on secret-sharing classical secrets by encoding them into a quantum state to achieve unclonability. One may be curious about the relationship of our new primitive to the existing studies on secret-sharing schemes where the secret messages are *quantum states* to begin with.

In short, all the existing quantum secret sharing schemes fall short of satisfying one crucial property in our model: the requirement of *no or low entanglement* for honest parties. Their unclonability also remains elusive, as they require much more complicated structures on quantum states than ours. We provide a detailed

[2] The adversary is polynomially bounded in queries but not in the pre-shared entanglement.

discussion below and will carefully incorporate all the discussions into the subsequent version.

In the paper, we consider a model where malicious parties can share some amount of entanglement before attacking the protocol. As illustrated in Fig. 1 and Fig. 2, the amount of entanglement (or more precisely, the entanglement graph) plays an important role in both the construction and barriers of such schemes. Therefore, we do not want the entanglement used in honest shares to scale to the same order or surpass what adversaries can access. Our constructions (Theorem 4 and Theorem 6) are based on unentangled quantum shares of single qubits, thus no entanglement required.

[HBB99] first proposed the idea of using quantum states to secret-share a classical bit. Their idea is to use n-qubit GHZ states for an n-out-of-n secret share scheme. However, an n-qubit GHZ state requires entanglement across n quantum registers, which enforces shareholders to maintain entanglement with each other. A subsequent proposal in [KKI99] followed a similar path but also required a large amount of entanglement. The idea of using quantum state to secret share classical secrets was also discussed by Gottesman [Got00], but they mostly focused on the lower bounds of general schemes (potentially requiring entanglement): for example, how many qubits are required to secret-share one classical bit.

There is another line of works on secret-sharing quantum secrets, including [CGL99,Smi00] and most recently [ÇGLR23] by Çakan et al. Since the goal is to secret-share a quantum state, entanglement is also necessary in these protocols.

2 Technical Overview

In this section, unless otherwise specified, we focus on 2-out-of-2 USS, with Share and $\mathsf{Reconstruct}$. Share takes as input a message m and outputs two shares ρ_0, ρ_1; whereas $\mathsf{Reconstruct}$ takes two quantum shares and outputs a string. We assume ρ_0, ρ_1 are unentangled. When we consider impossibility results, all arguments mentioned in this overview carry in the same way to the general cases; for constructions, we only require unentangled shares.

2.1 USS_1 Implies UE, UE Implies USS_2

We first examine two directions (directions (a) and (c) in Figs. 1 and 2); that is, how USS_1 implies UE and how UE implies USS_2. We briefly recall the definition of UE: it is a secret key encryption scheme with the additional property: there is no way to split a quantum ciphertext into two parts, both combining with the classical secret key can recover the original plaintext (with probability at least 1/2 plus negligible).

USS_1 *implies* UE*, Sect.* 6.3. Given a 2-out-of-2 USS, we now design a UE:

$\mathsf{UE.Enc}(k, m)$ takes as input a secret key k and a message,
1. it first produces two shares $(\rho_1, \rho_2) \leftarrow \mathsf{USS.Share}(m)$,

2. it parses $k = (a, b)$, let the unclonable ciphertext be $\mathsf{ct} = (\rho_1, X^a Z^b \rho_2 Z^b X^a)$. In other words, it sends out ρ_1 in clear, while having ρ_2 one-time padded by the key k.

Decryption is straightforward, by unpadding $X^a Z^b \rho_2 Z^b X^a$ and applying Reconstruct to (ρ_1, ρ_2). Correctness and semantic security follows easily. Its unclonability can be based on the unclonability of USS_1; indeed, the scheme corresponds to a special strategy of malicious $\mathcal{P}_1$ and $\mathcal{P}_2$. Suppose there exists an adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ that violates the above scheme, there exists $(\mathcal{P}_1, \mathcal{P}_2, \mathcal{B}, \mathcal{C})$ that violates the security of USS_1.

$\mathcal{P}_1$ and $\mathcal{P}_2$ share EPR pairs. $\mathcal{P}_2$ uses the EPR pairs to teleport ρ_2 to $\mathcal{P}_1$, with $\mathcal{P}_2$ having random (a, b) and $\mathcal{P}_1$ obtaining $(\rho_1, X^a Z^b \rho_2 Z^b X^a)$. As $\mathcal{P}_2$ only has classical information, it sends (a, b) to both $\mathcal{B}$ and $\mathcal{C}$, while $\mathcal{P}_1$ applies $\mathcal{A}$ on $(\rho_1, X^a Z^b \rho_2 Z^b X^a)$ and shares the bipartite state with both $\mathcal{B}$ and $\mathcal{C}$.

It is not hard to see that the above attacking strategy for USS_1 exactly corresponds to an attack in the UE we proposed above: $\mathcal{P}_1$ tries to split a ciphertext while $\mathcal{P}_2$ simply forwards the secret key $k = (a, b)$. Therefore, we can base the unclonability of the UE on that of USS_1, which completes the first direction.

UE *implies* USS_2*, Sect.* 5.2. Recall that 2-out-of-2 USS_2 describes adversarial parties who do not share any entanglement. We can simply set up our USS_2 scheme as follows, using UE:

Share(m) takes as input a message m, it samples a key k for UE, and let $|\mathsf{ct}\rangle$ be the unclonable ciphertext of m under k; the procedure Share outputs the first share as $\rho_1 = k$, and the second share as $\rho_2 = |\mathsf{ct}\rangle$.

As there is no entanglement between $\mathcal{P}_1$ and $\mathcal{P}_2$, $\mathcal{P}_1$ with $\rho_1 = k$ forwards the classical information to both Alice and Bob. In the meantime, $\mathcal{P}_2$ employs her cloning strategy, which remains entirely independent of the key k. Consequently, the unclonability of out USS_2 aligns with that of UE.

When we generalize the conclusion to n-out-of-n USS_2, we first secret share the targeted message m into n shares. For any two adjacent parties $\mathcal{P}_i$, $\mathcal{P}_{i+1}$ and the i-th share, the first part receives the key and the second one gets the unclonable ciphertext. As long as all the malicious parties form at least two connected components (as defined in USS_2), there must be two adjacent parties who do not have entanglement. Thus, we can incur the same logic to prove its unclonability, basing on the unclonability of UE.

2.2 Construction of $\mathsf{USS}_{\omega(\log\lambda)}$

For simplicity, we focus on an n-out-of-n USS, where $n = \omega(\log\lambda)$ and no entanglement is shared between any malicious parties, which is a special case of a general n-out-of-n $\mathsf{USS}_{\omega(\log\lambda)}$, for a larger $n \gg \omega(\log\lambda)$. Our construction is based on the BB84 states. Our scheme first classically secret-shares m into $(n-1)$ shares and encodes each classical share into a single-qubit BB84 state. One party will receive the basis information θ which contains $(n-1)$ basis; every other party will receive a BB84 state for the i-th classical share.

$\mathsf{Share}(m)$: it takes as input a secret $m \in \{0,1\}$,
- it samples $m_1, \cdots, m_{n-1}$ conditioned on their parity equals to m;
- it samples $\theta \in \{0,1\}^{n-1}$;
- let the first $(n-1)$ shares be $\rho_i = H^{\theta_i} |m_i\rangle \langle m_i| H^{\theta_i}$ and the last share $\rho_n = |\theta\rangle\langle\theta|$.

Reconstruction of shares is straightforward. After receiving all shares, one uses the basis information θ to recover all the classical shares m_i; m then is clearly determined by these m_i.

To reason about the unclonability of our protocol, we first recall a theorem on BB84 states, initially proposed by Tomamichel, Fehr, Kaniewski and Wehner [TFKW13] and later adapted in constructing unclonable encryption by Broadbent and Lord [BL20]. We start by considering a cloning game of single-qubit BB84 states.

1. $\mathcal{A}$ receives $H^\theta|x\rangle\langle x|H^\theta$ for uniformly random $x, \theta \in \{0,1\}$, it applies a channel and produces $\sigma_{\mathbf{BC}}$. Bob and Charlie receive their registers accordingly.
2. Bob $\mathcal{B}$ and Charlie $\mathcal{C}$ apply their POVMs and try to recover x; they win if and only if both guess x correctly.

Lemma 1 (Corollary 2 when $n = 1$, [BL20]). *No (unbounded) quantum $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ wins the above game with probability more than 0.855.*

Tomamichel, Fehr, Kaniewski and Wehner [TFKW13] and Broadbent and Lord [BL20] studied parallel repetitions of the above cloning game[3]. In the parallel repetition, n random and independent BB84 states are generated, which encode an n-bit string x. The goal of cloning algorithms is to guess the n-bit string x simultaneously. They showed that the cloning game follows parallel repetition, meaning that the optimal winning probability in an n-fold parallel repetition game is at most $(0.855)^n$.

Our proposed scheme also prepares these BB84 states in parallel, but hides the secret m as the XOR of the longer secret. Indeed, the XOR repetition of the BB84 cloning game has been a folklore and was considered as a candidate for UE. More specifically, it is conjectured that the following game can not be won by any algorithm with probability more than $1/2 + \exp(-\Omega(n))$:

XOR repetition of BB84 cloning games.

1. $\mathcal{A}$ receives $H^\theta|x\rangle\langle x|H^\theta$ for uniformly random $x, \theta \in \{0,1\}^n$, it applies a channel and produces $\sigma_{\mathbf{BC}}$. Bob and Charlie receive their register accordingly.
2. Bob $\mathcal{B}$ and Charlie $\mathcal{C}$ apply their POVMs and try to recover $\mathsf{parity}(x)$; they win if and only if both guess correctly.

Although there is no evidence to disprove the bound for the XOR repetition so far, the validity of the bound still remains unknown. In this work, we prove this

[3] Indeed, [TFKW13] proved a stronger statement on a different game, which ultimately implied the parallel repetition theorem, shown by [BL20].

bound, when $\mathcal{A}$ is restricted to a collection of strategies. It applies $\mathcal{C}_i$ on the i-th qubit of the BB84 state and get $\sigma_{\mathbf{BC}}^{(i)}$; the final state $\sigma_{\mathbf{BC}} = \bigotimes_i \sigma_{\mathbf{BC}}^{(i)}$. Note that the lemma does not put any constraint on the behaviors of $\mathcal{B}$ or $\mathcal{C}$.

Lemma 2 (An XOR lemma for BB84 cloning games, Sect. 5.1). *When $\mathcal{A}$ only applies a tensor cloning strategy to prepare $\sigma_{\mathbf{BC}}$, the optimal success probability in the XOR repetition of BB84 games is $1/2 + \exp(-\Omega(n))$.*

Equipped with it, it is straightforward to show the unclonability of our protocol.

A proof for the XOR repetition. Finally, we give a brief recap on the proof for Lemma 2.

For any $\mathcal{A}$'s tensor strategy with channels $\mathcal{C}_i$ applied on the i-th qubit of a BB84 state, we recall the notation $\sigma_{BC}^{(i)}$. This is the state produced from the i-th qubit of the B884 state, when θ_i, x_i was sampled uniformly at random. Let $\sigma_{\mathbf{B}}^{(i,0)}$ be the density matrix, describing the register that will be given to Bob, when $x_i = 0$. We can similarly define $\sigma_{\mathbf{B}}^{(i,1)}$, $\sigma_{\mathbf{C}}^{(i,0)}$ and $\sigma_{\mathbf{C}}^{(i,1)}$. Lemma 1 tells us that, there exists a constant $c > 0$, either

$$\mathsf{TD}(\sigma_{\mathbf{B}}^{(i,0)}, \sigma_{\mathbf{B}}^{(i,1)}) < c \qquad \text{or} \qquad \mathsf{TD}(\sigma_{\mathbf{C}}^{(i,0)}, \sigma_{\mathbf{C}}^{(i,1)}) < c.$$

This indicates that for every i, either Bob or Charlie can not perfectly tell the value of x_i, regardless of the channel $\mathcal{C}_i$. Furthermore, as the BB84 state has n qubits, w.l.o.g. we can assume that the above holds for Bob, for at least $n/2$ positions.

In the XOR repetition, Bob eventually will receive $\sigma_{\mathbf{B}}^{(i,m_i)}$. We show that Bob can not tell whether the parity of all m_i is odd or even. More precisely, we will show:

$$\mathsf{TD}\left(\sum_{\substack{m_1,\ldots,m_{n-1}: \\ \oplus_i m_i = 0}} \frac{1}{2^{n-2}} \left(\bigotimes_i \sigma_{\mathbf{B}}^{(i,m_i)}\right), \sum_{\substack{m_1,\ldots,m_{n-1}: \\ \oplus_i m_i = 1}} \frac{1}{2^{n-2}} \left(\bigotimes_i \sigma_{\mathbf{B}}^{(i,m_i)}\right)\right) \le c^{n/2}.$$

We connect the trace distance directly to the trace distance of *each pair of states* $\mathsf{TD}(\sigma_{\mathbf{B}}^{(i,0)}, \sigma_{\mathbf{B}}^{(i,1)})$ and demonstrate *an equality* (see Sect. 5.1):

$$\begin{aligned} &\mathsf{TD}\left(\sum_{\substack{m_1,\ldots,m_{n-1}: \\ \oplus_i m_i = 0}} \frac{1}{2^{n-2}} \left(\bigotimes_i \sigma_{\mathbf{B}}^{(i,m_i)}\right), \sum_{\substack{m_1,\ldots,m_{n-1}: \\ \oplus_i m_i = 1}} \frac{1}{2^{n-2}} \left(\bigotimes_i \sigma_{\mathbf{B}}^{(i,m_i)}\right)\right) \\ &= \prod_i \mathsf{TD}\left(\sigma_{\mathbf{B}}^{(i,0)}, \sigma_{\mathbf{B}}^{(i,1)}\right). \end{aligned}$$

Since every trace distance is bounded by 1 and there are at least $n/2$ terms in the product smaller than c, we conclude the result.

2.3 Impossibility of USS_1

Since USS_1 implies UE, it is natural to consider building UE from USS_1. Constructing UE in the basic model remained unresolved since [BL20]. Perhaps the connections in the last section provide a new avenue for constructing UE. In this section, we present two impossibility results (referred to as (b) in Fig. 1 and (f) in Fig. 2) that highlight challenges associated with USS_1.

Information-theoretic USS_1 *does not exist, Sect.* 6.1. We begin by examining the case of 2-out-of-2 USS_1 with unentangled shares, and our impossibility result extends to the general case. Let us consider two malicious parties, $\mathcal{P}_1$ and $\mathcal{P}_2$, who share an unlimited amount of entanglement. $\mathcal{P}_2$ receives the initial share, ρ_2, and teleports it to $\mathcal{P}_1$. This action leaves $\mathcal{P}_2$ with a random one-time pad key, denoted as (a, b) while $\mathcal{P}_1$ now possesses $(\rho_1, X^a Z^b \rho_2 Z^b X^a)$. Now, $\mathcal{P}_1$ aims to jointly apply the reconstruction procedure to (ρ_1, ρ_2), but there's a problem: $\mathcal{P}_1$ lacks all the necessary information, especially the one-time padded key. To address this challenge, we recall the concept of port-based teleportation [IH08, BK11] to help $\mathcal{P}_1$.

Port-based teleportation allows one party to teleport a d-qubit quantum state to another party, while leaving the state in plain. This is certainly impossible without paying any cost, as it contradicts with special relativity. Two parties need to pre-share about $O(d2^d)$ EPR pairs, divided into $O(2^d)$ blocks of d qubits. After the port-based teleportation, the teleported state will be randomly dropped into one of the blocks of $\mathcal{P}_2$, while only $\mathcal{P}_1$ has the classical information about which block consists of the original state.

Equipped with port-based teleportation, $\mathcal{P}_1$ teleports $(\rho_1, X^a Z^b \rho_2 Z^b X^a)$ to $\mathcal{P}_2$; it has the classical information ind specifying the location of the teleported state. $\mathcal{P}_2$ then runs $\mathsf{Reconstruct} \circ (I \otimes Z^b X^a)$ on every possible block among the pre-shared entanglement, yielding $O(2^d)$ different values; even though most of the execution is useless, the ind-th block will store the correct (classical) answer. Finally, both $\mathcal{P}_1$ and $\mathcal{P}_2$ sends all their classical information to Alice and Bob; each of them can independently determine the message. This clearly violates the unclonability of USS_1. Thus, for any 2-out-of-2 USS_1 whose shares are of length d, there is an attacking strategy that takes time and entanglement of order $\tilde{O}(d2^d)$ and completely breaks its unclonability.

We refer readers to Sect. 6.1 for the proof of a general theorem statement.

Impossibility of computationally secure USS_1*, with low-T* $\mathsf{Reconstruct}$*, Sect.* 6.2. We now focus on the case when the reconstruction circuit can be implemented by Clifford gates and logarithmically many T gates. Denote C to be the reconstruction circuit. That is, on input two shares of the form ρ_1, ρ_2, the output is the first bit of $C(\rho_1 \otimes \rho_2)C^\dagger = |m\rangle\langle m| \otimes \tau$.

We let $\mathcal{P}_2$ teleport ρ_2 to $\mathcal{P}_1$ and they try to compute $\mathsf{Reconstruct}$ in a non-local manner. In the previous attack, this is done by leveraging an exponential amount of entanglement. To avoid this and make the attack efficient, we hope that $\mathcal{P}_1$ can homomorphically compute on the one-time padded data $(\rho_1, X^a Z^b \rho_2 Z^b X^a)$, without decrypting it.

Suppose C is a Clifford circuit. We use the fact that the Clifford group is a normalizer for the Pauli group (specifically, the X^aZ^b operator). Let us assume each ρ_1, ρ_2 is of ℓ qubits. In other words, for any $a, b \in \{0,1\}^\ell$ and Clifford circuit C, there exists a polynomial-time computable $a', b' \in \{0,1\}^{2\ell}$ depending only on a, b and C, such that

$$C(\rho_1 \otimes X^a Z^b \rho_2 Z^b X^a)C^\dagger = X^{a'} Z^{b'} C(\rho_1 \otimes \rho_2) C^\dagger Z^{b'} X^{a'}.$$

Here a', b' act as a bigger quantum one-time pad operated on $C(\rho_1 \otimes \rho_2)C^\dagger = |m\rangle\langle m| \otimes \tau$.

Now $\mathcal{P}_1$ measures the first qubit in the computational basis, yielding $m \oplus a'_1$; whereas $\mathcal{P}_2$ compute a', b' (and most importantly, a'_1) from its classical information a, b. They send their knowledge to both Alice and Bob, who later simultaneously recover m.

Next, let us consider the more general case where C consists of Clifford gates and t number of T gates. The homomorphic evaluation of Clifford gates are as before. However, the homomorphic evaluation of T gates are handled differently.

Let us consider one single T gate that applies to the first qubit. We consider two identities, for any $x, z \in \{0,1\}$ and any single-qubit state $|\psi\rangle$

$$(i)\ T(X^x Z^z)|\psi\rangle = (X^x Z^{x \oplus z} P^x) T |\psi\rangle,$$
$$(ii)\ P(X^x Z^z)|\psi\rangle = (X^x Z^{x \oplus z}) P |\psi\rangle$$

Suppose, the current state is of the form $X^x Z^z |\psi\rangle$ and we apply $P^x T$ to the state. We would like to show that the resulting state is $X^{a'} Z^{b'} T |\psi\rangle$ for some $a' \in \{0,1\}, b' \in \{0,1\}$. We use the above identities:

$$(P^x T)(X^x Z^z)|\psi\rangle \overset{\text{From } (i)}{=} P^x (X^x Z^{x \oplus z} P^x) T |\psi\rangle \overset{\text{From } (ii)}{=} X^x Z^{x \oplus z} P^{x \oplus x} T |\psi\rangle.$$

Note that $P^2 = P^0 = I$. Thus, if we can learn x ahead, we can successfully homomorphic compute T on the encrypted data. However, in our case, x corresponds to any bit in the one-time pad key a of any stage. $\mathcal{P}_1$ has no way to learn x. This is where the limitation of low-T gate comes from. Instead of knowing x ahead, each time when a T homomorphic evaluation is needed, one simply guesses x'; as long as $x = x'$ (which happens with probability 1/2), we succeed. Thus, $\mathcal{P}_1$ only guesses all x's (for each T gate) correctly with probability 2^{-t}. If t is logarithmic, our attack violates the security with inverse polynomial probability; therefore, it rules out computationally secure USS_1 with a low-T $\mathsf{Reconstruct}$ procedure.

2.4 Barriers of USS_1 (Implication of PV)

To further demonstrate the challenge of building USS against entangled adversaries, we show that 2-party USS_1 implies a primitive called position verification. Position verification (PV) has remained a vexing problem since its inception [CGMO09].

We briefly introduce the notion of position verification for the 1-dimensional setting: two verifiers on a line will send messages to a prover who claims to be located at a position between the two verifiers. By computing a function of the verifiers' messages and returning the answers to the verifiers in time, the prover ensures them of its location. However, two malicious provers may collude to impersonate such an honest verifier by standing at the two sides of the claimed position.

We demonstrate that 2-party USS_1, even with the weaker search-based security, will imply PV: the two verifiers in the position verification protocol will generate secret shares (ρ_0, ρ_1) of a random string s; then they will each send the messages ρ_0 and ρ_1 respectively to the prover; the prover needs to reconstruct s and send s to both verifiers in time. Any attack against PV can be viewed as a two-stage strategy—one can perfectly turn the first-stage strategy in PV into the shareholders' strategy in USS and the second-stage strategy in PV into the recoverers' strategy in USS.

Despite many efforts, progress on PV in the computational setting against entangled adversaries has unfortunately been slow. We do not even know of any secure computational PV against adversaries with unbounded polynomial amount of entanglement in the plain model, nor any impossibility result. Moreover, some recent advancement in quantum gravity has unveiled some connections between the security of position verification and problems in quantum gravity [May19, May22] .

Any progress of USS_1 in the plain model will contribute towards resolving this long-standing open problem and unveil more implications.

3 Preliminaries

3.1 Notations

We assume that the reader is familiar with the basic background from [NC10]. The Hilbert spaces we are interested in are $\mathbb{C}^d$, for $d \in \mathbb{N}$. We denote the quantum registers with capital bold letters $\mathbf{R}$, $\mathbf{W}$, $\mathbf{X}$, ... We abuse the notation and use registers in place of the Hilbert spaces they represent. The set of all linear mappings from $\mathbf{R}$ to $\mathbf{W}$ is denoted by $L(\mathbf{R}, \mathbf{W})$, and $L(\mathbf{R})$ denotes $L(\mathbf{R}, \mathbf{R})$. We denote unitaries with capital letters C, E, ... and the set of unitaries on register $\mathbf{R}$ with $U(\mathbf{R})$. We denote the identity operator on $\mathbf{R}$ with $\mathbb{I}_{\mathbf{R}}$; if the register $\mathbf{R}$ is clear from the context, we drop the subscript $\mathbf{R}$ from the notation $\mathbb{I}_{\mathbf{R}}$. We denote the set of all positive semi-definite linear mappings in $L(\mathbf{R}, \mathbf{R})$ with trace 1 (i.e., set of all valid quantum states) by $D(\mathbf{R})$. For a register $\mathbf{R}$ in a multi-qubit system, we denote $\overline{\mathbf{R}}$ to be a register consisting of all the qubits in the system not contained in $\mathbf{R}$. We denote $\mathsf{Tr}_{\mathbf{R}}(\rho)$ to be the state obtained by tracing out all the registers of ρ except $\mathbf{R}$. A quantum channel Φ refers to a completely positive and trace-preserving (CPTP) map from a Hilbert space $\mathcal{H}_1$ to a possibly different Hilbert space $\mathcal{H}_2$.

3.2 Unclonable Encryption

Unclonable encryption was originally defined in [BL20] and they considered two security notions, namely search and indistinguishability security, with the latter being stronger than the former. We consider below a mild strengthening of the indistinguishability security due to [AK21].

Definition 1. *An unclonable encryption scheme* UE *is a triple of efficient quantum algorithms* $(\mathsf{UE.KeyGen}, \mathsf{UE.Enc}, \mathsf{UE.Dec})$ *with the following procedures:*

- $\mathsf{KeyGen}(1^\lambda)$*: On input a security parameter* 1^λ*, returns a classical key* sk[4]*.*
- $\mathsf{Enc}(\mathsf{sk}, m)$*: It takes the key* sk *and the message* m *for* $m \in \{0,1\}^{\mathrm{poly}(\lambda)}$ *as input and outputs a quantum ciphertext* ρ_{ct}*.*
- $\mathsf{Dec}(\mathsf{sk}, \rho_{ct})$*: It takes the key* sk *and the quantum ciphertext* ρ_{ct}*, it outputs a quantum state* τ*.*

Correctness. The following must hold for the encryption scheme. For every $\mathsf{sk} \leftarrow \mathsf{KeyGen}(1^\lambda)$ and every message m, we must have $\mathsf{Tr}[|m\rangle\langle m| \mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{sk}, |m\rangle\langle m|))] \geq 1 - \mathsf{negl}(\lambda)$.

Unclonability. In the rest of the work, we focus on unclonable IND-CPA security. The regular IND-CPA security follows directly from its unclonable IND-CPA security. To define unclonable security, we introduce the following security game.

Definition 2 (Unclonable IND-CPA game). *Let* $\lambda \in \mathbb{N}^+$*. Consider the following game against the adversary* $(\mathcal{A}, \mathcal{B}, \mathcal{C})$*.*

- *The adversary* $\mathcal{A}$ *generates* $m_0, m_1 \in \{0,1\}^{n(\lambda)}$ *and sends* (m_0, m_1) *to the challenger.*
- *The challenger randomly chooses a bit* $b \in \{0,1\}$ *and returns* $\mathsf{Enc}(\mathsf{sk}, m_b)$ *to* $\mathcal{A}$*.* $\mathcal{A}$ *produces a quantum state* $\rho_{\mathbf{BC}}$ *on registers* $\mathbf{B}$ *and* $\mathbf{C}$*, and sends the corresponding registers to* $\mathcal{B}$ *and* $\mathcal{C}$*.*
- $\mathcal{B}$ *and* $\mathcal{C}$ *receive the key* sk*, and output bits* $b_\mathcal{B}$ *and* $b_\mathcal{C}$ *respectively.*

The adversary wins if $b_\mathcal{B} = b_\mathcal{C} = b$*.*

We denote the success probability of the above game by $\mathsf{adv}_{\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda)$. We say that the scheme is information-theoretically (resp., computationally) secure if for all (resp., quantum polynomial-time) adversaries $(\mathcal{A}, \mathcal{B}, \mathcal{C})$,

$$\mathsf{adv}_{\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda) \leq 1/2 + \mathsf{negl}(\lambda).$$

4 Definitions and Notations

4.1 Unclonable Secret Sharing

An (t, n)-unclonable secret sharing scheme, associated with n parties $\mathcal{P}_1, \ldots, \mathcal{P}_n$, consists of the following QPT algorithms:

4 In our construction, we require sk being a uniform random string. Such a UE scheme can be constructed in QROM [AKL+22, AKL23].

- $\mathsf{Share}(1^\lambda, 1^n, 1^t, m) \rightarrow \rho_{\mathbf{R}_1\mathbf{R}_2\cdots\mathbf{R}_n}$: On input security parameter λ, n parties, a secret $m \in \{0,1\}^*$, output registers $\mathbf{R}_1, \mathbf{R}_2, \cdots, \mathbf{R}_n$.
- $\mathsf{Reconstruct}(\rho_{\mathbf{R}'_{i_1}}, \ldots, \rho_{\mathbf{R}'_{i_t}})$: On input shares $\mathbf{R}'_{i_1}, \ldots, \mathbf{R}'_{i_t}$, output a secret $\widehat{m}$.

When it is an n-out-of-n USS scheme, we ignore the input 1^t in Share. In the rest of the work, we will focus on constructions with unentangled shares and impossibility results for entangled shared. For sake of clarity, we will use $\rho_1, \cdots, \rho_n$ to denote these shares. We require the following properties to hold.

Correctness. We can recover the secret with probability (almost) 1, more formally:

$$\Pr[\mathsf{Reconstruct}(\rho_{i_1}, \cdots, \rho_{i_k}) = m | (\rho_1, \cdots, \rho_n) \leftarrow \mathsf{Share}(1^\lambda, 1^n, m) \cap k \geq t] = 1 - \mathsf{negl}(\lambda).$$

Soundness/Privacy. Given (at most) $(t-1)$ shares, it is information-theoretically impossible/computationally hard to recover the original message. Formally, for any unbounded/QPT $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\cdot)$, for every $m \in \{0,1\}$, for every $\lambda > 0$, $i_1, \cdots, i_{t-1} \in [n]$,

$$\Pr[\mathcal{A}(\rho_{i_1}, \cdots, \rho_{i_{t-1}}) = m | (\rho_1, \cdots, \rho_n) \leftarrow \mathsf{Share}(1^\lambda, 1^n, m)] = \frac{1}{2} + \mathsf{negl}(\lambda).$$

All our schemes satisfy information-theoretic soundness/privacy.

4.2 Indistinguishability-Based Security

In this work, we will mostly focus on the (n, n)-unclonable secret sharing case. For simplicity, we call it n-party USS.

In this section, we define indistinguishability-based security for n-party USS. The security guarantees that for any two messages m_0, m_1, no two reconstructing parties can simultaneously distinguish between whether the secret is m_0 or m_1, given their sets of respective cloned shares. Formally, we define the following experiment:

$\underline{\mathsf{Expt}_{(\{\mathcal{A}_i\}, \mathcal{B}, \mathcal{C}, \xi)}}$:

1. Let ξ be a quantum state on registers $\mathbf{Aux}_1, \ldots, \mathbf{Aux}_n$. For every $i \in [n]$, $\mathcal{A}_i$ gets the register $\mathbf{Aux}_i$.
2. $\mathsf{Adv} = (\{\mathcal{A}_i\}, \mathcal{B}, \mathcal{C}, \xi)$ sends (m_0, m_1) to the challenger such that $|m_0| = |m_1|$.
3. **Share Phase:** The challenger chooses a bit $b \xleftarrow{\$} \{0,1\}$. It computes $\mathsf{Share}(1^\lambda, 1^n, m_b)$ to obtain $(\rho_1, \ldots, \rho_n)$ and sends ρ_i to $\mathcal{A}_i$.
4. **Challenge Phase:** For every $i \in [n]$, $\mathcal{A}_i$ computes a bipartite state $\sigma_{\mathbf{X}_i\mathbf{Y}_i}$. It sends the register $\mathbf{X}_i$ to $\mathcal{B}$ and $\mathbf{Y}_i$ to $\mathcal{C}$.
5. $\mathcal{B}$ on input the registers $\mathbf{X}_1, \ldots, \mathbf{X}_n$, outputs a bit $b_\mathcal{B}$. $\mathcal{C}$ on input the registers $\mathbf{Y}_1, \ldots, \mathbf{Y}_n$, outputs a bit $b_\mathcal{C}$.
6. Output 1 if $b_\mathcal{B} = b$ and $b_\mathcal{C} = b$.

Definition 3 (Information-theoretic Unclonable Secret Sharing). *An n-party unclonable secret sharing scheme* $(\mathsf{Share}, \mathsf{Reconstruct})$ *satisfies 1-bit unpredictability if for any non-uniform adversary* $\mathsf{Adv} = \left(\{\mathcal{A}_i\}_{i\in[n]}, \mathcal{B}, \mathcal{C}, \xi\right)$*, the following holds:*

$$\Pr\left[1 \leftarrow \mathsf{Expt}_{(\{\mathcal{A}_i\},\mathcal{B},\mathcal{C},\xi)}\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

Definition 4 (Computational Unclonable Secret Sharing). *An n-party unclonable secret sharing scheme* $(\mathsf{Share}, \mathsf{Reconstruct})$ *satisfies 1-bit unpredictability if for any non-uniform quantum polynomial-time adversary* $\mathsf{Adv} = \left(\{\mathcal{A}_i\}_{i\in[n]}, \mathcal{B}, \mathcal{C}, \xi\right)$*, the following holds:*

$$\Pr\left[1 \leftarrow \mathsf{Expt}_{(\{\mathcal{A}_i\},\mathcal{B},\mathcal{C},\xi)}\right] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

Claim. Existence of $(n-1)$-party USS unconditionally implies n-party USS.

This is straightforward to see, by creating a dummy share.

4.3 Entanglement Graph

We will focus on the setting when there are multiple quantum adversaries with shared entanglement modeled as a graph, that we refer to as an *entanglement graph*. We formally define entanglement graphs below.

Definition 5 (Entanglement Graph). *Let ρ be a n-partite quantum state over the registers $\mathbf{X}_1, \cdots, \mathbf{X}_n$. Let $\rho[i]$ be the mixed state over register $\mathbf{X}_i$ (i.e., $\rho[i] = \mathsf{Tr}_{\mathbf{X}_i}(\rho)$) and $\rho[i,j]$ be the mixed state over the registers $\mathbf{X}_i, \mathbf{X}_j$ (i.e., $\rho[i,j] = \mathsf{Tr}_{\mathbf{X}_i,\mathbf{X}_j}(\rho)$). An entanglement graph $G = (V, E)$ associated with $(\rho, \mathbf{X}_1, \ldots, \mathbf{X}_n)$ is defined as follows:*

- *G is an undirected graph;*
- *$V = \{1, 2, \cdots, n\}$;*
- *E contains an edge (u, v) if and only if $\mathbf{X}_u$ and $\mathbf{X}_v$ are entangled; or in other words, there does not exist σ_u, σ_v such that $\rho[u, v] = \sigma_u \otimes \sigma_v$.*

Performing non-local operations on a state ρ, over the registers $\mathbf{X}_1, \ldots, \mathbf{X}_n$, could change the entanglement graph. For instance, performing arbitrary channels on some $\mathbf{X}_i$, could remove some edges associated with the node i; for example, a resetting channel that maps every state to $|0\rangle\langle 0|$. However, on the other hand, performing only unitary operations on each of $\mathbf{X}_1, \ldots, \mathbf{X}_n$ is not going to change the entanglement graph.

Unless otherwise specified, we assume that the amount of entanglement shared between the different parties is either unbounded for information-theoretic protocols, or arbitrarily polynomial for computational protocols.

Definition 6. *Let $\mathcal{P} = (\mathcal{P}_1, \ldots, \mathcal{P}_n)$ be the set of parties with ρ being the state received by all the parties. That is, ρ is an n-partite quantum state over the registers $\mathbf{X}_1, \ldots, \mathbf{X}_n$ such that the party $\mathcal{P}_i$ gets the register $\mathbf{X}_i$. We say that G is the entanglement graph associated with $\mathcal{P}$ if G is the entanglement graph associated with $(\rho, \mathbf{X}_1, \ldots, \mathbf{X}_n)$.*

Definition 7 (USS_d). *We say an information-theoretic/computational unclonable secret sharing scheme is a secure* USS_d *scheme, if it has indistinguishability-based security against all unbounded/efficient adversaries with pre-shared entanglement, whose entanglement graph has* at least d *connect components.*

It is not hard to see that, USS_1 is a USS satisfying the regular indistinguishability security.

5 Adversaries with Disconnected Entanglement Graphs

In this section, we give a construction of unclonable secret sharing with security against quantum adversaries with disconnected entanglement graphs.

5.1 $\mathsf{USS}_{\omega(\log\lambda)}$: an Information-Theoretic Approach

We present an information-theoretic protocol in the setting when there are $\omega(\log\lambda)$ connected components. For simplicity, we consider the case when there are $(n+1)$ parties and the entanglement graph does not have any edges. We demonstrate a construction of USS in this setting, where the security scales with n.

1. $\mathsf{Share}(1^\lambda, 1^{(n+1)}, m \in \{0,1\})$:
   (a) Sample uniformly random $r_1, \ldots, r_n \leftarrow \{0,1\}$ conditioned on $\oplus_i r_i = m$.
   (b) Sample $\theta_1, \ldots, \theta_n \leftarrow \{0,1\}$.
   (c) For each $i \in [n]$: let the i^{th} share be $\rho_i = H^{\theta_i}|r_i\rangle\langle r_i|H^{\theta_i}$. Let the $(n+1)^{th}$ share be $\rho_{n+1} = (\theta_1, \ldots, \theta_n)$.
   (d) Output $(\rho_1, \ldots, \rho_{n+1})$.
2. $\mathsf{Reconstruct}(\rho_1, \ldots, \rho_{n+1})$:
   (a) Measure ρ_{n+1} in the computational basis to get $(\theta_1, \ldots, \theta_n)$.
   (b) For every $i \in [n]$, apply H^{θ_i} to ρ_i. Measure the resulting state in the computational basis to get r_i.
   (c) Output $\oplus_i r_i = m$.

Correctness and Soundness. We refer readers to the full version. Note that the soundness only holds for $n = \Omega(\log n)$, i.e., the protocol should have at least $\Omega(\log n)$ shares.

Security. Consider the adversary to be $\mathsf{Adv} = (\{\mathcal{A}_i\}, \mathcal{B}, \mathcal{C}, \xi)$, where ξ is a product state. Henceforth, we omit mentioning $\xi = \xi_1 \otimes \cdots \otimes \xi_{n+1}$, where $\mathcal{A}_i$ receives ξ_i, since we can think of ξ_i to be part of the description of $\mathcal{A}_i$.

For $b \in \{0,1\}$, let $(\rho_1^{r_1}, \ldots, \rho_n^{r_n}, \rho_{n+1}) \leftarrow \mathsf{Share}(1^\lambda, 1^{(n+1)}, b)$, where $\oplus_i r_i = b$ and $\rho_i = H^{\theta_i}|r_i\rangle\langle r_i|H^{\theta_i}$ and $\rho_{n+1} = |\theta_1 \cdots \theta_n\rangle\langle\theta_1 \cdots \theta_n|$. Suppose upon receiving $\rho_i^{r_i}$, $\mathcal{A}_i$ sends registers $\{\mathbf{X}_i^{r_i}\}$ and $\{\mathbf{Y}_i^{r_i}\}$ respectively to $\mathcal{B}$ and $\mathcal{C}$. We denote the reduced density matrix on $\mathbf{X}_i^{r_i}$ to be $\sigma_i^{r_i}$ and on $\mathbf{Y}_i^{r_i}$ to be $\zeta_i^{r_i}$. We assume without loss of generality that ρ_{n+1} is given to both $\mathcal{B}$ and $\mathcal{C}$ since it is a computational basis state.

Define $\mathcal{S}_{\mathcal{B}}$ and $\mathcal{S}_{\mathcal{C}}$ as follows:

$$\mathcal{S}_{\mathcal{B}} = \left\{ i \in [n] \ : \mathsf{TD}\left(\sigma_i^0, \sigma_i^1\right) \leq 0.86 \right\}$$
$$\mathcal{S}_{\mathcal{C}} = \left\{ i \in [n] \ : \mathsf{TD}\left(\zeta_i^0, \zeta_i^1\right) \leq 0.86 \right\}$$

We prove the following claims.

Claim. Either $|\mathcal{S}_{\mathcal{B}}| \geq \lceil \frac{n}{2} \rceil$ or $|\mathcal{S}_{\mathcal{C}}| \geq \lceil \frac{n}{2} \rceil$.

Proof. We prove by contradiction; suppose it is not the case. Then there exists an index $i \in [n]$ such that $i \notin \mathcal{S}_{\mathcal{B}}$ and $i \notin \mathcal{S}_{\mathcal{C}}$. That is, $\mathsf{TD}\left(\sigma_i^0, \sigma_i^1\right) > 0.86$ and $\mathsf{TD}\left(\zeta_i^0, \zeta_i^1\right) > 0.86$, meaning the optimal state distinguishing circuit can distinguish σ_i^0, σ_i^1 with probability at least $0.93 = (1 + 0.86)/2$. Similarly, the optimal distinguishing probability for states ζ_i^0, ζ_i^1 is at least 0.93.

Using this, we design an adversary that violates the unclonable security of single-qubit BB84 states [BL20, Corollary 2]. Let us first recall the security game for the unclonability of single-qubit BB84 states:

1. $\mathcal{A}$ receives $H^\theta|x\rangle\langle x|H^\theta$ for uniformly random $x, \theta \in \{0, 1\}$, it applies a channel and produces $\sigma_{\mathbf{BC}}$. Bob and Charlie receive their register accordingly.
2. Bob $\mathcal{B}$ and Charlie $\mathcal{C}$ apply their POVMs and try to recover x; they win if and only if both guess x correctly.

Lemma 3 (Corollary 2 when $\lambda = 1$, [BL20]). *No (unbounded) quantum $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ wins the game with probability more than 0.855.*

We design an adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ as follows, with winning probability $0.86 > 0.855$, a contradiction.

- $\mathcal{A}$ receives as input an unknown BB84 state. It runs $\mathcal{A}_i$ on the state to obtain a bipartite state, which it shares with $\mathcal{B}$ and $\mathcal{C}$.
- $\mathcal{B}$ and $\mathcal{C}$ in the security game of BB84 state will receive θ_i from the challenger.
- $\mathcal{B}$ runs the optimal distinguisher distinguishing σ_i^0 and σ_i^1. Based on the output of the distinguisher, it outputs its best guess of the challenge bit. Similarly, Charlie runs the optimal distinguisher distinguishing ζ_i^0 and ζ_i^1. It outputs its best guess of the challenge bit.

By a union bound, the probability that one of $\mathcal{B}$ or $\mathcal{C}$ fails is at most $0.14 = 0.07 \times 2$. Thus, they simultaneously succeed with probability at least 0.86, a contradiction.

Claim. The following holds:

1.

$$\mathsf{TD}\left(\sum_{\substack{r_1,\dots,r_n: \\ \oplus_i r_i = 0}} \frac{1}{2^{n-1}} \left(\bigotimes_i \sigma_i^{r_i} \right), \sum_{\substack{r_1,\dots,r_n: \\ \oplus_i r_i = 1}} \frac{1}{2^{n-1}} \left(\bigotimes_i \sigma_i^{r_i} \right) \right) \leq 0.86^{|\mathcal{S}_{\mathcal{B}}|}$$

2.

$$\mathsf{TD}\left(\sum_{\substack{r_1,\ldots,r_n:\\ \oplus_i r_i=0}} \frac{1}{2^{n-1}}\left(\bigotimes_i \zeta_i^{r_i}\right), \sum_{\substack{r_1,\ldots,r_n:\\ \oplus_i r_i=1}} \frac{1}{2^{n-1}}\left(\bigotimes_i \zeta_i^{r_i}\right)\right) \leq 0.86^{|\mathcal{S}_\mathcal{C}|}$$

Proof. We prove bullet 1 since bullet 2 follows symmetrically.

$$\begin{aligned}
&\mathsf{TD}\left(\sum_{\substack{r_1,\ldots,r_n:\\ \oplus_i r_i=0}} \frac{1}{2^{n-1}}\left(\bigotimes_i \sigma_i^{r_i}\right), \sum_{\substack{r_1,\ldots,r_n:\\ \oplus_i r_i=1}} \frac{1}{2^{n-1}}\left(\bigotimes_i \sigma_i^{r_i}\right)\right)\\
&= \frac{1}{2}\left\|\sum_{\substack{r_1,\ldots,r_n:\\ \oplus_i r_i=0}} \frac{1}{2^{n-1}}\left(\bigotimes_i \sigma_i^{r_i}\right) - \sum_{\substack{r_1,\ldots,r_n:\\ \oplus_i r_i=1}} \frac{1}{2^{n-1}}\left(\bigotimes_i \sigma_i^{r_i}\right)\right\|_1\\
&= \left\|\bigotimes_i \frac{\left(\sigma_i^0 - \sigma_i^1\right)}{2}\right\|_1\\
&= \prod_i \left\|\frac{\left(\sigma_i^0 - \sigma_i^1\right)}{2}\right\|_1\\
&\leq \prod_{i\in\mathcal{S}_\mathcal{B}} \mathsf{TD}\left(\sigma_i^0, \sigma_i^1\right)\\
&\leq 0.86^{|\mathcal{S}_\mathcal{B}|}
\end{aligned}$$

Here $\|\cdot\|_1$ denotes the trace norm. In the above proof, we use the fact that $\|\bigotimes_i \tau_i\|_1 = \prod_i \|\tau_i\|_1$.

Lemma 4. *The above USS scheme satisfies indistinguishability security against any adversaries with no shared entanglement; i.e., it is a secure* USS_n *scheme (see Definition 7) with* $n = \omega(\log\lambda)$.

Proof. From Sect. 5.1, either $|\mathcal{S}_\mathcal{B}| \geq \lceil \frac{n}{2} \rceil$ or $|\mathcal{S}_\mathcal{C}| \geq \lceil \frac{n}{2} \rceil$. We will assume without loss of generality that $|\mathcal{S}_\mathcal{B}| \geq \lceil \frac{n}{2} \rceil$. From bullet 1 of Sect. 5.1, it holds that $\mathcal{B}$ can successfully distinguish whether it is in the experiment when the challenge bit 0 was used or when the challenge bit 1 was used, with probability at most $\frac{1+\nu(n)}{2}$, for some exponentially small function ν in n. Thus, both $\mathcal{B}$ and $\mathcal{C}$ can only simultaneously distinguish with probability at most $\frac{1+\nu(n)}{2}$. This completes the proof. □

5.2 USS_d, for $d \geq 2$: from Unclonable Encryption

We present a construction of USS with security against quantum adversaries associated with *any* disconnected entanglement graph. In the construction, we use an information-theoretically secure unclonable encryption scheme, $\mathsf{UE} = (\mathsf{UE.KeyGen}, \mathsf{UE.Enc}, \mathsf{UE.Dec})$. The resulting USS scheme is consequently information-theoretically secure.

1. $\mathsf{Share}(1^\lambda, 1^n, m)$:
   (a) Sample $r_1, \cdots, r_n \leftarrow \{0,1\}^{|m|}$.
   (b) For each $i \in [n]$, let $y_i = r_i$; let $y_n = m \oplus \sum_{i=1}^{n} r_i$.
   (c) For each $i \in [n]$:
      (a) Compute $\mathsf{sk}_i \leftarrow \mathsf{UE.KeyGen}(1^\lambda)$. We denote the length of sk_i to be $\ell = \ell(\lambda)$.
      (b) Compute $|\mathsf{ct}_i\rangle \leftarrow \mathsf{UE.Enc}(\mathsf{sk}_i, y_i)$
   (d) For each $i \in [n]$: let each share $\rho_i = (\mathsf{sk}_{i-1}, |\mathsf{ct}_i\rangle)$; here we define $\mathsf{sk}_0 = \mathsf{sk}_n$.
   (e) Output $(\rho_1, \cdots, \rho_n)$
2. $\mathsf{Reconstruct}(\rho_1, \cdots, \rho_n)$:
   (a) For each $i \in [n]$,
      i. Parse ρ_i as $(\mathsf{sk}_{i-1}, |\mathsf{ct}_i\rangle)$. We define $\mathsf{sk}_n = \mathsf{sk}_0$.
      ii. Compute $y_i \leftarrow \mathsf{UE.Dec}(\mathsf{sk}_i, |\mathsf{ct}_i\rangle)$
   (b) Output $m = \sum_{i=1}^{n} y_i$.

Theorem 8. *The above scheme satisfies indistinguishability-based security against adversaries with any disconnected entanglement graph. More precisely, it is a secure* USS_2 *scheme (see Definition 7).*

Proof. The correctness of the scheme follows from the correctness of UE decryption.

We now prove the security of the above scheme. Suppose we have an USS adversary $(\mathcal{A} = (\mathcal{A}_1, \cdots, \mathcal{A}_n), \mathcal{B}, \mathcal{C}, \xi)$ who succeeds with probability $\frac{1}{2} + \varepsilon$ in Definition 7, we construct an UE adversary $(\mathcal{A}', \mathcal{B}', \mathcal{C}')$ who succeeds with probability $\frac{1}{2} + \varepsilon$ in Definition 2.

Let $\mathcal{A}$ receive as input an n-partite state ξ over the registers $\mathbf{Aux}_1, \ldots, \mathbf{Aux}_n$ such that $\mathcal{A}_i$ receives as input the register $\mathbf{Aux}_i$. Additionally, without loss of generality, we can assume that $\mathcal{A}$ also receives as input the challenge messages (m_0, m_1), where $|m_0| = |m_1|$. Let $G = (V, E)$ be the entanglement graph associated with $(\xi, \mathbf{Aux}_1, \ldots, \mathbf{Aux}_n)$, where, $V = \{1, \ldots, n\}$. Since G is disconnected, there exists $i^* \in [n]$ such that $(i^*, i^* + 1) \notin E$. Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two subgraphs of G such that $V_1 \cup V_2 = V$, $V_1 \cap V_2 = \emptyset$, $i^* \in V_1$, $i^* + 1 \in V_2$. Moreover, G_1 and G_2 are disconnected with each other. This further means that ξ can be written as $\xi_{G_1} \otimes \xi_{G_2}$, for some states ξ_{G_1}, ξ_{G_2}, such that ξ_{G_1} is over the registers $\{\mathbf{Aux}_i\}_{i \in V_1}$ and ξ_{G_2} is over the registers $\{\mathbf{Aux}_i\}_{i \in V_2}$.

We describe $(\mathcal{A}', \mathcal{B}', \mathcal{C}')$ as follows:

Description of $\mathcal{A}'$. Fix $i^*, (m_0, m_1)$ (as defined above). Upon receiving a quantum state $|\mathsf{ct}^*\rangle$ $\mathcal{A}'$ does the following:

– It prepares quantum states $\xi_{G_1}, (\xi_{G_2})^{\otimes 2^\ell}$.
– It samples $r_i \xleftarrow{\$} \{0,1\}^{|m_0|}$, where $i \in [n]$, subject to the constraint that $\oplus_i r_i = m_0$.
– It submits $(r_{i^*}, r_{i^*} \oplus m_0 \oplus m_1)$ to the UE challenger and in return, it receives $|\mathsf{ct}^*\rangle$. It sets $|\mathsf{ct}_{i^*+1}\rangle = |\mathsf{ct}^*\rangle$.
– For every $i \in [n]$, generate $\mathsf{sk}_i \leftarrow \mathsf{UE.KeyGen}(1^\lambda)$; let $\mathsf{sk}_{n+1} = \mathsf{sk}_1$.

- For every $i \in [n]$ and $i \neq i^*$, generate $|\mathsf{ct}_i\rangle \leftarrow \mathsf{UE.Enc}(\mathsf{sk}_i, \mathsf{sh}_i)$.
- For every $i \in [n]$ and $i \neq i^* + 1$, define $\rho_i = (\mathsf{sk}_{i-1}, |\mathsf{ct}_i\rangle)$.
- We need to define $\rho_{i^*+1} = (\mathsf{sk}_{i^*}, |\mathsf{ct}_{i^*+1}\rangle)$. However, as sk_{i^*} will only be received by $\mathcal{B}'$ and $\mathcal{C}'$ in the UE security game later, we will enumerate all possible values of sk_{i^*} and the corresponding computation result in the subgraph G_2.
  - For every $x \in \{0,1\}^\ell$ (possible value of sk_{i^*}), compute $\{\mathcal{A}_i\}_{i \in V_2}$ on $\{\rho_i\}_{i \in V_2}$, ξ_{G_2} to obtain two sets of registers $\{\mathbf{X}_i^{(x)}\}_{i \in G_2}$ and $\{\mathbf{Y}_i^{(x)}\}_{i \in G_2}$.
- Compute $\{\mathcal{A}_i\}_{i \in V_1}$ on $\{\rho_i\}_{i \in V_1}$ and ξ_{G_1} to obtain two sets of registers $\{\mathbf{X}_i\}_{i \in G_1}$ and $\{\mathbf{Y}_i\}_{i \in G_1}$.
- Send the registers $\{\mathbf{X}_i\}_{i \in G_1}$ and $\{\mathbf{X}_i^{(x)}\}_{i \in G_2, x \in \{0,1\}^\lambda}$ to $\mathcal{B}'$. Send the registers $\{\mathbf{Y}_i\}_{i \in G_1}$ and $\{\mathbf{Y}_i^{(x)}\}_{i \in G_2, x \in \{0,1\}^\lambda}$ to $\mathcal{C}'$.

Description of $\mathcal{B}'$ and $\mathcal{C}'$. $\mathcal{B}'$ upon receiving the secret key k (which is sk_{i^*}), computes $\mathcal{B}$ on $\{\mathbf{X}_i\}_{i \in G_1}$ and $\{\mathbf{X}_i^{(k)}\}_{i \in G_2}$ to obtain a bit $b_{\mathcal{B}}$. $\mathcal{C}'$ is defined similarly. We denote the output of $\mathcal{C}'$ to be $b_{\mathcal{C}}$.

If the challenger of the UE security chooses the bit $b = 0$, then $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ in the above reduction are receiving shares of m_0; otherwise, they are receiving shares of m_1. Thus, the success probability of $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ in Definition 7 is precisely the same as the success probability of $(\mathcal{A}', \mathcal{B}', \mathcal{C}')$ in Definition 2. □

6 Impossibilities and Barriers

In this section, we present two impossibility results on USS. Furthermore, we present two implications of USS: namely, unclonable encryption and position verification secure against large amount of entanglement. Since no construction known for the latter two primitives, this further underscores the formidable barriers of building USS.

6.1 Impossibility in the Information-Theoretic Setting

Theorem 9. *Let $\mathcal{P}$ be a set of parties. Information-theoretically secure* USS *for $\mathcal{P}$ is impossible if the entanglement graph for $\mathcal{P}$ is connected and in particular, there is an edge from P_1 to everyone else.*

Proof. The attack strategy is as follows. The n parties $P_1, \cdots, P_n$ pre-share a large amount of entanglement with one another. In the protocol, each P_i receives its share ρ_i.

- *Regular Teleportation Stage*: all parties P_i, where $i \neq 1$ teleport their shares to party P_1 via regular teleportation. Each P_i obtains a measurement outcome (a_i, b_i).
- Now P_1 holds a state in the following format: $(\mathbb{I} \otimes X^{a_2} Z^{b_2} \otimes \cdots X^{a_n} \ Z^{b_n}) |\Psi\rangle_{P_1 P_2 \cdots P_n}$ which can be represented as mixed states $(\rho_1, X^{a_2} Z^{b_2} \rho_2 X^{a_2} Z^{b_2}, \cdots, X^{a_n} Z^{b_n} \rho_n X^{a_n} Z^{b_n})$. That is, quantum one-time padded shares from all other parties and its own share in the clear.

– *Port-Based Teleportation Stage*:
  - P_1 performs port-based teleportation for the state $(\mathbb{I} \otimes X^{a_2}Z^{b_2} \otimes \cdots X^{a_n}Z^{b_n}) |\Psi\rangle_{P_1P_2\cdots P_n}$ to P_2. P_1 obtains a measurement outcome that stands for some index i_1. Recall that by the guarantee of port-based teleportation, the index i_1 specifies the register of P_2 that holds the above state in the clear, *without any Pauli errors on top.*
  - P_2 will now remove the quantum one time pad information X^{a_2}, Z^{a_2} on its share in the teleported state above. Since P_2 does not have information about i_1, it simply performs $\mathbb{I} \otimes Z^{a_2}X^{a_2} \otimes \mathbb{I} \cdots \otimes \mathbb{I}$ on all exponentially many possible registers that it may receive the teleported state from P_1.
  - Next P_2 performs port-based teleportation with P_3 for *all registers that could possibly hold the state* $(\mathbb{I} \otimes \mathbb{I} \otimes X^{a_3}Z^{b_3} \otimes \cdots \otimes X^{a_n}Z^{b_n}) |\Psi\rangle_{P_1P_2\cdots P_n}$. Thus, P_2 obtains an exponential number of indices about the registers that will receive the teleported states on P_3's hands.
  - P_3 accordingly, applies $\mathbb{I} \otimes \mathbb{I} \otimes Z^{b_3}X^{a_3} \cdots \mathbb{I}$ on all the possible registers that can hold the teleported state; performs a port-based teleportation to P_4 with all of these registers and obtains a measurement outcome that has a doubly-exponential number of indices[5].
  - $\cdots$
  - Finally, P_n receives the teleported states from P_{n-1} and performs $\mathbb{I} \otimes \cdots \mathbb{I} \otimes Z^{b_n}X^{a_n}$ on all of them. One of these registers will hold the state $|\Psi\rangle_{P_1\cdots P_n} = (\rho_1, \cdots, \rho_n)$ in the clear. Then P_n performs the reconstruction algorithm on all of these registers to obtain a large number of possible outcomes. One of them will hold the correctly reconstructed secret s.

– *Reconstruction Stage*: now P_n sends all its measurement outcomes to both Bob and Charlie. All other P_i's send their indices information measured in the port teleportation protocol. Bob and Charlie can therefore find the correct index in P_n's measurement outcomes that holds s, by following a path of indices.

□

Remark 2. The above strategy can be easily converted into a strategy where the underlying entanglement graph is connected (but may not be a complete graph) and every pair of connected parties share (unbounded) entanglement. The similar idea applies by performing regular teleportation and port-based teleportation via any DFS order of the graph. Thus, we have the following theorem.

Theorem 10. *Let $\mathcal{P}$ be a set of parties. Information-theoretically secure* USS *for $\mathcal{P}$ is impossible if the entanglement graph for $\mathcal{P}$ is connected.*

6.2 Impossibility with Low T-gates for Efficient Adversaries

Our impossibility result above in the information-theoretic setting requires exponential amount of entanglement between the parties. We also present an attack

[5] For $P_i, 2 \leq i < n$, the measurement outcome will have its size grow in an exponential tower of height i.

that can be performed by efficient adversaries, albeit on USS schemes with restricted reconstruction algorithms.

We would like to mention that a similar result has already been shown in [Spe15] in the context of instantaneous non-local computation; we rediscovered the following simple attack for unclonable secret sharing. We also extend the attack to an n-party setting whereas [Spe15] considers only 2 parties.

Theorem 11. *Let $\mathcal{P}$ be a set of parties and if the entanglement graph for $\mathcal{P}$ is connected, then there exists an attack using polynomial-time and polynomial amount of entanglement on any* USS *scheme where the procedure* $\mathsf{Reconstruct}$ *consists of only Clifford gates and $O(\log \lambda)$ number of* T *gates.*

We refer readers to the full version for the proof.

6.3 USS Implies Unclonable Encryption

Theorem 12. *Unclonable secret sharing with IND-based security against adversaries with (bounded) polynomial amount of shared entanglement and connected pre-shared entanglement graph implies secure unclonable encryption.*

We will first look at the 2-party case, which can be easily extended to the $n(> 2)$-party case.

Proof. Assume a secure $\mathsf{USS} = (\mathsf{USS.Share}, \mathsf{USS.Reconstruct})$ with IND-based security, we construct the following UE scheme:

1. $\mathsf{KeyGen}(1^\lambda, 1^{|m|})$: samples a random $\mathsf{sk} \leftarrow \{0,1\}^{2\ell}$, where $\ell = \ell(\lambda)$ is the number of qubits in each share generated by $\mathsf{USS.Share}(1^\lambda, 1^{|m|}, \cdot)$. Output sk.
2. $\mathsf{Enc}(\mathsf{sk}, m)$:
   (a) compute $(\rho_1, \rho_2) \leftarrow \mathsf{USS.Share}(1^\lambda, 1^{|m|}, m)$.
   (b) sample random $(a, b) \leftarrow \{0,1\}^{2\ell}$. Use them to quantum one-time pad the second share ρ_2 to obtain $\mathsf{X}^a\mathsf{Z}^b\rho_2\mathsf{Z}^b\mathsf{X}^a$.
   (c) compute $s \leftarrow (a, b) \oplus \mathsf{sk}$
   (d) Output $\mathsf{ct} = (\rho_1, \mathsf{X}^a\mathsf{Z}^b\rho_2\mathsf{Z}^b\mathsf{X}^a, s)$.
3. $\mathsf{Dec}(\mathsf{ct}, \mathsf{sk})$:
   (a) parse $\mathsf{ct} = (\rho_1, \rho_2', s)$;
   (b) compute $(a, b) \leftarrow s \oplus \mathsf{sk}$;
   (c) output $m \leftarrow \mathsf{USS.Reconstruct}(\rho_1, \mathsf{X}^a\mathsf{Z}^b\rho_2'\mathsf{Z}^b\mathsf{X}^a)$.

Correctness. The correctness easily follows from the correctness of the underlying USS scheme.

Security. Suppose we have UE adversaries $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ that wins in the IND-based UE security game, we can construct adversary $(\mathcal{A}' = (\mathcal{A}_1, \mathcal{A}_2), \mathcal{B}', \mathcal{C}')$ for the USS IND-based security.

Before receiving the shares from the challenger, $\mathcal{A}_1$ and $\mathcal{A}_2$ agrees on a random strong $r \leftarrow \{0,1\}^{2\ell}$. When receiving the shares, $\mathcal{A}_2$ teleports its share ρ_2 to $\mathcal{A}_1$ and obtains Pauli errors (a, b).

$\mathcal{A}_1$ gives $(\rho_1, , r)$ the UE adversary $\mathcal{A}$. $\mathcal{A}_2$ computes $\mathsf{sk}' \leftarrow (a, b) \oplus r$.

In the USS challenge phase, $\mathcal{A}_2$ sends sk' to both $\mathcal{B}'$ and $\mathcal{C}'$. The UE adversaries $\mathcal{A}$ has finished giving the bipartite it generated from (ρ_1, r) state $\sigma_{\mathcal{B},\mathcal{C}}$ to $\mathcal{B}$ and $\mathcal{C}$.

Then $\mathcal{B}'$ feeds $\mathcal{B}$ with sk' as the secret key in the UE security game (and $\mathcal{C}'$ feeding sk' to $\mathcal{C}$,respectively), and outputs their output bit $b_{\mathcal{B}}, b_{\mathcal{C}}$ as the answer to USS game. Since the classical part in the unclonable ciphertext is the classical information (a, b) masked by a uniformly random sk, the reduction perfectly simulates the above scheme by first giving the UE adversary $\mathcal{A}$ a uniformly random string r and later feeding $\mathcal{B}, \mathcal{C}$ with $r \oplus (a, b)$.

Extending to n-party case. We can change the scheme to sample a longer $\mathsf{sk} \in \{0,1\}^{2(n-1)\ell}$ and let the unclonable ciphertext be $(\rho_1, \mathsf{X}^{a_2}\mathsf{Z}^{b_2}\rho_2\mathsf{Z}^{b_2}\mathsf{X}^{a_2}, \cdots, \mathsf{X}^{a_n}\mathsf{Z}^{b_n}\rho_n\mathsf{Z}^{b_n}\mathsf{X}^{a_n}, s = (a_1, b_1, \cdots, a_n, b_n) \oplus \mathsf{sk})$.

In the reduction, when receiving the shares, $\mathcal{A}_i, i \neq 1$ teleports its share ρ_i to $\mathcal{A}_1$ and obtains Pauli errors (a_i, b_i). The rest of the reduction follows easily.

□

Theorem 13. *Unclonable secret sharing with IND-based security against adversaries with disconnected entanglement graph, where one of the parties receives as a share a quantum state and all other parties receive classical shares (in other words, computational basis states), implies secure unclonable encryption.*

Proof. In the case where only one party has a quantum share, the others classical shares, we can easily modify the above construction to have a UE scheme from USS:

1. $\mathsf{KeyGen}(1^\lambda, 1^{|m|})$: samples a random $\mathsf{sk} \leftarrow \{0,1\}^{(n-1)\ell}$, where $\ell = \ell(\lambda)$ is the number of qubits/bits in each share generated by $\mathsf{USS.Share}(1^\lambda, 1^{|m|}, \cdot)$. Output sk.
2. $\mathsf{Enc}(\mathsf{sk}, m)$:
   (a) compute $(\rho_1, y_2, \cdots, y_n) \leftarrow \mathsf{USS.Share}(1^\lambda, 1^{|m|}, m)$. $y_1, \cdots, y_n$ are binary strings.
   (b) sample random $\mathsf{sk} \leftarrow \{0,1\}^{(n-1)\ell}$. Compute $s \leftarrow (y_1, \cdots, y_n) \oplus \mathsf{sk}$
   (c) Output $\mathsf{ct} = (\rho_1, s)$.
3. $\mathsf{Dec}(\mathsf{ct}, \mathsf{sk})$:
   (a) parse $\mathsf{ct} = (\rho_1, s)$;
   (b) compute $(y_1, \cdots, y_n) \leftarrow s \oplus \mathsf{sk}$;
   (c) output $m \leftarrow \mathsf{USS.Reconstruct}(\rho_1, y_1, \cdots, y_n)$.

Security. Suppose we have an UE adversary $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ that wins in the IND-based UE security game with probability $\frac{1}{2} + \varepsilon$, we construct an adversary $(\mathcal{A}' = (\mathcal{A}_1, \cdots \mathcal{A}_n), \mathcal{B}', \mathcal{C}')$ that wins in the USS IND-based security game with probability $\frac{1}{2} + \varepsilon$. Thus, if the USS scheme is secure then ε has to be negligible. We describe $\mathcal{A}_1, \cdots, \mathcal{A}_n$ as follows.

Before receiving the shares from the challenger, $\mathcal{A}_1, \cdots, \mathcal{A}_n$ agrees on a random string $r \leftarrow \{0,1\}^{(n-1)\ell}$.

$\mathcal{A}_1$ gives (ρ_1, r) to the UE adversary $\mathcal{A}$. $\mathcal{A}_i$, for $i \neq 1$, when receiving the classical share y_i from the challenger, computes $\mathsf{sk}'_i \leftarrow y_i \oplus r_i$, where r_i is the $(i-1)$-th block of length-ℓ string in r.

In the USS challenge phase, each $\mathcal{A}_i$, for $i \neq 1$, sends sk'_i to both $\mathcal{B}'$ and $\mathcal{C}'$. $\mathcal{A}_1$ sends the bipartite state $\sigma_{\mathcal{B},\mathcal{C}}$ to $\mathcal{B}'$ and $\mathcal{C}'$, where $\sigma_{\mathcal{B},\mathcal{C}}$ is the output of $\mathcal{A}$.

Then $\mathcal{B}'$ feeds $\mathcal{B}$ with $\mathsf{sk}' = (\mathsf{sk}'_2, \cdots, \mathsf{sk}'_n)$ as the secret key in the UE security game (and $\mathcal{C}'$ feeding sk' to $\mathcal{C}$, respectively), and outputs their output bit $b_{\mathcal{B}}, b_{\mathcal{C}}$ as the answer to USS game. Since the classical part in the unclonable ciphertext is the classical information $(y_2, \cdots, y_n)$ masked by a uniformly random sk, the reduction perfectly simulates the above scheme by first giving the UE adversary $\mathcal{A}$ a uniformly random string r and later feeding $\mathcal{B}, \mathcal{C}$ with $r \oplus (y_2, \cdots, y_n)$. Thus, the advantage of $(\mathcal{A}', \mathcal{B}', \mathcal{C}')$ in breaking the USS security game is precisely the same as the advantage of $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ breaking the UE security game.

6.4 Search-Based USS Implies Position Verification

The definition of quantum position verification is in the full version.

QPV with Pre-shared Entanglement. In QPV, we also consider different adversarial setup such as: (1) (P_0, P_1) do not have pre-shared entanglement; (2) (P_0, P_1) can share a bounded/unbounded polynomial amount of entanglement; (3) (P_0, P_1) can share unbounded amount of entanglement. We also divide the settings into computational and information-theoretic.

Theorem 14. *2-party* USS*(computational/IT resp.) with search-based security implies 1-dimensional QPV (computational/IT, resp.), where the two adversarial provers in the QPV protocol pre-share the same amount of entanglement as the two parties in the* USS *protocol do.*

The following theorem demonstrates from another point of view the barrier of constructing secure protocols against entangled adversaries for USS in the IT setting. Even if we consider computational assumptions, the development in building secure QPV protocols against entangled adversaries has been slow, which indicates further evidence on how challenging USS can be in the entangled setting.

Theorem 15 ([BK11, BCF+14]). *Quantum position verification is impossible in the information theoretic setting if we allow the adversaries to preshare entanglement.*

We leave the proof to the full version.

References

[Aar09] Scott Aaronson. "Quantum copy-protection and quantum money". In: *2009 24th Annual IEEE Conference on Computational Complexity*. IEEE. 2009, pp. 229–242 (cit. on p. 3).

[AC12] Scott Aaronson and Paul Christiano. *Quantum Money from Hidden Subspaces*. 2012. DOI: https://doi.org/10.48550/ARXIV.1203.4740. URL: https://arxiv.org/abs/1203.4740 (cit. on p. 3).

[AK21] Prabhanjan Ananth and Fatih Kaleoglu. "Unclonable Encryption, Revisited". In: *Theory of Cryptography Conference*. Springer. 2021, pp. 299–329 (cit. on pp. 3, 15).

[AKL+22] Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. "On the feasibility of unclonable encryption, and more". In: *Annual International Cryptology Conference*. Springer. 2022, pp. 212–241 (cit. on pp. 3, 15).

[AKL23] Prabhanjan Ananth, Fatih Kaleoglu, and Qipeng Liu. "Cloning Games: A General Framework for Unclonable Primitives". In: *Annual International Cryptology Conference*. Springer. 2023, pp. 66–98 (cit. on pp. 3, 15).

[AL20] Prabhanjan Ananth and Rolando L. La Placa. *Secure Software Leasing*. 2020. DOI: https://doi.org/10.48550/ARXIV.2005.05289. URL: https://arxiv.org/abs/2005.05289 (cit. on p. 3).

[BB20] Charles H Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *arXiv preprint* arXiv:2003.06557 (2020) (cit. on pp. 3, 6).

[BCF+14] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. "Position-based quantum cryptography: Impossibility and constructions". In: *SIAM Journal on Computing* 43.1 (2014), pp. 150–178 (cit. on p. 27).

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. "Random oracles in a quantum world". In: *International conference on the theory and application of cryptology and information security*. Springer. 2011, pp. 41–69 (cit. on p. 6).

[BK11] Salman Beigi and Robert König. "Simplified instantaneous nonlocal quantum computation with applications to position-based cryptography". In: *New Journal of Physics* 13.9 (2011), p. 093036 (cit. on pp. 3, 12, 27).

[BL20] Anne Broadbent and Sébastien Lord. "Uncloneable Quantum Encryption via Oracles". en. In: Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. DOI: https://doi.org/10.4230/LIPICS.TQC.2020.4. URL: https://drops.dagstuhl.de/opus/volltexte/2020/12063/ (cit. on pp. 3, 6, 10, 12, 15, 19).

[BS16] Shalev Ben-David and Or Sattath. *Quantum Tokens for Digital Signatures*. 2016. DOI: https://doi.org/10.48550/ARXIV.1609.09047. URL: https://arxiv.org/abs/1609.09047 (cit. on p. 3).

[CGL99] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. In: *Phys. Rev. Lett.* 83 (3 July 1999), pp. 648–651. DOI: https://doi.org/10.1103/PhysRevLett.83.648. URL: https://link.aps.org/doi/10.1103/PhysRevLett.83.648 (cit. on p. 8).

[ÇGLR23] Alper Çakan, Vipul Goyal, Chen-Da Liu-Zhang, and João Ribeiro. "Computational Quantum Secret Sharing". In: *arXiv preprint* arXiv:2305.00356 (2023) (cit. on p. 8).

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. "Position based cryptography". In: *Annual International Cryptology Conference*. Springer. 2009, pp. 391–407 (cit. on p. 14).

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. "Hidden Cosets and Applications to Unclonable Cryptography". In: *Advances in Cryptology – CRYPTO 2021*. Ed. by Tal Malkin and Chris Peikert. Cham: Springer International Publishing, 2021, pp. 556–584. ISBN: 978-3-030-84242-0 (cit. on p. 3).

[GC19] Alvin Gonzales and Eric Chitambar. "Bounds on instantaneous nonlocal quantum computation". In: *IEEE Transactions on Information Theory* 66.5 (2019), pp. 2951–2963 (cit. on p. 3).

[Got00] Daniel Gottesman. "Theory of quantum secret sharing". In: *Physical Review* A 61.4 (2000), p. 042311 (cit. on p. 8).

[Got02] Daniel Gottesman. "Uncloneable Encryption". In: (2002). DOI: https://doi.org/10.48550/ARXIV.QUANT-PH/0210062. URL: https://arxiv.org/abs/quant-ph/0210062 (cit. on p. 3).

[GSS21] Vipul Goyal, Yifan Song, and Akshayaram Srinivasan. "Traceable secret sharing and applications". In: *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part III 41*. Springer. 2021, pp. 718–747 (cit. on p. 2).

[HBB99] Mark Hillery, Vladimír Bu žek, and André Berthiaume. In: *Phys. Rev. A* 59 (3 Mar. 1999), pp. 1829–1834. DOI: https://doi.org/10.1103/PhysRevA.59.1829. URL: https://link.aps.org/doi/10.1103/PhysRevA.59.1829 (cit. on p. 8).

[IH08] Satoshi Ishizaka and Tohya Hiroshima. "Asymptotic teleportation scheme as a universal programmable quantum processor". In: *Physical review letters* 101.24 (2008), p. 240501 (cit. on pp. 3, 12).

[KKI99] Anders Karlsson, Masato Koashi, and Nobuyuki Imoto. "Quantum entanglement for secret sharing and secret splitting". In: *Phys. Rev. A* 59 (1 Jan. 1999), pp. 162–168. DOI: https://doi.org/10.1103/PhysRevA.59.162. URL: https://link.aps.org/doi/10.1103/PhysRevA.59.162 (cit. on p. 8).

[LMZ23] Jiahui Liu, Hart Montgomery, and Mark Zhandry. "Another Round of Breaking and Making Quantum Money: How to Not Build It from Lattices, and More". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2023, pp. 611–638 (cit. on p. 3).

[May19] Alex May. "Quantum tasks in holography". In: *Journal of High Energy Physics* 2019.10 (2019), pp. 1–39 (cit. on pp. 3, 14).

[May22] Alex May. "Complexity and entanglement in non-local computation and holography". In: *Quantum* 6 (2022), p. 864 (cit. on pp. 3, 14).

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010 (cit. on p. 14).

[Shm22] Omri Shmueli. "Public-key Quantum money with a classical bank". In: *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*. 2022, pp. 790–803 (cit. on p. 3).

[Smi00] Adam D Smith. "Quantum secret sharing for general access structures". In: *arXiv preprint quant-ph/0001087* (2000) (cit. on p. 8).

[Spe15] Florian Speelman. "Instantaneous non-local computation of low T-depth quantum circuits". In: *arXiv preprint* arXiv:1511.02839 (2015) (cit. on pp. 3, 24).

[TFKW13] Marco Tomamichel, Serge Fehr, Jê drzej Kaniewski, and Stephanie Wehner. "A monogamy-of-entanglement game with applications to device-independent quantum cryptography". In: *New Journal of Physics* 15.10 (Oct. 2013), p. 103002. DOI: https://doi.org/10.1088/1367-2630/15/10/103002. URL: https://doi.org/10.1088%2F1367-2630%2F15%2F10%2F103002 (cit. on pp. 6, 10).

[Vai03] Lev Vaidman. "Instantaneous measurement of nonlocal variables". In: *Physical review letters* 90.1 (2003), p. 010402 (cit. on p. 3).

[Zha17] Mark Zhandry. "Quantum Lightning Never Strikes the Same State Twice". In: *CoRR* abs/1711.02276 (2017). arXiv: 1711.02276. URL: http://arxiv.org/abs/1711.02276 (cit. on p. 3).