Split-State Non-Malleable Codes and Secret Sharing Schemes for Quantum Messages[*]

Naresh Goud Boddu[†]   Vipul Goyal[‡]   Rahul Jain[§]   João Ribeiro[¶]

Abstract

Non-malleable codes are fundamental objects at the intersection of cryptography and coding theory. These codes provide security guarantees even in settings where error correction and detection are impossible, and have found applications to several other cryptographic tasks. One of the strongest and most well-studied adversarial tampering models is 2-split-state tampering. Here, a codeword is split into two parts which are stored in physically distant servers, and the adversary can then independently tamper with each part using arbitrary functions. This model can be naturally extended to the secret sharing setting with several parties by having the adversary independently tamper with each share. Previous works on non-malleable coding and secret sharing in the split-state tampering model only considered the encoding of *classical* messages. Furthermore, until recent work by Aggarwal, Boddu, and Jain (IEEE Trans. Inf. Theory 2024 & arXiv 2022), adversaries with quantum capabilities and *shared entanglement* had not been considered, and it is a priori not clear whether previous schemes remain secure in this model.

In this work, we introduce the notions of split-state non-malleable codes and secret sharing schemes for quantum messages secure against quantum adversaries with shared entanglement. Then, we present explicit constructions of such schemes that achieve low-error non-malleability. More precisely, we construct efficiently encodable and decodable split-state non-malleable codes and secret sharing schemes for quantum messages preserving entanglement with external systems and achieving security against quantum adversaries having shared entanglement with codeword length n, any message length at most $n^{\Omega(1)}$, and error $\varepsilon = 2^{-n^{\Omega(1)}}$. In the easier setting of *average-case* non-malleability, we achieve efficient non-malleable coding with rate close to $1/11$.

[†]NTT Research, `naresh.boddu@ntt-research.com`.

[‡]Carnegie Mellon University and NTT Research, `vipul@vipulgoyal.org`.

[§]Centre for Quantum Technologies and Department of Computer Science, National University of Singapore and MajuLab, UMI 3654, Singapore, `rahul@comp.nus.edu.sg`.

[¶]NOVA LINCS and NOVA School of Science and Technology, `joao.ribeiro@fct.unl.pt`.

Contents

1   Introduction

Non-Malleable Codes (NMCs), introduced in the work of Dziembowski, Pietrzak, and Wichs [DPW18], are now considered fundamental cryptographic primitives that provide security guarantees even in adversarial settings where error correction and detection are impossible. Informally, NMCs guarantee that an adversary cannot change the encoding of a message into that of a related message. They encode a classical message M into a codeword C in such a way that tampering C into $f(C)$ using an allowed tampering function f results in the decoder either outputting the original message M or a message that is unrelated/independent of M. Note that it is impossible to construct NMCs that protect against *arbitrary* tampering functions. This is because an adversary could simply apply the decoder to C, recovering the message M, and then output the encoding of a related message $M + 1$ as the tampered version of C. Therefore, previous work on non-malleable coding has focused on constructing NMCs for restricted, but still large and meaningful, classes of tampering functions.

One of the strongest and most studied tampering models is *split-state tampering*, introduced by Liu and Lysyanskaya [LL12]. In the 2-state version of this model (which is the hardest), we view a codeword C as being composed of two parts, E_1 and E_2, and an adversary is allowed to *independently* tamper with each part using an arbitrary tampering function. In other words, a split-state tampering adversary consists of a pair of arbitrary functions (f, g), and a codeword (E_1, E_2) is tampered to $(f(E_1), g(E_2))$ (see Figure 1 for a diagram of this model). The split-state model is meaningful because we can imagine that the two parts of the codeword are stored in different physically isolated servers, making communication between tampering adversaries infeasible.

The notion of non-malleable secret sharing has also been widely studied as a strengthening of non-malleable codes. Secret sharing, dating back to the work of Blakley [Bla79] and Shamir [Sha79], is a fundamental cryptographic primitive where a dealer encodes a secret into p shares and distributes them among p parties. Each secret sharing scheme has an associated *monotone*[1] set $\Gamma \subseteq 2^{[p]}$, usually called an *access structure*, whereby any set of parties $T \in \Gamma$, called *authorized* sets, can reconstruct the secret from their shares, but any *unauthorized* set of parties $T \notin \Gamma$ gains essentially no information about the secret. One of the most natural and well-studied types of access structures are *threshold* access structures, where a set of parties T is authorized if and only if $|T| \geq t$ for some threshold t.

Non-Malleable Secret Sharing (NMSS), generalizing non-malleable coding, was introduced by Goyal and Kumar [GK18a] and has received significant interest in the past few years in the classical setting. NMSS schemes additionally guarantee that an adversary who is allowed to tamper all the shares (according to some restricted tampering model) cannot make an authorized set of parties reconstruct a different but related secret. Non-malleable secret sharing is particularly well-studied in the context of the split-state tampering model described above, whereby an adversary can independently tamper with each share. Once again, the motivation is that shares are being held in physically distant devices, making communication between the several tampering adversaries infeasible.

The split-state and closely related tampering models for codes and secret sharing schemes have witnessed a flurry of work in the past decade [LL12, DKO13, CG16, CG14, ADL18, CGL20, Li15, Li17, GK18a, GK18b, ADN+19, BS19, FV19, Li19, AO20, BFO+20, BFV21, GSZ21, AKO+22, CKOS22, Li23], culminating in recent explicit constructions of classical split-state NMCs of rate

---

[1]A set $\Gamma \subseteq 2^{[p]}$ is *monotone* if $A \in \Gamma$ and $A \subseteq B$ imply that $B \in \Gamma$.

1/3 [AKO+22] and constructions with a smaller constant rate but also smaller error [Li23] (with a known upper bound on the rate being 1/2 [CG16]). Split-state NMCs and NMSS schemes and related notions have also found applications in other cryptographic tasks, such as non-malleable commitments, secure message transmission, and non-malleable signatures [GPR16, GK18a, GK18b, ADN+19, SV19, CKOS22].

Split-state tampering and quantum computing. Given the rapid development of quantum technologies, it is natural to consider NMCs and NMSS schemes in the quantum setting and examine how adversaries with quantum capabilities affect previous assumptions made about tampering models. For instance, all known NMCs are tailored to classical messages, but it is equally important to design non-malleable coding schemes that allow us to encode quantum states as well. Moreover, the possibility of attackers with quantum capabilities challenges the *independence assumption* made in the split-state models described earlier. Although servers holding different parts of the codeword (or different secret shares) may be physically isolated from each other, the tampering adversaries attacking each server may have pre-shared a large amount of entangled quantum states. Access to such shared entanglement can provide non-trivial advantages to these adversaries beyond what has been considered in the classical tampering models. For example, in the Clauser-Horne-Shimony-Holt (CHSH) game [CHSH69], non-communicating parties can use local measurements on both halves of an EPR state to achieve a higher success probability than what is possible using fully classical strategies. Therefore, it is not clear whether any of the existing classical NMCs and NMSS schemes remain secure in the augmented split-state tampering models where the adversary is allowed to make use of arbitrary shared entanglement across multiple states (see Figure 2 for a diagram of the split-state tampering model for two states). The only exception to this are the recent work of Aggarwal, Boddu, and Jain [ABJ24] and the concurrent work of Batra, Boddu, and Jain [BBJ23]. The former constructs explicit NMCs for *classical* messages that are secure in the 2-split-state tampering model, while the latter focuses on explicit quantum-secure *non-malleable randomness encoders* (NMRE) with a higher rate in the same tampering model, and uses these objects to non-malleable codes in the 3-split-state model[2] for quantum messages.

The shortcomings of existing split-state non-malleable coding schemes in the face of quantum messages and adversaries raise the following natural question:

> Can we design efficient 2-split-state NMCs and split-state NMSS schemes for *quantum messages* secure against quantum adversaries with shared entanglement?

We resolve this question in the affirmative.

1.1 Our contributions

1.1.1 Split-state non-malleable codes for quantum messages

As our first contribution, we propose a definition of split-state non-malleability for quantum messages against adversaries with shared entanglement. Our definition is a natural extension of the one considered for classical messages in the literature [DPW18]. Here, we present it specifically for the 2-split-state case, which is our main setting of interest.

Let σ_M be an arbitrary state in a message register M, and $\sigma_{M\hat{M}}$ be its canonical purification. We consider a (2-split-state) coding schemes given by an encoding Completely Positive Trace-Preserving

---

[2]Meaning that the codeword is divided into three parts and the adversary tampers each part independently.
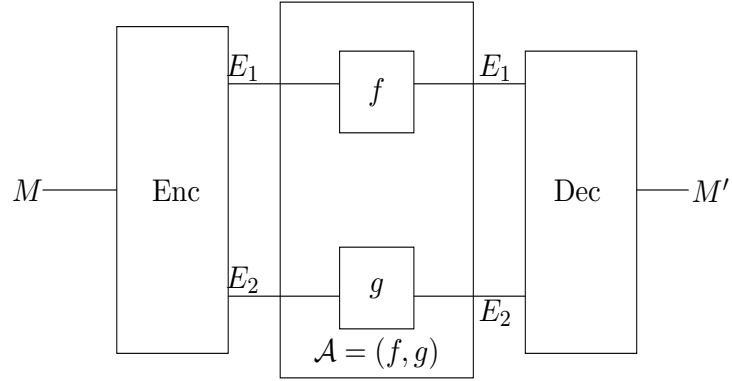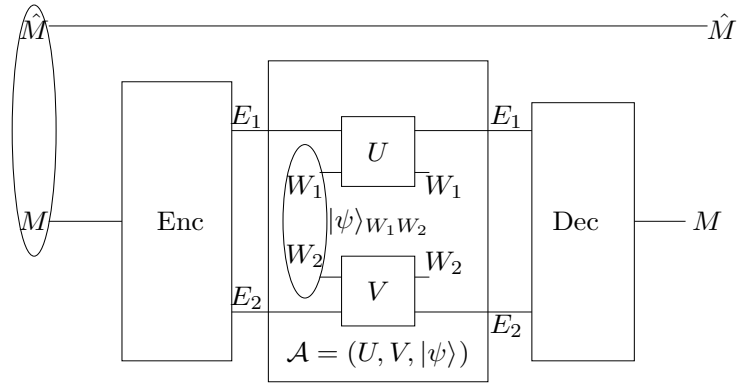
Figure 1: Classical split-state tampering model.

Figure 2: Split-state tampering model with shared entanglement. This shared entanglement is stored in registers W_1 and W_2.

(CPTP) map $\mathrm{Enc} : \mathcal{L}(\mathcal{H}_M) \to \mathcal{L}(\mathcal{H}_{E_1} \otimes \mathcal{H}_{E_2})$ and a decoding CPTP map $\mathrm{Dec} : \mathcal{L}(\mathcal{H}_{E_1} \otimes \mathcal{H}_{E_2}) \to \mathcal{L}(\mathcal{H}_M)$, where $\mathcal{L}(\mathcal{H})$ is the space of all linear operators in the Hilbert space $\mathcal{H}$.

The most basic property we require of this coding scheme $(\mathrm{Enc}, \mathrm{Dec})$ is correctness (which includes preserving entanglement with external systems), i.e.,

$$\mathrm{Dec}(\mathrm{Enc}(\sigma_{M\hat{M}})) = \sigma_{M\hat{M}},$$

where we use the shorthand T to represent the CPTP map $T \otimes \mathbb{I}$ whenever the action of the identity operator $\mathbb{I}$ is clear from context.

Before we proceed to define split-state non-malleability, we describe the split-state adversarial tampering model in the quantum setting. Let $\rho_{E_1 E_2} = \mathrm{Enc}(\sigma_M)$ be the split-state encoding of message σ_M. A split-state tampering adversary $\mathcal{A}$ is specified by two tampering maps[3] $U : \mathcal{L}(\mathcal{H}_{E_1} \otimes \mathcal{H}_{W_1}) \to \mathcal{L}(\mathcal{H}_{E_1} \otimes \mathcal{H}_{W_1})$ and $V : \mathcal{L}(\mathcal{H}_{E_2} \otimes \mathcal{H}_{W_2}) \to \mathcal{L}(\mathcal{H}_{E_2} \otimes \mathcal{H}_{W_2})$ along with a quantum state $|\psi\rangle_{W_1 W_2}$ that captures the shared entanglement between the non-communicating tampering adversaries. Finally, the decoding procedure Dec is applied to the tampered codeword. Figure 2 presents a diagram of this tampering model. Let

$$\eta = \mathrm{Dec}\left((U \otimes V)\left(\mathrm{Enc}(\sigma_{M\hat{M}}) \otimes |\psi\rangle\langle\psi|\right)(U^\dagger \otimes V^\dagger)\right)$$

be the final state after applying the split-state tampering adversary $\mathcal{A}$ followed by the decoding procedure.

We are now ready to define split-state non-malleability of the coding scheme $(\mathrm{Enc}, \mathrm{Dec})$.

Definition 1 (Worst-case and average-case non-malleable codes for quantum messages)**.** *We say that the coding scheme* $(\mathrm{Enc}, \mathrm{Dec})$ *is a (worst-case)* ε*-non-malleable code for quantum messages if for every split-state adversary* $\mathcal{A} = (U, V, |\psi\rangle_{W_1 W_2})$ *and every quantum message* σ_M *(with canonical purification* $\sigma_{M\hat{M}}$*) it holds that*

$$\eta_{M\hat{M}} \approx_\varepsilon p_{\mathcal{A}} \sigma_{M\hat{M}} + (1 - p_{\mathcal{A}}) \gamma_M^{\mathcal{A}} \otimes \sigma_{\hat{M}}, \tag{1}$$

where $p_{\mathcal{A}} \in [0, 1]$ *and* $\gamma_M^{\mathcal{A}}$ *depend only*[4] *on the split-state adversary* $\mathcal{A}$*, and* $\approx_\varepsilon$ *denotes that the two states are* ε*-close in trace distance.*

If Equation (1) is only guaranteed to hold when σ_M *is the maximally mixed state, then we say that* $(\mathrm{Enc}, \mathrm{Dec})$ *is an* average-case ε*-non-malleable code for quantum messages.*

Remark 1. Intuitively, our definition of average-case non-malleability for quantum messages in Definition 1 is analogous to requiring that the *average* non-malleability error of a given classical code is small when averaged over a uniformly random message. Later, in Lemma 9, we show that every average-case non-malleable code for quantum messages is also a worst-case non-malleable code, though with a larger error.

---

[3]Tampering maps are assumed to be unitary without any loss of generality. This is because, in the presence of unbounded arbitrary shared entanglement, tampering with unitary maps is equivalent to tampering with CPTP maps. More precisely, consider a tampering adversary that uses two CPTP maps Φ_1 and Φ_2 acting on registers $E_1 W_1$ and $E_2 W_2$, respectively. Then, the action of this adversary is equivalent to another adversary who tampers using Stinespring isometry extensions U and V of Φ_1 and Φ_2, respectively, which act on $E_1 W_1 A_1$ and $E_2 W_2 A_2$, respectively, where A_1 and A_2 are unentangled ancilla registers set to $|0\rangle$ without loss of generality and can be seen as part of the shared entanglement.

[4]By this, we mean that $p_{\mathcal{A}}$ can be computed and the state $\gamma_M^{\mathcal{A}}$ can be prepared without the knowledge of the input message $\sigma_{M\hat{M}}$.

Definition 1 can be readily extended to encompass arbitrary classes of tampering adversaries. However, for the sake of readability, we do not provide the generalization here. In the context of split-state tampering, we present the following two results.

Our first result gives an explicit average-case 2-split-state NMC for quantum messages with rate arbitrarily close to $1/11$.

Theorem 1 (Average-case 2-split-state NMC for quantum messages with constant rate). *For any fixed constant $\delta > 0$ there exist an integer $n_0 > 0$ and $c \in (0,1)$ such that the following holds: There exists a family of coding schemes $(\mathcal{C}_n)_{n \in \mathbb{N}}$ where each $\mathcal{C}_n$ has codeword length n and message length $\lfloor \left(\frac{1}{11} - \delta\right) n \rfloor$ such that C_n is average-case ε-non-malleable for quantum messages with error $\varepsilon = 2^{-n^c}$ for all integers $n \geq n_0$. Furthermore, there exist encoding and decoding procedures for the family $(\mathcal{C}_n)_{n \in \mathbb{N}}$ running in time $\mathrm{poly}(n)$.*

Our second result, which builds on Theorem 1, gives an explicit construction of a worst-case 2-split-state NMC for quantum messages.

Theorem 2 (Worst-case 2-split-state NMC for quantum messages). *There exist constants $c \in (0,1)$ and $n_0 \in \mathbb{N}$ such that the following holds: There exists a family of coding schemes $(\mathcal{C}_n)_{n \in \mathbb{N}}$ where each $\mathcal{C}_n$ has codeword length n and message length $\lfloor n^c \rfloor$ such that $\mathcal{C}_n$ is ε-non-malleable for quantum messages with error $\varepsilon = 2^{-n^c}$ for all integers $n \geq n_0$. Furthermore, there exist encoding and decoding procedures for the family $(\mathcal{C}_n)_{n \in \mathbb{N}}$ running in time $\mathrm{poly}(n)$.*

In fact, we show something stronger: The explicit code from Theorem 2 is actually a 2-out-of-2 non-malleable secret sharing scheme for quantum messages with share size n, any message of length at most $n^{\Omega(1)}$, and error $\varepsilon = 2^{-n^{\Omega(1)}}$. We refer the reader to Section 1.1.2 for more details on non-malleable secret sharing.

1.1.2 Split-state non-malleable secret sharing schemes for quantum messages

We begin by defining threshold non-malleable secret sharing schemes for quantum messages. This is an extension of our definition of 2-split-state non-malleable codes in Section 1.1.1, and it is analogous to the definition in the classical setting [GK18a]. We focus on threshold schemes for simplicity, but the definition can be easily generalized to other access structures.

Let σ_M be an arbitrary state in a message register M, and $\sigma_{M\hat{M}}$ be its canonical purification. An NMSS scheme for p parties is composed of two CPTP maps (nmShare, nmRec). nmShare is a sharing procedure $\mathrm{nmShare} : \mathcal{L}(\mathcal{H}_M) \to \mathcal{L}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2} \otimes \cdots \otimes \mathcal{H}_{S_p})$, where S_i is the share register for the i-th party, and nmRec is a reconstruction procedure $\mathrm{nmRec} : \mathcal{L}(\bigotimes_{i \in T} \mathcal{H}_{S_i}) \to \mathcal{L}(\mathcal{H}_M)$, where $\mathcal{L}(\mathcal{H})$ is the space of all linear operators in the Hilbert space $\mathcal{H}$. The reconstruction procedure nmRec acts on any authorized subset of shares T to reconstruct the original message.

Before we proceed to define non-malleability, we describe the adversarial tampering model for secret sharing. This is a simple extension of the 2-split-state tampering model described in Section 1.1.1. Fix an authorized subset T of parties. A tampering adversary $\mathcal{A}_T$ is specified by $|T|$ tampering maps[5] $U_i : \mathcal{L}(\mathcal{H}_{S_i} \otimes \mathcal{H}_{W_i}) \to \mathcal{L}(\mathcal{H}_{S_i} \otimes \mathcal{H}_{W_i})$ for $i \in T$ along with a quantum state $|\psi\rangle_{W_1 W_2 \ldots W_p}$ which captures the shared entanglement between non-communicating local tampering

---

[5]Tampering maps are assumed to be unitary without any loss of generality.

adversaries. We denote the overall tampered state by $\tau^{\mathcal{A}_T}$, which may be written as

$$\tau^{\mathcal{A}_T} = \left(\left(\bigotimes_{i \in T} U_i \right) \otimes \left(\bigotimes_{j \notin T} \mathbb{I} \right) \right) \left(\mathrm{nmShare}(\sigma_{M\hat{M}}) \otimes |\psi\rangle\langle\psi|_{W_1 W_2 \dots W_p} \right) \left(\left(\bigotimes_{i \in T} U_i^\dagger \right) \otimes \left(\bigotimes_{j \notin T} \mathbb{I} \right) \right).$$

Let the final state of the tampering experiment be

$$\eta = \mathrm{nmRec}\left(\tau_{S_T}^{\mathcal{A}_T} \right).$$

We are now ready to define split-state NMSS schemes, in a similar manner to Definition 1 for split-state NMCs.

Definition 2 (Threshold non-malleable secret sharing scheme for quantum messages)**.** *The coding scheme* $(\mathrm{nmShare}, \mathrm{nmRec})$ *is said to be a* t-out-of-p $(\varepsilon_{\mathsf{priv}}, \varepsilon_{\mathsf{nm}})$*-non-malleable secret sharing scheme for quantum messages if for any quantum message* $\sigma_M \in \mathcal{D}(\mathcal{H}_M)$ *(with canonical purification* $\sigma_{M\hat{M}}$*) the following properties are satisfied:*

- ***Correctness:*** *For any* $T \subseteq [p]$ *such that* $|T| \geq t$ *it holds that*

$$\mathrm{nmRec}(\mathrm{nmShare}(\sigma_{M\hat{M}})_{S_T}) = \sigma_{M\hat{M}},$$

  where we write $S_T = (S_i)_{i \in T}$*.*

- ***Statistical privacy:*** *For any* $T \subseteq [p]$ *such that* $|T| \leq t-1$ *it holds that*

$$\mathrm{nmShare}(\sigma)_{\hat{M}S_T} \approx_{\varepsilon_{\mathsf{priv}}} \sigma_{\hat{M}} \otimes \zeta_{S_T},$$

  where ζ_{S_T} *is a fixed quantum state independent of* $\sigma_{M\hat{M}}$*.*

- ***Non-malleability:*** *For any* $T \subseteq [p]$ *such that* $|T| = t$*, it holds that*

$$\eta_{M\hat{M}} \approx_{\varepsilon_{\mathsf{nm}}} p_{\mathcal{A}_T} \sigma_{M\hat{M}} + (1 - p_{\mathcal{A}_T}) \gamma_M^{\mathcal{A}_T} \otimes \sigma_{\hat{M}}, \tag{2}$$

  where $p_{\mathcal{A}_T} \in [0, 1]$ *and* $\gamma_M^{\mathcal{A}_T}$ *depend only[6] on the threshold tampering adversary* $\mathcal{A}_T$*, and* $\approx_\varepsilon$ *denotes that the two states are* ε*-close in trace distance.*

  If Equation (2) is only guaranteed to hold when σ_M *is the maximally mixed state, then we say that* $(\mathrm{nmShare}, \mathrm{nmRec})$ *is an* average-case t-out-of-p $(\varepsilon_{\mathsf{priv}}, \varepsilon_{\mathsf{nm}})$-non-malleable secret sharing scheme for quantum messages.*

As our main result in this direction, which builds on Theorem 2, we construct efficient split-state NMSS schemes for quantum messages realizing more general threshold access structures with low privacy and non-malleability errors.

Theorem 3 (Split-state threshold NMSS schemes for quantum messages)**.** *There exist constants* $c, C > 0$ *and an integer* $n_0 \in \mathbb{N}$ *such that the following holds for any number of parties* p *and threshold* $t \geq 3$ *such that* $t \leq p \leq 2t - 1$ *and for any* $n \geq n_0$*: There exists a family of* t-out-of-p $(\varepsilon_{\mathsf{priv}} = \varepsilon, \varepsilon_{\mathsf{nm}} = \varepsilon)$-non-malleable secret sharing schemes for quantum messages with shares of size at most* $(pn)^C$*, message length* $\lfloor n^c \rfloor$*, and error* $\varepsilon = 2^{-n^c}$*. Furthermore, the sharing and reconstruction procedures of this scheme can be computed in time polynomial in* p *and* n*.*

---

[6]By this, we mean that $p_{\mathcal{A}_T}$ can be computed and the state $\gamma_M^{\mathcal{A}_T}$ can be prepared without the knowledge of the input message $\sigma_{M\hat{M}}$.

Combined with our previously discussed 2-out-of-2 non-malleable secret sharing scheme for quantum messages, Theorem 3 covers all remaining threshold access structures for which secret sharing is possible in the quantum setting (i.e., those which do not violate no-cloning) except 2-out-of-3. We leave constructing a 2-out-of-3 non-malleable secret sharing scheme for quantum messages as a very interesting open problem.

Finally, an analogous realization of the approach behind Theorem 3 using the same techniques allows us to obtain *classical* threshold non-malleable secret sharing schemes secure against quantum adversaries with shared entanglement. See Section 4.7 for more details, including a formal result.

1.2 Other related work

In this section, we discuss relevant prior work on classical NMCs and on quantum non-malleability beyond what we covered above.

Classical NMCs. The first work on NMCs by Dziembowski, Pietrzak, and Wichs [DPW18] showed that, surprisingly, there exists a (possibly inefficient) NMC against any family of at most $2^{2^{\alpha n}}$ tampering functions, where $\alpha < 1$ is an arbitrary constant, and n is the message length. The best possible rate of (possibly inefficient) NMCs was studied by Cheraghchi and Guruswami [CG16], who showed that split-state NMCs can have a rate of at most $1/2$. To complement the above, [DPW18] constructed efficient NMCs in the *bitwise tampering model*, a strictly weaker model than split-state tampering, where each bit of the codeword is tampered independently. As discussed before, this spurred a deep line of work which recently culminated in explicit constructions of constant-rate NMCs in the split-state model [AO20, AKO+22].

Several works have also studied NMCs against computationally-bounded adversaries from various hardness assumptions and setups, such as a common reference string. Naturally, in such restricted settings, it is possible to achieve a better rate while allowing the adversary to perform many adaptive tamperings in a row. Computationally-restricted tampering models include polynomial-time algorithms [FMNV14], split-state polynomial-time adversaries [AAG+16], bounded-depth circuits [BDKM16, BDKM18, BFMV22], low-degree polynomials [BCL+20], decision trees [BDKM18, BGW19], and streaming space-bounded algorithms [FHMV17, BDKM18]. Some other works have studied constructions of short NMCs based on conjectured properties of practical block ciphers [FKM18, BFRV22] or extractable hash functions [KLT16].

We note that existing works in these settings only consider classical messages and adversaries.

Classical NMSS schemes. The notion of non-malleable secret sharing first appeared implicitly in the work of Aggarwal, Dziembowski, Kazana, and Obremski [ADKO15], where it was shown that every classical 2-split-state NMC is also a 2-out-of-2 secret sharing scheme with statistical privacy. NMSS schemes were then studied explicitly and in much greater generality by Goyal and Kumar [GK18a, GK18b], leading to a long line of research on classical split-state non-malleable secret sharing, as mentioned above.

Classical NMSS schemes have also been studied in tampering models beyond split-state tampering. For example, the original works of Goyal and Kumar [GK18a, GK18b] also consider a "joint" tampering model where, under certain restrictions, tampering adversaries may tamper with *subsets* of multiple shares, instead of only a single share. Stronger joint tampering models have been considered in the computational [BFO+20] and information-theoretic settings [GSZ21].

In an orthogonal direction, other notions of non-malleability where the adversary learns the reconstruction of tampered secrets with respect to multiple authorized subsets of parties have also been studied [ADN+19, BFO+20].

Other notions of quantum non-malleability. Some other notions of non-malleability for quantum messages have been studied in the context of *keyed* coding schemes by Ambainis, Bouda, and Winter [ABW09] and Alagic and Majenz [AM17]. In the keyed setting, quantum authentication schemes [BW16] also provide non-malleability, since they allow one to detect tampering on the encoded quantum data.

We can view the setting studied in [ABW09, AM17] for keyed coding schemes in the split-state model as follows (see Figure 3 for a diagram of the model): Let σ_M be the quantum message, and R be the key shared between the encoder and decoder. Let σ_M be encoded to $\rho_Z = \text{Enc}_R(\sigma_M)$. Then, the adversary tampers $\rho_Z \to \tau_Z$, and the decoder outputs $\eta_M = \text{Dec}_R(\tau_Z)$. Since the key R is available at both the encoder and decoder, we can view R as being the second part of the codeword, with the register Z being the first part of the codeword. Observe that in this model, the adversary is only allowed to tamper with the first part of the codeword, while our split-state tampering model allows the adversary to simultaneously but independently tamper with both parts of the codeword. Alagic and Majenz [AM17] used unitary 2-designs in their protocol for encoding and decoding. However, we note that their security definition involving mutual information appears a priori different from our Definition 1.

The question of whether one can even build split-state non-malleable coding schemes for quantum messages when there is no shared key and when the split-state adversary can tamper with both registers (with or without shared entanglement) remained open. In this work, we resolve this question in the affirmative.

Table 1 summarizes the main properties of known constructions of split-state NMCs and related constructions of keyed quantum schemes.

Concurrent work. In concurrent and independent work, Bergamaschi [Ber23] introduces, among other things, a natural quantum analogue of the *bitwise tampering* model [DPW18], where each qubit of the encoding is tampered independently, and constructs high-rate codes in this setting satisfying a restricted form of keyless authentication called tamper detection which is somewhat stronger than non-malleability. We note that this result is incomparable to ours. First, we consider tampering adversaries with access to shared entanglement, while Bergamaschi [Ber23] only studies the weaker setting where the various tampering adversaries are unentangled. In fact, tamper-detection codes (where the receiver either recovers the original message or aborts if they detect the adversary) are impossible to construct against adversaries with access to shared entanglement. This is because such adversaries can replace the quantum ciphertext with a fixed valid codeword. Second, the split-state tampering adversaries we study are much more powerful than bitwise tampering adversaries.

As already discussed above, in another concurrent work Batra, Boddu, and Jain [BBJ23] constructed a classical 2-split-state non-malleable randomness encoder secure against quantum adversaries having shared entanglement with rate close to 1/2. They use it to build constant-rate quantum secure 3-split-state NMCs for quantum messages.

11
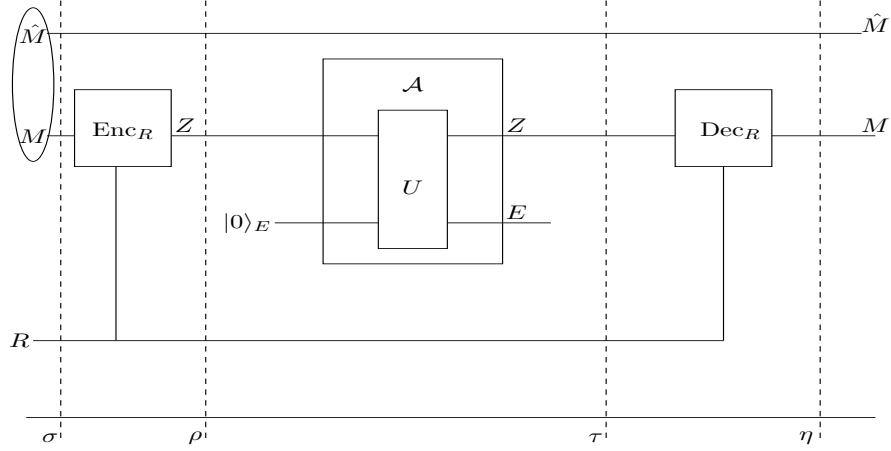
Figure 3: Quantum NMC with shared key.

Work by	Rate	Messages	Adversary	Shared key
[CGL20]	$\frac{1}{\text{poly}(n)}$	classical	classical	No
[Li17]	$\Omega\left(\frac{1}{\log n}\right)$	classical	classical	No
[Li19]	$\Omega\left(\frac{\log \log n}{\log n}\right)$	classical	classical	No
[AO20]	$\Omega(1)$	classical	classical	No
[Li23]	$\Omega(1)$	classical	classical	No
[AKO+22]	$1/3$	classical	classical	No
[ABJ24]	$\frac{1}{\text{poly}(n)}$	classical	**quantum**	No
[BBJ23]	$\approx 1/5$	(average-case) classical	**quantum**	No
[AM17]	$\Omega(1)$	**quantum**	**quantum**	Yes
This work	$\approx 1/11$	**(average-case) quantum**	**quantum**	No
This work	$\frac{1}{\text{poly}(n)}$	**quantum**	**quantum**	No

Table 1: Comparison between the best known explicit constructions of 2-split-state NMCs. Here, n denotes the codeword length.

1.3 Technical overview

1.3.1 Split-state NMCs for quantum messages

We follow a high-level strategy similar to that of Aggarwal, Agrawal, Gupta, Maji, Pandey, and Prabhakaran [AAG$^+$16], who used authenticated encryption to transform any (augmented) split-state non-malleable code into a high-rate split-state non-malleable code resilient to computationally-bounded tampering in the classical setting. The main challenge we have to deal with, and which is not considered in [AAG$^+$16], is that our tampering adversaries have quantum capabilities and are allowed to a priori share arbitrary *entangled quantum states*.

As a warm-up to our main construction, let us consider a simpler and natural approach that yields a 3-split-state non-malleable code for quantum messages. First, we observe that if we have a shared classical secret key R between the encoder and decoder, then we can detect whether *arbitrary* tampering has occurred by encoding the quantum message σ_M with a quantum authentication scheme $(\mathrm{Auth}_R, \mathrm{Ver}_R)$ [BCG$^+$02, BW16]. Therefore, a reasonable approach would be to first encode the message using this quantum authentication scheme, then encode the key R using an existing split-state non-malleable code for classical messages, and lastly output the split-state encoding of R as part of the final codeword.

Fortunately, since R is a classical string, we can use the split-state non-malleable code $(\mathrm{cEnc}, \mathrm{cDec})$ of Aggarwal, Boddu, and Jain [ABJ24], which protects against quantum adversaries! Less fortunately, $\mathrm{cEnc}(R)$ yields a codeword with two parts, call them R_1 and R_2, that cannot be stored together.

To elaborate on this approach, let's define a quantum authentication scheme as $(\mathrm{Auth}_R, \mathrm{Ver}_R)$, where Auth_R is a quantum encoding procedure that takes a quantum state σ_M and a classical secret key R and outputs an authenticated state $\psi = \mathrm{Auth}_R(\sigma_M)$. The verification procedure Ver_R takes an authenticated state ψ' and the secret key R as input, and outputs either 1 (accept) or 0 (reject). The overall encoding procedure $\mathrm{Enc}(\sigma_M)$ for our 3-split-state non-malleable code is as follows:

1. Sample a classical secret key R uniformly at random from an appropriate keyspace.

2. Compute the authenticated state $\psi = \mathrm{Auth}_R(\sigma_M)$ using the quantum authentication scheme.

3. Compute the classical split-state encoding $(R_1, R_2) = \mathrm{cEnc}(R)$.

4. Output the 3-state codeword (ψ, R_1, R_2).

To decode a possibly tampered codeword (ψ', R_1', R_2'), the decoding procedure Dec works as follows:

1. Use the classical decoder $\mathrm{cDec}(R_1', R_2')$ to obtain a candidate key R'.

2. Run the verification procedure $\mathrm{Ver}_{R'}(\psi')$ to check the authenticity of the quantum state ψ' using the candidate key R'.

3. If the verification procedure outputs 1 (accept), then output $\mathrm{Dec}(\psi', R_1', R_2')$. Otherwise, output a special symbol to indicate tampering.

This approach leverages the quantum authentication scheme to detect any tampering of the quantum message, and the classical split-state non-malleable code to protect the classical key R

against tampering. Intuitively, if we consider quantum adversaries *without* shared entanglement, the non-malleability of the 3-state coding scheme can be understood as follows: If the adversary attempts to tampering with R_1 and R_2, then the properties of the classical split-state non-malleable code (cEnc, cDec) guarantee that either the candidate key R' remains unchanged ($R' = R$) or that it becomes independent of R. In the former case, when the decoder Dec calls $\mathrm{Ver}_R(\psi')$, the quantum authentication scheme will, with high probability, detect whether $\psi' \neq \psi$, indicating tampering, and Dec will abort the decoding process. In the latter case, the decoder calls $\mathrm{Ver}_{R'}(\psi')$ with R' being independent of R and, consequently, independent of ψ' as well. Choosing a quantum authentication scheme, such as Clifford-based authentication, it is possible to show that $\mathrm{Ver}_{R'}(\psi')$ will output a state independent of (and thus unrelated to) the message σ with high probability.

Overall, this approach combines the strength of quantum authentication to detect tampering with the quantum message and the non-malleability property of the classical split-state code to protect the classical key R against tampering. By leveraging these properties together, we obtain a 3-split-state non-malleable code for quantum messages. Although the coding scheme above already gives some non-malleability guarantees for quantum messages, it features some major shortcomings. First, it requires dividing the codeword into three parts which must be stored separately. Ideally, we would like to construct efficient coding schemes that only need to be divided into *two* parts. Second, our argument above only works against quantum adversaries *without* shared entanglement. However, as we move to the more powerful setting with adversaries having shared entanglement, we need to develop more sophisticated techniques to ensure non-malleability.

Split-state non-malleable codes for average-case quantum messages. Perhaps the most natural approach to building a split-state non-malleable code secure against quantum adversaries with shared entanglement would be to take our 3-state code above and merge two of the parts. More precisely, we could attempt to analyze the code which outputs

$$(\psi, R_1) \quad \text{and} \quad R_2$$

as its two parts, where we recall that ψ is the authenticated state via the secret key R and $(R_1, R_2) = \mathrm{cEnc}(R)$ is the classical split-state non-malleable encoding of R.

This matches the approach taken in [AAG$^+$16]. However, as already mentioned above, they did not have to handle quantum adversaries with shared entanglement. Although this is also essentially the approach we successfully undertake, establishing non-malleability of this modified coding scheme is significantly more involved than the intuitive argument laid out above, and also requires some small further changes to the scheme. Indeed, one of the first difficulties arises due to the use of trap flags[7] in the authentication schemes, as we will discuss subsequently. We note that, unlike in an authentication scheme, the decoder need not output $\perp$ in a non-malleable code, since error detection is not required. We therefore get rid of the trap flags used in the authentication scheme specified in the 3-split argument above, and this is one of the first insights that allows our analysis to work.

We first describe a sub-optimal version of our approach in the setting of *average-case non-malleability*, and then discuss how its rate can be optimized. Per Definition 1, this corresponds

---

[7]Clifford-based quantum authentication schemes apply a random (secret) Clifford operator to the message plus several additional "trap registers" initialized to $|0\rangle$. Verifying whether tampering of the authenticated state occurred consists of checking whether the trap registers all return to the $|0\rangle$ state after applying the inverse Clifford operator. If this does not hold, then the verification procedure outputs the special symbol $\perp$, which we call the "trap flag".

to the scenario where the message σ_M is assumed to be a maximally mixed quantum state with canonical purification $\sigma_{M\hat{M}}$. To construct our split-state non-malleable code for quantum messages, we use random Clifford unitaries $\{(C_r, C_r^\dagger)\}_{r \leftarrow R}$ with underlying classical randomness R, along with the classical split-state coding scheme $(\mathrm{cEnc}, \mathrm{cDec})$ designed in [ABJ24] as a quantum-secure non-malleable code for the classical string R.

Inspired by the 3-state approach above, we use $(\mathrm{cEnc}, \mathrm{cDec})$ to protect the key R in a non-malleable manner, and then use the random Clifford C_R to protect the quantum message σ_M. This yields the following encoding procedure $\mathrm{Enc}(\sigma_M)$, where we use slightly different notation than the above to facilitate our analysis (see also Figure 5 for a diagram of our encoding and decoding procedures):

1. Sample a classical secret key R uniformly at random (independent of $\sigma_{M\hat{M}}$) from an appropriate keyspace;

2. Compute the state $(\sigma_1)_Z = C_R(\sigma_M)C_R^\dagger$;

3. Compute the split-state encoding $\mathrm{cEnc}(R) = (\sigma_1)_{XY}$;

4. Output the 2-part codeword $((\sigma_1)_{ZX}, (\sigma_1)_Y)$.

The message $\sigma_M = U_M$, along with its purification register $\hat{M}$, is thus encoded into $(\sigma_1)_{\hat{M}ZXY}$.

As our first observation, note that the register Z, which holds the Clifford-protected message, may carry information about the classical key R, since $(\sigma_1)_Z = C_R(\sigma_M)C_R^\dagger$. Fortunately, since $\sigma_M = U_M$, where U_M is a maximally mixed state, we have

$$(\sigma_1)_{ZXY} = (\sigma_1)_Z \otimes (\sigma_1)_{XY}.$$

One may then expect that we can use the argument of [ABJ24] for classical messages to argue that the key R remains secure even if the adversary sees the register Z when tampering one of the parts of $\mathrm{cEnc}(R)$. Unfortunately, the argument of [ABJ24] does not go through in this scenario. Namely, for $(\mathrm{cEnc}, \mathrm{cDec})$ to protect the key R in a non-malleable manner after adversarial tampering we need that

$$(\sigma_1)_{\hat{M}ZXY} = (\sigma_1)_{\hat{M}Z} \otimes (\sigma_1)_{XY}.$$

However, it can be verified that the registers $\hat{M}Z$ are not independent of XY in state σ_1. To circumvent this issue, we use the transpose method (see Fact 18) for state $\sigma_{M\hat{M}}$, and note that the application of the random Clifford gate C_R and the adversarial operations commute in σ_1 (see Figures 5 and 6). This allows us to delay the operation C_R on register $\hat{M}$ (see Figure 7). Crucially, we could not have used the transpose method in the presence of flag registers as employed in quantum authentication.

Carefully combining the above with arguments from [ABJ24], we conclude that $(\mathrm{cEnc}, \mathrm{cDec})$ can protect the key R after adversarial tampering on state θ_1 (which corresponds to the state prior to applying the C_R operation on register $\hat{M}$ in Figure 7), since

$$(\theta_1)_{\hat{M}ZXY} = (\theta_1)_{\hat{M}Z} \otimes (\theta_1)_{XY}.$$

Let θ_2 be the state obtained after adversarial tampering on θ_1. By the properties of $(\mathrm{cEnc}, \mathrm{cDec})$, we are essentially guaranteed that either $R' = R$ or that R' is independent of R in θ_2. However, this is not enough, and we observe that $(\mathrm{cEnc}, \mathrm{cDec})$ actually guarantees something even stronger! More precisely, in state θ_2 we have either:

- $R = R'$ and R is independent of registers $Z\hat{M}$;

- R is independent of $R'Z\hat{M}$.

In the case where R is independent of $R'Z\hat{M}$, applying the delayed operation C_R on register $\hat{M}$ decouples the registers $R'Z \otimes \hat{M}$, and so we are done. We are thus left to analyze the case where $R = R'$ and R is independent of registers $Z\hat{M}$. Here, we make use of the 2-design properties of the Clifford scheme $(C_R, C_R^\dagger)$. Roughly speaking, first suppose that the adversary applied $\mathbb{I}_Z$ on register Z. Then, since the message was maximally mixed, we conclude that we get an EPR state as the outcome of the tampering experiment (after the decoding procedure is applied). Now, suppose that the adversary applied some $P \neq \mathbb{I}_Z$ on register Z. We make use of Clifford randomization and the twirl property to handle this scenario. To elaborate, first note that the state

$$(\mathbb{I} \otimes P)(\theta_1)_{\hat{M}Z}(\mathbb{I} \otimes P^\dagger)$$

is in a subspace orthogonal to an EPR state in $\hat{M}Z$. Consider the state after applying the delayed operation C_R on register $\hat{M}$ and $C_R^\dagger$ on register Z. Here, Clifford randomization and the twirl property ensure that any state orthogonal to an EPR state in registers $\hat{M}Z$ is exactly maximally mixed in a subspace (of dimension $4^{|\hat{M}|} - 1$) orthogonal to this EPR state in registers $\hat{M}Z$ (see Lemma 8). As a result, the outcome of the tampering experiment after the decoding procedure is applied is close in trace distance to $U_{\hat{M}} \otimes U_M$. Our proof overall crucially uses interesting properties of the Pauli and Clifford unitaries including Pauli twirl, Clifford twirl, and Clifford randomization.

Improving the rate from sub-constant to constant in the average-case setting. An important quantity associated with a (non-malleable code) is its *rate* – the ratio between the size of a message and the size of its corresponding encoding. Looking at the proposed approach we discussed above, we conclude that its rate is sub-constant, i.e., the size of the encoding is a superlinear function of the message size. The main reasons behind this are as follows: First, the classical key R that we use to sample the Clifford operator C_R is much longer than the message σ_M (In fact $|R| = \mathcal{O}(|M|^2)$). Second, the rate of the underlying non-malleable code for classical messages $(\mathsf{cEnc}, \mathsf{cDec})$ from [ABJ24] is already sub-constant.

We now explain how our approach above can be modified to yield a constant-rate average-case non-malleable code for quantum messages. First, instead of using the whole Clifford group, we can use a shorter random key R to sample a Clifford operator from a smaller subgroup with special properties that suffice for our needs. A result of Cleve, Leung, Liu, and Wang [CLLW16] guarantees that this can be done efficiently with a classical key R of length at most $5|M|$. Second, observe that we only care about obtaining a split-state non-malleable encoding of a *uniformly random* classical key R. This means that we can replace the classical split-state non-malleable code $(\mathsf{cEnc}, \mathsf{cDec})$ from [ABJ24] by a *Non-Malleable Randomness Encoder* (NMRE), an object originally introduced by Kanukurthi, Obbattu, and Sekar [KOS18] and whose known constructions enjoy much better rates than non-malleable codes. Batra, Boddu, and Jain [BBJ23] recently constructed a classical NMRE secure against quantum adversaries having shared entanglement with a rate close to $1/2$.[8] In

---

[8]For the experienced reader, Batra, Boddu, and Jain [BBJ23] construct an explicit quantum-secure 2-source non-malleable extractor nmExt with a large output length. We can then sample classical bitstrings X and Y uniformly at random with appropriate lengths and set the classical key R to be $R = \mathsf{nmExt}(X, Y)$; this is the quantum-secure classical NMRE that we use in our optimized coding scheme.

contrast, as mentioned above, the NMC for classical messages from [ABJ24] only has a sub-constant rate.

Using these two results in our previously described approach allows us to improve the rate of our average-case NMC for quantum messages from sub-constant to close to $1/11$.

From average-case to worst-case NMCs for quantum messages. In the discussion above we assumed that the quantum message was maximally mixed. However, we would like to show that our code is a worst-case NMC, i.e., it is non-malleable for *any* fixed quantum message.

Consider an arbitrary quantum message ρ_M with canonical purification $\rho_{M\hat{M}}$. Recall that $\sigma_{\hat{M}M}$ is the canonical purification of $\sigma_M = U_M$. Using a quantum rejection sampling argument (see Fact 7), we obtain a measurement acting on register $\hat{M}$ of σ such that the state conditioned on "success" is exactly ρ. Moreover, this measurement on the register $\hat{M}$ commutes with Enc, Dec, and the adversarial operations, and it succeeds with probability $2^{-|M|}$. If the error of the underlying average-case NMC is ε, then this measurement allows us to argue non-malleability of the same NMC for any message ρ_M (i.e., worst-case non-malleability) with larger error $\varepsilon' = 2^{|M|} \cdot \varepsilon$, and we can easily handle this blow-up in the error at the expense of dropping the rate of the code from constant to sub-constant. Intuitively, this happens because of the following: Suppose that there is a fixed message ρ for which Equation (1) (with ρ in place of σ) holds only with error larger than ε'. Therefore, when faced with a maximally mixed message $\sigma_{M\hat{M}}$, we can apply the measurement above to $\hat{M}$ and, if the measurement succeeds and the resulting state is ρ, distinguish with advantage larger than ε'. Since the measurement succeeds with probability at least $2^{-|M|}$, the overall distinguishing advantage is larger than $2^{-|M|} \cdot \varepsilon' = \varepsilon$, which contradicts the average-case ε-non-malleability of the NMC.

1.3.2 Threshold split-state NMSS schemes for quantum messages

At a high level, in order to construct our threshold NMSS schemes for quantum messages, we combine our split-state NMC for quantum messages above with the approach of Goyal and Kumar [GK18a] used to construct NMSS schemes in the classical setting. However, as we will discuss, following this approach in the quantum setting poses various challenges.

Roughly speaking, the approach of Goyal and Kumar [GK18a] for building NMSS schemes proceeds as follows for p parties and a threshold $3 \leq t \leq p$. On input a message m, first encode it with the split-state NMC to generate two states, L and R. Now, apply a standard t-out-of-p secret sharing scheme to L (say, Shamir's secret sharing), yielding shares $L_1, \ldots, L_p$. Furthermore, apply a 2-out-of-p *leakage-resilient* secret sharing scheme to R, yielding shares $R_1, \ldots, R_p$. Intuitively, a secret sharing scheme is leakage-resilient if the input remains private even when the adversary learns an unauthorized subset of shares *plus* bounded side information from every other share. Finally, set the resulting i-th share S_i as $S_i = (L_i, R_i)$ for each $i \in [p]$.

To argue the non-malleability of this construction, Goyal and Kumar showed how to transform any tampering attack on the resulting secret sharing scheme into an essentially-as-good tampering attack on the underlying 2-split-state NMC. The main challenge in designing such a reduction is that the two tampering functions for the underlying NMC must act independently – we must tamper L without knowledge of R, and vice versa. On the other hand, the i-th tampering function for the secret sharing scheme tampers (L_i, R_i) into (L_i', R_i'), and so potentially has access to some information from both L and R. For simplicity, let L' and R' denote the tampered secrets

reconstructed from $(L'_1, \ldots, L'_t)$ and (R'_1, R'_2), respectively.

Showing that we can obtain R' from R without knowing L is easy. This follows because R' is fully determined by R'_1 and R'_2, which in turn only depend on L_1 and L_2. Since the L_i's are a t-out-of-p Shamir secret sharing of L with threshold $t \geq 3$, the two shares L_1 and L_2 are independent of L. However, arguing that we can (up to small error) obtain L' from L without knowledge of R is a lot trickier. The previous argument clearly does not immediately work since the t shares $L'_1, \ldots, L'_t$ depend on $R_1, \ldots, R_t$, respectively, which determine R. This is where the leakage-resilience property kicks in – if we see the L'_is as bounded leakage on the R_is, then leakage-resilience guarantees that R is (close to) independent of the leakages $L'_1, \ldots, L'_t$, and so is independent of L'.

Realizing this approach in the quantum setting. We follow the same high-level approach for a quantum message σ_M. To that end, we first replace the classical split-state NMC by our NMC for quantum messages discussed previously. We use additional key properties of our NMC: (1) The resulting left state L is quantum, but the right state R is *classical*, and (2) we prove that it is actually a 2-out-of-2 split-state NMSS scheme, and so, in particular, learning only one of L and R reveals nothing about σ_M. Since L is quantum, we now apply a standard t-out-of-p (for $p < 2t$) secret sharing scheme for quantum messages, such as "quantum" Shamir secret sharing [CGL99], to get quantum shares $(L_1, \ldots, L_p)$. And, since R is classical, we secret-share it using a 2-out-of-p scheme satisfying a special leakage-resilience property that we will determine later.

Establishing correctness and privacy of the resulting t-out-of-p secret sharing scheme is not difficult using property (2) of our NMC above. It remains to prove non-malleability. Arguing that R' can be obtained from R without knowledge of L still follows easily from the fact that R is shared using a 2-out-of-p scheme, while L is shared using a t-out-of-p scheme with $t \geq 3$. Here, it is crucial that R is classical. Otherwise, a 2-out-of-p scheme would not exist when $p \geq 4$, and this means that we would not be able to, say, construct $(p/2 + 1)$-out-of-p split-state NMSS schemes for quantum messages for *any* even p using this approach.

We also want to argue that L' can be obtained from L without knowledge of R. As before, we would like to see $L'_1, \ldots, L'_p$ as leakages on the secret shares $R_1, \ldots, R_p$, and then exploit the leakage-resilience of the scheme used to share R to conclude that R is independent of $L'_1, \ldots, L'_p$, and hence of L'. However, realizing this in our quantum setting requires stronger leakage-resilience properties: First, the tamperings $L'_1, \ldots, L'_p$ are now quantum states. Second, the tampering functions in our setting *share arbitrary entangled states*. This means that the i-th tampering function now sees (L_i, R_i, W_i), where $W_1, \ldots, W_p$ are quantum registers holding an arbitrary state. To overcome these barriers, we introduce *augmented* leakage-resilient secret sharing schemes. This corresponds to a setting where there are p local adversaries $\mathcal{A}_1, \ldots, \mathcal{A}_p$ sharing an arbitrary entangled state spread across registers $W_1, \ldots, W_p$, respectively, and each one having access to a share $R_1, \ldots, R_p$. We require that R remains hidden even if $\mathcal{A}_i$ knows the share R_i, local bounded quantum leakages $\mathsf{Leak}_1(R_1, W_1), \ldots, \mathsf{Leak}_{i-1}(R_{i-1}, W_{i-1}), \mathsf{Leak}_{i+1}(R_{i-1}, W_{i+1}), \ldots, \mathsf{Leak}_p(R_p, W_p)$ from every other share, *and also the entangled state W_i* (hence the "augmented" adjective). We prove that the 2-out-of-2 secret sharing scheme whereby R is shared into X and Y sampled uniformly such that $\langle X, Y \rangle = R$ is augmented leakage-resilient with good parameters. This relies on the randomness extraction properties of the inner product function and the formalism of "qpa-states"[9] [BJK21]. We can then extend this scheme to a 2-out-of-p augmented leakage-resilient scheme for classical messages in a standard manner. Although notions of leakage-resilience against quantum adversaries

---

[9]qpa-state stands for quantum purified adversary state.

with shared entanglement have been studied in other recent work [CGLR23], these do not cover augmented leakage-resilience.

Besides the above, proving non-malleability requires dealing with additional subtleties specific to the quantum setting. The original non-malleability argument in [GK18a] proceeds by fixing the values of certain components (e.g., shares, leakages). However, we cannot fully emulate this approach in the quantum setting: The left state L is quantum, and so are the bounded leakages that show up in the analysis. Therefore, we cannot fix them. Moreover, again because L is quantum, it is modified after the tampering functions are applied, but we still need to access the "original" L in the analysis. For this, with some work, we can use the message's canonical purification register $\hat{M}$ to generate a new register $\hat{L}$ which can be thought of as a coherent copy of the original left state L.

1.4 Open problems

We list here some interesting directions for future research:

- Can we design (worst-case) split-state NMCs for quantum messages with a constant rate? This is open even for classical messages against quantum adversaries with shared entanglement. More ambitiously, can we construct (worst-case) split-state NMSS schemes for quantum messages with a constant rate?

- Can we construct 2-out-of-3 split-state non-malleable secret sharing schemes for quantum messages?

- Can we design NMSS schemes for quantum messages that are secure against joint tampering of shares?

- What can we achieve if we consider computationally-bounded adversaries instead?

1.5 Acknowledgements

2 Preliminaries

This section collects basic notation and conventions alongside useful facts and lemmas that we use in the proofs of our main results. In this work, facts denote results already known from prior work, and lemmas denote auxiliary results that we prove here.

2.1 Basic general notation

All the logarithms are evaluated to the base 2. We denote sets by uppercase calligraphic letters such as $\mathcal{X}$ and use uppercase roman letters such as X and Y for both random variables and quantum registers. The distinction will be clear from context. The set $\{1, \ldots, n\}$ may be written as $[n]$, and we may also more generally write $[t, n]$ for the set $\{t, t + 1, \ldots, n\}$. We denote the uniform distribution over $\{0, 1\}^d$ by U_d. For a *random variable* $X \in \mathcal{X}$, we use X to denote both the random variable and its distribution, whenever it is clear from context. We use $x \leftarrow X$ to denote that x is drawn according to X, and, for a finite set $\mathcal{X}$, we use $x \leftarrow \mathcal{X}$ to denote that x is drawn uniformly at random from $\mathcal{X}$. For two random variables X, Y we use $X \otimes Y$ to denote their product distribution. We call random variables X and Y *copies* of each other if and only if $\Pr[X = Y] = 1$.

2.2 Quantum information theory

In this section we cover some important basic prerequisites from quantum information theory alongside some useful lemmas and facts.

2.2.1 Conventions and notation

Consider a finite-dimensional Hilbert space $\mathcal{H}$ endowed with an inner-product $\langle \cdot, \cdot \rangle$ (we only consider finite-dimensional Hilbert-spaces). A quantum state (or a density matrix or a state) is a positive semi-definite operator on $\mathcal{H}$ with trace value equal to 1. It is called *pure* if and only if its rank is 1. Let $|\psi\rangle$ be a unit vector on $\mathcal{H}$, that is $\langle \psi, \psi \rangle = 1$. With some abuse of notation, we use ψ to represent the state and also the density matrix $|\psi\rangle\langle\psi|$, associated with $|\psi\rangle$. Given a quantum state ρ on $\mathcal{H}$, the *support of* ρ, denoted by $\mathrm{supp}(\rho)$, is the subspace of $\mathcal{H}$ spanned by all eigenvectors of ρ with non-zero eigenvalues.

A *quantum register* A is associated with some Hilbert space $\mathcal{H}_A$. Define $|A| := \log(\dim(\mathcal{H}_A))$. For a sequence of registers $A_1, \ldots, A_n$ and a set $T \subseteq [n]$, we define the projection according to T as $A_T = (A_i)_{i \in T}$. Let $\mathcal{L}(\mathcal{H}_A)$ represent the set of all linear operators on the Hilbert space $\mathcal{H}_A$. For an operator $O \in \mathcal{L}(\mathcal{H}_A)$, we use O^T to represent the transpose of O. For operators $O, O' \in \mathcal{L}(\mathcal{H}_A)$, the notation $O \leq O'$ represents the Löwner order, that is, $O' - O$ is a positive semi-definite operator. We denote by $\mathcal{D}(\mathcal{H}_A)$ the set of all quantum states on the Hilbert space $\mathcal{H}_A$. The state ρ with subscript A indicates that $\rho_A \in \mathcal{D}(\mathcal{H}_A)$. If two registers A, B are associated with the same Hilbert space, we shall represent the relation by $A \equiv B$. For two states ρ and σ, we write $\rho \equiv \sigma$ if they are identical as states (potentially in different registers). Composition of two registers A and B, denoted AB, is associated with the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. For two quantum states $\rho \in \mathcal{D}(\mathcal{H}_A)$ and $\sigma \in \mathcal{D}(\mathcal{H}_B)$, $\rho \otimes \sigma \in \mathcal{D}(\mathcal{H}_{AB})$ represents the tensor product (*Kronecker* product) of ρ and σ. The identity operator on $\mathcal{H}_A$ is denoted $\mathbb{I}_A$. Let U_A denote the maximally mixed state in $\mathcal{H}_A$. Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$. Define

$$\rho_B \stackrel{\text{def}}{=} \mathrm{Tr}_A \rho_{AB} \stackrel{\text{def}}{=} \sum_i (\langle i| \otimes \mathbb{I}_B) \rho_{AB} (|i\rangle \otimes \mathbb{I}_B),$$

where $\{|i\rangle\}_i$ is an orthonormal basis for the Hilbert space $\mathcal{H}_A$. The state $\rho_B \in \mathcal{D}(\mathcal{H}_B)$ is referred to as the marginal state of ρ_{AB} on the register B. Unless otherwise stated, a missing register from subscript in a state represents partial trace over that register. Given $\rho_A \in \mathcal{D}(\mathcal{H}_A)$, a *purification* of ρ_A is a pure state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ such that $\mathrm{Tr}_B \rho_{AB} = \rho_A$. Purification of a quantum state

is not unique. Suppose $A \equiv B$. Given $\{|i\rangle_A\}$ and $\{|i\rangle_B\}$ as orthonormal bases over $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, the *canonical purification* of a quantum state ρ_A is a pure state $\rho_{AB} \overset{\text{def}}{=} (\rho_A^{\frac{1}{2}} \otimes \mathbb{I}_B) (\sum_i |i\rangle_A |i\rangle_B)$.

A quantum map $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is a completely positive and trace preserving (CPTP) linear map. A CPTP map $\mathcal{E}$ is described by the Kraus operators $\{M_i : \mathcal{H}_A \to \mathcal{H}_B\}_i$ such that $\mathcal{E}(\rho) = \sum_i M_i \rho M_i^\dagger$ and $\sum_i M_i^\dagger M_i = \mathbb{I}_A$. A *Hermitian* operator $H : \mathcal{H}_A \to \mathcal{H}_A$ is such that $H = H^\dagger$. A projector $\Pi \in \mathcal{L}(\mathcal{H}_A)$ is a Hermitian operator such that $\Pi^2 = \Pi$. A *unitary* operator $V_A : \mathcal{H}_A \to \mathcal{H}_A$ is such that $V_A^\dagger V_A = V_A V_A^\dagger = \mathbb{I}_A$. The set of all unitary operators on $\mathcal{H}_A$ is denoted by $\mathcal{U}(\mathcal{H}_A)$. An *isometry* $V : \mathcal{H}_A \to \mathcal{H}_B$ is such that $V^\dagger V = \mathbb{I}_A$. A *POVM* element is an operator $0 \le M \le \mathbb{I}$. We use the shorthand $\bar{M} \overset{\text{def}}{=} \mathbb{I} - M$, where $\mathbb{I}$ is clear from context. We use shorthand M to represent $M \otimes \mathbb{I}$, where $\mathbb{I}$ is clear from context.

2.2.2 Registers, quantum maps, and isometries

This section collects definitions of certain registers and operations on them.

Definition 3 (Classical register in a pure state). *Let $\mathcal{X}$ be a set. A* classical-quantum *(c-q) state ρ_{XE} is of the form*

$$\rho_{XE} = \sum_{x \in \mathcal{X}} p(x) |x\rangle\langle x| \otimes \rho_E^x,$$

where ρ_E^x are states.

Let ρ_{XEA} be a pure state. We call X a classical register *in ρ_{XEA} if ρ_{XE} (or ρ_{XA}) is a c-q state. Whenever it is clear from context, we identify the random variable X with the register X via $\Pr[X = x] = p(x)$.*

Definition 4 (Copy of a classical register). *Let $\rho_{X\hat{X}E}$ be a pure state with X being a classical register in $\rho_{X\hat{X}E}$ taking values in $\mathcal{X}$. Similarly, let $\hat{X}$ be a classical register in $\rho_{X\hat{X}E}$ taking values in $\mathcal{X}$. Let $\Pi_{\mathsf{Eq}} = \sum_{x \in \mathcal{X}} |x\rangle\langle x| \otimes |x\rangle\langle x|$ be the* equality *projector acting on the registers $X\hat{X}$. We call X and $\hat{X}$* copies *of each other (in the computational basis) if $\mathrm{Tr}\left(\Pi_{\mathsf{Eq}}\rho_{X\hat{X}}\right) = 1$.*

Definition 5 (Conditioning). *Let*

$$\rho_{XE} = \sum_{x \in \{0,1\}^n} p(x) |x\rangle\langle x| \otimes \rho_E^x,$$

be a c-q state. For an event $\mathcal{S} \subseteq \{0,1\}^n$, define

$$\Pr[\mathcal{S}]_\rho \overset{\text{def}}{=} \sum_{x \in \mathcal{S}} p(x) \quad and \quad (\rho | X \in \mathcal{S}) \overset{\text{def}}{=} \frac{1}{\Pr[\mathcal{S}]_\rho} \sum_{x \in \mathcal{S}} p(x) |x\rangle\langle x| \otimes \rho_E^x.$$

We sometimes shorthand $(\rho | X \in \mathcal{S})$ as $(\rho | \mathcal{S})$ when the register X is clear from context.

Let ρ_{AB} be a state with $|A| = n$. We define $(\rho | A \in \mathcal{S}) \overset{\text{def}}{=} (\sigma | \mathcal{S})$, where σ_{AB} is the c-q state obtained by measuring the register A in ρ_{AB} in the computational basis. In the case where $\mathcal{S} = \{s\}$ is a singleton set, we shorthand $(\rho | A = s) \overset{\text{def}}{=} \mathrm{Tr}_A(\rho | A = s)$.

Definition 6 (Safe maps). *We call an isometry $V : \mathcal{H}_X \otimes \mathcal{H}_A \to \mathcal{H}_X \otimes \mathcal{H}_B$, safe on X if and only if there is a collection of isometries $V_x : \mathcal{H}_A \to \mathcal{H}_B$ such that for all states $|\psi\rangle_{XA} = \sum_x \alpha_x |x\rangle_X |\psi^x\rangle_A$ we have that*

$$V|\psi\rangle_{XA} = \sum_x \alpha_x |x\rangle_X V_x |\psi^x\rangle_A.$$

Definition 7 (Extension). *Let*

$$\rho_{XE} = \sum_{x \in \mathcal{X}} p(x)|x\rangle\langle x| \otimes \rho_E^x,$$

be a c-q state. For a function $Z : \mathcal{X} \to \mathcal{Z}$, define the following extension of ρ_{XE},

$$\rho_{ZXE} \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}} p(x)|Z(x)\rangle\langle Z(x)| \otimes |x\rangle\langle x| \otimes \rho_E^x.$$

For a pure state ρ_{XEA} (with X classical and $X \in \mathcal{X}$) and a function $Z : \mathcal{X} \to \mathcal{Z}$, define $\rho_{Z\hat{Z}XEA}$ to be a pure state extension of ρ_{XEA} generated via a safe isometry $V : \mathcal{H}_X \to \mathcal{H}_X \otimes \mathcal{H}_Z \otimes \mathcal{H}_{\hat{Z}}$ (Z classical with copy $\hat{Z}$). We use the notation $\mathcal{M}_A(\rho_{AB})$ to denote measurement in the computational basis on register A in state ρ_{AB}.

All isometries considered in this paper are safe on classical registers that they act on. Isometries applied by adversaries can be assumed without loss of generality as safe on classical registers, by the adversary first making a (safe) copy of classical registers and then proceeding as before. This does not reduce the power of the adversary. The following notion of a Stinespring isometry extension will also be useful at times.

Fact 1 (Stinespring isometry extension [Wat11, Theorem 5.1]). *Consider a CPTP map $\Phi : \mathcal{L}(\mathcal{H}_X) \to \mathcal{L}(\mathcal{H}_Y)$. There exists an isometry $V : \mathcal{H}_X \to \mathcal{H}_Y \otimes \mathcal{H}_Z$ (called the Stinespring isometry extension of Φ) such that $\Phi(\rho_X) = \text{Tr}_Z(V\rho_X V^\dagger)$ for every state ρ_X.*

Fact 2 (Stinespring isometry extension for a classical map). *Let $\Phi : \mathcal{L}(\mathcal{H}_X) \to \mathcal{L}(\mathcal{H}_Y)$ be a classical map such that for every $X = x$ we have a fixed function f acting on register Y such that $\Pr(f(\Phi(x)) = x) = 1$. There exists an isometry $V_\Phi : \mathcal{H}_X \to \mathcal{H}_Y \otimes \mathcal{H}_{\hat{Y}}$ (called the Stinespring isometry extension of Φ) such that $\Phi(\rho_X) = \text{Tr}_{\hat{Y}}(V\rho_X V^\dagger)$ for every state ρ_X. Furthermore, for a classical register ρ_X, we also have $\Pr(Y = \hat{Y})_{V\rho_X V^\dagger} = 1$.*

2.2.3 Norms, trace distance, and divergences

This section collects definitions of some important quantum information-theoretic quantities and related useful properties.

Definition 8 (Schatten p-norm). *For $p \geq 1$ and a matrix A, the Schatten p-norm of A, denoted by $\|A\|_p$, is defined as $\|A\|_p \stackrel{\text{def}}{=} (\text{Tr}(A^\dagger A)^{\frac{p}{2}})^{\frac{1}{p}}$.*

Definition 9 (Trace distance). *The trace distance between two states ρ and σ is given by $\|\rho - \sigma\|_1$. We write $\rho \approx_\varepsilon \sigma$ if $\|\rho - \sigma\|_1 \leq \varepsilon$.*

Definition 10 (Fidelity). *The fidelity between two states ρ and σ, denoted by $\mathsf{F}(\rho, \sigma)$, is defined as*

$$\mathsf{F}(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1.$$

Definition 11 (Bures metric)**.** *The Bures distance between two states ρ and σ, denoted by $\Delta_B(\rho, \sigma)$, is defined as*

$$\Delta_B(\rho, \sigma) = \sqrt{1 - \mathsf{F}(\rho, \sigma)}.$$

Definition 12 (Max-divergence ([Dat09], see also [JRS02]))**.** *Given states ρ and σ such that $\operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma)$, the max-divergence between ρ and σ, denoted by $\mathrm{D}_{\max}(\rho\|\sigma)$, is defined as*

$$\mathrm{D}_{\max}(\rho\|\sigma) = \min\{\lambda \in \mathbb{R} : \rho \leq 2^\lambda \sigma\}.$$

Definition 13 (Max-information [Dat09])**.** *Given a state ρ_{AB}, the max-information between A and B, denoted by $\mathrm{I}_{\max}(A : B)_\rho$, is given by*

$$\mathrm{I}_{\max}(A : B)_\rho \stackrel{\text{def}}{=} \inf_{\sigma_B \in \mathcal{D}(\mathcal{H}_B)} \mathrm{D}_{\max}(\rho_{AB} \| \rho_A \otimes \sigma_B).$$

We state a useful fact about max-information.

Fact 3 ([BJL23, Fact 5])**.** *Let ρ_{XBD} be a c-q state (X classical) such that $\rho_{XB} = \rho_X \otimes \rho_B$. Then,*

$$\mathrm{I}_{\max}(X : BD)_\rho \leq 2|D|.$$

For the facts stated below without citation, we refer the reader to standard textbooks [NC00, Wat18]. The following facts state some basic properties of trace distance.

Fact 4 (Data-processing inequality)**.** *Let ρ, σ be states and $\mathcal{E}$ be a CPTP map. Then,*

- $\|\mathcal{E}(\rho) - \mathcal{E}(\sigma)\|_1 \leq \|\rho - \sigma\|_1$;

- $\Delta_B(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq \Delta_B(\rho, \sigma)$.

The inequality above is an equality whenever $\mathcal{E}$ is a CPTP map corresponding to an isometry.

Fact 5. *Let ρ, σ be states. Let Π be a projector. Then,*

$$\mathrm{Tr}(\Pi\rho) \left\| \frac{\Pi\rho\Pi}{\mathrm{Tr}(\Pi\rho)} - \frac{\Pi\sigma\Pi}{\mathrm{Tr}(\Pi\sigma)} \right\|_1 \leq \|\rho - \sigma\|_1.$$

Fact 6. *Let ρ, σ be states such that $\rho = \sum_x p_x \rho^x$, $\sigma = \sum_x p_x \sigma^x$, $\{\rho^x, \sigma^x\}_x$ are states and $\sum_x p_x = 1$. Then,*

$$\|\rho - \sigma\|_1 \leq \sum_x p_x \|\rho^x - \sigma^x\|_1.$$

The next result is useful for the rejection sampling step in the analysis of our candidate code.

Fact 7 ([JRS02])**.** *Let $\rho_{A'B}, \sigma_{AB}$ be pure states such that $\mathrm{D}_{\max}(\rho_B\|\sigma_B) \leq k$. Let Alice and Bob share σ_{AB}. There exists an isometry $V : \mathcal{H}_A \to \mathcal{H}_{A'} \otimes \mathcal{H}_C$ such that:*

1. *$(V \otimes \mathbb{I}_B)\sigma_{AB}(V \otimes \mathbb{I}_B)^\dagger = \phi_{A'BC}$, where C is a single qubit register.*

2. *Let C be the outcome of measuring ϕ_C in the standard basis. Then $\Pr[C = 1] \geq 2^{-k}$.*

3. *Conditioned on outcome $C = 1$, the state shared between Alice and Bob is $\rho_{A'B}$.*

The following fact connects the fidelity, trace distance, and the Bures metric.

Fact 8 (Fuchs-van de Graaf inequalities [FvdG06] (see also [Wat11, Theorem 4.10])). *Let ρ, σ be two states. Then,*

$$1 - \mathsf{F}(\rho, \sigma) \leq \frac{1}{2}\|\rho - \sigma\|_1 \leq \sqrt{1 - \mathsf{F}(\rho, \sigma)^2} \quad and \quad \Delta_B(\rho, \sigma)^2 \leq \frac{1}{2}\|\rho - \sigma\|_1 \leq \sqrt{2}\Delta_B(\rho, \sigma).$$

In the above fact, the second set of inequalities follows by noting that

$$1 - \mathsf{F}(\rho, \sigma)^2 \leq 2 - 2\mathsf{F}(\rho, \sigma) = 2\Delta_B(\rho, \sigma)^2.$$

We now state Uhlmann's Theorem, which relates the closeness of any two mixed states ρ, σ to the closeness of two purification states $|\rho\rangle, |\sigma\rangle$, respectively.

Fact 9 (Uhlmann's Theorem [Uhl76]). *Let $\rho_A, \sigma_A \in \mathcal{D}(\mathcal{H}_A)$ and let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ be a purification of ρ_A and $\sigma_{AC} \in \mathcal{D}(\mathcal{H}_{AC})$ be a purification of σ_A. Then, there exists an isometry V (from a subspace of $\mathcal{H}_C$ to a subspace of $\mathcal{H}_B$) such that*

$$\Delta_B\left(|\rho\rangle\langle\rho|_{AB}, |\theta\rangle\langle\theta|_{AB}\right) = \Delta_B(\rho_A, \sigma_A),$$

where $|\theta\rangle_{AB} = (\mathbb{I}_A \otimes V)|\sigma\rangle_{AC}$.

2.2.4 Pauli and Clifford operators

We proceed to define Pauli operators and the associated Pauli and Clifford groups.

Definition 14 (Pauli operators). *The single-qubit Pauli operators are given by*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

An n-qubit Pauli operator is given by the n-fold tensor product of single-qubit Pauli operators. We denote the set of all $|A|$-qubit Pauli operators on $\mathcal{H}_A$ by $\mathcal{P}(\mathcal{H}_A)$, where $|\mathcal{P}(\mathcal{H}_A)| = 4^{|A|}$. Any linear operator $L \in \mathcal{L}(\mathcal{H}_A)$ can be written as a linear combination of $|A|$-qubit Pauli operators with complex coefficients as $L = \sum_{P \in \mathcal{P}(\mathcal{H}_A)} \alpha_P P$. This is called the Pauli decomposition *of a linear operator.*

Definition 15 (Pauli group). *The single-qubit* Pauli group *is given by*

$$\{+P, -P, \ iP, \ -iP : P \in \{I, X, Y, Z\}\}.$$

The Pauli group on $|A|$-qubits is the group generated by the operators described above applied to each of $|A|$-qubits in the tensor product. We denote the $|A|$-qubit Pauli group on $\mathcal{H}_A$ by $\tilde{\mathcal{P}}(\mathcal{H}_A)$.

Definition 16 (Clifford group). *The* Clifford group $\mathcal{C}(\mathcal{H}_A)$ *is defined as the group of unitaries that normalize the Pauli group $\tilde{\mathcal{P}}(\mathcal{H}_A)$, i.e.,*

$$\mathcal{C}(\mathcal{H}_A) = \{V \in \mathcal{U}(\mathcal{H}_A) : V\tilde{\mathcal{P}}(\mathcal{H}_A)V^\dagger = \tilde{\mathcal{P}}(\mathcal{H}_A)\}.$$

The Clifford unitaries *are the elements of the Clifford group.*

We will also need to work with subgroups of the Clifford group with certain special properties. The following fact describes these properties and guarantees the existence of such subgroups.

Fact 10 (Subgroup of the Clifford group [CLLW16]). *There exists a subgroup $\mathcal{SC}(\mathcal{H}_A)$ of the Clifford group $\mathcal{C}(\mathcal{H}_A)$ such that given any non-identity Pauli operators $P, Q \in \mathcal{P}(\mathcal{H}_A)$ we have that*

$$|\{C \in \mathcal{SC}(\mathcal{H}_A) | C^\dagger P C = Q\}| = \frac{|\mathcal{SC}(\mathcal{H}_A)|}{|\mathcal{P}(\mathcal{H}_A)| - 1} \quad and \quad |\mathcal{SC}(\mathcal{H}_A)| = 2^{5|A|} - 2^{3|A|}.$$

Informally, applying a random Clifford operator from $\mathcal{SC}(\mathcal{H}_A)$ (by conjugation) maps P to a Pauli operator chosen uniformly at random over all non-identity Pauli operators. Furthermore, we have that $\mathcal{P}(\mathcal{H}_A) \subset \mathcal{SC}(\mathcal{H}_A)$.

Additionally, there exists a procedure Samp *which when given as input a uniformly random string $R \leftarrow \{0,1\}^{5|A|}$ outputs in time $\mathrm{poly}(|A|)$ the classical description* Samp(R) *of a Clifford operator $C_R \in \mathcal{SC}(\mathcal{H}_A)$ with the following property: Let $U_{\mathcal{SC}(\mathcal{H}_A)}$ denote the uniform distribution over the classical descriptions of Clifford operators in $\mathcal{SC}(\mathcal{H}_A)$. Then, it holds that*

$$\mathsf{Samp}(R) \approx_{2^{-2|A|}} U_{\mathcal{SC}(\mathcal{H}_A)}, \tag{3}$$

where, as before, $\approx_{2^{-2|A|}}$ means that the statistical distance between the two distributions is at most $2^{-2|A|}$.

Pauli twirling and related facts. The analysis of our construction will require the use of several facts related to Pauli twirling. We collect them below, beginning with the usual version of the Pauli twirl.

Fact 11 (Pauli twirl [DCEL09]). *Let $\rho \in \mathcal{D}(\mathcal{H}_A)$ be a state and $P, P' \in \mathcal{P}(\mathcal{H}_A)$ be Pauli operators such that $P \neq P'$. Then,*

$$\sum_{Q \in \mathcal{P}(\mathcal{H}_A)} Q^\dagger P Q \rho Q^\dagger P'^\dagger Q = 0.$$

Fact 12 (Subgroup Clifford twirl [BBJ23]). *Let $\rho \in \mathcal{D}(\mathcal{H}_A)$ be a state and $P, P' \in \mathcal{P}(\mathcal{H}_A)$ be Pauli operators such that $P \neq P'$. Let $\mathcal{SC}(\mathcal{H}_A)$ be the subgroup of Clifford group as defined in Fact 10. Then,*

$$\sum_{C \in \mathcal{SC}(\mathcal{H}_A)} C^\dagger P C \rho C^\dagger P'^\dagger C = 0.$$

As an immediate corollary, we conclude that for any normal operator $M \in \mathcal{L}(\mathcal{H}_A)$ such that $M^\dagger M = M M^\dagger$ we have that

$$\sum_{C \in \mathcal{SC}(\mathcal{H}_A)} C^\dagger P C M C^\dagger P'^\dagger C = 0,$$

since M has an eigen-decomposition.

Fact 13 (Modified twirl [BBJ23]). *Let $\rho_{\hat{A}A}$ be the canonical purification of ρ_A. Let $P \in \mathcal{P}(\mathcal{H}_A), P' \in \mathcal{P}(\mathcal{H}_A)$ be Pauli operators such that $P \neq P'$. Let $\mathcal{SC}(\mathcal{H}_A)$ be the subgroup of Clifford group as defined in Fact 10. Then,*

$$\sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (\mathbb{I} \otimes C^\dagger P C) \rho_{\hat{A}A} (\mathbb{I} \otimes C^\dagger P'C) = 0.$$

Fact 14 (Uniform Pauli conjugation). *Let $P \in \mathcal{P}(\mathcal{H}_A)$ be a Pauli operator. If $P = \mathbb{I}_A$, then*

$$\frac{1}{|\mathcal{P}(\mathcal{H}_A)|} \sum_{Q \in \mathcal{P}(\mathcal{H}_A)} QPQ^\dagger = \mathbb{I}_A,$$

else if $P \neq \mathbb{I}_A$

$$\frac{1}{|\mathcal{P}(\mathcal{H}_A)|} \sum_{Q \in \mathcal{P}(\mathcal{H}_A)} QPQ^\dagger = 0.$$

Proof. If $P = \mathbb{I}_A$, the statement trivially follows. If $P \neq \mathbb{I}_A$, the statement follows from Fact 11 by considering (P, P', ρ) in Fact 11 to be $(P, \mathbb{I}_A, U_A)$. $\qquad\square$

Similarly, the following result is a consequence of Fact 12.

Fact 15 (Uniform conjugation). *Let $P \in \mathcal{P}(\mathcal{H}_A)$ be a Pauli operator. If $P = \mathbb{I}_A$, then*

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} CPC^\dagger = \mathbb{I}_A.$$

Else, if $P \neq \mathbb{I}_A$, then

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} CPC^\dagger = 0.$$

The following fact is folklore. We provide a proof for completeness.

Fact 16 (Pauli 1-design). *Let ρ_{AB} be a state. Then,*

$$\frac{1}{|\mathcal{P}(\mathcal{H}_A)|} \sum_{Q \in \mathcal{P}(\mathcal{H}_A)} (Q \otimes \mathbb{I}) \rho_{AB} (Q^\dagger \otimes \mathbb{I}) = U_A \otimes \rho_B.$$

Proof. Let

$$\rho_{AB} = \sum_{P \in \mathcal{P}(\mathcal{H}_A), Q \in \mathcal{P}(\mathcal{H}_B)} \alpha_{PQ} (P \otimes Q)$$

$$= \sum_{P \in \mathcal{P}(\mathcal{H}_A)} \left(P \otimes \left(\sum_{Q \in \mathcal{P}(\mathcal{H}_B)} \alpha_{PQ} Q \right) \right)$$

$$= \sum_{P \in \mathcal{P}(\mathcal{H}_A)} \left(P \otimes M^P \right),$$

where $M^P \overset{\mathrm{def}}{=} \sum_{Q \in \mathcal{P}(\mathcal{H}_B)} \alpha_{PQ} Q$. It is easily seen that

$$\rho_B = \mathrm{Tr}_A(\rho_{AB}) = \mathrm{Tr}(\mathbb{I}_A) M^{\mathbb{I}_A}. \qquad (4)$$

Then, we have that

$$\frac{1}{|\mathcal{P}(\mathcal{H}_A)|} \sum_{Q \in \mathcal{P}(\mathcal{H}_A)} (Q \otimes \mathbb{I}) \left(\sum_{P \in \mathcal{P}(\mathcal{H}_A)} \left(P \otimes M^P\right) \right) (Q^\dagger \otimes \mathbb{I})$$

$$= \sum_{P \in \mathcal{P}(\mathcal{H}_A)} \left(\frac{1}{|\mathcal{P}(\mathcal{H}_A)|} \sum_{Q \in \mathcal{P}(\mathcal{H}_A)} (QPQ^\dagger) \otimes M^P \right)$$

$$= \sum_{P \in \mathcal{P}(\mathcal{H}_A) \setminus \mathbb{I}_A} \left(\frac{1}{|\mathcal{P}(\mathcal{H}_A)|} \sum_{Q \in \mathcal{P}(\mathcal{H}_A)} (QPQ^\dagger) \otimes M^P \right)$$

$$+ \sum_{P = \mathbb{I}_A} \left(\frac{1}{|\mathcal{P}(\mathcal{H}_A)|} \sum_{Q \in \mathcal{P}(\mathcal{H}_A)} (QPQ^\dagger) \otimes M^P \right)$$

$$= \mathbb{I}_A \otimes M^{\mathbb{I}_A} \hspace{6cm} \text{(Fact 14)}$$

$$= U_A \otimes \rho_B. \hspace{6cm} \text{(Equation (4))}$$

$\square$

The proof of the next fact follows similarly to that of Fact 16 using Fact 15.

Fact 17 (1-design). *Let ρ_{AB} be a state. Let $\mathcal{SC}(\mathcal{H}_A)$ be the subgroup of Clifford group as defined in Fact 10. Then,*

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C \otimes \mathbb{I})\rho_{AB}(C^\dagger \otimes \mathbb{I}) = U_A \otimes \rho_B.$$

2.2.5   The transpose method

The transpose method (see, e.g., [Ozo16]) is one of the most important tools for manipulating maximally entangled states. Note that the canonical purification of a maximally mixed state $\rho_A = U_A$, denoted $\rho_{A\hat{A}}$, is a maximally entangled state. Roughly speaking, the transpose method corresponds to the statement that some local action on one half of the maximally entangled state (say register A) is equivalent to performing the transpose of the same action on the other half of that state (register $\hat{A}$). We now state this formally.

Fact 18 (Transpose method). *Let $\rho_{A\hat{A}}$ be the canonical purification of $\rho_A = U_A$. For any $M \in \mathcal{L}(\mathcal{H}_A)$ it holds that*

$$(M \otimes \mathbb{I}_{\hat{A}})\rho_{A\hat{A}}(M^\dagger \otimes \mathbb{I}_{\hat{A}}) = (\mathbb{I}_A \otimes M^T)\rho_{A\hat{A}}(\mathbb{I}_A \otimes (M^T)^\dagger).$$

2.3   Quantum-secure randomness extractors

Randomness extractors are key objects in our constructions of non-malleable codes and secret sharing schemes. We introduce the relevant notions and auxiliary results here.

2.3.1 Min-entropy and weak sources

This section introduces information-theoretic formalism useful for our definitions of randomness extractors.

Definition 17 (Min-entropy)**.** *Given a state ρ_{XE}, the min-entropy of X conditioned on E, denoted by $\mathrm{H}_{\min}(X|E)_\rho$, is defined as*

$$\mathrm{H}_{\min}(X|E)_\rho = -\inf_{\sigma_E \in \mathcal{D}(\mathcal{H}_E)} \mathrm{D}_{\max}(\rho_{XE} \| \mathbb{I}_X \otimes \sigma_E).$$

We will require the following fact about the min-entropy.

Fact 19 ([CLW14, Lemma 2.14])**.** *Let $\Phi : \mathcal{L}(\mathcal{H}_M) \to \mathcal{L}(\mathcal{H}_{M'})$ be a CPTP map and define $\sigma_{XM'} = (\mathbb{I} \otimes \Phi)(\rho_{XM})$. We have that*
$$\mathrm{H}_{\min}\left(X\middle|M'\right)_\sigma \geq \mathrm{H}_{\min}(X|M)_\rho.$$

The formalism of qpa-states from [BJK21] will be useful when building leakage-resilient secret sharing schemes.

Definition 18 (qpa-state)**.** *A pure state $\sigma_{X\hat{X}Y\hat{Y}W_1W_2}$ with XY classical and $\hat{X}$ and $\hat{Y}$ copies of X and Y, respectively, is a (k_1, k_2)-qpa-state if*

$$\mathrm{H}_{\min}\left(X\middle|W_2Y\hat{Y}\right)_\sigma \geq k_1 \quad \text{and} \quad \mathrm{H}_{\min}\left(Y\middle|W_1X\hat{X}\right)_\sigma \geq k_2.$$

2.3.2 Quantum-secure 2-source extractors

A 2-source extractor transforms any two independent weak sources of randomness into an unbiased random string, provided that the input sources contain enough min-entropy. We will use the fact that the inner product function $\mathsf{IP} : \mathbb{F}_q^N \times \mathbb{F}_q^N \to \mathbb{F}_q$ given by

$$\mathsf{IP}(x, y) = \sum_{i=1}^N x_i y_i,$$

with operations performed over $\mathbb{F}_q$, is a 2-source extractor for qpa-states with good properties. This is captured in the following fact.

Fact 20 ([BJK21, Claim 5])**.** *Let $\rho_{X\hat{X}Y\hat{Y}W_1W_2}$ be an arbitrary (k_1, k_2)-qpa-state with $X, Y \in \mathbb{F}_q^N$ and*

$$k_1 + k_2 \geq (N + 1) \log q + 8 \log(1/\varepsilon) + 40.$$

Set $Z = \mathsf{IP}(X, Y)$. We have that

$$\|\rho_{ZXW_1} - U_Z \otimes \rho_{XW_1}\|_1 \leq \varepsilon \quad \text{and} \quad \|\rho_{ZYW_2} - U_Z \otimes \rho_{YW_2}\|_1 \leq \varepsilon,$$

where U_Z is uniformly distributed over $\mathbb{F}_q$.

2.3.3 Quantum-secure 2-source non-malleable extractors

Roughly speaking, a 2-source non-malleable extractor nmExt takes as input two (not necessarily) uniformly random and independent strings X and Y and outputs a string $R = \mathsf{nmExt}(X, Y)$ that is statistically close to uniform distribution. It is called *non-malleable* because learning $\mathsf{nmExt}(f(X), g(Y))$ for any known tampering functions f and g (without fixed points) reveals essentially nothing about $R = \mathsf{nmExt}(X, Y)$, in the sense that R should still be close to uniformly random given the tampered version $\mathsf{nmExt}(f(X), g(Y))$. We may thus see (X, Y) as a form of split-state encoding of R. Since our split-state tampering adversaries have quantum capabilities *and* access to shared quantum entanglement, we cannot use an arbitrary classical 2-source non-malleable extractor to generate R. Instead, we make use of an explicit *quantum-secure* 2-source non-malleable extractor recently constructed by Batra, Boddu, and Jain [BBJ23], which remains secure against such quantum adversaries and whose properties we detail below.

Fact 21 (Quantum-secure 2-source non-malleable extractor [BBJ23]). *Consider the split-state tampering experiment in Figure 4 with a split-state tampering adversary $\mathcal{A} = (U, V, |\psi\rangle_{W_1 W_2})$. Based on this figure, define $p_{\mathsf{same}} = \Pr[(X, Y) = (X', Y')]_{\hat{\rho}}$ and the conditioned quantum states*

$$\rho^{\mathsf{same}} = (\mathsf{nmExt} \otimes \mathsf{nmExt})(\hat{\rho}|(X, Y) = (X', Y'))$$

and

$$\rho^{\mathsf{tamp}} = (\mathsf{nmExt} \otimes \mathsf{nmExt})(\hat{\rho}|(X, Y) \neq (X', Y')).$$

For any given constant $\delta > 0$, there exists an explicit function $\mathsf{nmExt} : \{0,1\}^n \times \{0,1\}^{\delta n} \to \{0,1\}^r$ with output length $r = (1/2 - \delta)n$ such that for independent sources $X \leftarrow \{0,1\}^n$ and $Y \leftarrow \{0,1\}^{\delta n}$ and any such split-state tampering adversary $\mathcal{A} = (U, V, |\psi\rangle_{W_1 W_2})$ it holds that

1. $\|\mathsf{nmExt}(X, Y)X - U_r \otimes U_n\|_1 \leq \varepsilon$ *and* $\|\mathsf{nmExt}(X, Y)Y - U_r \otimes U_{\delta n}\|_1 \leq \varepsilon$,

2. $p_{\mathsf{same}} \|\rho^{\mathsf{same}}_{RW_2} - U_r \otimes \rho^{\mathsf{same}}_{W_2}\|_1 + (1 - p_{\mathsf{same}}) \|\rho^{\mathsf{tamp}}_{RR'W_2} - U_r \otimes \rho^{\mathsf{tamp}}_{R'W_2}\|_1 \leq \varepsilon$,

with $\varepsilon = 2^{-n^{\Omega_\delta(1)}}$. Furthermore, $\mathsf{nmExt}(x, y)$ can be computed in time $\mathrm{poly}(n)$.

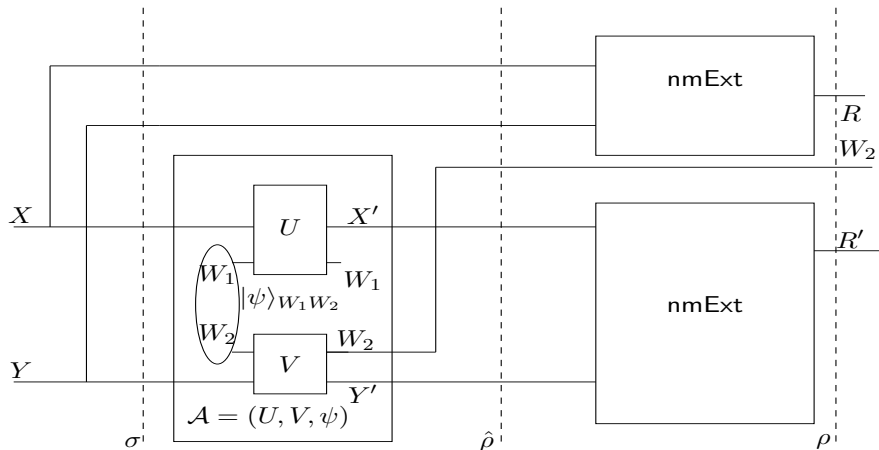
Figure 4: Split-state tampering experiment for quantum-secure 2-source non-malleable extractors.

Intuitively, Item 1 in Fact 21 guarantees that $R = \mathsf{nmExt}(X, Y)$ remains close to uniformly random even when one of the input sources X and Y is revealed. This property is usually called *strong extraction*. Item 2 spells out the non-malleability guarantees of nmExt: If the tampering attack does not change X and Y (i.e., $(X', Y') = (X, Y)$), then R should be close to uniformly random even given one of the updated entangled states shared by the adversaries attacking each source. On the other hand, if the tampering attack changed X and Y (i.e., $(X', Y') \neq (X, Y)$), then R should be close to uniformly random even given the additional output $R' = \mathsf{nmExt}(X', Y')$ *and* one of the updated entangled states.

2.4 Secret sharing schemes for quantum messages

Secret sharing schemes for quantum messages were first introduced in [HBB99, CGL99, KKI99]. As in the classical case, they allow a dealer to share a quantum message among p parties in a way that only authorized subsets of parties can reconstruct the quantum message, while unauthorized subsets of parties learn nothing about it. The no-cloning theorem imposes constraints on the type of access structures that can be realized by a secret sharing scheme for quantum messages. For example, there exists a t-out-of-p secret sharing scheme for quantum messages if and only if $t > p/2$. Conversely, it is known that any access structure that does not violate no-cloning[10] can be realized by a secret sharing scheme for quantum messages [Got00, Smi00].

We proceed to define secret sharing schemes for quantum messages and then state a known efficient construction of such threshold schemes due to Cleve, Gottesman, and Lo [CGL99] (a quantum analogue of Shamir's secret sharing scheme). We define secret sharing schemes for threshold access structure for simplicity, but this definition can be generalized to any access structure that does not violate no-cloning.

Let $\mathsf{qShare} : \mathcal{L}(\mathcal{H}_M) \to \mathcal{L}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2} \otimes \cdots \otimes \mathcal{H}_{S_p})$ and $\mathsf{qRec} : \mathcal{L}(\bigotimes_{i \in T} \mathcal{H}_{S_i}) \to \mathcal{L}(\mathcal{H}_M)$, be the sharing and reconstruction procedures respectively, where $\mathcal{L}(\mathcal{H})$ is the space of all linear operators in the Hilbert space $\mathcal{H}$. The reconstruction procedure qRec acts on any authorized subset of shares T to reconstruct the original message.

Definition 19 (Threshold secret sharing scheme for quantum messages)**.** *The coding scheme* $(\mathsf{qShare}, \mathsf{qRec})$ *is said to be a* t-*out-of-*p *secret sharing scheme for quantum messages if for any quantum message* $\sigma_M \in \mathcal{D}(\mathcal{H}_M)$ *(with canonical purification* $\sigma_{M\hat{M}}$*) the following two properties are satisfied:*

- **Correctness:** *For any* $T \subseteq [p]$ *such that* $|T| \geq t$ *it holds that*

$$\mathsf{qRec}(\mathsf{qShare}(\sigma_{M\hat{M}})_{S_T}) = \sigma_{M\hat{M}},$$

  where we recall that $S_T = (S_i)_{i \in T}$*.*

- **Perfect privacy:** *For any* $T \subseteq [p]$ *such that* $|T| \leq t - 1$ *it holds that*

$$(\mathsf{qShare}(\sigma))_{\hat{M}S_T} \equiv \sigma_{\hat{M}} \otimes \zeta_{S_T}.$$

  where ζ_{S_T} *is a fixed quantum state for every* $\sigma_{M\hat{M}}$*.*

---

[10] This amounts to requiring that if $T \subseteq [p]$ is authorized, then its complement $[p] \setminus T$ must be unauthorized.

Fact 22 ([CGL99]). *For any number of parties p and threshold t such that $p/2 < t \leq p$, there exists a t-out-of-p secret sharing scheme (qShare, qRec) for quantum messages of length b with share size at most $2\max(p, b)$, where both the sharing and reconstruction procedures run in time $\text{poly}(p, b)$.*

The following results state some useful properties satisfied by the threshold secret sharing scheme for quantum messages from Fact 22. The first fact states that the shares corresponding to any unauthorized set of parties are jointly uniformly distributed.

Fact 23 ([CGL99]). *Let (qShare, qRec) be the t-out-of-p secret sharing scheme from Fact 22. Let σ_M be a state such that $|M| = b$ and $\rho = \text{qShare}(\sigma_M)$. For any $T \subseteq [p]$ such that $|T| \leq t - 1$ it holds that*

$$\rho_{S_T} = U_{S_T}.$$

Lemma 1. *Let (qShare, qRec) be the t-out-of-p secret sharing scheme from Fact 22. Let $P \in \mathcal{P}(\mathcal{H}_M)$ be any non-identity Pauli operator. For any $T \subseteq [p]$ such that $|T| \leq t - 1$ it holds that $(\text{qShare}(P))_{S_T} = 0$.*

Proof. Consider the spectral decomposition of P. Let $P = \sum_{i=1}^{2^{|M|}} a_i |\psi\rangle\langle\psi|_i$. Note that half of the a_i's are exactly equal to 1, while the other half is -1. Since $\text{qShare}(|\psi\rangle\langle\psi|_i)_{S_T} = US_T$ for every i in $[2^{|M|}]$, we arrive at the desired result that $(\text{qShare}(P))_{S_T} = 0$. $\qquad\square$

The next lemma captures privacy properties in the presence of entangled quantum side information.

Lemma 2. *Let (qShare, qRec) be the t-out-of-p secret sharing scheme from Fact 22. Let σ_{EM} be a state such that $|M| = b$ and $\rho = \text{qShare}(\sigma_{EM})$. For any $T \subseteq [p]$ such that $|T| \leq t - 1$ it holds that*

$$\rho_{ES_T} \equiv \rho_E \otimes U_{S_T} \equiv \sigma_E \otimes U_{S_T}.$$

Proof. For each $Q \in \mathcal{P}(\mathcal{H}_M)$ and $Q' \in \mathcal{P}(\mathcal{H}_E)$ there exist coefficients $\alpha_{Q'Q}$ such that we may write

$$\sigma_{EM} = \sum_{Q \in \mathcal{P}(\mathcal{H}_M), Q' \in \mathcal{P}(\mathcal{H}_E)} \alpha_{Q'Q}(Q' \otimes Q)$$

$$= \sum_{Q \in \mathcal{P}(\mathcal{H}_M)} \left(\left(\sum_{Q' \in \mathcal{P}(\mathcal{H}_E)} \alpha_{Q'Q} Q' \right) \otimes Q \right)$$

$$= \sum_{Q \in \mathcal{P}(\mathcal{H}_M)} \left(G^Q \otimes Q \right),$$

where

$$G^Q \stackrel{\text{def}}{=} \sum_{Q' \in \mathcal{P}(\mathcal{H}_E)} \alpha_{Q'Q} Q'.$$

In particular, this implies that

$$\sigma_E = G^{\mathbb{I}_M} 2^{|M|}. \tag{5}$$

Then, we conclude that

$$
\begin{aligned}
\rho_{ES_T} &= \sum_{Q \in \mathcal{P}(\mathcal{H}_M)} \left(G^Q \otimes (\text{qShare}(Q))_{S_T} \right) \\
&= \sum_{Q = \mathbb{I}_M} \left(G^Q \otimes (\text{qShare}(Q))_{S_T} \right) + \sum_{Q \neq \mathbb{I}_M \wedge Q \in \mathcal{P}(\mathcal{H}_M)} \left(G^Q \otimes (\text{qShare}(Q))_{S_T} \right) \\
&= G^{\mathbb{I}_M} \otimes \left(\text{qShare} \left(2^{|M|} \cdot \frac{\mathbb{I}_M}{2^{|M|}} \right) \right)_{S_T} \\
&= G^{\mathbb{I}_M} \otimes 2^{|M|} U_{S_T} \\
&= \sigma_E \otimes U_{S_T}.
\end{aligned}
$$

The third equality above follows from Lemma 1. The fourth equality holds because of Fact 23. The final equality is a consequence of Equation (5). □

3 Split-state non-malleable codes for quantum messages

In this section, we describe and analyze our split-state non-malleable coding scheme for quantum messages. We begin by describing the encoding and decoding procedures Enc and Dec. In the analysis, we first show that (Enc, Dec) is an average-case non-malleable code with low error for quantum messages. This yields Theorem 1. Then, to conclude the argument and obtain Theorem 2, we show that every such average-case non-malleable code is also *worst-case* split-state non-malleable at the price of a blow-up in the error as a function of the input quantum message length.

3.1 Our candidate coding scheme for quantum messages

We proceed to describe our explicit candidate coding scheme for quantum messages. Suppose that we wish to encode a quantum state σ_M with canonical purification $\sigma_{M\hat{M}}$. Let $b = |M|$ denote the message length and fix an arbitrary constant $\delta > 0$. We will invoke the explicit quantum-secure 2-source ε-non-malleable extractor $\text{nmExt} : \{0,1\}^\ell \times \{0,1\}^{\delta\ell} \to \{0,1\}^r$ guaranteed by Fact 21 with output length r satisfying

$$
r = (1/2 - \delta)\ell \geq 5b \tag{6}
$$

and error

$$
\varepsilon = 2^{-\ell^{\Omega_\delta(1)}},
$$

where $\Omega_\delta(\cdot)$ hides constants which depend only on δ.

The encoding CPTP map Enc works as follows on input σ_M:

1. Sample classical bitstrings $X \leftarrow \{0,1\}^\ell$ and $Y \leftarrow \{0,1\}^{\delta\ell}$;

2. Compute the classical key $R = \text{nmExt}(X, Y) \in \{0,1\}^r$;

3. Let $\mathcal{SC}(\mathcal{H}_M)$ be the subgroup of the Clifford group described in Fact 10 and Samp be the associated sampling procedure. Compute $C_R = \text{Samp}(R)$ and the masked state $\psi_Z = C_R \sigma_M C_R^\dagger$. Note that the constraint in Equation (6) guarantees that R is long enough to sample such a Clifford operator as per Fact 10.

4. Output registers X and (Y, Z) as the two parts of the split-state encoding. Note that X and Y are classical strings while Z is a quantum state.

It is clear that Enc can be computed efficiently if nmExt is explicit. The decoding procedure Dec is straightforward, and proceeds as follows on input possibly tampered registers $(X, Y) \to (X', Y')$ and $\psi_Z \to \tau_Z$:

1. Compute the candidate key $R' = \mathsf{nmExt}(X', Y')$;

2. Let τ_Z denote the possibly tampered quantum state stored in register Z. Then, compute the candidate message $\eta_M = C_{R'}^\dagger \tau_Z C_{R'}$ where, as in the encoding procedure Enc above, $C_{R'} = \mathsf{Samp}(R')$ with Samp the sampling procedure corresponding to the subgroup $\mathcal{SC}(\mathcal{H}_M)$ of the Clifford group from Fact 10;

3. Output η_M.

It is easy to check that this coding scheme (Enc, Dec) satisfies the basic correctness property

$$\mathrm{Dec}(\mathrm{Enc}(\sigma_{M\hat{M}})) = \sigma_{M\hat{M}}.$$

3.2 Average-case non-malleability

In this section, we show that the coding scheme (Enc, Dec) described in Section 3.1 is average-case non-malleable with low-error. More precisely, we prove the following result.

Theorem 4 (Average-case non-malleable codes with constant rate). *For any fixed constant $\delta > 0$, the coding scheme* (Enc, Dec) *described in Section 3.1 with codewords of length n and message size $b \leq \left(\frac{1}{11} - \delta\right) n$ is average-case ε'-non-malleable with $\varepsilon' = 2^{-n^{\Omega_\delta(1)}}$. Moreover, both* Enc *and* Dec *can be computed in time* $\mathrm{poly}(n)$.

The claim about the computational complexity of Enc and Dec in Theorem 4 can be easily verified from the description in Section 3.1, using the fact that the codeword length n satisfies $n = O(\ell)$.

We prove the remainder of Theorem 4 through a sequence of lemmas. Throughout this proof we assume that C_R, the Clifford operator sampled from R via the sampling procedure Samp from Fact 10 used in Step 3 of Enc(σ) in Section 3.1, is uniformly distributed over $\mathcal{SC}(\mathcal{H}_M)$. Based on Equation (3) in Fact 10, this assumption will lead to an additive factor of 2^{-2b} in the final non-malleability error, which we add at the end of our argument.

For ease of readability, a detailed diagram of the complete split-state tampering experiment on (Enc, Dec) in Figure 5.

Taking into account the notation from Figure 5, in order to prove Theorem 4 it suffices to show that for any split-state adversary $\mathcal{A} = (U, V, \psi)$ and $\sigma_{M\hat{M}}$ maximally entangled it holds that

$$(\sigma_3)_{\hat{M}M} \approx_{\varepsilon' = 2^{-n^{\Omega_\delta(1)}}} p_\mathcal{A} \sigma_{\hat{M}M} + (1 - p_\mathcal{A})(U_{\hat{M}} \otimes \gamma_M^\mathcal{A}), \tag{7}$$

where $(p_\mathcal{A}, \gamma_M^\mathcal{A})$ depend only on the split-state adversary $\mathcal{A}$.

We begin by noting that in order to establish Equation (7) we can equivalently consider the modified tampering experiment described in Figure 6, where the (transposed) Clifford operator is applied to $\sigma_{\hat{M}}$ instead. More precisely, we have the following lemma.

Lemma 3. *For any fixed split-state adversary $\mathcal{A}$ it holds that the states $\rho, \rho_1, \rho_2, \rho_3$ in Figure 6 are equal to $\sigma, \sigma_1, \sigma_2, \sigma_3$ in Figure 5.*

Proof. The desired statement follows if we show that σ_1 and ρ_1 are equal. This is a direct consequence of the transpose method (Fact 18). □

We can further note that delaying the generation of R and the application of the corresponding Clifford operator C_R^T on the $\hat{M}$ register until the very end has no effect on the final state. Therefore, we can focus on the modified tampering experiment described in Figure 7. We capture this formally in the next brief lemma statement.

Lemma 4. *For any fixed split-state adversary $\mathcal{A}$ it holds that the final state θ_4 in Figure 7 is equal to the final state ρ_3 in Figure 6.*

In particular, combining Lemmas 3 and 4 implies that to establish Equation (7) it suffices to show that for any split-state adversary $\mathcal{A} = (U, V, \psi)$ and $\theta_{M\hat{M}}$ maximally entangled it holds that

$$(\theta_4)_{\hat{M}M} \approx_{\varepsilon'} p_{\mathcal{A}} \theta_{\hat{M}M} + (1 - p_{\mathcal{A}})(U_{\hat{M}} \otimes \gamma_M^{\mathcal{A}}), \tag{8}$$

where $(p_{\mathcal{A}}, \gamma_M^{\mathcal{A}})$ depend only on the split-state adversary $\mathcal{A}$. Here, the states $\theta, \theta_1, \theta_2, \theta_3, \theta_4$ correspond to the intermediate states of the modified tampering experiment in Figure 7.

We now set up some helpful definitions before proceeding to the next lemma. We may write θ_2 as

$$\theta_2 = (U \otimes V)(\theta_1 \otimes |\psi\rangle\langle\psi|_{W_1 W_2})(U \otimes V)^{\dagger}.$$

Our analysis will proceed by cases, depending on whether the X and Y registers are modified by the tampering experiment in Figure 7 (i.e., $XY \neq X'Y'$) or not. To this end, we consider two different conditionings of θ_2 based on these two cases. More precisely, taking into account Definition 5, we define

$$\theta_2^{\mathsf{tamp}} = \theta_2 | (XY \neq X'Y')$$

and

$$\theta_2^{\mathsf{same}} = \theta_2 | (XY = X'Y').$$

Note that we may write $\theta_2 = p_{\mathsf{same}} \theta_2^{\mathsf{same}} + (1 - p_{\mathsf{same}}) \theta_2^{\mathsf{tamp}}$, where $p_{\mathsf{same}} = \Pr[XY = X'Y']_{\theta_2}$ is the probability that XY are not modified in the tampering experiment from Figure 7.

Further taking into account that

$$\theta_3 = (\mathsf{nmExt}_{XY} \otimes \mathsf{nmExt}_{X'Y'})\theta_2,$$

let

$$\theta_3^{\mathsf{tamp}} = (\mathsf{nmExt}_{XY} \otimes \mathsf{nmExt}_{X'Y'})\theta_2^{\mathsf{tamp}}$$

and

$$\theta_3^{\mathsf{same}} = (\mathsf{nmExt}_{XY} \otimes \mathsf{nmExt}_{X'Y'})\theta_2^{\mathsf{same}}.$$

Let $D_{R\hat{M}}$ denote the controlled Clifford operator C_R^T acting on register $\hat{M}$. Similarly, let $\tilde{D}_{R'Z}$ denote the controlled Clifford operator $C_{R'}^{\dagger}$ acting on register Z. We can then write

$$(\theta_4)_{\hat{M}M} = (D_{R\hat{Z}} \otimes \tilde{D}_{R'Z})(\theta_3)_{RR'Z\hat{M}}(D_{R\hat{Z}}^{\dagger} \otimes \tilde{D}_{R'Z}^{\dagger}).$$

Analogously to the previous cases, we define

$$(\theta_4^{\mathsf{tamp}})_{\hat{M}M} \stackrel{\text{def}}{=} (D_{R\hat{Z}} \otimes \tilde{D}_{R'Z})(\theta_3^{\mathsf{tamp}})_{RR'Z\hat{M}}(D_{R\hat{Z}}^{\dagger} \otimes \tilde{D}_{R'Z}^{\dagger}) \tag{9}$$

and

$$(\theta_4^{\mathsf{same}})_{\hat{M}M} \stackrel{\text{def}}{=} (D_{R\hat{Z}} \otimes \tilde{D}_{R'Z})(\theta_3^{\mathsf{same}})_{RR'Z\hat{M}}(D_{R\hat{Z}}^{\dagger} \otimes \tilde{D}_{R'Z}^{\dagger}). \tag{10}$$

Recall from Equation (8) that, based on Lemmas 3 and 4, our end goal is to show that

$$(\theta_4)_{\hat{M}M} \approx_{\varepsilon'} p_{\mathcal{A}} \theta_{\hat{M}M} + (1 - p_{\mathcal{A}})(U_{\hat{M}} \otimes \gamma_M^{\mathcal{A}})$$

for some quantity $p_{\mathcal{A}} \in [0,1]$ and state $\gamma_M^{\mathcal{A}}$ depending only on the split-state adversary $\mathcal{A}$. Towards establishing this, we begin by writing

$$(\theta_4)_{\hat{M}M} = p_{\mathsf{same}}(\theta_4^{\mathsf{same}})_{\hat{M}M} + (1 - p_{\mathsf{same}})(\theta_4^{\mathsf{tamp}})_{\hat{M}M}.$$

We will focus on each of the two terms on the right-hand side of this equation separately. We invoke the two lemmas below, whose proofs we defer to later dedicated sections.

The first lemma is relevant for handling θ_4^{tamp}, and intuitively states that when tampering occurs and $X'Y' \neq XY$ the outcome of the tampering experiment is close (in trace distance) to being an unentangled message.

Lemma 5. *We have that*

$$(1 - p_{\mathsf{same}}) \left\| (\theta_4^{\mathsf{tamp}})_{\hat{M}M} - U_{\hat{M}} \otimes (\theta_4^{\mathsf{tamp}})_M \right\|_1 \leq \varepsilon.$$

The second lemma is relevant for handling θ_4^{same}, and intuitively states that when $X'Y' = XY$ the outcome of the tampering experiment is close (in trace distance) to being either the original message or a completely independent and unentangled message.

Lemma 6. *There exists a constant $p_{\mathsf{epr}} \in [0,1]$ depending only on the split-state adversary $\mathcal{A}$ such that*

$$p_{\mathsf{same}} \cdot \left\| (\theta_4^{\mathsf{same}})_{\hat{M}M} - \left(p_{\mathsf{epr}} \cdot \theta_{\hat{M}M} + (1 - p_{\mathsf{epr}})(U_{\hat{M}} \otimes U_M) \right) \right\|_1 \leq \varepsilon + 2 \cdot 4^{-b}.$$

Proofs of Lemmas 5 and 6 can be found in Sections 3.2.1 and 3.2.2, respectively. We now show how to wrap up the argument and establish Equation (8) using Lemmas 5 and 6. We have

$$(\theta_4)_{\hat{M}M} = p_{\mathsf{same}}(\theta_4^{\mathsf{same}})_{\hat{M}M} + (1 - p_{\mathsf{same}})(\theta_4^{\mathsf{tamp}})_{\hat{M}M}$$

$$\approx_{\varepsilon + 2 \cdot 4^{-b}} p_{\mathsf{same}} \left(p_{\mathsf{epr}} \theta_{M\hat{M}} + (1 - p_{\mathsf{epr}})(U_{\hat{M}} \otimes U_M) \right) + (1 - p_{\mathsf{same}})(\theta_4^{\mathsf{tamp}})_{\hat{M}M} \tag{11}$$

$$\approx_{\varepsilon} p_{\mathsf{same}} \left(p_{\mathsf{epr}} \cdot \theta_{M\hat{M}} + (1 - p_{\mathsf{epr}})(U_{\hat{M}} \otimes U_M) \right) + (1 - p_{\mathsf{same}})(U_{\hat{M}} \otimes (\theta_4^{\mathsf{tamp}})_M), \tag{12}$$

where Equation (11) follows from Lemma 6 and Equation (12) follows from Lemma 5. Combining Equations (11) and (12) with a triangle inequality shows that

$$(\theta_4)_{\hat{M}M} \approx_{2(\varepsilon + 4^{-b})} p_{\mathsf{same}} \left(p_{\mathsf{epr}} \cdot \theta_{M\hat{M}} + (1 - p_{\mathsf{epr}})(U_{\hat{M}} \otimes U_M) \right) + (1 - p_{\mathsf{same}})(U_{\hat{M}} \otimes (\theta_4^{\mathsf{tamp}})_M)$$

$$= p_{\mathsf{same}} \cdot p_{\mathsf{epr}} \cdot \theta_{M\hat{M}}$$

$$+ (1 - p_{\mathsf{same}} \cdot p_{\mathsf{epr}}) \left(U_{\hat{M}} \otimes \left(\frac{p_{\mathsf{same}}(1 - p_{\mathsf{epr}})}{1 - p_{\mathsf{same}} \cdot p_{\mathsf{epr}}} \cdot U_M + \frac{1 - p_{\mathsf{same}}}{1 - p_{\mathsf{same}} \cdot p_{\mathsf{epr}}} \cdot (\theta_4^{\mathsf{tamp}})_M \right) \right). \tag{13}$$

Consider setting

$$p_{\mathcal{A}} = p_{\mathsf{same}} \cdot p_{\mathsf{epr}}$$

and

$$\gamma_M^{\mathcal{A}} = \frac{p_{\mathsf{same}}(1 - p_{\mathsf{epr}})}{1 - p_{\mathsf{same}} \cdot p_{\mathsf{epr}}} \cdot U_M + \frac{1 - p_{\mathsf{same}}}{1 - p_{\mathsf{same}} \cdot p_{\mathsf{epr}}} \cdot (\theta_4^{\mathsf{tamp}})_M$$

in Equation (13). We claim that $p_{\mathcal{A}}$ and $\gamma_M^{\mathcal{A}}$ depend only on the split-state adversary $\mathcal{A}$. This holds because:

- $p_{\mathsf{same}} = \Pr[XY = X'Y']_{\theta_2}$ is a function of $\mathcal{A}$ and (X, Y), which are sampled independently of the message σ_M;

- Lemma 6 guarantees that p_{epr} is a function of $\mathcal{A}$ only;

- The state $(\theta_4^{\mathsf{tamp}})_M$ is a function of $(\theta_3^{\mathsf{tamp}})_{ZX'Y'}$, and one can prepare the latter by running an independent tampering experiment on registers $XYZ = U_l \otimes U_{\delta l} \otimes U_Z$.

Therefore, we conclude that both $p_{\mathcal{A}}$ and $\gamma_M^{\mathcal{A}}$ only depend on $\mathcal{A}$. In this case, we can write

$$(\theta_4)_{\hat{M}M} \approx_{2(\varepsilon + 4^{-b})} p_{\mathcal{A}} \cdot \theta_{M\hat{M}} + (1 - p_{\mathcal{A}}) \left(U_{\hat{M}} \otimes \gamma_M^{\mathcal{A}} \right).$$

By Lemmas 3 and 4, this implies that we have

$$(\sigma_3)_{\hat{M}M} \approx_{2(\varepsilon + 4^{-b})} p_{\mathcal{A}} \cdot \sigma_{M\hat{M}} + (1 - p_{\mathcal{A}}) \left(U_{\hat{M}} \otimes \gamma_M^{\mathcal{A}} \right) \tag{14}$$

in the original tampering experiment from Figure 5.

Setting parameters for Theorem 4. To conclude the proof of Theorem 4, it remains to argue that, given any constant $\delta > 0$, the coding scheme (Enc, Dec) is average-case ($\varepsilon' = 2^{-n^{\Omega_\delta(1)}}$)-non-malleable for message length $b \leq (\frac{1}{11} - \delta)n$.

Note that the total codeword length is

$$n = |X| + |Y| + |Z| = \ell + \delta\ell + b = (1 + \delta + 1/10 + \delta/5)\ell$$

and that the error ε of nmExt satisfies $\varepsilon = 2^{-\ell^{\Omega_\delta(1)}} = 2^{-n^{\Omega_\delta(1)}}$, since $n = O(\ell)$. Furthermore, recall from Equation (6) in Section 3.1 that we may set the message length to be as large as $r/5 = \frac{(1/2 - \delta)\ell}{5}$. In fact, even if $b < r/5$ we may always extend a message so that its length is exactly $b' = r/5$ by appending dummy independent uniformly random bits to it. Since the length-b message σ_M is maximally mixed, the resulting extended length-b' message will also be maximally mixed. Therefore, taking into account Equation (14) and recalling that our argument in this section assumed that the Clifford operator C_R is sampled uniformly at random from $\mathcal{SC}(\mathcal{H}_A)$ while Fact 10 only guarantees that $C_R \approx_{2^{-b'}} U_{\mathcal{SC}(\mathcal{H}_A)}$ with $U_{\mathcal{SC}(\mathcal{H}_A)}$ uniformly distributed over $\mathcal{SC}(\mathcal{H}_A)$, the resulting coding scheme is average-case ε'-non-malleable with

$$\varepsilon' = 2(\varepsilon + 4^{-b'}) + 2^{-2b'} = 2^{-n^{\Omega_\delta(1)}},$$

as desired.

Finally, simple algebraic manipulation yields

$$r/5 = \frac{(1/2 - \delta)\ell}{5} \geq \left(\frac{1}{11} - c \right) n$$

for some constant $c = O(\delta)$. This means that we may encode messages of length at least $\left(\frac{1}{11} - c \right) n$, and the constant $c > 0$ can be made arbitrarily small. This concludes the proof of Theorem 4.
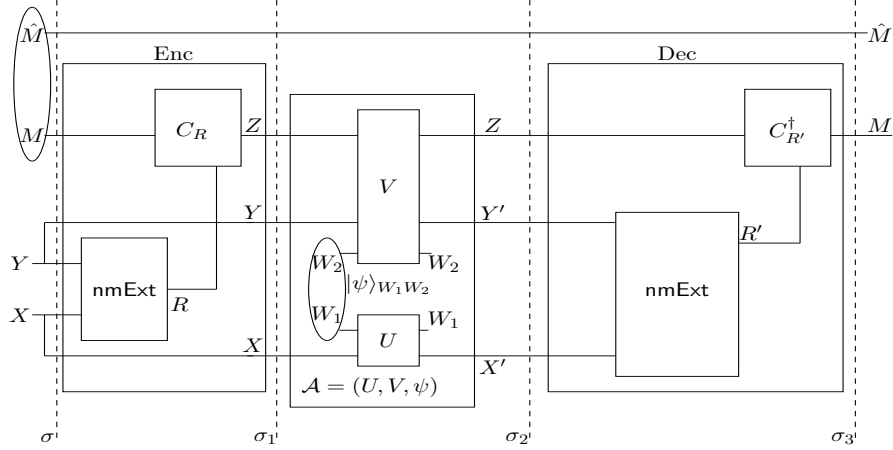
36

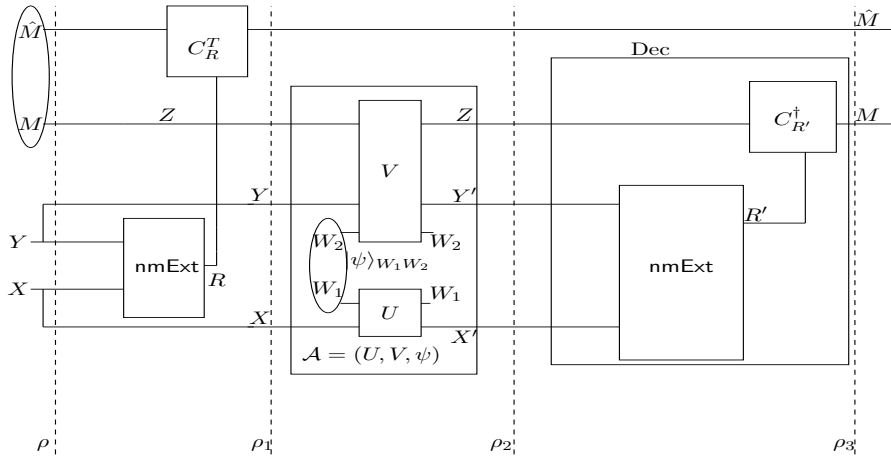Figure 5: Split-state tampering experiment.

Figure 6: Split-state tampering experiment after applying the transpose method.
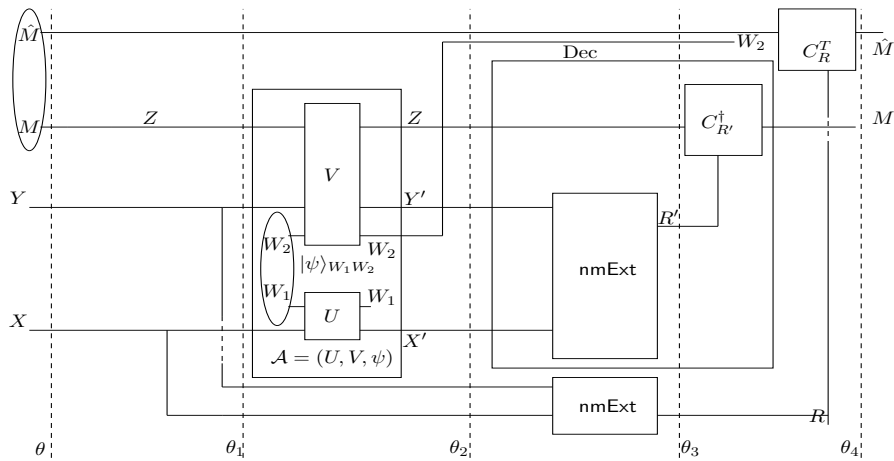

Figure 7: Split-state tampering experiment after applying the transpose method and delaying both the generation of register R and the application of the corresponding Clifford operator.

3.2.1 Proof of Lemma 5

We begin by writing

$$(\theta_3)_{RR'W_2Z\hat{M}} = p_{\text{same}}(\theta_3^{\text{same}})_{RR'W_2Z\hat{M}} + (1 - p_{\text{same}})(\theta_3^{\text{tamp}})_{RR'W_2Z\hat{M}}.$$

Observe that $(\theta_1)_{\hat{M}M}$ is a pure state (thus independent of other registers in θ_1). We invoke Item 2 of Fact 21 with the assignment of states/registers (the states/registers on the left below are from the statement of Fact 21, while the states/registers on the right are those from this proof)

$$\left(\sigma, \hat{\rho}, \rho, \rho^{\text{same}}, \rho^{\text{tamp}}, W_1, W_2, X, Y\right) \leftarrow \left(\theta_1, \theta_2, \theta_3, \theta_3^{\text{same}}, \theta_3^{\text{tamp}}, W_1, W_2M\hat{M}, X, Y\right)$$

to conclude that

$$p_{\text{same}}\|(\theta_3^{\text{same}})_{RW_2Z\hat{M}} - U_r \otimes (\theta_3^{\text{same}})_{W_2Z\hat{M}}\|_1 +$$
$$(1 - p_{\text{same}})\|(\theta_3^{\text{tamp}})_{RR'W_2Z\hat{M}} - U_r \otimes (\theta_3^{\text{tamp}})_{R'W_2Z\hat{M}})\|_1 \leq \varepsilon. \quad (15)$$

In particular, it holds that

$$(1 - p_{\text{same}})\|(\theta_3^{\text{tamp}})_{RR'W_2Z\hat{M}} - U_m \otimes (\theta_3^{\text{tamp}})_{R'W_2Z\hat{M}}\|_1 \leq \varepsilon. \quad (16)$$

As a result, we have that

$$(1 - p_{\text{same}})\|(\theta_4^{\text{tamp}})_{\hat{M}M} - U_{\hat{M}} \otimes (\theta_4^{\text{tamp}})_M\|_1$$
$$= (1 - p_{\text{same}})\|(\mathbb{I} \otimes D)(\tilde{D} \otimes \mathbb{I})(\theta_3^{\text{tamp}})_{RR'Z\hat{M}}(\tilde{D}^\dagger \otimes \mathbb{I})(\mathbb{I} \otimes D)$$
$$- (\mathbb{I} \otimes D)\left(U_r \otimes (\tilde{D} \otimes \mathbb{I})(\theta_3^{\text{tamp}})_{R'Z\hat{M}}(\tilde{D}^\dagger \otimes \mathbb{I})\right)(\mathbb{I} \otimes D)\|_1$$
$$\leq (1 - p_{\text{same}})\|(\tilde{D} \otimes \mathbb{I})(\theta_3^{\text{tamp}})_{RR'Z\hat{M}}(\tilde{D}^\dagger \otimes \mathbb{I}) - U_r \otimes (\tilde{D} \otimes \mathbb{I})(\theta_3^{\text{tamp}})_{R'Z\hat{M}}(\tilde{D}^\dagger \otimes \mathbb{I})\|_1 \quad \text{(Fact 17 and Fact 4)}$$
$$\leq (1 - p_{\text{same}})\|(\theta_3^{\text{tamp}})_{RR'Z\hat{M}} - U_r \otimes (\theta_3^{\text{tamp}})_{R'Z\hat{M}}\|_1 \quad \text{(Fact 4)}$$
$$\leq (1 - p_{\text{same}})\|(\theta_3^{\text{tamp}})_{RR'W_2Z\hat{M}} - U_r \otimes (\theta_3^{\text{tamp}})_{R'W_2Z\hat{M}}\|_1 \quad \text{(Fact 4)}$$
$$\leq \varepsilon. \quad \text{(Equation (16))}$$

The first inequality invokes Fact 17 with the assignment of registers $(A, B, \rho) \longleftarrow (\hat{M}, M, \theta_4^{\text{tamp}})$, where the registers on the left hand side correspond to those in the statement Fact 17 and the registers on the right hand side are those used in this proof.

3.2.2 Proof of Lemma 6

Before we proceed to the proof of Lemma 6, we prove two auxiliary lemmas.

Lemma 7. *Let $\rho_{A\hat{A}}$ be the canonical purification of $\rho_A = U_A$, $\mathcal{SC}(\mathcal{H}_A)$ be the subgroup of Clifford group as defined in Fact 10, and $P, Q \in \mathcal{P}(\mathcal{H}_A)$ be any two Pauli operators. If $P \neq Q$, then*

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)(\mathbb{I} \otimes P)\rho_{A\hat{A}}(\mathbb{I} \otimes Q^\dagger)((C^T)^\dagger \otimes C) = 0.$$

Else, if $P = Q = \mathbb{I}_A$, then

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)(\mathbb{I} \otimes P)\rho_{A\hat{A}}(\mathbb{I} \otimes P^\dagger)((C^T)^\dagger \otimes C) = \rho_{A\hat{A}}.$$

Else, if $P = Q \neq \mathbb{I}_A$, then

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)(\mathbb{I} \otimes P)\rho_{A\hat{A}}(\mathbb{I} \otimes P^\dagger)((C^T)^\dagger \otimes C) \approx_{\frac{2}{|\mathcal{P}(\mathcal{H}_A)|}} \rho_A \otimes \rho_{\hat{A}}.$$

Proof. We have that

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)(\mathbb{I} \otimes P)\rho_{A\hat{A}}(\mathbb{I} \otimes Q^\dagger)((C^T)^\dagger \otimes C)$$

$$= \frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (\mathbb{I} \otimes C^\dagger P)(C^T \otimes \mathbb{I})\rho_{A\hat{A}}((C^T)^\dagger \otimes \mathbb{I})(\mathbb{I} \otimes Q^\dagger C)$$

$$= \frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (\mathbb{I} \otimes C^\dagger P)(\mathbb{I} \otimes C)\rho_{A\hat{A}}(\mathbb{I} \otimes C^\dagger)(\mathbb{I} \otimes Q^\dagger C) \qquad \text{(Fact 18)}$$

$$= \frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (\mathbb{I} \otimes C^\dagger PC)\rho_{A\hat{A}}(\mathbb{I} \otimes C^\dagger Q^\dagger C).$$

When $P \neq Q$ we can invoke Fact 13 to conclude that

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (\mathbb{I} \otimes C^\dagger PC)\rho_{A\hat{A}}(\mathbb{I} \otimes C^\dagger Q^\dagger C) = 0.$$

When $P = Q = \mathbb{I}_A$, it holds that

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (\mathbb{I} \otimes C^\dagger PC)\rho_{A\hat{A}}(\mathbb{I} \otimes C^\dagger P^\dagger C)$$

$$= \frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (\mathbb{I} \otimes C^\dagger C)\rho_{A\hat{A}}(\mathbb{I} \otimes C^\dagger C)$$

$$= \rho_{A\hat{A}}. \qquad (C^\dagger C = \mathbb{I})$$

Finally, when $P = Q \neq \mathbb{I}_A$ we have that

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (\mathbb{I} \otimes C^\dagger PC)\rho_{A\hat{A}}(\mathbb{I} \otimes C^\dagger P^\dagger C)$$

$$= \frac{1}{|\mathcal{P}(\mathcal{H}_A)| - 1} \sum_{Q \in \mathcal{P}(\mathcal{H}_A) \setminus \mathbb{I}} (\mathbb{I} \otimes Q)\rho_{A\hat{A}}(\mathbb{I} \otimes Q^\dagger) \qquad \text{(Fact 10)}$$

$$= \frac{|\mathcal{P}(\mathcal{H}_A)|(\rho_A \otimes \rho_{\hat{A}}) - \rho_{A\hat{A}}}{|\mathcal{P}(\mathcal{H}_A)| - 1}. \qquad \text{(Fact 16)}$$

The desired result follows since

$$\left\| \frac{|\mathcal{P}(\mathcal{H}_A)|(\rho_A \otimes \rho_{\hat{A}}) - \rho_{A\hat{A}}}{|\mathcal{P}(\mathcal{H}_A)| - 1} - (\rho_A \otimes \rho_{\hat{A}}) \right\|_1 \leq \frac{2}{|\mathcal{P}(\mathcal{H}_A)|}.$$

$\square$

Lemma 8. *Let $|\psi\rangle_{\hat{A}A}$ be the canonical purification of $\psi_A = U_A$, $\rho_{\hat{A}A}$ be any state, and $\mathcal{SC}(\mathcal{H}_A)$ be the subgroup of Clifford group as defined in* Fact 10. *Define $\Pi = |\psi\rangle\langle\psi|$. Then, we have that*

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)\rho_{\hat{A}A}((C^T)^\dagger \otimes C)$$

$$= \mathrm{Tr}(\Pi\rho)\psi + (1 - \mathrm{Tr}(\Pi\rho))\frac{|\mathcal{P}(\mathcal{H}_A)|(U_{\hat{A}} \otimes U_A) - \psi_{A\hat{A}}}{|\mathcal{P}(\mathcal{H}_A)| - 1}$$

$$\approx_{\frac{2}{4|A|}} \mathrm{Tr}(\Pi\rho)\psi + (1 - \mathrm{Tr}(\Pi\rho))(U_{\hat{A}} \otimes U_A). \quad (17)$$

Proof. Let $|\phi\rangle_{\hat{A}A}$ be an eigenvector of $\rho_{\hat{A}A}$. Consider the decomposition

$$|\phi\rangle_{\hat{A}A} = \sum_{P \in \mathcal{P}(\mathcal{H}_A)} \alpha_P(\mathbb{I} \otimes P)|\psi\rangle_{\hat{A}A},$$

where $\sum_{P \in \mathcal{P}(\mathcal{H}_A)} |\alpha_P|^2 = 1$. Define

$$\tau(P, Q) \overset{\text{def}}{=} (\mathbb{I} \otimes P)|\psi\rangle\langle\psi|(\mathbb{I} \otimes Q^\dagger).$$

Then, we have that

$$\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)|\phi\rangle\langle\phi|((C^T)^\dagger \otimes C)$$

$$= \frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)\left(\sum_{P,Q \in \mathcal{P}(\mathcal{H}_A)} \alpha_P \alpha_Q^* \tau(P, Q)\right)((C^T)^\dagger \otimes C)$$

$$= \sum_{P,Q \in \mathcal{P}(\mathcal{H}_A)} \alpha_P \alpha_Q^* \left(\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)\tau(P, Q)((C^T)^\dagger \otimes C)\right)$$

$$= \sum_{P,Q \in \mathcal{P}(\mathcal{H}_A) \wedge (P \neq Q)} \alpha_P \alpha_Q^* \left(\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)\tau(P, Q)((C^T)^\dagger \otimes C)\right)$$

$$+ \sum_{P,Q \in \mathcal{P}(\mathcal{H}_A) \wedge (P = Q = \mathbb{I}_A)} \alpha_P \alpha_Q^* \left(\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)\tau(P, Q)((C^T)^\dagger \otimes C)\right)$$

$$+ \sum_{P,Q \in \mathcal{P}(\mathcal{H}_A) \wedge (P = Q \neq \mathbb{I}_A)} \alpha_P \alpha_Q^* \left(\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)\tau(P, Q)((C^T)^\dagger \otimes C)\right)$$

$$= |\alpha_{\mathbb{I}_A}|^2 |\psi\rangle\langle\psi|$$

$$+ \sum_{P \in \mathcal{P}(\mathcal{H}_A) \setminus \mathbb{I}_A} |\alpha_P|^2 \left(\frac{1}{|\mathcal{SC}(\mathcal{H}_A)|} \sum_{C \in \mathcal{SC}(\mathcal{H}_A)} (C^T \otimes C^\dagger)\tau(P, P)((C^T)^\dagger \otimes C)\right)$$

$$= |\alpha_{\mathbb{I}_A}|^2 |\psi\rangle\langle\psi| + (1 - |\alpha_{\mathbb{I}_A}|^2)\left(\frac{|\mathcal{P}(\mathcal{H}_A)|(U_A \otimes U_{\hat{A}}) - \psi_{A\hat{A}}}{|\mathcal{P}(\mathcal{H}_A)| - 1}\right).$$

The last equality follows from Lemma 7. Now, the first equality in Equation (17) from the lemma statement follows by observing that $\rho_{\hat{A}A}$ is a convex combination of its eigenvectors, and the approximation in Equation (17) follows from Fact 6 by observing that

$$\left\| \frac{|\mathcal{P}(\mathcal{H}_A)|(U_A \otimes U_{\hat{A}}) - \psi_{A\hat{A}}}{|\mathcal{P}(\mathcal{H}_A)| - 1} - (U_A \otimes U_{\hat{A}}) \right\|_1 \leq \frac{2}{|\mathcal{P}(\mathcal{H}_A)|}.$$

$\square$

We are now ready to prove Lemma 6.

Proof of Lemma 6. Recall from Equation (15) that, in particular,

$$p_{\mathsf{same}}\|(\theta_3^{\mathsf{same}})_{RW_2 Z\hat{M}} - U_r \otimes (\theta_3^{\mathsf{same}})_{W_2 Z\hat{M}}\|_1 \leq \varepsilon. \tag{18}$$

Recall also that $\tilde{D}_{R'Z}$ denotes the controlled Clifford unitary $C_{R'}^\dagger$ acting on register Z and that $D_{R\hat{M}}$ denotes the controlled Clifford operator C_R^T acting on register $\hat{M}$.

By the conditioning in θ_3^{same}, we have that

$$\Pr[R = R']_{(\theta_3^{\mathsf{same}})} = 1.$$

Let Π denote the maximally entangled state in registers $Z\hat{M}$ and write $p_{\mathsf{epr}} = \mathrm{Tr}(\Pi(\theta_3^{\mathsf{same}})_{Z\hat{M}}))$. Consider the state $\tau_{RR'}$ such that $\Pr[R = R']_\tau = 1$ and $\tau_R = U_r$, and for ease of readability define

$$\beta \stackrel{\mathrm{def}}{=} \tau_{RR'} \otimes (\theta_3^{\mathsf{same}})_{Z\hat{M}} \quad ; \quad \gamma \stackrel{\mathrm{def}}{=} (\tilde{D} \otimes D)\beta(\tilde{D}^\dagger \otimes D^\dagger).$$

Intuitively, the states β and γ are "approximate" versions of $(\theta_3^{\mathsf{same}})_{RR'Z\hat{M}}$ and $(\theta_4^{\mathsf{same}})_{\hat{M}M}$ which are easier to reason about. Our argument proceeds in two steps. First, we show that $\gamma_{\hat{M}M}$ is close in trace distance to

$$\left(p_{\mathsf{epr}}\Pi + (1 - p_{\mathsf{epr}})(U_{\hat{M}} \otimes U_M)\right).$$

Then, we argue that $(\theta_4^{\mathsf{same}})_{\hat{M}M}$ and $\gamma_{\hat{M}M}$ are close in trace distance, and an application of the triangle inequality to these two statements finishes the proof (after arguing that p_{epr} depends only on $\mathcal{A}$). More formally, we have that

$$p_{\mathsf{same}}\|(\theta_4^{\mathsf{same}})_{\hat{M}M} - \left(p_{\mathsf{epr}}\Pi + (1 - p_{\mathsf{epr}})(U_{\hat{M}} \otimes U_M)\right)\|_1$$
$$\leq p_{\mathsf{same}}\|(\theta_4^{\mathsf{same}})_{\hat{M}M} - \gamma_{\hat{M}M}\|_1$$
$$\qquad + p_{\mathsf{same}}\|\gamma_{\hat{M}M} - \left(p_{\mathsf{epr}}\Pi + (1 - p_{\mathsf{epr}})(U_{\hat{M}} \otimes U_M)\right)\|_1$$
$$\leq p_{\mathsf{same}}\|(\theta_4^{\mathsf{same}})_{\hat{M}M} - \gamma_{\hat{M}M}\|_1 + 2 \cdot 4^{-|M|} \tag{19}$$
$$\leq p_{\mathsf{same}}\|(\tilde{D} \otimes D)(\theta_3^{\mathsf{same}})_{RR'\hat{M}M}(\tilde{D}^\dagger \otimes D^\dagger) - \gamma\|_1 + 2 \cdot 4^{-|M|} \tag{20}$$
$$\leq p_{\mathsf{same}}\|(\theta_3^{\mathsf{same}})_{RR'Z\hat{M}} - \tau_{RR'} \otimes (\theta_3^{\mathsf{same}})_{Z\hat{M}}\|_1 + 2 \cdot 4^{-|M|} \tag{21}$$
$$\leq p_{\mathsf{same}}\|(\theta_3^{\mathsf{same}})_{RZ\hat{M}} - U_r \otimes (\theta_3^{\mathsf{same}})_{Z\hat{M}}\|_1 + 2 \cdot 4^{-|M|} \tag{22}$$
$$\leq p_{\mathsf{same}}\|(\theta_3^{\mathsf{same}})_{RW_2 Z\hat{M}} - U_r \otimes (\theta_3^{\mathsf{same}})_{W_2 Z\hat{M}}\|_1 + 2 \cdot 4^{-|M|} \tag{23}$$
$$\leq \varepsilon + 2 \cdot 4^{-|M|}. \tag{24}$$

Equation (19) follows from Lemma 8 with the assignment of registers (the registers on the left below are from Lemma 8 and the registers on the right are the registers in this proof)

$$(\hat{A}, A, \rho) \longleftarrow (\hat{M}, Z, \theta_3^{\mathsf{same}}).$$

Equations (20) to (23) follow from Fact 4. We provide some more detail on Equation (22). The difference between the expressions in Equations (21) and (22) is that the (classical) register R' is removed. The stated inequality (which is even an equality) follows from data-processing because in the states θ_3^{same} and τ we have that R' is a copy of R, and so can be generated based on R. This is because in these states we have $R = \mathsf{nmExt}(X, Y)$, $R' = \mathsf{nmExt}(X', Y')$, and $(X, Y) = (X', Y')$. The final Equation (24) follows from Equation (18).

To conclude the proof, it remains to argue that p_{epr} depends only on the split-state adversary $\mathcal{A}$. This holds because p_{epr} is a function of the state $(\theta_3^{\mathsf{same}})_{Z\hat{M}}$, which can be prepared by running an independent tampering experiment with another maximally entangled state independent of the original input message. $\qquad\square$

3.3   From average-case to worst-case non-malleability

In this section, we show that every average-case non-malleable code is also worst-case non-malleable with larger error, provided that the message length is not too large. More precisely, we have the following.

Lemma 9. *If* (Enc, Dec) *is an average-case ε-non-malleable code for quantum messages of length b, then it is also a (worst-case) ε'-non-malleable code for quantum messages of length b, where $\varepsilon' = 2^b \cdot \varepsilon$.*

Combining Theorem 4 with Lemma 9 immediately implies the following result.

Theorem 5. *There exists a constant $c \in (0, 1)$ such that the following holds: The coding scheme* (Enc, Dec) *described in Section 3.1 with codewords of length n and message size $b \le n^c$ is (worst-case) ε-non-malleable with $\varepsilon = 2^{-n^{\Omega(1)}}$. Moreover, both Enc and Dec can be computed in time* poly(n).

Note that the only barrier towards obtaining a constant rate code in Theorem 5 is the fact that the average-case non-malleable code from Theorem 4 has error $\varepsilon = 2^{-n^{\Omega(1)}}$, where n is the codeword size. Therefore, Lemma 9 only allows for quantum messages of length up to $n^{\Omega(1)}$, as otherwise the resulting error $(2^b \cdot \varepsilon)$ becomes trivial.

We now proceed to prove Lemma 9.

Proof of Lemma 9. Fix a split-state adversary $\mathcal{A} = (U, V, |\psi\rangle_{W_1 W_2})$. Let $\rho_{M\hat{M}}$ be the canonical purification of $\rho_M = U_M$, and denote by η the outcome of the tampering experiment of $\mathcal{A}$ on the encoding of ρ, i.e.,

$$\eta = \mathrm{Dec}((U \otimes V)(\mathrm{Enc}(\rho_{\hat{M}M}) \otimes |\psi\rangle\langle\psi|)(U^\dagger \otimes V^\dagger)).$$

Since (Enc, Dec) is an average-case ε-non-malleable code and $\rho_{M\hat{M}}$ is maximally entangled (and so ρ_M is maximally mixed), we know that

$$\eta_{\hat{M}M} \approx_\varepsilon p_{\mathcal{A}}\rho_{\hat{M}M} + (1 - p_{\mathcal{A}})\rho_{\hat{M}} \otimes \gamma_M^{\mathcal{A}}, \tag{25}$$

where $(p_{\mathcal{A}}, \gamma_M^{\mathcal{A}})$ depend only on the split-state adversary $\mathcal{A}$. Note also that $\eta_{\hat{M}} = \rho_{\hat{M}} = U_{\hat{M}}$.

Towards showing that $(\mathrm{Enc}, \mathrm{Dec})$ is also worst-case non-malleable, consider an arbitrary quantum message σ_M of size b with canonical purification $\sigma_{M\hat{M}}$. If

$$\zeta = \mathrm{Dec}((U \otimes V)(\mathrm{Enc}(\sigma_{\hat{M}M}) \otimes |\psi\rangle\langle\psi|)(U^\dagger \otimes V^\dagger))$$

is the outcome of the tampering experiment of $\mathcal{A}$ on message σ, to derive the theorem statement it suffices to show that

$$\zeta_{\hat{M}M} \approx_{2^b \varepsilon} p_{\mathcal{A}} \sigma_{\hat{M}M} + (1 - p_{\mathcal{A}})(\sigma_{\hat{M}} \otimes \gamma_M^{\mathcal{A}}), \tag{26}$$

where $(p_{\mathcal{A}}, \gamma_M^{\mathcal{A}})$ depend only on $\mathcal{A}$ and come from Equation (25).

Recalling the definition of max-divergence (Definition 12), we have that

$$\mathrm{D}_{\max}(\sigma_M \| \rho_M) \leq b,$$

since $\sigma_M \leq \mathbb{I}_M$ and $\rho_M = \mathbb{I}_M / 2^b$. Therefore, by Fact 7 there exists a measurement $\{\Pi, \bar{\Pi}\}$ on register $\hat{M}$ in state ρ with success probability $\mathrm{Tr}(\Pi\rho) \geq 2^{-b}$ such that conditioned on success we have that

$$\sigma_{\hat{M}M} = \frac{\Pi\rho\Pi}{\mathrm{Tr}(\Pi\rho)}.$$

First, note that Π commutes with the operations of $(\mathrm{Enc}, \mathrm{Dec})$ and $\mathcal{A}$, since it is applied on register $\hat{M}$. Consequently, again conditioned on the measurement being successful, we have that

$$\zeta_{\hat{M}M} = \frac{\Pi\eta_{\hat{M}M}\Pi}{\mathrm{Tr}(\Pi\rho)},$$

and so

$$\begin{aligned}
\zeta_{\hat{M}M} &= \frac{\Pi\eta_{\hat{M}M}\Pi}{\mathrm{Tr}(\Pi\rho)} \\
&\approx_{2^b \varepsilon} p_{\mathcal{A}} \frac{\Pi\rho_{\hat{M}M}\Pi}{\mathrm{Tr}(\Pi\rho)} + (1 - p_{\mathcal{A}}) \frac{\Pi\rho_{\hat{M}}\Pi}{\mathrm{Tr}(\Pi\rho)} \otimes \gamma_M^{\mathcal{A}} \\
&= p_{\mathcal{A}} \sigma_{\hat{M}M} + (1 - p_{\mathcal{A}})(\sigma_{\hat{M}} \otimes \gamma_M^{\mathcal{A}}).
\end{aligned}$$

The approximation above follows from Fact 5 and by noting that

$$\eta_{\hat{M}M} \approx_\varepsilon p_{\mathcal{A}}\rho_{\hat{M}M} + (1 - p_{\mathcal{A}})\rho_{\hat{M}} \otimes \gamma_M^{\mathcal{A}}.$$

This completes the proof. $\qquad\square$

3.4 Privacy of our split-state NMC for quantum messages

We show that our split-state (worst-case) non-malleable code for quantum messages is also a 2-out-of-2 secret sharing scheme for quantum messages.

Theorem 6. *Let* $(\mathrm{Enc}, \mathrm{Dec})$ *be the* $(\varepsilon' = 2^{-n^{\Omega(1)}})$*-non-malleable code described in Section 3.1. Then,* $(\mathrm{Enc}, \mathrm{Dec})$ *is also an* $(\varepsilon_{\mathsf{priv}} = 2^{-n^{\Omega(1)}}, \varepsilon_{\mathsf{nm}} = 2^{-n^{\Omega(1)}})$*-2-out-of-2 non-malleable secret sharing scheme for quantum messages.*

Proof. Since (Enc, Dec) is already known to be ($\varepsilon' = 2^{-n^{\Omega(1)}}$)-non-malleable by Theorem 2, it remains to show that it also satisfies statistical privacy with error $\varepsilon_{\mathsf{priv}} = 2^{-n^{\Omega(1)}}$.

Let σ_M be an arbitrary message. Recall that $\mathrm{Enc}(\sigma_M)$ is composed of two parts X and $(Y, C_R\sigma_M C_R^\dagger)$, where $X \leftarrow \{0,1\}^\ell$, $Y \leftarrow \{0,1\}^{\delta\ell}$ are independent and $R = \mathsf{nmExt}(X, Y)$ with nmExt being the explicit function described in Fact 21. Additionally, we have $C_R = \mathsf{Samp}(R)$ with Samp being the sampling procedure for the special Clifford subgroup from Fact 10.

First, note that X, the first part of $\mathrm{Enc}(\sigma_M)$, is clearly sampled independently of the message σ_M, and so statistical privacy trivially holds when an adversary only has access to this first part. Therefore, we only need to focus on the case where an adversary holds the second part $(Y, C_R\sigma_M C_R^\dagger)$ of $\mathrm{Enc}(\sigma_M)$. Item 1 of Fact 21 guarantees that

$$RY = \mathsf{nmExt}(X, Y)Y \approx_{2^{-n^{\Omega(1)}}} U_r \otimes U_{\delta n}.$$

This means that we can from here onwards assume in our argument that R and Y are independent and both uniformly distributed (i.e., $RY = U_r \otimes U_{\delta n}$) at the expense of an extra additive factor $2^{-n^{\Omega(1)}}$ in the final statistical privacy error $\varepsilon_{\mathsf{priv}}$.

Observe that, for a fixed message σ_M, the state $(Y, C_R\sigma_M C_R^\dagger)$ corresponding to the second part of $\mathrm{Enc}(\sigma_M)$ is a (randomized) function of RY only. Since we are assuming that Y is independent of R, it suffices to argue that

$$C_R \sigma_{\hat{M}M} C_R^\dagger \approx_{2^{-n^{\Omega(1)}}} \sigma_{\hat{M}} \otimes U_M \tag{27}$$

for any message $\sigma_{\hat{M}M}$. If C_R was uniformly distributed over the Clifford subgroup $\mathcal{SC}(\mathcal{H}_M)$, then Fact 17 would guarantee that

$$C_R \sigma_{\hat{M}M} C_R^\dagger = \sigma_{\hat{M}} \otimes U_M. \tag{28}$$

Although C_R is not uniformly distributed over the Clifford subgroup $\mathcal{SC}(\mathcal{H}_M)$, we know from Fact 10 that

$$\mathsf{Samp}(R) \approx_{2^{-n^{\Omega(1)}}} U_{\mathcal{SC}(\mathcal{H}_M)}, \tag{29}$$

where $\mathsf{Samp}(R)$ is the classical description of C_R and $U_{\mathcal{SC}(\mathcal{H}_M)}$ is uniformly distributed over classical descriptions of Clifford operators in $\mathcal{SC}(\mathcal{H}_M)$. Combining Equations (28) and (29) yields Equation (27). Finally, summing the various trace distances along the way yields the final statistical privacy error $\varepsilon_{\mathsf{priv}} = 2^{-n^{\Omega(1)}}$ via the triangle inequality. $\qquad\square$

4 Threshold non-malleable secret sharing schemes for quantum messages

In this section, we present and analyze our non-malleable threshold secret sharing schemes for quantum messages. Before doing so, we must first introduce auxiliary objects, which we call *quantum-secure augmented leakage-resilient secret sharing schemes for classical messages*.

Our final construction of a non-malleable secret sharing scheme will combine our split-state non-malleable code for quantum messages from Theorem 1 with a standard secret sharing scheme for quantum messages and a quantum-secure leakage-resilient secret sharing scheme for classical messages. This overall approach can be seen as the quantum analogue of the argument by Goyal and Kumar [GK18a].

4.1 Quantum-secure augmented leakage-resilient secret sharing schemes for classical messages

Roughly speaking, a (locally) leakage-resilient secret sharing scheme allows a dealer to share a secret among p parties in such a way that authorized subsets of parties can reconstruct the secret, but unauthorized subsets of parties gain almost no information about the secret even when they learn bounded quantum leakage from other shares.

We proceed to define what we call, quantum-secure augmented leakage-resilient secret sharing schemes for classical messages. Let σ_M be a classical message in a register M, and let $\sigma_{M\hat{M}}$ be such that $\hat{M}$ is a copy of M. We wish to share σ_M among p parties in a way that any subset of at least t parties can reconstruct the secret, but subsets of at most $t-1$ parties gain almost no information about the secret, even if they learn some *quantum* leakage from every other share, and even when these $t-1$ parties share arbitrary entangled states with the leakage adversaries for the remaining shares.

Towards this end, we consider a coding scheme given by a classical encoding map lrShare : $\mathcal{L}(\mathcal{H}_M) \to \mathcal{L}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2} \otimes \cdots \otimes \mathcal{H}_{S_p})$ and a classical decoding map lrRec : $\mathcal{L}(\bigotimes_{i \in T} \mathcal{H}_{S_i}) \to \mathcal{L}(\mathcal{H}_M)$, where $\mathcal{L}(\mathcal{H})$ is the space of all linear operators in the Hilbert space $\mathcal{H}$. The reconstruction procedure lrRec acts on any authorized subset of shares T to reconstruct the original message M.

We now describe the adversarial leakage model we work under. Let $\rho_{S_1 S_2 \dots S_p} = \text{lrShare}(\sigma_M)$ be the secret sharing of message σ_M and fix a subset T of parties. An ℓ-*bounded local leakage adversary* $\mathcal{A}_T$ is specified by $p - |T|$ leakage maps $\Phi_j : \mathcal{L}(\mathcal{H}_{S_j} \otimes \mathcal{H}_{W_j}) \to \mathcal{L}(\mathcal{H}_{Z_j})$ for $j \in [p] \setminus T$ along with a quantum state $|\psi\rangle_{W_1 W_2 \dots W_p}$ which captures the shared entanglement between non-communicating local leakage adversaries. The outcome of the leakage operation on the j-th share S_j, is stored in register Z_j with Z_j being the leakage register, is obtained by applying Φ_j to the contents of registers S_j and W_j. We assume that the leakage Z_j is bounded, in the sense that $|Z_j| \leq \ell$ for every $j \in [p] \setminus T$, where ℓ is some leakage bound parameterizing the leakage adversary. We denote the outcome of the leakage experiment against $\mathcal{A}_T$ by $\tau^{\mathcal{A}_T}$, which may be written as

$$\tau^{\mathcal{A}_T} = \left(\left(\bigotimes_{i \in T} \mathbb{I} \right) \otimes \left(\bigotimes_{j \notin T} \Phi_j \right) \right) \left(\text{lrShare}(\sigma_{M\hat{M}}) \otimes |\psi\rangle\langle\psi|_{W_1 W_2 \dots W_p} \right).$$

We are now ready to define quantum-secure augmented leakage-resilient secret sharing schemes for classical messages. It is easy to extend this definition to more general access structures. For simplicity and because it suffices for our needs, we focus on threshold access structures only.

Definition 20 (Quantum-secure threshold augmented leakage-resilient secret sharing)**.** *We say that the coding scheme* (lrShare, lrRec) *is an* (ℓ, ε)-*quantum-secure* t-*out-of-*p *augmented leakage-resilient secret sharing scheme if the following properties hold:*

- **Correctness:** *For any set* $T \subseteq [p]$ *of size* $|T| \geq t$ *it holds that*

$$\text{lrRec}(\text{lrShare}(\sigma)_{\hat{M}T}) = \sigma_{\hat{M}M}.$$

- **Leakage-resilience:** *For any set* $T \subseteq [p]$ *of size* $|T| = t - 1$, *every* ℓ-*bounded local leakage adversary*

$$\mathcal{A}_T = ((\Phi_j)_{j \notin T}, |\psi\rangle_{W_1 W_2 \dots W_p}),$$

and every classical message σ_M (with the register $\hat{M}$ being a copy of M) it holds that

$$\tau^{\mathcal{A}_T}_{\hat{M}S_T W_T (Z_j)_{j\notin T}} \approx_\varepsilon \sigma_{\hat{M}} \otimes \gamma^{\mathcal{A}_T}_{S_T W_T (Z_j)_{j\notin T}},$$

where $\gamma^{\mathcal{A}_T}_{S_T W_T (Z_j)_{j\notin T}}$ is a fixed state depending only[11] on the adversary

$$\mathcal{A}_T = ((\Phi_j)_{j\notin T}, |\psi\rangle_{W_1 W_2 \ldots W_p}).$$

Moreover, we say that the coding scheme (lrShare, lrRec) *is an (ℓ, ε)-quantum-secure average-case t-out-of-p augmented leakage-resilient secret sharing scheme if the above holds for a uniformly random message $\sigma_M = U_M$.*

As was the case for our non-malleability definitions, our notion of average-case leakage-resilience is akin to requiring that the *average* leakage-resilience error over the uniform choice of input message be small.

We use the adjective "augmented" because we consider a leakage experiment where the distinguisher learns not only the shares S_T corresponding to the parties in T and the leakage $(Z_j)_{j\notin T}$, but (crucially) also the entangled states W_T corresponding to parties in T. Note that every (ℓ, ε)-quantum-secure t-out-of-p augmented leakage-resilient secret sharing scheme is also average-case with the same parameters.

4.1.1 A 2-out-of-2 scheme

On the way to constructing a quantum-secure 2-out-of-p augmented leakage-resilient secret sharing scheme, we first focus on the special case where $t = p = 2$. We show that a well-known secret sharing scheme based on the inner product extractor is a quantum-secure augmented leakage-resilient scheme with good parameters.

Suppose that we wish to share a b-bit classical message. Let $q = 2^b$ and recall the inner product function $\mathsf{IP} : \mathbb{F}_q^N \times \mathbb{F}_q^N \to \mathbb{F}_q$ given by

$$\mathsf{IP}(x, y) = \sum_{i=1}^{N} x_i y_i,$$

where operations are performed over $\mathbb{F}_q$. Consider the following coding scheme (2lrShare, 2lrRec). On input a message $s \in \mathbb{F}_q$, the sharing procedure $2\mathrm{lrShare}(s)$ works as follows:

1. Sample $(X, Y) \leftarrow \mathsf{IP}^{-1}(s) = \{(x, y) \in \mathbb{F}_q^N \times \mathbb{F}_q^N : \mathsf{IP}(x, y) = s\}$;

2. Set the two shares as $S_1 = X$ and $S_2 = Y$.

To reconstruct the secret, we set $\mathrm{lrRec}(S_1, S_2) = \mathsf{IP}(S_1, S_2)$. Note that both the sharing and reconstruction procedures run in time $\mathrm{poly}(N, b)$. The following theorem, proved using the extractor properties of IP (see Fact 20), states the main properties of this scheme.

---

[11]By this, we mean that the state $\gamma^{\mathcal{A}_T}_{S_T W_T (L_j)_{j\notin T}}$ can be prepared without the knowledge of the input message $\sigma_{M\hat{M}}$.

Theorem 7. *The coding scheme* $(\mathrm{2lrShare}, \mathrm{2lrRec})$ *defined above is an* (ℓ, ε)-*quantum-secure 2-out-of-2 augmented leakage-resilient secret sharing scheme provided that the share size* $N \cdot b$ *(in bits) satisfies*

$$N \cdot b \geq 9b + 2\ell + 8 \log(1/\varepsilon) + 40.$$

Moreover, the sharing and reconstruction procedures run in time $\mathrm{poly}(N, b)$.

Proof. The correctness and runtime of this coding scheme are straightforward. We focus on establishing leakage-resilience. We briefly discuss the intuition behind the proof. First, we consider an "ideal" case where the message σ_M is uniformly random. This corresponds to the two shares, X and Y, being independent and uniformly random. In this unrealistic case we can invoke the randomness extraction properties of IP from Fact 20 to conclude that $\mathsf{IP}(X, Y)$ will still be extremely close to uniformly random even when conditioned on, say, X along the entangled state W_1 and the leakage Z_2 from Y. Then, we move to the real case where $\mathsf{IP}(X, Y) = s$ for an arbitrary fixed message s by conditioning the ideal distribution above on this event, which happens with probability 2^{-b}. This incurs a blowup factor of 2^b on the final statistical error when moving from the ideal case to the real case, which we can survive.

Without loss of generality, fix $T = \{1\}$ and some leakage adversary $\mathcal{A} = (\Phi_2, |\psi\rangle_{W_1 W_2})$. First, we consider the "ideal" case where X and Y are independent and uniformly distributed over $\mathbb{F}_q^N$. Define $\rho = \rho_{X\hat{X}} \otimes \rho_{Y\hat{Y}}$, where $\hat{X}$ and $\hat{Y}$ are canonical purification registers of X and Y, respectively. Let Z_2 be the leakage register after applying the leakage function Φ_2 to the contents of registers Y and W_2. Invoking Fact 1, let $V_{\Phi_2} : \mathcal{H}_Y \otimes \mathcal{H}_{W_2} \to \mathcal{H}_Y \otimes \mathcal{H}_{Z_2} \otimes \mathcal{H}_{W_2'}$ be the Stinespring isometry corresponding to the leakage map Φ_2. Denote by γ the state $\rho \otimes |\psi\rangle\langle\psi|$ and τ by the state obtained by applying the leakage attack defined by $\mathcal{A}$ to registers (Y, W_2), i.e.,

$$\tau = V_{\Phi_2} \gamma V_{\Phi_2}^{\dagger}.$$

We begin by lower bounding the min-entropy of certain random variables in order to be able to apply the extractor properties of IP. By independence of X and Y, we have that

$$\mathrm{H}_{\min}\left(X \middle| Y\hat{Y}W_2\right)_{\gamma} \geq N \log q \quad \text{and} \quad \mathrm{H}_{\min}\left(Y \middle| X\hat{X}W_1\right)_{\gamma} \geq N \log q. \tag{30}$$

In fact, we claim that we actually have the inequalities

$$\mathrm{H}_{\min}\left(X \middle| Y\hat{Y}W_2'\right)_{\tau} \geq N \log q \quad \text{and} \quad \mathrm{H}_{\min}\left(Y \middle| X\hat{X}W_1 Z_2\right)_{\tau} \geq N \log q - 2\ell. \tag{31}$$

The leftmost inequality of Equation (31) follows by combining the leftmost inequality of Equation (30) with Fact 19, since $\tau_{Y Z_2 W_2'} = V_{\Phi_2} \gamma_{Y W_2} V_{\Phi_2}^{\dagger}$. To see the rightmost inequality of Equation (31), first note that $\tau_{Y X\hat{X}W_1} = \tau_Y \otimes \tau_{X\hat{X}W_1} = U_Y \otimes \tau_{X\hat{X}W_1}$. Furthermore, we have that

$$\mathrm{I}_{\max}(Y : X\hat{X}W_1 Z_2)_{\tau} \leq 2|Z_2| \leq 2\ell, \tag{32}$$

where we recall that $\mathrm{I}_{\max}$ is the max-information and the inequality follows from Fact 3. The rightmost inequality of Equation (31) now follows from Definition 13 and Definition 17 after noting that $\tau_Y = U_Y$.

Now, set $Z = \mathsf{IP}(X, Y)$ and store this string in register M. Taking into account Equation (31), we invoke Fact 20 with the assignment of states/registers (the states/registers on the left below are from the statement of Fact 20, while the states/registers on the right are those from this proof)

$$(\rho, W_1, W_2, X, Y) \leftarrow \left(\tau, W_1 Z_2, W_2', X, Y\right)$$

to conclude that

$$\tau_{MXW_1Z_2} \approx_{\varepsilon'=\varepsilon \cdot 2^{-b}} U_M \otimes \tau_{XW_1Z_2}, \tag{33}$$

provided that $N \log q = N \cdot b \geq 9b + 2\ell + 8 \log(1/\varepsilon) + 40$.

To conclude the proof, we would like to show that Equation (33) holds not only when X and Y are uniformly random over $\mathbb{F}_q^N$, but also when X and Y are sampled uniformly at random from any preimage $\mathsf{IP}^{-1}(s)$ with $\sigma_M = s \in \mathbb{F}_q$ any fixed message. Let τ' denote the state τ conditioned on the event that $\tau_M = \sigma_M$. Then, τ' corresponds exactly to the state obtained by sharing s using 2lrShare and then applying the leakage attack defined by $\mathcal{A}$ above on the resulting shares. Since $\Pr[U_M = \sigma_M] = 2^{-b}$, conditioning both sides of Equation (33) on the event that $\tau_M = \sigma_M$ yields

$$\tau'_{MXW_1Z_2} \approx_{\varepsilon' \cdot 2^b = \varepsilon} \sigma_M \otimes \tau_{XW_1Z_2},$$

as desired. $\qquad\square$

4.1.2 A 2-out-of-p scheme

We now use our 2-out-of-2 augmented leakage-resilient secret sharing scheme to obtain a 2-out-of-p scheme for any number of parties $p \geq 3$. This is accomplished by following the high-level approach of Goyal and Kumar [GK18a] in the classical setting.

Let $(\text{2lrShare}, \text{2lrRec})$ be our secret sharing scheme from Theorem 7 for b-bit messages with share size $N \cdot b$. Then, we define our 2-out-of-p secret sharing scheme $(\text{lrShare}, \text{lrRec})$ for b-bit messages as follows. To share a message $s \in \{0,1\}^b$ among p parties, the sharing procedure $\text{lrShare}(s)$ proceeds as follows:

1. For each pair $(i,j) \in [p] \times [p]$ with $i < j$, compute the 2-out-of-2 secret sharing $(X_i^j, X_j^i) \leftarrow \text{2lrShare}(s)$.

2. Set the final i-th share as $S_i = (X_i^1, X_i^2, \ldots, X_i^{i-1}, X_i^{i+1}, \ldots, X_i^p)$ for each $i \in [p]$.

For an authorized subset of parties T (i.e., $|T| \geq 2$), the reconstruction procedure $\text{lrRec}(S_T)$ works as follows: Pick any two indices $i, j \in T$ such that $i < j$. Then, output $s = \text{2lrRec}(X_i^j, X_j^i)$.

Note that $(\text{lrShare}, \text{lrRec})$ above has share size $(p-1) \cdot N \cdot b$. The following theorem states the secret sharing and leakage-resilience properties of $(\text{lrShare}, \text{lrRec})$.

Theorem 8. *The coding scheme $(\text{lrShare}, \text{lrRec})$ is an (ℓ, ε)-quantum-secure 2-out-of-p augmented leakage-resilient secret sharing scheme whenever the share size $(p-1) \cdot N \cdot b$ satisfies*

$$(p-1) \cdot N \cdot b \geq (p-1)(9b + 2\ell + 8\log(1/\varepsilon) + 16\log p + 40).$$

Moreover, the sharing and reconstruction procedures run in time $\text{poly}(p, N, b)$. Furthermore, the fixed leaked state in the leakage-resilience property of Definition 20 can be obtained by running the leakage tampering experiment for a uniform input message.

Proof. The correctness of this coding scheme is straightforward. Therefore, we focus on showing leakage-resilience, which follows via a hybrid argument analogous to that of [GK18a, Theorem 6].

Without loss of generality we may set $T = \{1\}$. Fix a secret $s \in \mathbb{F}_q$ and an arbitrary leakage adversary $\mathcal{A} = (\Phi_2, \ldots, \Phi_p, |\psi\rangle_{W_1 W_2 \ldots W_p})$, where $\Phi_i : \mathcal{L}(\mathcal{H}_{S_i} \otimes \mathcal{H}_{W_i}) \to \mathcal{L}(\mathcal{H}_{Z_i})$ with Z_i being the leakage register for every $i \in [2, p]$.

Let $\sigma^s_{S_1 S_2 \ldots S_p}$ where $S_i \equiv X_i^1 \ldots X_i^{i-1} X_i^{i+1} \ldots X_i^p$ be the p shares corresponding to the encoding of secret s, and let

$$\rho^s_{S_1 W_1 Z_2 \ldots Z_p} = (\Phi_2 \otimes \ldots \otimes \Phi_p)(\sigma^s_{S_1 S_2 \ldots S_p} \otimes |\psi\rangle\langle\psi|_{W_1 W_2 \ldots W_p}).$$

Let $H^s_{0,0}$ denote the original leakage experiment when run on $\sigma^s_{S_1 S_2 \ldots S_p}$, which outputs $\rho^s_{S_1 W_1 Z_2 \ldots Z_p}$. For all pairs $(i,j) \in [p] \times [p]$ with $i < j$, let Y_i^j and Y_j^i be independent and uniformly distributed over $\mathbb{F}_q^N$. We consider hybrids $H^s_{i,j}$ where for all pairs (i',j') up to (i,j) in lexicographic order we replace X_i^j and X_j^i by Y_i^j and Y_j^i, respectively.

Note that the output of $H^s_{p-1,p}$ is independent of the secret s, since it can be obtained by running the leakage tampering experiment for a uniform input message. Furthermore, there are $\binom{p}{2} < p^2$ hybrids. Therefore, the theorem statement will follow if we show that the outputs of any two consecutive hybrids are (ε/p^2)-close in trace distance and then repeatedly apply the triangle inequality. We show here that

$$H^s_{0,0} \approx_{\varepsilon/p^2} H^s_{1,2}. \tag{34}$$

The desired analogous statement for any given pair of consecutive hybrids follows in exactly the same manner. Recall that the only thing that changes from $H^s_{0,0}$ to $H^s_{1,2}$ is that X_1^2 and X_2^1 are replaced by Y_1^2 and Y_2^1, respectively. Furthermore, observe that, since s is fixed, we may sample any other pair $(X_i^j, X_j^i) \leftarrow \mathsf{IP}^{-1}(s)$ for index pairs $(i,j) \neq (1,2)$ using randomness independent of $(X_1^2, X_2^1, Y_1^2, Y_2^1)$. Consider an arbitrary fixing $(X_i^j, X_j^i) = (x_i^j, x_j^i)$ of all pairs $(i,j) \neq (1,2)$ with $i < j$ such that $\mathsf{IP}(x_i^j, x_j^i) = s$. Let us denote the arbitrary fixing as fix, and $\sigma^{\mathsf{fix}}_{\mathsf{rest}}$ to mean that the rest of the registers except (X_1^2, X_2^1) are set to fix. Let $H^{s,\mathsf{fix}}_{0,0}$ be the original tampering experiment when run after fixing fix. Then, we have that

$$H^{s,\mathsf{fix}}_{0,0} = (\Phi_2 \otimes \ldots \otimes \Phi_p)(\sigma^s_{X_1^2 X_2^1} \otimes \sigma^{\mathsf{fix}}_{\mathsf{rest}} \otimes |\psi\rangle\langle\psi|_{W_1 \cdots W_p})$$

and

$$H^{s,\mathsf{fix}}_{1,2} = (\Phi_2 \otimes \ldots \otimes \Phi_p)(U_{Y_1^2} \otimes U_{Y_2^1} \otimes \sigma^{\mathsf{fix}}_{\mathsf{rest}} \otimes |\psi\rangle\langle\psi|_{W_1 \cdots W_p}).$$

Furthermore, it holds that

$$H^s_{0,0} = \mathbb{E}_{\mathsf{fix}} H^{s,\mathsf{fix}}_{0,0} \quad \text{and} \quad H^s_{1,2} = \mathbb{E}_{\mathsf{fix}} H^{s,\mathsf{fix}}_{1,2},$$

where $\mathbb{E}_{\mathsf{fix}}$ stands for expectation taken over all the fixings. If we show that for every fixing fix, $H^{s,\mathsf{fix}}_{0,0} \approx_{\varepsilon/p^2} H^{s,\mathsf{fix}}_{1,2}$, we will be done as this implies $H^s_{0,0} \approx_{\varepsilon/p^2} H^s_{1,2}$ by invoking Fact 6. We now proceed to show that $H^{s,\mathsf{fix}}_{0,0} \approx_{\varepsilon/p^2} H^{s,\mathsf{fix}}_{1,2}$.

By post-processing of trace distance (Fact 4) it suffices to show that

$$\Phi_2(\sigma^s_{X_1^2 X_2^1} \otimes \sigma^{\mathsf{fix}}_{\mathsf{rest}} \otimes |\psi\rangle\langle\psi|_{W_1 \cdots W_p}) \approx_{\varepsilon/p^2} \Phi_2(U_{Y_1^2} \otimes U_{Y_2^1} \otimes \sigma^{\mathsf{fix}}_{\mathsf{rest}} \otimes |\psi\rangle\langle\psi|_{W_1 \cdots W_p}). \tag{35}$$

Noting that Φ_2 is an ℓ-bounded leakage function we see that Equation (35) follows from Theorem 7 and the definition of quantum-secure augmented leakage-resilient secrete sharing, provided that $N \log q = N \cdot b \geq 9b + 2\ell + 8 \log(1/\varepsilon) + 16 \log p + 40$. This completes the proof. $\qquad\square$

4.2 Our candidate non-malleable secret sharing scheme for quantum messages

We proceed to leverage our split-state non-malleable code for quantum messages from Theorem 1 and quantum-secure augmented leakage-resilient secret sharing scheme for classical messages from Theorem 8 to construct non-malleable threshold secret sharing schemes for quantum messages. The high-level approach we follow can be seen as the quantum analogue of the construction of classical non-malleable secret sharing schemes due to Goyal and Kumar [GK18a]. We exploit two crucial properties of our split-state non-malleable code for quantum messages: First, one of its states is fully classical. Second, it is also a 2-out-of-2 secret sharing scheme for quantum messages.

Fix a threshold $t \geq 3$ and a number of parties p such that $t \leq p \leq 2t - 1$. We will require the following objects:

- A 2-out-of-2 $(\varepsilon_{\mathsf{nm}} = \varepsilon, \varepsilon_{\mathsf{priv}} = \varepsilon)$-non-malleable secret sharing scheme $(\mathrm{2nmShare}, \mathrm{2nmRec})$ for quantum messages of length b with a quantum left share of length b_1 and a classical right share of length b_2, guaranteed by Theorem 6;

- A t-out-of-p secret sharing scheme $(\mathrm{qShare}, \mathrm{qRec})$ for quantum messages of length b_1 with shares of length at most ℓ, guaranteed by Fact 22;

- A 2-out-of-p $(\ell, \varepsilon_{\mathsf{leak}})$-quantum-secure augmented leakage-resilient secret sharing scheme $(\mathrm{lrShare}, \mathrm{lrRec})$ for classical messages of length b_2, guaranteed by Theorem 8.

We proceed to describe our candidate t-out-of-p scheme $(\mathrm{nmShare}, \mathrm{nmRec})$. On input a quantum message σ_M with canonical purification $\sigma_{M\hat{M}}$, the sharing algorithm $\mathrm{nmShare}(\sigma)$ proceeds as follows:

1. Compute the split-state encoding $\rho_{LR} = \mathrm{2nmShare}(\sigma_M)$, where R is a classical register;

2. Apply qShare to the contents of register L to obtain p quantum shares stored

3. Apply lrShare to the contents of register R to obtain p classical shares stored in registers $R_1, \ldots, R_p$;

4. Form the i-th final share $S_i = (L_i, R_i)$.

The correctness and runtime of this coding scheme are clear. In the following sections we establish its statistical privacy and non-malleability.

4.3 Statistical privacy

Consider an arbitrary message σ_M with canonical purification $\sigma_{M\hat{M}}$. Let $\rho_{\hat{M}LR} = \mathrm{2nmShare}(\sigma_{M\hat{M}})$ be the split-state encoding of σ with L the quantum register and R the classical register. Let $\gamma = \mathrm{qShare}(\rho)$ denote the state after encoding the contents of register L using the t-out-of-p secret sharing scheme $(\mathrm{qShare}, \mathrm{qRec})$ for quantum messages, and let $\theta = \mathrm{nmShare}(\sigma_{M\hat{M}}) = \mathrm{lrShare}(\gamma)$ denote the final state after encoding σ. In order to establish the desired privacy property for $(\mathrm{nmShare}, \mathrm{nmRec})$, we must show that for any subset of parties $T \subseteq [p]$ of size $|T| \leq t - 1$ it holds that

$$\theta_{\hat{M}S_T} \approx_{\varepsilon_{\mathsf{priv}}} \sigma_{\hat{M}} \otimes \zeta_{S_T},$$

for a fixed state ζ_{S_T} (recall the notation $S_T = (S_i)_{i \in T}$).

Since $\gamma = \mathrm{qShare}(\rho)$, invoking Lemma 2 with the assignment of registers (where the registers on the left are those from the statement of Lemma 2 and the registers on the right are the registers used in this proof)

$$(\rho, \sigma, \sigma_E, \sigma_M) \leftarrow (\gamma, \rho, \rho_{\hat{M}R}, \rho_L)$$

ensures that

$$\gamma_{\hat{M}RL_T} \equiv \rho_{\hat{M}R} \otimes U_{L_T}. \tag{36}$$

Since $(\mathrm{2nmShare}, \mathrm{2nmRec})$ satisfies $\varepsilon_{\mathsf{priv}}$-privacy, we also have that

$$\rho_{\hat{M}R} \approx_{\varepsilon_{\mathsf{priv}}} \sigma_{\hat{M}} \otimes U_R. \tag{37}$$

Thus, combining Equations (36) and (37) with the triangle inequality yields

$$\gamma_{\hat{M}RL_T} \approx_{\varepsilon_{\mathsf{priv}}} \sigma_{\hat{M}} \otimes U_R \otimes U_{L_T}.$$

Since $\theta = \mathrm{lrShare}(\gamma)$, the post-processing property of trace distance (Fact 4) implies that

$$\theta_{\hat{M}R_T L_T} \approx_{\varepsilon_{\mathsf{priv}}} \sigma_{\hat{M}} \otimes \mathrm{lrShare}(U_R)_{R_T} \otimes U_{L_T}. \tag{38}$$

We conclude that

$$\theta_{\hat{M}S_T} \equiv \theta_{\hat{M}R_T L_T} \approx_{\varepsilon_{\mathsf{priv}}} \sigma_{\hat{M}} \otimes \zeta_{S_T},$$

where $\zeta_{S_T} = \mathrm{lrShare}(U_R)_{R_T} \otimes U_{L_T}$ is the fixed state.

4.4 Average-case non-malleability

We proceed to show average-case non-malleability for our coding scheme $(\mathrm{nmShare}, \mathrm{nmRec})$. In this case we take $\sigma_M = U_M$, and so the canonical purification $\sigma_{M\hat{M}}$ is maximally entangled. Without loss of generality, we may take $T = \{1, \ldots, t\}$.

Fix an arbitrary tampering adversary $\mathcal{A} = (U_1, U_2, \ldots, U_t, |\psi\rangle\langle\psi|_{E_1 E_2 \ldots E_p})$, where the quantum registers $E_1, \ldots, E_p$ store an arbitrary quantum state to be used as shared entanglement across the several tampering adversaries. Our goal is to reduce the non-malleability of $(\mathrm{nmShare}, \mathrm{nmRec})$ to the non-malleability of $(\mathrm{2nmShare}, \mathrm{2nmRec})$. In order to do this, we show that if $\mathcal{A}$ breaks the $(\varepsilon_{\mathsf{nm}} + 2\sqrt{\varepsilon_{\mathsf{leak}}})$-non-malleability of $(\mathrm{nmShare}, \mathrm{nmRec})$ via the authorized subset T, then we can build, using $\mathcal{A}$, a split-state adversary $\mathcal{A}' = (U, V, |\gamma\rangle\langle\gamma|_{W_1 W_2})$ that breaks the $\varepsilon_{\mathsf{nm}}$-non-malleability of $(\mathrm{2nmShare}, \mathrm{2nmRec})$. Since we know that $(\mathrm{2nmShare}, \mathrm{2nmRec})$ is $\varepsilon_{\mathsf{nm}}$-non-malleable, the desired result follows.

To build the 2-split-state tampering adversary $\mathcal{A}'$ from our original adversary $\mathcal{A}$, we would like to follow the high-level approach of Goyal and Kumar [GK18a] in the classical setting and extend it to the quantum setting. However, as already mentioned in Section 1.3.2, naively replicating this argument in the quantum setting is not possible since the quantum side information cannot be fixed. We require a quantum-secure *augmented* leakage-resilient secret sharing scheme to overcome this issue. Another thing that complicates the approach in the quantum setting is that the register L in the split-state encoding (L, R) of the message σ_M is quantum and so is lost after tampering. We get around this issue by considering "coherent copies" of L and R which we will be able to access in our analysis even after L has been destroyed.

To be more precise and because it will be useful during the following argument to generate coherent copies of registers, we recall some properties of $(\mathrm{2nmShare}, \mathrm{2nmRec})$. First, $\mathrm{2nmShare}(\sigma_M)$

is composed of two parts, R and $L = (L^1, L^2)$, where $R = U_R$ and $L^1 = U_{L^1}$ are classical registers, and L^2 is the quantum register. Moreover, we have that $L^2 = C_K \sigma_M C_K^\dagger = U_{L^2}$ with $K = \mathsf{nmExt}(R, L^1)$, where nmExt is the explicit quantum-secure 2-source non-malleable extractor from Fact 21, and C_K is an appropriate Clifford gate. It follows from the procedure that

$$2\mathsf{nmShare}(\sigma_M) = U_L \otimes U_R. \tag{39}$$

Note that 2nmShare is a CPTP map and not an isometry – to access "coherent copies" of L and R, we will have to consider the Stinespring isometry extention of 2nmShare. Let $V_{2\mathsf{nmShare}} : \mathcal{H}_M \to (\mathcal{H}_L \otimes \mathcal{H}_R \otimes \mathcal{H}_F)$ be the Stinespring isometry extension (see Fact 1) of 2nmShare, where the register F in the definition of $V_{2\mathsf{nmShare}}$ is the external ancilla register required to implement the operation 2nmShare as an isometry. Let $\nu = V_{2\mathsf{nmShare}} \sigma_{M\hat{M}} V_{2\mathsf{nmShare}}^\dagger$. Observe that ν is a pure state and $2\mathsf{nmShare}(\sigma_M) = \mathrm{Tr}_{\hat{M}F} \left(V_{2\mathsf{nmShare}} \sigma_{M\hat{M}} V_{2\mathsf{nmShare}}^\dagger \right)$. Combining this with Equation (39), we have that

$$\mathrm{Tr}_{\hat{M}F} (\nu) = U_L \otimes U_R. \tag{40}$$

Let $\rho_{L\hat{L}R\hat{R}}$ be the canonical purification of $\rho_{LR} = U_L \otimes U_R$. We now invoke Uhlmann's theorem (Fact 9) with the following assignment of registers (where the registers on the left are those from the statement of Fact 9 and the registers on the right are the registers used in this proof):

$$(\sigma_A, \rho_A, \sigma_{AC}, \rho_{AB}) \leftarrow (\nu_{LR}, \rho_{LR}, \nu_{LRF\hat{M}}, \rho_{LR\hat{L}\hat{R}}).$$

This guarantees the existence of an isometry $\mathsf{Uhlmann} : \mathcal{H}_{\hat{M}} \otimes \mathcal{H}_F \to \mathcal{H}_{\hat{L}} \otimes \mathcal{H}_{\hat{R}}$ such that

$$\Delta_B \left(\rho_{LR\hat{L}\hat{R}}, (\mathsf{Uhlmann})\nu_{LRF\hat{M}}(\mathsf{Uhlmann}^\dagger) \right) = \Delta_B(\rho_{LR}, \nu_{LR}) = 0,$$

where the rightmost inequality holds because $\rho_{LR} = \nu_{LR} = U_L \otimes U_R$. Thus, we conclude that the state ρ as depicted in Figure 8 satisfies

$$\rho_{L\hat{L}R\hat{R}} = \rho_{L\hat{L}} \otimes \rho_{R\hat{R}} \quad \text{and} \quad \rho_{LR} = U_L \otimes U_R. \tag{41}$$

With access to coherent copies of $\hat{L}, \hat{R}$ in state ρ, we now move on to consider the two relevant tampering experiments are described in Figures 8 and 9 for some adversaries $\mathcal{A}'$ and $\mathcal{A}$, respectively. We will refer to states in those figures throughout our argument. First, observe that the state ρ is the same in Figures 8 and 9. Moreover, the procedures applied to the states τ' and τ in Figures 8 and 9, respectively, are also the same. This means that in order to prove the desired result it suffices to show that given any adversary $\mathcal{A}$ in Figure 9 we can come up with a corresponding 2-split-state adversary $\mathcal{A}' = (U, V, |\gamma\rangle\langle\gamma|_{W_1 W_2})$ (which transforms the state ρ into τ' in Figure 8) such that τ' in Figure 8 is appropriately close (in trace distance) to the state τ in Figure 9.

As a stepping stone towards defining $\mathcal{A}'$, we begin by studying the state θ in Figure 9, which is obtained from ρ through an application of the qShare and lrShare procedures. Note that θ is not pure – to facilitate the analysis, we will from here onwards work with the pure state extension of θ, which, because the context is clear, we will also call θ. More precisely, let $V_{\mathsf{qShare}} : \mathcal{H}_L \to (\mathcal{H}_{L_1} \otimes \cdots \otimes \mathcal{H}_{L_p} \otimes \mathcal{H}_{\tilde{L}})$ be the Stinespring isometry extension (see Fact 1) of qShare, and let $V_{\mathsf{lrShare}} : \mathcal{H}_R \to (\mathcal{H}_{R_1} \otimes \cdots \otimes \mathcal{H}_{R_p} \otimes \mathcal{H}_{\tilde{R}_1} \otimes \cdots \otimes \mathcal{H}_{\tilde{R}_p})$ be the Stinespring isometry extension (see Fact 2) of lrShare. The registers $\tilde{L}$ and $\tilde{R}_1, \ldots, \tilde{R}_p$ in the definitions of V_{qShare} and V_{lrShare},

respectively, are the external ancilla registers required to implement the operations lrShare and qShare (which are CPTP maps) as isometries. Then, we define

$$\theta \overset{\text{def}}{=} (V_{\text{qShare}} \otimes V_{\text{lrShare}}) \rho (V_{\text{qShare}}^{\dagger} \otimes V_{\text{lrShare}}^{\dagger}).$$

We also consider the following intermediate state θ' obtained from θ by tampering with the first $t-1$ shares according to $\mathcal{A}$, i.e.,

$$\theta' \overset{\text{def}}{=} (U_1 \otimes \ldots \otimes U_{t-1} \otimes \mathbb{I}_t \otimes \ldots \mathbb{I}_p)(\theta \otimes |\psi\rangle\langle\psi|_{E_1 \ldots E_p})(U_1^{\dagger} \otimes \ldots \otimes U_{t-1}^{\dagger} \otimes \mathbb{I}_t^{\dagger} \otimes \ldots \mathbb{I}_p^{\dagger}).$$

The registers associated with θ' are found in Figure 9 after applying $U_1, \ldots, U_{t-1}$ to θ. In what follows we will need to refer to several registers of θ'. To help with readability, we define

$$W_1' \equiv R_t L_{[t-1]} E_{[t,p]} \tilde{L} L_{[t,p]} \quad \text{and} \quad W_2' \equiv R_{[t-1]} E_{[t-1]} R_{[t+1,p]} \tilde{R}_{[p]}$$

as shorthand, where we recall that $[t,p]$ denotes the set $\{t, t+1, \ldots, p\}$. The notation W_1' and W_2' is justified by the fact that we will use $\gamma_{W_1 W_2} \equiv \theta'_{W_1 W_2}$ with

$$W_1 \equiv R_t L_{[t-1]} E_{[t,p]} \hat{L} \tilde{L} L_{[t,p]} \quad \text{and} \quad W_2 \equiv R_{[t-1]} E_{[t-1]} \hat{R} R_{[t+1,p]} \tilde{R}_{[p]},$$

obtained by adding $\hat{R}$ to W_2' and $\hat{L}$ to W_1', respectively, as the shared entanglement for the 2-split-state adversary $\mathcal{A}'$.

We now present some important properties of the state θ'. Their proofs appear later in Sections 4.4.1 and 4.4.2. The first claim states that the coherent copy $\hat{L}$ defined above is independent of $\hat{R}$ even when W_2' is revealed as side information.

Claim 1. *We have that*

$$\theta'_{\hat{L}\hat{R}W_2'} = \theta'_{\hat{L}} \otimes \theta'_{\hat{R}W_2'}.$$

The second claim states that $\hat{R}$ is close to being independent of $\hat{L}$ given the side information W_1'. This uses the augmented leakage-resilience property of the (lrShare, lrRec) scheme.

Claim 2. *We have that*

$$\theta'_{\hat{R}\hat{L}W_1'} \approx_{\varepsilon_{\text{leak}}} \theta'_{\hat{R}} \otimes \theta'_{\hat{L}W_1'}.$$

We use these claims as starting points towards constructing the tampering maps U and V of the 2-split-state adversary $\mathcal{A}'$. First, we show that there exist maps $U' : \mathcal{H}_L \otimes \mathcal{H}_{W_1} \to \mathcal{H}_{W_1'}$ and $V' : \mathcal{H}_R \otimes \mathcal{H}_{W_2} \to \mathcal{H}_{W_2'}$ and a pure state $\gamma_{W_1 W_2}$ that depends only on $(U_1, U_2, \ldots, U_{t-1}, |\psi\rangle\langle\psi|_{E_1 \ldots E_p})$ such that

$$\theta'_{W_1 W_2} \approx_{2\sqrt{\varepsilon_{\text{leak}}}} (U' \otimes V')(\rho \otimes \gamma_{W_1 W_2})((U')^{\dagger} \otimes (V')^{\dagger}). \tag{42}$$

Equation (42) is a consequence of a careful instantiation of the following fact. A variation of the fact below in terms of mutual information already appears in [JPY14, Lemma II.15]. For the sake of completeness, we provide a proof of the version we need in Section 4.4.3.

Fact 24. *Let ϕ_{XABY} be a pure state such that*

$$\phi_{XBY} \approx_{\varepsilon_1} \phi_X \otimes \phi_{BY} \quad \text{and} \quad \phi_{YAX} \approx_{\varepsilon_2} \phi_Y \otimes \phi_{AX}.$$

53

Furthermore, let κ be a pure state such that

$$\kappa_{X_1 \hat{X}_1 Y_1 \hat{Y}_1} = \kappa_{X_1 \hat{X}_1} \otimes \kappa_{Y_1 \hat{Y}_1},$$

where $\hat{X}_1$ and $\hat{Y}_1$ are the canonical purification registers of X_1 and Y_1, respectively, and

$$\kappa_{X_1} \equiv \phi_X \quad and \quad \kappa_{Y_1} \equiv \phi_Y.$$

Then, there exist two isometries $U' : \mathcal{H}_{\hat{X}_1} \otimes \mathcal{H}_A \otimes \mathcal{H}_X \to \mathcal{H}_A$ and $V' : \mathcal{H}_{\hat{Y}_1} \otimes \mathcal{H}_B \otimes \mathcal{H}_Y \to \mathcal{H}_B$ alongside a pure state γ_{XABY} such that

$$\phi_{XABY} \approx_{2(\sqrt{\varepsilon_1} + \sqrt{\varepsilon_2})} (U' \otimes V')(\kappa \otimes \gamma)((U')^\dagger \otimes (V')^\dagger).$$

To be precise, we obtain Equation (42) from Fact 24 via the assignment of registers (below the registers on the left are from Fact 24 and the registers on the right are the registers in this proof)

$$(\phi, \phi_X, \phi_Y, \phi_A, \phi_B, \kappa, \kappa_{X_1}, \kappa_{X_2}, \kappa_{\hat{X}_1}, \kappa_{\hat{X}_2}) \leftarrow (\theta', \theta'_{\hat{L}}, \theta'_{\hat{R}}, \theta'_{W'_1}, \theta'_{W'_2}, \rho, \rho_{\hat{L}}, \rho_{\hat{R}}, \rho_L, \rho_R),$$

and by setting $\varepsilon_1 = 0$ and $\varepsilon_2 = \varepsilon_{\text{leak}}$, which is justified by Claims 1 and 2, respectively. Furthermore, we have used Claims 1 and 2 to satisfy the conditions of state ϕ (which will be state θ' in this proof) in Fact 24.

We use U' and V' to construct the CPTP 2-split-state tampering maps $U : \mathcal{L}(\mathcal{H}_L \otimes \mathcal{H}_{W_1}) \to \mathcal{L}(\mathcal{H}_L)$ and $V : \mathcal{L}(\mathcal{H}_R \otimes \mathcal{H}_{W_2}) \to \mathcal{L}(\mathcal{H}_R)$ of $\mathcal{A}'$ as follows:

- On input the contents of registers ρ_L and γ_{W_1}, the map U first applies the unitary $U' : \mathcal{H}_L \otimes \mathcal{H}_{W_1} \to \mathcal{H}_{W'_1}$ to generate the contents of register $\theta'_{W'_1}$ (approximately). In particular, note that registers $L_{[t-1]} R_t L_t E_t$ are part of W'_1. Then, it uses the unitary U_t followed by qRec to generate τ_L and traces out the remaining registers of W'_1.

- On input the contents of registers ρ_R and γ_{W_2}, the map V first applies the unitary $V' : \mathcal{H}_R \otimes \mathcal{H}_{W_2} \to \mathcal{H}_{W'_2}$ to generate the contents of register $\theta'_{W'_2}$ (approximately). In particular, note that $R_{[2]}$ is part of W'_2 (this crucially uses the fact that $t > 2$). Then, it uses lrRec to generate τ_R from $\theta'_{R_{[2]}}$ and traces out the remaining registers of W'_2;

Let $\tau'_{\hat{L}\hat{R}LR} = (U \otimes V)(\rho \otimes \gamma_{W_1 W_2})$ be the state obtained after applying the 2-split-state tampering attack defined by $\mathcal{A}' = (U, V, \gamma_{W_1 W_2})$ on ρ in Figure 8. By inspecting the definition of θ' above, the state $\tau_{\hat{L}\hat{R}LR}$ obtained after applying the tampering attack defined by $\mathcal{A}$ on ρ in Figure 9 can be written as

$$\tau_{\hat{L}\hat{R}LR} = (\text{qRec} \otimes \text{lrRec}) \left(\left(U_t \theta' U_t^\dagger \right)_{\hat{L}\hat{R}L_{[t]} R_{[2]}} \right). \tag{43}$$

Recall from our discussion above that our main goal is to show that these two states τ and τ' are appropriately close in trace distance. Combining Equation (43) with Equation (42) and the postprocessing property of trace distance (Fact 4) yields

$$\tau_{\hat{L}\hat{R}LR} \approx_{2\sqrt{\varepsilon_{\text{leak}}}} \tau'_{\hat{L}\hat{R}LR}, \tag{44}$$

To see this, first note that registers $\theta'_{L_1 \dots L_{t-1} L_t R_t E_t}$ are obtained by applying U' to $\rho_L \otimes \gamma_{W_1}$. Then, the register τ_L is generated using qRec($U_t \theta'_{L_1 \dots L_{t-1} L_t R_t E_t} U_t^\dagger$). On the other hand, the register τ_R is
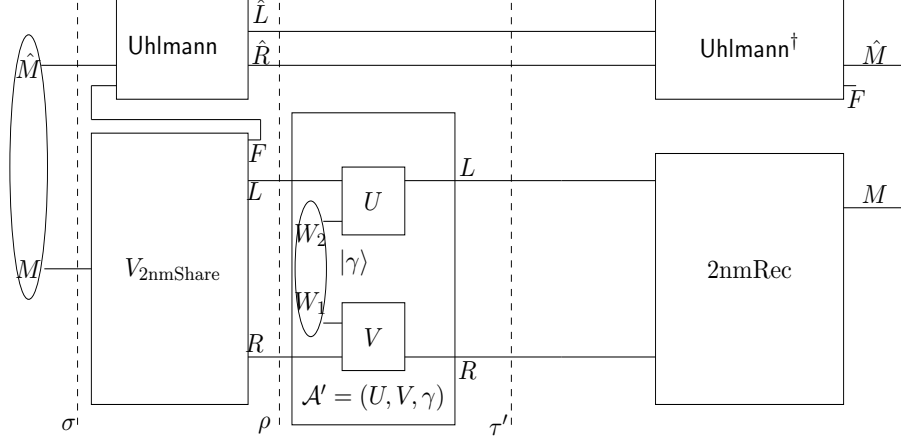
Figure 8: Tampering experiment for average-case 2-out-of-2 NMSS.

generated using lrRec with input the registers $\theta'_{R_{[2]}}$, which are themselves generated from ρ_R and γ_{W_2} via V'.

Recalling that the operations applied to τ' and τ in Figures 8 and 9, respectively, are the same, we conclude from Equation (44) and postprocessing (Fact 4) that the final decoded tampered state η in Figure 9 satisfies

$$\eta_{\hat{M}M} \approx_{2\sqrt{\varepsilon_{\mathsf{leak}}}} \mathrm{Tr}_F\left((\mathsf{Uhlmann}^\dagger \otimes 2\mathsf{nmRec})((U \otimes V)(\rho \otimes \gamma_{W_1 W_2})) \right). \tag{45}$$

Moreover, from the $\varepsilon_{\mathsf{nm}}$-non-malleability of $(2\mathsf{nmShare}, 2\mathsf{nmRec})$ we get that

$$\mathrm{Tr}_F\left((\mathsf{Uhlmann}^\dagger \otimes 2\mathsf{nmRec})((U \otimes V)(\rho \otimes \gamma_{W_1 W_2})) \right) \approx_{\varepsilon_{\mathsf{nm}}} p_{\mathcal{A}} \sigma_{\hat{M}M} + (1 - p_{\mathcal{A}}) \sigma_{\hat{M}} \otimes \zeta_M^{\mathcal{A}}, \tag{46}$$

where $(p_{\mathcal{A}}, \zeta_M^{\mathcal{A}})$ depend only on $(U, V, \gamma_{W_1 W_2})$, which further depend only on the initial adversary $\mathcal{A} = (U_1, U_2, \ldots, U_t, |\psi\rangle\langle\psi|_{E_1 \ldots E_p})$. Finally, combining Equations (45) and (46) with the triangle inequality leads to

$$\eta_{\hat{M}M} \approx_{\varepsilon_{\mathsf{nm}} + 2\sqrt{\varepsilon_{\mathsf{leak}}}} p_{\mathcal{A}} \sigma_{\hat{M}M} + (1 - p_{\mathcal{A}}) \sigma_{\hat{M}} \otimes \zeta_M^{\mathcal{A}},$$

which completes the proof of average-case non-malleability.

4.4.1 Proof of Claim 1

For convenience, we restate the relevant claim.

Claim 1. *We have that*

$$\theta'_{\hat{L}\hat{R}W_2'} = \theta'_{\hat{L}} \otimes \theta'_{\hat{R}W_2'}.$$

Proof. From Equation (41), we have that $\rho_{L\hat{L}R\hat{R}} = \rho_{L\hat{L}} \otimes \rho_{R\hat{R}}$. Further we have $\theta = (V_{\mathsf{qShare}} \otimes V_{\mathsf{lrShare}})\rho(V_{\mathsf{qShare}}^\dagger \otimes V_{\mathsf{lrShare}}^\dagger)$. Since V_{qShare} and V_{lrShare} act on two different registers L and R, respectively, we have that

$$\theta_{\hat{L}\tilde{L}L_{[p]}\hat{R}R_{[p]}\tilde{R}_{[p]}} = \theta_{\hat{L}\tilde{L}L_{[p]}} \otimes \theta_{\hat{R}R_{[p]}\tilde{R}_{[p]}}. \tag{47}$$
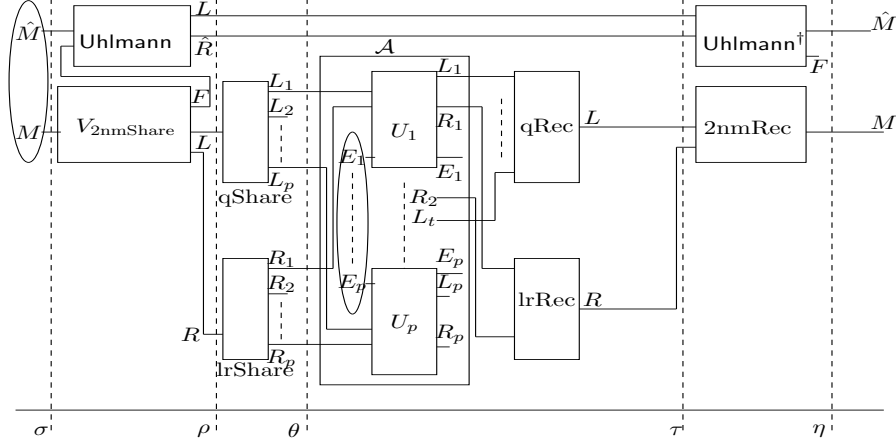
55

Figure 9: Tampering experiment for average-case t-out-of-p quantum NMSS.

Furthermore, using the fact that V_{qShare} is a t-out-of-p secret sharing scheme and invoking Lemma 2, we have that

$$\theta_{\hat{L}L_{[t-1]}} = \theta_{\hat{L}} \otimes \theta_{L_{[t-1]}} = \theta_{\hat{L}} \otimes U_{L_{[t-1]}}.$$

This means that

$$\theta_{\hat{L}L_{[t-1]}\hat{R}R_{[p]}\tilde{R}_{[p]}} = \theta_{\hat{L}} \otimes \theta_{L_{[t-1]}} \otimes \theta_{\hat{R}R_{[p]}\tilde{R}_{[p]}},$$

and so by postprocessing (Fact 4) it follows that

$$\theta'_{\hat{L}L_{[t-1]}R_{[t-1]}E_{[t-1]}E_{[t,p]}\hat{R}R_{[t,p]}\tilde{R}_{[p]}} = \theta'_{\hat{L}} \otimes \theta'_{L_{[t-1]}R_{[t-1]}E_{[t-1]}E_{[t,p]}\hat{R}R_{[t,p]}\tilde{R}_{[p]}},$$

which, again by postprocessing (Fact 4) and by the definition of W'_2, implies the desired statement. $\qquad\square$

4.4.2 Proof of Claim 2

For convenience, we restate the relevant claim here.

Claim 2. *We have that*

$$\theta'_{\hat{R}\hat{L}W'_1} \approx_{\varepsilon_{\text{leak}}} \theta'_{\hat{R}} \otimes \theta'_{\hat{L}W'_1}.$$

Proof. We use the 2-out-of-p $(\ell, \varepsilon_{\text{leak}})$-quantum-secure augmented leakage-resilient secret sharing property of lrShare to conclude that

$$\theta'_{\hat{R}R_tL_{[t-1]}E_{[t,p]}\hat{L}\tilde{L}L_{[t,p]}} \approx_{\varepsilon_{\text{leak}}} \theta'_{\hat{R}} \otimes \theta'_{R_tL_{[t-1]}E_{[t,p]}\hat{L}\tilde{L}L_{[t,p]}}. \tag{48}$$

Recalling the definition of W'_2, this corresponds exactly to the statement of Claim 2.

To see why Equation (48) holds, first recall that

$$\theta' = (U_1 \otimes \ldots \otimes U_{t-1} \otimes \mathbb{I}_t \otimes \ldots \mathbb{I}_p)(\theta \otimes |\psi\rangle\langle\psi|_{E_1\ldots E_p})(U_1^\dagger \otimes \ldots \otimes U_{t-1}^\dagger \otimes \mathbb{I}_t^\dagger \otimes \ldots \mathbb{I}_p^\dagger),$$

with θ illustrated in Figure 9. We now consider the following leakage attack on the $R_{[p]}$ registers: Taking into account the notation from Section 4.1, we set $T = [t-1]$ and for each $i \in [t-1]$ we

56

see $W_i = (L_i, E_i)$ as the entangled register for the local leakage adversary attacking R_i. Recall that the i-th tampering map U_i is applied to $(S_i, E_i) = (L_i, R_i, E_i)$, yielding tampered registers (L_i, R_i, E_i). Given this, we see L_i, which satisfies $|L_i| \leq \ell$, as the ℓ-bounded leakage on the i-th share R_i produced by the i-th local leakage adversary for lrShare with access to R_i and the entangled registers (L_i, E_i). Furthermore, we set the entangled register associated with the share R_t as $W_t = (E_{[t,p]}, \hat{L}, \tilde{L}, L_{[t,p]})$, and for $i > t$ we set the entangled registers W_i to be empty. Note that from Equation (47) we have that

$$\theta_{\hat{L}\tilde{L}L_{[p]}\hat{R}R_{[p]}\tilde{R}_{[p]}} = \theta_{\hat{L}\tilde{L}L_{[p]}} \otimes \theta_{\hat{R}R_{[p]}\tilde{R}_{[p]}},$$

and so the selected shared entangled state stored in registers $W_1, \ldots, W_n$ does not depend on the contents of R and $\hat{R}$. Invoking Theorem 8 and the augmented leakage-resilience property of $(\text{lrShare}, \text{lrRec})$ under this leakage attack yields Equation (48), which completes the proof. $\quad\square$

4.4.3 Proof of Fact 24

For convenience, we restate the relevant fact here.

Fact 24. *Let ϕ_{XABY} be a pure state such that*

$$\phi_{XBY} \approx_{\varepsilon_1} \phi_X \otimes \phi_{BY} \quad and \quad \phi_{YAX} \approx_{\varepsilon_2} \phi_Y \otimes \phi_{AX}.$$

Furthermore, let κ be a pure state such that

$$\kappa_{X_1\hat{X}_1Y_1\hat{Y}_1} = \kappa_{X_1\hat{X}_1} \otimes \kappa_{Y_1\hat{Y}_1},$$

where $\hat{X}_1$ and $\hat{Y}_1$ are the canonical purification registers of X_1 and Y_1, respectively, and

$$\kappa_{X_1} \equiv \phi_X \quad and \quad \kappa_{Y_1} \equiv \phi_Y.$$

Then, there exist two isometries $U' : \mathcal{H}_{\hat{X}_1} \otimes \mathcal{H}_A \otimes \mathcal{H}_X \to \mathcal{H}_A$ and $V' : \mathcal{H}_{\hat{Y}_1} \otimes \mathcal{H}_B \otimes \mathcal{H}_Y \to \mathcal{H}_B$ alongside a pure state γ_{XABY} such that

$$\phi_{XABY} \approx_{2(\sqrt{\varepsilon_1}+\sqrt{\varepsilon_2})} (U' \otimes V')(\kappa \otimes \gamma)((U')^\dagger \otimes (V')^\dagger).$$

Proof. We are given a state ϕ_{XABY} such that

$$\phi_{XBY} \approx_{\varepsilon_1} \phi_X \otimes \phi_{BY} \quad and \quad \phi_{YAX} \approx_{\varepsilon_2} \phi_Y \otimes \phi_{AX}.$$

We intend to show that we can generate a state close to ϕ using only $\kappa_{X_1Y_1} \equiv \phi_X \otimes \phi_Y$, shared entanglement γ, and isometries U, V. We use an independent copy of ϕ as shared entanglement, i.e., $\gamma_{XABY} \equiv \phi_{XABY}$. We first correlate registers $\kappa_{X_1\hat{X}_1}$ and shared entanglement γ_{XABY} using the isometry U to obtain state ϕ'. We next correlate registers $\kappa_{Y_1\hat{Y}_1}$ and state ϕ' using the isometry V to obtain ϕ''. Then, we show that state ϕ'' is the final state which will be close to ϕ in trace distance, as desired. We use Uhlmann's theorem (Fact 9) to argue closeness in trace distance.

Consider the pure state

$$\eta = \kappa_{X_1\hat{X}_1} \otimes \gamma_{XABY}.$$

Using the fact that $\kappa_{X_1} \equiv \phi_X$, we have that $\eta_{X_1BY} \equiv \phi_X \otimes \phi_{BY}$. Moreover, since $\phi_X \otimes \phi_{BY} \approx_{\varepsilon_1} \phi_{XBY}$ by hypothesis, it follows that $\eta_{X_1BY} \approx_{\varepsilon_1} \phi_{XBY}$.

We invoke Uhlmann's theorem (Fact 9) with the following assignment of registers (where the registers on the left are those from the statement of Fact 9 and the registers on the right are the registers used in this proof):

$$(\sigma_A, \rho_A, \sigma_{AC}, \rho_{AB}) \leftarrow (\eta_{X_1 BY}, \phi_{XBY}, \eta_{X_1 BY \hat{X}_1 XA}, \phi_{XBYA}).$$

This guarantees the existence of an isometry $U : \mathcal{H}_{\hat{X}_1} \otimes \mathcal{H}_A \otimes \mathcal{H}_X \to \mathcal{H}_A$ such that

$$\Delta_B \left(\phi'_{X_1 BYA}, \phi_{XBYA} \right) = \Delta_B(\eta_{X_1 BY}, \phi_{XBY}) \leq \sqrt{\varepsilon_1/2} \tag{49}$$

with $\phi'_{X_1 AYB} = U \left(\kappa_{X_1 \hat{X}_1} \otimes \gamma_{XABY} \right) U^\dagger$ and where the rightmost inequality follows from Fact 8 and the fact that $\eta_{X_1 BY} \approx_{\varepsilon_1} \phi_{XBY}$.

Now, consider the state $\eta' = \phi'_{X_1 AYB} \otimes \kappa_{Y_1 \hat{Y}_1}$. Observe that

$$\eta'_{X_1 AY_1} = \phi'_{X_1 A} \otimes \kappa_{Y_1} \equiv \phi'_{X_1 A} \otimes \phi_Y. \tag{50}$$

Using Fact 8 and the fact that $\phi_Y \otimes \phi_{AX} \approx_{\varepsilon_2} \phi_{YAX}$ (by hypothesis), we get

$$\Delta_B(\phi_Y \otimes \phi_{AX}, \phi_{YAX}) \leq \sqrt{\varepsilon_2/2}. \tag{51}$$

From Equation (49) and Fact 4, we get $\Delta_B(\phi'_{X_1 A}, \phi_{XA}) \leq \sqrt{\varepsilon_1/2}$. This further implies that

$$\Delta_B(\phi'_{X_1 A} \otimes \phi_Y, \phi_{XA} \otimes \phi_Y) \leq \sqrt{\varepsilon_1/2}. \tag{52}$$

Combining Equations (50) to (52) along with the triangle inequality, we have that

$$\Delta_B(\eta'_{X_1 AY_1}, \phi_{XAY}) \leq \sqrt{\varepsilon_1/2} + \sqrt{\varepsilon_2/2}.$$

We use Fact 9 with the following assignment of registers (below the registers on the left are from Fact 9 and the registers on the right are the registers in this proof),

$$(\sigma_A, \rho_A, \sigma_{AC}, \rho_{AB}) \leftarrow (\eta'_{X_1 AY_1}, \phi_{XAY}, \eta_{X_1 AY_1 \hat{Y}_1 YB}, \phi_{XAYB}).$$

From Fact 9 we get an isometry $V : \mathcal{H}_{\hat{Y}_1} \otimes \mathcal{H}_B \otimes \mathcal{H}_Y \to \mathcal{H}_B$ such that

$$\Delta_B \left(\phi''_{X_1 AY_1 B}, \phi_{XAYB} \right) = \Delta_B(\phi'_{X_1 AY_1}, \phi_{XAY}) \leq \sqrt{\varepsilon_1/2} + \sqrt{\varepsilon_2/2}, . \tag{53}$$

where,

$$\phi''_{X_1 AY_1 B} = V \left(\phi'_{X_1 AYB} \otimes \kappa_{Y_1 \hat{Y}_1} \right) V^\dagger = (U \otimes V)(\kappa \otimes \gamma)(U^\dagger \otimes V^\dagger).$$

From Equation (53) and Fact 8, we obtain the desired statement. □

4.5 From average-case to worst-case non-malleability

In Section 4.4, we showed that our secret sharing scheme (nmShare, nmRec) for quantum messages described in Section 4.2 is *average-case* $(\varepsilon_{\text{nm}} + 2\sqrt{\varepsilon_{\text{leak}}})$-non-malleable. To obtain our Theorem 3, we would like to upgrade from average-case to worst-case non-malleability. This can be done in exactly the same manner as was done for our 2-split-state NMC for quantum messages in Section 3.3, and so we avoid repeating the argument here. More precisely, the following easy extension of Lemma 9 holds in the secret sharing setting.

Lemma 10. *If* (Share, Rec) *is an average-case* $(\varepsilon_{\mathsf{priv}}, \varepsilon_{\mathsf{nm}})$*-non-malleable secret sharing scheme for quantum messages of length* b*, then it is also a worst-case* $(\varepsilon_{\mathsf{priv}}, \varepsilon'_{\mathsf{nm}})$*-non-malleable secret sharing scheme for quantum messages of length* b*, where* $\varepsilon'_{\mathsf{nm}} = 2^b \cdot \varepsilon_{\mathsf{nm}}$.

Combining Lemma 10 with the statistical privacy property shown in Section 4.3 and the average-case non-malleability property shown in Section 4.4 yields the following result.

Theorem 9. *Given a threshold* $t \geq 3$ *and a number of parties* p *such that* $t \leq p \leq 2t - 1$*, it holds that the scheme* (nmShare, nmRec) *described in Section 4.2 is a t-out-of-p* $(\varepsilon_{\mathsf{priv}}, \varepsilon'_{\mathsf{nm}})$*-non-malleable secret sharing scheme for quantum messages of length* b *with* $\varepsilon'_{\mathsf{nm}} = 2^b(\varepsilon_{\mathsf{nm}} + 2\sqrt{\varepsilon_{\mathsf{leak}}})$.

It remains to set the parameters in Theorem 9 (which come from the underlying objects used to define our secret sharing scheme in Section 4.2) appropriately so that we can obtain Theorem 3.

4.6 Setting the parameters

To conclude our argument, we now show how to instantiate the objects used to define our secret sharing scheme in Section 4.2 to get Theorem 3. First, due to Theorem 6, the underlying 2-out-of-2 $(\varepsilon_{\mathsf{priv}}, \varepsilon_{\mathsf{nm}})$-non-malleable scheme (2nmShare, 2nmRec) can be set so that $\varepsilon_{\mathsf{priv}} = \varepsilon_{\mathsf{nm}} = 2^{-n^{\Omega(1)}}$ and that the quantum left share and classical right share have lengths b_1 and b_2, respectively, satisfying $b_1 + b_2 = n$, provided that the input quantum message has length $b \leq n^c$ for some sufficiently small absolute constant $c > 0$. Since $b_1 \leq n$, the scheme (qShare, qRec) produces shares of length $\ell = \mathrm{poly}(p, n)$ by Fact 22. Finally, by Theorem 8, the scheme (lrShare, lrRec) can be set so that it is $(\ell = \mathrm{poly}(p, n), \varepsilon_{\mathsf{leak}} = 2^{-n^{\Omega(1)}})$-augmented leakage-resilient with shares of length $\mathrm{poly}(p, n)$. Additionally, all of these procedures run in time $\mathrm{poly}(p, n)$. Combining this with Theorem 9 yields the desired Theorem 3, provided that the input quantum message length b is at most n^c for a sufficiently small absolute constant $c > 0$. We restate the resulting theorem here for convenience.

Theorem 3 (Split-state threshold NMSS schemes for quantum messages)**.** *There exist constants* $c, C > 0$ *and an integer* $n_0 \in \mathbb{N}$ *such that the following holds for any number of parties* p *and threshold* $t \geq 3$ *such that* $t \leq p \leq 2t - 1$ *and for any* $n \geq n_0$*: There exists a family of t-out-of-p* $(\varepsilon_{\mathsf{priv}} = \varepsilon, \varepsilon_{\mathsf{nm}} = \varepsilon)$*-non-malleable secret sharing schemes for quantum messages with shares of size at most* $(pn)^C$*, message length* $\lfloor n^c \rfloor$*, and error* $\varepsilon = 2^{-n^c}$*. Furthermore, the sharing and reconstruction procedures of this scheme can be computed in time polynomial in* p *and* n.

4.7 Quantum-secure classical non-malleable secret sharing schemes

In this section, we present and analyze non-malleable threshold secret sharing schemes for classical messages secure against quantum adversaries with shared entanglement. Here, both the sharing and reconstruction procedures are classical, and we call these schemes *quantum-secure non-malleable*. We obtain such schemes via a simpler and entirely analogous realization of the approach laid out earlier in this Section 4, combining a known split-state non-malleable code for classical messages from [BBJ23] with Shamir's secret sharing scheme and a quantum-secure leakage-resilient secret sharing scheme for classical messages.

We begin by defining threshold quantum-secure non-malleable secret sharing schemes. This definition follows along the lines of Definition 2 specialized to classical messages and with a different definition of the register $\hat{M}$. Let σ_M be a classical message, and set $\hat{M}$ to contain a copy of this

message.[12] We consider a classical scheme $(\mathrm{nmShare}, \mathrm{nmRec})$ with a classical sharing procedure $\mathrm{nmShare} : \mathcal{L}(\mathcal{H}_M) \to \mathcal{L}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2} \otimes \cdots \otimes \mathcal{H}_{S_n})$ and a classical reconstruction procedure $\mathrm{nmRec} : \mathcal{L}(\bigotimes_{i \in T} \mathcal{H}_{S_i}) \to \mathcal{L}(\mathcal{H}_M)$, where $\mathcal{L}(\mathcal{H})$ is the space of all linear operators in the Hilbert space $\mathcal{H}$ and the reconstruction procedure nmRec acts on any authorized set T.

Let $\rho = \mathrm{nmShare}(\sigma_{M\hat{M}})$ be the classical sharing of σ_M, and denote by $S_1, S_2, \ldots, S_p$ the classical registers corresponding to the p resulting shares. The most basic property we require of this scheme is correctness, i.e., for any subset of shares $T \subseteq [p]$ such that $|T| \geq t$, we must have that

$$\mathrm{nmRec}(\rho_{\hat{M}S_T}) = \sigma_{M\hat{M}}.$$

A split-state tampering adversary $\mathcal{A}_T$ for some authorized subset T of size $|T| = t$ is specified as

$$\mathcal{A}_T = \left(\bigotimes_{i \in T} U_i, |\psi\rangle_{W_1 W_2 \ldots W_p} \right),$$

where $|\psi\rangle_{W_1 W_2 \ldots W_p}$ represents the entangled quantum state shared among tampering adversaries and $U_i : \mathcal{L}(\mathcal{H}_{S_i}) \otimes \mathcal{L}(\mathcal{H}_{W_i}) \to \mathcal{L}(\mathcal{H}_{S_i}) \otimes \otimes \mathcal{L}(\mathcal{H}_{W_i})$ are the tampering maps. We denote the resulting tampered state by

$$\tau^{\mathcal{A}_T} = \left(\left(\bigotimes_{i \in T} U_i \right) \otimes \left(\bigotimes_{j \notin T} \mathbb{I} \right) \right) \left(\mathrm{nmShare}(\sigma) \otimes |\psi\rangle\langle\psi|_{W_1 \cdots W_p} \right) \left(\left(\bigotimes_{i \in T} U_i^\dagger \right) \otimes \left(\bigotimes_{j \notin T} \mathbb{I}^\dagger \right) \right).$$

We are now ready to define threshold quantum-secure non-malleable secret sharing schemes.

Definition 21 (Threshold quantum-secure non-malleable secret sharing scheme). *The coding scheme* $(\mathrm{nmShare}, \mathrm{nmRec})$ *is said to be a* t-out-of-p $(\varepsilon_{\mathsf{priv}}, \varepsilon_{\mathsf{nm}})$-quantum-secure non-malleable secret sharing *scheme, if for any classical message* $\sigma_M \in \mathcal{D}(\mathcal{H}_M)$ *(with copy* $\sigma_{\hat{M}}$ *in* $\sigma_{M\hat{M}}$*) the following properties are satisfied:*

- **Correctness:** *For any* $T \subseteq [p]$ *such that* $|T| \geq t$ *it holds that*

$$\mathrm{nmRec}(\mathrm{nmShare}(\sigma_{M\hat{M}})_{S_T}) = \sigma_{M\hat{M}},$$

  where we write $S_T = (S_i)_{i \in T}$.

- **Statistical privacy:** *For any* $T \subseteq [p]$ *such that* $|T| \leq t - 1$ *it holds that*

$$\mathrm{nmShare}(\sigma_{M\hat{M}})_{\hat{M}S_T} \approx_{\varepsilon_{\mathsf{priv}}} \sigma_{\hat{M}} \otimes \zeta_{S_T},$$

  where ζ_{S_T} *is a fixed state independent of* σ_M.

- **Non-malleability:** *For any* $T \subseteq [p]$ *such that* $|T| = t$ *and for every split-state tampering adversary* $\mathcal{A}_T$ *as above, it holds that*

$$\mathrm{nmRec}(\tau^{\mathcal{A}_T}_{\hat{M}S_T}) \approx_{\varepsilon_{\mathsf{nm}}} p_{\mathcal{A}_T} \cdot \sigma_{\hat{M}M} + (1 - p_{\mathcal{A}_T})\sigma_{\hat{M}} \otimes \gamma_M^{\mathcal{A}_T}, \tag{54}$$

  where $p_{\mathcal{A}_T} \in [0, 1]$ *and* $\gamma_M^{\mathcal{A}_T}$ *depend only on the adversary* $\mathcal{A}_T$.

  If Equation (54) is only guaranteed to hold when $\sigma_M = U_M$*, we say that* $(\mathrm{nmShare}, \mathrm{nmRec})$ *is an* average-case t-out-of-p $(\varepsilon_{\mathsf{priv}}, \varepsilon_{\mathsf{nm}})$-quantum-secure non-malleable secret sharing scheme.

---

[12] Here, the register $\hat{M}$ is a classical copy of M, while in our definition of NMSS schemes for quantum messages $\hat{M}$ is the canonical purification register of M.

We will require the following known quantum-secure 2-out-of-2 non-malleable secret sharing scheme from [BBJ23], along with standard Shamir's threshold secret sharing scheme.

Theorem 10 (Average-case 2-out-of-2 quantum-secure non-malleable secret sharing scheme with constant rate [BBJ23]). *For any fixed constant $c > 0$, there exists an average-case 2-out-of-2 $(\varepsilon_{\mathsf{priv}}, \varepsilon_{\mathsf{nm}})$-quantum-secure non-malleable secret sharing scheme for classical messages with code-word length n, message length at most $\left(\frac{1}{5} - c\right) n$, $\varepsilon_{\mathsf{priv}} = 2^{-n^{\Omega_c(1)}}$ and $\varepsilon_{\mathsf{nm}} = 2^{-n^{\Omega_c(1)}}$, where $\Omega_c(\cdot)$ hides constants which depend only on c. Furthermore, the sharing and reconstruction procedures can be computed in time $\mathrm{poly}(n)$.*

Fact 25 (Classical Shamir's secret sharing [Sha79]). *For any number of parties p and threshold t such that $t \leq p$, there exists a t-out-of-p secret sharing scheme $(\mathrm{Share}, \mathrm{Rec})$ for classical messages of length b with share size at most $\max(p, b)$, where both the sharing and reconstruction procedures run in time $\mathrm{poly}(p, b)$.*

4.7.1 Our candidate quantum-secure non-malleable secret sharing scheme

We leverage the 2-out-of-2 quantum-secure non-malleable secret sharing scheme from Theorem 10 and our quantum-secure augmented leakage-resilient secret sharing scheme for classical messages from Theorem 8 to construct quantum-secure non-malleable threshold secret sharing schemes. As mentioned before, we accomplish this via the same techniques we used to construct our NMSS schemes for quantum messages earlier in this section.

Fix a threshold $t \geq 3$ and a number of parties p such that $t \leq p$. We will require the following objects:

- A 2-out-of-2 $(\varepsilon_{\mathsf{nm}} = \varepsilon, \varepsilon_{\mathsf{priv}} = \varepsilon)$-quantum-secure non-malleable secret sharing scheme, which we denote by $(\mathrm{2nmShare}, \mathrm{2nmRec})$, for messages of length b with a left share of length b_1 and a right share of length b_2, guaranteed by Theorem 10;

- A t-out-of-p secret sharing scheme $(\mathrm{Share}, \mathrm{Rec})$ for messages of length b_1 with shares of length at most ℓ, guaranteed by Fact 25;

- A 2-out-of-p $(\ell, \varepsilon_{\mathsf{leak}})$-quantum-secure augmented leakage-resilient secret sharing scheme, which we denote by $(\mathrm{lrShare}, \mathrm{lrRec})$, for classical messages of length b_2, guaranteed by Theorem 8.

We proceed to describe our candidate t-out-of-p scheme $(\mathrm{nmShare}, \mathrm{nmRec})$. On input a classical message σ_M (with a copy $\hat{M}$ in $\sigma_{M\hat{M}}$), the classical sharing algorithm $\mathrm{nmShare}(\sigma)$ proceeds as follows:

1. Compute the encoding $\rho_{LR} = \mathrm{2nmShare}(\sigma_M)$;

2. Apply Share to the contents of register L to obtain p shares stored in registers $L_1, \ldots, L_p$;

3. Apply $\mathrm{lrShare}$ to the contents of register R to obtain p shares stored in registers $R_1, \ldots, R_p$;

4. Form the i-th final share $S_i = (L_i, R_i)$.

The corresponding reconstruction algorithm nmRec is straightforward. The differences between our quantum-secure NMSS scheme considered here and the NMSS scheme for quantum messages from Section 4.2 are the following:

- The NMSS scheme for quantum messages from Section 4.2 uses (2nmShare, 2nmRec) guaranteed by Theorem 6, while we use (2nmShare, 2nmRec) guaranteed by Theorem 10.

- The NMSS scheme for quantum messages from Section 4.2 uses quantum Shamir's secret sharing (qShare, qRec) guaranteed by Fact 22, while we use classical Shamir's secret sharing (Share, Rec) guaranteed by Fact 25. This ensures that for classical messages we get t-out-of-p NMSS schemes for any $t \leq p$ and $t \geq 3$.

- In the non-malleability argument for our NMSS scheme for quantum messages in Section 4.4, we have used the Uhlmann isometry to create the coherent copies of quantum registers. For the non-malleability argument of our quantum-secure NMSS scheme we can completely ignore such an argument and just copy the classical registers and proceed with the rest of argument.

We have the following result.

Theorem 11 (Average-case t-out-of-p quantum-secure non-malleable secret sharing scheme). *The coding scheme* (nmShare, nmRec) *as described in Section 4.7.1 is an average-case* $(\varepsilon_{\mathsf{priv}}, \varepsilon_{\mathsf{nm}} + 2\sqrt{\varepsilon_{\mathsf{leak}}})$-*quantum-secure non-malleable secret sharing scheme.*

Proof. The correctness and runtime of this coding scheme are clear. Establishing the statistical privacy and average-case non-malleability of our scheme follows analogously to the arguments in Section 4.3 and Section 4.4, respectively, and we opt to not repeat them. □

As before, it remains to upgrade average-case non-malleability to worst-case non-malleability. This is also generically possible in the present setting, as captured by the following lemma whose proof is analogous to those of Lemmas 9 and 10.

Lemma 11. *If* (Share, Rec) *is an average-case* $(\varepsilon_{\mathsf{priv}}, \varepsilon_{\mathsf{nm}})$-*quantum-secure non-malleable secret sharing scheme for messages of length b, then it is also a worst-case* $(\varepsilon_{\mathsf{priv}}, \varepsilon'_{\mathsf{nm}})$-*quantum-secure non-malleable secret sharing scheme for messages of length b, where $\varepsilon'_{\mathsf{nm}} = 2^b \cdot \varepsilon_{\mathsf{nm}}$.*

Finally, the choices of parameters used to instantiate our construction in this section are analogous to those of Section 4.6. We obtain the following final result by combining Theorem 11 with Lemma 11.

Theorem 12 (Threshold quantum-secure NMSS schemes). *There exists a constant $c \in (0, 1)$ such that the following holds: Given a threshold $t \geq 3$ and a number of parties p such that $t \leq p$, there exists a* $(\varepsilon_{\mathsf{priv}} = \varepsilon, \varepsilon_{\mathsf{nm}} = \varepsilon)$-$t$-*out-of-$p$ quantum-secure non-malleable secret sharing scheme for messages with shares of size at most* $\mathrm{poly}(p, n)$, *any message length at most n^c, and $\varepsilon = 2^{-n^{\Omega(1)}}$. Furthermore, the sharing and reconstruction procedures of this scheme can be computed in time* $\mathrm{poly}(p, n)$.

References

[AAG+16] Divesh Aggarwal, Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, and Manoj Prabhakaran. Optimal computational split-state non-malleable codes. In Eyal Kushilevitz and Tal Malkin, editors, *Theory of Cryptography*, pages 393–417, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[ABJ24]   Divesh Aggarwal, Naresh Goud Boddu, and Rahul Jain. Quantum secure non-malleable codes in the split-state model. *IEEE Transactions on Information Theory*, 70(1):349–371, 2024.

[ABW09]   Andris Ambainis, Jan Bouda, and Andreas Winter. Nonmalleable encryption of quantum information. *Journal of Mathematical Physics*, 50(4):042106, 2009.

[ADKO15]   Divesh Aggarwal, Stefan Dziembowski, Tomasz Kazana, and Maciej Obremski. Leakage-resilient non-malleable codes. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *Theory of Cryptography*, pages 398–426, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[ADL18]   Divesh Aggarwal, Yevgeniy Dodis, and Shachar Lovett. Non-malleable codes from additive combinatorics. *SIAM Journal on Computing*, 47(2):524–546, 2018. Preliminary version in STOC 2014.

[ADN+19]   Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, João Ribeiro, and Mark Simkin. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 510–539, Cham, 2019. Springer International Publishing.

[AKO+22]   Divesh Aggarwal, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, Maciej Obremski, and Sruthi Sekar. Rate one-third non-malleable codes. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2022, page 1364–1377, New York, NY, USA, 2022. Association for Computing Machinery.

[AM17]   Gorjan Alagic and Christian Majenz. Quantum non-malleability and authentication. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017*, pages 310–341, Cham, 2017. Springer International Publishing.

[AO20]   Divesh Aggarwal and Maciej Obremski. A constant rate non-malleable code in the split-state model. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1285–1294, Los Alamitos, CA, USA, nov 2020. IEEE Computer Society.

[BBJ23]   Rishabh Batra, Naresh Goud Boddu, and Rahul Jain. Quantum secure non-malleable randomness encoder and its applications, 2023. https://arxiv.org/abs/2308.07340.

[BCG+02]   Howard Barnum, Claude Crepeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2002*, pages 449–458, 2002.

[BCL+20]   Marshall Ball, Eshan Chattopadhyay, Jyun-Jie Liao, Tal Malkin, and Li-Yang Tan. Non-malleability against polynomial tampering. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020*, pages 97–126. Springer, 2020.

[BDKM16] Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, and Tal Malkin. Non-malleable codes for bounded depth, bounded fan-in circuits. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016*, pages 881–908. Springer, 2016.

[BDKM18] Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, and Tal Malkin. Non-malleable codes from average-case hardness: AC^0, decision trees, and streaming space-bounded tampering. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018*, pages 618–650. Springer, 2018.

[Ber23] Thiago Bergamaschi. Pauli manipulation detection codes and applications to quantum communication over adversarial channels, 2023. Available at https://arxiv.org/abs/2304.06269.

[BFMV22] Gianluca Brian, Sebastian Faust, Elena Micheli, and Daniele Venturi. Continuously non-malleable codes against bounded-depth tampering. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology - ASIACRYPT 2022*, pages 384–413. Springer, 2022.

[BFO+20] Gianluca Brian, Antonio Faonio, Maciej Obremski, Mark Simkin, and Daniele Venturi. Non-malleable secret sharing against bounded joint-tampering attacks in the plain model. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020*, pages 127–155, Cham, 2020. Springer International Publishing.

[BFRV22] Gianluca Brian, Antonio Faonio, João Ribeiro, and Daniele Venturi. Short non-malleable codes from related-key secure block ciphers, revisited. *IACR Transactions on Symmetric Cryptology*, 2022(3):1–19, Sep. 2022.

[BFV21] Gianluca Brian, Antonio Faonio, and Daniele Venturi. Continuously non-malleable secret sharing: Joint tampering, plain model and capacity. In Kobbi Nissim and Brent Waters, editors, *Theory of Cryptography*, pages 333–364, Cham, 2021. Springer International Publishing.

[BGW19] Marshall Ball, Siyao Guo, and Daniel Wichs. Non-malleable codes for decision trees. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019*, pages 413–434. Springer, 2019.

[BJK21] Naresh Goud Boddu, Rahul Jain, and Upendra Kapshikar. Quantum secure non-malleable-extractors, 2021. Available at https://arxiv.org/abs/2109.03097.

[BJL23] Naresh Goud Boddu, Rahul Jain, and Han-Hsuan Lin. On relating one-way classical and quantum communication complexities. *Quantum*, 7:1010, May 2023. *Contributed talk at 21th Asian Quantum Information Science Conference.*

[Bla79] G. R. Blakley. Safeguarding cryptographic keys. In *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318, 1979.

[BS19] Saikrishna Badrinarayanan and Akshayaram Srinivasan. Revisiting non-malleable secret sharing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 593–622, Cham, 2019. Springer International Publishing.

[BW16]   Anne Broadbent and Evelyn Wainewright. Efficient simulation for quantum message authentication. In Anderson C.A. Nascimento and Paulo Barreto, editors, *Information Theoretic Security*, pages 72–91, Cham, 2016. Springer International Publishing.

[CG14]   Mahdi Cheraghchi and Venkatesan Guruswami. Non-malleable coding against bit-wise and split-state tampering. In *Proceedings of Theory of Cryptography Conference (TCC)*, pages 440–464, 2014. Extended version in Journal of Cryptology.

[CG16]   Mahdi Cheraghchi and Venkatesan Guruswami. Capacity of non-malleable codes. *IEEE Transactions on Information Theory*, 62(3):1097–1118, 2016.

[CGL99]   Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83:648–651, Jul 1999.

[CGL20]   Eshan Chattopadhyay, Vipul Goyal, and Xin Li. Nonmalleable extractors and codes, with their many tampered extensions. *SIAM Journal on Computing*, 49(5):999–1040, 2020. Preliminary version in STOC 2016.

[CGLR23]   Alper Cakan, Vipul Goyal, Chen-Da Liu-Zhang, and João Ribeiro. Unbounded leakage-resilience and leakage-detection in a quantum world. Cryptology ePrint Archive, Paper 2023/410, 2023.

[CHSH69]   John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[CKOS22]   Nishanth Chandran, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, and Sruthi Sekar. Short leakage resilient and non-malleable secret sharing schemes. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022*, pages 178–207. Springer, 2022.

[CLLW16]   Richard Cleve, Debbie Leung, Li Liu, and Chunhao Wang. Near-linear constructions of exact unitary 2-designs. *Quantum Info. Comput.*, 16(9–10):721–756, jul 2016.

[CLW14]   Kai-Min Chung, Xin Li, and Xiaodi Wu. Multi-source randomness extractors against quantum side information, and their applications. 2014.

[Dat09]   Nilanjana Datta. Min- and max- relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55:2816–2826, 2009.

[DCEL09]   Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A*, 80:012304, Jul 2009.

[DKO13]   Stefan Dziembowski, Tomasz Kazana, and Maciej Obremski. Non-malleable codes from two-source extractors. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, pages 239–257, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[DPW18]   Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. Non-malleable codes. *J. ACM*, 65(4), April 2018. Preliminary version in ICS 2010.

[FHMV17] Sebastian Faust, Kristina Hostáková, Pratyay Mukherjee, and Daniele Venturi. Non-malleable codes for space-bounded tampering. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017*, pages 95–126. Springer, 2017.

[FKM18] Serge Fehr, Pierre Karpman, and Bart Mennink. Short non-malleable codes from related-key secure block ciphers. *IACR Transactions on Symmetric Cryptology*, 2018(1):336–352, Mar. 2018.

[FMNV14] Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, and Daniele Venturi. Continuous non-malleable codes. In Yehuda Lindell, editor, *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014*, pages 465–488. Springer, 2014.

[FV19] Antonio Faonio and Daniele Venturi. Non-malleable secret sharing in the computational setting: Adaptive tampering, noisy-leakage resilience, and improved rate. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 448–479, Cham, 2019. Springer International Publishing.

[FvdG06] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inf. Theor.*, 45(4):1216–1227, September 2006.

[GK18a] Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2018, page 685–698, New York, NY, USA, 2018. Association for Computing Machinery.

[GK18b] Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing for general access structures. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology – CRYPTO 2018*, pages 501–530, Cham, 2018. Springer International Publishing.

[Got00] Daniel Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, Mar 2000.

[GPR16] Vipul Goyal, Omkant Pandey, and Silas Richelson. Textbook non-malleable commitments. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '16, page 1128–1141, New York, NY, USA, 2016. Association for Computing Machinery.

[GSZ21] Vipul Goyal, Akshayaram Srinivasan, and Chenzhi Zhu. Multi-source non-malleable extractors and applications. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 468–497, Cham, 2021. Springer International Publishing.

[HBB99] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829–1834, Mar 1999.

[JPY14] Rahul Jain, Attila Pereszlényi, and Penghui Yao. A parallel repetition theorem for entangled two-player one-round games under product distributions. In *2014 IEEE 29th Conference on Computational Complexity (CCC)*, pages 209–216, 2014.

[JRS02]   Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, pages 429–438, 2002.

[KKI99]   Anders Karlsson, Masato Koashi, and Nobuyuki Imoto. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A*, 59:162–168, Jan 1999.

[KLT16]   Aggelos Kiayias, Feng-Hao Liu, and Yiannis Tselekounis. Practical non-malleable codes from ℓ-more extractable hash functions. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 1317–1328, New York, NY, USA, 2016. Association for Computing Machinery.

[KOS18]   Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, and Sruthi Sekar. Non-malleable randomness encoders and their applications. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 589–617, Cham, 2018. Springer International Publishing.

[Li15]   Xin Li. Three-source extractors for polylogarithmic min-entropy. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 863–882, 2015.

[Li17]   Xin Li. Improved non-malleable extractors, non-malleable codes and independent source extractors. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, page 1144–1156, New York, NY, USA, 2017. Association for Computing Machinery.

[Li19]   Xin Li. Non-malleable extractors and non-malleable codes: Partially optimal constructions. In *Proceedings of the 34th Computational Complexity Conference*, CCC '19, Dagstuhl, DEU, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[Li23]   Xin Li. Two source extractors for asymptotically optimal entropy, and (many) more, 2023. Available at https://arxiv.org/abs/2303.06802. To appear at FOCS 2023.

[LL12]   Feng-Hao Liu and Anna Lysyanskaya. Tamper and leakage resilience in the split-state model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, pages 517–532, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[NC00]   Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[Ozo16]   Maris Ozols. Lecture 5: Quantum information processing protocols. Quantum computing: Exercise sheet 2. Available at https://www.cl.cam.ac.uk/teaching/1617/QuantComp/exercise2.pdf, 2016.

[Sha79]   Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, nov 1979.

[Smi00]   Adam D. Smith. Quantum secret sharing for general access structures. *arXiv e-prints*, January 2000. Available at https://arxiv.org/abs/quant-ph/0001087.

[SV19]   Akshayaram Srinivasan and Prashant Nalini Vasudevan. Leakage resilient secret sharing and applications. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, pages 480–509, Cham, 2019. Springer International Publishing.

[Uhl76]   A. Uhlmann. The "transition probability" in the state space of a *-algebra. *Rep. Math. Phys.*, 9:273–279, 1976.

[Wat11]   John Watrous. Chapter 5, Naimark's theorem; characterizations of channels. Lecture notes on Theory of Quantum Information, 2011.

[Wat18]   John Watrous. *The Theory of Quantum Information*. Cambridge University Press, Cambridge, UK, 2018.