Quantum Secure Non-Malleable Codes in the Split-State Model

Divesh Aggarwal, Naresh Goud Boddu, and Rahul Jain

Abstract—Non-malleable codes introduced by Dziembowski et al. (2018) encode a classical message $S$ in a manner such that the tampered codeword either decrypts to the original message $S$ or a message that is unrelated/independent of $S$. Constructing non-malleable codes for various tampering function families has received significant attention in the recent years. We consider the well studied (2-part) split-state model, in which the message $S$ is encoded into two parts $X$ and $Y$, and the adversary is allowed to arbitrarily tamper with each $X$ and $Y$ individually. Non-malleable codes in the split-state model have found applications in other important security notions like non-malleable commitments and non-malleable secret sharing. Thus, it is vital to understand if such non-malleable codes are secure against quantum adversaries. We consider the security of non-malleable codes in the split-state model when the adversary is allowed to make use of arbitrary entanglement to tamper the parts $X$ and $Y$. We construct explicit quantum secure non-malleable codes in the split-state model. Our construction of quantum secure non-malleable codes is based on the recent construction of quantum secure 2-source non-malleable extractors by Boddu et al. (2021). 1) We extend the connection of Cheraghchi and Guruswami (2016) between 2-source non-malleable extractors and non-malleable codes in the split-state model in the classical setting to the quantum setting, i.e. we show that explicit quantum secure 2-source non-malleable extractors in $(k_1,k_2)$-qqa-state framework of Boddu et al. (2021) give rise to explicit quantum secure non-malleable codes in the split-state model. 2) We construct the first quantum secure non-malleable code with efficient encoding and decoding procedures for message length $m = 2^{\Omega(1)}$, error $\epsilon = 2^{-n^{\Omega(1)}}$ and codeword of size $2n$. Prior to this work, it remained open to provide such quantum secure non-malleable code even for a single bit message in the split-state model. 3) We also study its natural extension when the tampering of the codeword is performed $t$-times. We construct quantum secure one-many non-malleable code with efficient encoding and decoding procedures for $t = n^{\Omega(1)}$, message length $m = n^{\Omega(1)}$, error $\epsilon = 2^{-n^{\Omega(1)}}$ and codeword of size $2n$. 4) As an application, we also construct the first quantum secure 2-out-of-2 non-malleable secret sharing scheme for messages of length $\Omega(n)$.

Index Terms—Multi-source extractors, non-malleable extractors, non-malleable codes, quantum security.

I. INTRODUCTION

In a seminal work, Dziembowski et al. [1] introduced non-malleable codes to provide a meaningful guarantee for the encoded message $S$ in situations where traditional error-correction or even error-detection is impossible. Informally, non-malleable codes encode a classical message $S$ in a manner such that tampering the codeword results in decoder either outputting the original message $S$ or a message that is unrelated/independent of $S$. Using probabilistic arguments, [1] showed the existence of such non-malleable codes against any family $\mathcal{F}$ of tampering functions of size as large as $2^{\alpha n}$ for any fixed constant $\alpha < 1$, where $n$ is the length of codeword for messages of length $\Omega(n)$.

Subsequent works continued to study non-malleable codes in various tampering models. Perhaps the most well known of these tampering function families is the so called split-state model introduced by Liu and Lysyanskaya [4], who constructed efficient constant rate non-malleable codes against computationally bounded adversaries under strong cryptographic assumptions. We refer to the (2-part) split-state model as the split-state model in this paper. In the split-state model, the message $S$ is encoded into two parts, $X$ and $Y$, after which the adversary is allowed to arbitrarily tamper $(X,Y) \rightarrow (X',Y')$ such that $(X',Y') = (f(X),g(Y))$ for any functions $(f,g)$ such that $f,g : \{0,1\}^n \rightarrow \{0,1\}^m$. Dziembowski, Kazana and Obremski [5] proposed a construction that provides non-malleable codes for a single bit message based on strong extractors. Subsequently, multiple works considered non-malleable codes for multi-bit messages leading to constant rate non-malleable codes in the split-state model [3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15].

More formally, a non-malleable code in the split-state model in the classical setting can be defined as follows. Let $n,m$ represent positive integers and $k,e,e' > 0$ represent reals. Let $\mathcal{F}$ denote the set of all functions $f : \{0,1\}^n \rightarrow \{0,1\}^m$. 0018-9448 © 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
We consider an encoding and decoding scheme \((\text{Enc}, \text{Dec})\) in the split-state model where \(\text{Enc}(S) = (X, Y)\). Here \(S \sim U_m\) \((U_m\) is uniform distribution on \(m\) bits) represents the plaintext/message and \(X, Y \in \{0, 1\}^n\) are the two parts of the codeword. \(\text{Enc}\) is a randomized function and \(\text{Dec}(X, Y)\) is a deterministic function, such that \(\Pr(\text{Dec}(\text{Enc}(S)) = S) = 1\).

We define the function \(\text{copy} : \{0, 1\}^* \cup \{\text{same}\} \times \{0, 1\}^* \rightarrow \{0, 1\}^*\). \(\text{copy}(x, s) = s\) if \(x = \text{same}\), otherwise \(\text{copy}(x, s) = x\).

**Definition 1 (Non-Malleable Codes in the Split-State Model)**: \((\text{Enc}, \text{Dec})\) is an \((m, n, \varepsilon)\)-non-malleable code with respect to a family of tampering functions \(\mathcal{F} \times \mathcal{F}\), if for every \(f = (g_1, g_2) \in \mathcal{F} \times \mathcal{F}\), there exists a random variable \(D_f = D_{(g_1, g_2)}\) on \(\{0, 1\}^m \cup \{\text{same}\}\) which is independent of the randomness in \(\text{Enc}\) such that for all messages \(s \in \{0, 1\}^m\), it holds that

\[
\|\text{Dec}(f(\text{Enc}(s))) - \text{copy}(D_f, s)\|_1 \leq \varepsilon.
\]

Intuitively, if the adversary doesn’t tamper the codeword (in which case \((X, Y) = (X', Y')\)), the decoded message is same (captured by the variable same) as original message \(S\). If the adversary does tamper the codeword (in which case either \(X \neq X'\) or \(Y \neq Y'\)), the decoded message is (approximately) distributed according to a distribution \((D_f\) minus same normalized) that only depends on \(f\) and is independent of the original message \(S\).

1) **Previous Classical Results in the Split-State Model**: [5] constructed the first non-malleable code for a 1-bit message. Following that Aggarwal et al. [8] gave the first information-theoretic construction for \(m\)-bit messages, but the length of codeword being \(2n = m^{O(1)}\). Chattopadhyay et al. [6] gave a non-malleable code for message length \(m = n^{\Omega(1)}\), error \(\varepsilon = 2^{-n^{O(1)}}\) and codeword of size \(2n\). Improving upon the work of [6], Li [13] gave a non-malleable code for message length \(m = n^{\Omega(1)}\), error \(\varepsilon = 2^{-n^{O(1)}}\) and codeword of size \(2n\). Only recently Aggarwal and Obrenski [14] gave the first constant rate non-malleable code for message length \(m = \Omega(n)\), error \(\varepsilon = 2^{-n^{\Omega(1)}}\) and codeword of size \(2n\). This construction was improved to a rate 1/3 construction in [15].

2) **Motivation to Consider the Quantum Setting**: Given the rapid development of quantum technologies, it is natural to consider non-malleable codes security against the quantum adversaries, and also how adversaries with quantum capabilities affect previous assumptions made about tampering models. For example, all known non-malleable codes studied in the literature assume the so called independence assumption. Additionally, and just as important, the possibility of attackers with quantum capabilities challenges the independence assumption made in the split-state model. For example, in the classical setting, when split-state codewords \((X, Y)\) are tampered using shared randomness \(E\), i.e. \((X, E) \rightarrow (X', E)\) and \((Y, E) \rightarrow (Y', E)\), we still have the independence assumption after fixing \(E = e\), \(XX'YY' = XX' \otimes YY'\). For attackers with access to shared entanglement such an argument does not hold and thus it is apriori not clear on how to argue anything post-adversarial tampering.

Furthermore, even though codewords may be physically isolated from each other, the tampering adversaries attacking each codeword with access to a large amount of entangled quantum states may provide non-trivial advantages well beyond what has been considered in the classical tampering models. For example, quantum entanglement between various parties, used to generate classical information introduces non-local correlations [16]. For example in the CHSH game, one can use local measurements on both the halves of a EPR state to generate a probability distribution which contains correlations stronger than those possible classically. Entanglement is of course known to yield several such unexpected effects with no classical counterparts, e.g., super-dense coding [17]. Thus, it motivates us to consider if one can provide non-malleable codes when adversary in the split-state model is allowed to make use of an arbitrary entanglement (between the two parts) to tamper the two parts \(X\) and \(Y\) (both classical) of an encoded message \(S\). We note to the reader that the \((\text{Enc}, \text{Dec})\) schemes considered in this paper are classical, and we provide quantum security in the sense that the adversary is allowed to do quantum operations to tamper \((X, Y) \rightarrow (X', Y')\) using pre-shared unbounded entanglement.

3) **Non-Malleable Secret Sharing**: The notion of non-malleable secret sharing has also been widely studied as a strengthening of non-malleable codes in the split-state model. Secret sharing, going back to work of Blakley [18] and Shamir [19], is a fundamental cryptographic primitive where a dealer encodes a secret into \(n\) shares and distributes them among \(n\) parties. Each secret sharing scheme has an associated monotone\(^1\) set \(\Gamma \subseteq [2^n]\), 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 secret sharing schemes are the so called \(t\)-out-of-\(n\) secret sharing schemes where at least \(t\)-parties are required to decode the secret.

Non-malleable secret sharing, generalizing non-malleable codes, was introduced by Goyal and Kumar [20] and has received significant interest in the past few years in the classical setting. Non-malleable secret sharing 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. Again, the motivation is that shares are being held in physically distant locations, and so communication between the tampering adversaries is infeasible.

Non-malleable codes in the split-state model and non-malleable secret sharing schemes and related notions have also found applications to other cryptographic tasks, such as non-malleable commitments, secure message transmission, and non-malleable signatures [20], [21], [22], [23], [24].

\(^1\)A set \(\Gamma \subseteq [2^n]\) is monotone if \(A \subseteq \Gamma\) and \(A \subseteq B\) implies that \(B \in \Gamma\).
In this paper, we focus only on quantum secure 2-out-of-2 non-malleable secret sharing schemes.

4) Our Results: Our first contribution is setting up the required analogue/framework to define quantum secure non-malleable codes in the quantum setting.

5) Quantum Split-State Adversary: To tamper \((X, Y) \rightarrow (X', Y')\), we let the adversary share an arbitrary entanglement \(\psi_{NM}\) between the two different locations where split codewords are stored. The adversary then applies isometries \(U: \mathcal{H}_X \otimes \mathcal{H}_N \rightarrow \mathcal{H}_{X'} \otimes \mathcal{H}_{N'}\) and \(V: \mathcal{H}_Y \otimes \mathcal{H}_M \rightarrow \mathcal{H}_{Y'} \otimes \mathcal{H}_{M'}\) to tamper \((X, Y) \rightarrow (X', Y')\). The decoding process begins by first measuring \((X', Y')\) and then outputting the decoded message \(S'\) from \((X', Y')\) (post measurement in the computational basis). To show that non-malleable codes are secure against such an adversary, it is sufficient to show that if the adversary doesn’t tamper the codeword, the decoded message \(S'\) is same as the original message \(S\). If the adversary does tamper the codeword, the decoded message \(S'\) is (approximately) distributed according to a distribution \((\mathcal{D}_{U,V,\psi})\) that only depends on \((U, V, \psi)\) that is independent of the original message \(S\). For simplicity, we denote quantum split-state adversary as \(\mathcal{A} = (U, V, \psi)\) in this paper.

We now formally define a quantum split-state adversary in the split-state model.

Definition 2 (Quantum Split-State Adversary (See Figure 1)): Let \(\sigma_{SXY}\) be the state after encoding the message \(S\). The quantum split-state adversary (denoted \(\mathcal{A} = (U, V, \psi)\)) will act via two isometries, \((U, V)\) using an additional shared entangled state \(\psi_{NM}\) as specified by \(U: \mathcal{H}_X \otimes \mathcal{H}_N \rightarrow \mathcal{H}_{X'} \otimes \mathcal{H}_{N'}\) and \(V: \mathcal{H}_Y \otimes \mathcal{H}_M \rightarrow \mathcal{H}_{Y'} \otimes \mathcal{H}_{M'}\). Let \(\rho = (U \otimes V)(\sigma \otimes |\psi\rangle \langle \psi|)(U \otimes V)\) and \(\rho\) be the final state after measuring the registers \((X'Y')\) in computational basis.

Our work provides the first quantum secure non-malleable code with efficient encoding and decoding procedures for message length \(m = n^{\Omega(1)}\), error \(\varepsilon = 2^{-n^{\Omega(1)}}\) and codeword of size \(2n\). When the tampering of the codeword is performed \(t\)-times, we also provide the first quantum secure one-many non-malleable code with efficient encoding and decoding procedures for \(t = n^{\Omega(1)}\), message length \(m = n^{\Omega(1)}\), error \(\varepsilon = 2^{-n^{\Omega(1)}}\) and codeword of size \(2n\). Prior to our work, it remained open to provide such quantum secure non-malleable codes even for a single bit message in the split-state model.

Remark: We would like to inform the reader that, by a quantum secure non-malleable code, we refer to a non-malleable code for input classical messages, where both encoding and decoding are classical procedures, designed to defend against quantum adversaries with pre-shared entanglement in the split-state model.

We next formally define the quantum secure non-malleable codes in the split-state model.

Definition 3 (Quantum Secure Non-Malleable Codes in the Split-State Model): \((\text{Enc}, \text{Dec})\) is an \((m, n, \varepsilon)\)-quantum secure non-malleable code in the split-state model with error \(\varepsilon\), if for state \(\rho\) and adversary \(\mathcal{A} = (U, V, \psi)\) (as defined in Definition 2), there exists a random variable \(\mathcal{D}_A\) on \(\{0, 1\}^m \cup \{\text{same}\}\) such that

\[
\forall s \in \{0, 1\}^m : \|S'_s - \text{copy}(\mathcal{D}_A, s)\|_1 \leq \varepsilon.
\]

Above \(S'_s = \text{Dec}(X', Y'), S'_s = (S'|S = s)\) and the function \(\text{copy}(x, s)\) is such that \(\text{copy}(x, s) = s\) if \(x = \text{same}\), otherwise \(\text{copy}(x, s) = x\).

Our first result is to show that a quantum secure non-malleable code in the split-state model can be constructed using a quantum secure 2-source non-malleable extractor. We use the 2-source non-malleable extractor of Boddu et al. [2]. This is analogous to the classical result by Cheraghchi and Guruswami [7], however additional novelty over classical arguments is needed. This is to take care of the specific adversary model in which the security of 2-source...
non-malleable extractor is shown by [2] and other additional issues involving quantum information (example purifications of states).

6) Previous Adversary Models: Various tampering adversaries are studied in [2] and [25] in the context of multi-source extractors and 2-source non-malleable extractors. Quantum multi-source extractors were considered by Kasper and Kempe [26] (for the quantum independent adversary and the quantum bounded storage adversary), Chung et al. [27] (for the general entangled adversary), and Arnon-Friedman, Portmann, and Scholz [28] (for the quantum Markov adversary).

The critical difference among all the adversary models lies in how the adversary obtains quantum side information on sources from which randomness is extracted.

The codewords upon which adversaries act. Moreover, prior to tampering, it is not clear how the security can be reduced to non-malleable non-malleable codes to the security of non-malleable extractors. We can view split-state codewords as follows. Let us consider the quantum Markov adversary model. Theorem 4: There exists a quantum secure one-many non-malleable code in the split-state model with efficient encoding and decoding procedures for message length \( m = n^{\Omega(1)} \), error \( \varepsilon = 2^{-n^{\Omega(1)}} \) and codeword of size \( 2n \).

Prior to this work, it remained open to provide such construction for quantum secure non-malleable codes, even for a single bit message in the split-state model.

We also study the natural extension when the tampering of the codeword is performed \( t \)-times (see Appendix A). Here, the adversary is allowed to tamper

\[
(X, Y) \rightarrow (X^1X^2 \ldots X^t, Y^1Y^2 \ldots Y^t)
\]

making use of an arbitrary entanglement between two parts \( X \) and \( Y \). We require, in case of tampering, the original message \( S \) to be independent of \( S^1 \ldots S^t = \text{Dec}(X^1, Y^1) \ldots \text{Dec}(X^t, Y^t) \).

Theorem 3 (Quantum Secure One-Many Non-Malleable Codes in the Split-State Model): Let \( t \)-2nmExt : \( \{0, 1\}^n \rightarrow \{0, 1\}^m \) be a \( t \)-quantum secure \( t \)-non-malleable extractor. There exists a \( (t; m, n, \varepsilon') \)-quantum secure one-many non-malleable code with parameter \( \varepsilon' = 2^{m(2^{2-k} + \varepsilon') + \varepsilon} \).

Theorem 4: There exists a \( (t; m, n, \varepsilon') \)-quantum secure one-many non-malleable code in the split-state model with efficient

---

6All the quantum secure non-malleable codes in the split-state model we construct are qualitatively same as the non-malleable codes in the split-state model constructed in [6].
encoding and decoding procedures for parameters $t = n^{\Omega(1)}$, $m = n^{\Omega(1)}$, error $\varepsilon = 2^{-n^{\Omega(1)}}$ and codeword of size $2n$.

As an application, we present the first quantum-secure 2-out-of-2 non-malleable secret sharing scheme for a message/secret length of $m = n^{\Omega(1)}$, error $\varepsilon = 2^{-n^{\Omega(1)}}$, and shares of size $n$. Interestingly, our quantum-secure non-malleable code in the split-state model also serves as a quantum-secure 2-out-of-2 non-malleable secret sharing scheme. We provide comprehensive details of this construction in Section V.

7) Proof Overview: Let $2\text{new}\text{-ext}$ refer to the 2-source non-malleable extractor from [6]. Let $X = U_n \otimes U_n$ (represents independence). Let $Z = 2\text{new}\text{-ext}(X, Y)$. According to the scheme by [7], efficient construction of non-malleable codes requires us to, given any $z$, sample efficiently from the distribution $(XY|Z = z)$. It is not apriori clear that such efficient (reverse) sampling for $2\text{new}\text{-ext}$ is possible. [6] modified $2\text{new}\text{-ext}$ to come up with a new 2-source non-malleable extractor (say $2\text{new}\text{-ext}\text{-q}$) and exhibited efficient reverse sampling for $2\text{new}\text{-ext}\text{-q}$. A key difference between the constructions of $2\text{new}\text{-ext}$ and $2\text{new}\text{-ext}\text{-q}$ is the seeded extractor that is used in the alternating extraction argument (for both the constructions). $2\text{new}\text{-ext}$ uses the seeded extractor from [GUV09] while new-$2\text{new}\text{-ext}\text{-q}$ uses a seeded extractor $\text{IExt}$ constructed by [6]. Two key properties of $\text{IExt}$ that are crucially used are:

1) Let $W$ be the source, $S$ be the seed and $O = \text{IExt}(W, S)$ be the output. For $WS = U_n \otimes U_d$, we have $OS = U_m \otimes U_d$.

2) $\text{IExt}$ is a bilinear function. This implies that for every $(o, s)$, one can sample (exactly) from $(W|OS = (o, s))$.

This allows [6] exact reverse sampling. That is for any $z$, they are able to efficiently sample from the distribution $(XY|Z = z)$ exactly.

There are a few other modifications required to finally make $2\text{new}\text{-ext}\text{-q}$ suitable for efficient reverse sampling. For example, the input sources $X$ and $Y$ are divided into $n^{\Omega(1)}$ different blocks (since there are $n^{\Omega(1)}$ rounds of alternating extraction in the construction of $2\text{new}\text{-ext}$). This enables to use different blocks (each with almost full min-entropy) as sources to seeded extractors in each round of alternating extraction. This further ensures the linear constraints that are imposed in the alternating extraction are on different variables of input sources, $X, Y$ in each round which is crucial for the exact reverse sampling argument of [6].

Let us now consider the quantum setting. Let $2\text{new}\text{-ext}\text{-q}$ refer to the 2-source non-malleable extractor from [2]. Again it is not apriori clear that efficient reverse sampling for $2\text{new}\text{-ext}\text{-q}$ is possible. Hence we modify the $2\text{new}\text{-ext}\text{-q}$ from [2] to construct (say $2\text{new}\text{-ext}\text{-q}$) in the full version. We follow the argument of dividing the input sources $X$ and $Y$ into different blocks (as stated in previous paragraph) and make necessary modifications to $2\text{new}\text{-ext}\text{-q}$. Next, we note the seeded extractor used in alternating extraction of both $2\text{new}\text{-ext}$, new-$2\text{new}\text{-ext}\text{-q}$ is the Trevisan extractor (say $\text{Trev}$) which is quantum secure [29]. One can modify $2\text{new}\text{-ext}\text{-q}$ using a similar modification as that of [6], by considering $\text{IExt}$ instead of $\text{Trev}$. However then one would need to first show the quantum security of $\text{IExt}$. This is not known as of now and we leave it for future work. For now we choose to make the arguments work with $\text{Trev}$. We note the two key properties for $\text{Trev}$:

1) For $WS = U_n \otimes U_d$, we have $OS \approx U_m \otimes U_d$, where $O = \text{Trev}(W, S)$ (approx represent close in $\ell_1$ norm).

2) For every $s$, Trevisan is a linear function of $W$. Hence for every $(o, s)$, we can sample efficiently (exactly) from $W|OS = (o, s)$.

Point 1. above is the differentiating property between $\text{IExt}$ and $\text{Trev}$. Hence, unlike [6], we cannot do exact reverse sampling and can only do approximate reverse sampling. We therefore have to carefully keep the overall error introduced under control.

While generating $Z = \text{new}\text{-2new}\text{-ext}\text{-q}(X, Y)$, starting from $(X, Y)$, several intermediate random variables (say $(R_1, R_2, \ldots, R_k)$ in this order) are generated. During the reverse sampling, starting from $Z$, they need to be generated in the reverse order. We call this process backtracking. Since we have to keep the overall error under control, we need to note and use important Markov-chain structures between the intermediate random variables (see Claim 2 and Claim 3). This is additional technical novelty over [6].

8) Organization: In Section II, we describe useful quantum information facts and other preliminaries. It also contains useful lemmas and claims. We describe the existential proof of quantum secure non-malleable codes, i.e. Theorem 1 in Section III. Section IV contains the construction of modified 2-source non-malleable extractor along with proof of Theorem 2. Section V contains a quantum secure 2-out-of-2 non-malleable secret sharing scheme. The $t$-tampered version of non-malleable codes can be found in the Appendix A.

II. PRELIMINARIES

Let $n, m, d, t$ represent positive integers and $l, k, k_1, k_2$, $\delta, \gamma, \varepsilon \geq 0$ represent reals.

A. Quantum Information Theory

All the logarithms are evaluated to the base 2. Let $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ be finite sets (we only consider finite sets in this paper). 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 the context. We use $x \leftarrow X$ to denote $x$ drawn according to $X$. We also use $x \leftarrow \mathcal{X}$ to denote $x$ drawn uniformly from $\mathcal{X}$. For two random variables $X, Y$ we use $X \otimes Y$ to denote independent random variables.

We call random variables $X, Y$, copies of each other iff $\Pr[X = Y] = 1$. Let $Y_1, Y_2, \ldots, Y^t$ be random variables. We denote the joint random variable $Y_1Y_2\ldots Y^t$ by $Y^t$. Similarly for any subset $S \subseteq [t]$, we use $Y^S$ to denote the joint random variable comprised of all the $Y^s$ such that $s \in S$. For a random variable $X \in \{0, 1\}^n$ and $0 < d_1 \leq d_2 \leq n$, let $\text{Crop}(X, d_1, d_2)$ represent the bits from $d_1$ to $d_2$ of $X$, i.e. $X_{[d_1:d_2]}$. Let $U_q$ represent the uniform distribution over $\{0, 1\}^q$. For a random variable $X \in \mathbb{F}_q$ for a prime power $q$, we view $X$ as a row vector $(X^1, X^2, \ldots, X^n)$ where each $X^i \in \mathbb{F}_q$.®
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 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 $\psi$ to represent the state and also the density matrix $|\psi\rangle\langle\psi|$, associated with $|\psi\rangle$. A given quantum state $\rho$ on $\mathcal{H}$, support of $\rho$, called supp($\rho$) is the subspace of $\mathcal{H}$ spanned by all eigenvectors of $\rho$ with non-zero eigenvalues.

A quantum register $A$ is associated with some Hilbert space $\mathcal{H}_A$. Define $|A\rangle := \log (\dim(\mathcal{H}_A))$. Let $\mathcal{L}(\mathcal{H}_A)$ represent the set of all linear operators on the Hilbert space $\mathcal{H}_A$. 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 $\mathcal{H}_A$. State $\rho$ with subscript $A$ indicates $\rho_A \in \mathcal{D}(\mathcal{H}_A)$. If two registers $A, B$ are associated with the same Hilbert space, we shall represent the relation by $A \equiv B$.

For two states $\rho, \sigma$, we let $\rho \equiv \sigma$ represent that 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 $\sigma \in \mathcal{D}(\mathcal{H}_B)$, $\rho \otimes \sigma \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ represents the tensor product (Kronecker product) of $\rho$ and $\sigma$. The identity operator on $\mathcal{H}_A$ is denoted $I_A$. Let $U_A$ denote the maximally mixed state in $\mathcal{H}_A$. Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$.

Define

$$\rho_B := \text{Tr}_{A} \rho_{AB} := \sum_i (|i\rangle \otimes \rho_B) \rho_{AB} (|i\rangle \otimes I_B),$$

where $\{|i\rangle\}$, 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 $\rho_{AB}$ on the register $B$. Unless otherwise stated, a missing register from a subscript in a state represents partial trace over that register. Given $\rho_A \in \mathcal{D}(\mathcal{H}_A)$, a purification of $\rho_A$ is a pure state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ such that $\text{Tr}_{B} \rho_{AB} = \rho_A$. 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 $\rho_A$ is $\rho_A = (|A\rangle \otimes I_B) \sum_i |i\rangle \langle i| A |i\rangle \langle i| B).$

A quantum map $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B)$ is a completely positive and trace preserving (CPTP) linear map. A Hermitian operator $H : \mathcal{H}_A \rightarrow \mathcal{H}_A$ 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 $V_A : \mathcal{H}_A \rightarrow \mathcal{H}_A$ is such that $V_A^\dagger V_A = V_A V_A^\dagger = I_A$. The set of all unitary operators on $\mathcal{H}_A$ is denoted by $U(\mathcal{H}_A). A$ isometry $V : \mathcal{H}_A \rightarrow \mathcal{H}_B$ is an operator such that $V^\dagger V = I_A$. A POVM element is an operator $0 \leq M \leq I$. We use the shorthand $M : = I - M$, where $I$ is clear from the context. We use shorthand $M$ to represent $\mathbb{M} \equiv I - M$, where $I$ is clear from the context. We use $\mathbb{M}$ to represent $\mathbb{M}$.

A classical-quantum (c-q) state $\rho_{XE}$ is of the form

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

where $\rho_E$ are states. In a pure state $\rho_{XE}$, in which $\rho_{XE}$ is c-q, we call $X$ a classical register and identify random variable $X$ with it with $\Pr(X = x) = p(x)$. For an event $S \subseteq X$, define

$$\Pr(S) := \sum_{x \in S} p(x) ;$$

and

$$\langle \rho \mid S \rangle := \frac{1}{\Pr(S)} \sum_{x \in S} p(x) |x\rangle \langle x| \otimes \rho_E.$$

For a function $Z : X \rightarrow Z$, define the following extension of $\rho_{XE}$

$$\rho_{ZX} := \sum_{x \in X} p(x) |Z(x)\rangle \langle Z(x)| \otimes |x\rangle \langle x| \otimes \rho_E.$$

We call an isometry $V : \mathcal{X} \otimes \mathcal{H}_A \rightarrow \mathcal{X} \otimes \mathcal{H}_B$, safe on $X$ iff there is a collection of isometries $V_x : \mathcal{H}_A \rightarrow \mathcal{H}_B$ such that the following holds. For all states $|\psi\rangle_{XA} = \sum_x \alpha_x |x\rangle \chi_x |\psi\rangle_A$,

$$|\psi\rangle_{XA} = \sum_x \alpha_x |x\rangle \chi_x V_x |\psi\rangle_A.$$

All the isometries considered in this paper are safe on classical registers they act upon. For a function $Z : X \rightarrow Z$, define $\rho_{Z\times E}$ to be a pure state extension of $\rho_{XE}$ generated via a safe isometry $V : \mathcal{H}_X \rightarrow \mathcal{H}_X \otimes \mathcal{H}_Z \otimes \mathcal{H}_2$ (Z classical with copy $Z$). For a pure state $\rho_{XE}$ and measurement $\mathcal{M}$ in the computational basis on register $X$, define $\rho_{ZXE}$ a pure state extension post the measurement $\mathcal{M}$ of state $\rho_{XE}$ generated via a safe isometry $V : \mathcal{H}_X \rightarrow \mathcal{H}_X \otimes \mathcal{H}_Z$ such that $\rho_{ZXE} = V\rho_{Z\times E}$ and $X$ a copy of $X$.

Definition 4: 1) For $p \geq 1$ and matrix $A$, let $\|A\|_p$ denote the Schatten $p$-norm defined as $\|A\|_p \equiv (\text{Tr}(A^\dagger A)^{\frac{p}{2}})^{\frac{2}{p}}$. 2) For states $\rho, \sigma$ : $\Delta(\rho, \sigma) \equiv \frac{1}{2} \|\rho - \sigma\|_1$. We write $\rho \approx \sigma$ to denote $\Delta(\rho, \sigma) \leq \varepsilon$. 3) Fidelity: For states $\rho, \sigma : F(\rho, \sigma) \equiv \|\sqrt{\rho} \sqrt{\sigma}\|_1$. 4) Bures metric: For states $\rho, \sigma : \Delta_B(\rho, \sigma) \equiv \sqrt{1 - F(\rho, \sigma)}$. 5) Max-divergence ( [30], see also [31]): For states $\rho, \sigma$ such that supp($\rho$) $\subset$ supp($\sigma$),

$$D_{\text{max}}(\rho\mid\sigma) \equiv \min\{\lambda \in \mathbb{R} : \rho \leq 2^\lambda \sigma\}. $$

6) Min-entropy and conditional-min-entropy: For a state $\rho_{XE}$, the min-entropy of $X$ is defined as

$$H_{\text{min}}(X) \rho \equiv -\inf_{\sigma \in \mathcal{D}(\mathcal{H}_E)} \mathcal{D}_{\text{max}}(\rho_{XE} \parallel X \otimes \sigma_E).$$

The conditional-min-entropy of $X$, conditioned on $E$, is defined as

$$H_{\text{min}}(X|E) \rho \equiv -\inf_{\sigma \in \mathcal{D}(\mathcal{H}_E)} \mathcal{D}_{\text{max}}(\rho_{XE} \parallel X \otimes \sigma_E).$$

7) Markov-chain: A state $\rho_{XEY}$ forms a Markov-chain (denoted $(X \rightarrow E \rightarrow Y)_{\rho}$) iff $I(X : Y|E)_{\rho} = 0.$ For the facts stated below without citation, we refer the reader to standard text books [32], [33].
Fact 1 (Uhlmann’s Theorem [34]): Let $\rho_A, \sigma_A \in D(\mathcal{H}_A)$. Let $\rho_{AB} \in D(\mathcal{H}_{AB})$ be a purification of $\rho_A$ and $\sigma_{AC} \in D(\mathcal{H}_{AC})$ be a purification of $\sigma_A$. There exists an isometry $V$ (from a subspace of $\mathcal{H}_C$ to a subspace of $\mathcal{H}_B$) such that,
\[
\Delta_B(\theta^{(A)}|\theta^{AB}, \rho)\rho^{(AB)} = \Delta_B(\rho_A, \sigma_A),
\]
where $\theta^{(A)} = (\mathcal{A} \otimes \mathcal{V})|_{\mathcal{H}_C}$. Let $\rho_{X', M'} = (\mathbb{I} \otimes \mathcal{E})(\rho_{XM'})$. Then,
\[
H_{\min}(X|M')_\rho \geq H_{\min}(X|M)_\rho.
\]
Above is equality iff $\mathcal{E}$ is a CPTP map corresponding to an isometry.

Fact 2 ([27]): Let $\mathcal{E} : \mathcal{L} \mathcal{H}_M \rightarrow \mathcal{L} \mathcal{H}_M$ be a CPTP map and let $\sigma_{XM'} = (\mathbb{I} \otimes \mathcal{E})(\rho_{XM'})$. Then,
\[
H_{\min}(X|M')_\rho \geq H_{\min}(X|M)_\rho.
\]

Fact 3 (Stinespring Isometry Extension [33]): Let $\Phi : \mathcal{L} \mathcal{H}_X \rightarrow \mathcal{L} \mathcal{H}_Y$ be a CPTP map. Then there exists an isometry $V : \mathcal{H}_X \rightarrow \mathcal{H}_Y \otimes \mathcal{H}_Z$ (Stinespring isometry extension of $\Phi$) such that $\Phi(\rho_X) = \text{Tr}_Z(V \rho_X V^\dagger)$ for every state $\rho_X$.

Fact 4 ([35]): Let $\rho, \sigma$ be states. Then,
\[
1 - F(\rho, \sigma) \leq \Delta(\rho, \sigma) \leq \sqrt{1 - F^2(\rho, \sigma)}
\]
and
\[
\Delta_B(\rho, \sigma) \leq \Delta(\rho, \sigma) \leq \sqrt{2}\Delta_B(\rho, \sigma).
\]

Fact 5 (Data-Processing): Let $\rho, \sigma$ be states and $\mathcal{E}$ be a CPTP map. Then
\begin{itemize}
  \item $\Delta(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq \Delta(\rho, \sigma)$,
  \item $\Delta_B(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq \Delta_B(\rho, \sigma)$,
  \item $D_{\max}(\mathcal{E}(\rho)\|\mathcal{E}(\sigma)) \leq D_{\max}(\rho\|\sigma)$.
\end{itemize}

The inequalities above are equalities in case $\Phi$ is a CPTP map corresponding to an isometry.

Fact 6 (i): Let $\rho_{XE}, \sigma_{XE} = c-$q states. Then,
\begin{itemize}
  \item $\|\rho_{XE} - \sigma_{XE}\|_1 \leq E_{z \rightarrow p_x}\|\rho_{E}^{z} - \sigma_{E}^{z}\|_1$,
  \item $\Delta_B(\rho_{XE}, \sigma_{XE}) \geq E_{z \rightarrow p_x} \Delta_B(\rho_{E}^{z}, \sigma_{E}^{z})$.
\end{itemize}

The above inequalities are equalities iff $\rho_{XE} = \sigma_{XE}$. In the above inequalities, $x \rightarrow \rho_X$ corresponds to $x$ drawn from marginal classical distribution $\rho_X$.

Fact 7: Let $\rho, \sigma$ be states such that $\rho = \sum_z p_x \rho_x$, $\sigma = \sum_z p_x \rho_x$, $\{\rho_x, \sigma_x\}$ are states and $\sum_x p_x = 1$. Then,
\[
\Delta(\rho, \sigma) \leq \sum_x p_x \Delta(\rho_x, \sigma_x).
\]

Fact 8: Let $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a state and $M \in \mathcal{L} \mathcal{H}_B$ such that $M^\dagger M \leq 1_B$. Let $\rho_{AB} = \frac{M^\dagger \rho_{AB} M}{\text{Tr}_{M^\dagger \rho_{AB} M}}$. Then,
\[
D_{\max}(\rho_A\|\rho_A) \leq \log \left(\frac{1}{\text{Tr} M^\dagger \rho_{AB} M}\right).
\]

Fact 9: For random variables $A, B$ such that $A = A_1 \otimes A_2$, $B = B_1 \otimes B_2$, we have
\[
\|A - B\|_1 = \|A_1 - B_1\|_1 + \|A_2 - B_2\|_1.
\]

Fact 10: For random variables $A, B, \tilde{A}, \tilde{B}$, we have
\[
\|\tilde{A}B - AB\|_1 \leq \|\tilde{B} - B\|_1 + E_{b \rightarrow B} \|\tilde{A}(B = b) - A(B = b)\|_1.
\]

Fact 11 (Folklore): Let $m, n$ be positive integers such that $m \leq n$. Let $A$ be any $m \times n$ matrix over the Field $\mathbb{F}$. For any string $a \in \mathbb{F}^m$, let $S_a = \{x \in \mathbb{F}^n : Ax^t = o\}$. There exists an efficient algorithm that runs in time polynomial in $(m, n, |\mathbb{F}|)$ and outputs sample $x \leftarrow S_a$.

Proof: (Sketch) Let $a \in \mathbb{F}^m$. Sampling $x$ uniformly from the set $S_a$ can be done in the following way:
\begin{itemize}
  \item perform standard Gauss-Jordan elimination to convert $Ax^t = o$ to $Ax^t = \tilde{0}$, where $\tilde{A}$ is the matrix in row-echelon form. Note $\text{rank}(A) = \text{rank}(\tilde{A})$ and sampling from the set $\{x : Ax^t = \tilde{0}\}$ is same as sampling from the set $\{x : Ax^t = \tilde{0}\}$.
  \item For every $i \in [\text{rank}(A) + 1, n]$, sample $x_i \leftarrow \mathbb{F}$.
  \item Solve the linear equations given by $Ax^t = \tilde{0}$ to find the unique $(x_1, x_2, \ldots, x_n)$ satisfying it.
  \item Output $(x_1, x_2, \ldots, x_n)$.
\end{itemize}

The efficiency of the above sampling process follows since Gauss-Jordan elimination and linear equations can be solved efficiently.

Fact 12 (Corollary 5.2 in [6]): For any constant $\delta \in (0, 1)$, there exist constants $\alpha, \beta$ such that $3\beta \leq \alpha \leq 1/4$ and for all positive integers $\nu, r, t$, with $r \geq \nu^\alpha$ and $t = O(\nu^\beta)$ the following holds.

There exists a polynomial time computable function $\text{Samp} : \{0, 1\}^r \rightarrow \nu^t$, such that for any set $\mathcal{S} \subset \nu$ of size $\delta\nu$,
\[
\text{Pr}(\text{Samp}(U_r) \cap \mathcal{S}) \geq 1 \geq 1 - 2^{-\Omega(\nu^\alpha)}.
\]

Definition 5: Let $M = 2^m$. The inner-product function, $\text{IP}_M^\nu : \mathbb{F}_M^m \times \mathbb{F}_M^n \rightarrow \mathbb{F}_M$ is defined as follows:
\[
\text{IP}_M^\nu(x, y) = \sum_{i=1}^n x_i y_i,
\]
where the operations are over the Field $\mathbb{F}_M$.

B. Extractors and Non-Malleable Codes

Throughout the paper we use extractor to mean seeded extractor unless stated otherwise.

Definition 6 (Quantum Secure Extractor): An $(n, d, m)$-extractor $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ is said to be $(k, \epsilon)$-quantum secure if for every state $\rho_{XES}$, such that $H_{\min}(X|E)_\rho \geq k$ and $\rho_{XES} = \rho_{XE} \otimes U_d$, we have
\[
\|\rho_{\text{Ext}(X, S)E} - U_m \otimes \rho_E\|_1 \leq \epsilon.
\]

In addition, the extractor is called strong if
\[
\|\rho_{\text{Ext}(X, S)E} - U_m \otimes U_d \otimes \rho_E\|_1 \leq \epsilon.
\]

$S$ is referred to as the seed for the extractor.

Fact 13 ([29]): There exists an explicit $(2m, \epsilon)$-quantum secure strong $(n, d, m)$-extractor $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ for parameters $d = O(\log^2(n/\epsilon) \log m)$. Moreover the extractor $\text{Ext}$ is linear extractor, i.e. for every fixed seed, the output of the extractor is a linear function of the input source.

Definition 7 (l-qma-state [25]): Let $\tau_{XX}, \tau_{YY}$ be the canonical purifications of independent and uniform sources $X, Y$ respectively. Let $\tau_{NM}$ be a pure state. Let
\[
\theta_{XXNMYY} = \tau_{XX} \otimes \tau_{NM} \otimes \tau_{YY}.
\]
Let $U : \mathcal{H}_X \otimes \mathcal{H}_Y \rightarrow \mathcal{H}_X \otimes \mathcal{H}_{X'} \otimes \mathcal{H}_A$ and $V : \mathcal{H}_Y \otimes \mathcal{H}_M \rightarrow \mathcal{H}_Y \otimes \mathcal{H}_{M'} \otimes \mathcal{H}_B$ be isometries such that registers $A, B$ are single qubit registers. Let

$$\rho_{X^{A'N'M'}BY} = (U \otimes V) \theta_{X^{ANMY'}} (U \otimes V)^\dagger,$$

$$l = \log \left( \frac{1}{\Pr(A = 1, B = 1)} \rho \right)$$

and

$$\sigma_{X^{A'N'M'}Y'Y} = (\rho_{X^{A'N'M'}BY} | A = 1, B = 1).$$

We call $\sigma_{X^{A'N'M'}Y'Y}$ an l-qma-state.

Fact 14 (IP Security Against l-qma-state [25]): Let $n = n_{\text{max}}$ and $n_1 - l \geq 2 \log \left( \frac{1}{\epsilon} \right) + m$. Let $\sigma_{X'X'N'M'}$ be an l-qma-state with $|X| = |Y| = n_1$. Then

$$\| \sigma_{ip_{n}^{l}(X,Y)X'} \sigma_{X'} - U_m \otimes \sigma_{X'} \|_1 \leq \epsilon$$

and

$$\| \sigma_{ip_{n}^{l}(X,Y)Y'} \sigma_{Y'} - U_m \otimes \sigma_{Y'} \|_1 \leq \epsilon.$$  

Fact 15 (Theorem 7 in [6]): Let $X, Y$ be independent sources on $\mathbb{F}_2^n$ with min-entropy $k_1, k_2$ respectively. Then

$$\| \text{IP}_{n}^{l}(X,Y) - U_m \otimes Y \|_1 \leq \epsilon$$

and

$$\| \text{IP}_{n}^{l}(X,Y) - X \otimes U_m \|_1 \leq \epsilon,$$

where $\epsilon = 2^{-\left(\frac{n}{2}\right)} \left[ k_1 + k_2 \right].$

Definition 8 ($(k_1, k_2)$-qpa-state [2]): We call a pure state $\sigma_{X'X'N'M'}$ with $(XY)$ classical and $(X'Y')$ copy of $(XY)$, a $(k_1, k_2)$-qpa-state iff

$$\Pr(Y \neq Y')_{\sigma} \geq k_1 \quad \text{or} \quad \Pr(X \neq X')_{\sigma} \geq k_2.$$  

Definition 9 ($(k_1, k_2)$-qnm-state [2]): Let $\sigma_{X'X'N'M'}$ be a $(k_1, k_2)$-qpa-state. Let $U : \mathcal{H}_X \otimes \mathcal{H}_N \rightarrow \mathcal{H}_X \otimes \mathcal{H}_{X'} \otimes \mathcal{H}_N$ and $V : \mathcal{H}_Y \otimes \mathcal{H}_M \rightarrow \mathcal{H}_Y \otimes \mathcal{H}_{Y'} \otimes \mathcal{H}_M$ be isometries such that for $\rho = (U \otimes V) \sigma (U \otimes V)^\dagger$, we have $(XY')$ classical (with copy $(X'Y')$) and

$$\Pr(Y \neq Y')_{\rho} = 1 \quad \text{or} \quad \Pr(X \neq X')_{\rho} = 1.$$  

We call state $\rho$ a $(k_1, k_2)$-qnm-state.

Definition 10 (Quantum Secure 2-Source Non-Malleable Extractor [2]): An $(n, n, m)$-non-malleable extractor $\text{2nmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m$ is $(k_1, k_2, \epsilon)$-secure against qnm-adv if for every $(k_1, k_2)$-qnm-state $\rho$ (chosen by the adversary qnm-adv),

$$\| \rho_{2\text{nmExt}(X,Y)} \otimes \rho_{2\text{nmExt}(X',Y')} \sigma_{YY'} \otimes M'M - U_m \otimes \rho_{2\text{nmExt}(X,Y')} \sigma_{YY'} \otimes M'M \|_1 \leq \epsilon.$$  

C. Error Correcting Codes

Definition 11: Let $\Sigma$ be a finite set. A mapping $\text{ECC} : \Sigma^k \rightarrow \Sigma^n$ is called an error correcting code with relative distance $\gamma$ if for any $x, y \in \Sigma^k$ such that $x \neq y$, the Hamming distance between $\text{ECC}(x)$ and $\text{ECC}(y)$ is at least $\gamma n$. The rate of the code denoted by $\delta$, is defined as $\delta = \frac{k}{n}$. The alphabet size of the code is the number of elements in $\Sigma$.

Fact 16 (MDS Codes): Let $q$ be a prime power. For every positive integer $k$, there exists a large enough $n$ such that there exists an efficiently computable linear error correcting code $\text{ECC} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$ with rate $\frac{k}{n}$ and relative distance $\gamma = k + 1$. Such codes are known as maximum distance separable (MDS) codes. Reed-Solomon codes is a typical example of an MDS code family.

D. Other Useful Facts, Claims and Lemmas

Fact 17 [2]: Let $\rho_{ABC} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ be a state and $M \in \mathcal{L}(\mathcal{H}_C)$ such that $M^\dagger M \leq I_C$. Let $\rho_{ABC} = \frac{M \rho_{ABC} M^\dagger}{\text{Tr}(M \rho_{ABC} M^\dagger)}$. Then,

$$\text{H}_{\min}(A|B)_{\rho} \geq \text{H}_{\min}(A|B)_{\rho} - \log \left( \frac{1}{\text{Tr}(M \rho_{ABC} M^\dagger)} \right)$$

Fact 18 [2]: Let $\rho_{XE} \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_E)$ be a c-q state such that $|X| = n$ and $\text{H}_{\min}(X|E)_{\rho} \geq n - k$. Let $X = \text{CROP}(X, d_1, d_2)$ for some positive integer $k \leq d_2 - d_1$ and $1 \leq d_1 < d_2 \leq n$. Then,

$$\text{H}_{\min}(X|E)_{\rho} \geq d_2 - d_1 + 1 - k.$$  

Fact 19 [2]: Let $\rho_{X'X'N'M'}$ be a $(k_1, k_2)$-qpa-state such that $|X| = |X'| = |Y| = n$. There exists an l-qma-state, $\rho^{(1)}$, such that

$$\Delta_B(\rho^{(1)}, \rho) \leq 3\epsilon \quad \text{and} \quad l \leq 2n - k_1 - k_2 + 4 + 4\log \left( \frac{1}{\epsilon} \right).$$  

Fact 20 (Quantum Secure 2-Source Non-Malleable Extractor [2]): Let $k = O(n^{1/4})$ and $\epsilon = 2^{-n^{1/4}}$. There exists an efficient 2-source non-malleable extractor $\text{2nmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^{n/4}$ that is $(n - k, n - k, O(\epsilon))$-quantum secure.

Fact 21 (Alternating Extraction [2]): Let $\theta_{XASB}$ be a pure state with $(XS)$ classical, $|X| = n, |S| = d$ and

$$\text{H}_{\min}(X|S)_{\theta} \geq k \quad \text{and} \quad \Delta_B(\theta_{XAS}, \theta_{XA} \otimes U_d) \leq \epsilon'.$$

Let $T \overset{\text{def}}{=} \text{Ext}(X, S)$ where Ext is a $(k, \epsilon)$-quantum secure strong $(n, d, m)$-extractor. Then,

$$\Delta_B(\theta_{TB}, U_m \otimes \theta_B) \leq 2\epsilon' + \sqrt{\epsilon}.$$  

Fact 22 (Min-Entropy Loss Under Classical Interactive Communication [2]): Let $\rho_{XNM}$ be a pure state where Alice holds registers $(XN)$ and Bob holds register $M$, such that register $X$ is classical and

$$\text{H}_{\min}(X|M)_{\rho} \geq k.$$  

Let Alice and Bob proceed for $t$-rounds, where in each round Alice generates a classical register $R_i$ and sends it to Bob, followed by Bob generating a classical register $S_i$ and sending it to Alice. Alice applies an isometry $V_i : \mathcal{H}_X \otimes \mathcal{H}_{N_{i-1}} \rightarrow \mathcal{H}_X \otimes \mathcal{H}_{N_{i-1}} \otimes \mathcal{H}_{R_i}$ (in round $i$) to generate $R_i$. Let $\theta_{X_{NM_{i}}, M_{i}}$ be the state at the end of round-$i$, where Alice holds registers $X_{Ni}$ and Bob holds register $M_i$. Then,

$$\text{H}_{\min}(X|M_{i})_{\theta} \geq k - t \sum_{j=1}^{i} |R_j|.$$
Claim 1: Let $\sigma_{XNY|YM}$ be a $(k_1, k_2)$-qpa-state with $|X| = n$ and $|Y| = n$. Let $2nm\text{Ext} : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^m$ be an efficient $(k_1, k_2, \varepsilon)$-quantum secure 2-source non-malleable extractor. Let $S = 2nm\text{Ext}(X, Y)$. Then,

$$||\sigma_{SYM} - U_m \otimes \sigma_{YM}||_1 \leq \varepsilon.$$

Proof: Let $U : \mathcal{H}_X \rightarrow \mathcal{H}_X \otimes \mathcal{H}_X \otimes \mathcal{H}_Y$, $V : \mathcal{H}_Y \rightarrow \mathcal{H}_Y \otimes \mathcal{H}_Y \otimes \mathcal{H}_Y$, be (safe) isometries such that for $\rho = (U \otimes V)\sigma((U \otimes V)^\dagger)$, we have $X'Y'$ classical (with copies $X'Y'$ respectively) and either $\Pr(X \neq X') = 1$ or $\Pr(Y \neq Y') = 1$. \(^{8}\) Notice the state $\rho$ is a $(k_1, k_2)$-qnm-state. Since $2nm\text{Ext}$ is a $(k_1, k_2, \varepsilon)$-quantum secure 2-source non-malleable extractor (see Definition 10), we have

$$||\rho_{SYY'M} - U_m \otimes \rho_{SYY'M}||_1 \leq \varepsilon.$$ 

Using Fact 5, we further get

$$||\rho_{SY} - U_m \otimes \rho_{Y}||_1 \leq \varepsilon.$$ 

The desired now follows by noting $\sigma_{XNY|MY} = \rho_{XNY|MY}$. \( \square \)

Claim 2: Let random variables $ABC, \tilde{A} \tilde{B} \tilde{C}$ be such that

$$A \leftrightarrow B \leftrightarrow C ; \quad \tilde{A} \leftrightarrow \tilde{B} \leftrightarrow \tilde{C} ;$$

$$||AB - \tilde{A}\tilde{B}||_1 \leq \varepsilon_1 ; \quad ||BC - \tilde{B}\tilde{C}||_1 \leq \varepsilon_2.$$ 

Then,

$$||ABC - \tilde{A}\tilde{B}\tilde{C}||_1 \leq 2\varepsilon_1 + \varepsilon_2.$$ 

Proof: Since $||AB - \tilde{A}\tilde{B}||_1 \leq \varepsilon_1$, using Fact 5, we have

$$||B - \tilde{B}||_1 \leq \varepsilon_1.$$ 

Since $A \leftrightarrow B \leftrightarrow C, \tilde{A} \leftrightarrow \tilde{B} \leftrightarrow \tilde{C}$, we have

$$(AC)|(B = b) = A|(B = b) \otimes C|(B = b)$$

and

$$(\tilde{A}\tilde{C})|(\tilde{B} = b) = \tilde{A}|(\tilde{B} = b) \otimes \tilde{C}|(\tilde{B} = b).$$

(2)

Consider,

$$||\tilde{A}\tilde{B}\tilde{C} - ABC||_1$$

$$\leq ||\tilde{B} - B||_1 + E_{b\rightarrow B}||(\tilde{A}\tilde{C})|(\tilde{B} = b))$$

$$- (AC)|(B = b)||_1$$

$$= ||\tilde{B} - B||_1 + E_{b\rightarrow B}||(\tilde{A}|(\tilde{B} = b) \otimes \tilde{C}|(\tilde{B} = b))$$

$$- A|(B = b) \otimes C|(B = b)||_1$$

$$= ||\tilde{B} - B||_1 + E_{b\rightarrow B}||(\tilde{A}||\tilde{B} = b - A|(B = b)||_1$$

$$+ ||\tilde{C}||(\tilde{B} = b) - C|(B = b)||_1$$

$$= ||\tilde{B} - B||_1 + E_{b\rightarrow B}||(\tilde{A}||\tilde{B} = b - A|(B = b)||_1$$

$$+ E_{b\rightarrow B}||\tilde{C}||(\tilde{B} = b) - C|(B = b)||_1$$

$$\leq ||\tilde{B} - B||_1 + ||\tilde{A}\tilde{B} - AB||_1 + ||\tilde{B}\tilde{C} - BC||_1$$

$$\leq \varepsilon_1 + ||\tilde{A}\tilde{B} - AB||_1 + ||\tilde{B}\tilde{C} - BC||_1$$

$$\leq 2\varepsilon_1 + \varepsilon_2.$$ 

The first inequality follows from Fact 10, the second inequality follows from Fact 6 and the third inequality follows from Eq. (1). The first equality follows from Eqs. (2), (3) and the second equality follows from Fact 9. This completes the proof.

Since the construction of the quantum secure non-malleable extractor is composed of alternating extraction using Ext from Fact 13, we first state a claim about the invertibility of the Ext given the output (close to the desired).

Claim 3: Let $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ be an explicit $(2m, \varepsilon)$-quantum secure strong extractor from Fact 13 \(^{9}\) with error $\varepsilon$. \(^{10}\) Let $X, H, O, \tilde{O}$ be random variables such that,

$$||XH - U_n \otimes U_d||_1 \leq \varepsilon' ; \quad O = \text{Ext}(X, H) ; \quad ||\tilde{O} - U_m||_1 \leq \varepsilon''.$$ 

Given samples from $(\tilde{o}, \tilde{h}) \leftarrow \tilde{O}H = \tilde{O} \otimes U_d$, we can sample from $X[(\tilde{O}H = \tilde{o}h)]$ (which is same as sampling $\tilde{x} \leftarrow \{x : \text{Ext}(x, h) = \tilde{o}\}$) in time polynomial in $(m, n)$ such that

$$||\tilde{O}\tilde{H}X - OHX||_1 \leq \varepsilon + \varepsilon' + \varepsilon'' ; \quad \tilde{O} = \text{Ext}X, \tilde{H}.$$ 

Proof: Let $\tilde{X}H = U_n \otimes U_d$ and $\tilde{O} = \text{Ext}(X, \tilde{H})$ be the output of the extractor. Since $||XH - \tilde{X}H||_1 \leq \varepsilon'$, using Fact 5 we have

$$||OXH - \tilde{O}\tilde{X}H||_1 \leq \varepsilon'.$$ 

(4)

Also, since $\tilde{O} = \text{Ext}X, \tilde{H}$ is the output of the strong extractor, we have

$$||\tilde{O}H - U_m \otimes U_d||_1 \leq \varepsilon.$$ 

(1) \( \square \)

Since $\tilde{O}H = \tilde{O} \otimes U_d$ and $||\tilde{O} - U_m||_1 \leq \varepsilon''$, we have $||\tilde{O}H - U_m \otimes U_d||_1 \leq \varepsilon''$. Using triangle inequality, we have

$$||\tilde{O}H - \tilde{O}H||_1 \leq \varepsilon + \varepsilon''.$$ 

(5)

We now proceed by noting that the extractor is linear. In other words, for every seed $H = h$, the output of the extractor $O = o$ is a linear function of the input $X = x$. For a fixed output $o$ of the extractor and seed $h$, we have a matrix $A_h$ of size $m \times n$ such that $A_hx = o$. \(^{11}\) Note for any fixing of the seed $h$ and output $o$, the size of the set $\{x : \text{Ext}(x, h) = o\}$ is $2^{n-\text{rank}(A_h)}$ and sampling $x$ uniformly from the set can be done efficiently from Fact 11.

Given samples $(\tilde{o}, \tilde{h}) \leftarrow \tilde{O}H = \tilde{O} \otimes U_d$, we use the following sampling strategy:

- Sample $\tilde{x} \leftarrow X[(\tilde{O}H = \tilde{o}h)]$ which is same as sampling $\tilde{x} \leftarrow \{x : \text{Ext}(x, h) = \tilde{o}\}$.

Note for any fixing of the seed $\tilde{h}$ and output $\tilde{o}$ of the extractor, $X[(\tilde{O}H = \tilde{o}h)] = \tilde{X}[(\tilde{O}H = \tilde{o}h)]$ since $\tilde{X}H = U_n \otimes U_d$. Thus, from Fact 5 and Eq. (5), we have

$$||\tilde{O}\tilde{X}H - \tilde{O}\tilde{X}H||_1 \leq \varepsilon + \varepsilon''.$$ 

(6) \( \square \)

Using Eqs. (4), (6) along with triangle inequality, we have the desired. \( \square \)

\(^{8}\)It is easily seen that such isometries exist.

\(^{9}\)The same claim holds even if Ext is replaced with IP from Fact 15 where inputs are of same size, i.e. $d = n$.

\(^{10}\)We assume there is enough min-entropy in the sources for the extractors to work.
Corollary 1: Let $\text{Ext} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$ be an explicit $(2m,\varepsilon)$-quantum secure strong extractor from Fact 13\footnote{The same Claim holds even if $\text{Ext}$ is replaced with IP from Fact 15 where inputs are of same size, i.e. $d = n$.} with error $\varepsilon$. Let
\[ \|XH - U_n \otimes U_d\|_1 \leq \varepsilon' \quad ; \quad O = \text{Ext}(X, H). \]
Then, $\|O - U_m\|_1 \leq \varepsilon + \varepsilon'$.

Proof: Let $\hat{X} \hat{H} = U_n \otimes U_d$ and $\hat{O} = \text{Ext}(\hat{X}, \hat{H})$ be the output of the extractor. Since $\|XH - \hat{X}\hat{H}\|_1 \leq \varepsilon'$, using Fact 5 we have
\[ \|OXH - \hat{O}\hat{X}\hat{H}\|_1 \leq \varepsilon'. \]
Using Fact 5 again, we further have
\[ \|O - \hat{O}\|_1 \leq \varepsilon'. \quad (7) \]
Also, since $\hat{O} = \text{Ext}(\hat{X}, \hat{H})$ is the output of the extractor, we have
\[ \|\hat{O} - U_m\|_1 \leq \varepsilon. \]
Using Eq. (7) along with triangle inequality, we have the desired. □

Lemma 1: Let $\text{ECC} : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$ be an $(n, k, n-k+1)$ Reed-Solomon code from Fact 16 for $q \geq n+1$. Let random variable $M \in \mathbb{F}_q^n$ be uniformly distributed over $\mathbb{F}_q^n$. Let $C = \text{ECC}(M)$ and $t$ be any positive integer such that $t < k$. Let $S$ be a subset of $[n]$ such that $|S| = t$ and $Q$ be a subset of $[k]$ such that $|Q| = j \leq k - t$. Then, for every fixed string $c$ in $\mathbb{F}_q^t$ and $C^S = c$\footnote{$C^S$ corresponds to codeword corresponding to columns $S$ of codeword $C$.}, the distribution $M^c \overset{\Delta}{=} M|(C^S = c)$ is $(M^c)^Q = U_{j \log q}$. Further more, for any fixed string $l$ in $\mathbb{F}_q^t$, we can efficiently (in time polynomial in $(k, q)$) sample from the distribution $(M^c)^{[k]\setminus Q}|((M^c)^Q = l)$.

Proof: The generator matrix for ECC is given by
\[
G = \begin{pmatrix}
1 & \alpha_1 & \ldots & \alpha_{k-1}^t \\
1 & \alpha_2 & \ldots & \alpha_{k-1}^t \\
\vdots & \vdots & \ddots & \vdots \\
1 & \alpha_n & \ldots & \alpha_{k-1}^t
\end{pmatrix},
\]
where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct non-zero elements of $\mathbb{F}_q$ (this is possible since $q \geq n+1$). Let $S = \{s_1, s_2, \ldots, s_t\}$ and
\[
G_S = \begin{pmatrix}
1 & \alpha_{s_1} & \ldots & \alpha_{s_1}^{k-1} \\
1 & \alpha_{s_2} & \ldots & \alpha_{s_2}^{k-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \alpha_{s_t} & \ldots & \alpha_{s_t}^{k-1}
\end{pmatrix}.
\]
Note we have $G_SM^t = (C^S)^t$. By fixing $C^S = c$, we have imposed the following linear constraints as given by $G_SM^t = c^t$. Note $G_S$ is a Vandermonde matrix for any fixed subset $S \subset [n]$, $|S| = t$ and $t < k$. Thus, any $t \times t$ submatrix of $G_S$ has full rank. Note $k - j \geq t$. Note $M^c$ is exactly the distribution, $m \leftarrow \{m \in \mathbb{F}_q^k : G_SM^t = c^t\}$. Let $\mathcal{P} = [k] \setminus Q$ and $\mathcal{P} = \{p_1, p_2, \ldots, p_{k-j}\}$ with elements in the set $\mathcal{P}$ in any fixed order. Equivalent way to define $M^c$ is the distribution, $m \leftarrow \{m \in \mathbb{F}_q^k : G^t = c^t\}$, such that $G$ is $t \times k$ matrix, the submatrix of $G$ corresponding to columns given by $\mathcal{P}$ is exactly $I_{t \times t}$ (since any $t \times t$ submatrix of $G_S$ has full rank). Note one can get $(G, \hat{c})$ from $(G_S, c)$ using standard Gaussian elimination procedure (in time polynomial in $(k, q)$). Thus, sampling $m = \{m_1, m_2, \ldots, m_t\}$ from the distribution $M^c$ can be achieved as follows:

- Sample for every $i \in Q$, $m_i$ uniformly and independently from $\mathbb{F}_q$.
- Sample for every $i \in \mathcal{P} \setminus \mathcal{P}'$, $m_i$ uniformly and independently from $\mathbb{F}_q$.
- For every $i \in \mathcal{P}'$, set $m_i \in \mathbb{F}_q$ such that it satisfies the linear constraints $G_m = c$\footnote{Note the variables in $Q$ that appear in this linear constraint are already sampled before.}.

Thus, $(M^c)^Q = U_{j \log q}$. Further more, for any fixed string $l$ in $\mathbb{F}_q^t$, we can efficiently (in time polynomial in $(k, q)$) sample from the distribution $(M^c)^{[k]\setminus Q}|((M^c)^Q = l)$. □

III. A QUANTUM SECURE NON-MALLEABLE CODE IN THE SPLIT-STATE MODEL

Theorem 5 (Quantum Secure Non-Malleable Code in the Split-State Model): Let $2\text{nmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m$ be an $(n-k, n-k, \varepsilon)$-quantum secure 2-source non-malleable extractor. There exists an $(m, n, \varepsilon')$-quantum secure non-malleable code with parameter $\varepsilon' = 2^{m(4(2-k^2) + \varepsilon) + \varepsilon}$.

Proof: Let $\sigma_S = U_m$. Given a $2\text{nmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m$, let $(\text{Enc}, \text{Dec})$ be defined as follows:

- For any fixed message $S = s \in \{0,1\}^m$, the encoder, Enc outputs a uniformly random string from the set $2\text{nmExt}^{-1}(s) \subset \{0,1\}^{2m}$.
- $\text{Dec}(x,y) = 2\text{nmExt}(x,y)$ for every $(x,y) \in \{0,1\}^{2m}$.

Note for every $s \in \{0,1\}^m$, $\text{Pr}(\text{Dec}(\text{Enc}(s))) = 1$.

We first show that $(\text{Enc}, \text{Dec})$ is a quantum secure non-malleable code in the split-state model (see Definition 3 and Figure 1). Note
\[
\sigma_{S\text{Enc}(S)} = \sigma_{SXY}
\]
\[
= \sum_{s \in \{0,1\}^m} \left( \frac{1}{2^m} |s\rangle \langle s| \otimes \left( \frac{1}{2\text{nmExt}^{-1}(s)} \sum_{(x,y) : 2\text{nmExt}(x,y) = s} |xy\rangle \langle xy| \right) \right)
\]
after encoding a uniform message $S$. Note $(X,Y) = \text{Enc}(S)$.

Let $\theta_{X,X,Y,Y} = \theta_{X,X,Y,Y_1} = \theta_{X,X_1} \otimes \theta_{Y,Y_1}$ be a pure state such that $\theta_X = \theta_Y = U_n$. $(X_1, \hat{X})$ are copies of $X$, $(Y_1, \hat{Y})$ are copies of $Y$ respectively. Note $\theta_{X,Y} = U_n \otimes U_n$. Let $S_1 = 2\text{nmExt}(X_1, Y_1), S = 2\text{nmExt}(X,Y)$. For the state $\theta$ with the following assignment (terms on the left are from Definition 8 and on the right are from here).
\[
(X, \hat{X}, N, M, Y, \hat{Y}) \leftarrow (X_1, \hat{X}, X, Y, Y_1, \hat{Y}),
\]
one can note $\theta$ is an $(n,n)$-qpa-state. Using Claim 14\footnote{$(n,n)$-qpa-state is also an $(n-k, n-k)$-qpa-state.} along with Fact 5, we have
\[
\|\theta_{2\text{nmExt}(X_1,Y_1)} - \sigma_S\|_1 = \|\theta_{2\text{nmExt}(X_1,Y_1)} - U_m\|_1 \leq \varepsilon.
\]
\[
\sigma_{SXY}|(S = s) = |s\rangle\langle s| \otimes \left( \frac{1}{|2nmExt^{-1}(s)|} \sum_{(x,y):2nmExt(x,y)=s} |xy\rangle\langle xy| \right).
\]

Also,
\[
\theta_{S_{1},XY}|(S_{1} = s) = |s\rangle\langle s| \otimes \left( \frac{1}{|2nmExt^{-1}(s)|} \sum_{(x,y):2nmExt(x,y)=s} |xy\rangle\langle xy| \right).
\]

Thus using Fact 5 after noting Eq. (8) and Eq. (10), we have
\[
\|\theta_{S_{1},XY} - \sigma_{SXY}\| \leq \|\theta_{S_{1}} - \sigma_{S}\|.
\]

Since, \(\|\theta_{S_{1}} - \sigma_{S}\| \leq \varepsilon\), we get
\[
\|\theta_{S_{1},XY} - \sigma_{SXY}\| \leq \varepsilon.
\]

Let \(A = (U, V, \psi)\) be the quantum split-state adversary from Definition 2. Note \(\psi_{NM}\) is an entangled pure state, \(U : \mathcal{H}_{X} \otimes \mathcal{H}_{N} \rightarrow \mathcal{H}_{X} \otimes \mathcal{H}_{N}\), and \(V : \mathcal{H}_{Y} \otimes \mathcal{H}_{M} \rightarrow \mathcal{H}_{Y} \otimes \mathcal{H}_{M}\) are isometries without any loss of generality.

In the analysis, we consider a pure state \(\rho'\) which is generated from \(\theta_{X_{1}X_{1}Y_{1}Y_{1}} = \theta_{X_{1}X_{1}} \otimes \theta_{Y_{1}Y_{1}}\), in the following way (see Figure 2):
\begin{itemize}
  \item Let \(\rho' = (U \otimes V)(\theta \otimes |\psi\rangle\langle \psi|)(U \otimes V)\) be the state after the action of quantum split-state adversary.
  \item Let \(\rho'\) be the pure state extension after measuring the registers \((X', Y')\) in the computational basis in \(\rho'\). Note the measurement in the computational basis of registers \((X', Y')\) corresponds to applying CNOT\(^{15}\) to modify \((X', Y') \rightarrow (X', \hat{X}', Y', \hat{Y}')\) such that \(\hat{X}', \hat{Y}'\) are copies of \(X', Y'\) respectively.
\end{itemize}

Let binary variables \(C, D\) (with copies \(\hat{C}, \hat{D}\)) be such that \(C = 1\) indicates \(X_{1} \neq X'\) and \(D = 1\) indicates \(Y_{1} \neq Y'\) (in state \(\rho'\)).

Let \(S' = 2nmExt(X', Y')\). Since \(\|\theta_{S_{1},XY} - \sigma_{SXY}\| \leq \varepsilon\) from Eq. (12), using Fact 5 we have \(\|\rho'_{S_{1},S'} - \rho_{SS'}\| \leq \varepsilon\).

We will show
\[
\|\rho'_{S_{1},S'} - Z_{copy}(D_{A}, Z)\| \leq 4(2^{-k} + \varepsilon),
\]

for \(Z = U_{m}\) and distribution \(D_{A}\) that depends only on \(A\). We get that
\[
\|\rho_{SS'} - Z_{copy}(D_{A}, Z)\| \leq 4(2^{-k} + \varepsilon) + \varepsilon,
\]

from \(\|\rho'_{S_{1},S'} - \rho_{SS'}\| \leq \varepsilon\) and the triangle inequality, which implies the desired (using Fact 6).

\[
\|S'_{s} - copy(D_{A}, s)\| \leq 2^{m}(4(2^{-k} + \varepsilon) + \varepsilon),
\]

\[\forall s \in \{0, 1\}^{m}\].

We now proceed to prove Eq. (13). For \(C = c \in \{0, 1\}, D = d \in \{0, 1\}\), denote \(\rho_{c,d}^{e} = \rho_{((C, D) = (c, d))}\).

Claim 4: For every \(c, d \in \{0, 1\}\) except \((c, d) = (0, 0)\), we have
\[
Pr((C, D) = (c, d))\rho_{c,d}^{e}\|\rho'_{S_{1},S'} - Z \otimes \rho'_{S_{1},S'}\| \leq 2^{-k} + \varepsilon.
\]

For \((c, d) = (0, 0)\), we have
\[
Pr((C, D) = (c, d))\rho_{c,d}^{e}\|\rho'_{S_{1},S'} - ZZ\| \leq 2^{-k} + \varepsilon,
\]

where \(Z = U_{m}\).

Proof: Fix \(c, d \in \{0, 1\}\). Suppose \(Pr((C, D) = (c, d))\rho'_{c,d} \leq 2^{-k}\), then we are done. Thus we assume otherwise. Note in state \(\rho'_{c,d}\), we have
\[
\rho'_{X_{1}X_{1}Y_{1}Y_{1}X'X'X'X'Y'Y'} = U_{n} \otimes \rho'_{X_{1}X_{1}X'X'X'X'X'X'X'Y'Y'Y'Y'}.
\]

\[^{15}\text{By CNOT on n qubit register, we mean applying NOT gate on different ancilla each time conditioned on each qubit independently. This operation amounts to performing measurement in the computational basis.}\]
Thus,
\[ H_{\min}(X_1 | Y_1 Y'_{1} Y'_{2} M') \rho_{\delta} = n \];
\[ H_{\min}(Y_1 | X_1 X'_{1} X'_{2} N') \rho_{\delta} = n. \]

Using Fact 2, we have
\[ H_{\min}(X_1 | Y_1 Y'_{1} Y'_{2} M') \rho_{\delta} = n \];
\[ H_{\min}(Y_1 | X_1 X'_{1} X'_{2} N') \rho_{\delta} = n. \]

We use Fact 17, with the following assignment of registers (below the registers on the right are from Fact 17 and the registers on the right are the registers in this proof),
\[(\rho_A, \rho_B, \rho_C) \leftarrow (\rho_X, \rho_{X'}, \rho_{Y'}, \rho_{M'}, \rho_{C}).\]

From Fact 17, we get that
\[ H_{\min}(X_1 | Y_1 Y'_{1} Y'_{2} M') \rho_{\delta} \geq n - k. \]

Similarly, \[ H_{\min}(Y_1 | X_1 X'_{1} X'_{2} N') \rho_{\delta} \geq n - k. \]

Let \( (c, d) = (0, 0) \). Note \( \rho_{\delta}^{0,0} \) is an \( (n-k, n-k) \)-qpp-state. Using Claim 1 along with Fact 5, we have \( \|\rho_{\delta}^{0,0}||_{1} \leq \varepsilon \). We also have \( X_1 = X' \) and \( Y_1 = Y' \) in \( \rho_{\delta}^{0,0} \). Thus Fact 5 will imply
\[ \|\rho_{\delta}^{0,0}||_{1} \leq \varepsilon. \]

Let \( (c, d) \neq (0, 0) \). Note \( \rho_{\delta}^{c,d} \) is an \( (n-k, n-k) \)-qpp-state since either \( \Pr((X_1 \neq X') \cup (Y_1 \neq Y')) = 1 \) in \( \rho_{\delta}^{c,d} \).

Since, \( 2nmExt : \{0, 1\}^{n} \times \{0, 1\}^{n} \rightarrow \{0, 1\}^{m} \) is a \( (n-k, n-k, \varepsilon) \)-secure two-source non-malleable extractor (see Definition 10), using Fact 5 we have
\[ \|\rho_{\delta}^{c,d}||_{1} \leq \varepsilon. \]

This completes the proof. □

For every \( c, d \in \{0, 1\} \) except \( (c, d) = (0, 0) \), let \( D_{A}^{c,d} \) be the distribution that is deterministically equal to same. Let \( D_{A} = \sum_{c,d \in \{0, 1\}} \Pr((C, D) = (c, d)) \rho_{\delta}^{c,d} \). Note for every \( c, d \in \{0, 1\} \), the value \( \Pr((C, D) = (c, d)) \rho_{\delta}^{c,d} \) depends only on \( A \). We have,
\[ \rho_{S_{1}, S_{2}}^{c,d} = \sum_{c,d \in \{0, 1\}} \Pr((C, D) = (c, d)) \rho_{\delta}^{c,d}. \]

and
\[ Z_{copy}(D_{A}, Z) = \sum_{c,d \in \{0, 1\}} \Pr((C, D) = (c, d)) Z_{copy}(D_{A}^{c,d}, Z). \]

Consider,
\[ \|\rho_{S_{1}, S_{2}}^{c,d} - Z_{copy}(D_{A}, Z)\|_{1} \]
\[ = \| \sum_{c,d \in \{0, 1\}} \Pr((C, D) = (c, d)) \rho_{\delta}^{c,d} - Z_{copy}(D_{A}, Z)\|_{1} \]
\[ \leq \sum_{c,d \in \{0, 1\}} \Pr((C, D) = (c, d)) \|\rho_{\delta}^{c,d} - Z_{copy}(D_{A}^{c,d}, Z)\|_{1} \]
\[ \leq (2^{-k} + \varepsilon). \]

The first inequality follows from Eq. (14), the first inequality follows from Eq. (15) and Fact 7 and the second inequality follows from Claim 4. This completes the proof. □

IV. EFFICIENT QUANTUM SECURE NON-MALLEABLE CODES

For any quantum secure non-malleable extractor 2nmExt\((\ldots)\), we have shown that \((Enc, Dec) = (2nmExt^{-1}(\ldots), 2nmExt(\ldots))\) forms a quantum secure non-malleable code in the split state model. Note that 2nmExt\((\ldots)\) is an efficient algorithm. However, the challenging aspect lies in demonstrating that for any message \( s \), efficient sampling from the set 2nmExt\(^{-1}\)(\( s \)) is possible. It is not clear a priori whether such sampling can be performed efficiently.

To achieve efficient preimage sampling for the non-malleable extractor, several modifications are required. In this section, we present the modified non-malleable extractor, referred to as new-2nmExt. We begin with a brief overview of the necessary modifications to construct a non-malleable extractor efficiently for non-malleable code encoding. We modify the construction of 2nmExt from [2], incorporating ideas from [6] to create new-2nmExt : \( \{0, 1\}^{n} \times \{0, 1\}^{n} \rightarrow \{0, 1\}^{m} \), ensuring \( n - n_{1}, n - n_{2} \)-security against qm-adv with parameters \( n_{1} = n^{\Omega(1)}, m = n^{-1-\Omega(1)} \), and \( \varepsilon = 2^{-n^{\Omega(1)}} \). We divide the sources \( X \) and \( Y \) into \( n^{\Omega(1)} \) blocks, each of size \( n^{-1-\Omega(1)} \). The main idea is to use new blocks of \( X \) and \( Y \) for each round of alternating extraction in the non-malleable extractor construction. This approach ensures that the linear constraints imposed during alternating extraction apply to different variables of the input sources, \( X \) and \( Y \). Additionally, since \( X \) and \( Y \) each possess almost full min-entropy, they can be viewed as block sources with each block having almost full min-entropy, which is supported by Fact 18. This property enables the generation of suitable intermediate seed random variables (approximately uniform) using alternating extraction.

While generating \( S = \text{new-2nmExt}(X, Y) \), several intermediate random variables (denoted as \((R_1, R_2, \ldots, R_k)\)) in this order are generated starting from \((X, Y)\). During the reverse sampling process, starting from \( S \), these variables need to be generated in reverse order, and we refer to this process as backtracking. To maintain control over the overall error, it is essential to take into account and utilize the important Markov-chain structures between these intermediate random variables.

A. Modified Non-Malleable Extractor

These parameters hold throughout this section.

B. Parameters

Let \( \delta, \delta_{1}, \delta_{2} > 0 \) be small enough constants such that \( \delta_{1} < \delta_{2} \). Let \( n, n_{1}, n_{2}, n_{x}, n_{y}, \ldots, n_{y}, a, s, b, h \) be positive integers and \( \varepsilon, \varepsilon > 0 \) such that:
\[ n_{1} = n^{\delta_{2}}; \ n_{2} = n - 3n_{1} ; \]
\[ q = 2^{\log(n+1)} \quad \varepsilon = 2^{-O(n^{\delta})} \]

\[ n_3 = \frac{n_1}{10} \quad n_4 = \frac{n_2}{\log(n + 1)} \quad n_5 = n_2^{\delta/3} \]

\[ a = 6n_1 + 2O(n_5) \log(n + 1) = O(n_1) \]

\[ n_6 = 3n_1^3 \quad n_7 = n - 3n_1 - n_6 \quad n_x = \frac{n_2^2}{12a} \]

\[ n_y = \frac{n_2^n}{12a} \quad 2^O(a) \sqrt{\varepsilon} = \varepsilon \]

\[ s = O \left( \log^2 \left( \frac{n}{\varepsilon} \right) \log n \right) \]

\[ b = O \left( \log^2 \left( \frac{n}{\varepsilon} \right) \log n \right) \quad h = 10s \]

- IP1 be IP3^{n_1}/n_3, Ext1 be (2b, \varepsilon')-quantum secure \((n_y, s, b)\)-extractor,
- Ext2 be (2s, \varepsilon')-quantum secure \((h, b, s)\)-extractor,
- Ext3 be \((4h, \varepsilon')\)-quantum secure \((n_x, b, 2h)\)-extractor,
- Ext4 be \((n_y/4, \varepsilon, 2^h)\)-quantum secure \((4n_y, 2h, n_y/8)\)-extractor,
- IP2 be IP3^{n_2}/2h,
- Ext5 be \((2^b, \varepsilon')\)-quantum secure \((4n_x, n_y/8, n_x/4)\)-extractor.

\(S_{X_i}X^{[a+1]}Y_3 Y^{[b+1]}(G = g)\)

The accomplishment of this task is realized through the provisions outlined in Claim 7. Within the proof of Claim 7, a pivotal utilization comes from the distinct utilization of source blocks for each iteration of the flip-flop procedure, as illustrated by Algorithm 3. To facilitate the backtracking of each intermediate random variable, we capitalize on the implications of Claim 3. Furthermore, we leverage the inherent Markov chain structures (as established by Claim 2) among the intermediate random variables. These factors collectively enable us to contend that the cumulative error in the backtracking process remains well-controlled. This succinctly outlines the overarching argument at a higher level.

**Theorem 6 (Security of new-2nmExt):** Let \(\rho_{X^{[a]}Y^{[b]}M}^{[a]}\) be an \((n - n_1, n - n_1\times q)\)-state with \(|X| = |Y| = n\). Then,

\[ \|\rho_{X^{[a]}Y^{[b]}M}^{[a]} - U_{n_x/4} \otimes \rho_{S^{[a]}M}^{[b]}\|_1 \leq O(\varepsilon) \]

\[ S = \text{new-2nmExt}(X,Y) \quad S' = \text{new-2nmExt}(X',Y') \]

**Proof:** The proof proceeds in similar lines to the proof of Theorem 6 in [2] using Fact 21 for alternating extraction argument, Fact 22 for bounding the min-entropy required in alternating extraction, Facts 14, 19 for the security of inner-product function in \((k_1, k_2)\)-qpa-state framework, Fact 4 for relation between \(\Delta_B, \Delta \) and we do not repeat it. \(\square\)

**D. Efficiently Sampling From the Preimage of new-2nmExt**

Recall that we have shown the existence of a quantum secure non-malleable code where the encoding scheme is based on inverting 2nmExt, a quantum secure 2-source non-malleable extractor. Specifically, for any fixed message \(S = s\), the encoder Enc outputs a uniformly random string from the set \(2^{nmExt} - s\). The decoder is the function 2nmExt itself. We refer to this as the encoding and decoding based on 2nmExt. Now, we state the main result of this paper.

**Theorem 7 (Main Theorem):** Let \(\text{new-2nmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m\) be the quantum secure 2-source non-malleable extractor from Algorithm 1, where \(m = n_x/4\). Let \((\text{Enc}, \text{Dec})\) be the encoding and decoding based on new-2nmExt. Let \(\tilde{S}_{\text{Enc}}(S) = \tilde{S}XY\) for a uniform message \(\tilde{S} = U_m\). There exists an efficient algorithm that can sample
from a distribution $\tilde{S}X\tilde{Y}$ such that $\|\tilde{S}X\tilde{Y} - \tilde{S}X\tilde{Y}\|_1 \leq O(\varepsilon)$ and $\tilde{S} = U_m$.

**Proof:** Consider $XY = U_n \otimes U_n$. Let $S = \text{new-2nmExt}(X,Y)$. From Eq. (12) in the proof of Theorem 5 (after noting $\tilde{S}X\tilde{Y} = (SXY)_0$ in Eq. (12) and $SXY = (SXY)_0$ in Eq. (12)), we have

$$\|SXY - \tilde{S}X\tilde{Y}\|_1 \leq O(\varepsilon).$$

(17)

From Claim 5, we have an efficient algorithm that can sample from a distribution $\tilde{S}X\tilde{Y}$ such that

$$\|SXY - \tilde{S}X\tilde{Y}\|_1 \leq O(\varepsilon) ; \quad \tilde{S} = U_m.$$  

From Eq. (17) and using triangle inequality, we have

$$\|SXY - \tilde{S}X\tilde{Y}\|_1 \leq O(\varepsilon) ; \quad \tilde{S} = U_m,$$

which completes the proof. □

We have the following corollary.

**Corollary 2:** Let $0 < \varepsilon < \delta_1$ and $m' = n^{\delta_3}$ be an integer. Let $\text{new-2nmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m$ be the quantum secure 2-source non-malleable extractor from Algorithm 1, where $m = n_x/4$. Let $\text{2nmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m$ be such that $\text{2nmExt}(X,Y)$ is same as $\text{new-2nmExt}(X,Y)$ truncated to first $m'$ bits. Let $(\text{Enc}, \text{Dec})$ be the encoding and decoding based on $\text{2nmExt}$. Let $\text{SEnc}(\tilde{S}) = \tilde{S}X\tilde{Y}$ for a uniform message $\tilde{S} = U_{m'}$. There
exists an efficient algorithm that can sample from a distribution
\(\tilde{S}XY\) such that \(\tilde{S} = U_{mn}\) and for every \(s \in \{0, 1\}^m\), we have
\[\|(\tilde{X}Y)(\tilde{S} = s) - (XY)(\tilde{S} = s)\|_1 \leq O(2^n e) \leq 2^{-n(\epsilon)} \\].

**Claim 5:** Let \(2n\text{Ext} : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}^{n/4}\) be the new-2nExt from Algorithm 1. Let \(XY = U_n \otimes U_n\), \(S = 2n\text{Ext}(X, Y)\) and intermediate random variables
\[X_1, Y_1, R, G, X_3, Y_3, X'[a_1, 1], Y'[a_1, 1],\]
\[X'[a_2, 3a], Y'[a_2, 3a], S\]
be as defined in Algorithms 1, 2, 3. Then, we have
\[G X_3 Y_3 X'[a_1, 1] Y'[a_1, 1] = G \otimes X_3 Y_3 X'[a_1, 1] Y'[a_1, 1].\]

Furthermore, given \(g \in \text{supp}(G)\) and \(x_3 y_3 [a_1, 1, y] [a_1, 1]\), we can efficiently (in time polynomial in \(n\)) sample from the distribution
\[X'[a_2, 3a], Y'[a_2, 3a]|(G = g, X_3 Y_3 X'[a_1, 1] Y'[a_1, 1] = x_3 y_3 [a_1, 1, y] [a_1, 1]).\]

**Proof:** Our goal is to show that \(G X_3 Y_3 X'[a_1, 1] Y'[a_1, 1] = G \otimes X_3 Y_3 X'[a_1, 1] Y'[a_1, 1]\). It suffices to instead show that for every fixing of \(G = g\), distribution of \(X_3 Y_3 X'[a_1, 1] Y'[a_1, 1]\) remains unchanged.

Note \(X = X_1 \circ X_2, Y = Y_1 \circ Y_2\) and \(G = X_1 \circ \text{ECC}(X_2)\text{Samp}(\text{IP}(X_1, Y_1)) \circ Y_1 \circ \text{ECC}(Y_2)\text{Samp}(\text{IP}(X_1, Y_1))\) from the construction of 2nExt. Note \(X_2 Y_2 = U_n = U_n\) and for fixed \(G = g\), the distribution \(X_3 Y_2|2(G = g) = X_2|2(G = g) \otimes Y_2|2(G = g)\).

We now view \(X_2 \in \mathbb{F}_q^m\), where \(q = n + 1\). Let \(j \in [n]\); be such that \(\text{Crop}(X_2, 1, j, \log(n + 1))\) has the string \((X_3, X'[a_1, 1])\) as prefix. Thus, \((n_4 - j) \log(n + 1) \leq (2a - 1) n_4 x\).

For our choice of parameters, \(j < n_4 - n_5\). We now fix \(G = x_1 \circ x_2 \circ y_1 \circ y_2\) and let \(T_g = \text{Samp}(\text{IP}(x_1, y_1)) = \{t_1, t_2, \ldots, t_{n_5}\}\).

Using Lemma 1, with the following assignment of terms (terms on left are from Lemma 1 and terms on right are from here)

\(k, q, n, t, S, Q, M, = (n, n_1, n + 1, n, n_5, T_g, [j], X_2)\),

we get that \(X_2|2(G = g)\) restricted to first \(j \log(n + 1)\) bits is uniform. Thus, \(\text{Crop}(X_2|2(G = g), 1, j, \log(n + 1))\) is uniform.

This further implies \((X_3, X'[a_1, 1])|2(G = g)\) is uniform since \((X_3, X'[a_1, 1])\) is a prefix of \(\text{Crop}(G, 2|G = g, 1, j, \log(n + 1))\). Also, sampling from \(X'[a_2, 3a]|2(G = g, X_3 X'[a_1, 1] = x_3 x'[a_1, 1])\) in time polynomial in \((n_4, n + 1)\) follows from Lemma 1.

Using similar argument one can also note \((Y_3, Y'[a_1, 1])|2(G = g)\) is uniform and sampling from \(Y'[a_2, 3a]|2(G = g, Y_3 Y'[a_1, 1] = y_3 y'[a_1, 1])\) can be done in time polynomial in \((n_4, n + 1)\). Thus, \(G X_3 Y_3 X'[a_1, 1] Y'[a_1, 1] = G \otimes X_3 Y_3 X'[a_1, 1] Y'[a_1, 1]\) follows since

\[X_3 Y_3 X'[a_1, 1] Y'[a_1, 1]|2(G = g) = X_3 Y_3 X'[a_1, 1] Y'[a_1, 1],\]

\[X_3 Y_3 X'[a_1, 1] Y'[a_1, 1] = U_{n_4} \otimes U_{n_4} \otimes U_{(a_1 + 4)n} \otimes U_{(a_1 + 4)n}.\]

**Claim 7:** Let \(2n\text{Ext} : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}^{n/4}\) be the new-2nExt from Algorithm 1. Let \(XY = U_n \otimes U_n, S = 2n\text{Ext}(X, Y)\) and intermediate random variables
\[X_1, Y_1, R, G, X_3, Y_3, X'[a_1, 1], Y'[a_1, 1], Z'[a], A'[a], B'[a], C[a], Z'[a], A'[a], B'[a], C'[a], Z'[a], A'[a], B'[a], C'[a], Z'[a], A'[a], B'[a], C'[a], F, S\]
be as defined in Algorithms 1, 2, 3. For any \(g \in \text{supp}(G)\), we can sample efficiently from a distribution
\[\{(X_3 Y_3 X'[a_1, 1] Y'[a_1, 1]|S)|(G = g) - (X_3 Y_3 X'[a_1, 1] Y'[a_1, 1]|S)|(G = g)|\|_1 \leq O(e)\text{ ; } S\|(G = g) = U_{n_4/4}\].

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
Proof: As evident from Claim 6, the relation \( G_X Y_3 X^{|a+1|} Y^{|a+1|} = G \otimes X_3 Y_3 X^{|a+1|} Y^{|a+1|} \) holds true. Consequently, when \( G \) is fixed to \( g \), the distribution of sources within the alternating extraction process remains unchanged, precisely uniform. Additionally, under the condition that \( G = g \), the output \( S \) is solely contingent on \( X_3 X^{|a+1|} Y_3 X^{|a+1|} \), an implication stemming from the construction of the non-malleable extractor. This insight paves the way for a sampling approach from the distribution \((X_3 Y_3 X^{|a+1|} Y^{|a+1|} S)\) \((G = g)\). The process commences with the sampling of \( S = U_{n_3/4} \) followed by the sampling from the distribution \((X_3 Y_3 X^{|a+1|} Y^{|a+1|} S)\) \((G = g, S = s)\).

At a higher level, the process of sampling from \((X_3 Y_3 X^{|a+1|} Y^{|a+1|} S)\) \((G = g, S = s)\) entails the following considerations:

- Within each \( i \)-th invocation of Algorithm 3, the utilization of blocks \( X^i \) and \( Y^i \) in conjunction with the intermediate random variable \( Z^i \) results in the generation of \( Z^{i+1} \).
- Notably, the blocks \( X^i \) and \( Y^i \) remain distinct for each \( i \in [a] \).

The backtrack process commences from the random variable \( S \). Initially, sampling from \( Z^a X^a Y^a X^{a+1} Y^{a+1} | S \) is pursued. Given that \( Z^a \) solely depends on \( X^{a-1} Y^{a-1} Z^{-1} \), the subsequent step involves backtracking to sample from \( X^{a-1} Y^{a-1} Z^{-1} X^a Y^a X^{a+1} Y^{a+1} | S \). In light of these two successive backtracking steps, the focal argument pertains to the assertion that the distribution obtained by sampling \( Z^a X^a Y^a X^{a+1} Y^{a+1} | S \) closely approximates the distribution resulting from first sampling \( Z^a X^a Y^a X^{a+1} Y^{a+1} | S \) and subsequently \( Z^{a-1} X^{a-1} Y^{a-1} Z^{a-1} X^{a-1} Y^{a+1} | S \). In a more explicit fashion:

\[
Z^{a-1} X^{a-1} Y^{a-1} Z^a X^a Y^a X^{a+1} Y^{a+1} | S \approx Z^a X^a Y^a X^{a+1} Y^{a+1} | S.
\]

The pivotal step lies in the argument pertaining to how the error accumulates through multiple backtracking steps. This is precisely where the critical Markov chain structures (as established by Claim 2) among the intermediate random variables come into play. These structures facilitate the assertion that the cumulative error introduced through the backtracking process remains within manageable limits.

Indeed, in our analysis, we employ notations to indicate the random variables in different stages of the process:

- Tilde notation: Used to denote the random variables that are sampled in the reverse order during the backtracking process.
- Hat notation: Used to denote the intermediate random variables that result from invoking Algorithm 3 on uniform input random variables.

For each backtracking step, we first show the actual random variables are approximately close to hat random variables in trace distance (for example, see Eq. (20)). Further more, it is easier to note important Markov chain structures (Claim 2) between the intermediate hat random variables (for example, see Eq. (22)). Utilizing the triangle inequality, our focus narrows down to proving that the hat random variables remain closely aligned with the tilde random variables throughout the argument.

To bridge this gap, we repeatedly rely on arguments stemming from Claim 3. These arguments are applied iteratively, all while taking into account the cumulative error that accrues during the backtracking process. This approach completes the high-level argument of the backtracking procedure.

Let \( g = g_1 g_2 \ldots g_a \). Suppose \( g_a = 1 \). We now show how to efficiently sample from distribution \((Z^a X^a Y^a X^{a+1} Y^{a+1} S)\) \((G = g)\) approximately.\(^{16}\) We remove conditioning of \( G = g \) for the rest of the proof. From Algorithms 1, 2 and 3, we have

\[
Y^a = Y^a a \odot Y^a a \odot Y^a a \odot Y^a a \quad X^a = X^a a \odot X^a a \odot X^a a \odot X^a a
\]

and \( \{A^a, B^a, C^a, Z^a, A^a, Z^a, +1, F, S\} \) as intermediate random variables for \( g_a = 1 \). From Claim 8, we have \( \|Z^a - U_{2n}\| \leq O(a^c) \). From construction of 2mnExt, we have \( Z^a Y^a Y^a X^a X^a Y^a X^{a+1} Y^{a+1} = Z^a Y^a a \odot Y^a a \odot Y^a a \odot X^a a \odot X^a a \odot X^a a \odot X^a a + X^a a \). Thus, we have

\[
\|Z^a Y^a Y^a X^a X^a Y^a X^{a+1} Y^{a+1} - U_{2n} \odot U_{n_a} \odot U_{n_y} \| \leq O(a^c) \quad (18)
\]

We now proceed flip-flop procedure (Algorithm 3) with \( Z^a Y^a Y^a X^a X^a Y^a X^{a+1} Y^{a+1} - U_{2n} \odot U_{n_a} \odot U_{n_y} \odot U_{n_a} \odot U_{n_a} \odot U_{n_a} \odot U_{n_a} \odot U_{n_y} \odot U_{n_y} \) and denote intermediate random variables as hat variables. Using Fact 5 and Eq. (18), we have

\[
Z^a Y^a Y^a X^a X^a Y^a X^{a+1} Y^{a+1} - U_{2n} \odot U_{n_a} \odot U_{n_y} \odot U_{n_a} \odot U_{n_a} \odot U_{n_a} \odot U_{n_a} \odot U_{n_y} \odot U_{n_y} \|
\]

We use the following sampling strategy to sample from a distribution \((Z^a Y^a Y^a X^a X^a Y^a X^{a+1} Y^{a+1} F X^{a+1} S)\):

1. Sample \( (\tilde{z}_a, \tilde{a}_a, z_{a+1} \odot 1, \tilde{f}, \tilde{s}) \) \( \sim \tilde{Z}^a \tilde{A} \tilde{Z}^a \tilde{A} \tilde{F} \tilde{S} = U_{2n} \odot U_{2n} \odot U_{n_a} \odot U_{n_y} \odot U_{n_a} / 4 \).
2. Sample \( \tilde{z}_{a+1} \) \( \sim X^{a+1} (\tilde{f} \tilde{s}) \) which is same as \( \tilde{z}_{a+1} \sim \tilde{x}^{a+1} : \tilde{s} = \text{Ext}_x(y^{a+1}, \tilde{f}) \).
3. Sample \( \tilde{g}_{a+1} \) \( \sim Y^{a+1} \tilde{F} = \tilde{z}_{a+1} \tilde{f} \) which is same as \( \tilde{g}_{a+1} \sim \tilde{y}^{a+1} : \tilde{f} = \text{Ext}_y(y^{a+1}, \tilde{z}_{a+1}) \).
4. Sample \( \tilde{x}_a \) \( \sim X_a \tilde{A} \tilde{Z}^a \tilde{A} = \tilde{A} \tilde{z}_a \) which is same as \( \tilde{x}_a \sim x_a : \tilde{z}_{a+1} = \text{Ext}_x(x_a, \tilde{a}_a) \).
5. Sample \( \tilde{y}_a \) \( \sim \tilde{Y}_a \tilde{A} \tilde{Z}^a \tilde{A} \tilde{z}_a \) which is same as \( \tilde{y}_a \sim y_a : \tilde{a}_a = \text{Ext}_y(y_a, \tilde{a}_a) \).
6. Sample \( \tilde{y}_{a+1} \) \( \sim \tilde{Y}_{a+1} \) independently of \( \tilde{Z}^a \tilde{Y}_a \tilde{A} \tilde{X}^{a+1} F X^{a+1} S \).
7. Sample \( \tilde{x}_a \) \( \sim \tilde{X}_a \) \( \sim \tilde{U}_{n_a} \) independently of \( \tilde{Z}^a \tilde{Y}_a \tilde{A} \tilde{X}^{a+1} F X^{a+1} S \).

We next would like to argue the closeness of tilde random variables \( Z^a Y^a Y^a X^a X^a Y^a X^{a+1} Y^{a+1} F X^{a+1} S \) and hat random variables \( Z^a Y^a Y^a X^a X^a Y^a X^{a+1} Y^{a+1} F X^{a+1} S \).

From Algorithms 1, 2, 3 and using block structure of sources to generate intermediate random variables, we have

\[
(\tilde{Z}_a \otimes \tilde{Y}_a) \leftrightarrow (\tilde{A} \otimes \tilde{X}_a) \leftrightarrow (\tilde{Z}^{a+1} \otimes \tilde{Y}^{a+1}) \leftrightarrow (F \otimes \tilde{X}^{a+1}) \leftrightarrow \tilde{S}. \quad (23)
\]

\(^{16}\)Similar argument holds when \( g_a = 0 \).
Using Corollary 1 and noting \( \hat{Z}^a Y^a_3 = U_s \otimes U_n \), we have, 
\[
\|\hat{A}^a \hat{X}^a_4 - U_b \otimes U_n\|_1 \leq \epsilon'.
\]
Noting \( \hat{A}^a \hat{X}^a_4 = A^a \otimes U_n \), we further have
\[
\|\hat{A}^a \hat{X}^a_4 - U_b \otimes U_n\|_1 \leq \epsilon'.
\]
Using similar arguments, we also get
\[
\|\hat{Z}^{a+1} \hat{Y}^{a+1} - U_{2h} \otimes U_{n_{2h}}\|_1 \leq 2\epsilon';
\]
\[
\|\hat{F} \hat{X}^{a+1} - U_{n_{2h}} / U_{4n_{2h}}\|_1 \leq 2\epsilon' + \epsilon^2.
\]
Note, we have
\[
\|\hat{F} \hat{X}^{a+1} - U_{n_{2h}} / U_{4n_{2h}}\|_1 \leq 2\epsilon' + \epsilon^2 ;
\]
\[
\hat{S} = \text{Ext}_\theta(\hat{X}^{a+1}, \hat{F}).
\]
Using Claim 3, with the below assignment of terms (terms on the left are from Claim 3 and on the right are from here),
\[
(X, H, O, \hat{X}, \hat{H}, \hat{O}, \epsilon''') \leftarrow
\]
\[(\hat{X}^{a+1}, \hat{F}, \hat{S}, \hat{X}^{a+1}, \hat{F}, \hat{S}, 0),
\]
we get that the sampled distribution \( \hat{F} \hat{X}^{a+1} \hat{S} \) satisfies
\[
\|\hat{F} \hat{X}^{a+1} \hat{S} - \hat{F} \hat{X}^{a+1} \hat{S}\|_1 \leq 2\epsilon' + \epsilon^2.
\]
Noting (from Eq. (25)),
\[
\|\hat{Z}^{a+1} \hat{Y}^{a+1} - U_{2h} \otimes U_{4n_{2h}}\|_1 \leq 2\epsilon';
\]
\[
\hat{F} = \text{Ext}_\theta(\hat{Y}^{a+1}, \hat{Z}^{a+1})
\]
and using Claim 3 again, with the below assignment of terms (terms on the left are from Claim 3 and on the right are from here),
\[
(X, H, O, \hat{X}, \hat{H}, \hat{O}, \epsilon''') \leftarrow
\]
\[(\hat{Y}^{a+1}, \hat{Z}^{a+1}, \hat{F}, \hat{Y}^{a+1}, \hat{Z}^{a+1}, \hat{F}, \hat{S}, 0),
\]
we get that the sampled distribution \( \hat{Z}^{a+1} \hat{Y}^{a+1} \hat{F} \) satisfies
\[
\|\hat{Z}^{a+1} \hat{Y}^{a+1} \hat{F} - \hat{Z}^{a+1} \hat{Y}^{a+1} \hat{F}\|_1 \leq 2\epsilon' + \epsilon^2.
\]
Note \( \hat{Z}^{a+1} \hat{Y}^{a+1} \hat{F} \leftarrow \hat{F} \leftarrow \hat{X}^{a+1} \hat{S} \) (from Eq. (22)).
\[
\hat{Z}^{a+1} \hat{Y}^{a+1} \hat{F} \leftarrow \hat{F} \leftarrow \hat{X}^{a+1} \hat{S}
\]
we get that the sampled distribution \( \hat{Z}^{a+1} \hat{Y}^{a+1} \hat{F} \hat{X}^{a+1} \hat{S} \) satisfies
\[
\|\hat{Z}^{a+1} \hat{Y}^{a+1} \hat{F} \hat{X}^{a+1} \hat{S}\|_1 \leq 2\epsilon' + \epsilon^2.
\]
Using Eqs. (20) (which states the closeness of actual random variables and hat random variables), (32) (which states the closeness of tilde random variables and hat random variables) and triangle inequality, we get
\[
\|\hat{Z}^{a+1} \hat{Y}^{a+1} \hat{F} \hat{X}^{a+1} \hat{S}\|_1 \leq O((a + 1\epsilon') + 4\epsilon).
\]
Using Fact 5, we further have that the sampled distribution \( \hat{Z}^{a+1} \hat{Y}^{a+1} \hat{F} \hat{X}^{a+1} \hat{S} \) satisfies
\[
\|\hat{Z}^{a+1} \hat{Y}^{a+1} \hat{F} \hat{X}^{a+1} \hat{S}\|_1 \leq O((a + 1\epsilon') + 4\epsilon).
\]
From Claim 8, we have \( \|Z^a - U_{2h}\|_1 \leq O(a\epsilon') \). From Algorithms 1, 2, 3, we have \( Z^a Y^a_2 X^a_2 X^a_1 \) and \( Y^a_2 \otimes X^a_1 \). Thus, we have
\[
\|Z^a Y^a_2 X^a_1 X^a_2 - 2h \otimes U_{2h} \otimes U_{n_{2h}} \otimes U_{4n_{2h} + n_{2h}}\|_1 \leq O(a\epsilon')
\]
Proceed flip-flop procedure with \( \hat{Z}^a X^a_1 X^a_2 Y^a_1 Y^a_2 = U_{2h} \otimes U_{4n_{2h} + n_{2h}} \otimes U_{2h} \otimes U_{n_{2h}} \otimes U_{4n_{2h} + n_{2h}} \) and denote intermediate random variables as hat variables. Using Fact 5 and Eq. (34), we have
\[
\|Z^a Y^a_2 X^a_1 X^a_2 A^a C^a B^a Z^a - Z^a Y^a_2 X^a_1 X^a_2 A^a C^a B^a Z^a\|_1 \leq O(a\epsilon')
\]
Using Fact 5, we further can sample from a distribution arguments involving Corollary 1, Claim 3, Claim 2 like before (in this proof), we can sample from a distribution \( Z^a Y_1 Y_2 X_1 X_2 A^a C^a B^a Z^a \) such that
\[
\| \hat{Z}^a Y_1 Y_2 X_1 X_2 A^a C^a B^a \hat{Z}^a \|_1 \leq O(\varepsilon'). \tag{37}
\]
Using Eq. (37) along with Fact 5 we have,
\[
\| \hat{Z} - U_{2h} \|_1 \leq O(\varepsilon'). \tag{38}
\]
From Eqs. (35), (37) and triangle inequality, we have
\[
\| Z^a Y_1 Y_2 X_1 X_2 A^a C^a B^a Z^a - \hat{Z}^a Y_1 Y_2 X_1 X_2 A^a C^a B^a \hat{Z}^a \|_1 \leq O((a + 1)\varepsilon'). \tag{39}
\]
Using Fact 5, we further can sample from a distribution \( Z^a Y_1 Y_2 X_1 X_2 Z^a \) such that
\[
\| Z^a Y_1 Y_2 X_1 X_2 Z^a - \hat{Z}^a Y_1 Y_2 X_1 X_2 \hat{Z}^a \|_1 \leq O((a + 1)\varepsilon'). \tag{40}
\]
Claim 8: Let \( 2n \text{Ext} : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^{n/4} \) be the new-2nExt from Algorithm 1. Let \( XY = U_n \otimes U_n \), \( S = 2n \text{Ext}(X, Y) \) and set
\[
P \triangleq \{ G, Z^a, A^a, B^a, C^a, \bar{Z}^a, \bar{A}^a, \bar{B}^a, \bar{C}^a, Z^{a+1} \}
\]
be the intermediate random variables as defined in Algorithms 1, 2, 3. Then, we have for any random variable \( Q \in P \setminus \{ G \} \) and any fixing \( G = g \),
\[
\| Q(G = g) - U_{Q|G} \|_1 \leq O(a\varepsilon').
\]
Proof: From Claim 6, we have
\[
G X_3 Y_3 X^{[a+1]} Y^{[a+1]} = G \otimes X_3 Y_3 X^{[a+1]} Y^{[a+1]},
\]
where \( X = X_1 \circ X_3 \circ X^{[a+1]} \circ X^{[a+2, 3a]} \) and \( Y = Y_1 \circ Y_3 \circ Y^{[a+1]} \circ Y^{[a+2, 3a]} \). Also, from Algorithms 1, 2, 3, any random variable \( Q \in P \setminus \{ G \} \) is extracted from sources \( X_3 Y_3 X^{[a+1]} Y^{[a+1]} \). Note for any \( i \in [a] \) and \( i \)-th flip-flop procedure (Algorithm 3), intermediate random variables \( \{ A^i, B^i, C^i, \bar{Z}^i, A^{i+1}, B^{i+1}, C^{i+1}, Z^{i+1} \} \) are extracted from \( X^{i+1} Y^{i+1} Z^i = X^i \otimes Y^i \otimes Z^i \). We remove conditioning on \( G = g \) for the random variables for the rest of the proof.

Since \( Z^i = IP(X_3, Y_3) \), using Fact 15 we have
\[
\| Z^i - U_{2h} \|_1 \leq 2^{-2(n)} \leq \varepsilon'.
\]
We show if for any round \( i \), \( \| Z^i - U_{2h} \|_1 \leq O(i\varepsilon') \), then for any \( Q \in \{ A^i, B^i, C^i, \bar{Z}^i, A^{i+1}, B^{i+1}, C^{i+1}, Z^{i+1} \} \) we have \( \| Q - U_{Q|Z} \|_1 \leq O((i + 2)\varepsilon') \).

We denote generated intermediate random variables \( A^i, B^i, C^i, \bar{Z}^i \) from \( \hat{Z}^i = Z_1 Z_2 = U_{2h} \) (instead of \( Z^i \)) as respective hat random variables. Using Fact 5 repeatedly, we have
\[
\| X_1 X_2 Y_1 Y_2 Z^i A^i B^i C^i \hat{Z}^i - X_1 X_2 Y_1 Y_2 Z^i A^i B^i C^i \hat{Z}^i \|_1 \leq O(i\varepsilon'). \tag{41}
\]
Since \( \hat{A}^i = \text{Ext}_1(Y_1^i, \hat{Z}^i), Y_1^i \hat{Z}^i = U_{n y} \otimes U_n \), using Corollary 1 we have
\[
\| \hat{A}^i - U_{h} \|_1 \leq \varepsilon'. \tag{42}
\]
Since \( \hat{C}^i = \text{Ext}_2(\hat{Z}^i, \hat{A}^i), \hat{Z}^i \hat{A}^i = U_{h} \otimes \hat{A}^i \) and \( \| \hat{A}^i - U_{h} \|_1 \leq \varepsilon' \), using Corollary 1 we have
\[
\| \hat{C}^i - U_{h} \|_1 \leq 2\varepsilon'. \tag{43}
\]
Since \( \hat{B}^i = \text{Ext}_1(Y_2^i, \hat{C}^i), Y_2^i \hat{C}^i = U_{n y} \otimes \hat{C}^i \) and \( \| \hat{C}^i - U_{h} \|_1 \leq 2\varepsilon' \), using Corollary 1 we have
\[
\| \hat{B}^i - U_{h} \|_1 \leq 3\varepsilon'. \tag{44}
\]
If \( g_i = 1 \), we have \( \hat{Z}^i = \text{Ext}_1(X_1^i, \hat{B}^i), X_1^i \hat{B}^i = U_{n y} \otimes \hat{B}^i \) and \( \| \hat{B}^i - U_{h} \|_1 \leq 3\varepsilon' \). Using Corollary 1, we further have
\[
\| \hat{Z}^i - U_{2h} \|_1 \leq 4\varepsilon'. \tag{45}
\]
Similarly, if \( g_i = 0 \), we will have
\[
\| \hat{Z}^i - U_{2h} \|_1 \leq 2\varepsilon'. \tag{46}
\]
Using Fact 5, Eqs. (41), (42), (43), (44), (45) and (46) along with appropriate triangle inequalities, for any \( Q \in \{ A^i, B^i, C^i, \hat{Z}^i \} \) we have \( \| Q - U_{Q|Z} \|_1 \leq O((i + 1)\varepsilon') \). Using
similar arguments and noting $X^i_1X^i_2Y^i_1Z^i = X^i_3X^i_4Y^i_3Z^i$, one can note for any $Q \in \{A^i, B^i, C^i, Z^i+1\}$ we have $\|Q - U_{ij}\| \leq O(i + 2)^{\epsilon'}$. Thus, since we have $a$ rounds of flip-flop procedure, the desired follows from induction argument. □

V. A QUANTUM SECURE NON-MALLEABLE SECRET SHARING SCHEME

Secret sharing is a fundamental primitive in cryptography where a dealer encodes a secret/message into shares and distributes among many parties. Only the authorized subsets of parties should be able to recover the initial secret. Most well known secret sharing schemes are the so called $t$-out-of-$n$ secret sharing schemes where at least $t$ parties are required to decode the secret [18], [19]. In this paper, we focus only on 2-out-of-2 secret sharing schemes.

Recently non-malleable secret sharing schemes are introduced by Goyal and Kumar [20] with the additional guarantee that when the adversary tampers with possibly all the shares of the secret independently, then the reconstruction procedure outputs original secret or something that is unrelated to the original secret.

In this paper, in addition, we allow the adversary to make use of arbitrary entanglement to tamper the shares. We then require the reconstruction procedure to output original secret or something that is unrelated to the original secret. We call such secret sharing schemes as quantum secure non-malleable secret sharing schemes. We show that quantum secure non-malleable codes in the split-state model gives rise to quantum secure 2-out-of-2 non-malleable secret sharing schemes.

We consider an encoding and decoding scheme $(\text{Enc}, \text{Dec})$ where $\text{Enc}(S) = (X, Y)$. Here $S \sim U_m$ ($U_m$ is uniform distribution on $m$ bits) represents the secret/message and $X, Y \in \{0, 1\}^m$ are the two shares/parts of the codeword. Enc is a randomized function and $\text{Dec}(X, Y)$ is a deterministic function, such that $\Pr(\text{Dec}(\text{Enc}(S)) = S) = 1$. Let $\mathcal{F}$ denote the set of all functions $f : \{0, 1\}^m \rightarrow \{0, 1\}^m$.

Definition 12 (2-Out-of-2 Non-Malleable Secret Sharing Scheme [20]): $(\text{Enc}, \text{Dec})$ is an $(m, n, \varepsilon_1, \varepsilon_2)$-2-out-of-2 non-malleable secret sharing scheme, if

- **statistical privacy:** for any two secrets $s_1, s_2 \in \{0, 1\}^m$, it holds that

  $$\|X_{s_1} - X_{s_2}\| \leq \varepsilon_1 \quad \|Y_{s_1} - Y_{s_2}\| \leq \varepsilon_1,$$

  where $(X_{s_1}, Y_{s_1}) = \text{Enc}(s_1)$ and $(X_{s_2}, Y_{s_2}) = \text{Enc}(s_2)$.

- **non-malleability:** for every $f = (g_1, g_2) \in \mathcal{F} \times \mathcal{F}$, there exists a random variable $D_f = \mathcal{D}(g_1, g_2)$ on $\{0, 1\}^m \cup \{\text{same}\}$ which is independent of the randomness in $\text{Enc}$ such that for all secrets $s \in \{0, 1\}^m$, it holds that

  $$\|F(f(\text{Enc}(s))) - \text{copy}(D_f, s)\| \leq \varepsilon_2,$$

  where the function $\text{copy}(x, s)$ is such that $\text{copy}(x, s) = s$ if $x = \text{same}$, otherwise $\text{copy}(x, s) = x$.

Definition 13 (Quantum Secure 2-Out-of-2 Non-Malleable Secret Sharing Scheme): $(\text{Enc}, \text{Dec})$ is an $(m, n, \varepsilon_1, \varepsilon_2)$-quantum secure 2-out-of-2 non-malleable secret sharing scheme, if

- **statistical privacy:** is as defined in Definition 12

- **non-malleability:** for state $\rho$ and adversary $A = (U, V)$ as defined in Definition 2, there exists a random variable $\mathcal{D}_A$ on $\{0, 1\}^m \cup \{\text{same}\}$ such that

  $$\forall s \in \{0, 1\}^m : \|S'_{s} - \text{copy}(\mathcal{D}_A, s)\| \leq \varepsilon_2.$$

Above $S' = \text{Dec}(X', Y')$, $S_{s}' = (S_{s}'|S = s)$ and the function copy is as defined in Definition 12.

Fact 23 (Lemma 6.1 in [36]): Let $(\text{Enc}, \text{Dec})$ be an $(m, n, \varepsilon)$-non-malleable code in the split-state model. Then, for any two messages $u, v \in \{0, 1\}^m$, it holds that

$$\|X_u - X_v\| \leq 2\varepsilon \quad \|Y_u - Y_v\| \leq 2\varepsilon,$$

where $(X_u, Y_u) = \text{Enc}(u)$ and $(X_v, Y_v) = \text{Enc}(v)$.

Remark: Since a quantum secure non-malleable code is also a classical non-malleable code in the split-state model, the above fact also applies for quantum secure non-malleable code in the split-state model.

Corollary 3: Let $(\text{Enc}, \text{Dec})$ be an $(m, n, \varepsilon)$-quantum secure non-malleable code in the split-state model. Then, $(\text{Enc}, \text{Dec})$ is also an $(m, n, 2\varepsilon')$-secure 2-out-of-2 non-malleable secret sharing scheme.

Proof: Statistical privacy follows from the Fact 23. Non-malleability property follows from the Definition 3 of quantum secure non-malleable code in the split-state model. □

APPENDIX A

A QUANTUM SECURE ONE-MANY NON-MALLEABLE CODE IN THE SPLIT-STATE MODEL

A. Preliminaries for Quantum Secure One-Many Non-Malleable Code in the Split-State Model

Let $m, n, k, t$ be positive integers and $\varepsilon, \varepsilon' > 0$. Let $\mathcal{F}$ denote the set of all the functions from $\{0, 1\}^m \rightarrow \{0, 1\}^n$. We next define $\text{copy}^{(i)} : \{0, 1\}^i \cup \{\text{same}\}^i \times \{0, 1\}^i \rightarrow \{0, 1\}^i$ where the first input is a $t$-tuple as follows: $\text{copy}^{(i)}((x_1, x_2, \ldots, x_t), s) = (\text{copy}(x_1, s), \text{copy}(x_2, s), \ldots, \text{copy}(x_t, s))$. Recall the function copy : $\{0, 1\}^i \cup \{\text{same}\} \times \{0, 1\}^i \rightarrow \{0, 1\}^i$ such that $\text{copy}(x, s) = s$ if $x = \text{same}$, otherwise $\text{copy}(x, s) = x$.

Definition 14 (One-Many Non-Malleable Codes in the Split-State Model [6]): An encoding and decoding scheme $(\text{Enc}, \text{Dec})$ is a $(t; m, n, \varepsilon)$-non-malleable code with respect to a family of tampering functions $(\mathcal{F} \times \mathcal{F})^t$, if for every

$$f = ((g_1, h_1), (g_2, h_2), \ldots, (g_t, h_t)) \in (\mathcal{F} \times \mathcal{F})^t,$$

there exists a random variable $D_f = \mathcal{D}(g_1, g_2, \ldots, g_t, h_t)$ on $\{0, 1\}^m \cup \{\text{same}\}$ which is independent of the randomness in $\text{Enc}$ such that for all messages $s \in \{0, 1\}^m$, it holds that

$$\|\text{Dec}((g_1, h_1)(\text{Enc}(s))) \ldots \text{Dec}((g_t, h_t)(\text{Enc}(s))) - \text{copy}^{(i)}(D_f, s)\| \leq \varepsilon.$$

Definition 15 ($t: (k_1, k_2)$-qnm-state [2]): Let $\sigma_{X^{k_1}X^{k_2}N^{XY}}$ be a $(k_1, k_2)$-qna-state. Let $U : \mathcal{H}_X \otimes \mathcal{H}_N \rightarrow \mathcal{H}_X \otimes \mathcal{H}_{X^{(i)} \otimes \mathcal{H}}$.
Claim 9: Let \( \sigma_{X}^{N} \) be a \((k_1, k_2)\)-qpa-state with \( |X| = n \) and \( |Y| = n \). Let \( U : H_X \otimes H_Y \rightarrow H_{X'} \otimes H_{Y'} \) be isometries such that for \( \rho = \rho(S^{i}) \| \psi \rangle \) we have \( X'[i][Y'] \) classical (with copies \( X'[i][Y'] \)) respectively and for every \( i \in [t] \) either \( \operatorname{Pr}(X \neq X') \rho = 1 \) or \( \operatorname{Pr}(Y \neq Y') \rho = 1 \).

The desired now follows by noting \( \sigma_{X}^{N} \) is a \((k_1, k_2)\)-quantum secure \( 2\)-source \( n\)-malleable extractor. Then, \( t\)-2mExt is also a \((j; k_1, k_2)\)-quantum secure \( 2\)-source \( j\)-non-malleable extractor for any positive integer \( j \leq t \).

Proof: Let \( \sigma_{X}^{N} \) be a \((k_1, k_2)\)-qpa-state with \( |X| = n \) and \( |Y| = n \). Let \( U : H_X \otimes H_Y \rightarrow H_{X'} \otimes H_{Y'} \) be isometries such that for \( \rho = \rho(S^{i}) \| \psi \rangle \) we have \( X'[i][Y'] \) classical (with copies \( X'[i][Y'] \)) respectively and for every \( i \in [t] \) either \( \operatorname{Pr}(X \neq X') \rho = 1 \) or \( \operatorname{Pr}(Y \neq Y') \rho = 1 \). Notice the state \( \rho \) is a \((j; k_1, k_2)\)-qnm-state.

Let \( U' : H_X \otimes H_Y \rightarrow H_{X'} \otimes H_{Y'} \), \( V' : H_Y \otimes H_M \rightarrow H_{Y'} \otimes H_{M'} \). Let \( \hat{\rho} = U'(U \otimes V') \| \psi \rangle \) and \( \rho' = U(\hat{\rho}) \). Let \( \sigma_{X}^{N} \) be a \((k_1, k_2)\)-qpa-state with \( |X| = n \) and \( |Y| = n \). Let \( U : H_X \otimes H_Y \rightarrow H_{X'} \otimes H_{Y'} \) be isometries such that for \( \rho = \rho(S^{i}) \| \psi \rangle \) we have \( X'[i][Y'] \) classical (with copies \( X'[i][Y'] \)) respectively and for every \( i \in [t] \) either \( \operatorname{Pr}(X \neq X') \rho = 1 \) or \( \operatorname{Pr}(Y \neq Y') \rho = 1 \). Notice the state \( \rho \) is a \((j; k_1, k_2)\)-qnm-state. Then, \( t\)-2mExt is a \((t; k_1, k_2)\)-quantum secure (Definition 16), we have

\[
\| \rho_{SS^{i}YY^{i}M} - U_m \otimes \rho_{SS^{i}YY^{i}M} \| \leq \varepsilon.
\]

where \( S^{i} \) is \( t\)-2mExt \((X'[i][Y']\) Using Fact 5, we get
\[
\| \rho_{SY} - U_m \otimes \rho_{Y} \| \leq \varepsilon.
\]
Let $\rho'$ be the final pure state after we generate $t$-bit classical registers $C, D$ (with copies $\hat{C}, \hat{D}$ respectively) such that $C_i = 1$ indicates $X_{i} \neq X_i$ in state $\rho'$ and $D_i = 1$ indicates $Y_i \neq Y_i$ in state $\rho'$ for every $i \in [t]$.

Using similar arguments as in Theorem 5, one can note that the state $\rho'$ is an $(n, n)$-qpa-state. For $C = c \in \{0, 1\}^t, D = d \in \{0, 1\}^t$, denote $S_{c,d} = \{i \in [t] : (c_i = 1) \lor (d_i = 1)\}$ and $\rho_{c,d}^{S_{c,d}} = \rho'|(C, D) = (c, d)\).

For every $c, d \in \{0, 1\}^t$, let $D_{A,c,d} = D_{A,c,d}(U, V, \psi) = (D_{A;1}^{c,d}, \ldots, D_{A,t}^{c,d})$, where $D_{A; j}^{c,d} = \rho_{c,d}^{t-2nmExt(X_j, Y_j)}$ for $j \in S_{c,d}$. Let $D_{A,c,d}$ be the distribution that is deterministically equal to same otherwise. Let $D_A = \sum_{c,d \in \{0, 1\}^t}Pr((C, D) = (c, d))_{\rho'}$ depend only on $(U, V, \psi)$. Note for every $c, d \in \{0, 1\}^t$, the value $Pr((C, D) = (c, d))_{\rho'}$ depends only on $(U, V, \psi)$. Note

$$
\rho_{S_{c,d}}^{t-2nmExt} = \sum_{c,d \in \{0, 1\}^t}Pr((C, D) = (c, d))_{\rho'}\rho_{c,d}^{S_{c,d}}, \quad \text{(47)}
$$

and

$$
Z_{copy}(D_A, Z) = \sum_{c,d \in \{0, 1\}^t}Pr((C, D) = (c, d))_{\rho'}Z_{copy}(D_{A,c,d}, Z), \quad \text{(48)}
$$

where $Z = U_m$.

Claim 11: For every $c, d \in \{0, 1\}^t$, we have

$$
Pr((C, D) = (c, d))_{\rho'}\|\rho_{S_{c,d}}^{t-2nmExt} - Z_{copy}(D_{A,c,d}, Z)\|_1 \leq 2^{-k} + \epsilon,
$$

where $Z = U_m$.

Proof: Fix $c, d \in \{0, 1\}^t$. Suppose $Pr((C, D) = (c, d))_{\rho'} \leq 2^{-k}$, then we are done. Thus we assume otherwise. Note $S_{c,d}$ is empty only when $(c, d) = (0^t, 0^t)$.

First let $S_{c,d} = \{i_1, \ldots, i_j\}$ be non-empty. Using arguments similar to Claim 4 involving Fact 17 and noting that state $\rho'$ is an $(n, n)$-qpa-state, we get that $\rho_{c,d}^{S_{c,d}}$ is a $(j; n - k, n - k, \epsilon)$-qnm-state. Using Claim 10 to note $t-2nmExt$ is also $(j; n - k, n - k, \epsilon)$-qnm-secure for any positive integer $j \leq t$ and using Fact 5, we have

$$
\|\rho_{S_{c,d}}^{t-2nmExt} - U_m \otimes \rho_{S_{c,d}}^{t-2nmExt} \otimes Z_{copy}(D_{A,c,d}, Z)\|_1 \leq \epsilon. \quad \text{(49)}
$$

For any $p \in [t] \setminus S_{c,d}$, we have $\rho_{S_{c,d}}^{t-2nmExt} = \rho_{S_{p}}^{t-2nmExt}$. Thus from Eq. (49) and using Fact 5, we have

$$
\|\rho_{S_{c,d}}^{t-2nmExt} - Z_{copy}(D_{A,c,d}, Z)\|_1 \leq \epsilon.
$$

For $(c, d) = (0^t, 0^t)$, the proof follows noting $\rho_{c,d}^{S_{c,d}}$ is an $(n - k, n - k)$-qpa-state and using Claim 9 along with Fact 5. □

Consider,

$$
\|\rho_{S_{c,d}}^{t-2nmExt} - Z_{copy}(D_{A,c,d}, Z)\|_1
= \|\sum_{c,d \in \{0, 1\}^t}Pr((C, D) = (c, d))_{\rho'}\rho_{S_{c,d}}^{t-2nmExt} - Z_{copy}(D_{A,c,d}, Z)\|_1
\leq \sum_{c,d \in \{0, 1\}^t}Pr((C, D) = (c, d))_{\rho'}\|\rho_{S_{c,d}}^{t-2nmExt} - Z_{copy}(D_{A,c,d}, Z)\|_1
\leq (2^{-k} + \epsilon)2^t.
$$

The first equality follows from Eq. (47), the first inequality follows from Eq. (48) and Fact 7 and the second inequality follows from Claim 11. This completes the proof. □

B. A Quantum Secure Modified 2-Source t-Non-Malleable Extractor

We modify the construction of $t$-2nmExt from [2], using ideas from [6] to construct a new $t$-2nmExt : $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^m$ that is $(n - n_1, n - n_1, O(\epsilon))$-secure against qnm-adv for parameters $n_1 = n^{\Omega(1)}, m = n^{1 - \Omega(1)}, t = n^{\Omega(1)}$ and $\epsilon = 2^{-n^{\Omega(1)}}$. 

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
Algorithm 4: new-t-2nmExt : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^{n/4t}

**Input:** X, Y

1) Advice generator:

\[ X_1 = \text{Cryp}(X, 1, 3n_1) \quad ; \quad Y_1 = \text{Cryp}(Y, 1, 3n_1) \quad ; \quad R = \text{IP}(X_1, Y_1) \quad ; \]
\[ X_2 = \text{Cryp}(X, 3n_1 + 1, n) \quad ; \quad Y_2 = \text{Cryp}(Y, 3n_1 + 1, n) \quad ; \]
\[ G = X_1 \circ \tilde{X}_2 \circ Y_1 \circ \tilde{Y}_2 = X_1 \circ \text{ECC}(X_2 \circ \text{Samp}(R)) \circ Y_1 \circ \text{ECC}(Y_2 \circ \text{Samp}(R)) \]

2) \[ X_3 = \text{Cryp}(X, 3n_1 + 1, 3n_1 + n_6) \quad ; \quad Y_3 = \text{Cryp}(Y, 3n_1 + 1, 3n_1 + n_6) \quad ; \quad Z^1 = \text{IP}(X_3, Y_3) \]
3) \[ X_4 = \text{Cryp}(X, 3n_1 + n_6 + 1, n) \quad ; \quad Y_4 = \text{Cryp}(Y, 3n_1 + n_6 + 1, n) \]
4) Correlation breaker with advice: \[ F = 2\text{AdvCB}(Y_4, X_4, Z^1, G) \]
5) \[ X_5 = \text{Cryp}(X_4, 4n_xa + 1, 4n_xa + 4n_x) \]
6) \[ S = \text{Extr}(X_5, F) \]

**Output:** S

---

1) **Parameters:** Let \( \delta, \delta_1, \delta_2, \delta_3 > 0 \) be small enough constants such that \( \delta_1 < \delta_2 \). Let \( n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_x, n_y, a, b, h, t \) be positive integers and \( \varepsilon', \varepsilon > 0 \) such that:

\[ n_1 = n^{\delta_2} \quad ; \quad n_2 = n - 3n_1 \quad ; \quad q = 2^{\log(n+1)} \quad ; \quad \varepsilon = 2^{-\Theta(n^{\delta_1})} \quad ; \quad n_3 = n^{1/10} \quad ; \quad n_4 = \frac{n_2}{\log(n+1)} \quad ; \quad n_5 = n^{3/2} \quad ; \quad n_6 = 3n_4^3 \quad ; \quad n_7 = n - 3n_1 - n_6 \quad ; \quad n_x = \frac{n_7}{12a} \quad ; \quad n_y = \frac{n_7}{12a} \quad ; \quad 2^{\Theta(n)} \sqrt{\varepsilon'} = \varepsilon \]

\[ s = \Theta \left( \log^2 \left( \frac{n}{\varepsilon'} \right) \log n \right) \quad ; \quad \rho = \Theta \left( \log^2 \left( \frac{n}{\varepsilon'} \right) \log n \right) \quad ; \quad t \leq n^{\delta_3} \quad ; \quad h = 10ts \]

- \( \text{IP}_1 \) be \( \text{IP}_{3n_1/n} \)
- \( \text{Ext}_1 \) be \( (2h, \varepsilon') \)-quantum secure \( (n_y, s, b) \)-extractor,
- \( \text{Ext}_2 \) be \( (2s, \varepsilon') \)-quantum secure \( (h, b, s) \)-extractor,
- \( \text{Ext}_3 \) be \( (4h, \varepsilon') \)-quantum secure \( (n_x, b, 2h) \)-extractor,
- \( \text{Ext}_4 \) be \( (n_y/4t, \varepsilon^2) \)-quantum secure \( (4n_y, 2h, n_y/8t) \)-extractor,
- \( \text{IP}_2 \) be \( \text{IP}_{3n_1/2h} \)
- \( \text{Ext}_6 \) be \( (n_x/2, \varepsilon^2) \)-quantum secure \( (4n_x, n_y/8t, n_x/4t) \)-extractor.

2) **Definition of 2-Source t-Non-Malleable Extractor:** The following theorem shows that the function new-t-2nmExt as defined in Algorithm 4 is \( \langle t; n - n_1, n - n_1, \Omega(\varepsilon) \rangle \)-secure against qnm-adv by noting that \( S = \text{new-t-2nmExt}(X, Y) \) and \( S^i = \text{new-t-2nmExt}(X^i, Y^i) \) for every \( i \in [t] \). Note that 2AdvCB in Algorithm 4 is same as the one in Algorithm 2 except for parameters and extractors which are to be used as mentioned in this section.

**Theorem 9 (Security of new-t-2nmExt):** Let \( \rho_{XX^i|\tilde{X}^i} \circ YY^i|\tilde{Y}^i \mid M \) be a \( \langle t; n - n_1, n - n_1 \rangle \)-qnm-state. Then,

\[ ||\rho_{SS^i|\tilde{Y}^i}\mid M - U_{n/4t} \otimes \rho_{SS^i|YY^i}\mid M||_1 \leq O(\varepsilon). \]

---

**Proof:** The proof proceeds in similar lines to the proof of Theorem 9 in [2] using Fact 21 for alternating extraction argument, Fact 22 for bounding the min-entropy required in alternating extraction and Facts 14, 19 for the security of inner-product function in \((k_1, k_2)\)-qpa-state framework, Fact 4 for relation between \( \Delta_B, \Delta \) and we do not repeat it.

---

**REFERENCES**

[1] S. Dziembowski, K. Pietrzak, and D. Wichs, “Non-malleable codes,” J. ACM, vol. 65, no. 4, pp. 1–32. Apr. 2018.
[2] N. G. Boddu, R. Jain, and U. Kapshikar, “Quantum secure non-malleable-extractors,” in Proc. Contributed Talk 17th Conf. Theory Quantum Comput., Commun. Cryptogr., 2022.
[3] M. Cheraghchi and V. Guruswami, “Capacity of non-malleable codes,” IEEE Trans. Inf. Theory, vol. 62, no. 3, pp. 1097–1118, Mar. 2016.

[4] F.-H. Liu and A. Lysyanskaya, “Tamper and leakage resilience in the split-state model,” in Advances in Cryptology—CRYPTO, R. Safavi-Naini and R. Canetti, Eds. Berlin, Germany: Springer, 2012, pp. 517–532.

[5] S. Dziembowski, T. Kazana, and M. Obremski, “Non-malleable codes from two-source extractors,” in Advances in Cryptology—CRYPTO, R. Canetti and J. A. Garay, Eds. Berlin, Germany: Springer, 2013, pp. 239–257.

[6] E. Chattopadhyay, V. Goyal, and X. Li, “Nonmalleable extractors and codes, with their many tampered extensions,” SIAM J. Comput., vol. 49, no. 5, pp. 999–1040, Jan. 2020.

[7] M. Cheraghchi and V. Guruswami, “Non-malleable coding against bit-wise and split-state tampering,” in Proc. Theory Cryptog. Conf. (TCC), 2014, pp. 440–464.

[8] D. Aggarwal, Y. Dodis, and S. Lovett, “Non-malleable codes from additive combinatorics,” SIAM J. Comput., vol. 47, no. 2, pp. 524–546, Jan. 2018.

[9] D. Aggarwal, “Affine-evasive sets modulo a prime,” Inf. Process. Lett., vol. 115, no. 2, pp. 382–385, Feb. 2015.

[10] X. Li, “Three-source extractors for polylogarithmic min-entropy,” in Proc. IEEE 56th Ann. Symp. Found. Comput. Sci., Oct. 2015, pp. 863–882.

[11] D. Aggarwal and J. Böttger, “Revisiting the Sanders-Bogolyubov-Ruzsa theorem in $F_p$ and its application to non-malleable codes,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jul. 2016, pp. 1322–1326.

[12] X. Li, “Improved non-malleable extractors, non-malleable codes and independent source extractors,” in Proc. 49th Ann. ACM SIGACT Symp. Theory Comput. (STOC). New York, NY, USA: Association for Computing Machinery, 2017, pp. 1144–1156.

[13] X. Li, “Non-malleable extractors and non-malleable codes: Partially optimal constructions,” in Proc. 34th Comput. Complex. Conf. (CCC). Wadern, Germany: Dagstuhl, DEU, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2019, vol. 137, pp. 28:1–28:49.

[14] D. Aggarwal and M. Obremski, “A constant rate non-malleable code in the split-state model,” in Proc. IEEE 61st Ann. Symp. Found. Comput. Sci. (FOCS), Los Alamitos, CA, USA, Nov. 2020, pp. 1285–1294.

[15] D. Aggarwal, B. Kunakurthi, S. L. B. Obbattu, M. Obremski, and S. Sekar, “Rate one-third non-malleable codes,” in Proc. 54th Ann. ACM SIGACT Symp. Theory Comput. (STOC). New York, NY, USA: Association for Computing Machinery, 2022, pp. 1364–1377.

[16] J. S. Bell, “On the Einstein podolsky rosen paradox,” Phys. Phys. Fizika, vol. 1, pp. 195–200, Nov. 1964.

[17] C. H. Bennett and S. J. Wiesner, “Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states,” Phys. Rev. Lett., vol. 69, no. 20, pp. 2881–2884, Nov. 1992.

[18] G. R. Blakley, “Safeguarding cryptographic keys,” in Proc. Int. Workshop Manag. Requirements Knowl. (MARK), Mar. 1979, pp. 313–318.

[19] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[20] V. Goyal and A. Kumar, “Non-malleable secret sharing,” in Proc. 50th Ann. ACM SIGACT Symp. Theory Comput. (STOC). New York, NY, USA, Jun. 2018, pp. 685–698.

[21] V. Goyal, O. Pandey, and S. Richelson, “Textbook non-malleable commitments,” in Proc. 49th Ann. ACM SIGP Symp. Theory Comput. (STOC). New York, NY, USA: Association for Computing Machinery, 2016, pp. 1128–1141.

[22] V. Goyal and A. Kumar, “Non-malleable secret sharing for general access structures,” in Advances in Cryptology—CRYPTO 2018, H. Shacham and A. Boldyreva, Eds. Cham, Switzerland: Springer, 2018, pp. 501–530.

[23] D. Aggarwal et al., “Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures,” in Advances in Cryptology—CRYPTO 2019, A. Boldyreva and D. Micciancio, Eds. Cham, Switzerland: Springer, 2019, pp. 510–539.

[24] A. Srinivasan and P. N. Vasudevan, “Leakage resilient secret sharing and applications,” in Advances in Cryptology—CRYPTO 2019, A. Boldyreva and D. Micciancio, Eds. Cham, Switzerland: Springer, 2019, pp. 480–509.

[25] D. Aggarwal, N. G. Boddu, R. Jain, and M. Obremski, “Quantum measurement adversary,” IEEE Trans. Inf. Theory, early access, Sep. 8, 2023, doi: 10.1109/TIT.2023.33513149.

[26] R. Kasher and J. Kempe, “Two-source extractors secure against quantum adversaries,” in Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, M. Serna, R. Shaltiel, K. Jansen, and J. Rolim, Eds. Berlin, Germany: Springer, 2010, pp. 656–669.

[27] K. Chung, X. Li, and X. Wu, “Multi-source randomness extractors against quantum side information, and their applications,” 2014, arXiv:1411.2315.

[28] R. Amon-Friedman, C. Portmann, and V. B. Scholz, “Quantum-proof multi-source randomness extractors in the Markov model,” in Proc. 11th Conf. Theory Quantum Comput., Commun. Cryptogr. (TQC), vol. 61, A. Broadbent, Ed. Dagstuhl, Germany: Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016, pp. 2:1–2:34.

[29] A. De, C. Portmann, T. Vidick, and R. Renner, “Trevisan’s extractor in the presence of quantum side information,” SIAM J. Comput., vol. 41, no. 4, pp. 915–940, Jan. 2012.

[30] N. Datta, “Min- and max-relative entropies and a new entanglement monotone,” IEEE Trans. Inf. Theory, vol. 55, no. 6, pp. 2816–2826, Jun. 2009.

[31] R. Jain, J. Radhakrishnan, and P. Sen, “Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states,” in Proc. 43rd Ann. IEEE Symp. Found. Comput. Sci., Nov. 2002, pp. 429–438.

[32] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[33] J. Watrous, “Naimark’s theorem; characterizations of channels,” Theory Quantum Inf., Lect. Notes, 2011, ch. 5.

[34] A. Uhligmann, “The transition probability in the state space of a*-algebra,” Rep. Math. Phys., vol. 9, pp. 273–279, Apr. 1976.

[35] C. A. Fuchs and J. van de Graaf, “Cryptographic distinguishability measures for quantum-mechanical states,” IEEE Trans. Inf. Theory, vol. 45, no. 4, pp. 1216–1227, May 1999.

[36] D. Aggarwal, S. Dziembowski, T. Kazana, and M. Obremski, “Leakage-resilient non-malleable codes,” in Theory of Cryptography, Y. Dodis and J. B. Nielsen, Eds. Berlin, Germany: Springer, 2015, pp. 398–426.

Divesh Aggarwal received the Ph.D. degree from the Swiss Federal Institute of Technology Zürich (ETH Zürich) in 2012. He is currently an Associate Professor with the Department of Computer Science and a Principal Investigator with the Centre for Quantum Technologies, National University of Singapore. Before joining the National University of Singapore, he was a Post-Doctoral Researcher for two years with the Swiss Federal Institute of Technology Lausanne (EPFL) and New York University. His research interests are in information-theoretic cryptography, algorithms, computational complexity, and coding theory.

Naresh Goud Boddu received the Ph.D. degree from the Centre for Quantum Technologies, National University of Singapore, in 2022. He is currently a Post-Doctoral Research Fellow with the Cryptography and Information Security Laboratory, NTT Research, Sunnyvale, USA. His research interests are in quantum information-theoretic cryptography and complexity theory.

Rahul Jain received the Ph.D. degree in computer science from TIFR, India, in 2003. He was a Research Fellow with UC Berkeley, USA, followed by IQC, University of Waterloo, Canada. He joined the Centre for Quantum Technologies (CQT) as a Principal Investigator (PI) and the Computer Science (CS) Department, National University of Singapore (NUS), Singapore, as an Assistant Professor in 2008, where he is currently a Professor with the CS Department and a PI with CQT. His research interests are in the areas of quantum and classical information theory, cryptography, and complexity theory.