Quantum Measurement Adversary

Divesh Aggarwal, Naresh Goud Boddu, Rahul Jain, and Maciej Obrenski

Abstract—Multi-source extractors are functions that extract uniform randomness from multiple (weak) sources of randomness. Quantum multi-source extractors were considered by Kasher and Kempe (2010) (for the quantum independent adversary and the quantum bounded storage adversary), Chung et al. (2014) (for the general entangled adversary) and Arnon-Friedman et al. (2016) (for the quantum Markov adversary). One of the main objectives of this work is to unify all the existing quantum multi-source adversary models. We propose two new models of adversaries: 1) the quantum measurement adversary (qma), which generates side information using entanglement and on post-measurement; and 2) the quantum communication adversary (qca), which generates side information using entanglement and communication between multiple sources. We show that: 1) qma is the strongest adversary among all the known adversaries, in the sense that the side information of all other adversaries can be generated by qma; 2) The (generalized) inner-product function (in fact a general class of two-wise independent functions) continues to work as a good extractor with matching parameters as that of Chor and Goldreich (1985) against classical adversaries; 3) A non-malleable extractor proposed by Li (2012) (against classical adversaries) continues to be secure against quantum side information. This result implies a non-malleable extractor result of Aggarwal et al. (2019) with uniform seed. We strengthen their result via a completely different proof to make the non-malleable extractor of Li secure against quantum side information even when the seed is not uniform; 4) A modification (working with weak local randomness instead of uniform local randomness) of the Dodis and Wichs (2009) protocol for privacy-amplification is secure against active quantum adversaries (those who arbitrarily modify the messages exchanged in the protocol). This strengthens on a recent result due to Aggarwal et al. (2019) which uses uniform local randomness; 5) A tight efficiency lower bound for the (generalized) inner-product function (in fact a general class of two-wise independent functions).

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

I. INTRODUCTION

RANDOMIZED algorithms are designed under the assumption that randomness used within the algorithms is uniformly distributed. However, random sources in nature are often not necessarily uniform (aka weak). Thus, it is important to understand how to extract uniform randomness from weak-sources. Extractors are functions that transform weak-sources to uniform randomness. Extractors have numerous applications including privacy-amplification, pseudo-randomness, derandomization, expanders and cryptography. A general model of weak-sources is the so-called min-entropy source (please refer to Section II for definitions of information-theoretic quantities). Let \( n, t, m \) be positive integers and \( k, k_1, k_2, k_3, b_1, b_2, b, l \) be positive reals.

Definition 1 [8]: An \((n, k)\)-source denotes an \( n \)-bit source \( X \in \{0, 1\}^n \) with the min-entropy bound \( k, i.e. \ H_{\text{min}}(X) \geq k \).

It can be argued that no deterministic function can extract even one uniform bit given an (arbitrary) \((n, k)\)-source as long as \( k \leq n - 1 \) [4]. This lead to designing extractors using an additional uniform source (aka seed) called seeded extractors [9]. Another approach is to consider multiple independent weak-sources.

Definition 2 [2], [8]: An \((n, k_1, k_2, \ldots, k_t)\)-source denotes \( t \) independent \( n \)-bit sources \( X_1, X_2, \ldots, X_t \) with min-entropy bounds \( H_{\text{min}}(X_i) \geq k_i \) for every \( i \in [t] \).

Multi-source extractors are functions that transform multiple weak-sources to uniform randomness. Multi-source extractors have been studied extensively in the classical setting [4], [10], [11], [12], [13], [14]. With the advent of quantum computers, it is natural to investigate the security of extractors against a quantum adversary with quantum side information on weak-sources. As expected quantum side information presents many more challenges compared to classical side information. Gavinsky et al. [15] gave an example of a seeded extractor secure against a classical adversary but not secure against a quantum adversary (even with a very small side information). Several definitions of quantum multi-source adversaries have been proposed in the literature. Kasher and Kempe [1] introduced quantum bounded storage adversary (qbsa), where the adversary has bounded memory. They also introduced quantum independent adversary (qia) which obtains independent side information from various sources. Arnon-Friedman et al. [3] introduced quantum Markov adversary (qma), such that \( X - E - Y \) forms a Markov-chain \((I(X : Y | E) = 0)\)\(^1\), where \( E \) is adversary’s side

\(^{1}I(A : B | C)_p\) represents conditional mutual information between registers \( A, B \) given register \( C \) in state \( p \).

---

1 Manuscript received 1 August 2022; revised 2 June 2023; accepted 27 August 2023. Date of publication 8 September 2023; date of current version 26 December 2023. This work was supported in part by NRF under Grant NRF-NRF2013-13 and Grant NRF2021-QEP2-02-P05; in part by the Prime Minister’s Office and the Ministry of Education, Singapore, under the Research Centers of Excellence Program under Grant MOE2012-T3-1-009 and Grant MOE2019-T2-1-145; in part by the VanQuTe Grant and the Visiting Advanced Joint Research (V AJRA) Grant, Department of Science and Technology, Government of India, under Grant NRF2017-NRF-ANR004.

(Di remed author: Naresh Goud Boddu.)

Divesh Aggarwal is with the Centre for Quantum Technologies and the Department of Computer Science, National University of Singapore, Singapore 119077 (e-mail: dcsgdiva@nus.edu.sg).

Naresh Goud Boddu is with NTT Research, Sunnyvale, CA 94085 USA (e-mail: naresh.boddu@ntt-research.com).

Rahul Jain is with the Centre for Quantum Technologies and the Department of Computer Science, National University of Singapore, Singapore 119077, and also with the Majelab, UMI 3654, Singapore 117543 (e-mail: rahul@comp.nus.edu.sg).

Maciej Obrenski is with the Center for Quantum Technologies, National University of Singapore, Singapore 119077 (e-mail: obrenski.math@gmail.com).

Communicated by M. Berta, Associate Editor for Quantum.

Digital Object Identifier 10.1109/TIT.2023.3313149
information. Chung et al. [2] introduced general entangled adversary (gea). A natural question that arises is what is the relationship/hierarchy between these different adversary models. Previous works [1], [2], [3] also ask if there is a model which is stronger than the existing models. To quote [1]

In light of this, it is not clear if and how entangled guessing entropy sources can be incorporated into the model, and hence we only consider bounded storage adversaries in the entangled case.

A difficulty that they point is that in the quantum setting (unlike the classical setting), measuring the adversary side information might break the independence of the sources [1]. Quantum entanglement between various parties, used to generate side information raises additional issues. Entanglement is of course known to yield several unexpected effects with no classical counterparts, e.g., non-local correlations [16] and super-dense coding [17] etc.

A main objective of this work is to unify all the existing quantum multi-source adversary models. We propose two new models of adversaries: 1) the quantum measurement adversary (qma, Definition 3), which generates side information using entanglement and conditioned on post-measurement outcomes and 2) the quantum communication adversary (qca, Definition 4), which generates side information using entanglement and communication between multiple sources.

Definition 3 (l-qma, l-qma-state): Let \( \tau_{XY}, \tau_{Y\hat{Y}} \) be canonical purifications of uniform sources \( X, Y \) respectively (registers \( X\hat{Y} \) with Reference).

1) Alice and Bob hold \( X, Y \) respectively. They also share an entangled state \( \tau_{NM} \) (Alice holds \( N \), Bob holds \( M \)).

2) Alice applies an (safe) isometry \( V_A : \mathcal{H}_X \otimes \mathcal{H}_N \rightarrow \mathcal{H}_X \otimes \mathcal{H}_N' \otimes \mathcal{H}_A \) and Bob applies an (safe) isometry \( V_B : \mathcal{H}_Y \otimes \mathcal{H}_M \rightarrow \mathcal{H}_Y \otimes \mathcal{H}_M' \otimes \mathcal{H}_B \). Registers \( A, B \) are single qubit registers. Let

\[
\rho_{XAN'M'BYY} = (V_AV_B)(\tau_{XY} \otimes \tau_{NM} \otimes \tau_{Y\hat{Y}})(V_A^\dagger V_B^\dagger).
\]

3) Alice and Bob perform a measurement in the computational basis on the registers \( A \) and \( B \) respectively. Let

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

and

\[
\Phi_{X\hat{X}N'M'Y\hat{Y}} = \rho_{XAN'M'BYY}\big|_{(A = 1, B = 1)}.
\]

4) Adversary gets access to either \( \Phi_{XY} \) or \( \Phi_{M'Y} \). The pure state \( \Phi \) is called an l-qma-state.

Motivation for the l-qma Model: A general model classically for two sources with side information is the Markov model of the form

\[
\mathcal{C} = \{X \rightarrow E \rightarrow Y : \text{Hmin}(X|E) \geq k_1 \text{ and Hmin}(Y|E) \geq k_2 \}.
\]

We can generate Markov-chain as above via the following procedure. Let Alice and Bob hold independent and uniform sources \( X' \) and \( Y' \) respectively. In addition, let Alice and Bob share independent randomness \( E' \). Let Alice generate a local random variable \( A \in \{0, 1\} \) (using \( X'E' \)) and Bob generate a local random variable \( B \in \{0, 1\} \) (using \( Y'E' \)). It can be readily verified that \( (X'E'Y' | A = B = 1) \) is a Markov-chain. It can also be checked that any Markov-chain \( X \rightarrow E \rightarrow Y \) can be generated using this procedure.

The natural analogue of this procedure in the quantum setting is as described in Definition 3. A key difference with the classical setting is that, in the quantum setting, the resultant post-measurement state, does not form a Markov-chain and thus bringing the elusive nature of quantum side information. This brings us to consider sources\(^2\) of the form

\[
Q = \{\sigma_{X\hat{X}N'M'Y\hat{Y}} : \sigma_{X\hat{X}N'M'Y\hat{Y}} \text{ is an l-qma-state} \}.
\]

A question may be asked if one can provide both the registers \( M' \) and \( N' \) as side information to the adversary. However this may allow adversary to gain complete knowledge of \( X, Y \) (since \( N' \) may contain a copy of \( X \) and \( M' \) may contain a copy of \( Y \)) making the model trivial. Thus we settle on the model as in Definition 3.

We next define 2-source quantum communication adversary inspired from quantum communication protocols.

Definition 4 ((k_1, k_2)-qca, (k_1, k_2)-qca-state): Let \( \tau_{XY}, \tau_{Y\hat{Y}} \) be the canonical purifications of the independent sources \( X, Y \) respectively (registers \( X\hat{Y} \) with Reference).

1) Alice and Bob hold \( X, Y \) respectively. They also share an entangled pure state \( \tau_{NM} \) (Alice holds \( N \), Bob holds \( M \)).

2) Alice and Bob execute a quantum communication protocol, at the end of which the final state is \( |\Phi\rangle_{XY\hat{X}N'M'Y\hat{Y}} \). (Alice holds \( XN' \) and Bob holds \( YM' \)), with \( H_{\text{min}}(X|Y) \geq k_1 \) and \( H_{\text{min}}(Y|N) \geq k_2 \).

3) Adversary gets access to either one of \( \Phi_{XY} \) or \( \Phi_{M'Y} \) of its choice. The state \( \Phi \) is called a \((k_1, k_2)\)-qca-state.

Remark: We note to the reader that indeed every \((k_1, k_2)\)-qca-state is a \((k_1, k_2)\)-qpa-state (where, qpa-state stands for quantum purified adversary state) defined in Boddu et al. [18] (see Definition 10). But, it is apriori not clear if every \((k_1, k_2)\)-qpa-state can be generated via a communication protocol as in Definition 4.

A. Our Results

We show that,

1) \( \text{qma} \) is the strongest adversary among all the known adversaries (Theorem 1), in the sense that the side information of all other adversaries can be generated by \( \text{qma} \).

2) The (generalized) inner-product function (in fact a general class of two-wise independent functions) continues to work as a good extractor against \( \text{qma} \) (Theorem 2) with matching parameters as that of Chor and Goldreich [4] against classical adversaries.

3) A non-malleable extractor proposed by Li [5] (against classical adversaries) continues to be secure against quantum side information (Theorem 3). A non-malleable extractor (nmExt) for sources \( (X, Y) \) is an extractor such that nmExt\((X, Y)\) is uniform and independent of nmExt\((X, Y')\) where \( Y' \neq Y \) is generated by the adversary using \( Y \) and the side information on \( X \).

\(^2\)Even though the state contain adversary side information, we call entire pure state as source for simplicity.
This result implies a non-malleable extractor result of Aggarwal et al. [6] with uniform $Y$. We strengthen their result via a completely different proof to make the non-malleable extractor of Li $(\text{nmExt}(X, Y) = \langle X, Y \mid Y^2 \rangle)$ secure against quantum side information even when $Y$ is not uniform.

4) A modification (working with weak local randomness instead of uniform local randomness) of the Dodis and Wichs [7] protocol for privacy-amplification (PA) is secure against active quantum adversaries (those who arbitrarily modify the messages exchanged in the protocol). This strengthens on a recent result due to [6] which uses uniform local randomness.

5) We also show a tight efficiency lower bound (Corollary 1) for the (generalized) inner-product function (in fact a general class of two-wise independent functions).

**B. qma Can Simulate Other Adversaries**

We show that the side information of all the adversaries can be simulated (see Definition 22) in the model of qma.

**Theorem 1:** Quantum side information of $(b_1, b_2)$-qlsa (see Definition 23), $(k_1, k_2)$-qia (see Definition 24), $(k_1, k_2)$-gea (see Definition 25), acting on an $(n, k_1', k_2')$-source can be simulated by an l-qma for some $l \leq 2 \min\{b_1, b_2\} + 2n - k_1' - k_2'$, $l \leq 2n - k_1 - k_2$, $l \leq 2n - k_1 - k_2$ respectively.

Quantum side information of $(k_1, k_2)$-qMara (see Definition 26) and $(k_1, k_2)$-qca (see Definition 4) can be simulated $\varepsilon$-approximately by an l-qma for some $l \leq 2n - k_1 - k_2 + 25 + 6 \log(1/\varepsilon)$, $l \leq 2n - k_1 - k_2 + 25 + 6 \log(1/\varepsilon)$ respectively.

**C. Inner-Product Is Secure Against qma**

A 2-source extractor secure against l-qma is defined as follows:

**Definition 5:** An $(n, n, m)$-2-source extractor $\text{2Ext} : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^m$ is said to be $(l, \varepsilon)$-quantum secure against l-qma if for every l-qma-state $\Phi$ (chosen by l-qma), we have

$$\|\Phi_{\text{2Ext}(X, Y) N'} - U_m \otimes \Phi_{N'}\|_1 \leq \varepsilon$$

and

$$\|\Phi_{\text{2Ext}(X, Y) M'} - U_m \otimes \Phi_{M'}\|_1 \leq \varepsilon.$$ 

The extractor is called $Y$-strong if

$$\|\Phi_{\text{2Ext}(X, Y) M' Y} - U_m \otimes \Phi_{M' Y}\|_1 \leq \varepsilon,$$

and $X$-strong if

$$\|\Phi_{\text{2Ext}(X, Y) N' X} - U_m \otimes \Phi_{N' X}\|_1 \leq \varepsilon.$$

We show that the inner-product extractor (in fact a general class of $X$-two-wise independent function (Definition 16 [4])) of Chor and Goldreich [4] continues to be secure against l-qma.

**Theorem 2:** Let $p = 2^m$ and $n' = n \log p$. Let $\rho_{X X N M Y M}$ be an l-qma-state such that $|X| = |X| = |Y| = |Y| = n'$ and $XY$ classical (with copies $\tilde{X}Y$ respectively). Let $f : X \times Y \rightarrow Z$ be a $X$-two-wise independent function such that $X = Y = \mathbb{F}_p^n$, $Z = \mathbb{F}_p$ and $(X, Y) \in (X, Y)$. Let $Z = f(X, Y) \in Z$. Then,

$$\|\rho_\text{NM} - U_m \otimes \rho_\text{N}\|_1 \leq \varepsilon,$$

for parameters $l \leq (n' - m - 40 + 8 \log(\varepsilon))/2$.

Symmetric results follow for a $Y$-two-wise independent function $f : X \times Y \rightarrow Z$ by exchanging $(N, X) \leftrightarrow (M, Y)$ above.

As a corollary of Theorem 2, we also get a tight efficiency (Definition 21) lower bound for a $X$-two-wise independent function.

**Corollary 1 (Efficiency Lower Bound for a $X$-Two-Wise Independent Function):** Let function $f : X \times Y \rightarrow Z$ be a $X$-two-wise independent function such that $|X| = |Y|$. Let $U$ be the uniform distribution on $X \times Y$. For any $\gamma > 0$,

$$\log \left( \text{eff}_\gamma(f, U) \right) \geq \frac{1}{2} \left( \log |X| - \log |Z| - 40 + 8 \log \left( 1 - \gamma - \frac{1}{|Z|} \right) \right).$$

Noting entanglement-assisted communication complexity of a function $f$ is lower bounded by efficiency of a function $f$ (Fact 29) and that the (generalized) inner-product function is a $X$-two-wise independent function (note $X = \mathbb{F}_p^n$), we immediately get the following as a corollary.

**Corollary 2:** Let $\text{IP}_p^n : \mathbb{F}_p^n \times \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ be defined as,

$$\text{IP}_p^n(x, y) = \sum_{i=1}^{n} x_i y_i \mod p.$$

We have,

$$Q_\gamma(\text{IP}_p^n) \geq \frac{(n - 1) \log p}{4} + \log \left( 1 - \gamma - \frac{1}{p} \right) - 20.$$
Without any loss of generality, we consider the adversary operation to be isometry (since one can consider Stinespring extension of a CPTP map as an isometry (see Fact 18) if the adversary operation is a CPTP map). This leads us to consider $(k_1, k_2)$-wqnm-state.

Definition 7 ($(k_1, k_2)$-wqnm-state): Let $\sigma_{X^N Y^N}$ be a $(k_1, k_2)$-wqpa-state. Let $V : \mathcal{H}_Y \otimes \mathcal{H}_M \rightarrow \mathcal{H}_Y \otimes \mathcal{H}_Y \otimes \mathcal{H}_Y^c \otimes \mathcal{H}_M^c$ be an isometry such that for $p = V\sigma V^\dagger$, we have $Y'$ classical (with copy $Y'$) and $\Pr(Y \neq Y') = 1$. We call state $\rho$ a $(k_1, k_2)$-wqnm-state.

Since we require the non-malleable extractor to extract from every $(k_1, k_2)$-wqnm-state, we phrase an adversary qnma (short for quantum non-malleable adversary) to choose the $(k_1, k_2)$-wqnm-state.

Definition 8 (Quantum Secure Weak-Seeded Non-Malleable Extractor): An $(n_1, n_2, m)$-non-malleable extractor $\text{nmExt} : \{0, 1\}^{n_1} \times \{0, 1\}^{n_2} \rightarrow \{0, 1\}^m$ is $\rho$-secure against qnma if for every $(k_1, k_2)$-wqnm-state $\rho$ (chosen by the adversary qnma),

$$\|\rho_{\text{nmExt}(X,Y)\text{nmExt}(X,Y')}Y/Y' M'\| - U_{n_2} \otimes \rho_{\text{nmExt}(X,Y)Y'Y' M'\|} \leq \epsilon.$$

Following is an inner-product based non-malleable extractor proposed by Li [5].

Definition 9 [5]: Let $p \neq 2$ be a prime and $n$ be an integer. Define $\text{nmExt} : F_p^n \times F_p^n \rightarrow F_p^n$ given by $\text{nmExt}(X,Y) \overset{\text{def}}{=} \langle X, Y \rangle Y^2$, where $\| \|$ represents concatenation of strings and $Y^2$ is computed via multiplication in $F_p/2$. We show that the inner-product based non-malleable extractor proposed by Li [5] continues to be secure against quantum side information.

Theorem 3: Let $p \neq 2$ be a prime, $n$ be an even integer and $\epsilon > 0$. The function $\text{nmExt}(X,Y)$ is a $(k_1, k_2, \epsilon)$-quantum secure weak-seeded non-malleable extractor against qnma for the parameters $k_1 + k_2 \geq (n + 17)\log p + 33 + 16\log \frac{1}{\epsilon}$.

E. Privacy-Amplification With Weak-Sources

We study the problem of privacy-amplification (PA) [19], [20], [21], [22]. In this problem, two parties, Alice and Bob, share a weak secret $X$ (with $H_{\text{min}}(X|E) \geq k$, where $E$ is adversary Eve side information). Using $X$ and an insecure communication channel, Alice and Bob would like to securely agree on a secret key $R$ that is close to uniformly random to an active adversary Eve who may have full control over their communication channel. In all prior protocols including [6], we assume that Alice and Bob have local access to uniform sources of randomness. In practice, uniform sources are hard to come by, and it is more reasonable to assume that Alice and Bob have only weak-sources of randomness. For this we make use of breakthrough result by Dodis and Wichs [7], who were first to show the existence of a two-round PA protocol with optimal (up to constant factors) entropy loss, for any initial min-entropy. We modify the protocol of [7], to accommodate the non-uniform local randomness at Alice and Bob side. Based on our construction of a quantum secure weak-seeded non-malleable extractor (Theorem 3) we obtain a PA protocol working with weak local sources of randomness and is secure against active quantum adversaries as long as the initial secret $X$ has min-entropy rate of more than half.

F. Proof Overview

For the proof of Theorem 1, we first prove Lemma 1. To prove Lemma 1, we first establish Claims 1 and 2 using the standard quantum information-theoretic techniques. Claim 1 corresponds to correlating independent and uniform $X$ with quantum side information while Claim 2 corresponds to correlating independent and uniform $Y$ with quantum side information conditioned on post-measurement by Alice. In particular, we used a quantum analogue of the rejection-sampling argument of [23] to prove them. Next, using Lemma 1, we generate side information (of other adversary models) in the $l$-qma model, since it suffices to showing appropriate conditional-min-entropy and modified-conditional-min-entropy bounds of various adversary models in the purification picture.

For the proof of Theorem 4, let initial state of $l$-qma model be $\tau$, state after the Alice measurement outcome $A = 1$ be $\rho$ and state after the Bob measurement outcome $B = 1$ conditioned on Alice post-measurement outcome $A = 1$ be $\Phi$. We first reduce the task of bounding $\|\Phi_{ZYM} - U_{Z} \otimes \Phi_{YM}\|_1$ to bounding the collision-probability $\Gamma(\rho_{ZYM} | | \rho_{YM})$ at the expense of multiplicative factor given by $\left| \frac{\text{supp}(Z)}{\text{supp}(E)1} \right|$, using Cauchy Schwarz inequality as key ingredient. Notice, in state $\rho$, we have $\rho_{YYXN'} = \rho_Y \otimes \rho_{XXN'}$. Thus, this enables us to use the argument of Renner [24] to further bound the collision-probability $\Gamma(\rho_{ZYM} | | \rho_{YM})$ to be exponentially small in min-entropy $H_{\text{min}}(X|YM)$ for pairwise-independent function $f$ such that $Z = f(X,Y)$. Additionally when $\tau_{YM} = \rho_{YM}$, the proof follows by noting the relation of $H_{\text{min}}(X|YM)$ with probability of Alice’s measurement outcome $A = 1$ ($\Pr(A = 1)$).

For the proof of Theorem 3, we first make use the result of [6] which reduces the task of showing non-malleable extractor security of Li’s extractor to showing hardness of inner-product in a guessing game. We note that it is equivalent to showing hardness of inner-product in a $(k_1, k_2)$-wqnm-state (see Definition 7). We next show that we can get the conditional-min-entropy bounds required to make use of Fact 30 to simulate $(k_1, k_2)$-wqnm-state as $(k_1, k_2)$-qpa-state. Thus, hardness of inner-product in a guessing game further reduces to showing security of inner-product against $(k_1, k_2)$-qpa-state. Using Fact 30, the proof now follows.

G. Comparison With [6]

Both [6] and Theorem 3 have considered the inner-product based non-malleable extractor proposed by Li [5]. Reference [6] extends the first step of classical proof, the reduction provided by the non-uniform XOR lemma, to the quantum case. This helps in reducing the task of showing non-malleable extractor property of inner-product to showing security of inner-product in a certain communication game. They then approach the problem of showing security of inner-product in a communication game by using the “reconstruction paradigm” of [25] to guess the entire input $X$ from the modified side information.

On the other hand, in Theorem 3, we reduce the security of inner-product in a communication game to the security of inner-product against the quantum measurement adversary. In the process, both [6] and Theorem 3 crucially use the
combinatorial properties of inner-product. For example, in the proof of Theorem 3, we heavily uses the pairwise independence property of inner-product.

H. Other Related Works

Seeded extractors have been studied extensively in the classical setting [9], [26]. König et al. [27] showed that any one-bit output extractor is also secure against quantum adversaries, with roughly the same parameters. Ta-Shma [28], De and Vidick [29], and later De et al. [31] gave seeded extractors with short seeds that are secure against quantum side information and can extract almost all of min-entropy and are based on Trevisan’s extractor [30]. The extractor of Impagliazzo et al. [26] was shown to be secure against quantum side information by [24], [31], and [32].

In the multi-source setting, a probabilistic argument shows the existence of 2-source extractors for min-entropy $k = \log n + O(1)$. Explicit constructions of multi-source extractors with access to more than 2-sources has been considered in the successful line of work [5], [33], [34], [35], [36] leading to a near optimal 3-source extractor that works for polylogarithmic min-entropy and has negligible error [37]. Explicit constructions of 2-source extractors has been first considered in [4] who showed that inner-product is a 2-source extractor for min-entropy $k \geq n/2$. After nearly two decades, Bourgain [10] broke the “half entropy barrier”, and constructed a 2-source extractor for min-entropy $(1/2 - \delta)n$, for some tiny constant $\delta > 0$. A long line of research starting with [4], [10], [13], [38], and [39] leading to a near optimal 2-source extractor that works for polylogarithmic min-entropy and has inverse polynomial error [38], [39].

I. Subsequent Works

Inspired from our work, Boddu et al. [18] have defined $(k_1, k_2)$-qpa-state as specified below.

**Definition 10** $(k_1, k_2)$-qpa-state: A pure state $\sigma_{X^N Y^M Z} = \langle X | Y | Z \rangle$ classical and (X̃Ỹ) copy of (XY), a $(k_1, k_2)$ qpa-state iff

$$H_{\min}(X | MYY \hat{Y})_\sigma \geq k_1 \quad ; \quad H_{\min}(Y | NXX \hat{X})_\sigma \geq k_2.$$

They showed that every l-qma-state is also a $(k_1, k_2)$-qpa-state as stated in the below fact.

**Fact 1** [18]: Let $\sigma_{X^N Y^M Z}$ be an l-qma-state such that $|X| = |X| = |Y| = |Z| = n$. There exists $k_1, k_2$ such that $\sigma$ is a $(k_1, k_2)$-qpa-state. $k_1 \geq n - l$ and $k_2 \geq n - l$.

They also showed that for every $(k_1, k_2)$-qpa-state there is a close-by l-qma-state as stated in the below fact.

**Fact 2** [18]: Let $\rho_{X^N Y^M Z}$ be a $(k_1, k_2)$-qpa-state such that $|X| = |X| = |Y| = |Z| = n$. There exists an l-qma-state $\rho^{(1)}$ such that,

$$\Delta_B(\rho^{(1)}; \rho) \leq 6 \varepsilon \quad \text{and} \quad l \leq 2n - k_1 - k_2 + 4 + 6 \log \left( \frac{1}{\varepsilon} \right).$$

Furthermore,

$$H_{\min}(X | MYY \hat{Y})_{\rho^{(1)}} \geq k_1 - 2 \log \left( \frac{1}{\varepsilon} \right).$$

They used $(k_1, k_2)$ qpa-state framework to construct the first explicit quantum secure non-malleable extractor for (source) min-entropy $\geq \text{polylog} \left( \frac{n}{\varepsilon} \right)$ and seed length of $\text{polylog} \left( \frac{n}{\varepsilon} \right)$ ($n$ is the length of the source and $\varepsilon$ is the error parameter) which lead to a 2-round privacy-amplification protocol that is secure against active quantum adversaries with communication polylog $\left( \frac{n}{\varepsilon} \right)$, exponentially improving upon the linear communication required by the protocol due to [6].

In addition, using our result, the security of inner-product against l-qma as key ingredient, they constructed the first explicit quantum secure 2-source non-malleable extractor for min-entropy $k_1, k_2 \geq n - n^{O(1)}$, with an output of size $n/4$ and error $2 - n^{O(1)}$.

Additionally, Jain and Kudzu [42] have used our efficiency lower bound result (Corollary 4) to obtain a direct-product result for two-wise independent functions including for the generalized inner-product function (IP).

J. Organization

In Section II, we present our notations, definitions and other information-theoretic preliminaries. In Section III, we present the proof of Theorem 4 and Fact 30. In Section IV, we present the proof of Theorem 1. In Section V we present the proof of Theorem 3.

II. PRELIMINARIES

A. Quantum Information Theory

Let $X, Y, Z$ be finite sets (we only consider finite sets in this paper). We use $x \leftarrow X$ to denote $x$ drawn uniformly from $X$. All the logarithms are evaluated to the base 2. 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 matrix on $\mathcal{H}$ with trace equal to 1. It is called pure if and only if its rank is 1. Let $|\psi\rangle$ be a unit vector on $\mathcal{H}$, that is $\langle \psi, \psi \rangle = 1$. With some abuse of notation, we use $\psi$ to represent the state and also the density matrix $|\psi\rangle\langle\psi|$ associated with $|\psi\rangle$. Given a 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 $|A| := \log \dim(\mathcal{H}_A)$. Let $\mathcal{L}(\mathcal{H}_A)$ represent the set of all linear operators on $\mathcal{H}_A$. 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 matrix. We denote by $\mathcal{D}(\mathcal{H}_A)$, the set of quantum states on the Hilbert space $\mathcal{H}_A$. 

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
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 $\rho_A, \sigma_B$, we let $\rho_A \equiv \sigma_B$ represent that they are identical as states, just in different registers. Composition of two registers $A$ and $B$, denoted $AB$, is associated with the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. For two quantum states $\rho \in \mathcal{D}(\mathcal{H}_A)$ and $\sigma \in \mathcal{D}(\mathcal{H}_B)$, $\rho \otimes \sigma \in \mathcal{D}(\mathcal{H}_{AB})$ represents the tensor product (Kronecker product) of $\rho$ and $\sigma$. The identity operator on $\mathcal{H}_A$ is denoted $I_A$. Let $U_A$ denote maximally mixed state in $\mathcal{H}_A$. We also use $U_m$ to denote uniform distribution supported on $m$-bit strings. Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$. Define $$\rho_B \equiv \text{Tr}_A \rho_{AB} = \sum_i \langle i | \otimes I_B \rangle \rho_{AB} | i \rangle \otimes I_B,$$
where $\{|i\rangle\}_i$ is an orthonormal basis for the Hilbert space $\mathcal{H}_A$. The state $\rho_B \in \mathcal{D}(\mathcal{H}_B)$ is referred to as the marginal state of $\rho_{AB}$. Unless otherwise stated, a missing register from subscript in a state will represent partial trace over that register. Given $\rho_A \in \mathcal{D}(\mathcal{H}_A)$, a purification of $\rho_A$ is a pure state $\rho_A \in \mathcal{D}(\mathcal{H}_{AB})$ 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 $\rho_A = |i\rangle \langle i|_A$ is $|i\rangle \otimes |i\rangle_\beta = (\sum_i |i\rangle_\beta) |i\rangle \otimes |i\rangle_B$.

A quantum map $\mathcal{E} : \mathcal{H}(A) \rightarrow \mathcal{L}(\mathcal{H}_B)$ is a completely positive and trace preserving (CPTP) linear map (mapping states in $\mathcal{D}(\mathcal{H}_A)$ to states in $\mathcal{D}(\mathcal{H}_B)$). 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 $U(\mathcal{H}_A)$. An isometry $V : \mathcal{H}_A \rightarrow \mathcal{H}_B$ is such that $V^* V = I_A$ and $V V^* = I_B$. A POVM element is an operator $0 \leq M \leq I$. We use shorthand $M \equiv I - M$, where $I$ is clear from the context. We use shorthand $M$ to represent $M \otimes 1$, where $1$ is clear from the context.

**Definition 11 (Classical Register in a Pure State):** Let $\mathcal{X}$ be a set. A classical-quantum (c-q) state $\rho_{XE}$ is of the form
$$\rho_{XE} = \sum_{x \in \mathcal{X}} p(x) |x\rangle \langle x| \otimes \rho_E,$$
where $\rho_E$ are states. Let $\rho_{XEA}$ be a pure state. We call $X$ a classical register in $\rho_{XEA}$, if $\rho_{XE}$ (or $\rho_{X}$) is a c-q state. We identify random variable $X$ with the register $X$ with $\text{Pr}(X = x) = p(x)$.

**Definition 12 (Copy of a Classical Register):** Let $\rho_{XXE}$ be a pure state with $X$ being a classical register in $\rho_{XXE}$ (see Definition 11) taking values in $\mathcal{X}$. Similarly, let $\tilde{X}$ be a classical register in $\rho_{\tilde{X}XE}$ taking values in $\mathcal{X}$. Let $\Pi_{XE} = \sum_{x \in \mathcal{X}} |x\rangle \langle x| \otimes |x\rangle \langle x|$ be the equality projector acting on the registers $X \tilde{X}$. We call $X$ and $\tilde{X}$ copies of each other (in the computational basis) if $\text{Tr} (\Pi_{XE} \rho_{X\tilde{X}}) = 1$.

**Definition 13 (Conditioning):** Let
$$\rho_{XE} = \sum_{x \in \{0, 1\}^n} p(x) |x\rangle \langle x| \otimes \rho_E,$$
be a c-q state. For an event $S \subset \{0, 1\}^n$, define
$$\text{Pr}(S)_{\rho} \equiv \sum_{x \in S} p(x)$$
and
$$(\rho|X \in S) \equiv \frac{1}{\text{Pr}(S)_{\rho}} \sum_{x \in S} p(x) |x\rangle \langle x| \otimes \rho_E.$$
7) **Max-divergence** [23, 43]: For states $\rho, \sigma$ such that $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$,
\[
D_{\max}(\rho||\sigma) \overset{\text{def}}{=} \min\{\lambda \in \mathbb{R} : \rho \leq 2^\lambda \sigma\}.
\]

8) **Sandwitched-Rényi-divergence**: Let $1 \neq \alpha > 0$. For states $\rho, \sigma$ such that $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$,
\[
D_{\alpha}(\rho||\sigma) \overset{\text{def}}{=} \frac{1}{\alpha - 1} \log \left(\frac{\text{Tr}(\sigma^{1-\frac{1}{\alpha}} \rho^{\frac{1}{\alpha}})}{\alpha}\right).
\]

9) **Collision-probability** [24]: For state $\rho_{AB}$,
\[
\Gamma(\rho_{AB}||\rho_B) \overset{\text{def}}{=} \left(\text{Tr}(\rho_{AB}(I_A \otimes \rho_B^{-1/2}))\right)^2 = 2^{D_{\min}(I_A \otimes \rho_B)} = \| (I_A \otimes \rho_B^{-1/4})\rho_{AB}(I_A \otimes \rho_B^{-1/4}) \|^2.
\]

10) **Min-entropy**: For a random variable $X$,
\[
H_{\min}(X) = \min_{x \in \text{supp}(X)} \log \left(\frac{1}{P_X(x)}\right).
\]

11) **Conditional-min-entropy**: For state $\rho_{XE}$, min-entropy of $X$ conditioned on $E$ is defined as,
\[
H_{\min}(X|E)_{\rho} = -\inf_{\rho_{E|X} \in \mathcal{D}(H_E)} D_{\max}(\rho_{XE}||I_X \otimes \rho_{E}).
\]

12) **Max-information** [43]: For a state $\rho_{AB}$,
\[
I_{\max}(A:B)_{\rho} \overset{\text{def}}{=} \inf_{\rho_{E|X} \in \mathcal{D}(\mathcal{H}_E)} D_{\max}(\rho_{AB}||\rho_A \otimes \rho_{B}).
\]

13) **Modified-conditional-min-entropy**: For state $\rho_{XE}$, the modified-min-entropy of $X$ conditioned on $E$ is defined as,
\[
\tilde{H}_{\min}(X|E)_{\rho} = -D_{\max}(\rho_{XE}||I_X \otimes \rho_{E}).
\]

14) **Markov-chain**: A state $\rho_{XEY}$ forms a Markov-chain (denoted $(X - E - Y)_{\rho}$) iff $I(X : Y|E)_{\rho} = 0$.

**Fact 3**: For each $p$ : $\|A\|^p = \text{Tr}(A^p)$/$p!^2$.$^p$.

**Fact 4** [48]:
For a c-q state $\rho_{XA}$ (X classical) : $\rho_{XA} \leq I_X \otimes \rho_A$ and $\rho_{AX} \leq \rho_X \otimes I_A$.

**Fact 5** [48]: Let $\rho_{XBD}$ be a c-q state (X classical) such that $\rho_{XB} = \rho_X \otimes \rho_B$.
\[
I_{\max}(X:BD)_{\rho} \leq 2|D|.
\]

**Fact 6** For a quantum state $\rho_{XE}$ :
\[
H_{\min}(X|E)_{\rho} \geq \tilde{H}_{\min}(X|E)_{\rho}.
\]

**Fact 7** [18]: Let $\rho \in \mathcal{D}(\mathcal{H}_{AB})$. There exists $\rho' \in \mathcal{D}(\mathcal{H}_{AB})$ such that $\Delta_B(\rho||\rho') \leq \varepsilon$ and
\[
\tilde{H}_{\min}(A|B)_{\rho} \leq H_{\min}(A|B)_{\rho'}, \leq \tilde{H}_{\min}(A|B)_{\rho} + 2\log \left(\frac{1}{\varepsilon}\right).
\]

**Fact 8** [2]: Let $\Phi : \mathcal{L}(\mathcal{H}_M) \rightarrow \mathcal{L}(\mathcal{H}_{M'})$ be a CPTP map and let $\sigma_{X'M'} = (I \otimes \Phi(\rho_{XM}))$. Then
\[
H_{\min}(X|M')_{\rho} \geq H_{\min}(X|M)_{\rho}.
\]

**Fact 9**: Let $\rho, \sigma, \tau$ be quantum states. Then $\Delta(\rho; \tau) \leq \Delta(\rho; \tau) + \Delta(\sigma; \tau)$.

**Fact 10** [49]: Let $\rho, \sigma$ be two states. Then,
\[
1 - F(\rho||\sigma) \leq \Delta(\rho;\sigma) \leq \sqrt{1 - F^2(\rho||\sigma)}
\]
and
\[
\Delta^2_B(\rho;\sigma) \leq \Delta(\rho;\sigma) \leq \sqrt{2} \Delta_B(\rho;\sigma).
\]

**Fact 11** (Data-Processing): Let $\rho, \sigma$ be quantum states and $\Phi$ be a CPTP map. Then
- $\Delta(\Phi(\rho)||\Phi(\sigma)) \leq \Delta(\rho;\sigma)$.
- $\Delta_B(\Phi(\rho)||\Phi(\sigma)) \leq \Delta_B(\rho;\sigma)$.
- $D_{\max}(\Phi(\rho)||\Phi(\sigma)) \leq D_{\max}(\rho||\sigma)$.
- (50) For all $1 \neq \alpha > 0$ : $D_{\alpha}(\Phi(\rho)||\Phi(\sigma)) \leq D_{\alpha}(\rho||\sigma)$.

**Fact 12** [51]: A Markov-chain $(X - E - Y)_{\rho}$ can be decomposed as follows:
\[
\rho_{X'YE} = \sum_{t} \text{Pr}(T = t|t) \otimes (\rho_{X'E_{t}} \otimes \rho_{Y'E_{t}}),
\]
where $T$ is some classical register over a finite alphabet.

**Fact 13** [52]: For a Markov-chain $(X - E - Y)_{\rho}$, there exists a CPTP map $\Phi : \mathcal{L}(\mathcal{H}_E) \rightarrow \mathcal{L}(\mathcal{H}_E \otimes \mathcal{H}_Y)$ such that $\rho_{X'YE} = (I_X \otimes \Phi)\rho_{XEY}$.

**Fact 14** (Hölder’s Inequality): For matrices $A, B, C : \text{Tr}(ABC) = \text{Tr}(CBA)$.

**Fact 15** (Hölder’s Inequality, Special Case): For matrices $A, B : \|BAB\|^1_1 \leq \|A\|_2\|B\|_2^2$.

**Fact 16** (Cyclicity of Trace): For matrices $A, B, C : \text{Tr}(AB) = \text{Tr}(BC)$.

**Fact 17**: Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a state and $M \subseteq \mathcal{L}(\mathcal{H}_B)$ such that $M^\dagger M \leq 1_B$. Let $\rho_{AB} = \frac{M_{\rho_{AB}} M^\dagger}{\text{Tr}M_{\rho_{AB}} M^\dagger}$. Then,
\[
D_{\max}(\rho_A||\rho) \leq \log \left(\frac{1}{\text{Tr}M_{\rho_{AB}} M^\dagger}\right).
\]

**Fact 18** (Stinespring Isometry Extension [45]): Let $\Phi : \mathcal{L}(\mathcal{H}_X) \rightarrow \mathcal{L}(\mathcal{H}_Y)$ be a CPTP map. 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 19** (Corollary 5.5 in [45]): Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a pure state and $V_B : \mathcal{L}(\mathcal{H}_B) \rightarrow \mathcal{L}(\mathcal{H}_B \otimes \mathcal{H}_C)$ be an isometry such that $|C| = 1$. Let $\sigma_{ABC} = (I_A \otimes V_B)\rho_{AB}(I_A \otimes V_B)^\dagger$ and $\Phi_{ABC} = (I_{AC}\otimes V_B)\rho_{AB}(I_A \otimes V_B)^\dagger$. There exists an operator $M_B$ such that $0 \leq M_B M_B^\dagger \leq 1_B$.
\[
\Phi_{ABC} = \frac{(I_A \otimes M_B)\rho_{AB}(I_A \otimes M_B)^\dagger}{\text{Tr}(I_A \otimes M_B)\rho_{AB}(I_A \otimes M_B)^\dagger}
\]
and
\[
\text{Pr}[C = 1] = \text{Tr}M_B \rho_B M_B^\dagger.
\]

**Fact 20** (Lemma 5.4.3 [24]): Let $\rho_{XM}$ be a c-q state (X classical). Let $Z = f(X)$, where $f \rightarrow F$ is drawn from a two-wise independent hash function family $F$. Let $\sigma_M \in \mathcal{D}(\mathcal{H}_M)$ be any state. Then,
\[
E_{f \rightarrow F} \left[\text{Tr}\left((I_Z \otimes \sigma_M^{-1/2}) (\rho_{f(X)M} - U_Z \otimes \rho_M)^2\right)\right] \leq \text{Tr}\rho_{XM}(I_X \otimes \sigma_M^{-1/2})\rho_{XM}(I_X \otimes \sigma_M^{-1/2}).
\]
Fact 21 [24]: Let $p$ be a prime number and $n$ be a positive integer. Let $\rho_{XM}$ be a c-q state (X classical) with $\rho_X \in \mathbb{F}_p^n$. Let $Z = f(X)$, where $f \in \mathcal{F}$ is drawn from a two-wise independent hash function family $\mathcal{F}$. Then,

$$
E_{f \in \mathcal{F}} \left[ \text{Tr} \left( (I_Z \otimes \rho_M^{-1/2})(\rho_{f(X)M} - U_Z \otimes \rho_M) \right)^2 \right] \leq 2 - \tilde{H}_{\min}(X|M)_\rho.
$$

**Proof:** Consider,

$$
E_{f \in \mathcal{F}} \left[ \text{Tr} \left( (I_Z \otimes \rho_M^{-1/2})(\rho_{f(X)M} - U_Z \otimes \rho_M) \right)^2 \right] \leq \text{Tr} \rho_{XM}(I_X \otimes \rho_M^{-1/2}) \rho_{XM}(I_X \otimes \rho_M^{-1/2}) \leq \| (I_X \otimes \rho_M^{-1/2}) \rho_{XM}(I_X \otimes \rho_M^{-1/2}) \|_\infty
$$

$$
= 2 - \tilde{H}_{\min}(X|M)_\rho.
$$

The two inequalities follow from Fact 20 and Fact 14 respectively. The final equality follows from Definition 16 [13]. □

Fact 22 (Uhlmann’s Theorem [53]): 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,

$$
F(\rho_A; \sigma_A) = F(V \rho_A V^\dagger; V \sigma_A V^\dagger) = F(V \rho_A V^\dagger; V \sigma_A V^\dagger),
$$

where $|\theta\rangle_A = (I_A \otimes V)|\sigma_A\rangle_C$.

Fact 23 (Rejection-Sampling [23]): Let $X, Y$ be random variables such that $D_{\text{max}}(X||Y) \leq k$. There exists a random variable $Z \in \{0, 1\}$, correlated with Y such that $X \equiv (Y|Z = 1)$ and $\Pr(Z = 1) \geq 2^{-k}$.

Fact 24 [23]: Let $\rho_{A'B'}, \sigma_{A'B'}$ be pure states such that $D_{\text{max}}(\rho_{A'B'}||\sigma_{A'B'}) \leq k$. Let Alice and Bob share $\sigma_{A'B'}$. There exists an isometry $V : A \to A'$ such that,

1. $(V \otimes 1_B)\sigma_{A'B'}(V \otimes 1_B)^\dagger = \phi_{A'B'C}$, where $C$ is a single qubit register.
2. Let $C$ be the outcome of measuring $\phi_C$ in the standard basis. Then $\Pr(C = 1) \geq 2^{-k}$.
3. Conditioned on outcome $C = 1$, the state shared between Alice and Bob is $\rho_{A'B'}$.

We present a proof here for completeness.

**Proof:** Since $D_{\text{max}}(\rho_{A'B'}||\sigma_{A'B'}) \leq k$, let $\sigma_B = 2^{-k} \rho_B + (1 - 2^{-k})\tau_B$. Let $\tau_{A'B'}$ be a purification of $\rho_{A'B'}$. Consider,

$$
\phi_{CAB} = \sqrt{(1 - 2^{-k})|0\rangle_C \otimes \tau_{A'B'} + \sqrt{2^{-k}}|1\rangle_C \otimes \rho_{A'B'}).
$$

Notice $\phi_{A'BC}$ is a purification of $\sigma_{A'B'}$. From Fact 22, there exists an isometry $V : A \to A'$ such that $(V \otimes 1_B)\sigma_{A'B'}(V \otimes 1_B)^\dagger = \phi_{A'BC}$. The desired properties can be readily verified. □

Fact 25 [18]: Let $\rho_{ABC} \in D(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ be a state and $M \in \mathcal{L}(\mathcal{H}_C)$ such that $M \dagger M \leq I_C$. Let $\tilde{\rho}_{ABC} = \frac{M \rho_{ABC} M^\dagger}{\text{Tr} M \rho_{ABC} M^\dagger}$. Then,

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

Furthermore, if $\rho_B = \rho_B$, we also get,

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

Fact 26 [18]: Let $\rho_{XZ}, \rho'_{XZ}$ be states such that $\Delta(\rho; \rho') \leq \varepsilon$. Let $d(Z|A)_{\rho'} \leq \varepsilon$ then $d(Z|A)_\rho \leq 2\varepsilon' + \varepsilon$.

Claim 1: Let $\phi_{XX'AB}$ be a pure state such that $H_{\min}(X|B)_\phi \geq k$. Let $X$ be a classical register (with copy $X'$). Let $\theta_{X_1, X_2}$ be the canonical purification of $\theta_{X_1}$ such that $\theta_{X_2} = U_{X}. Let \theta_{X_1, X_2} be shared between Reference $(X_1)$ and Alice $(X_2)$. There exists a pure state $\sigma_{AB}$ such that when shared between Alice (A) and Bob (B), Alice can perform a measurement which succeeds with probability at least $2^{k-|X|}$ and on success joint shared state is $\phi_{X_1, X'AB}$ between Reference $(X_1)$, Alice $(X'A)$ and Bob $(B)$ such that $\phi_{X_1, X'AB} \equiv \phi_{XX'AB}$.

**Proof:** Let $H_{\min}(X|B)_\phi \geq k$, we have

$$
\inf_{\rho_B} D_{\text{max}}(\phi_{X|B}; U_X \otimes \sigma_B) \leq |X| - k.
$$

Let the infimum above be achieved by $\phi_{AB}$ and let $\sigma_{AB}$ be its purification shared between Alice (A) and Bob (B). The desired now follows from Fact 24 by treating Bob (in Fact 24) as Reference and Bob (here), state $\sigma_{AB}$ (in Fact 24) as $\theta_{X_1, X_2} \otimes \sigma_{AB}$ (here) and state $\rho_{AB}$ (in Fact 24) as $\phi_{X_1, X'AB}$ (here).

Claim 2: Let $\phi_{XX'AYY'B}$ be a pure state such that $H_{\min}(X|BYY')_\phi \geq k_1$ and $\tilde{H}_{\min}(Y|XX')_\phi \geq k_2$.

Let $X, Y$ be classical registers (with copy $X'$ and $Y'$ respectively). Let $\theta_{X_1, X_2}$ be a canonical purification of $\theta_{X_1}$ such that $\theta_{X_2} = U_X$. Let $\theta_{Y_1, Y_2}$ be shared between Reference $(Y_1)$ and Alice $(Y_2)$. Then, $\phi_{XX'AYY'B}$ be a canonical purification of $\phi_{YY'}$ such that when shared between Alice (A) and Bob (BY’Y), Alice and Bob can each perform a measurement which jointly succeeds with probability at least $2^{k_1 + k_2 - |X| - |Y|}$ and on success the joint shared state is $\phi_{X_1, X'AYY'B}$ between Reference $(X_1Y_1)$, Alice $(X'A)$ and Bob $(Y'B)$, such that $\phi_{X_1, X'AYY'B} \equiv \phi_{XX'AYY'B}$.

**Proof:** Since $H_{\min}(X|BY')_\phi \geq k_1$, we have

$$
\inf_{\rho_{BY'}} D_{\text{max}}(\phi_{XY'|BY'}; U_X \otimes \sigma_{BY'}) \leq |X| - k_1.
$$

Let the infimum above be achieved by $\sigma_{BY'}$ and let $\sigma_{BY'}$ be its purification shared between Alice (A) and Bob (BY’). From Claim 1, Alice can do a measurement such that on success $\phi_{X_1, X'AYY'B}$ is shared between Reference $(X_1)$, Alice $(X'A)$ and Bob $(BY'B)$ (such that $\phi_{X_1, X'AYY'B} \equiv \phi_{XX'AYY'B}$). Also, since $H_{\min}(Y|XX')_\phi \geq k_2$, we have

$$
D_{\text{max}}(\phi_{X_1, X'AYY'B}; U_Y \otimes \phi_{XX'}) \leq |X| - k_2.
$$

Again from Claim 1, Bob can do a measurement such that on success $\phi_{X_1, X'AYY'B}$ is shared between Reference $(X_1Y_1)$, Alice $(X'A)$ and Bob $(Y'B)$ (such that $\phi_{X_1, X'AYY'B} \equiv \phi_{XX'AYY'B}$). This completes the proof by noting probability

---

\(^3\)The proof in [18] can be easily modified to prove the inequality for $\tilde{H}_{\min}(\cdot)$.

\(^4\)Claim holds even when $\Delta_B(\cdot)$ is replaced with $\Delta(\cdot)$. 

---

**AGGARWAL et al.: QUANTUM MEASUREMENT ADVANTAGE** 

325
of success in the first and second steps as $2^{k_1 - |X|}$ and $2^{k_2 - |Y|}$ respectively.

Claim 3: Let $\rho_{XX'AYY'B}$ be a pure state such that $H_{\text{min}}(X|BYY')_{\rho} \geq k_1$ and $H_{\text{min}}(Y|XX'A)_{\rho} \geq k_2$. Let $X, Y$ be classical registers (with copy $X'$ and $Y'$ respectively). Let $\theta_{X_2}$ be a canonical purification of $\theta_{X_2}$ such that $\theta_{X_2} \equiv U_X$. Let $\theta_{X_2}$ be shared between Reference $(X_1)$ and Alice $(X_2)$. Let $\gamma_{Y_2}$ be a canonical purification of $\gamma_{Y_2}$ such that $\gamma_{Y_2} \equiv U_Y$. Let $\gamma_{Y_2}$ be shared between Reference $(Y_1)$ and Bob $(Y_2)$. There exists a pure state $\sigma_{ABYY'}$ such that $\sigma_{ABYY'} \equiv \phi_{BYY'}$ and when shared between Alice $(A)$ and Bob $(BYY')$, Alice and Bob each perform a measurement which jointly succeeds with probability at least $2^{k_1 - k_2 - |X| - |Y|}$ and on success the joint shared state is $\phi_{X_1X'AYY'B}$ between Reference $(X_1Y_1)$, Alice $(X'AY)$ and Bob $(Y'B)$. Theorem follows in similar lines of Claim 2 after a simple modification. We state the modification required and do not repeat the entire argument. Considering $\sigma_{ABYY'}$ to be any purification of $\sigma_{BYY'}$, such that $\sigma_{BYY'} \equiv \phi_{BYY'}$ in Claim 2 and repeating the argument of Claim 2, the result follows.

Lemma 1: Let $\rho_{XXNY\hat{Y}M}$ be a pure state such that $|X| = |\hat{X}| = |Y| = |\hat{Y}| = n$, $XY$ classical (with copies $XY$ respectively) and $H_{\text{min}}(X|YY\hat{M})_{\rho} \geq k_1$; $H_{\text{min}}(Y|XXN)_{\rho} \geq k_2$.

Then $\rho$ is also an $l$-qma-state (see Definition 3) for some $l \leq 2n - k_1 - k_2$.

Proof: Simulation of the state $\rho$ in the model of $l$-qma follows from Claim 2. Using Claim 2, with the following assignment of registers (below the registers on the left are from Claim 2 and the registers on the right are the registers in this proof)

$$(X, Y, X', Y', A, B, \Phi) \leftrightarrow (X, Y, \hat{X}, \hat{Y}, N, M, \rho),$$

we have

$$l \leq \log(2^{n-k_1+n-k_2}) = 2n - k_1 - k_2.$$ 

Corollary 3: Let $\rho$ be a $(k_1, k_2)$-wqpa-state such that $|X| = |Y| = n$. Then $\rho$ is also an $l$-qma-state for the parameters $l \leq 2n - k_1 - k_2$.

Proof: Note $\rho_{XXNY\hat{Y}M} = \rho_{XXNM} \otimes \rho_{YY}$, where $\rho_{XXNM}$ is the purification of $\rho_{XM}$ such that $H_{\text{min}}(X|M)_{\rho} \geq k_1$ and $H_{\text{min}}(Y)_{\rho} \geq k_2$. Since $\rho_{XXNY\hat{Y}M} = \rho_{XXNM} \otimes \rho_{YY}$, we have

$$H_{\text{min}}(X|YY\hat{M})_{\rho} \geq k_1$$

and

$$D_{\text{max}}(\rho_{YXXN}||U_Y \otimes \rho_{XXN}) \leq \log(\text{dim}(|H_{YY}|)) - k_2 = n - k_2.$$ 

The first inequality follows since $\rho_{YXXN} = \rho_Y \otimes \rho_{XXN}$ and $H_{\text{min}}(Y)_{\rho} \geq k_2$. Thus, $H_{\text{min}}(Y|XXN)_{\rho} \geq k_2$. Simulation of the $(k_1, k_2)$-wqpa-state in the model of $l$-qma now follows from Lemma 1.

B. Extractors

Definition 17 (Quantum Secure Seeded Extractor): An $(n, d, m)$-seeded extractor $Ext : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ is said to be $(k, \varepsilon)$-quantum secure if for every state $\rho_{XXES}$, such that $H_{\text{min}}(X|E)_{\rho} \geq k$ and $\rho_{XXES} = \rho_{XE} \otimes U_d$, we have

$$\|\rho_{\text{Ext}(X, S, E)} - U_m \otimes \rho_{E}||_1 \leq \varepsilon.$$ 

In addition, the extractor is called strong if

$$\|\rho_{\text{Ext}(X, S, E)} - U_m \otimes U_d \otimes \rho_{E}||_1 \leq \varepsilon.$$ 

The extractor is called $Y$-strong if

$$\|\rho_{\text{Ext}(X, Y, E)} - U_m \otimes \rho_{EY}||_1 \leq \varepsilon,$$

and $X$-strong if

$$\|\rho_{\text{Ext}(X, Y, E)} - U_m \otimes \rho_{EX}||_1 \leq \varepsilon.$$ 

Definition 19: A function $MAC : \{0, 1\}^{2m} \times \{0, 1\} \rightarrow \{0, 1\}^m$ is an $\varepsilon$-information-theoretically secure one-time message authentication code if for any function $A : \{0, 1\}^m \rightarrow \{0, 1\}^m$, it holds that for all $\mu \in \{0, 1\}^m$,

$$\Pr_{k \leftarrow \{0, 1\}^{2m}} [(MAC(k, \mu') = \sigma') \wedge (\mu' \neq \mu)] = A(\mu, MAC(k, \mu)) \leq \varepsilon.$$ 

Efficient constructions of MAC satisfying the conditions of Definition 19 are known. The following fact summarizes some parameters that are achievable using a construction based on polynomial evaluation.

Fact 28 (Proposition 1 in [55]): For any integer $m > 0$, there exists an efficient family of $2^m$-information-theoretically secure one-time message authentication codes

$$MAC : \{0, 1\}^{2m} \times \{0, 1\}^m \rightarrow \{0, 1\}^m.$$ 

C. Quantum Communication Complexity

In a quantum communication protocol $\Pi$ for computing a function $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$, the inputs $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ are given to Alice and Bob respectively. They also start with an entangled pure state independent of the inputs. They perform local operations and exchange quantum messages. The goal is to minimize the communication between them. Please refer to preliminaries of [56] and [57] for details of an entanglement-assisted quantum communication protocol. Let $O(x, y)$ refer to the output of the protocol, on input $(x, y)$.
Let $C_i$ (on $c_i$ qubits) refer to the $i$-th message sent in the protocol.

**Definition 20:** Define,

Worst-case error: $\text{err}(\Pi) \overset{\text{def}}{=} \max_{(x,y)} \{\Pr[O(x,y) \neq f(x,y)]\}$.

Communication of a quantum protocol: $\text{QCC}(\Pi) \overset{\text{def}}{=} \sum_i c_i$.

Entanglement-assisted communication complexity of $f$:

$$Q_\gamma(f) \overset{\text{def}}{=} \min_{\Pi : \text{err}(\Pi) \leq \gamma} \text{QCC}(\Pi).$$

1) **Protocols With Abort and Efficiency:** Consider the following zero-communication protocol with abort for a function $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$. Let the inputs $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ be given to Alice and Bob respectively according to distribution $\mu$. They also start with an entangled pure state $\tau_{NM}$ independent of the inputs (Alice holds $N$ and Bob holds $M$). They apply local operations and measurements are allowed to abort with some probability. Let the state shared between Alice and Bob after their local operations be $\tau_{XN'M'YAB}$. Let $\perp$ represent the abort symbol. Let $\Pr(A = \perp \land B = \perp) \leq 1 - \eta$, and

$$\Phi_{XN'M'YAB} = (\tau_{XN'M'YAB} | A \neq \perp \land B \neq \perp),$$

where Alice holds $XN'$ and Bob holds $MYB$. Let $\gamma > 0$. The goal of Alice and Bob is to maximize $\eta$ such that

$$\Pr(B \neq f(X,Y)) \Phi \leq \eta.$$

**Definition 21:** Define:

Error of $\Pi$ under $\mu$ on non-abort: $\text{err}(\Pi, \mu) \overset{\text{def}}{=} \Pr(B \neq f(X,Y)) \Phi$.

Efficiency of $\Pi$ under $\mu$: $\text{eff}(\Pi, \mu) \overset{\text{def}}{=} \frac{1}{\eta}$.

Efficiency of $f$ under $\mu$: $\text{eff}_\gamma(f, \mu) \overset{\text{def}}{=} \min_{\Pi : \text{err}(\Pi, \mu) \leq \gamma} \text{eff}(\Pi, \mu)$.

Efficiency of $f$: $\text{eff}_\gamma(f) \overset{\text{def}}{=} \max_{\mu} \text{eff}_\gamma(f, \mu)$.

**Fact 29 (Theorem 4 in [58]):** For a function $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ and $\gamma > 0$,

$$Q_\gamma(f) \geq \frac{1}{2} \log(\text{eff}_\gamma(f)).$$

III. INNER-PRODUCT IS SECURE AGAINST qma

We show that the inner-product extractor of Chor and Goldreich [4] is secure against qma (with nearly the same parameters as that of classical adversary). More generally we show any $\mathcal{X}$-two-wise independent function (Definition 16 [4]) continues to be secure against l-qma. We first show that the security of $\mathcal{X}$-two-wise independent function against l-qma.

**Theorem 4:** Let $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ be a $\mathcal{X}$-two-wise independent function such that $|\mathcal{X}| = |\mathcal{Y}|$.

1) Let $\tau = \tau_{XX_1} \otimes \tau_{NM} \otimes \tau_{YY_1}$, where $\tau_{XX_1}$ is the canonical purification of $\tau_X$ (maximally mixed in $\mathcal{X}$), $\tau_{YY_1}$ is canonical purification of $\tau_Y$ (maximally mixed in $\mathcal{Y}$) and $\tau_{NM}$ is a pure state.

2) Let $V_A : H_{X_1} \otimes H_N \rightarrow H_{X_1} \otimes H_{N'} \otimes H_A$ be a (safe) isometry. Let $\rho = (V_A \rho V_A^\dagger | A = 1)$.

3) Let $V_B : H_Y \otimes H_M \rightarrow H_Y \otimes H_{M'} \otimes H_B$ be a (safe) isometry. Let $\Theta = V_B \rho V_B^\dagger$ and $\Phi = (\Theta | B = 1)$.

4) Let $Z = f(X,Y) \in \mathcal{Z}$ and $\varepsilon \overset{\text{def}}{=} \|\Phi_{ZY'M'} - U_Z \otimes \Phi_{Y'M'}\|_1$.

Then

$$\tilde{H}_\text{min}(X|M) - \log |Z| + \log(\Pr(B = 1)\Theta) \leq 2 \log \frac{1}{\varepsilon}.$$

Additionally if $\tau_M = \rho_M$, we further have,

$$\log |\mathcal{X}| - \log |Z| + \log(\Pr(A = 1, B = 1)\tilde{\rho}_A \tilde{\rho}_B (\tilde{\rho}_A \tilde{\rho}_B)) \leq 2 \log \frac{1}{\varepsilon}.$$

Symmetric results follow for a $\mathcal{Y}$-two-wise independent function $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ by exchanging $(N,A,X) \leftrightarrow (M,B,Y)$ above.

**Proof:** From Fact 19, there exists operator $C_{YM}$ such that

$$0 \leq C_{YM}^\dagger C_{YM} \leq I_{YM},$$

$$\Phi_{ZY'M'} = \frac{C_{YM} \rho_{ZXY'M'} C_{YM}^\dagger}{\text{Tr} C_{YM} \rho_{ZXY'M'} C_{YM}^\dagger},$$

and

$$\text{Pr}(B = 1)\Theta = \text{Tr} C_{YM} \rho_{YM} C_{YM}^\dagger.$$

This implies,

$$\Phi_{ZY'M'} = \frac{C_{YM} \rho_{ZXY'M'} C_{YM}^\dagger}{\text{Tr} C_{YM} \rho_{ZXY'M'} C_{YM}^\dagger}.$$
where the final inequality follows from Fact 21, we have

\[ l \leq \log(2^{n' - k_1 + n' - k_2}) = 2n' - k_1 - k_2. \]

Lemma 2: Let \( p = 2^{n'} \) and \( n' = n \log p \). Let \( \rho_{X^k Y^m} \) be a pure state such that \(|X| = |X| = |Y| = |Y| = n'\). \( XY \) classical (with copies \( XY \) respectively) and

\[ \mathbb{H}_{\min}(X|Y) \geq k_1 \quad \text{and} \quad \mathbb{H}_{\min}(Y|X) \geq k_2. \]

Let \( Z = \text{IP}_p(X, Y) \). Then \( Z \) is also an l-qma-state (see Definition 3) for some \( l \leq 2n' - k_1 - k_2 \). Furthermore,

\[ \|\rho_{XY} - U_m \otimes \rho_{XY}\|_1 \leq \varepsilon, \]

for parameters \( k_1 + k_2 \geq n' + m + 2 \log \left( \frac{1}{\varepsilon} \right) \).

Proof: Simultation of the state \( \rho \) in the model of l-qma follows from Claim 3. Using Claim 3, with the following assignment of registers (below the registers on the left are from Claim 3 and the registers on the right are the registers in this proof)

\[ (X, Y, X', Y', A, B, \Phi) \leftrightarrow (X, Y, \hat{X}, \hat{Y}, N, M, \rho), \]

we have

\[ l \leq \log(2^{n' - k_1 + n' - k_2}) = 2n' - k_1 - k_2. \]

Let \( X \in \mathcal{X}, Y \in \mathcal{Y} \). Note that IP\(_p^n\) is a \( \mathcal{X}\)-two-wise independent function. Further state \( \rho_{X^k Y^m} \) is an l-qma-state with \( (\tau_M, \rho_M) \) in Theorem 4 equivalent to \( (\tau_M, \rho_M) \) in the simulation of the state \( \rho \) using Claim 3. Let \( \varepsilon' \) \( \equiv 2\Delta(\rho_{XY} - U \otimes \rho_{XY}) \). Using Theorem 4, we get \( \varepsilon' \leq 2^{-k_1 + k_2 - n' - m} \). For the choice of parameters \( k_1 + k_2 \geq n' + m + 2 \log \left( \frac{1}{\varepsilon} \right) \), we get \( \varepsilon' \leq \varepsilon \). Thus, \( \|\rho_{XY} - U \otimes \rho_{XY}\|_1 \leq \varepsilon \). Symmetric result follows noting IP\(_p^n\) is also a \( \mathcal{Y}\)-two-wise independent function.

Using Lemma 2 as a key ingredient, \([18]\) showed that inner-product extractor (in fact a general class of \( \mathcal{X}\)-two-wise independent function (Definition 16 [4])) of Chor and Goldreich [4] is secure against qpa-state. We state the result from \([18]\) as follows.

Fact 30 \([18]\): Let \( p = 2^m \) and \( n' = n \log p \). Let \( \rho_{X^k Y^m} \) be a \((k_1, k_2)\)-qpa-state such that \(|X| = |X| = |Y| = |Y| = n'\) and \( XY \) classical (with copies \( XY \) respectively). Let \( f : \mathcal{X} \times \mathcal{Y} \longrightarrow \mathcal{Z} \) be a \( \mathcal{X}\)-two-wise independent function such that \( \mathcal{X} = \mathcal{Y} = \mathbb{F}_p^n \). Let \( Z = \mathbb{F}_p^n \) and \((X, Y) \in (\mathcal{X}, \mathcal{Y})\). Then, \( \|\rho_{XY} - U \otimes \rho_{XY}\|_1 \leq \varepsilon \).

for parameters \( k_1 + k_2 \geq n' + m + 40 + 8 \log \left( \frac{1}{\varepsilon} \right) \).

Symmetric results follow for a \( \mathcal{Y}\)-two-wise independent function \( f : \mathcal{X} \times \mathcal{Y} \longrightarrow \mathcal{Z} \) by exchanging \((N, X) \leftrightarrow (M, Y)\) above.

Theorem 5: Let \( p = 2^m \) and \( n' = n \log p \). Let \( \rho_{X^k Y^m} \) be an l-qma-state such that \(|X| = |X| = |Y| = |Y| = n'\) and \( XY \) classical (with copies \( XY \) respectively). Let \( f : \mathcal{X} \times \mathcal{Y} \longrightarrow \mathcal{Z} \) be a \( \mathcal{X}\)-two-wise independent function such that \( \mathcal{X} = \mathcal{Y} = \mathbb{F}_p^n \). Let \( Z = \mathbb{F}_p^n \) and \((X, Y) \in (\mathcal{X}, \mathcal{Y})\). Then, \( \|\rho_{XY} - U \otimes \rho_{XY}\|_1 \leq \varepsilon \).

for parameters \( l \leq (n' - m - 40 + 8 \log \varepsilon)/2 \).

Symmetric results follow for a \( \mathcal{Y}\)-two-wise independent function \( f : \mathcal{X} \times \mathcal{Y} \longrightarrow \mathcal{Z} \) by exchanging \((N, X) \leftrightarrow (M, Y)\) above.

Proof: The proof follows from Fact 30 after noting Fact 1.

We also get a tight efficiency (Definition 21) lower bound for a \( \mathcal{X}\)-two-wise independent function.

Corollary 4 (Efficiency Lower Bound for a \( \mathcal{X}\)-Two-Wise Independent Function): Let function \( f : \mathcal{X} \times \mathcal{Y} \longrightarrow \mathcal{Z} \) be a \( \mathcal{X}\)-two-wise independent function such that \(|X| = |Y|\). Let \( U \)
be the uniform distribution on $X \times Y$. For any $\gamma > 0$, we have
\[
\log \left( \text{eff}_\gamma(f, U) \right) \geq \frac{1}{2} \left( \log |X| - \log |Z| - 40 + 8 \log \left( 1 - \gamma - \frac{1}{|Z|} \right) \right).
\]

**Proof:** Let the inputs $X \in X$ and $Y \in Y$ be given to Alice and Bob respectively according to distribution $U$. Consider an optimal zero-communication protocol $\Pi$ with error of protocol under $U$ on non-abort being $\gamma$. Let the state shared between Alice and Bob after their local operations be $\tau_{XN'M'YAB}$. Let $\bot$ represent the abort symbol. Let $\Pr(A = \bot \land B = \bot) = 1 - \eta$, and
\[
\Phi_{XN'M'YAB} = \left( \tau_{XN'M'YAB} | A \neq \bot \land B \neq \bot \right),
\]
where Alice holds $XN'$ and Bob holds $M'YB$. We have,
\[
\Pr(B \neq f(X, Y)) \leq \gamma \iff \Pr(B = f(X, Y)) \leq 1 - \gamma.
\]

\[
\| \Phi_{BYM'} - U_{\log |Z|} \otimes \Phi_{YM'} \|_1 \leq \epsilon.
\]

This implies, $1 - \gamma \leq \Pr(B = f(X, Y)) \Phi \leq \frac{1}{|Z|} + \epsilon$. Noting $A \neq \bot$ (here) as $A = 1$ (in Definition 3), $B \neq \bot$ (here) as $B = 1$ (in Definition 3), $\Phi$ is an $l$-qma-state with $l \geq \log \left( \frac{1}{\Pr(A = \bot \land B = \bot)} \right)$. Since, $\| \Phi_{BYM'} - U_{\log |Z|} \otimes \Phi_{YM'} \|_1 = \epsilon \geq \log \left( \frac{1}{\gamma - \frac{1}{|Z|}} \right)$, using Theorem 5 we have
\[
\log \left( \text{eff}_\gamma(f, U) \right) \geq \frac{1}{2} \left( \log |X| - \log |Z| - 40 + 8 \log \left( 1 - \gamma - \frac{1}{|Z|} \right) \right),
\]
which gives the desired.

From Fact 29, noting that the (generalized) inner-product function is a $X$-two-wise independent function (note $X = \mathbb{F}_p^n$). We have,

**Corollary 5:** Let $\text{IP}_p^n : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p$ be defined as,
\[
\text{IP}_p^n(x, y) = \sum_{i=1}^{n} x_i y_i \mod p.
\]

We have,
\[
Q_\gamma(\text{IP}_p^n) \geq \frac{(n - 1) \log p}{4} + \log \left( 1 - \gamma - \frac{1}{p} \right) - 20.
\]

**Corollary 7:** Let $p = 2^m$ and $n' = n \log p$. Let $\sigma_{XEY} = \sigma_X \otimes \sigma_Y$ such that $H_{\min}(X|E) \sigma \geq k_1$, $H_{\min}(Y) \sigma \geq k_2$ and $|X| = |Y| = n'$. Let $Z = \text{IP}_p^n(X, Y)$. Then,
\[
\| \sigma_{ZE} - U_m \otimes \sigma_X \|_1 \leq \epsilon,
\]
for parameters $k_1 + k_2 \geq n' + m + 40 + 8 \log \left( \frac{1}{\epsilon} \right)$.

**Proof:** Let $X \in X, Y \in Y$ such that $X = Y = \mathbb{F}_p^n$. The result follows from Fact 30 and noting that $\text{IP}_p^n$ is both $X$-two-wise independent function and $Y$-two-wise independent function.

**IV. qma CAN SIMULATE OTHER ADVERSARIES**

We show how qma can simulate all adversaries known in the literature and qca as well. By simulation we mean that the quantum side information of an adversary can be generated by qma. More precisely,

**Definition 22 (Simulation):** Let $\rho_{XEY}$ be the final state generated appropriately in the adversary model, adversary holds $\rho_E$. We say $\rho_{XEY}$ can be simulated by qma for parameter $l$, if there exists an $l$-qma-state, $\Phi_{XN'M'Y}$ (qma gets registers $EM'$) and $\Phi_{XYE} = \rho_{XEY}$. Analogously, we say $\rho_{XEY}$ can be simulated $\epsilon$-approximately by qma for parameter $l$, if there exists an $l$-qma-state, $\Phi_{XN'M'Y}$ and $\Phi_{XYE} \approx \epsilon \rho_{XYE}$.

**Theorem 6:** Quantum side information of $(b_1, b_2)$-qbsa (see Definition 23), $(k_1, k_2)$-qia (see Definition 24), $(k_1, k_2)$-qca (see Definition 25) acting on an $(n, k_1, k_2)$-source can be simulated by an $l$-qma for some $l \leq \min \{b_1, b_2\} + 2n - k_1 - k_2, l \leq 2n - k_1 - k_2, l \leq 2n - k_1 - k_2$.

**Quantum side information of $(k_1, k_2)$-Q Mara (see Definition 26) and $(k_1, k_2)$-qca (see Definition 4) can be simulated $\epsilon$-approximately by an $l$-qma for some $l \leq 2n - k_1 - k_2 + 25 + 6 \log(1/\epsilon)$.

**Proof:** The proof follows from Claims 4, 5, 6, 7 and 8.

**IV. A. Quantum Bounded Storage Adversary**

Kasher and Kempe [1] introduced the quantum bounded storage adversary (qbsa) model, where the adversary obtains quantum side information of bounded memory from both sources.

**Definition 23 ($(b_1, b_2)$-qbsa [1]):** Let $\tau_{X', Y'}$ be the canonical purifications of independent sources $X, Y$ respectively (registers $XY$ with Reference).

1. Alice and Bob hold $X, Y$ respectively. They also share an entangled pure state $\phi_{NM}$ (Alice holds $N$, Bob holds $M$).
2. Alice applies a CPTP map $\psi_A : \mathcal{L}(\mathcal{H}_X \otimes \mathcal{H}_N) \to \mathcal{L}(\mathcal{H}_X \otimes \mathcal{H}_{N'})$ and Bob applies a CPTP map $\psi_B : \mathcal{L}(\mathcal{H}_Y \otimes \mathcal{H}_M) \to \mathcal{L}(\mathcal{H}_Y \otimes \mathcal{H}_{M'})$. Let
\[
\rho_{X'N'M'Y'} = (\psi_A \otimes \psi_B) (\tau_{X'N'M'Y'}) = (\psi_A \otimes \psi_B) (\tau_{XY} \otimes \phi_{NM} \otimes \tau_{Y'}) \approx \rho_{X'N'M'Y'}.
\]
3. Adversary gets access to $\rho_{N'M'}$ with $\log \dim(\mathcal{H}_{N'}) \leq b_1, \log \dim(\mathcal{H}_{M'}) \leq b_2$.\footnote{This amounts to giving more quantum side information $(ME)$ than other adversary model provide $(E)$.}
We show how to simulate a \((b_1, b_2)\)-qbsa in the model of an \(l\)-qma.

**Claim 4:** A \((b_1, b_2)\)-qbsa acting on an \((n, k_1, k_2)\)-source can be simulated by an \(l\)-qma for some \(l \leq 2\min\{b_1, b_2\} + 2n - k_1 - k_2\).

**Proof:** Let \(V_A : \mathcal{H}_X \otimes \mathcal{H}_N \to \mathcal{H}_X \otimes \mathcal{H}_{N'} \otimes \mathcal{H}_N\), \(V_B : \mathcal{H}_Y \otimes \mathcal{H}_M \to \mathcal{H}_Y \otimes \mathcal{H}_M' \otimes \mathcal{H}_M\), be the Stinespring isometry extensions of CPTP maps \(\psi_A, \psi_B\) respectively i.e. 
\[
\psi_A(\theta) = Tr_{\mathcal{X}N}(V_A(\theta V_A^\dagger))
\]
for every state \(\theta_{XN}\) and \(\psi_B(\theta) = Tr_{\mathcal{Y}M}(V_B(\theta V_B^\dagger))\) for every state \(\theta_{YM}\). Let 
\[
\rho_{A_{X^N'N'M}'M'} = (V_A \otimes 1)(\tau_{XX} \otimes \phi_{NM})(V_A \otimes 1)^\dagger
\]
and 
\[
\rho_{X^N'M^{'N}'M'M'YY} = (V_A \otimes V_B)(\tau_{XX} \otimes \phi_{NM} \otimes \tau_{YY})(V_A \otimes V_B)^\dagger.
\]
Note \(\rho_{A_{X^N'N'M}'M'}\) is such that \(\rho_{A_{X^N'N'M}^{'M'}} = \tau_{XX} \otimes \phi_{MM}\). Thus, from Fact 5, we have 
\[
I_{\min}(\hat{X} : N'M')_{\rho^A} \leq 2\log(\dim(\mathcal{H}_N)) \leq 2b_1. \]
Let \(\sigma_{N'M'}\) be such that 
\[
D_{\max}(\rho_{N'M'}^A \| \rho_{N'M'}^\sigma) \leq 2b_1.
\]
Also, note \(\rho_{A_X^N} = \tau_{XX} \leq 2^{-k_1}I_{XX}\). The inequality follows since the min-entropy of \(\tau_{XX}\) is at least \(k_1\) and \(\tau_{XX}\) is canonical purification of \(\tau_{XX}\). Thus, we further have 
\[
D_{\max}(\rho_{A_{X^N'N'M}^{'M'}} \| I_{X} \otimes \sigma_{MN'}) \leq 2b_1 - k_1.
\]
Thus \(H_{\min}(X|N'M')_{\rho^A} = H_{\min}(\hat{X} : N'M')_{\rho^A} \geq k_1 - 2b_1\). Note the first equality is because \(\rho_{A_{X^N'N'M}^{'M'}} = \rho_{A_{X^N'N'M}^{'M'}}^\sigma\). Using Fact 8, we further have 
\[
H_{\min}(X|N'M'M'YY) \geq H_{\min}(X|N'M')_{\rho^A} \geq k_1 - 2b_1.
\]
Note 
\[
D_{\max}(\rho_{X^N'M'YY} \| U_{YY} \otimes \rho_{X^N'M'}) \leq n - k_2 \quad \text{since} \quad \rho_{YX^N'M'} = \tau_{YY} \otimes \rho_{X^N'M'}, \quad \text{the min-entropy of} \quad \tau_{YY} \quad \text{is at least} \quad k_2 \quad \text{and} \quad \tau_{YY} \quad \text{is canonical purification of} \quad \tau_{YY}.
\]
Thus 
\[
H_{\min}(Y|XX^N'M')_{\rho} = H_{\min}(Y|XX^N')_{\rho} \geq k_2.
\]
Note the first equality is because \(H_{\min}(Y|XX^N')_{\rho} = H_{\min}(Y|XX^N')_{\rho}\). Simulation of the state \(\rho\) in the model of \(l\)-qma follows from Lemma 1. Using Lemma 1, with the following assignment of registers (below the registers on the left are from Lemma 1 and the registers on the right are the registers in this proof) 
\[
(X, Y, \hat{X}, \hat{Y}, N, M, \rho) \leftarrow (X, Y, \hat{X}, \hat{Y}, \hat{N}', \hat{N}', \hat{N}', M'M', \rho),
\]
we have \(l \leq 2n + 2b_1 - k_1 - k_2\).

A similar argument can be given by exchanging the roles of Alice and Bob. The desired follows.

As a corollary, we reproduce the security of one-bit output inner-product against \((b_1, b_2)\)-qbsa acting on \((n, k_1, k_2)_\text{source from [1]}\) as follows.

**Corollary 8 [1]:** An \((n, n, 1)_\text{2-source extractor IP}_2^n : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}\) is \((b_1, b_2, \varepsilon)_\text{quantum secure against qbsa on} (n, k_1, k_2)_\text{source for parameters} k_1 + k_2 - 2\min\{b_1, b_2\} \geq n + 4 + 8\log(1/\varepsilon)\).

**Proof:** The proof follows from Claim 4 (noting \(l\)-qma is also a \((k_1 - 2b_1, k_2)\)-qia or \((k_1, k_2 - 2b_2)\)-qqa) and Corollary 6.

\[\]
C. General Entangled Adversary

Chung et al. [2] introduced general entangled adversary (gaa) defined as follows:

**Definition 25** ((k₁, k₂)-gaa, (k₁, k₂)-gaa-state [2]): Let τₓᵧ, τᵧᵧ be the canonical purifications of independent sources X, Y respectively (registers ḳ ᴵ  ᴹ with Reference).

1) Alice and Bob hold X, Y respectively. They also hold entangled pure state φₓᵧ (Alice holds X, Bob holds Y).
2) Alice applies a CPTP map ψₐ : L(Hₓ ⊗ Hᵧ) → L(Hₓ ⊗ Hᵧ) and Bob applies a CPTP map ψₗ : L(Hᵧ ⊗ Hᵧ) → L(Hᵧ ⊗ Hᵧ).

Consider, with the following assignment of registers (below the registers on the left are from Lemma 1 and the registers on the right are the registers in this proof)

\([X, Y, X, Y, Y, N, M, \rho] \leftarrow (X, Y, X, Y, Y, N', M', \rho),\]

we have \(l \leq 2n - k₁ - k₂\).

D. Quantum Markov Adversary

Arnon-Friedman et al. [3] introduced quantum Markov adversary (qMara), such that adversary’s side information forms a Markov-chain with both sources.

**Definition 26** ((k₁, k₂)-qMara, (k₁, k₂)-qMara-state [3]): Let \(\rho_{XEY}^{T} \) be a Markov-chain (X, E, Y), with \(H_{\min}(X|E|) ≥ k₁ \) and \(H_{\min}(Y|E|) ≥ k₂\). The state \(\rho\) is called a (k₁, k₂)-qMara-state.

**Claim 7:** A (k₁, k₂)-qMara-state can be simulated \(\varepsilon\)-approximately by an l-qma for some \(l ≤ 2n - k₁ - k₂ + 25 + 6 \log(1/\varepsilon)\).

**Proof:** From Fact 12,

\(\rho_{XEY} = \sum_{t} \text{Pr}(T = t)|t⟩⟨t| \otimes (\rho_{XEt}^{T} \otimes \rho_{YEt}^{T})\),

where \(T\) is some classical register over finite alphabet. Let \(\rho_{XN'T'YEt'12}^{A} \) be a pure state extension of \(\rho_{XEY}^{T}\) such that,

\[\rho_{XN'T'YEt'12}^{A} = \sum_{t} \sqrt{\text{Pr}(T = t)}|t⟩⟨t| \otimes (\rho_{XEt}^{A} \otimes \rho_{YEt}^{A})\]

registers (X, Y, T) are classical (with copies X ᴵ ᴹ ᴶ ᴹ ᴹ ᴶ) and \(|t⟩\) is an optimal canonical purification of \(\rho_{XEt}^{A}, \rho_{YEt}^{A}\) respectively. Since \(E \equiv E_{T}T_{E}\), using Fact 11, we have

\[H_{\min}(X|E|) ≥ k₁ \; ; \; H_{\min}(Y|E|) ≥ k₂.\]

Consider,

\[H_{\min}(X|Y|E_{t}E_{t}^{T}) ≥ H_{\min}(X|Y|E_{t}E_{t}^{T}),\]

where \(T\) is the first equality is because conditioned on \(E_{t}\) fixed, \(\rho_{XN'T'YEt'12} = \rho_{XN'T'YEt'12}^{A}\). The first inequality follows from Fact 8 and second inequality follows from Eq. (1). Consider,

\[H_{\min}(X|Y|E_{t}E_{t}^{T}) ≥ H_{\min}(X|Y|E_{t}E_{t}^{T}),\]

\[H_{\min}(Y|E_{t}E_{t}^{T}) ≥ k₂.\]
The first equality is because conditioned on every \( \hat{T} = t \), 
\[ \rho_{Y \hat{E}_1 \hat{E}_2 X \hat{X}}^t = \rho_{Y \hat{E}_2} \otimes \rho_{\hat{E}_1 \hat{E}_2 X \hat{X}}^t. \]
The second equality is because \( \rho_{Y \hat{E}_2} \otimes \rho_{\hat{E}_1 \hat{E}_2 X \hat{X}}^t \). The first inequality follows from Fact 8 and second inequality follows from Eq. (2).

For the state \( \rho \) with the following assignment (on the left are from Definition 10 and on the right are from here),
\[ (X, \hat{X}, N, M, Y, \hat{Y}) \leftarrow (X, \hat{X}, \hat{E}_2 \hat{E}_1 T, E_2 E_1 T, Y, \hat{Y}), \]
we have \( \rho \) is a \((k_1, k_2)\)-qpa-state. Using Fact 2, we have an \(l\)-qma-state \( \rho' \) such that \( l \leq 2n - k_1 - k_2 + 25 + 6 \log(1/\varepsilon) \) and \( \rho' \approx \rho \).

**E. Quantum Communication Adversary**

We show how to simulate a \((k_1, k_2)\)-qca (see Definition 4) in the model of an \(l\)-qma.

**Claim 8:** A \((k_1, k_2)\)-qca-state can be simulated \( \varepsilon \)-approximately by an \(l\)-qma for some \( l \leq 2n - k_1 - k_2 + 25 + 6 \log(1/\varepsilon) \).

**Proof:** Let \( \Phi_{X, \hat{X}, N'X'Y'Y'} \) be the end state after the action of \((k_1, k_2)\)-qca (adversary gets registers either \(M'Y' \) or \(N'X' \) of his choice).

We note to the reader that every \((k_1, k_2)\)-qca-state is a \((k_1, k_2)\)-qpa-state. Now using Fact 2, we have an \(l\)-qma-state \( \rho' \) such that \( l \leq 2n - k_1 - k_2 + 25 + 6 \log(1/\varepsilon) \) and \( \rho' \approx \rho \).

This completes the proof.

**V. A Quantum Secure Weak-Seeded Non-Malleable Extractor and Privacy-Amplification**

**A. A Quantum Secure Weak-Seeded Non-Malleable Extractor**

**Theorem 7:** Let \( p \neq 2 \) be a prime, \( n \) be an even integer and \( \varepsilon > 0 \). The function \( \text{nmExt}(X, Y) \) as defined in Definition 9 is a \((k_1, k_2)\)-quantum secure weak-seeded non-malleable extractor against qmna for the parameters \( k_1 + k_2 \geq (n + \log \log 2) \).

**Proof:** Let \( \rho \) be a \((k_1, k_2)\)-qmna-state. From [6] (see Theorem 1), to show,
\[ \| \rho_{\text{nmExt}(X, Y)} \otimes \rho_{\text{nmExt}(X', Y') \otimes Y'M'} - U_{\log p} \otimes \rho_{YY'M'} \|_1 \leq \varepsilon, \]
for \( \text{nmExt}(X, Y) \) as defined in Definition 9 it is enough to show,
\[ \| \rho_{(X, g(Y, Y') \otimes Y'M') - U_{\log p} \otimes \rho_{YY'M'} \|_1 \leq \frac{2 \varepsilon^2}{p^2}, \]
where \( g: \mathbb{F}_p^{n/2} \times \mathbb{F}_p^{n/2} \rightarrow \mathbb{F}_p^{n} \) is an (appropriately defined) function such that for any \( z \in \mathbb{F}_p^{n} \) there are at most two possible pairs \((y, y')\) and \( y \neq y'\) such that \( g(y, y') = z \). Let \( U: \mathbb{H}_Y \otimes \mathbb{H}_Y' \rightarrow \mathbb{H}_Y \otimes \mathbb{H}_Y' \otimes \mathbb{H}_Z \otimes \mathbb{H}_Z \) be a safe isometry such that \( Z = g(Y, Y') \).

Let \( \theta = U_{\rho M'Y'Y'} \). Noting \( \theta_{X'Y'M'Y'} = \rho_{XM'Y'Y'} \), we have \( \| \|\theta_{(X, g(Y, Y') \otimes Y'M') - U_{\log p} \otimes \rho_{YY'M'} \|_1 = \| \theta_{(X, g(Y, Y') \otimes Y'M') - U_{\log p} \otimes \rho_{YY'M'} \|_1 \| \leq \frac{2 \varepsilon^2}{p^2}, \]
for parameters \( k_1 + k_2 \geq (n + \log \log 2) \).

**B. Privacy-Amplification With Local Weak-Sources**

Let \( n, m, d, l \) be positive integers and \( k_1, k_2, \varepsilon, \delta > 0 \). We start with the definition of a quantum secure privacy-amplification protocol against active adversaries. The following description is from [6]. A privacy-amplification protocol \( (P_1, P_2) \) is defined as follows. If the protocol is executed by two parties Alice and Bob sharing a secret \( X \in \{0,1\}^n, \)
whose actions are described by \( P_A, P_B \) respectively. In addition there is an active, computationally unbounded adversary Eve, who might have some quantum side information \( E \) correlated with \( X \) but satisfying \( H_{min}(X|E) \rho \geq k \), where \( \rho_{XE} \) denotes the initial state at beginning of the protocol.

Informally, the goal for the protocol is that whenever a party (Alice or Bob) does not reject, the key \( R \) output by this party is random and statistically independent of Eve’s view. Moreover, if both parties do not reject, they must output the same keys \( R_A = R_B \) with overwhelming probability.

More formally, we assume that Eve is in full control of the communication channel between Alice and Bob, and can arbitrarily insert, delete, reorder or modify messages sent by Alice and Bob to each other. At the end of the protocol, Alice outputs a key \( R_A \in \{0,1\}^l \cup \{\perp\} \), where \( \perp \) is a special symbol indicating rejection. Similarly, Bob outputs a key \( R_B \in \{0,1\}^l \cup \{\perp\} \). For a random variable \( R \in \{0,1\}^l \cup \{\perp\} \), let \( \Pr[R] \) be a random variable on \( l \)-bit strings that is deterministically equal to \( \perp \) if \( R = \perp \), and is otherwise uniformly distributed over \( \{0,1\}^l \). The following definition generalizes the classical definition in [59].

**Definition 27:** Let \( k, l \) be integer and \( \varepsilon > 0 \). A privacy-amplification protocol \( (P_A, P_B) \) is a \((k, l, \varepsilon)\)-privacy-amplification protocol secure against active quantum adversaries if it satisfies the following properties for any initial state \( \rho_{XE} \) such that \( H_{min}(X|E) \rho \geq k \), and \( \sigma \) being the joint state of Alice, Bob and Eve at the end of the protocol given by \( (P_A, P_B) \) including \( \text{purify}(R_A) \) and \( \text{purify}(R_B) \).

1) **Correctness.** If the adversary does not interfere with the protocol, then \( \Pr[R_A = R_B \land R_A \neq \perp \land R_B \neq \perp] = 1 \).

2) **Robustness.** This property states that even in the presence of an active adversary, \( \Pr[R_A \neq R_B \land R_A \neq \perp \land R_B \neq \perp] \leq \varepsilon \).

3) **Extraction.** Let \( \sigma_E \) be the final quantum state possessed by Eve (including the transcript of the protocol). The following should hold:

\[
\left\| \sigma_{R_A E} - \sigma_{\text{purify}(R_A)E} \right\|_1 \leq \varepsilon \quad \text{and} \quad \left\| \sigma_{R_B E} - \sigma_{\text{purify}(R_B)E} \right\|_1 \leq \varepsilon.
\]

In other words, whenever a party does not reject, the party’s key is (approximately) indistinguishable from a fresh random string to the adversary.

The quantity \( k - l \) is called the **entropy loss**.

1) **Our Protocol:** In Protocol 1, we describe a slight modification of the DW protocol [7], that achieves PA in the setting where Alice and Bob only have weak local randomness \( A \) and \( B \) respectively, such that \( A, B, (X, E) \) are independent. Let \( A \) be \((n/2, k_1)\)-source and \( B \) be \((n, k_2)\)-source. We need the following primitives.

- Let \( \text{nmExt} : \{0,1\}^n \times \{0,1\}^{n/2} \rightarrow \{0,1\}^{2m} \) be a \((k, k_1, \varepsilon)\)-quantum secure \((n, n/2, 2m)\)-weak-seeded non-malleable extractor against qma. Then we have from Theorem 7,

\[
k + k_1 \geq n + 34m + 33 + 16 \log \left( \frac{1}{\varepsilon} \right).
\]

- Let \( \text{Ext} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m \) be \( \text{IP}_{2m}^{/m} \). For any state \( \sigma_{XE} \) such that \( \sigma_{XE} = \sigma_X \otimes \sigma_E \), \( H_{min}(X|E) \rho \geq k \) and \( H_{min}(B) \rho \geq k_2 \), we have

\[
\left\| \sigma_{\text{Ext}(X,E)} - U_m \otimes \sigma_{XE} \right\|_1 \leq \varepsilon,
\]

for the parameters \( k + k_2 \geq n + m + 40 + 8 \log \left( \frac{1}{\varepsilon} \right) \) from Corollary 7.

- Let \( \text{MAC} : \{0,1\}^{2m} \times \{0,1\}^m \rightarrow \{0,1\}^m \) be a one-time \( 2^{-m} \)-information-theoretically secure message authentication code from Fact 28 for \( m = O \left( \log^3 \left( \frac{1}{\varepsilon} \right) \right) \). Note \( 2^{-m} \leq \varepsilon \).

- Let \( \text{Tre} : \{0,1\}^n \times \{0,1\}^m \rightarrow \{0,1\}^l \) be a \((2l, \varepsilon)\)-quantum secure strong \((n, m, l)\)-seeded extractor for \( m = O \left( \log^3 \left( \frac{1}{\varepsilon} \right) \right) \) from Fact 27. Taking \( l = (1 - \delta)k \) for any small constant \( \delta > 0 \) suffices for the privacy-amplification application.

In Protocol 1, there are only two messages exchanged, \( A \) from Alice to Bob and \((W', T')\) from Bob to Alice. To each of these messages the adversary may apply an arbitrary transformation, that may depend on its side information.

**Definition 28** (Active Attack): An active attack against PA protocol is described by 3 parameters.

- A c-q state \( \rho_{XE} \) (of adversary choice) such that \( H_{min}(X|E) \rho \geq k \).
- A CPTP map \( T_1 : \mathcal{H}_E \otimes \mathcal{H}_A \rightarrow \mathcal{H}_E \otimes \mathcal{H}_A \otimes \mathcal{H}_A' \).
- A CPTP map \( T_2 : \mathcal{H}_E \otimes \mathcal{H}_W \otimes \mathcal{H}_T \rightarrow \mathcal{H}_E' \otimes \mathcal{H}_W' \otimes \mathcal{H}_T' \otimes \mathcal{H}_W \otimes \mathcal{H}_T \).

**Theorem 8:** For any active attack \((\rho_{XE}, T_1, T_2)\), Protocol 1 is \((k, (1 - \delta)k, O(\varepsilon))\)-secure as defined in Definition 27 as long as

\[
\begin{align*}
k + k_1 &\geq n + m + 40 + 8 \log \left( \frac{1}{\varepsilon} \right) ; \\
k + k_1 &\geq n + 34m + 33 + 16 \log \left( \frac{1}{\varepsilon} \right) ; \\
m &\geq O \left( \log^3 \left( \frac{1}{\varepsilon} \right) \right).
\end{align*}
\]

**Proof:** The security of Protocol 1 follows from the observation that the protocol is nearly identical to that in [6] and [18]. There are two main differences:

- The seed \( A \) for the non-malleable extractor is a weak-source. This is secure via Theorem 7.
- In the protocol from [6] and [18], Bob has immediate access to uniform \( W' \). Here, we obtain \( W' \) using strong extractor property of inner-product from Corollary 7. Since \( B \) is independent of \( X, A \), we get that \( W' \) is independent of \( X, A \), and hence independent of \( X, S \), which is required in the proof of security in [6] and [18].

We refer the reader to Appendix.D of [18] for the complete proof of privacy-amplification when the sources \( A, B \) are completely uniform. The proof of security follows similar to that of [18] privacy-amplification protocol, with the following assignment of terms (terms on left are from

---

7It is not necessary for the definition to specify exactly how the protocols are formulated; informally, each player’s actions is described by a sequence of efficient algorithms that compute the player’s next message, given the past interaction.
C. Open Questions

1) We have shown that the inner-product function is secure against qma. It is natural to ask if the other known 2-source extractors are secure against qma. For example is Bourgain’s extractor [10], which works for 2-sources with min-entropy \((\frac{1}{2} - \delta)n\) (for constant \(\delta\)), secure against qma?

2) Are the multi-source extractor constructions of [5], [13], [33], [34], [35], [36], [38], and [39] secure against a natural multi-source extension of qma?

3) We have shown the security of Li’s non-malleable extractor against quantum side information. Recently [18] have shown another non-malleable extractor secure against quantum side information in the 2-source setting. Several near optimal non-malleable extractor constructions are known in the classical setting, for example constructions of [5], [39], and [60]. Are they secure against quantum side information?

ACKNOWLEDGMENT

The work of Naresh Goud Boddu was done while he was a graduate student at the Centre for Quantum Technologies, NUS, Singapore.

REFERENCES

[1] 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.

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

[3] R. Arnon-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: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016, p. 2.

[4] B. Chor and O. Goldreich, “Unbiased bits from sources of weak randomness and probabilistic communication complexity,” in Proc. 26th Annu. Symp. Found. Comput. Sci. (SFCS), 1985, pp. 429–442.

[5] X. Li, “Non-malleable extractors, two-source extractors and privacy amplification,” in Proc. IEEE 53rd Annu. Symp. Found. Comput. Sci., Oct. 2012, pp. 688–697.

[6] D. Aggarwal, K.-M. Chung, H.-H. Lin, and T. Vidick, “A quantum-proof non-malleable extractor,” in Advances in Cryptology—EUROCRYPT, Y. Ishai and V. Rijmen, Eds. Cham, Switzerland: Springer, 2019, pp. 442–469.

[7] Y. Dodis and D. Wichs, “Non-malleable extractors and symmetric key cryptography from weak secrets,” in Proc. 41st Annu. ACM Symp. Theory Comput. New York, NY, USA: Association for Computing Machinery, May 2009, pp. 601–610.

[8] D. Zuckerman, “General weak random sources,” in Proc. 31st Annu. Symp. Found. Comput. Sci., vol. 2, 1990, pp. 534–543.

[9] R. Shaltiel, “Recent developments in explicit constructions of extractors,” Bull. EATCS, vol. 77, pp. 67–95, 2002.

[10] J. Bourgain, “More on the sum-product phenomenon in prime fields and its applications,” Int. J. Number Theory, vol. 1, no. 1, pp. 1–32, Mar. 2005.

[11] Y. T. Kalai, X. Li, A. Rao, and D. Zuckerman, “Network extractor protocols,” in Proc. 49th Annu. IEEE Symp. Found. Comput. Sci., Oct. 2008, pp. 654–663.

[12] A. Rao, “Extractors for a constant number of polynomially small min-entropy independent sources,” in Proc. 38th Annu. ACM Symp. Theory Comput. New York, NY, USA: Association for Computing Machinery, May 2006, pp. 497–506.

[13] R. Raz, “Extractors with weak random seeds,” in Proc. 37th Annu. ACM Symp. Theory Comput., May 2005, pp. 11–20.

[14] Y. T. Kalai, X. Li, and A. Rao, “2-source extractors under computational assumptions and cryptography with defective randomness,” in Proc. 50th Annu. IEEE Symp. Found. Comput. Sci., Oct. 2009, pp. 617–626.

[15] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf, “Exponential separations for one-way quantum communication complexity, with applications to cryptography,” in Proc. 39th Annu. ACM Symp. Theory Comput. New York, NY, USA: Association for Computing Machinery, Jan. 2007, pp. 516–525.

[16] J. S. Bell, “On the Einstein Podolsky Rosen paradox,” Physica, vol. 1, no. 3, pp. 195–200, 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] N. Goud Boddu, R. Jain, and U. Kapshikar, “Quantum secure non-malleable-extractors,” 2021, arXiv:2109.03097.

[19] C. H. Bennett, G. Brassard, and J.-M. Robert, “Privacy amplification by public discussion,” SIAM J. Comput., vol. 17, no. 2, pp. 210–229, Apr. 1988.

[20] U. M. Maurer, “Conditionally-perfect secrecy and a provably-secure randomized cipher,” J. Cryptol., vol. 5, no. 1, pp. 53–66, Jan. 1992.

[21] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, “Generalized privacy amplification,” IEEE Trans. Inf. Theory, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[22] U. Maurer and S. Wolf, “Privacy amplification secure against active adversaries,” in Advances in Cryptology—CRYPTO, B. S. Kaliski, Ed. Berlin, Germany: Springer, 1997, pp. 307–321.
