Interactive Leakage Chain Rule for Quantum Min-entropy

Ching-Yi Lai and Kai-Min Chung

Abstract

The leakage chain rule for quantum min-entropy quantifies the change of min-entropy when one party gets additional leakage about the information source. Herein we provide an interactive version that quantifies the change of min-entropy between two parties, who share an initial classical-quantum state and are allowed to run a two-party protocol. As an application, we prove new versions of lower bounds on the complexity of quantum communication of classical information.

I. INTRODUCTION

Let \((X, Y, Z)\) be a classical distribution over \(\{0, 1\}^n \times \{0, 1\}^m \times \{0, 1\}^\ell\). (Classical) leakage chain rule states that

\[ H(X|Y, Z) \geq H(X|Y) - \ell, \]

which says that an \(\ell\)-bit “leakage” \(Z\) can decrease the entropy of \(X\) (conditioned on \(Y\)) by at most \(\ell\). Note that the statement is different from the standard chain rule for Shannon entropy that \(H(X, Y) = H(X) + H(Y|X)\). Leakage chain rule generally holds for various entropy notions and is especially useful for cryptographic applications. In particular, a computational leakage chain rule for computational min-entropy, first proved by [1], [2], has found several applications in classical cryptography [3], [4], [5], [6], [7].

The notion of (smooth) min- and max- entropies in the quantum setting are proposed by Renner and Wolf [8]. The leakage chain rule for quantum min-entropy has also been discussed and is more complicated than its classical analogue due to the effect of quantum entanglement. Consider a state \(\rho_{XYZ}\) on the state space \(\mathcal{X} \otimes \mathcal{Y} \otimes \mathcal{Z}\), where \(\mathcal{Z}\) is an \(\ell\)-qubit system. The leakage chain for quantum min-entropy states that

\[
H_{\text{min}}(X|Y, Z)_{\rho} \geq \begin{cases} 
H_{\text{min}}(X|Y)_{\rho} - \ell, & \text{if } \rho \text{ is a separable state on } (\mathcal{X} \otimes \mathcal{Y}) \text{ and } \mathcal{Z} \\
H_{\text{min}}(X|Y)_{\rho} - 2\ell, & \text{otherwise.}
\end{cases}
\]

In other words, the leakage \(Z\) can decrease the quantum min-entropy of \(X\) conditioned on \(Y\) by at most \(\ell\) if there is no entanglement, and \(2\ell\) in general. Note that the factor of 2 is tight by the application of superdense coding [9]. The separable case is proved by Desrosiers and Dupuis [10], and the general case is proved by Winkler et al. [11], both of which are motivated by cryptographic applications. Furthermore, a computational version of quantum leakage chain rule is explored in [12] with applications in quantum leakage-resilient cryptography.

Herein we formulate an interactive version of leakage chain rule with initial classical-quantum (cq) states. Let \(\rho_{XY}\) be a cq-state shared between Alice and Bob. Consider that \(X\) is a classical input that remains constant during the interaction. This is formalized by allowing Alice to perform only quantum operations controlled by \(X\) on her system.

**Theorem 1.** [Interactive leakage chain rule for quantum min-entropy] Suppose Alice and Bob share a cq state \(\rho = \rho_{XY} \in D(\mathcal{X} \otimes \mathcal{Y})\), where Alice holds the classical system \(X\) and Bob holds the quantum system \(Z\). If an interactive protocol \(\Pi\) is executed by Alice and Bob and \(m_B\) and \(m_A\) are the total numbers of qubits that Bob and Alice send to each other, respectively, then

\[
H_{\text{min}}(X|Y)_{\sigma} \geq H_{\text{min}}(X|Y)_{\rho} - \min\{m_B + m_A, 2m_A\},
\]

where \(\sigma_{XY} = \Pi(\rho_{XY})\) is the joint state at the end of the protocol.

It is interesting to discuss the implication of Theorem 1 to Holevo’s problem of conveying classical messages by transmitting quantum states. In the interactive setting, Cleve et al. [13] and Nayak and Salzman [14] showed that for Alice to reliably communicate \(n\) bits of classical information to Bob, roughly \(n\) qubits of total communication and \(n/2\) qubits of one-way communication from Alice to Bob are necessary. The same conclusion follows immediately from Theorem 1.

CYL is with the Institute of Communications Engineering, National Chiao Tung University, Hsinchu 30010, Taiwan. (email: cylai@nctu.edu.tw)

KMC is with the Institute of Information Science, Academia Sinica, Nankang, Taipei 11529, Taiwan. (email: kmchung@iis.sinica.edu.tw)
In fact, in the case without initial shared cq-states, the general form of the result in [14] (Theorem 1.4) agrees to the above interactive leakage chain rule. Thus our interactive leakage chain rule can be viewed as a generalization of [14] to allow initial correlation between $X$ and $Y$. We remark that our proof is not a generalization of the proof in [14], although we both used Yao’s lemma [15]. Conceptually, the use of interactive leakage chain rule makes the proof simple.

This manuscript is organized as follows. In Sec. [III] we give some basics about quantum information. Then we discuss the leakage chain rule for quantum min-entropy and its application to the problem of communicating classical information in Sec. [III].

II. Preliminaries

We give notation and briefly introduce basics of quantum mechanics here. The Hilbert space of a quantum system $A$ is denoted by the corresponding calligraphic letter $A$, and its dimension is denoted by $d_A$. Let $L(A)$ be the space of linear operators on $A$. A quantum state of system $A$ is described by a density operator $\rho_A \in L(A)$ that is positive semidefinite and with unit trace ($\text{tr}(\rho_A) = 1$). Let $D(A) = \{\rho_A \in L(A) : \rho_A \geq 0, \text{tr}(\rho_A) = 1\}$ be the set of density operators on $A$. When $\rho_A \in D(A)$ is of rank one, it is called a pure quantum state and we can write $\rho = |\psi\rangle_A \langle \psi|$ for some unit vector $|\psi\rangle_A \in A$, where $\langle \psi \rangle = |\psi\rangle^\dagger$ is the conjugate transpose of $|\psi\rangle$. If $\rho_A$ is not pure, it is called a mixed state and can be expressed as a convex combination of pure quantum states.

The evolution of a quantum state $\rho \in D(A)$ is described by a completely positive and trace-preserving (CPTP) map $\Psi : D(A) \rightarrow D(A')$ such that $\Psi(\rho) = \sum_k E_k \rho E_k^\dagger$, where $\sum_k E_k^\dagger E_k = \text{id}_A$. In particular, if the evolution is a unitary $U$, we have the evolved state $\Psi(\rho) = U \rho U^\dagger$.

The Hilbert space of a joint quantum system $AB$ is the tensor product of the corresponding Hilbert spaces $A \otimes B$. Let $\text{id}_A$ denote the identity on system $A$. For $\rho_{AB} \in D(A \otimes B)$, we will use $\rho_A = \text{tr}_B(\rho_{AB})$ to denote its reduced density operator in system $A$, where

$$\text{tr}_B(\rho_{AB}) = \sum_i \text{id}_A \otimes \langle i|_B \rho_{AB} \text{id}_A \otimes |i\rangle_B$$

for an orthonormal basis $\{|i\rangle_B\}$ for $B$. A separable state $\rho_{AB}$ has a density operator of the form

$$\rho_{AB} = \sum_x p_x \rho^x_A \otimes \rho^x_B,$$

where $\rho^x_A \in D(A)$ and $\rho^x_B \in D(B)$. In particular, a classical-quantum (cq) state $\rho_{AB}$ has a density operator of the form

$$\rho_{AB} = \sum_a p_a |a\rangle_A \langle a| \otimes \rho^a_B,$$

where $\{|a\rangle_A\}$ is an orthonormal basis for $A$ and $\rho^a_B \in D(B)$. We define the following specific quantum operations on cq-states that preserve the classical system.

Definition 2. A quantum operation $\Gamma$ on a classical-quantum system $AB$ is said to be controlled by the classical system $A$ if, for a cq state $\rho_{AB} = \sum_a p_a |a\rangle_A \langle a| \otimes \rho^a_B$, $\Gamma(\rho_{AB}) = \sum_a p_a |a\rangle_A \langle a| \otimes \Gamma^a(\rho^a_B)$, where $\Gamma^a$ are CPTP maps. In this case, $\Gamma$ is called a \textit{classically-controlled quantum operation}. In particular, if $\Gamma^a$ are unitaries, $\Gamma$ is called a \textit{classically-controlled unitary}.

Note that the reduced state for classical system $A$ of a cq-state $\rho_{AB}$ remains the same after a classically-controlled quantum operation $\Gamma$. That is, $\text{tr}_B \rho_{AB} = \text{tr}_B \Gamma(\rho_{AB})$.

Lemma 3. [Schmidt decomposition] For a pure state $|\psi\rangle_{AB} \in A \otimes B$, there exist orthonormal states $\{|i\rangle_A\} \in A$ and $\{|i\rangle_B\} \in B$ such that

$$|\psi\rangle_{AB} = \sum_{i=1}^s \lambda_i |i\rangle_A \otimes |i\rangle_B,$$

where $\lambda_i \geq 0$, $s \leq \min\{d_A, d_B\}$, and the smallest such $s$ is called the Schmidt rank of $|\psi\rangle_{AB}$.

Lemma 4. [Purification] Suppose $\rho_A \in D(A)$ of finite dimension $d_A$. Then there exists $B$ of dimension $d_B \geq d_A$ and $|\psi\rangle_{AB} \in A \otimes B$ such that

$$\text{tr}_B |\psi\rangle_{AB} \langle \psi| = \rho_A.$$

The trace distance between two quantum states $\rho$ and $\sigma$ is

$$||\rho - \sigma||_{\text{tr}},$$
where $||X||_{tr} = \frac{1}{2} \text{tr} \sqrt{X^\dagger X}$ is the trace norm of $X$. The fidelity between $\rho$ and $\sigma$ is

$$F(\rho, \sigma) = \text{tr} \sqrt{\rho^{1/2} \sigma \rho^{1/2}}.$$ 

**Theorem 5.** [Uhlmann’s theorem [16]]

$$F(\rho_A, \sigma_A) = \max_{|\phi\rangle} |\langle \phi | \phi' \rangle|,$$

where the maximization is over all purification of $\sigma_A$.

Below is a variant of Uhlmann’s theorem.

**Corollary 6.** Suppose $\rho_A$ is a reduced density operator of $\rho_{AB}$. Suppose $\rho_A$ and $\sigma_A$ have fidelity $F(\rho_A, \sigma_A) \geq 1 - \epsilon$. Then there exists $\sigma_{AB}$ with $\text{tr}_B(\sigma_{AB}) = \sigma_A$ such that $F(\rho_{AB}, \sigma_{AB}) \geq 1 - \epsilon$.

**Proof.** Let $|\psi\rangle_{ABR}$ be a purification of $\rho_{AB}$, which is immediately a purification of $\rho_A$. Suppose $|\phi\rangle$ is a purification of $\sigma_A$ such that $|\langle \psi | \phi \rangle| \geq 1 - \epsilon$. Let $\sigma_{AB} = \text{tr}_R(|\phi\rangle \langle \phi |)$. Then $F(\rho_{AB}, \sigma_{AB}) \geq |\langle \psi | \phi' \rangle| \geq 1 - \epsilon$. \[ \]

A relation between the fidelity and the trace distance of two quantum states $\sigma$ and $\rho$ was proved by Fuchs and van de Graaf [17] that

$$1 - F(\rho, \sigma) \leq ||\rho - \sigma||_{tr} \leq \sqrt{1 - F^2(\rho, \sigma)}.$$ 

(3)

The purified distance is defined as

$$P(\rho, \sigma) = \sqrt{1 - F^2(\rho, \sigma)}.$$ 

(4)

For a one-sided two-party protocol (that is, only one party will have the output), where Alice has no (or little) information about Bob’s input, Lo showed that it is possible for Bob to cheat by changing his input at a later time [18]. The basic idea can be formulated as the following lemma, which is proved by a standard argument using Uhlmann theorem and the Fuchs and van de Graaf inequality [17] (for a proof, see, e.g., [19]).

**Lemma 7.** Suppose $\rho_A, \sigma_A \in \mathcal{A}$ are two quantum states with purifications $|\phi\rangle_{AB}$, $|\psi\rangle_{AB} \in \mathcal{A} \otimes \mathcal{B}$, respectively, and $||\rho_A - \sigma_A||_{tr} \leq \epsilon$. Then there exists a unitary $U_B \in L(\mathcal{B})$ such that

$$|||\phi\rangle_{AB} - \text{id}_A \otimes U_B |\psi\rangle_{AB}||_{tr} \leq \sqrt{2(1 - \epsilon)}.$$

A. Protocol Definition

![An interactive two-party quantum protocol.](image)

We basically follow the definition of two-party quantum protocol [20], [21]. Consider a quantum protocol between two parties $\mathcal{A}$ and $\mathcal{B}$, where the party $\mathcal{A}$ sends the first and the last messages without loss of generality. Such a two-party quantum protocol is defined as follows.

**Definition 8.** (Two-party quantum protocol) An $(r, m_A, m_B)$ protocol $\Pi = (\mathcal{A}, \mathcal{B})$ is a two-party protocol with $r$ rounds of interaction defined as follows:

1. input spaces $A_0$ and $B_0$ for parties $\mathcal{A}$ and $\mathcal{B}$, respectively;
2. memory spaces $A_1, \ldots, A_r$ for $\mathcal{A}$ and $B_1, \ldots, B_r$ for $\mathcal{B}$;
3. communication spaces $\mathcal{X}_1, \ldots, \mathcal{X}_r, \mathcal{Y}_1, \ldots, \mathcal{Y}_{r-1}$;
4. a series of quantum operations $\Phi_1, \ldots, \Phi_r$ for $\mathcal{A}$ and a series of quantum operations $\Psi_1, \ldots, \Psi_r$ for $\mathcal{B}$, where

   \[
   \begin{align*}
   \Phi_1 & : L(A_0) \rightarrow L(A_1 \otimes \mathcal{X}_1); \\
   \Phi_i & : L(A_{i-1} \otimes \mathcal{Y}_{i-1}) \rightarrow L(A_i \otimes \mathcal{X}_i), \ i = 2, \ldots, r; \\
   \Psi_j & : L(B_{j-1} \otimes \mathcal{X}_j) \rightarrow L(B_j \otimes \mathcal{Y}_j), \ j = 1, \ldots, r - 1; \\
   \Psi_r & : L(B_{r-1} \otimes \mathcal{X}_r) \rightarrow L(B_r).
   \end{align*}
   \]
The one-way communication complexities (in terms of qubits) sent from Alice to Bob and from Bob to Alice are \( m_A = \sum_{i=1}^{r} \log d_X \), and \( m_B = \sum_{j=1}^{r} \log d_Y \), respectively. The (total) communication complexity of this protocol is \( m_A + m_B \).

For input state \( \rho \in D(A_0 \otimes B_0 \otimes R) \), where \( R \) is a reference system of dimension \( d_R = d_{A_0}d_{B_0} \), let

\[
[\mathcal{A}^i_1 \otimes \mathcal{B}^i_1^{-1}](\rho) = (\Phi_i \otimes \text{id}_{B_1^{-1,R}})(\Psi_i^{-1} \otimes \text{id}_{A_1^{-1,R}}) \cdots (\Phi_1 \otimes \text{id}_{B_0,R})(\rho),
\]

and let \( \Pi(\rho) = [\mathcal{A}^r_1 \otimes \mathcal{B}^r_1](\rho) \) denote the final state of protocol \( \Pi = (\mathcal{A}, \mathcal{B}) \) on input \( \rho \).

Figure 1 illustrates an interactive two-party quantum protocol. Note that the input state \( \rho_{A_0B_0} \in D(A_0 \otimes B_0) \) may consist of a classical string, tensor products of pure quantum states, or an entangled quantum state, depending on the context of the underlying protocol. For example, a part of it can be EPR pairs shared between Alice and Bob. Also the reference system \( R \) is not shown in Fig. 1.

Remark 9. In the following discussion we will consider a specific two-party protocol, where the input of \( \mathcal{A} \) is a classical system \( A_0 \) that is preserved throughout the protocol and its quantum operations

\[
\Phi_1 : L(A_0) \rightarrow L(A_0 \otimes A_1 \otimes \mathcal{X}_1),
\]

\[
\Phi_i : L(A_0 \otimes A_{i-1} \otimes \mathcal{Y}_{i-1}) \rightarrow L(A_0 \otimes A_i \otimes \mathcal{X}_i), \quad i = 2, \ldots, r
\]

are classically-controlled quantum operations controlled by \( A_0 \).

III. LEAKAGE CHAIN RULE FOR QUANTUM MIN-ENTROPY

We first review the notion of quantum (smooth) min-entropy [8].

Definition 10. Consider a bipartite quantum state \( \rho_{AB} \in D(A \otimes B) \). The min-entropy of \( A \) conditioned on \( B \) is defined as

\[
H_{\text{min}}(A|B)_{\rho} = -\inf_{\sigma_B} \{ \lambda \in \mathbb{R} : \rho_{AB} \leq 2^\lambda \text{id}_A \otimes \sigma_B \}.
\]

When \( \rho_{AB} \) is a cq-state, the quantum min-entropy has an operational meaning in terms of guessing probability [22]. Specifically, if \( H_{\text{min}}(A|B)_{\rho} = k \), then the optimal probability of predicting the value of \( A \) given \( \rho_B \) is exactly \( 2^{-k} \).

The smooth min-entropy of \( A \) conditioned on \( B \) is defined as

\[
H_{\text{min}}^c(A|B)_{\rho} = \sup_{\rho' : P(\rho' , \rho) < \epsilon} H_{\text{min}}(A|B)_{\rho'}.
\]

For simplicity we focus on the discussion of min-entropy and our results can be generalized to smooth min-entropy without much effort.

In cryptography, we would like to see how much (conditional) min-entropy is left in an information source when the adversary gains additional information leakage. This is characterized by the leakage chain rule for min-entropy. In the quantum case, the situation is different due to the phenomenon of quantum entanglement. When two parties share a separable quantum state, this is like the classical case and we have the following leakage chain rule for conditional quantum min-entropy [10]:

Lemma 11. [10] Lemma 7] Let \( \rho = \rho_{AXB} = \sum_k p_k \rho_{AX}^k \otimes \rho_B^k \) be a separable state in \( D(A \otimes X \otimes B) \). Then

\[
H_{\text{min}}(A|XB)_{\rho} \geq H_{\text{min}}(A|B)_{\rho} - \log d_X.
\]

Winkler et al. [11] proved the leakage chain rule for quantum (smooth) min-entropy for general quantum states with entanglement.

Lemma 12. [11] Lemma 13] Let \( \rho = \rho_{AXB} \) be a quantum state in \( D(A \otimes X \otimes B) \). Then

\[
H_{\text{min}}(A|XB)_{\rho} \geq H_{\text{min}}(A|B)_{\rho} - 2 \log d.
\]

where \( d = \min\{d_A, d_B, d_X\} \).

Lemma 12 only characterizes the entropy loss regarding the one-way communication complexity. We would like to find one that characterizes the two-way communication complexity. First we prove a variant of Yao’s lemma [13] (see also [24] Lemma 4). For our purpose, the formulation is not symmetric in \( \mathcal{A} \) and \( \mathcal{B} \).

Lemma 13. Suppose \( \Pi = (\mathcal{A}, \mathcal{B}) \) is an \((r, m_A, m_B)\) quantum protocol with initial state \( (|x\rangle |0\rangle)_{A_0} \otimes |\xi\rangle_{B_0} \), where \( x \) is a binary string, and that the quantum operations \( \Phi_i \) for \( \mathcal{A} \) are classical-controlled unitaries controlled by \( |x\rangle_{A_0} \), respectively. Then the final state of the protocol can be written as

\[
\sum_{i \in \{0,1\}^{m_A+m_B}} \lambda_i |x\rangle_{A_0} \otimes |\xi_i\rangle_{A_r} \otimes |\zeta_i\rangle_{B_r},
\]
where $\lambda_i \geq 0$; $|\xi_i\rangle_{A_i}$ can be determined by $\Pi$ and $x$; and $|\zeta_i\rangle_{B_i}$ can be determined by $\Pi$ and $|\zeta\rangle_{B_0}$.

**Proof.** We prove it by induction. For simplicity, we will ignore the fixed register $|x\rangle_{A_0}$ in the following and remember that $\Phi_i$ are classically-controlled unitaries controlled by $|x\rangle_{A_0}$. Suppose $\Pi = (\mathcal{A}, \mathcal{B})$ is defined as in Def. 8. Let $m_B^{(i)} = \sum_{j=1}^i \log d_{X_j}$ and $m_A^{(i)} = \sum_{j=1}^i \log d_{X_j}$. The statement is true for the initial state $\rho = |0\rangle_{A_0} \otimes |\zeta\rangle_{B_0}$, which is of rank one. Suppose the statement holds after $k$ rounds. Then,

$$[\mathcal{A}^k_{1} \otimes \mathcal{B}^k_{1}] (\rho) = \sum_{i \in \{0, 1\}^{m_A^{(k)} + m_B^{(k)}}} \lambda_i^{(k)} |\zeta_i^{(k)}\rangle_{A_k} Y_k \otimes |\zeta_i^{(k)}\rangle_{B_k},$$

where we use the superscript $(k)$ to indicate the states $|\xi_i\rangle$, $|\zeta_i\rangle$ or coefficients $\lambda_i$ after $k$ rounds.

Thus

$$\sum_{i \in \{0, 1\}^{m_A^{(k)} + m_B^{(k)}}} \lambda_i^{(k)} |\zeta_i^{(k)}\rangle_{A_k} Y_k \otimes |\zeta_i^{(k)}\rangle_{B_k} = \sum_{i \in \{0, 1\}^{m_A^{(k)} + m_B^{(k)}}} \lambda_i^{(k)} |\zeta_i^{(k)}\rangle_{A_k} Y_k \otimes |\zeta_i^{(k)}\rangle_{B_k}$$

where $(a)$ and $(b)$ are by Schmidt decomposition on $\Phi_{k+1} |\zeta_i^{(k)}\rangle_{A_k} Y_k$ and $\Psi_{k+1} |\zeta_i^{(k)}\rangle_{A_k} Y_k$, respectively, with $\alpha_{i,a}, \beta_{i,a,b} > 0$; in $(c)$ the indexes $i, a$, and $b$ are merged and $\lambda_i^{(k+1)} = \lambda_i^{(k)} \alpha_{i,a} \beta_{i,a,b}$. (We use $a : b$ to denote the concatenation of two strings $a$ and $b$.)

Next we consider a special type of interactive two-party protocol on an input cq-state $\rho = \rho_{AB}$, where the system $A$ is classical and will be preserved throughout the protocol. The interactive leakage chain rule bounds how much the min-entropy $H_{\min}(A|B)_\rho$ can be decreased by an “interactive leakage” generated by applying a two-party protocol $\Pi = \{\mathcal{A}, \mathcal{B}\}$ to $\rho$, where $A$ is treated as a classical input to $\mathcal{A}$ and $B$ is given to $\mathcal{B}$ as part of its initial state.

**Theorem 14.** [Interactive leakage chain rule for quantum min-entropy] Suppose $\rho_{A_0 B_0}$ is a cq-state, where $A_0$ is classical. Let $\Pi = \{\mathcal{A}, \mathcal{B}\}$ be an $(r, m_A, m_B)$ two-party protocol with classically-controlled quantum operations $\Phi_i$ controlled by $A_0$. Let $\sigma_{A_0 A_r B_r} = [\mathcal{A} \otimes \mathcal{B}] (\rho_{A_0 B_0})$ be the final state of the protocol. Then

$$H_{\min}(A_0|B_r)_\sigma \geq H_{\min}(A_0|B_0)_\rho - \min\{m_A + m_B, 2m_A\},$$

(6)

We say that $\sigma_{B_r}$ is an interactive leakage of $A_0$ generated by $\Pi$.

**Proof.** Suppose $\lambda = \log d_A - H_{\min}(A|B)_\rho$. By definition (5) there exists a density operator $\tau_{B_0}$ such that

$$\rho_{A_0 B_0} \leq 2^\lambda \sigma_{A_0} \otimes \tau_{B_0}.$$

Suppose $|\xi\rangle_{B_0 E}$ is a purification of $\tau_{B_0}$ over $B_0 \otimes E$. Without loss of generality, we assume that Alice and Bob have auxiliary quantum systems $R_1, R_2$, respectively, initialized in $|0\rangle_{R_1} |0\rangle_{R_2}$, so that the protocol $\Pi$ can be extended to a protocol $\tilde{\Pi}$ such that the quantum operations of $\tilde{\Pi}$ are unitary operations controlled by $A_0$ for $\mathcal{A}$ and unitaries for $\mathcal{B}$, and

$$tr_{R_1 R_2} \left( \tilde{\Pi}(\rho_{A_0 B_0} \otimes |0\rangle_{R_1} |0\rangle_{R_2}) \right) = \Pi(\rho_{A_0 B_0}).$$

Now initially we have

$$\rho_{A_0 B_0 R_1 R_2} \leq 2^\lambda \sigma_{A_0} (a) \otimes tr_E (|\xi\rangle_{B_0 E} \langle \xi|) \otimes |0\rangle_{R_1} |0\rangle_{R_2}$$

and

$$\rho_{A_0 B_0 R_1 R_2} \leq 2^\lambda \sigma_{A_0} (a) \otimes |0\rangle_{A_0} (a) \otimes tr_E (|\xi\rangle_{B_0 E} \langle \xi|) \otimes |0\rangle_{R_1} |0\rangle_{R_2}.$$
After the protocol the inequality becomes

\[
\sigma_{A_0 B_r} = \text{tr}_{A_r R_2} \sigma_{A_0 B_r R_1 R_2} \leq \frac{2^\lambda}{d_{A_0}} \sum_a |a\rangle A_0 \langle a| \otimes \text{tr}_{E_2} \left( |\xi_i\rangle B_{0E} \langle \xi_i| \otimes |0\rangle R_1 \langle 0| \right) \\
= \frac{2^\lambda}{d_{A_0}} \sum_a |a\rangle A_0 \langle a| \otimes \text{tr}_{E_2} \left( \Pi \otimes \text{id}_{E} \left( |\xi_i\rangle B_{0E} \langle \xi_i| \otimes |0\rangle R_1 \langle 0| \right) \right) \\
= \frac{2^\lambda}{d_{A_0}} \sum_a |a\rangle A_0 \langle a| \otimes \text{tr}_{E_2} \left( \sum_{i=1}^{2^m_A + m_B} \lambda_i^2 |\xi_i\rangle B_{0E} \langle \xi_i| \otimes |0\rangle R_1 \langle 0| \right) \\
\leq \frac{2^\lambda}{d_{A_0}} \sum_a |a\rangle A_0 \langle a| \otimes \text{tr}_{E_2} \left( \sum_{i=1}^{2^m_A + m_B} \lambda_i^2 |\xi_i\rangle B_{0E} \langle \xi_i| \otimes |0\rangle R_1 \langle 0| \right) \\
= \frac{2^\lambda}{d_{A_0}} \sum_a |a\rangle A_0 \langle a| \otimes \omega_{B_r},
\]

where \( \omega_{B_r} = \text{tr}_{E_2} \left( \sum_{i=1}^{2^m_A + m_B} |\xi_i\rangle B_{0E} \langle \xi_i| \otimes |0\rangle R_1 \langle 0| \right) \). Therefore, we have, by Definition \[10\]

\[
H_{\min}(A_0|B_r)_\sigma \geq H_{\min}(A_0|B_0)_\rho - (m_B + m_A).
\]

Each round of the interactive protocol consists of the following steps:
1) Bob performs a unitary operation on his qubits.
2) Bob sends some qubits to Alice.
3) Alice performs a (classical-controlled) quantum operation on her qubits.
4) Alice sends some qubits to Bob.

Note that only when Alice sends qubits Bob does the min-entropy change and by Lemma \[12\] the entropy decreases by at most two for each qubit that Alice sends to Bob. Thus, we have

\[
H_{\min}(A_0|B_r)_\sigma \geq H_{\min}(A_0|B_0)_\rho - 2m_A.
\]

In fact, interactive leakage chain rule can be strengthened to allow pre-shared entanglement between Alice and Bob by considering only the one-way communication complexity from Alice to Bob.

**Theorem 15.** [Interactive leakage chain rule for quantum min-entropy with pre-shared entanglement] Suppose Alice and Bob share an initial state \( \rho_{A_0 B_0} = |\Phi^+\rangle_{A_0^c B_0^c} ^{\otimes m} \otimes \rho_{A_0^c B_0^c} \), where \( A_0^c = A_0^c \otimes B_0^c \), \( B_0^c = B_0^c \otimes B_0^c \), \( |\Phi^+\rangle ^{\otimes m} \) are EPR pairs, and \( \rho_{A_0^c B_0^c} \) is a cq state. If an \((r, m_A, m_B)\) two-party interactive protocol \( \Pi \) exists where the quantum operations for \( \mathcal{A} \) are classically controlled by \( A_0 \), is executed by Alice and Bob with \( m_A \leq m \), then

\[
H_{\min}(A_0|B_r)_\sigma \geq H_{\min}(A_0|B_0)_\rho - 2m_A,
\]

where \( \sigma_{A_0 B_r} = \text{tr}_{A_r} \left[ \mathcal{A} \otimes \mathcal{B} \right] (\rho_{A_0 B_0}) \).

**A. Communication Lower Bound**

In the problem of classical communication over (two-way) quantum channels, Alice wishes to send \( n \) classical bits \( X \) to Bob, who then applies a quantum measurement and observes outcome \( Y \). The famous Holevo theorem \[24\] established a lower bound that the mutual information between \( X \) and \( Y \) is at most \( m \) if \( m \) qubits are sent from Alice to Bob. Cleve \textit{et al.} extended the Holevo theorem to interactive protocols \[13, \text{Theorem 2} \]: for Bob to acquire \( m \) bits of mutual information, Alice has to send at least \( m/2 \) qubits to Bob and the two-way communication complexity is at least \( m \) qubits. Nayak and Salzman further improved these results in that Bob only recovers \( X \) with probability \( p \) \[14\].

Herein we provide another version of the classical communication lower bound. Our results are more general since we allow the initial shared states to be separable.
Corollary 16. Suppose Alice and Bob share a cq state \( \rho = \rho_{AB}^A = \sum_a p_a |a\rangle_A \langle a| \otimes \rho_{B0}^a \in D(A_0 \otimes B_0) \), where Alice holds system \( A_0 \) of classical information and Bob holds system \( B_0 \). Suppose Alice wants to send \( a \) to Bob by an \((r, m_A, m_B)\) interactive protocol \( \Pi \) such that Bob can recover \( a \) with probability at least \( p \in (0, 1) \). Then

\[
m_B + m_A \geq H_{\min}(A_0 | B_0)_{\rho} - \log_2 \frac{1}{p} \tag{8}
\]

\[
2m_A \geq H_{\min}(A_0 | B_0)_{\rho} - \log_2 \frac{1}{p}. \tag{9}
\]

Remark 17. A protocol that uses the superdense coding techniques \([9]\) can achieve Eqs. (8) and (9) with equalities.

Remark 18. As an application, we can recover the communication lower bounds by Nayak and Salzman \([14]\) Theorems 1.1 and 1.3\([1] when \( H_{\min}(A_0 | B_0)_{\rho} = n \), where \( A_0 \) is of \( n \) bits. Note that they did a round reduction argument by using Yao’s lemma so that the two-party protocol can be simulated by Alice sending a single message of length \((m_A + m_B)\) to Bob. However, this method requires a compression and decompression procedure, which unlikely generalizes to the case with initial correlations.

IV. CONCLUSION

We proved an interactive leakage chain rule for quantum min-entropy and discussed its applications in quantum communication complexity of classical information and the lower bounds for quantum private information retrieval. We may also apply our result to other scenarios. For example, our result can also derive limitations for information-theoretically secure quantum fully homomorphic encryption \([25, 26, 27]\), where the essential ingredient of the proof is Nayak’s bound \([28]\). To be more specific, instead of using Nayak’s bound, we can use the communication lower (Corollary \([16]\) derived by the interactive leakage chain rule (Theorem \([14]\)) to develop new limitations. This is our ongoing research.

CYL was financially supported from the Young Scholar Fellowship Program by Ministry of Science and Technology (MOST) in Taiwan, under Grant MOST107-2636-E-009-005. KMC was partially supported by 2016 Academia Sinica Career Development Award under Grant No. 23-17 and the Ministry of Science and Technology, Taiwan under Grant No. MOST 103-2221-E-001-022-MY3.

REFERENCES

[1] S. Dziembowski and K. Pietrzak, “Leakage-resilient cryptography,” in 49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA, 2008, pp. 293–302.

[2] O. Reingold, L. Trevisan, M. Tsudzumi, and S. P. Vadhan, “Dense subsets of pseudorandom sets,” Electronic Colloquium on Computational Complexity (ECCC), vol. 15, no. 045, 2008. [Online]. Available: http://eccc.hpi-web.de/eccc-reports/2008/TR08-045/index.html

[3] C. Gentry and D. Wichs, “Separating succinct non-interactive arguments from all falsifiable assumptions,” in Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011, pp. 99–108.

[4] K. Chung, Y. T. Kalai, F. Liu, and R. Raz, “Memory delegation,” in Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings, 2011, pp. 151–168.

[5] B. Haller, A. O’Neill, and L. Ryhrin, “Unified Approach to Deterministic Encryption: New Constructions and a Connection to Computational Entropy,” Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 582–590.

[6] J. M. Jan不知道和K. Pietrzak, “How to fake auxiliary input,” in Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014, pp. 556–560.

[7] K. Chung, E. Lui, and R. Pass, “From weak to strong zero-knowledge and applications,” in Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I, 2015, pp. 66–92.

[8] R. Renner and S. Wolf, “Smooth renyi entropy and applications,” in International Symposium on Information Theory, 2004. ISIT 2004. Proceedings., June 2004, pp. 233–.

[9] C. H. Bennett and S. J. Wiesner, “Communication via one- and two-particle operators on einstein-podolsky-rosen states,” Phys. Rev. Lett., vol. 69, pp. 2881–2884, Nov 1992. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.69.2881

[10] S. P. Desrosiers and F. Dupuis, “Quantum entropic security and approximate quantum encryption,” IEEE Trans. Inf. Theory, vol. 56, no. 7, pp. 3455–3464, July 2010.

[11] S. Winkler, M. Tomamichel, S. Hengl, and R. Renner, “Impossibility of growing quantum bit commitments,” Physical review letters, vol. 107, no. 9, p. 090502, 2011.

[12] Y.-H. Chen, K.-M. Chung, C.-Y. Lai, S. P. Vadhawan, and X. Wu, “Computational notions of quantum min-entropy,” 2017. [Online]. Available: arXiv:1704.07399

[13] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, “Quantum entanglement and the communication complexity of the inner product function,” in Quantum Computing and Quantum Communications, C. P. Williams, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 61–74.

[14] A. Nayak and J. Salzman, “Limits on the ability of quantum states to convey classical messages,” J. ACM, vol. 53, no. 1, pp. 184–206, Jan. 2006. [Online]. Available: http://doi.acm.org/10.1145/1120582.1120587

[15] A. C.-C. Yao, “Quantum circuit complexity,” in Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science, Nov 1993, pp. 352–361.

[16] A. Uhlmann, “The Transition Probability in the state space of a *-algebra,” Rep. Math. Phys., vol. 9, pp. 273–276, 1979.

[17] 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.

[18] H.-K. Lo, “Insecurity of quantum secure computations,” Physical Review A, vol. 56, no. 2, p. 1154, 1997.

[19] A. Baumeister and A. Broadbent, “Quantum private information retrieval has linear communication complexity,” Journal of Cryptology, vol. 28, no. 1, pp. 161–175, 2015.

\(^1\)Nayak and Salzman have another stronger result \([14]\) Theorem 1.4) when there is no initial correlation between Alice and Bob.
[20] G. Gutoski and J. Watrous, “Toward a general theory of quantum games,” in Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing, ser. STOC ’07. New York, NY, USA: ACM, 2007, pp. 565–574.

[21] F. Dupuis, J. B. Nielsen, and L. Salvail, “Secure two-party quantum evaluation of unitaries against specious adversaries,” in Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings, 2010, pp. 685–706.

[22] R. Konig, R. Renner, and C. Schaffner, “The operational meaning of min- and max-entropy,” IEEE Trans. Inf. Theory, vol. 55, no. 9, pp. 4337–4347, Sept 2009.

[23] I. Kremer, “Quantum communication,” Master’s thesis, The Hebrew University of Jerusalem, Mar 1995. [Online]. Available: http://www.cs.huji.ac.il/~noam/kremer-thesis.ps.

[24] A. S. Holevo, “Bounds for the quantity of information transmitted by a quantum communication channel,” Probl. Peredachi Inf., vol. 9, no. 3, pp. 3–11, 1973, English translation Problems Inform. Transmission, vol. 9, no. 3, pp.177–183, 1973.

[25] C.-Y. Lai and K.-M. Chung, “On statistically-secure quantum homomorphic encryption,” Quant. Inf. Comput., vol. 18, no. 9&10, pp. 0785–0794, 2018.

[26] M. Newman and Y. Shi, “Limitations on transversal computation through quantum homomorphic encryption,” Quant. Inf. Comput., vol. 18, no. 11&12, pp. 0927–0948, 2018.

[27] M. Newman, “Further limitations on information-theoretically secure quantum homomorphic encryption,” 2018. arXiv:1809.08719

[28] A. Nayak, “Optimal lower bounds for quantum automata and random access codes,” in Foundations of Computer Science, 1999. 40th Annual Symposium on, 1999, pp. 369–376.