Maximal α-Leakage for Quantum Privacy Mechanisms and Operational Meaning of Measured Rényi Capacity

Bo-Yu Yang[1,2], Hsuan Yu[1,2] and Hao-Chung Cheng[1,2,3]
[1]*Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan (R.O.C.)*
[2]*Physics Division, National Center for Theoretical Sciences, Taipei 10617, Taiwan (R.O.C.)*
[3]*Hon Hai (Foxconn) Quantum Computing Centre, New Taipei City 236, Taiwan (R.O.C.)*
Email:{106yang, yu.sherry3, haochung.ch}@gmail.com

Abstract—**In this work, maximal α-leakage is introduced to quantify how much a quantum adversary can learn about any sensitive information of data upon observing its disturbed version via a quantum privacy mechanism. We first show that an adversary's maximal expected α-gain using optimal measurement is characterized by measured conditional Rényi entropy. This can be viewed as a parametric generalization of König *et al.*'s famous guessing probability formula [*IEEE Trans. Inf. Theory*, 55(9), 2009]. Then, we prove that the α-leakage and maximal α-leakage for a quantum privacy mechanism are determined by measured Arimoto information and measured Rényi capacity, respectively. Various properties of maximal α-leakage, such as data processing inequality and composition property are established as well. Moreover, we show that regularized α-leakage and regularized maximal α-leakage for identical and independent quantum privacy mechanisms coincide with α-tilted sandwiched Rényi information and sandwiched Rényi capacity, respectively.**

A full version of this paper is accessible at: https://arxiv.org/pdf/2403.14450 [1].

I. Introduction

A. Background

In the era of Internet of Things, data are published and shared almost ubiquitously, which have significantly increased possible paths where private information can leak. For instance, political preferences may be unveiled through movie ratings [2]. Besides, publishing data while maintaining desirable privacy and utility guarantee has also come to issues in many fields such as business [3], healthcare [4], and so on. How can we prevent adversaries from inferring sensitive data via reverse engineering while preserving at least some levels of utility? A common approach is to perturb the data by properly designing a *privacy mechanism*: a stochastic map aiming to control the private information leakage to adversaries. Conventionally, there are two mainstream approaches: (i) *differential privacy* (DP) [5], [6], proposed by Dwork in 2006, guarantees the indistinguishability between neighboring data, addressing the paradox of learning less about an individual while gaining useful information about a population, which is further generalized to *pufferfish privacy* [7], [8] by Kifer *et al.* in 2014; (ii) *information-theoretic privacy*, which has been investigated in variant settings (e.g. Shannon's mutual information [9] and information bottleneck function [10]), adopts the viewpoints from statistics and information-theoretic security to study how the privacy is quantified [11]–[14].

When quantum devices become mature in the future, it is natural to consider protecting sensitive data via a *quantum privacy mechanism*. To this end, we may construct quantum privacy mechanisms via encoding sensitive classical data into quantum states. On the other hand, a quantum adversary may observe the encoded quantum states by applying certain quantum measurement. Various methods and metrics have been proposed to help design quantum privacy mechanisms, including quantum differential privacy [15]–[20] and quantum pufferfish privacy [21]; meanwhile, maximal quantum leakage [22], an extension of MaxL for quantum privacy mechanisms, has also been studied.

B. Problem Formulation

In this work, we consider the problem of information leakage formulated as follows (Fig. 1). Assume that random variable X on a finite set $\mathcal{X}$ with probability distribution p_X represents the non-sensitive data, which may be correlated with another random variable S, denoting some sensitive data. A user wants to share non-sensitive X with the service provider to gain utility while maintaining privacy, especially protecting information of sensitive S. The user may apply a quantum privacy mechanism, namely, a classical-quantum channel $\mathcal{N}_{\mathcal{X}\to B} : x \mapsto \rho_B^x$, mapping each realization $x \in \mathcal{X}$ to a quantum state ρ_B^x as a perturbation. In this manner, a fundamental question naturally arises:

How much information does a quantum system B leak about S?

To observe the released quantum data B, adversaries can guess the non-sensitive data X via a quantum measurement to obtain their inference $\hat{X}$ according to Born's rule [23]:

$$\Pr\{\hat{X} = X \mid X = x, B\} = \operatorname{Tr}[\rho_B^x \Pi_B^x], \qquad (1)$$

where $X - B - \hat{X}$ forms a classical-quantum-classical Markov chain. Here, the collection $\{\Pi_B^x\}_{x\in\mathcal{X}}$ of positive semi-definite matrices satisfying unity of resolution: $\sum_x \Pi_B^x = \mathbb{1}_B$, i.e. *positive operator-valued measure* (POVM), represents a quantum

979-8-3503-8284-6/24/$31.00 ©2024 IEEE

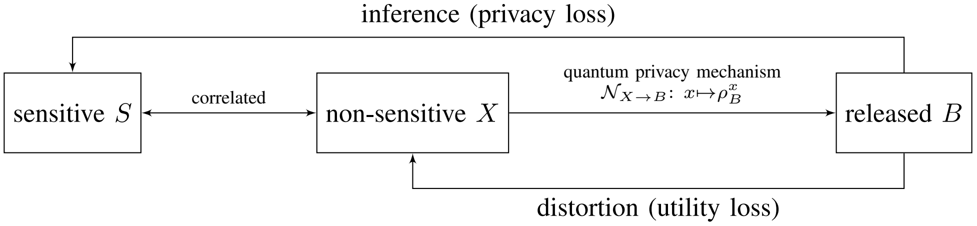
inference (privacy loss)
sensitive S
correlated
non-sensitive X
quantum privacy mechanism
$\mathcal{N}_{X\to B}\colon x\mapsto\rho_B^x$
released B
distortion (utility loss)

Fig. 1. Information leakage framework with quantum privacy mechanisms. Here, systems S and X are classical, while system B is quantum. A quantum adversary may apply a quantum measurement on quantum system B to infer data X or S.

measurement, which can be viewed as the quantum generalization of classical decisions.

Liao *et al.* characterized various classical adversarial actions by proposing α-loss with $\alpha \in [1,\infty]$, interpolating between log-loss (for $\alpha = 1$) and 0-1 loss (also known as hard decision, for $\alpha = \infty$). Since α-leakage can be directly captured by the multiplicative gain increase upon an adversary observes the released data, motivated by Diaz *et al.* 's observation of maximal expected gain function [24, Eq. (8)], we introduce the *maximal expected α-gain* of a quantum ensemble $\{p_X(x), \rho_B^x\}_{x\in\mathcal{X}}$ (Def. 4) to characterize how much an adversary correctly guesses the non-sensitive data X when using an optimal measurement strategy for observing the released quantum system B.

In order to quantify how much information B leaks about the non-sensitive X, we introduce the *α-leakage* (Def. 5) from non-sensitive data X to quantum system B as the multiplicative increase of maximal expected gain upon observing B, which is a quantum generalization of the classical α-leakage [25]. Moreover, we define the *maximal α-leakage* (Def. 6) to quantify how much information leaks about any sensitive function S correlated to the non-sensitive X via the released quantum system B, which considers the maximal advantage of adversary for all sensitive data S through a quantum privacy mechanism.

This paper is organized as follows. Section II formally introduces measured quantities and their properties. In Section III, we define α-leakage and maximal α-leakage for a quantum privacy mechanism, establish their equivalence to measured Arimoto information and measured Rényi capacity, and derive various properties for maximal α-leakage. In Section IV, we discuss the implications of our results.

II. Preliminaries

A. Notation

Throughout this paper, we let $\mathcal{X}$ and $\mathcal{Y}$ be finite sets. Let $\mathcal{H}_X$ be an $|\mathcal{X}|$-dimensional Hilbert space (i.e. complex Euclidean space) with an orthonormal basis $\{|x\rangle\}_{x\in\mathcal{X}}$. The outer product $|x\rangle\langle x|$ means an orthogonal projection onto the subspace spanned by vector $|x\rangle$. The set of probability distributions on $\mathcal{X}$ is denoted as $\mathcal{P}(\mathcal{X})$. For a probability distribution $p_X \in \mathcal{P}(\mathcal{X})$, we denote its support by $\texttt{supp}(p_X)$. Let $\mathcal{S}(\mathcal{H}_B)$ be the set of density matrices (i.e. positive semi-definite matrices with unit trace) on Hilbert space $\mathcal{H}_B$, and $\mathbb{1}_B$ be the identity matrix on $\mathcal{H}_B$. The state of a quantum system B is modeled by some density matrix $\rho_B \in \mathcal{S}(\mathcal{H}_B)$. We denote $\texttt{supp}(\rho_B)$ as the subspace spanned by the set of vectors in the eigenspace of ρ_B corresponding to positive eigenvalues. For two Hermitian matrices K and L on the same Hilbert space, we define the Hilbert–Schmidt inner product as $\langle K, L\rangle := \mathrm{Tr}\,[KL]$, where Tr is the standard trace.

A classical-quantum (c-q) state on $\mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_B)$ is $\rho_{XB} := \sum_{x\in\mathcal{X}} p_X(x)\,|x\rangle\langle x| \otimes \rho_B^x$, where $p_X \in \mathcal{P}(\mathcal{X})$ and each $\rho_B^x \in \mathcal{S}(\mathcal{H}_B)$. Namely, a c-q state ρ_{XB} represents a quantum ensemble $\{p_X(x), \rho_B^x\}_{x\in\mathcal{X}}$. Let $\{\Pi_B^x\}_{x\in\mathcal{X}}$ be a POVM, i.e. each Π_B^x is a positive semi-definite matrix on $\mathcal{H}_B$ and $\sum_{x\in\mathcal{X}} \Pi_B^x = \mathbb{1}_B$; equivalently, we also use $\Pi_{XB} := \sum_{x\in\mathcal{X}} |x\rangle\langle x| \otimes \Pi_B^x$ to denote it for brevity. For a c-q state ρ_{XB}, the partial trace over system X is denoted by $\mathrm{Tr}_X[\rho_{XB}] = (\mathrm{Tr}_X \otimes \mathrm{id}_B)(\rho_{XB}) = \sum_{x\in\mathcal{X}}(\langle x| \otimes \mathbb{1}_B)\rho_{XB}(|x\rangle \otimes \mathbb{1}_B)$, where id_B is the identity map on system B. For a power function $f : M \mapsto M^\alpha$ of a matrix M, we refer to f as acting on the support of M. Moreover, let $\mathcal{N}_{\mathcal{X}\to B} : \mathcal{X} \ni x \mapsto \rho_B^x \in \mathcal{S}(\mathcal{H}_B)$ be a c-q channel that maps each letter in the input set $x \in \mathcal{X}$ to a density matrix $\rho_B^x \in \mathcal{S}(\mathcal{H}_B)$. The exponential function is denoted by $(\cdot) \mapsto \mathrm{e}^{(\cdot)}$. The logarithmic function $(\cdot) \mapsto \log(\cdot)$ denotes natural logarithm.

B. Information-Theoretic Quantities

In this section, we briefly review the measured counterpart of entropic quantities, and refer readers to [26], [27] for more details.

Definition 1. *Let $\rho_{XB} = \sum_x p_X(x)\,|x\rangle\langle x| \otimes \rho_B^x \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_B)$ be a c-q state.*

1) ***Order-α Rényi divergence*** [28]: *For $\alpha \in (0,1) \cup (1,\infty)$ and probability distributions $p_Y, q_Y \in \mathcal{P}(\mathcal{Y})$, $D_\alpha(p_Y \| q_Y) := \frac{1}{\alpha-1}\log\sum_{y\in\mathcal{Y}} p_Y(y)^\alpha q_Y(y)^{1-\alpha}$, if $\alpha \in (0,1)$ or $\texttt{supp}(p_Y) \subseteq \texttt{supp}(q_Y)$; otherwise, it is defined as $+\infty$. In the limit $\alpha \to 1$, since Rényi divergence converges to Kullback–Leibler divergence, we denote it as $D_1(p_Y\|q_Y) \equiv D(p_Y\|q_Y) := \sum_{y\in\mathcal{Y}} p_Y(y)\log\frac{p_Y(y)}{q_Y(y)}$. As $\alpha \to \infty$, Rényi divergence converges to max-divergence $D_\infty(p_Y\|q_Y) := \lim_{\alpha\to\infty} D_\alpha(p_Y\|q_Y) = \sup_{y\in\mathcal{Y}}\log\frac{p_Y(y)}{q_Y(y)}$. The order-0 Rényi divergence is defined by taking limit $\alpha \to 0$.*

2) ***Measured Rényi divergence*** [26]: *For $\alpha \in [0, \infty]$ and density matrices ρ, σ,*

$$D_\alpha^{\mathbb{M}}(\rho\|\sigma) := \sup_{(\mathcal{Y},\Pi)} D_\alpha\left(\{\mathrm{Tr}[\rho\Pi_y]\}_{y\in\mathcal{Y}}\|\{\mathrm{Tr}[\sigma\Pi_y]\}_{y\in\mathcal{Y}}\right). \quad (2)$$

The supremum is over all finite sets $\mathcal{Y}$ and POVMs $\{\Pi^y\}_{y\in\mathcal{Y}}$.

3) ***Measured conditional Rényi entropy*** [29, Eq. (64)]: *For $\alpha \in [0, \infty]$ and a c-q state ρ_{XB},$H_\alpha^{\mathbb{M}}(X|B)_\rho := -\inf_{\sigma_B\in\mathcal{S}(\mathcal{H}_B)} D_\alpha^{\mathbb{M}}(\rho_{XB}\|\mathbb{1}_X \otimes \sigma_B)$.*

4) ***Measured Rényi information*** [30]: *For $\alpha \in [0, \infty]$ and a c-q state ρ_{XB}, $I_\alpha^{\mathbb{M}}(X; B)_\rho := \inf_{\sigma_B\in\mathcal{S}(\mathcal{H}_B)} D_\alpha^{\mathbb{M}}(\rho_{XB}\|\rho_X \otimes \sigma_B)$.*

5) ***Measured Arimoto information*** [31]: *For $\alpha \in [0, \infty]$ and a c-q state ρ_{XB}, $I_\alpha^{\mathrm{A},\mathbb{M}}(X; B)_\rho := H_\alpha(X)_p - H_\alpha^{\mathbb{M}}(X|B)_\rho$, where $H_\alpha(X)_p := \frac{1}{1-\alpha}\log\sum_{x\in\mathcal{X}} p_X(x)^\alpha$, and for $\alpha = 1$ and ∞, $H_\alpha(X)_p$ is defined as taking limit $\alpha \to 1$ and $\alpha \to \infty$ respectively.*

6) ***Measured Rényi divergence radius*** [30]: *For a c-q channel $\mathcal{N}_{\mathcal{X}\to B} : x \mapsto \rho_B^x$ and $\alpha \in [0, \infty]$, $R_\alpha^{\mathbb{M}}(\mathcal{N}_{\mathcal{X}\to B}) := \inf_{\sigma_B\in\mathcal{S}(\mathcal{H}_B)} \sup_{x\in\mathcal{X}} D_\alpha^{\mathbb{M}}(\mathcal{N}(x)\|\sigma_B)$, which is the measured counterpart of the quantum Rényi divergence radius* [32, Eq. (85)].

7) ***Measured Rényi capacity****: For $\alpha \in [0, \infty]$ and a c-q channel $\mathcal{N}_{\mathcal{X}\to B} : x \mapsto \rho_B^x$, $C_\alpha^{\mathbb{M}}(\mathcal{N}_{\mathcal{X}\to B}) := \sup_{p_X\in\mathcal{P}(\mathcal{X})} I_\alpha^{\mathbb{M}}(X; B)_\rho$.*

8) ***Measured Arimoto capacity****: For $\alpha \in [0, \infty]$ and a c-q channel $\mathcal{N}_{\mathcal{X}\to B} : x \mapsto \rho_B^x$, $C_\alpha^{\mathrm{A},\mathbb{M}}(\mathcal{N}_{\mathcal{X}\to B}) := \sup_{p_X\in\mathcal{P}(\mathcal{X})} I_\alpha^{\mathrm{A},\mathbb{M}}(X; B)_\rho$.*

9) ***Sandwiched Rényi divergence*** [33], [34]: *For density matrices ρ, σ and $\alpha \in [1/2, 1) \cup (1, \infty]$, $D_\alpha^*(\rho\|\sigma) := \frac{1}{\alpha-1}\log\mathrm{Tr}\left[(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}})^\alpha\right]$ if $\alpha \in [1/2, 1)$ or $\mathtt{supp}(\rho) \subseteq \mathtt{supp}(\sigma)$; otherwise, it is defined as $+\infty$.*

10) ***Umegaki's quantum relative entropy*** [35]: *For density matrices ρ, σ, $D(\rho\|\sigma) := \mathrm{Tr}[\rho(\log\rho - \log\sigma)]$, if* $\mathtt{supp}(\rho) \subseteq \mathtt{supp}(\sigma)$; *otherwise, it is defined as $+\infty$. Continuous extension of sandwiched Rényi divergence for $\alpha \to 1$ reduces to Umegaki's quantum relative entropy.*

11) ***Sandwiched Rényi information*** [30], [36], [37]: *For $\alpha \in [1/2, \infty]$, $I_\alpha^*(X; B)_\rho := \inf_{\sigma_B\in\mathcal{S}(\mathcal{H}_B)} D_\alpha^*(\rho_{XB}\|\rho_X \otimes \sigma_B)$.*

12) ***Sandwiched Arimoto information****: For $\alpha \in [0, \infty]$ and a c-q state ρ_{XB}, $I_\alpha^{\mathrm{A},*}(X : B)_\rho := H_\alpha(X)_p + \inf_{\sigma_B\in\mathcal{S}(\mathcal{H}_B)} D_\alpha^*(\rho_{XB}\|\mathbb{1}_X \otimes \sigma_B)$.*

13) ***Sandwiched Rényi divergence radius*** [32, Eq. (85)]: *For a c-q channel $\mathcal{N}_{\mathcal{X}\to B} : x \mapsto \rho_B^x$ and $\alpha \in [0, \infty]$, $R_\alpha^*(\mathcal{N}_{\mathcal{X}\to B}) := \inf_{\sigma_B\in\mathcal{S}(\mathcal{H}_B)} \sup_{x\in\mathcal{X}} D_\alpha^*(\mathcal{N}(x)\|\sigma_B) \equiv \inf_{\sigma_B\in\mathcal{S}(\mathcal{H}_B)} \sup_{x\in\mathcal{X}} D_\alpha^*(\rho_B^x\|\sigma_B)$.*

14) ***Sandwiched Rényi capacity*** [30]: *For $\alpha \in [1/2, \infty]$, $C_\alpha^*(\mathcal{N}_{\mathtt{supp}(p_X)\to B}) := \sup_{p_X\in\mathcal{P}(\mathcal{X})} I_\alpha^*(X; B)_\rho$.*

15) ***Sandwiched Arimoto capacity****: For $\alpha \in [0, \infty]$ and a c-q channel $\mathcal{N}_{\mathcal{X}\to B} : x \mapsto \rho_B^x$, $C_\alpha^{\mathrm{A},*}(\mathcal{N}_{\mathcal{X}\to B}) := \sup_{p_X\in\mathcal{P}(\mathcal{X})} I_\alpha^{\mathrm{A},*}(X : B)_\rho$..*

For $\alpha \in \{1/2, \infty\}$, measured Rényi divergence coincides with sandwiched Rényi divergence [26], [38]–[40]. In particular for $\alpha = +\infty$, it is named *maximum relative entropy* [41], i.e.

$$D_\infty^{\mathbb{M}}(\rho\|\sigma) = D_\infty^*(\rho\|\sigma) = \inf\{\lambda \in \mathbb{R} : \rho \leq \mathrm{e}^\lambda\sigma\}. \quad (3)$$

For all $\alpha \in (1/2, \infty)$, we have the strict relation $D_\alpha^{\mathbb{M}}(\rho\|\sigma) < D_\alpha^*(\rho\|\sigma)$ unless ρ commutes with σ [26, Thm. 6].

Definition 2 (α-tilted distribution [25], [42])**.** *Given a parameter $\alpha \in (0, \infty)$ and a probability distribution $p_X \in \mathcal{P}(\mathcal{X})$, the α-tilted distribution of p_X is defined as*

$$p_X^{(\alpha)}(x) := \frac{p_X(x)^\alpha}{\sum_{x\in\mathcal{X}} p_X(x)^\alpha}. \quad (4)$$

Lemma 1 (Variational formula of measured Rényi divergence [26, Lemma. 3] [43], [44])**.** *For density matrices ρ, σ and $\alpha \in [0, \infty]$, $D_\alpha^{\mathbb{M}}(\rho\|\sigma) =$*

$$\begin{cases} \sup\limits_{\omega>0} \mathrm{Tr}\left[\rho\log\omega\right] - \log\mathrm{Tr}\left[\sigma\omega\right], & \alpha = 1; \quad (5a) \\ \sup\limits_{\omega>0} \dfrac{1}{\alpha-1}\log\left(\left(\mathrm{Tr}\left[\rho\omega^{1-\frac{1}{\alpha}}\right]\right)^\alpha\left(\mathrm{Tr}\left[\sigma\omega\right]\right)^{1-\alpha}\right), & \alpha \neq 1. \quad (5b) \end{cases}$$

Lemma 2 (Data-processing inequality of measured Rényi divergence [43, Prop. 5.4])**.** *Let ρ, σ be density matrices and $\mathcal{N}$ be a fully quantum channel. Then, for all $\alpha \in [0, \infty]$, $D_\alpha^{\mathbb{M}}(\rho\|\sigma) \geq D_\alpha^{\mathbb{M}}(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$.*

Lemma 3 (Super-additivity of measured Rényi divergence [26, Eq. (65)])**.** *Let $\rho_A, \sigma_A \in \mathcal{S}(\mathcal{H}_A)$ and $\rho_B, \sigma_B \in \mathcal{S}(\mathcal{H}_B)$ be density matrices. For all $\alpha \in [0, \infty]$, $D_\alpha^{\mathbb{M}}(\rho_A\otimes\rho_B\|\sigma_A\otimes\sigma_B) \geq D_\alpha^{\mathbb{M}}(\rho_A\|\sigma_A) + D_\alpha^{\mathbb{M}}(\rho_B\|\sigma_B)$.*

Lemma 4 (Super-additivity of operational quantities [26, Sec. V])**.** *Let $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ and $\rho_B \in \mathcal{S}(\mathcal{H}_B)$ be density matrices. Then, for all $\alpha \in [0, \infty]$,*
$\inf_{\sigma_{AB}\in\mathcal{S}(\mathcal{H}_A\otimes\mathcal{H}_B)} D_\alpha^{\mathbb{M}}(\rho_A \otimes \rho_B\|\sigma_{AB}) \geq$
$\inf_{\sigma_A\in\mathcal{S}(\mathcal{H}_A)} D_\alpha^{\mathbb{M}}(\rho_A\|\sigma_A) + \inf_{\sigma_B\in\mathcal{S}(\mathcal{H}_B)} D_\alpha^{\mathbb{M}}(\rho_B\|\sigma_B)$.

Lemma 5 (Invariant maximal value over α-tilted distribution [45, Prop. 1])**.** *Let $\alpha \in (0, \infty)$. Given a distribution $p_X \in \mathcal{P}(\mathcal{X})$ and a continuous function $f : \mathcal{P}(\mathcal{X}) \to \mathbb{R}$, $\max_{p_X\in\mathcal{P}(\mathcal{X})} f(p_X) = \max_{p_X\in\mathcal{P}(\mathcal{X})} f\left(p_X^{(\alpha)}\right)$.*

Lemma 6. *For $\alpha \geq 0$ and a c-q channel $\mathcal{N}_{\mathcal{X}\to B} : x \mapsto \rho_B^x$, we have $C_\alpha^{\mathbb{M}}(\mathcal{N}_{\mathcal{X}\to B}) = R_\alpha^{\mathbb{M}}(\mathcal{N}_{\mathcal{X}\to B}) = C_\alpha^{\mathrm{A},\mathbb{M}}(\mathcal{N}_{\mathcal{X}\to B})$; on the other hand, for $\alpha \geq 1/2$, $C_\alpha^*(\mathcal{N}_{\mathcal{X}\to B}) = R_\alpha^*(\mathcal{N}_{\mathcal{X}\to B}) = C_\alpha^{\mathrm{A},*}(\mathcal{N}_{\mathcal{X}\to B})$.*

A detailed proof of Lemma 6 is in [1, Appendix B].

III. Information Leakage Measures and Main Results

A. Minimal Expected α-Loss and Maximal Expected α-Gain

Definition 3 (Minimal expected α-loss)**.** *For any c-q state $\rho_{XB} := \sum_x p_X(x)\,|x\rangle\langle x| \otimes \rho_B^x$ and $\alpha \in [1, \infty]$, we define the minimal expected α-loss for ρ_{XB} as: $\varepsilon_\alpha(X|B)_\rho :=$*

$$\begin{cases} \inf\limits_{\text{POVM}\,\Pi_{XB}} \dfrac{\alpha}{\alpha-1}\left(1 - \mathrm{Tr}\left[\rho_{XB}\Pi_{XB}^{\frac{\alpha-1}{\alpha}}\right]\right), & \textit{for } \alpha > 1; \quad (6a) \\ \inf\limits_{\text{POVM}\,\Pi_{XB}} -\mathrm{Tr}\left[\rho_{XB}\log\Pi_{XB}\right], & \textit{for } \alpha = 1, \quad (6b) \end{cases}$$

where the minimization is over all POVM*s on $\mathcal{H}_B$, i.e. for all POVM Π_{XB} such that $\mathrm{Tr}_X[\Pi_{XB}] = \mathbb{1}_B$ and $\Pi_{XB} \geq 0$.*

On the other hand, we define the minimal expected α-loss for an inference $\hat{X}$ without observing B as $\varepsilon_\alpha(X)_\rho :=$

$$\begin{cases} \inf\limits_{p_{\hat{X}} \in \mathcal{P}(\mathcal{X})} \dfrac{\alpha}{\alpha - 1}\left(1 - \mathbb{E}_{x\sim p_X}\left[p_{\hat{X}}(x)^{\frac{\alpha-1}{\alpha}}\right]\right), & \textit{for } \alpha \neq 1; \quad \text{(7a)} \\ \inf\limits_{p_{\hat{X}} \in \mathcal{P}(\mathcal{X})} -\mathbb{E}_{x\sim p_X}\left[\log p_{\hat{X}}(x)\right], & \textit{for } \alpha = 1. \quad \text{(7b)} \end{cases}$$

Definition 4 (Maximal expected α-gain)**.** *For any c-q state $\rho_{XB} := \sum_x p_X(x)\,|x\rangle\langle x| \otimes \rho_B^x$, POVM Π_{XB}, and $\alpha \in [1,\infty]$, we define the maximal expected α-gain for ρ_{XB} as:*

$$\mathsf{P}_\alpha(X|B)_\rho := \sup_{\text{POVM } \{\Pi_B^x\}_{x\in\mathcal{X}}} \sum_{x\in\mathcal{X}} p_X(x)\,\mathrm{Tr}\left[\rho_B^x (\Pi_B^x)^{\frac{\alpha-1}{\alpha}}\right], \quad (8)$$

where the maximization is over all POVMs *on $\mathcal{H}_B$, i.e. for all Π_{XB} such that $\mathrm{Tr}_X[\Pi_{XB}] = \mathbb{1}_B$ and $\Pi_{XB} \geq 0$.*

On the other hand, we define the maximal expected α-gain for an inference $\hat{X}$ without observing B as

$$\mathsf{P}_\alpha(X)_\rho := \sup_{p_{\hat{X}}:\hat{X}\perp X} \mathbb{E}_{x\sim p_X}\left[\Pr(\hat{X} = X|X = x)^{\frac{\alpha-1}{\alpha}}\right], \quad (9)$$

where the condition $\hat{X} \perp X$ of the supremum in the first expression springs from conditional independence of Markov chain $X - B - \hat{X}$. Without the prior knowledge embedded in B, an adversary can only guess $\hat{X}$ independently.

Remark 1. *Note that for POVM $\Pi_{XB} > 0$, minimal expected α-loss and maximal expected α-gain are related by*

$$\mathsf{P}_\alpha(X|B)_\rho = 1 - \frac{\alpha-1}{\alpha}\varepsilon_\alpha(X|B)_\rho. \quad (10)$$

Moreover, maximal expected α-gain lies in the interval $[0,1]$ because $\Pi_{XB} \leq \Pi_{XB}^{\frac{\alpha-1}{\alpha}} \leq \mathbb{1}_{XB}$ for $\alpha \in [1,\infty]$.

Our first result is the following characterization of the maximal expected α-gain for a c-q state ρ_{XB} via the measured conditional Rényi entropy. This thereby provides an operational meaning for measured conditional Rényi entropy.

Theorem 1 (Characterization of the maximal expected α-gain)**.** *For any $\alpha \in [1,\infty]$,*

$$\mathsf{P}_\alpha(X|B)_\rho = \mathrm{e}^{\frac{1-\alpha}{\alpha} H_\alpha^{\mathbb{M}}(X|B)_\rho}. \quad (11)$$

A detailed proof for Theorem 1 is provided in [1, Appendix C].

Remark 2. *For $\alpha = \infty$ and recalling the max relative entropy in* (3)*, the error exponent in* (11) *is reduced to the so-called min-entropy introduced by König, Renner, and Schaffner* [38, Thm. 1]*, i.e.,*

$$-\log \mathsf{P}_\infty(X|B)_\rho = H_\infty^*(X|B)_\rho \quad (12)$$

$$= -\inf_{\sigma_B\in\mathcal{S}(\mathcal{H}_B)} D_\infty^*(\rho_{XB} \,\|\, \mathbb{1}_X \otimes \sigma_B) \quad (13)$$

$$= -\inf_{\sigma_B\in\mathcal{S}(\mathcal{H}_B)} \inf\{\lambda \in \mathbb{R} : \rho_{XB} \leq \mathrm{e}^\lambda(\mathbb{1}_X \otimes \sigma_B)\}. \quad (14)$$

Via (10), the minimal expected α-loss is expressed as $\varepsilon_\alpha(X|B)_\rho =$

$$\begin{cases} \dfrac{\alpha}{\alpha-1}\left(1 - \mathrm{e}^{\frac{1-\alpha}{\alpha} H_\alpha^{\mathbb{M}}(X|B)_\rho}\right), & \text{for } \alpha \in (1,\infty], \quad \text{(15a)} \\ H_1^{\mathbb{M}}(X|B)_\rho, & \text{for } \alpha = 1. \quad \text{(15b)} \end{cases}$$

We remark that (15a) and (15b) recover the classical results given in [25, Lemma 1] and [24, Proposition 1].

B. Main Results: α-Leakage and Maximal α-Leakage

Definition 5 (α-leakage)**.** *Given $\alpha \in [1,\infty]$ and a c-q state $\rho_{XB} \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_B)$, the α-leakage from X to B is defined for $\alpha > 1$ as*

$$\mathcal{L}_\alpha(X \to B)_\rho := \frac{\alpha}{\alpha-1}\log\frac{\mathsf{P}_\alpha(X|B)_\rho}{\mathsf{P}_\alpha(X)_\rho}. \quad (16)$$

When $\alpha = 1$, the α-leakage is $\mathcal{L}_1(X \to B)_\rho := \varepsilon_1(X)_\rho - \varepsilon_1(X|B)_\rho$ by continuous extension.

Theorem 2 (Characterization of α-leakage)**.** *For $\alpha \in [1,\infty]$, α-leakage defined in Def. 5 can be expressed as*

$$\mathcal{L}_\alpha(X \to B)_\rho = I_\alpha^{\mathrm{A},\mathbb{M}}(X;B)_\rho. \quad (17)$$

A detailed proof of Theorem 2 is in [1, Appendix D].

Definition 6 (Maximal α-leakage)**.** *Given a joint c-q state $\rho_{XB} \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_B)$, the maximal α-leakage from X to B is defined as for $\alpha \in [1,\infty]$,*

$$\mathcal{L}_\alpha^{\max}(X \to B)_\rho := \sup_{p_{S|X}:S-X-B} \mathcal{L}_\alpha(S \to B)_\rho, \quad (18)$$

where S denotes any function of X and takes values from an arbitrary finite set. When $\alpha = 1$, maximal α-leakage reduced to Shannon information; when $\alpha = \infty$, maximal α-leakage reduced to maximal leakage proposed in [22].

Theorem 3 (Characterization of the maximal α-leakage)**.** *For $\alpha \in [1,\infty]$, the maximal α-leakage defined in Def. 6 can be expressed as*

$$\mathcal{L}_\alpha^{\max}(X \to B)_\rho = \begin{cases} I_1^{\mathrm{A},\mathbb{M}}(X;B)_\rho, & \alpha = 1; \quad \text{(19a)} \\ C_\alpha^{\mathbb{M}}(\mathcal{N}_{\mathrm{supp}(p_X)\to B}), & \alpha \neq 1, \quad \text{(19b)} \end{cases}$$

where $C_\alpha^{\mathbb{M}}(\mathcal{N}_{\mathrm{supp}(p_X)\to B}) = C_\alpha^{\mathrm{A},\mathbb{M}}(\mathcal{N}_{\mathrm{supp}(p_X)\to B}) = R_\alpha^{\mathbb{M}}(\mathcal{N}_{\mathrm{supp}(p_X)\to B})$, as proved in Lemma 6.

A detailed proof of Theorem 3 is in [1, Appendix E]. Theorem 3 hereby provides an operational meaning of measured Rényi capacity. Note that when $\alpha = 1$, maximal α-leakage depends on input probability distribution p_X; when $\alpha > 1$, maximal α-leakage depends on input probability distribution only through its support $\mathtt{supp}(p_X)$.

C. Properties of Maximal α-Leakage

To further analyze the performance of quantum privacy mechanisms, now we explore some properties of maximal α-leakage.

Theorem 4. *Denote by $\bar{\rho}_{XB} = \sum_{x\in\mathcal{X}} \bar{p}_X(x)|x\rangle\langle x| \otimes \rho_B^x$ for any input distribution $\bar{p}_X \in \mathcal{P}(\mathcal{X})$ as an optimization* *variable. For $\alpha \in [1,\infty]$ and given a c-q state $\rho_{XB} = \sum_{x\in\mathcal{X}} p_X(x)|x\rangle\langle x| \otimes \rho_B^x$, maximal α-leakage has the following properties:*

1) *is a concave program of optimization variable $\bar{p}_X$ for $\alpha > 1$, and a concave function of input distribution p_X for $\alpha = 1$;*
2) *is quasi-convex in ρ_B^x given optimization variable $\bar{p}_X$ for $\alpha > 1$ or given input distribution p_X for $\alpha = 1$;*
3) *is non-decreasing in α;*
4) *satisfies data-processing inequality;*
5)

$$0 \le \mathcal{L}_\alpha^{\max}(X \to B)_\rho \le \begin{cases} \log(|\mathrm{supp}(p_X)|), & \textit{for } \alpha > 1; \quad \text{(20a)} \\ H_1(X)_p, & \textit{for } \alpha = 1; \quad \text{(20b)} \end{cases}$$

A detailed proof of Theorem 4 is provided in [1, Appendix F]. Sometimes, an adversary can access more than one released version of non-sensitive data X. The following theorem shows that even an adversary receives multiple independently released data B, they cannot obtain information about sensitive data S more than marginal sums of maximal α-leakage. This behavior is also known as composition property [46, Sec. 3] [47, Lemma. 6] [25, Thm. 5].

Theorem 5 (Composition property)**.** *Given a probability distribution $p_X \in \mathcal{P}(\mathcal{X})$ and quantum privacy mechanisms $\mathcal{N}_{\mathcal{X}\to B_1} : x \mapsto \rho_{B_1}^x$ and $\mathcal{N}_{\mathcal{X}\to B_2} : x \mapsto \rho_{B_2}^x$, for any $\alpha \in [1,\infty]$, the maximal α-leakage from X to $B_1 B_2$ is bounded above by*

$$\mathcal{L}_\alpha^{\max}(X \to B_1, B_2)_\rho \le \mathcal{L}_\alpha^{\max}(X \to B_1)_\rho + \mathcal{L}_\alpha^{\max}(X \to B_2)_\rho, \tag{21}$$

where $\rho_{XB_1B_2} := \sum_{x\in\mathcal{X}} p_X(x)\, |x\rangle\langle x| \otimes \rho_{B_1}^x \otimes \rho_{B_2}^x$.

A detailed proof of Theorem 5 is in [1, Appendix G].

D. Asymptotic behavior of α-leakage and maximal α-leakage

In previous sections, we have considered α-leakage and maximal α-leakage for a quantum privacy mechanism in the *one-shot setting*. Here, we discuss the asymptotic behaviors of α-leakage and maximal α-leakage when non-sensitive data X^n are released via i.i.d. quantum privacy mechanisms: $\mathcal{N}_{\mathcal{X}\to B}^{\otimes n} : x_1 x_2 \cdots x_n \mapsto \rho_{B_1}^{x_1} \otimes \rho_{B_2}^{x_2} \otimes \cdots \otimes \rho_{B_n}^{x_n} =: \rho_{B^n}^{x^n}$. More precisely, we will study both $\mathcal{L}_\alpha$ and $\mathcal{L}_\alpha^{\max}$ under $\mathcal{N}_{\mathcal{X}\to B}^{\otimes n}$ and normalize the quantities by n to study the average information leakage when $n \to \infty$, which is termed *regularization* in quantum information theory.

While the i.i.d. assumption is not often adopted in information-theoretic security because one cannot restrict quantum adversaries to attack only in an i.i.d. manner; nevertheless, in the scenario of information leakage, the quantum privacy mechanism is employed by the system designer, and an i.i.d. quantum privacy mechanism $\mathcal{N}_{\mathcal{X}\to B}^{\otimes n}$ is arguably easier to perform than a general n-shot privacy mechanism $\mathcal{N}_{\mathcal{X}^n\to B^n}$: that may output a multipartite entangled state on system B^n.

Theorem 6 (Characterization of regularized α-leakage)**.** *Let $\rho_{XB} = \sum_{x\in\mathcal{X}} p_X(x)|x\rangle\langle x| \otimes \rho_B^x$. For $\alpha \ge 1$, then regularized α-leakage from i.i.d. X^n to B^n under $\mathcal{N}_{\mathcal{X}\to B}^{\otimes n}$ is given by*

$$\lim_{n\to\infty} \frac{1}{n} \mathcal{L}_\alpha(X^n \to B^n)_{\rho^{\otimes n}} = I_\alpha^*(X : B)_{\rho^{(\alpha)}}, \tag{22}$$

where the α-tilted distribution $p_X^{(\alpha)}$ is introduced in Def. 2 and we denote $\rho_{XB}^{(\alpha)} \equiv \sum_{x\in\mathcal{X}} p_X^{(\alpha)}(x)\, |x\rangle\langle x| \otimes \rho_B^x$.

Theorem 7 (Characterization of regularized maximal α-leakage)**.** *For any $\alpha > 1$, the regularized maximal α-leakage from X^n with any arbitrary distribution $p_{X^n} \in \mathcal{P}(\mathcal{X}^n)$ that has full support to B^n under $\mathcal{N}_{\mathcal{X}\to B}^{\otimes n}$ is given by*

$$\lim_{n\to\infty} \frac{1}{n} \mathcal{L}_\alpha^{\max}(X^n \to B^n)_{\rho^n} = C_\alpha^*(\mathcal{N}_{\mathcal{X}\to B}) = R_\alpha^*(\mathcal{N}_{\mathcal{X}\to B}), \tag{23}$$

where $\rho_{X^nB^n}^n := \sum_{x^n\in\mathcal{X}^n} p_{X^n}(x^n)|x^n\rangle\langle x^n| \otimes \rho_{B^n}^{x^n}$.

The proof of Theorem 6 and 7 is provided in [1, Sec. 3.4]

IV. Discussions

The goal of a privacy mechanism is to preserve information leakage subject to some desired level of utility. By adopting maximal α-leakage $\mathcal{L}_\alpha^{\max}(X \to B)_\rho$ (Def. 6) as the privacy metric and any quantum-classical distortion $d(X,B)_\rho$ (see e.g. [48]) as the utility metric bounded by the maximal permitted distortion δ, we can model this privacy-utility tradeoff (PUT) problem as the optimization problem below: for any probability distribution p_X on $\mathcal{X}$,

$$\begin{cases} \min\limits_{x\mapsto\rho_B^x} & \mathcal{L}_\alpha^{\max}(X \to B)_\rho \quad \text{(24a)} \\ \text{subject to} & d(X,B)_\rho \le \delta, \quad \text{(24b)} \end{cases}$$

the optimal PUT is denoted as $\mathrm{PUT}(\delta)_\rho := \inf_{d(X,B)_\rho \le \delta} \mathcal{L}_\alpha^{\max}(X \to B)_\rho$.

We have shown that for $\alpha > 1$, the objective function of maximal α-leakage $\mathcal{L}_\alpha^{\max}(X \to B)$ is concave in optimization variable $\bar{p}_X$ and quasi-convex in ρ_B^x given $\bar{p}_X$ in Theorem 4. Therefore, if the distortion function $d(X,B)_\rho$ is convex in ρ_B^x, this problem belongs to quasi-convex programs [49]. However, given the released quantum state B, does our framework differ from measuring it and then tackling it directly with classical techniques? To address this issue, we can consider the Markov chain $X - B - Y$, where Y is a classical state obtained by measuring B. Observing that $\mathcal{H}_Y \subseteq \mathcal{H}_B$, we immediately obtain $\mathrm{PUT}(\delta)_{\rho_{XB}} \le \mathrm{PUT}(\delta)_{\rho_{XY}}$ due to contraction of the constraint set. Therefore, we suppose that the classical method cannot outperform our quantum privacy mechanism in PUT problem with the privacy metric of maximal α-leakage.

Acknowledgment

H.-C. Cheng is supported under Grants No. NSTC 112-2636-E-002-009, No. NSTC 112-2119-M-007-006, No. NSTC 112-2119-M-001-006, No. NSTC 112-2124-M-002-003, No. NTU-112V1904-4, No. NTU-CC-112L893405, NTU-CC-113L891605 and NTU-113L900702.

References

[1] B.-Y. Yang, H. Yu, and H.-C. Cheng, "Maximal α-leakage for quantum privacy mechanisms," *arXiv preprint arXiv:2403.14450*, 2024.

[2] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, 2008, pp. 111–125.

[3] M. Hu, "Cambridge analytica's black box," *Big Data & Society*, vol. 7, no. 2, p. 2053951720938091, 2020.

[4] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," *Journal of big data*, vol. 5, no. 1, pp. 1–18, 2018.

[5] C. Dwork, "Differential privacy," in *International colloquium on automata, languages, and programming*. Springer, 2006, pp. 1–12.

[6] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.

[7] D. Kifer and A. Machanavajjhala, "Pufferfish: A framework for mathematical privacy definitions," *ACM Transactions on Database Systems (TODS)*, vol. 39, no. 1, pp. 1–36, 2014.

[8] T. Nuradha and Z. Goldfeld, "Pufferfish privacy: An information-theoretic study," *IEEE Transactions on Information Theory*, 2023.

[9] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[10] N. Tishby, F. C. Pereira, and W. Bialek, "The information bottleneck method," *arXiv preprint physics/0004057*, 2000.

[11] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *2012 50th annual Allerton conference on communication, control, and computing (Allerton)*. IEEE, 2012, pp. 1401–1408.

[12] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 838–852, 2013.

[13] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Information extraction under privacy constraints," *Information*, vol. 7, no. 1, p. 15, 2016.

[14] H. Wang and F. P. Calmon, "An estimation-theoretic view of privacy," in *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2017, pp. 886–893.

[15] L. Zhou and M. Ying, "Differential privacy in quantum computation," in *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*. IEEE, 2017, pp. 249–262.

[16] S. Aaronson and G. N. Rothblum, "Gentle measurement of quantum states and differential privacy," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, 2019, pp. 322–333.

[17] W. M. Watkins, S. Y.-C. Chen, and S. Yoo, "Quantum machine learning with differential privacy," *Scientific Reports*, vol. 13, no. 1, p. 2453, 2023.

[18] A. Angrisani, M. Doosti, and E. Kashefi, "Differential privacy amplification in quantum and quantum-inspired algorithms," *arXiv preprint arXiv:2203.03604*, 2022.

[19] Y. Du, M.-H. Hsieh, T. Liu, S. You, and D. Tao, "Quantum differentially private sparse regression learning," *IEEE Transactions on Information Theory*, vol. 68, no. 8, pp. 5217–5233, 2022.

[20] C. Hirche, C. Rouzé, and D. S. França, "Quantum differential privacy: An information theory perspective," *IEEE Transactions on Information Theory*, 2023.

[21] T. Nuradha, Z. Goldfeld, and M. M. Wilde, "Quantum pufferfish privacy: A flexible privacy framework for quantum systems," *arXiv preprint arXiv:2306.13054*, 2023.

[22] F. Farokhi, "Maximal quantum information leakage," *arXiv preprint arXiv:2307.12529*, 2023.

[23] A. M. GLEASON, "Measures on the closed subspaces of a hilbert space," *Journal of Mathematics and Mechanics*, vol. 6, no. 6, pp. 885–893, 1957. [Online]. Available: http://www.jstor.org/stable/24900629

[24] M. Diaz, H. Wang, F. P. Calmon, and L. Sankar, "On the robustness of information-theoretic privacy measures and mechanisms," *IEEE Transactions on Information Theory*, vol. 66, no. 4, pp. 1949–1978, 2019.

[25] J. Liao, O. Kosut, L. Sankar, and F. du Pin Calmon, "Tunable measures for information leakage and applications to privacy-utility tradeoffs," *IEEE Transactions on Information Theory*, vol. 65, no. 12, pp. 8043–8066, 2019.

[26] M. Berta, O. Fawzi, and M. Tomamichel, "On variational expressions for quantum relative entropies," *Letters in Mathematical Physics*, vol. 107, pp. 2239–2265, 2017.

[27] F. Hiai and M. Mosonyi, "Different quantum f-divergences and the reversibility of quantum operations," *Reviews in Mathematical Physics*, vol. 29, no. 07, p. 1750023, 2017.

[28] A. Rényi, "On measures of entropy and information," *Proc. 4th Berkeley Symp. on Math. Statist. Probability*, vol. 1, pp. 547–561, 1962.

[29] E. P. Hanson, V. Katariya, N. Datta, and M. M. Wilde, "Guesswork with quantum side information," *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 322–338, 2021.

[30] S. Beigi and M. Tomamichel, "Lower bounds on error exponents via a new quantum decoder," *arXiv preprint arXiv:2310.09014*, 2023.

[31] S. Arimoto, "Information measures and capacity of order α for discrete memoryless channels," in *Topics in Information Theory, Proc. Coll. Math. Soc. János Bolyai*, 1975, pp. 41–52.

[32] M. Mosonyi and T. Ogawa, "Strong converse exponent for classical-quantum channel coding," *Communications in Mathematical Physics*, vol. 355, pp. 373–426, 2017.

[33] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum rényi entropies: A new generalization and some properties," *Journal of Mathematical Physics*, vol. 54, no. 12, Dec. 2013. [Online]. Available: http://dx.doi.org/10.1063/1.4838856

[34] M. M. Wilde, A. Winter, and D. Yang, "Strong converse for the classical capacity of entanglement-breaking and hadamard channels via a sandwiched rényi relative entropy," *Communications in Mathematical Physics*, vol. 331, no. 2, p. 593–622, Jul. 2014. [Online]. Available: http://dx.doi.org/10.1007/s00220-014-2122-x

[35] H. Umegaki, "Conditional expectation in an operator algebra," *Tohoku Mathematical Journal, Second Series*, vol. 6, no. 2-3, pp. 177–181, 1954.

[36] H.-C. Cheng, L. Gao, and M.-H. Hsieh, "Properties of noncommutative rényi and Augustin information," *Communications in Mathematical Physics*, feb 2022.

[37] K. Li and Y. Yao, "Operational interpretation of the sandwiched r\'enyi divergences of order 1/2 to 1 as strong converse exponents," *arXiv preprint arXiv:2209.00554*, 2022.

[38] R. König, R. Renner, and C. Schaffner, "The operational meaning of min-and max-entropy," *IEEE Transactions on Information theory*, vol. 55, no. 9, pp. 4337–4347, 2009.

[39] M. Mosonyi and T. Ogawa, "Quantum hypothesis testing and the operational interpretation of the quantum rényi relative entropies," *Communications in Mathematical Physics*, vol. 334, no. 3, p. 1617–1648, Dec. 2014. [Online]. Available: http://dx.doi.org/10.1007/s00220-014-2248-x

[40] C. A. Fuchs, "Distinguishability and accessible information in quantum theory," *arXiv preprint quant-ph/9601020*, 1996.

[41] N. Datta, "Min- and max-relative entropies and a new entanglement monotone," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2816–2826, Jun 2009.

[42] S. Verdú, "α-mutual information," in *2015 Information Theory and Applications Workshop (ITA)*. IEEE, feb 2015.

[43] F. Hiai, *Quantum f-Divergences in von Neumann Algebras*, 1st ed., ser. Mathematical Physics Studies. Singapore, Singapore: Springer, Jan. 2021.

[44] H.-C. Cheng and L. Gao, "On strong converse theorems for quantum hypothesis testing and channel coding," *arXiv preprint quant-ph/2403.13584*, 2024. [Online]. Available: https://arxiv.org/abs/2403.13584

[45] A. Kamatsuka, Y. Ishikawa, K. Kazama, and T. Yoshida, "New algorithms for computing sibson capacity and arimoto capacity," *arXiv preprint arXiv:2401.14241*, 2024.

[46] P. Kairouz, S. Oh, and P. Viswanath, "The composition theorem for differential privacy," in *International conference on machine learning*. PMLR, 2015, pp. 1376–1385.

[47] I. Issa, A. B. Wagner, and S. Kamath, "An operational approach to information leakage," *IEEE Transactions on Information Theory*, vol. 66, no. 3, pp. 1625–1657, 2019.

[48] N. Datta, M.-H. Hsieh, M. M. Wilde, and A. Winter, "Quantum-to-classical rate distortion coding," *Journal of Mathematical Physics*, vol. 54, no. 4, 2013.

[49] A. Agrawal and S. Boyd, "Disciplined quasiconvex programming," *Optimization Letters*, vol. 14, pp. 1643–1657, 2020.