Strong Asymptotic Composition Theorems for Mutual Information Measures

Benjamin Wu, *Member, IEEE*, Aaron B. Wagner, *Fellow, IEEE*, Ibrahim Issa, *Member, IEEE*, and G. Edward Suh, *Fellow, IEEE*

***Abstract*— We characterize the growth of the Sibson and Arimoto mutual informations and α-maximal leakage, of any order that is at least unity, between a random variable and a growing set of noisy, conditionally independent and identically-distributed observations of the random variable. Each of these measures increases exponentially fast to a limit that is order- and measure-dependent, with an exponent that is order- and measure-independent.**

***Index Terms*— Composition theorem, maximal leakage, mutual information, side-channel leakage.**

I. Introduction

IN THE context of information leakage, composition theorems characterize how leakage increases as a result of multiple, independent, noisy observations of the sensitive data. Equivalently, they characterize how security (or privacy) degrades under the "composition" of multiple observations (or queries). In practice, attacks are often sequential in nature, whether the application is side channels in computer security [1], [2], [3] or database privacy [4], [5], [6]. Thus composition theorems are practically relevant. They also raise theoretical questions that are interesting in their own right.

Various composition theorems for differential privacy and its variants have been established (e.g., [4], [5], [6]). For the information-theoretic metrics of mutual information and maximal leakage [7], [8], [9], [10] (throughout we assume discrete alphabets and base-2 logarithms)

$$I(X;Y) = \sum_{x,y} P(x,y) \log \frac{P(x,y)}{P(x)P(y)} \tag{1}$$

$$\mathcal{L}(X \to Y) = \log \sum_{y} \max_{x: P(x)>0} P(y|x), \tag{2}$$

and α-maximal leakage [11], less is known. While some results are available in the case that $P(y|x)$ is not known [12], here we assume it is known. For the metrics in (1)-(2) it is straightforward to show the "weak" composition theorem that if $Y_1, \ldots, Y_n$ are conditionally independent given X, then

$$I(X;Y^n) \le \sum_{i=1}^{n} I(X;Y_i)$$

$$\mathcal{L}(X \to Y^n) \le \sum_{i=1}^{n} \mathcal{L}(X \to Y_i).$$

These bounds are indeed weak in that if $Y_1, \ldots, Y_n$ are conditionally i.i.d. given X, then as $n \to \infty$, the right-hand sides generally tend to infinity while the left-hand sides remain bounded. A "strong" (asymptotic) composition theorem would identify the limit and characterize the speed of convergence.

Such a result for mutual information is known [13, Theorem 2]. We prove an analogous result for maximal leakage. The limits are readily identified as the entropy and log-support size, respectively, of a minimal sufficient statistic of Y given X. Notably, in both cases, the speed of convergence to the limit is exponential, and the exponent is the same. Specifically, it is the minimum Chernoff information among all pairs of distinct distributions $Q_{Y|X}(\cdot|x)$ and $Q_{Y|X}(\cdot|x')$.

Mutual information and maximal leakage are both instances of Sibson mutual information [10], [14], [15], the former being order 1 and the latter being order ∞. The striking fact that the exponents governing the convergence to the limit are the same at these two extreme points suggests that Sibson mutual information of all orders satisfies a strong asymptotic composition theorem, with the convergence rate (but not the limit) being independent of the order. Meanwhile, Shannon mutual information can also be viewed as Arimoto mutual information of order 1 [16], and α-maximal leakage is equivalently expressed as a maximization of Sibson or Arimoto mutual information of order α over $P(X)$ for $\alpha > 1$; for $\alpha = 1$, it equals Shannon mutual information [11], as opposed to the Shannon capacity. Due to the intimate interrelation between these measures, it is reasonable to suspect that similar strong asymptotic composition theorems obtain for them all. Indeed, we prove strong composition theorems for Sibson mutual information, Arimoto mutual information, and α-maximal leakage, for all orders of at least unity. In particular, we find that they all approach their respective limits at the same α-independent exponential rate, namely the minimum Chernoff information mentioned earlier. Our proofs rely on type-theoretic methods [17, Ch.11], [18].

The composition theorems proven here are different in nature from those in the differential privacy literature. Here we assume that the relevant probability distributions are known,

Manuscript received 24 November 2021; revised 22 September 2022; accepted 5 October 2022. Date of publication 20 December 2022; date of current version 23 April 2024. This work was supported in part by the U.S. National Science Foundation under Grant 1704443, Grant 1815893, and Grant 1934985; and in part by the U.S. Army Research Office under Grant W911NF-18-1-0426. An earlier version of this paper was presented in part at the 2020 IEEE International Symposium on Information Theory [DOI: 10.1109/ISIT44484.2020.9174456]. *(Corresponding author: Benjamin Wu.)*

Benjamin Wu is with L3Harris Technologies Inc., Anaheim, CA 92805 USA (e-mail: bhw49@cornell.edu).

Aaron B. Wagner and G. Edward Suh are with the School of Electrical and Computer Engineering, Cornell University, Ithaca, NY 14850 USA (e-mail: wagner@cornell.edu; suh@ece.cornell.edu).

Ibrahim Issa is with the Department of Electrical and Computer Engineering, American University of Beirut, Beirut 1107 2020, Lebanon (e-mail: ii19@aub.edu.lb).

Communicated by V. Jog, Associate Editor for Shannon Theory and Information Measures.

Digital Object Identifier 10.1109/TIT.2022.3228519

and we characterize the growth of leakage with repeated looks from those distributions. We also assume that $Y_1, \ldots, Y_n$ are conditionally i.i.d. given X. Composition theorems in differential privacy consider the worst-case distributions given leakage levels for each of $Y_1, \ldots, Y_n$ individually, assuming only conditional independence.

Although our motivation is averaging attacks in side channels, the results may have some use in capacity studies of channels with multiple conditionally i.i.d. outputs given the input [17, Prob. 7.20].

The balance of the paper is organized as follows. The next section introduces the remaining mutual information measures and other important quantities. Our main result is stated in Sec. II. Secs. III-VIII contain the proofs separated out by information measure. A preliminary version [19] of this work provided results for Sibson mutual information for all orders in $[1, \infty]$. This paper extends those results by also including results for channel capacity, Arimoto mutual information, and α-maximal leakage.

II. Sibson, Arimoto, Rényi, and Chernoff

This study relies on both Sibson's and Arimoto's tunable mutual information metrics as well as α-maximal leakage. All random variables in the paper are assumed discrete.

Definition 1 ([14], [15]): The *Sibson mutual information of order* α between random variables X and Y is defined by

$$I_\alpha^S(X;Y) = \frac{\alpha}{\alpha-1} \log \sum_{y\in\mathcal{Y}} \Big(\sum_{x\in\mathcal{X}} P(x)P(y|x)^\alpha \Big)^{1/\alpha}, \tag{3}$$

for $\alpha \in (0,1)\cup(1,\infty)$ and for $\alpha = 1$ and $\alpha = \infty$ by its continuous extensions. These are

$$I_1^S(X;Y) = I(X;Y)$$
$$I_\infty^S(X;Y) = \mathcal{L}(X \to Y),$$

defined in (1)-(2) above.

Definition 2 [16]: The *Arimoto mutual information of order* α between random variables X and Y is defined by

$$I_\alpha^A(X;Y) = \frac{\alpha}{\alpha-1} \log \sum_{y\in\mathcal{Y}} \Big(\frac{\sum_{x\in\mathcal{X}} P(x)^\alpha P(y|x)^\alpha}{\sum_{x\in\mathcal{X}} P(x)^\alpha} \Big)^{1/\alpha} \tag{4}$$

for $\alpha \in (0,1)\cup(1,\infty)$ and for $\alpha = 1$ and $\alpha = \infty$ by its continuous extensions. Note that [16]

$$I_1^A(X;Y) = I(X;Y)$$

but

$$I_\infty^A(X;Y) \neq \mathcal{L}(X \to Y).$$

Definition 3 [11]: The *α-maximal leakage* for $\alpha \in (1,\infty]$ is equivalently defined using either Sibson or Arimoto mutual information as:[1]

$$\mathcal{L}_\alpha^{max}(X \to Y) = \max_{Q(X)} I_\alpha^S(X;Y) = \max_{Q(X)} I_\alpha^A(X;Y), \tag{5}$$

where the maxima are over all distributions of X that have full support. For $\alpha = 1$, we have

$$\mathcal{L}_\alpha^{max}(X \to Y) = I(X;Y). \tag{6}$$

as opposed to the (Shannon) capacity

$$\mathcal{C}(X;Y) = \max_{Q(X)} I(X;Y). \tag{7}$$

Liao et al. [11] define α-maximal leakage operationally. The identities in (5)-(6) are a theorem in that work, which we shall take as a definition. Likewise, Issa et al. [7] define maximal leakage operationally, and (2) is a theorem therein that we take as a definition.

We are interested in how $I_\alpha^S(X;Y^n)$, $I_\alpha^A(X;Y^n)$, and $\mathcal{L}_\alpha^{max}(X \to Y^n)$ grow with n when $Y_1, \ldots, Y_n$ are conditionally i.i.d. given X for $\alpha \geq 1$. The question for $\alpha < 1$ is meaningful in all cases but is not considered here because we are interested in the behavior of operational leakage measures, and the $\alpha < 1$ regime is not known to be relevant to measuring leakage. We do not consider the mutual information meaures put forward by Csiszár [20] and Lapidoth and Pfister [21], [22] for the same reason. For the quantities under study, we shall see that the limits are given by *Rényi entropy*. As they will be needed for the proofs later, we also define *Arimoto-Rényi conditional entropy* and *Rényi divergence*.

Definition 4: The *Rényi entropy* of order α of a random variable X is given by:

$$H_\alpha(X) = \frac{1}{1-\alpha} \log \sum_{x\in\mathcal{X}} P(x)^\alpha \tag{8}$$

for $\alpha \in (0,1)\cup(1,\infty)$ and for $\alpha = 0$, $\alpha = 1$, and $\alpha = \infty$ by its continuous extensions. These are

$$H_0(X) = \log |\{x : P(x) > 0\}| \tag{9}$$
$$H_1(X) = H(X) \tag{10}$$
$$H_\infty(X) = \log \frac{1}{\max_x P(x)}. \tag{11}$$

where $H(X)$ is the regular Shannon entropy.

Definition 5: The *Arimoto-Rényi conditional entropy* of order α of a random variable X given Y is defined as:

$$H_\alpha(X|Y) = \frac{\alpha}{1-\alpha} \log \sum_{y\in\mathcal{Y}} \Big(\sum_{x\in\mathcal{X}} P(x)^\alpha P(y|x)^\alpha \Big)^{\frac{1}{\alpha}}. \tag{12}$$

Remark: One can verify that it holds

$$I_\alpha^A(X;Y) = H_\alpha(X) - H_\alpha(X|Y). \tag{13}$$

Definition 6: The *Rényi divergence* of order α between probability distributions P and Q is defined for $\alpha \in [0,\infty)$, $\alpha \neq 1$ as:

$$D_\alpha(P||Q) = \frac{1}{\alpha-1} \log \sum_{x\in\mathcal{X}} P(x)^\alpha Q(x)^{1-\alpha}, \tag{14}$$

where the continuous extension at $\alpha = 1$ is given by the standard Kullback-Leibler divergence

$$D(P||Q) = \sum_{x\in\mathcal{X}} P(x) \log \frac{P(x)}{Q(x)}. \tag{15}$$

[1] The second equality in (5) is apparent for $1 < \alpha < \infty$ from (3) and (4) since the tilting of $P(x)$ in the latter can be absorbed into the maximization. For $\alpha = \infty$, see [11, Thm. 2].

As will be shown in Theorem 1, the speed of convergence of $I_\alpha^S(X;Y^n)$, $I_\alpha^A(X;Y^n)$, $\mathcal{L}_\alpha^{max}(X \to Y^n)$, and $\mathcal{C}(X;Y^n)$ to their respective limits turns out to be governed by *Chernoff information.*

Definition 7 [17]: The *Chernoff information* between two probability mass functions, P_1 and P_2, over the same alphabet $\mathcal{X}$ is given as follows. First, for all $x \in \mathcal{X}$ and $\lambda \in [0,1]$, let:

$$P_\lambda(x) = P_\lambda(P_1,P_2,x) = \frac{P_1(x)^\lambda P_2(x)^{1-\lambda}}{\sum_{x' \in \mathcal{X}} P_1(x')^\lambda P_2(x')^{1-\lambda}}. \quad (16)$$

Then the Chernoff information is given by

$$\mathscr{C}(P_1||P_2) = D(P_{\lambda^*}||P_1) = D(P_{\lambda^*}||P_2), \quad (17)$$

where λ^* is any value of λ such that the above two relative entropies are equal. Equivalently, the Chernoff information is also given by:

$$\mathscr{C}(P_1||P_2) = -\min_{0 \le \lambda < 1} \log\left(\sum_x P_1(x)^\lambda P_2(x)^{1-\lambda}\right). \quad (18)$$

Since we consider finite alphabets, the Chernoff information is infinite if and only if P_1 and P_2 have disjoint support.

Other Notation: We use standard type-theoretic ideas and notation [17, Ch.11], [18]. We use $\mathcal{P}_n$ to denote the set of all possible empirical distributions of Y^n. We let $\mathcal{P}$ denote the set of all possible probability distributions over $\mathcal{Y}$. For any $P \in \mathcal{P}$, let

$$T(P) = \{y^n \in \mathcal{Y}^n | P_{y^n} = P\},$$

where P_{y^n} is the empirical distribution of y^n. Note that $T(P)$ is empty if $P \notin \mathcal{P}_n$. We use $Q(\cdot)$ to denote the true distributions of X and Y^n. We let Q_x denote the distribution of Y given x for a given $x \in \mathcal{X}$. For any $P \in \mathcal{P}$, let $x_k(P)$ denote $x \in \mathcal{X}$ such that $D(P||Q_x)$ is the k^{th} smallest relative entropy across all elements of $\mathcal{X}$. Ties can be broken by the ordering of $\mathcal{X}$. Note that from the standard type-theoretic result [17, Thm. 11.1.2] that for any $P \in \mathcal{P}_n$,

$$Q_x(T(P)) = |T(P)| \cdot 2^{-n(H(P)+D(P||Q_x))} \quad (19)$$

we infer the ordering

$$Q_{x_1(P)}(T(P)) \ge Q_{x_2(P)}(T(P)) \ge \cdots \ge Q_{x_{|\mathcal{X}|}(P)}(T(P)). \quad (20)$$

We shall also use the standard type-theoretic bound [17, Theorem 11.1.4] [18, Lemma 2.6]:

$$\frac{1}{(n+1)^{|\mathcal{Y}|}} 2^{-nD(P||Q_x)} \le Q(T(P)|x) \le 2^{-nD(P||Q_x)}. \quad (21)$$

We also define x-domains for fixed n in two slightly different ways. Let

$$D_x = \{P \in \mathcal{P} | D(P||Q_x) < D(P||Q_{x'}) \; \forall x' \ne x\} \quad (22)$$
$$\bar{D}_x = \{P \in \mathcal{P} | D(P||Q_x) \le D(P||Q_{x'}) \; \forall x' \in \mathcal{X}\} \quad (23)$$

Note that for any $P \in \bar{D}_x$, $D(P||Q_x) = \min_{x' \in \mathcal{X}} D(P||Q_{x'})$.

III. The Result

Let X be a random variable with alphabet $\mathcal{X} = \{x_1, x_2, \dots x_{|\mathcal{X}|}\}$. Let $Y^n = (Y_1, Y_2, \dots Y_n)$ be a vector of discrete random variables with a shared alphabet $\mathcal{Y} = \{y_1, y_2, \dots y_{|\mathcal{Y}|}\}$. We assume that $Y_1, Y_2, \dots, Y_n$ are conditionally i.i.d. given X. Our goal is to characterize the growth of $I_\alpha^S(X;Y^n)$, $I_\alpha^A(X;Y^n)$, and $\mathcal{L}_\alpha^{max}(X \to Y^n)$ with n. For this we may assume, without loss of generality, that X and Y have full support. We may also assume that the distributions $P_{Y|X}(\cdot|x)$ are distinct over x, which we call the *distinct row assumption*. For Sibson mutual information and α-max leakage, this is without loss of generality, since we can divide $\mathcal{X}$ into equivalence classes based on their respective $P_{Y|X}(\cdot|x)$ distributions and define $\tilde{X}$ to be the equivalence class of X. Then both Markov chains $X \leftrightarrow \tilde{X} \leftrightarrow Y^n$ and $\tilde{X} \leftrightarrow X \leftrightarrow Y^n$ hold and so

$$I_\alpha^S(X;Y^n) = I_\alpha^S(\tilde{X};Y^n) \quad (24)$$
$$\mathcal{L}_\alpha^{max}(X \to Y^n) = \mathcal{L}_\alpha^{max}(\tilde{X} \to Y^n), \quad (25)$$

by the data processing inequality for Sibson mutual information [23] and α-maximal leakage [11, Thm. 3]. We may then replace X with $\tilde{X}$ in the case of these measures. For Arimoto mutual information, the chain rule does not hold, and in fact an arbitrarily large discrepancy can exist between $I_\alpha^A(X;Y)$ and $I_\alpha^A(\tilde{X};Y)$, as shown in Appendix B, where it is also shown that the distinct row assumption is nonetheless still without loss of generality.

Our measures of interest satisfy the following upper bounds:

$$I(X;Y^n) \le H(X) \quad (26)$$
$$\mathcal{C}(X;Y^n) \le \log|\mathcal{X}| \quad (27)$$
$$I_\alpha^S(X;Y^n) \le H_{1/\alpha}(X) \quad \text{[15, Ex. 2 and Thm. 3]} \quad (28)$$
$$I_\alpha^A(X;Y^n) \le H_\alpha(X) \quad \text{[24, Prop. 3] and (13)} \quad (29)$$
$$\mathcal{L}_\alpha^{max}(X \to Y^n) \le \begin{cases} H(X) & \text{if } \alpha = 1 \\ \log|\mathcal{X}| & \text{if } \alpha > 1 \end{cases} \quad \text{[11, Thm. 3]} \quad (30)$$
$$=: \mathcal{L}_\alpha(X),$$

where each inequality holds for all n and all $\alpha \in [1,\infty]$. Comparing (28) and (29) suggests that perhaps the Arimoto mutual information of order α should be associated with the Sibson mutual information of order $1/\alpha$; the identity in (5) suggests otherwise.

Kanaya and Han [13, Theorem 2] have shown that $I(X;Y^n)$ approaches $H(X)$ exponentially fast, with a rate equal to the minimum Chernoff information among all pairs of distinct distributions $Q_{Y|X}(\cdot|x)$ and $Q_{Y|X}(\cdot|x')$ (equation (32)). Our main result shows that all quantities mentioned above approach their corresponding upper bounds at this same rate.

Theorem 1: Under the distinct row assumption, for all $\alpha \in [1,\infty]$,

$$\min_{x \ne x'} \mathscr{C}(Q_x||Q_{x'}) \quad (31)$$
$$= \lim_{n\to\infty} -\frac{1}{n}\log\Big(H(X) - I(X;Y^n)\Big) \quad (32)$$
$$= \lim_{n\to\infty} -\frac{1}{n}\log\Big(\log|\mathcal{X}| - \mathcal{C}(X;Y^n)\Big) \quad (33)$$

$$= \lim_{n\to\infty} -\frac{1}{n}\log\left(H_{1/\alpha}(X) - I_\alpha^S(X;Y^n)\right) \tag{34}$$
$$= \lim_{n\to\infty} -\frac{1}{n}\log\left(H_\alpha(X) - I_\alpha^A(X;Y^n)\right) \tag{35}$$
$$= \lim_{n\to\infty} -\frac{1}{n}\log\left(\mathcal{L}_\alpha(X) - \mathcal{L}_\alpha^{max}(X\to Y^n)\right). \tag{36}$$

Thus the Chernoff information governs the exponential rate-of-approach for all measures and for all values of α. This Chernoff information is infinite if Q_x and $Q_{x'}$ have disjoint support for all $x \neq x'$; in this case, the bounds in (26)-(30) are met with equality already for $n = 1$. Channels with this property arise naturally in certain applications [25].

Observe that (34)-(36) coincide with (32) when $\alpha = 1$. Also, (34) and (36) coincide for $\alpha = \infty$; otherwise the assertions are independent.

For continuous random variables, it is meaningful and interesting to study how $I_\alpha^S(X;Y^n)$, $\mathcal{C}(X;Y^n)$, and $\mathcal{L}_\alpha^{max}(X\to Y^n)$ grow with n. The behavior would be fundamentally different from the discrete case, however. See Aishwarya and Madiman [26] for a discussion of Arimoto mutual information in the continuous case.

The remainder of the paper is devoted to proving the various assertions contained within Theorem 1. The assertions are evidently asymptotic in nature, and our proofs are not optimized to provide the best finite-n bounds. Numerical experiments show that in many cases our lower and upper bounds are quite far apart for moderate values of n.

IV. Proof for Capacity

To prove the upper bound in (33), let $Q^{(u)}$ denote the uniform distribution over $\mathcal{X}$. Then by (32) we have

$$\liminf_{n\to\infty} -\frac{1}{n}\log\left(\log|\mathcal{X}| - C(X;Y^n)\right) \tag{37}$$
$$\geq \liminf_{n\to\infty} -\frac{1}{n}\log\left(\log|\mathcal{X}| - I(X;Y^n)_{Q^{(u)}}\right) \tag{38}$$
$$= \min_{x\neq x'} \mathscr{C}(Q_x||Q_{x'}). \tag{39}$$

For the reverse inequality, for each n, let Q_n be a maximizer of $I(X;Y^n)$. We shall show that Q_n is asymptotically uniform. We have

$$D(Q_n||Q^{(u)}) = \log|\mathcal{X}| - H(X)_{Q_n} \tag{40}$$
$$\leq \log|\mathcal{X}| - I(X;Y^n)_{Q_n} \tag{41}$$
$$\overset{(a)}{\leq} \log|\mathcal{X}| - I(X;Y^n)_{Q^{(u)}} \tag{42}$$
$$\overset{(b)}{\leq} \log|\mathcal{X}| \tag{43}$$
$$- \left(\log|\mathcal{X}| - e^{-\frac{n}{2}\min_{x\neq x'}\mathscr{C}(Q_x||Q_{x'})}\right)$$
$$\leq e^{-\frac{n}{2}\min_{x\neq x'}\mathscr{C}(Q_x||Q_{x'})}, \tag{44}$$

where (a) follows from the fact that Q_n is a maximizer of $I(X;Y^n)$, and (b) follows from (32) for sufficiently large n. Thus Q_n converges to $Q^{(u)}$ as desired. Moreover, it is known [13, Lemma1] that for any $\delta > 0$, there exists n large enough such that

$$H(X|Y^n)_{Q_n} \tag{45}$$
$$\geq e^{-n\left(\min_{x\neq x'}\mathscr{C}(Q_x||Q_{x'})+\delta\right)} \cdot \min_{x\neq x'}\left\{Q_n(x) + Q_n(x')\right\}.$$

Combining (44) and (45) yields, for any $\delta > 0$ and sufficiently large n,

$$\mathcal{C}(X;Y^n) = I(X;Y^n)_{Q_n} \tag{46}$$
$$\leq H(X)_{Q_n} - \Bigg[e^{-n\left(\min_{x\neq x'}\mathscr{C}(Q_x||Q_{x'})+\delta\right)}. \tag{47}$$
$$\min_{x\neq x'}\left\{Q_n(x) + Q_n(x')\right\}\Bigg]$$
$$\leq \log|\mathcal{X}| - \frac{1}{|\mathcal{X}|}e^{-n\left(\min_{x\neq x'}\mathscr{C}(Q_x||Q_{x'})+\delta\right)}. \tag{48}$$

The result follows by noting that δ was chosen arbitrarily.

V. Proof for Sibson ($\alpha \in (1,\infty)$)

We turn to (34), focusing on the regime $\alpha \in (1,\infty)$, since the $\alpha = 1$ case is established in (32) and the $\alpha = \infty$ case will be proven subsequently. First, we derive a lower bound of $I_\alpha^S(X;Y^n)$ for $\alpha > 1$ that will be useful in this and subsequent proofs.

Lemma 2:

$$I_\alpha^S(X;Y^n) \geq H_{1/\alpha}(X) - \frac{\alpha}{(\alpha-1)\ln 2}\left(\Gamma_n + \frac{\Gamma_n^2}{2(1-\Gamma_n)}\right) \tag{49}$$

for $\alpha > 1$, where

$$\Gamma_n = \min(1, (n+1)^{|\mathcal{Y}|}\cdot 2^{-n\cdot\min_{x\neq x'}\mathscr{C}(Q_x||Q_{x'})}). \tag{50}$$

Remark: If Q_x and $Q_{x'}$ have disjoint support for every $x \neq x'$, then $\Gamma_n = 0$ and this lemma establishes that $I_\alpha^S(X;Y^n) = H_{1/\alpha}(X)$ for any $n \geq 1$.

Proof: We begin by expressing the Sibson mutual information as a sum over types:

$$\frac{\alpha-1}{\alpha}I_\alpha^S(X;Y^n) \equiv \log\sum_{y^n\in\mathcal{Y}^n}\left(\sum_{x\in\mathcal{X}}Q(x)Q(y^n|x)^\alpha\right)^{1/\alpha} \tag{51}$$
$$= \log\sum_{P\in\mathcal{P}_n}\left(\sum_{x\in\mathcal{X}}Q(x)Q(T(P)|x)^\alpha\right)^{1/\alpha}. \tag{52}$$

We then decompose $\mathcal{P}_n$ using the D_x sets defined in (22):

$$\geq \log\sum_{x\in\mathcal{X}}\sum_{P\in D_x\cap\mathcal{P}_n}\left(\sum_{x'\in\mathcal{X}}Q(x')Q(T(P)|x')^\alpha\right)^{1/\alpha} \tag{53}$$
$$\geq \log\sum_{x\in\mathcal{X}}Q(x)^{1/\alpha}\sum_{P\in D_x\cap\mathcal{P}_n}Q(T(P)|x), \tag{54}$$

where we have retained only the $x' = x$ term in the inner sum. Continuing,

$$= \log\sum_{x\in\mathcal{X}}Q(x)^{1/\alpha}\Big(1 - \sum_{P\in\mathcal{P}_n\setminus D_x}Q(T(P)|x)\Big) \tag{55}$$
$$= \log\left(\sum_{x\in\mathcal{X}}Q(x)^{1/\alpha} - \sum_{x\in\mathcal{X}}\sum_{P\in\mathcal{P}_n\setminus D_x}Q(x)^{1/\alpha}Q(T(P)|x)\right). \tag{56}$$

Define

$$\gamma_n = \frac{\sum_{x\in\mathcal{X}} \sum_{P\in\mathcal{P}_n\setminus D_x} Q(x)^{1/\alpha} Q(T(P)|x)}{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}} \leq 1. \tag{57}$$

Then we can write

$$I_\alpha^S(X;Y^n) \geq \frac{\alpha}{\alpha-1} \log \left\{ \Big(\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha} \Big)(1-\gamma_n) \right\} \tag{58}$$

$$= H_{1/\alpha}(X) + \frac{\alpha}{\alpha-1}\log(1-\gamma_n). \tag{59}$$

Now γ_n can be bounded from above:

$$\gamma_n \leq \frac{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}(n+1)^{|\mathcal{Y}|} \cdot \max_{P\in\mathcal{P}_n\setminus D_x} Q(T(P)|x)}{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}} \tag{60}$$

$$\leq \frac{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}(n+1)^{|\mathcal{Y}|} \cdot \max_{x'\in\mathcal{X}} \max_{P\in\mathcal{P}_n\setminus D_{x'}} Q(T(P)|x')}{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}} \tag{61}$$

$$= (n+1)^{|\mathcal{Y}|} \cdot \max_{x\in\mathcal{X}} \max_{P\in\mathcal{P}_n\setminus D_x} Q(T(P)|x). \tag{62}$$

Applying the type-theoretic bound from (21), this gives

$$\gamma_n \leq (n+1)^{|\mathcal{Y}|} \cdot 2^{-n(\min_{x\in\mathcal{X}} \min_{P\in\mathcal{P}_n\setminus D_x} D(P||Q_x))}. \tag{63}$$

The exponent is in fact the one that we desire:

$$\min_{x\in\mathcal{X}} \min_{P\in\mathcal{P}_n\setminus D_x} D(P||Q_x) = \min_{x\neq x'} \inf_{P\in\bar{D}_{x'}} D(P||Q_x) \tag{64}$$

$$= \inf_{P\in\mathcal{P}_n} \min_{x:x\neq x_1(P)} D(P||Q_x) \tag{65}$$

$$= \inf_{P\in\mathcal{P}_n} D(P||Q_{x_2(P)}) \tag{66}$$

$$= \min_{x\neq x'} \mathscr{C}(Q_x||Q_{x'}), \tag{67}$$

where we have used Lemma 4 in Appendix A for the equality in the last step. The result then follows from the expansion:

$$\ln(1-\epsilon) = -\sum_{i=1}^{\infty} \frac{\epsilon^i}{i} \tag{68}$$

$$\geq -\epsilon - \frac{\epsilon}{2}\Big(\sum_{i=1}^{\infty} \epsilon^i\Big) = -\epsilon - \frac{\epsilon^2}{2(1-\epsilon)} \tag{69}$$

for $0 < \epsilon < 1$.

□

We next prove an analogous upper bound.

Lemma 3: For $\alpha > 1$, define

$$F(x,P) = Q(x)Q(T(P)|x)^\alpha. \tag{70}$$

For each n, let $\{E_{x_i}^{(n)}\}_{i=1}^{|\mathcal{X}|}$ be a partition of $\mathcal{P}_n$ such that $P \in E_x^{(n)}$ implies $F(x,P) = \max_{x'\in\mathcal{X}} F(x',P)$. Then

$$I_\alpha^S(X;Y^n) \leq H_{1/\alpha}(X) + \frac{\alpha}{(\alpha-1)\ln 2} \cdot \sum_{x\in\mathcal{X}} \sum_{P\notin E_x^{(n)}} F(x,P) \cdot \left[\frac{F(x_1(P),P)^{1/\alpha-1} - F(x,P)^{1/\alpha-1}}{\sum_{x'\in\mathcal{X}} Q(x')^{1/\alpha}} \right], \tag{71}$$

where for the remainder of this section we redefine $x_k(P)$ so that they are ordered by $F(x,P)$ instead of relative entropy. That is,

$$F(x_1(P),P) \geq F(x_2(P),P) \geq \cdots \geq F(x_{|\mathcal{X}|}(P),P). \tag{72}$$

Note that this ordering now depends on n.

Proof: We have

$$\frac{\alpha-1}{\alpha} I_\alpha^S(X;Y^n)$$

$$= \log \sum_{x\in\mathcal{X}} \sum_{P\in E_x^{(n)}} \Big(\sum_{x'\in\mathcal{X}} F(x',P) \Big)^{1/\alpha} \tag{73}$$

$$= \log \sum_{x\in\mathcal{X}} \sum_{P\in E_x^{(n)}} F(x,P)^{1/\alpha} \Big(1 + \sum_{x'\neq x} \frac{F(x',P)}{F(x,P)} \Big)^{1/\alpha} \tag{74}$$

$$\leq \log \sum_{x\in\mathcal{X}} \sum_{P\in E_x^{(n)}} F(x,P)^{1/\alpha} \Big(1 + \sum_{x'\neq x} \frac{F(x',P)}{F(x,P)} \Big) \tag{75}$$

$$\leq \log \sum_{x\in\mathcal{X}} \sum_{P\in E_x^{(n)}} \Big(F(x,P)^{1/\alpha} + F(x,P)^{1/\alpha-1} \sum_{x'\neq x} F(x',P) \Big), \tag{76}$$

where we have used the fact that $\alpha > 1$. Considering the second term in isolation,

$$\sum_{x\in\mathcal{X}} \sum_{P\in E_x^{(n)}} F(x,P)^{1/\alpha-1} \sum_{x'\neq x} F(x',P)$$

$$= \sum_{x\in\mathcal{X}} \sum_{P\in E_x^{(n)}} \max_{\hat{x}\in\mathcal{X}} F(\hat{x},P)^{1/\alpha-1} \cdot \Big(\sum_{x'\in\mathcal{X}} F(x',P) - \max_{\hat{x}\in\mathcal{X}} F(\hat{x},P) \Big) \tag{77}$$

$$= \sum_{x\in\mathcal{X}} \sum_{P\in E_x^{(n)}} F(x_1(P),P)^{1/\alpha-1} \cdot \Big(\sum_{x'\in\mathcal{X}} F(x',P) - F(x_1(P),P) \Big) \tag{78}$$

$$= \sum_{P\in\mathcal{P}_n} F(x_1(P),P)^{1/\alpha-1} \sum_{x'\neq x_1(P)} F(x',P) \tag{79}$$

$$= \sum_{x\in\mathcal{X}} \sum_{P\notin E_x^{(n)}} F(x_1(P),P)^{1/\alpha-1} F(x,P), \tag{80}$$

where the first and second equalities follow from the definitions of the partition and $x_1(P)$ in Lemma 3. Substituting this into (76),

$$\frac{\alpha-1}{\alpha} I_\alpha^S(X;Y^n)$$

$$= \log \sum_{x\in\mathcal{X}} \Big(\sum_{P\in E_x^{(n)}} F(x,P)^{1/\alpha} + \sum_{P\notin E_x^{(n)}} F(x_1(P),P)^{1/\alpha-1} F(x,P) \Big) \tag{81}$$

$$= \log \sum_{x\in\mathcal{X}} \Big(\sum_{P\in E_x^{(n)}} F(x,P)^{1/\alpha} \tag{82}$$

$$
\begin{aligned}
&\quad + \sum_{P\notin E_x^{(n)}} F(x_1(P),P)^{1/\alpha-1}F(x,P) \\
&\qquad + \sum_{P\notin E_x^{(n)}} F(x,P)^{1/\alpha} - \sum_{P\notin E_x^{(n)}} F(x,P)^{1/\alpha}\Big) \\
&= \log \sum_{x\in\mathcal{X}} \Big(\sum_{P\in\mathcal{P}_n} F(x,P)^{1/\alpha} \qquad (83) \\
&\quad + \sum_{P\notin E_x^{(n)}} \big(F(x_1(P),P)^{1/\alpha-1} - F(x,P)^{1/\alpha-1}\big)F(x,P)\Big).
\end{aligned}
$$

Using $\ln(1+x) \le x$ then gives the result. □

The lower bound in (34) for $\alpha \in (1,\infty)$ follows directly from Lemma 2. For the upper bound, pick $x_a \neq x_b$ and $P^* \in D_{x_b}$. Let $\{P_n\}_{n=1}^{\infty}$ be a sequence of types converging to P^*. From Lemma 3 we have

$$
\begin{aligned}
I_\alpha^S(X;Y^n) \le H_{1/\alpha}(X) + \frac{\alpha}{(\alpha-1)\ln 2} \sum_{x\in\mathcal{X}} \sum_{P\notin E_x^{(n)}} F(x,P)\cdot \\
\left[\frac{F(x_1(P),P)^{1/\alpha-1} - F(x,P)^{1/\alpha-1}}{\sum_{x'\in\mathcal{X}} Q(x')^{1/\alpha}}\right].
\end{aligned}
\tag{84}
$$

Note that for sufficiently large n, $P_n \in E_{x_b}^{(n)}$, $x_1(P_n) = x_b$. Moreover, by equations (21) and (70),

$$
\begin{aligned}
\frac{F(x_a,P_n)}{F(x_b,P_n)} &= \frac{Q(x_a)Q(T(P_n)|x_a)^\alpha}{Q(x_b)Q(T(P_n)|x_b)^\alpha} &(85)\\
&\ge \frac{1}{(n+1)^{\alpha|\mathcal{Y}|}} 2^{-n\alpha(D(P_n||Q_{x_a})-D(P_n||Q_{x_b})}. &(86)
\end{aligned}
$$

Since for sufficiently large n, $D(P_n||Q_{x_b}) < D(P_n||Q_{x_a})$ ($P^\star \in D_{x_b}$), the ratio can be made arbitrarily small. Hence, $F(x_b,P_n)^{1/\alpha-1} = F(x_1(P_n),P_n)^{1/\alpha-1} < \frac{1}{2}F(x_a,P_n)^{1/\alpha-1}$ for sufficiently large n. Thus,

$$
\begin{aligned}
I_\alpha^S(X;Y^n) &\le H_{1/\alpha}(X) + \frac{\alpha F(x_a,P_n)}{(\alpha-1)\ln 2}\cdot &(87)\\
&\qquad \frac{F(x_1(P_n),P_n)^{1/\alpha-1} - F(x_a,P_n)^{1/\alpha-1}}{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}} \\
&\le H_{1/\alpha}(X) - \frac{\alpha}{2(\alpha-1)\ln 2}\cdot\frac{F(x_a,P_n)^{1/\alpha}}{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}}. &(88)
\end{aligned}
$$

From the type-theoretic bound (21),

$$
\begin{aligned}
I_\alpha^S(X;Y^n) &\le H_{1/\alpha}(X) \\
&\quad - \frac{\alpha}{2(\alpha-1)\ln 2}\frac{Q_{\min}(X)^{1/\alpha}}{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}}\cdot\frac{2^{-nD(P_n||Q_{x_a})}}{(n+1)^{|\mathcal{Y}|}},
\end{aligned}
\tag{89}
$$

where $Q_{\min}(X) = \min_{x\in\mathcal{X}} Q(x)$. This implies

$$
\begin{aligned}
&\limsup_{n\to\infty} -\frac{1}{n}\log\left(H_{1/\alpha}(X) - I_\alpha^S(X;Y^n)\right) \\
&\le \lim_{n\to\infty} D(P_n||Q_{x_a}) = D(P^*||Q_{x_a}).
\end{aligned}
\tag{90}
$$

Since $x_a \neq x_b$ and $P \in D_{x_b}$ were arbitrarily chosen, this implies:

$$
\begin{aligned}
&\limsup_{n\to\infty} -\frac{1}{n}\log\left(H_{1/\alpha}(X) - I_\alpha^S(X;Y^n)\right) \\
&\qquad \le \min_{x\neq x'} \inf_{P\in\bar{D}_x} D(P||Q_{x'}) = \min_{x\neq x'} \mathscr{C}(Q_x||Q_{x'}),
\end{aligned}
\tag{91}
$$

where the last step used Lemma 4 in Appendix A.

VI. Proof for Maximal Leakage

We turn to proving (34) for the case $\alpha = \infty$. While the lower bound on $I_\infty^S(X;Y^n)$ can be proven directly, we will instead note that it can be obtained from Lemma 2 by letting $\alpha \to \infty$ and then $n \to \infty$.

For the upper bound, recalling the x-domains defined in (22) and (23), fix $x_a \neq x_b \in \mathcal{X}$ and a $P \in D_{x_b}$ and let $\{P_n\}_{n=1}^{\infty}$ be a sequence such that $P_n \in \mathcal{P}_n$ for each n and $P_n \to P$. Using the fact that $\cup_x \bar{D}_x$ covers $\mathcal{P}_n$ and $\max_{x'} Q(T(P)|x') = Q(T(P)|x)$ if $P \in \bar{D}_x$, we have

$$
\begin{aligned}
I_\infty^S(X;Y^n) &\le \log \sum_{x\in\mathcal{X}} \sum_{P\in\bar{D}_x\cap\mathcal{P}_n} Q(T(P)|x) &(92)\\
&= \log\Big[|\mathcal{X}| - \sum_{x\in\mathcal{X}} \sum_{P\in\mathcal{P}_n\setminus\bar{D}_x} Q(T(P)|x)\Big]. &(93)
\end{aligned}
$$

Now $P_n \in D_{x_b}$ for sufficiently large n so

$$
\begin{aligned}
&\le \log\Big[|\mathcal{X}| - \sum_{P\in\mathcal{P}_n\setminus\bar{D}_{x_a}} Q(T(P)|x_a)\Big] &(94)\\
&\le \log\big[|\mathcal{X}| - Q(T(P_n)|x_a)\big], &(95)
\end{aligned}
$$

for sufficiently large n. Thus for sufficiently large n, from (21),

$$
\begin{aligned}
I_\infty^S(X;Y^n) &\le \log\Big[|\mathcal{X}| - \frac{1}{(n+1)^{|\mathcal{Y}|}}2^{-nD(P_n||Q_{x_a})}\Big] &(96)\\
&\le \log\big[|\mathcal{X}|\big] - \frac{2^{-nD(P_n||Q_{x_a})}}{(\ln 2)|\mathcal{X}|(n+1)^{|\mathcal{Y}|}}, &(97)
\end{aligned}
$$

and

$$
\begin{aligned}
&\limsup_{n\to\infty} -\frac{1}{n}\log\left(|\mathcal{X}| - I_\infty^S(X;Y^n)\right) \\
&\qquad \le \lim_{n\to\infty} D(P_n||Q_{x_a}) = D(P||Q_{x_a}).
\end{aligned}
\tag{98}
$$

Since $x_a \neq x_b$ and P were arbitrary, the result follows by Lemma 4 in Appendix A.

VII. Proof for Arimoto

Note that (35) for the case $\alpha = 1$ has already been proven. We prove the lower and upper bounds for the $\alpha > 1$ case as follows.

From (13), we have

$$
H_\alpha(X) - I_\alpha^A(X;Y^n) = H_\alpha(X|Y^n). \tag{99}
$$

Sason and Verdú [27, Propositions 1 and 2] showed that

$$
H_\infty(X|Y^n) \le H_\alpha(X|Y^n) \le \frac{\alpha}{\alpha-1}H_\infty(X|Y^n). \tag{100}
$$

Therefore,

$$\begin{align}&\lim_{n\to\infty} -\frac{1}{n}\log\Big(H_\alpha(X) - I_\alpha^A(X;Y^n)\Big)\\ &\qquad = \lim_{n\to\infty} -\frac{1}{n}\log\Big(H_\infty(X|Y^n)\Big). \tag{101}\end{align}$$

Define

$$\epsilon_{X|Y^n} = \min_{f:\mathcal{Y}^n\to X} P(X \neq f(Y^n)). \tag{102}$$

By the definition of H_∞, we have

$$H_\infty(X|Y^n) = \log\frac{1}{1-\epsilon_{X|Y^n}}. \tag{103}$$

Now note that for $0<\epsilon\leq 1/2$,

$$\frac{\epsilon}{\ln 2} \leq \log\frac{1}{1-\epsilon} \leq \frac{1}{\ln 2}\frac{\epsilon}{1-\epsilon} \leq \frac{2\epsilon}{\ln 2}. \tag{104}$$

Combining (101), (103), and (104) yields

$$\begin{align}&\lim_{n\to\infty} -\frac{1}{n}\log\Big(H_\alpha(X) - I_\alpha^A(X;Y^n)\Big)\\ &\qquad = \lim_{n\to\infty} -\frac{1}{n}\log\epsilon_{X|Y^n}. \tag{105}\end{align}$$

The result then follows from the result of Kanaya and Han [13, Theorem 2] stating that

$$\lim_{n\to\infty} -\frac{1}{n}\log\epsilon_{X|Y^n} = \min_{x\neq x'}\mathscr{C}(Q_x||Q_{x'}). \tag{106}$$

VIII. Proof for α-Maximal Leakage

Note that for $\alpha=1$, α-maximal leakage is given by regular mutual information, so that case is already proven.

A. Proof of Lower Bound

Proof: We obtain the lower bound by choosing $X\sim Q^{(u)}$, where $Q^{(u)}(X)$ denotes the uniform distribution over $\mathcal{X}$. Then

$$\mathcal{L}_\alpha^{max}(X\to Y) = \max_{Q(X)} I_\alpha^S(X;Y^n) \geq I_\alpha^S(X;Y^n)|_{Q^{(u)}(X)}. \tag{107}$$

Then by (34),

$$\begin{align}&\liminf_{n\to\infty} -\frac{1}{n}\log(\log|\mathcal{X}| - \mathcal{L}_\alpha^{max}(X\to Y))\\ &\qquad \geq \min_{x\neq x'}\mathscr{C}(Q_x||Q_{x'}). \tag{108}\end{align}$$

□

B. Proof of Upper Bound

Proof: As with the proof for Shannon capacity, the idea is to show that the maximizing $Q(X)$ must eventually be contained in a neighborhood of the uniform distribution. Over this neighborhood, we can use Lemma 3 to uniformly bound the difference

$$\log|\mathcal{X}| - \max_{Q(X)} I_\alpha^S(X;Y^n). \tag{109}$$

First, for each n, let

$$Q_n(X) \in \arg\max_{Q(X)} I_\alpha^S(X;Y^n). \tag{110}$$

We have [15, Ex. 2 and Thm. 3]

$$H_{1/\alpha}(X)|_{Q_n(X)} \geq I_\alpha^S(X;Y^n)|_{Q_n(X)}, \tag{111}$$

and thus, by Lemma 2,

$$\begin{align}&H_{1/\alpha}(X)|_{Q_n(X)}\\ &\geq I_\alpha^S(X;Y^n)|_{Q^{(u)}(X)} \tag{112}\\ &\geq H_{1/\alpha}(X)|_{Q^{(u)}(X)} - \frac{\alpha}{(\alpha-1)\ln 2}\left(\Gamma_n + \frac{\Gamma_n^2}{2(1-\Gamma_n)}\right). \tag{113}\end{align}$$

Then,

$$\begin{align}&H_{1/\alpha}(X)|_{Q_n(X)} \geq H_{1/\alpha}(X)|_{Q^{(u)}(X)} \tag{114}\\ &\qquad\qquad - \frac{\alpha}{(\alpha-1)\ln 2}\left(\Gamma_n + \frac{\Gamma_n^2}{2(1-\Gamma_n)}\right)\\ &H_{1/\alpha}(X)|_{Q^{(u)}(X)} - H_{1/\alpha}(X)|_{Q_n(X)} \tag{115}\\ &\qquad\qquad \leq \frac{\alpha}{(\alpha-1)\ln 2}\left(\Gamma_n + \frac{\Gamma_n^2}{2(1-\Gamma_n)}\right)\\ &D_{1/\alpha}(Q_n(X)||Q^{(u)}(X)) \tag{116}\\ &\qquad\qquad \leq \frac{\alpha}{(\alpha-1)\ln 2}\left(\Gamma_n + \frac{\Gamma_n^2}{2(1-\Gamma_n)}\right) \equiv \epsilon_n,\end{align}$$

where we have used the fact that $H_{1/\alpha}(X)|_{Q^{(u)}(X)} - H_{1/\alpha}(X)|_{Q_n(X)} = D_{1/\alpha}(Q_n(X)||Q^{(u)}(X))$. Note that $\lim_{n\to\infty}\epsilon_n = 0$. Then, using the Rényi version of Pinsker's Inequality ([28, Thm. 31]),

$$\begin{align}D_{1/\alpha}(Q_n(X)||Q^{(u)}(X)) &\geq \frac{2}{\alpha}\sup_A |Q_n(A) - Q^{(u)}(A)|^2 \tag{117}\\ &\geq \frac{2}{\alpha}\sup_x |Q_n(x) - Q^{(u)}(x)|^2, \tag{118}\end{align}$$

and so

$$\epsilon_n \geq \frac{2}{\alpha}\sup_x |Q_n(x) - Q^{(u)}(x)|^2. \tag{119}$$

It also follows that, under this constraint,

$$\begin{align}\epsilon_n &\geq \frac{2}{\alpha}(Q^{(u)}(x) - \min_{x'} Q_n(x'))^2 \tag{120}\\ \sqrt{\frac{\alpha\epsilon_n}{2}} &\geq Q^{(u)}(x) - \min_{x'} Q_n(x') \tag{121}\\ \min_{x'} Q_n(x') \equiv Q_{\min,n}(X) &\geq \frac{1}{|\mathcal{X}|} - \sqrt{\frac{\alpha\epsilon_n}{2}} \tag{122}\end{align}$$

and similarly,

$$\max_{x'} Q_n(x') \equiv Q_{\max,n}(X) \leq \frac{1}{|\mathcal{X}|} + \sqrt{\frac{\alpha\epsilon_n}{2}} \tag{123}$$

Let A_n be the set of distributions over X that satisfy both (122) and (123) and note that $Q_n \in A_n$ for sufficiently large n. Recalling (70), define

$$F(x, P, \tilde{Q}) = \tilde{Q}(x)Q(T(P)|x)^\alpha, \tag{124}$$

where we now indicate the dependence on the input distribution $\tilde{Q}(x)$. Similarly, we let $\{E_{x_i,\tilde{Q}}^{(n)}\}$ be a partition of $\mathcal{P}_n$

such that $P \in E^{(n)}_{x,\tilde{Q}}$ implies $F(x,P,\tilde{Q}) = \max_{x'} F(x',P,\tilde{Q})$ and we let $x_1(P,\tilde{Q})$, $x_2(P,\tilde{Q})$, $\ldots$, denote the letters of $\mathcal{X}$ in decreasing order of (124). By Lemma 3, we have, for sufficiently large n,

$$\begin{aligned}
&\max_{\tilde{Q}} I^S_\alpha(X;Y^n)\\
&= \max_{\tilde{Q}\in A_n} I^S_\alpha(X;Y^n)\\
&\le \max_{\tilde{Q}\in A_n} H_{1/\alpha}(X) + \frac{\alpha}{(\alpha-1)\ln 2} \sum_{x\in\mathcal{X}} \sum_{P\notin E^{(n)}_{x,\tilde{Q}}} \frac{F(x,P,\tilde{Q})}{\sum\limits_{x'\in\mathcal{X}} \tilde{Q}(x')^{1/\alpha}}\\
&\qquad \left[F(x_1(P,\tilde{Q}),P,\tilde{Q})^{1/\alpha-1} - F(x,P,\tilde{Q})^{1/\alpha-1}\right].
\end{aligned} \tag{125}$$

Fix $x_a \neq x_b$ and $P^* \in D_{x_b}$ and let P_n be a sequence of types converging to P^*. Then for all sufficiently large n, we have that $P_n \in E^{(n)}_{x_b,\tilde{Q}}$ for all $\tilde{Q} \in A_n$. Then because the summands in (125) are nonpositive, we have

$$\begin{aligned}
&\max_{\tilde{Q}\in A_n} I^S_\alpha(X;Y^n)\\
&\le \max_{\tilde{Q}\in A_n} H_{1/\alpha}(X) + \Bigg[\alpha F(x_a,P_n,\tilde{Q})\cdot \qquad (126)\\
&\qquad \frac{F(x_1(P_n,\tilde{Q}),P_n,\tilde{Q})^{1/\alpha-1} - F(x_a,P_n,\tilde{Q})^{1/\alpha-1}}{(\alpha-1)\ln 2 \sum\limits_{x\in\mathcal{X}} \tilde{Q}(x)^{1/\alpha}}\Bigg].
\end{aligned}$$

Note that, since $P^* \in D_{x_b}$, for all sufficiently large n, for some $\epsilon > 0$ we have $D(P_n||Q_{x_b}) < \epsilon < D(P_n||Q_x)$ for all $x \neq x_b$. This implies that, for sufficiently large n, $x_1(P_n,\tilde{Q}) = x_b$ for all $\tilde{Q} \in A_n$ and $F(x_b,P_n,\tilde{Q})^{1/\alpha-1} < \frac{1}{2}F(x_a,P_n,\tilde{Q})^{1/\alpha-1}$ for all $\tilde{Q} \in A_n$ (by the same argument as the one made in equation (85), $F(x_a,P_n,\tilde{Q})$ and $F(x_b,P_n,\tilde{Q})$ decrease exponentially fast with the former decreasing at a faster rate). The remainder of the argument proceeds analogously to the Sibson proof. For sufficiently large n, we have

$$\max_{\tilde{Q}\in A_n} I^S_\alpha(X;Y^n) \tag{127}$$

$$\le \max_{\tilde{Q}\in A_n} H_{1/\alpha}(X) - \frac{1}{2}\frac{\alpha}{(\alpha-1)\ln 2}\cdot\frac{1}{\sum_{x\in\mathcal{X}} \tilde{Q}(x)^{1/\alpha}} \tag{128}$$

$$\cdot F(x_a,P_n,\tilde{Q})^{1/\alpha} \tag{129}$$

$$\le \max_{\tilde{Q}\in A_n} H_{1/\alpha}(X) - \frac{1}{2}\frac{\alpha}{(\alpha-1)\ln 2}\cdot\frac{1}{|\mathcal{X}|\left(\frac{1}{|\mathcal{X}|}+\sqrt{\frac{\alpha\epsilon_n}{2}}\right)^{1/\alpha}} \tag{130}$$

$$\cdot\left(\frac{1}{|\mathcal{X}|}-\sqrt{\frac{\alpha\epsilon_n}{2}}\right)^{1/\alpha}\frac{1}{(n+1)^{|\mathcal{Y}|}}2^{-nD(P_n||Q_{x_a})} \tag{131}$$

$$\le \log|\mathcal{X}| - \frac{1}{2}\frac{\alpha}{(\alpha-1)\ln 2}\frac{1}{|\mathcal{X}|\left(\frac{1}{|\mathcal{X}|}+\sqrt{\frac{\alpha\epsilon_n}{2}}\right)^{1/\alpha}} \tag{132}$$

$$\cdot\left(\frac{1}{|\mathcal{X}|}-\sqrt{\frac{\alpha\epsilon_n}{2}}\right)^{1/\alpha}\frac{1}{(n+1)^{|\mathcal{Y}|}}2^{-nD(P_n||Q_{x_a})}. \tag{133}$$

This implies that

$$\begin{aligned}
&\lim_{n\to\infty} -\frac{1}{n}\log\left(\log|\mathcal{X}| - \max_{\tilde{Q}(X)} I^S_\alpha(X;Y^n)\right)\\
&\qquad\le \min_{x\neq x'} \mathscr{C}(Q_x||Q_{x'}),
\end{aligned} \tag{134}$$

by Lemma 4 in Appendix A, which implies the result for $1 < \alpha < \infty$. The $\alpha = \infty$ case follows from (34) since $I^S_\infty(X;Y^n)$ does not depend on $Q(X)$, and $H_{1/\alpha}(X) = \log|\mathcal{X}|$ in that case. □

Appendix A
An Ancillary Lemma

Recall that Q_x denotes the distribution of Y given x, and for any $P \in \mathcal{P}$, $x_k(P)$ denotes $x \in \mathcal{X}$ such that $D(P||Q_x)$ is the k^{th} smallest relative entropy across all elements of $\mathcal{X}$.

Lemma 4:

$$\inf_{P\in\mathcal{P}} D(P||Q_{x_2(P)}) = \min_{x\neq x'} \mathscr{C}(Q_x||Q_{x'}), \tag{135}$$

where both quantities may be infinite.

Proof: We will separately prove that

$$\inf_{P\in\mathcal{P}} D(P||Q_{x_2(P)}) \le \min_{x\neq x'} \mathscr{C}(Q_x||Q_{x'}) \tag{136}$$

and

$$\inf_{P\in\mathcal{P}} D(P||Q_{x_2(P)}) \ge \min_{x\neq x'} \mathscr{C}(Q_x||Q_{x'}). \tag{137}$$

To prove the upper bound, fix $x \neq x'$ and consider $P_\lambda(y) = P_\lambda(Q_x,Q_{x'},y)$ as defined in (16). Choose λ^* such that $D(P_{\lambda^*}||Q_x) = D(P_{\lambda^*}||Q_{x'})$. Then, certainly

$$D(P_{\lambda^*}||Q_{x_2(P_{\lambda^*})}) \le \mathscr{C}(Q_x||Q_{x'}) \tag{138}$$

since we know of two X-values whose corresponding $Q(Y|X)$ distributions are equidistant to P_{λ^*}, from which (136) follows.

For the lower bound, we first define subsets of $\mathcal{P}$:

$$E_x = \{P\in\mathcal{P} \mid D(P||Q_x) \le \mathscr{C}(Q_x||Q_{x'})\} \tag{139}$$

$$E_{x'} = \{P\in\mathcal{P} \mid D(P||Q_{x'}) \le \mathscr{C}(Q_x||Q_{x'})\}. \tag{140}$$

Note that E_x and $E_{x'}$ are convex sets since $D(\cdot||\cdot)$ is convex and that P_{λ^*} achieves the minimum distance to $Q_{x'}$ in E_x and the minimum distance to Q_x in $E_{x'}$ [17, Sec. 11.9].

Choose any $P \in \mathcal{P}$. There are three cases to consider, depending on the location of P in $\mathcal{P}$-space.

Case 1: $P \notin E_x$ and $P \notin E_{x'}$. By construction, $D(P||Q_x) \ge \mathscr{C}(Q_x||Q_{x'})$ and $D(P||Q_{x'}) \ge \mathscr{C}(Q_x||Q_{x'})$.

Case 2: $P \in E_x$. Using the Pythagorean theorem for relative entropy [17, Thm. 11.6.1],

$$D(P||Q_{x'}) \ge D(P||P_{\lambda^*}) + D(P_{\lambda^*}||Q_{x'}) \tag{141}$$

Case 3: $P \in E_{x'}$. By the same argument,

$$D(P||Q_x) \ge D(P||P_{\lambda^*}) + D(P_{\lambda^*}||Q_x). \tag{142}$$

Hence, for any $P \in \mathcal{P}$,

$$\max\{D(P||Q_x), D(P||Q_{x'})\} \ge \mathscr{C}(Q_x||Q_{x'}) \tag{143}$$

Since $D(P||Q_{x_2(P)}) = \min_{x \neq x'} \max\{D(P||Q_x), D(P||Q_{x'})\}$,

$$\inf_{P \in \mathcal{P}} D(P||Q_{x_2(P)}) \geq \min_{x \neq x'} \mathscr{C}(Q_x||Q_{x'}). \tag{144}$$

□

The following result is standard and the proof is omitted.

Lemma 5: For any discrete distributions P_1 and P_2 on a common alphabet $\mathcal{X}$,

$$\mathscr{C}(P_1^n||P_2^n) = n\mathscr{C}(P_1||P_2) \tag{145}$$

Appendix B
Data Processing for Arimoto Mutual Information

As a generalization of Shannon conditional entropy, Arimoto-Rényi conditional entropy satisfies a number of desirable properties. In particular, the rule that conditioning cannot increase entropy carries over to the Arimoto-Rényi version [16], [24, Thm. 2], [26, Corr. 1], [29, Prop. 2]:

$$H_\alpha(X|Y,Z) \leq H_\alpha(X|Y). \tag{146}$$

It follows from (13) that a "right-hand" data processing inequality therefore holds: if $X \leftrightarrow Y \leftrightarrow Z$ form a Markov chain, then

$$I_\alpha^A(X;Z) \leq I_\alpha^A(X;Y). \tag{147}$$

To reduce our problem to an instance satisfying the distinct row assumption using the technique in Section III, we require a "left-hand" version of the inequality, i.e.,

$$I_\alpha^A(X;Z) \leq I_\alpha^A(Y;Z)? \tag{148}$$

In fact, this inequality can fail dramatically.

Proposition 1: For any $1 < \alpha < \infty$, there exist random variables X, Y, and Z such that $X \leftrightarrow Y \leftrightarrow Z$ and $Y \leftrightarrow X \leftrightarrow Z$ with $I_\alpha^A(X;Z)$ being arbitrarily small and $I_\alpha^A(Y;Z)$ being arbitrarily large.

Proof: Fix positive integers K and L and $0 < \epsilon < 1/L$. Let Y and Z be jointly distributed as

$$P(Y = i) = \begin{cases} \epsilon & \text{if } i \in \{1, \ldots, L\} \\ \frac{1-L\epsilon}{K} & \text{if } i \in \{L+1, \ldots, L+K\} \end{cases} \tag{149}$$

$$P(Z = j|Y = i) = \begin{cases} 1 & \text{if } j = i \text{ and } i \in \{1, \ldots, L\} \\ \frac{1}{L} & \text{if } i \in \{L+1, \ldots, L+K\} \\ 0 & \text{otherwise.} \end{cases} \tag{150}$$

We then couple X to Y and Z via

$$X = \min(Y, L+1). \tag{151}$$

From (4), as $\epsilon \to 0$, we have that $I_\alpha^A(X;Z) \to 0$. Fix ϵ so that $I_\alpha^A(X;Z)$ is as small as desired. If we then let $K \to \infty$, we have

$$I_\alpha^A(Y;Z) \to \frac{\alpha}{\alpha - 1} \log L. \tag{152}$$

But L was arbitrary. □

For Sibson mutual information and α-maximal leakage, we could reduce our problem to one satisfying the distinct row assumption by dividing $\mathcal{X}$ into equivalence classes based on $P_{Y|X}(\cdot|x)$ and assigning to a "leader" realization in each equivalence class the probability of all of the x realizations in that class. This approach fails for Arimoto mutual information, due to the above result, but the reduction is still possible if one accounts for the exponential tilting of $P(x)$ in (4).

Proposition 2: Fix $\alpha > 0$. If (X, Y) does not satisfy the distinct row assumption then there exists $\tilde{X}$ such that

(*i*) The support of $\tilde{X}$ is strictly contained within the support of X;

(*ii*) $P_{Y|X}(y|x) = P_{Y|\tilde{X}}(y|x)$ for all x and y;

(*iii*) $(\tilde{X}, Y)$ satisfies the distinct row assumption; and

(*iv*) $I_\alpha^A(X;Y) = I_\alpha^A(\tilde{X};Y)$.

Proof: For $\alpha = 1$, this follows directly from the chain rule for mutual information. For $\alpha \neq 1$, without loss of generality, we may assume that there exists a $k < |\mathcal{X}|$ such that

$$P_{Y|X}(\cdot|x_j) \neq P_{Y|X}(\cdot|x_i) \tag{153}$$

for all $1 \leq i < j \leq k$, and for all $k < j \leq |\mathcal{X}|$ there exists $1 \leq i \leq k$ such that

$$P_{Y|X}(y|x_j) = P_{Y|X}(y|x_i) \text{ for all } y. \tag{154}$$

That is, the first k rows of $P_{Y|X}$, viewed as a stochastic matrix, are distinct, and every other row is a copy of one of those k rows. For each $1 \leq i \leq k$, define the set of X realizations

$$C_i = \left\{x \in \mathcal{X} : P_{Y|X}(y|x) = P_{Y|X}(y|x_i) \text{ for all } y\right\}, \tag{155}$$

and note that $C_1, \ldots, C_k$ are nonempty and form a partition of $\mathcal{X}$. Define $\tilde{X}$ to have support $\{x_1, \ldots, x_k\}$ with marginal distribution

$$P(\tilde{X} = x_i) = \frac{1}{\Gamma}\left(\sum_{x \in C_i} P(X = x)^\alpha\right)^{1/\alpha}, \tag{156}$$

where

$$\Gamma = \sum_{i=1}^k \left(\sum_{x \in C_i} P(X = x)^\alpha\right)^{1/\alpha}. \tag{157}$$

Define the joint distribution between $\tilde{X}$ and Y through (*ii*). Then (*i*)-(*iii*) clearly hold and we have

$$\begin{aligned} &I_\alpha^A(X;Y) \\ &= \frac{\alpha}{\alpha - 1} \log \sum_y \left(\frac{\sum_{i=1}^k \sum_{x \in C_i} P(x)^\alpha P(y|x)^\alpha}{\sum_{i=1}^k \sum_{x \in C_i} P(x)^\alpha}\right)^{1/\alpha} && (158) \\ &= \frac{\alpha}{\alpha - 1} \log \sum_y \left(\frac{\sum_{i=1}^k \sum_{x \in C_i} (P(x)^\alpha/\Gamma^\alpha) P(y|x)^\alpha}{\sum_{i=1}^k \sum_{x \in C_i} (P(x)^\alpha/\Gamma^\alpha)}\right)^{1/\alpha} && (159) \\ &= \frac{\alpha}{\alpha - 1} \log \sum_y \left(\frac{\sum_{i=1}^k P(\tilde{X} = x_i)^\alpha P(y|x)^\alpha}{\sum_{i=1}^k P(\tilde{X} = x_i)^\alpha}\right)^{1/\alpha} && (160) \\ &= I_\alpha^A(\tilde{X};Y). && (161) \end{aligned}$$

□

Acknowledgment

The authors would like to thank the anonymous reviewers for their helpful feedback, and, in particular, the reviewer who called our attention to [13] and pointed out that our proof in the Arimoto case could be shortened by relying more heavily on the results in [27].

References

[1] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proc. IACR CRYPTO*, in Lecture Notes in Computer Science, vol. 1109, Aug. 1996, pp. 104–113.

[2] C. Wampler, S. Uluagac, and R. Beyah, "Information leakage in encrypted IP video traffic," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–7.

[3] Y. Zhu, Y. Lu, and A. Vikram, "On privacy of encrypted speech communications," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 4, pp. 470–481, Jul. 2012.

[4] P. Kairouz, S. Oh, and P. Viswanath, "The composition theorem for differential privacy," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 4037–4049, Jun. 2017.

[5] C. Dwork and G. N. Rothblum, "Concentrated differential privacy," 2016, *arXiv:1603.01887*.

[6] I. Mironov, "Rényi differential privacy," in *Proc. IEEE Comp. Sec. Found. Symp.*, Jun. 2017, pp. 263–275.

[7] I. Issa, A. B. Wagner, and S. Kamath, "An operational approach to information leakage," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1625–1657, Mar. 2020.

[8] I. Issa, S. Kamath, and A. B. Wagner, "Maximal leakage minimization for the Shannon cipher system," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2016, pp. 520–524.

[9] I. Issa and A. B. Wagner, "Operational definitions for some common information leakage metrics," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2017, pp. 769–773.

[10] I. Issa, S. Kamath, and A. B. Wagner, "An operational measure of information leakage," in *Proc. Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2016, pp. 234–239.

[11] J. Liao, O. Kosut, L. Sankar, and F. P. Calmon, "Tunable measures for information leakage and applications to privacy-utility tradeoffs," *IEEE Trans. Inf. Theory*, vol. 65, no. 12, pp. 8043–8066, Dec. 2019.

[12] D. M. Smith and G. Smith, "Tight bounds on information leakage from repeated independent runs," in *Proc. IEEE 30th Comput. Secur. Found. Symp. (CSF)*, Aug. 2017, pp. 318–327.

[13] F. Kanaya and T. Sun Han, "The asymptotics of posterior entropy and error probability for Bayesian estimation," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1988–1992, Nov. 1995.

[14] R. Sibson, "Information radius," *Z. Wahrscheinlichkeitstheorie Verwandte Gebiete*, vol. 14, no. 2, pp. 149–160, 1969. [Online]. Available: http://link.springer.com/10.1007/BF00537520

[15] S. Verdú, "A-mutual information," in *Proc. Inf. Theory Appl. Workshop (ITA)*, Feb. 2015, pp. 1–6.

[16] S. Arimoto, "Information measures and capacity of order α for discrete memoryless channels," in *Topics in Information*, J. Bolyai, Ed. 1975, pp. 41–52.

[17] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. 2006.

[18] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Budapest: Akadémiai Kiadó, 1981.

[19] B. Wu, A. B. Wagner, G. E. Suh, and I. Issa, "Strong asymptotic composition theorems for sibson mutual information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 2222–2227.

[20] I. Csiszar, "Generalized cutoff rates and Renyi's information measures," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 26–34, Jan. 1995.

[21] A. Lapidoth and C. Pfister, "Two measures of dependence," in *Proc. IEEE Int. Conf. Sci. Electr. Eng. (ICSEE)*, Nov. 2016, pp. 1–5.

[22] A. Lapidoth and C. Pfister, "Testing against independence and a Rényi information measure," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2018, pp. 1–5.

[23] Y. Polyanskiy and S. Verdu, "Arimoto channel coding converse and Rényi divergence," in *Proc. 48th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2010, pp. 1327–1333.

[24] S. Fehr and S. Berens, "On the conditional Rényi entropy," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6801–6810, Nov. 2014.

[25] B. Wu, A. B. Wagner, and G. E. Suh, "Optimal mechanisms under maximal leakage," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2020, pp. 1–6.

[26] G. Aishwarya and M. Madiman, "Remarks on Rényi versions of conditional entropy and mutual information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 1117–1121.

[27] I. Sason and S. Verdú, "Arimoto–Rényi conditional entropy and Bayesian M-ary hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 4–25, Jan. 2018.

[28] T. van Erven and P. Harremoës, "Rényi divergence and Kullback–Leibler divergence," 2012, *arXiv:1206.2459*.

[29] E. Arikan, "An inequality on guessing and its application to sequential decoding," *IEEE Trans. Inf. Theory*, vol. 42, no. 1, pp. 99–105, 1996.

Benjamin Wu (Member, IEEE) received the B.S. degree in applied and computational mathematics from the California Institute of Technology in 2015 and the Ph.D. degree in electrical and computer engineering from Cornell University in 2021. He is currently a Systems Engineer with L3Harris Technologies Inc., Anaheim, CA, USA.

Aaron B. Wagner (Fellow, IEEE) received the B.S. degree in electrical engineering from the University of Michigan, Ann Arbor, in 1999, and the M.S. and Ph.D. degrees in electrical engineering and computer sciences from the University of California at Berkeley in 2002 and 2005, respectively.

From 2005 to 2006, he was a Post-Doctoral Research Associate with the Coordinated Science Laboratory, University of Illinois at Urbana–Champaign, and a Visiting Assistant Professor with the School of Electrical and Computer Engineering, Cornell University. Since 2006, he has been with the School of Electrical and Computer Engineering, Cornell University, where he is currently a Professor. He has received the NSF CAREER Award, the David J. Sakrison Memorial Prize from the U.C. Berkeley EECS Department, the Bernard Friedman Memorial Prize in Applied Mathematics from the U.C. Berkeley Department of Mathematics, the James L. Massey Research and Teaching Award for Young Scholars from the IEEE Information Theory Society, and teaching awards at the department, college, and university level at Cornell University. He was a Distinguished Lecturer of the IEEE Information Theory Society from 2018 to 2019.

Ibrahim Issa (Member, IEEE) received the B.E. degree in computer and communications engineering from the American University of Beirut, Lebanon, in 2012, and the Ph.D. degree in electrical and computer engineering from Cornell University, USA, in 2017. From August 2017 to December 2018, he was a Post-Doctoral Researcher with the Laboratory for Information in Networked Systems, École Polytechnique Fédérale de Lausanne, Switzerland. In January 2019, he joined the Electrical and Computer Engineering Department, American University of Beirut, as an Assistant Professor. His current research interests include privacy and security, information theory, machine learning, and quantum information theory. He received the Outstanding ECE Ph.D. Thesis Research Award at Cornell University for his thesis on information leakage.

G. Edward Suh (Fellow, IEEE) received the B.S. degree in electrical engineering from Seoul National University in 1999 and the M.S. and Ph.D. degrees in electrical engineering and computer science from the Massachussets Institute of Technology in 2001 and 2005, respectively. He is currently a Professor with the School of Electrical and Computer Engineering, Cornell University, and a Research Scientist with Meta AI. Before joining Cornell University in 2007, he led the Commercial Development of the Physical Unclonable Function (PUF) Technology at Veryao Inc., which is now used in products, such as Xilinx UltraScale+ MPSoC for storing secret keys. He also did early research work on dynamic cache partitioning and secure processor technologies. His current research interests include building systems with verifiable security/privacy guarantees and developing tools and architecture for application-specific accelerators, with a focus on machine learning applications.