# Strong Asymptotic Composition Theorems for Sibson Mutual Information

Benjamin Wu, Aaron B. Wagner, and G. Edward Suh
School of Electrical and Computer Engineering
Cornell University
Ithaca, NY 14853 USA
Email: {bhw49@,wagner@,suh@ece}.cornell.edu

Ibrahim Issa
Dept. of Electrical and Computer Engineering
American University of Beirut
Beirut, Lebanon
Email: ii19@aub.edu.lb

***Abstract*—We characterize the growth of the Sibson mutual information, of any order that is at least unity, between a random variable and an increasing set of noisy, conditionally independent observations of the random variable. The Sibson mutual information increases to an order-dependent limit exponentially fast, with an exponent that is order-independent. The result is contrasted with composition theorems in differential privacy.**

## 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]–[3] or database privacy [4]–[6]. Thus composition theorems are practically useful. They also raise theoretical questions that are interesting in their own right.

Various composition theorems for differential privacy and its variants have been established [4]–[6]. For the information-theoretic metrics of mutual information and maximal leakage [7]–[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 $\alpha$-maximal leakage [11], less is known. While similar theorems have been studied in the case that $P(y|x)$ not known [12], 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 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.

We prove such a result for both mutual information and maximal leakage. The limits are readily identified as the entropy and log-support size, respectively, of the minimal sufficient statistic of $Y$ given $X$. In both cases, the speed of convergence to the limit is exponential, and the exponent turns out to the same. Specifically, it is the minimum Chernoff information among all pairs of distributions $Q_{Y|X}(\cdot|x)$ and $Q_{Y|X}(\cdot|x')$, where $x$ and $x'$ are distinct realizations of $X$.

Mutual information and maximal leakage are both instances of Sibson mutual information [10], [13], [14], the former being order 1 and the latter being order $\infty$. 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. We show that this is indeed the case.

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, and characterize the growth of leakage with repeated looks in terms of 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 [15, Prob. 7.20].

## II. Sibson, Rényi, and Chernoff

The central quantity of this study is the *Sibson mutual information*.

**Definition 1** ( [13], [14])**.** *The Sibson mutual information of order $\alpha$ 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 $\alpha \in (0,1) \cap (1,\infty)$ 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.*

We are interested in how $I_\alpha^S(X;Y^n)$ grows 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 but is not considered here. For $\alpha \geq 1$, we shall see that the limit is given by a *Rényi entropy*.

**Definition 2.** *The Rényi entropy of order $\alpha$ of a random variable $X$ is given by:*

$$H_\alpha(X) = \frac{1}{1-\alpha}\log\sum_{x\in\mathcal{X}} P(x)^\alpha \tag{4}$$

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

$$H_0(X) = \log|\{x : P(x) > 0\}| \tag{5}$$
$$H_1(X) = H(X). \tag{6}$$

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

The speed of convergence of $I_\alpha^S(X;Y^n)$ to its limit will turn out to be governed by a *Chernoff information.*

**Definition 3** ( [15])**.** *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:*

$$P_\lambda(x) = P_\lambda(P_1,P_2,x) = \frac{P_1(x)^\lambda P_2(x)^{1-\lambda}}{\sum_{x'\in\mathcal{X}} P_1(x')^\lambda P_2(x')^{1-\lambda}} \tag{7}$$

*Then, the Chernoff information is given by:*

$$\mathscr{C}(P_1||P_2) = D(P_{\lambda^*}||P_1) = D(P_{\lambda^*}||P_2) \tag{8}$$

*where $\lambda^*$ is the value of $\lambda$ such that the above two relative entropies are equal.*

## III. Main Result

Let $X$ be a random variable with finite alphabet $\mathcal{X} = \{x_1,x_2,...x_{|\mathcal{X}|}\}$. Let $Y^n = (Y_1,Y_2,...Y_n)$ be a vector of discrete random variables with a shared alphabet $\mathcal{Y} = \{y_1,y_2,...y_{|\mathcal{Y}|}\}$. We assume that $Y_1,Y_2,\ldots,Y_n$ are conditionally i.i.d. given $X$. We assume, without loss of generality, that $X$ and $Y$ have full support. We may also assume, without loss of generality, that the distributions $P_{Y|X}(\cdot|x)$ are unique over $x$, which we call the *unique row assumption*. For if this is not the case, 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, so

$$I_\alpha^S(X;Y^n) = I_\alpha^S(\tilde{X};Y^n)$$

by the data processing inequality for Sibson mutual information [16]. We may then work with $\tilde{X}$ in place of $X$. Thus the unique row assumption is without loss of generality.

Note that, again by the data processing inequality, we have

$$I_\alpha^S(X;Y^n) \leq I_\alpha^S(X;X) = H_{1/\alpha}(X)$$

for all $n$ and all $\alpha \in [1,\infty]$. Our main result is the following.

**Theorem 1.** *Under the unique row assumption,*

$$\lim_{n\to\infty} I_\alpha^S(X;Y^n) = H_{1/\alpha}(X) \tag{9}$$

*for any $\alpha \in [1,\infty]$ and the speed of convergence is independent of $\alpha$ in the sense that for all $\alpha \in [1,\infty]$,*

$$\lim_{n\to\infty} -\frac{1}{n}\log\Big(H_{1/\alpha}(X) - I_\alpha^S(X;Y^n)\Big) = \min_{x\neq x'} \mathscr{C}(Q_x||Q_{x'}).$$

We prove the result separately for the cases $\alpha = 1$, $\alpha = \infty$, and $1 < \alpha < \infty$ in the next three sections. For this, the following alternate characterization of the exponent is useful. Let $Q_x$ denote the distribution of $Y$ given $x$ for a given $x \in \mathcal{X}$, and let $\mathcal{P}$ denote the set of all possible probability distributions over $\mathcal{Y}$. 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 $\mathcal{X}$.

**Lemma 2.**

$$\inf_{P\in\mathcal{P}} D(P||Q_{x_2(P)}) = \min_{x\neq x'} \mathscr{C}(Q_x||Q_{x'}). \tag{10}$$

*Proof.* The proof uses the Pythagorean theorem for relative entropy [15, Thm. 11.6.1] and is omitted due to space constraints. □

*Other Notation:* We use $\mathcal{P}_n$ to denote the set of all possible empirical distributions of $Y^n$. 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 $T(P)$ may be empty if $P \notin \mathcal{P}_n$. We use $Q(\cdot)$ to denote true distributions of $X$ and $Y^n$.

## IV. Proof for Mutual Information ($\alpha = 1$)

We derive separate upper and lower bounds for mutual information. Since $I(X;Y^n) = H(X) - H(X|Y^n)$, we can equivalently upper and lower bound $-H(X|Y^n)$. For the lower bound,

$$-H(X|Y^n) \equiv \sum_{y^n\in\mathcal{Y}^n} Q(y^n)\sum_{x\in\mathcal{X}} Q(x|y^n)\log Q(x|y^n) \tag{11}$$

$$= \sum_{P\in\mathcal{P}_n}\sum_{y^n\in T(P)} Q(y^n)\sum_{x\in\mathcal{X}}\frac{Q(y^n|x)Q(x)}{Q(y^n)}\log\frac{Q(y^n|x)Q(x)}{Q(y^n)} \tag{12}$$

$$= \sum_{P\in\mathcal{P}_n}\sum_{y^n\in T(P)}\sum_{x\in\mathcal{X}}\frac{1}{|T(P)|}Q(T(P)|x)Q(x) \cdot\log\frac{\frac{1}{|T(P)|}Q(T(P)|x)Q(x)}{\sum_{x'\in\mathcal{X}}\frac{1}{|T(P)|}Q(T(P)|x')Q(x')} \tag{13}$$

$$= \sum_{P\in\mathcal{P}_n}\sum_{x\in\mathcal{X}} Q(T(P)|x)Q(x)\log\frac{Q(T(P)|x)Q(x)}{\sum_{x'\in\mathcal{X}}Q(T(P)|x')Q(x')} \tag{14}$$

$$\begin{aligned}= -\sum_{\substack{P\in\mathcal{P}_n:\\ Q(T(P))>0}} &\big[Q(T(P)|x_1(P))Q(x_1(P)) \\ &\cdot\log\frac{\sum_{x'\in\mathcal{X}}Q(T(P)|x')Q(x')}{Q(T(P)|x_1(P))Q(x_1(P))} \\ &+\sum_{\substack{x\neq x_1(P):\\ Q(T(P)|x)>0}} Q(T(P)|x)Q(x) \\ &\cdot\log\frac{\sum_{x'\in\mathcal{X}}Q(T(P)|x')Q(x')}{Q(T(P)|x)Q(x)}\big],\end{aligned} \tag{15}$$

due to the convention that $0\log 0 = 0$. Then, replacing weighted sums over $x$ with their largest summand gives

$$\begin{aligned}\geq -\sum_{\substack{P\in\mathcal{P}_n:\\ Q(T(P))>0}} &\Bigg[Q(T(P)|x_1(P))Q(x_1(P)) \\ &\cdot\log\Big(1+\frac{\sum_{x'\neq x_1(P)}Q(T(P)|x')Q(x')}{Q(T(P)|x_1(P))Q(x_1(P))}\Big) \\ &+\max_{\substack{x\neq x_1(P):\\ Q(T(P)|x)>0}}\Big\{Q(T(P)|x)\log\frac{\max_{x'\in\mathcal{X}}Q(T(P)|x')}{Q(T(P)|x)Q(x)}\Big\}\Bigg].\end{aligned} \tag{16}$$

Note that the entire expression inside the summation over $P$ is 0 if $Q(T(P)|x_2(P))=0$. Letting $Q_{\min}(X)=\min_{x\in\mathcal{X}}Q(x)$ and using $\ln(1+x)\leq x$ for the $x=x_1(P)$ term,

$$\begin{aligned}\geq -\sum_{\substack{P\in\mathcal{P}_n:\\ Q(T(P))>0}} &\Bigg[\frac{1}{\ln 2}\sum_{x'\neq x_1(P)}Q(T(P)|x')Q(x') \\ &+\max_{\substack{x\neq x_1(P):\\ Q(T(P)|x)>0}}\Big\{Q(T(P)|x)\Big\} \\ &\cdot\log\frac{1}{\min_{\substack{x\neq x_1(P):\\ Q(T(P)|x)>0}} Q(T(P)|x)\cdot Q_{\min}(X)}\Bigg]\end{aligned} \tag{17}$$

$$\begin{aligned}\geq -\sum_{\substack{P\in\mathcal{P}_n:\\ Q(T(P))>0}} &\Bigg[\frac{1}{\ln 2}2^{-nD(P||Q_{x_2(P)})}+2^{-nD(P||Q_{x_2(P)})} \\ &\cdot\big[nD_{sup}+\log\frac{(n+1)^{|\mathcal{X}|}}{Q_{\min}(X)}\big]\Bigg]\end{aligned} \tag{18}$$

where

$$D_{sup}\equiv \sup_{\substack{x,P'\in\mathcal{P}\\ D(P'||Q_x)<\infty}} D(P'||Q_x) \tag{19}$$

$$= \sup_{\substack{x,P'\in\mathcal{P}:\\ D(P'||Q_x)<\infty}}\sum_{y\in\mathcal{Y}}P'(y)\log\frac{P'(y)}{Q(y|x)} \tag{20}$$

$$= \sup_{\substack{x,P'\in\mathcal{P}:\\ D(P'||Q_x)<\infty}}\sum_{y\in\mathcal{Y}}P'(y)\log\frac{1}{Q(y|x)}-H(P') \tag{21}$$

$$\leq \sup_x\log\frac{1}{\min_{Q(y|x)>0}Q(y|x)}<\infty. \tag{22}$$

Hence,

$$\begin{aligned}&-H(X|Y^n) \\ &\geq -(n+1)^{|\mathcal{X}|}2^{-nD_n^*}\big[\frac{1}{\ln 2}+\log\frac{(n+1)^{|\mathcal{X}|}}{Q_{\min}(X)}+nD_{sup}\big]\end{aligned} \tag{23}$$

where

$$D_n^* = \min_{P\in\mathcal{P}_n} D(P||Q_{x_2(P)}) \tag{24}$$

and $P_n^*$ is its minimizer.

For the upper bound,

$$-H(X|Y^n)$$

$$= \sum_{P\in\mathcal{P}_n}\sum_{x\in\mathcal{X}} Q(T(P)|x)Q(x)\log\frac{Q(T(P)|x)Q(x)}{\sum_{x'\in\mathcal{X}}Q(T(P)|x')Q(x')} \tag{25}$$

$$\leq \sum_{x\in\mathcal{X}} Q(T(P_n^*)|x)Q(x)\log\frac{Q(T(P_n^*)|x)Q(x)}{\sum_{x'\in\mathcal{X}}Q(T(P_n^*)|x')Q(x')} \tag{26}$$

$$\begin{aligned}&\leq Q(T(P_n^*)|x_1(P_n^*))Q(x_1(P_n^*)) \\ &\quad\cdot\log\frac{Q(T(P_n^*)|x_1(P_n^*))Q(x_1(P_n^*))}{\sum_{x'\in\mathcal{X}}Q(T(P_n^*)|x')Q(x')}\end{aligned} \tag{27}$$

$$\begin{aligned}&= Q(T(P_n^*)|x_1(P_n^*))Q(x_1(P_n^*)) \\ &\quad\cdot\log\big[1-\frac{\sum_{x'\neq x_1(P_n^*)}Q(T(P_n^*)|x')Q(x')}{\sum_{x'\in\mathcal{X}}Q(T(P_n^*)|x')Q(x')}\big]\end{aligned} \tag{28}$$

recalling that $-\ln(1-x)\geq x$,

$$\begin{aligned}&\leq -Q(T(P_n^*)|x_1(P_n^*))Q(x_1(P_n^*)) \\ &\quad\cdot\frac{\sum_{x'\neq x_1(P_n^*)}Q(T(P_n^*)|x')Q(x')}{\sum_{x'\in\mathcal{X}}Q(T(P_n^*)|x')Q(x')}\cdot\frac{1}{\ln 2}\end{aligned} \tag{29}$$

$$\begin{aligned}&\leq -Q(T(P_n^*)|x_1(P_n^*))Q(x_1(P_n^*)) \\ &\quad\cdot\frac{Q(T(P_n^*)|x_2(P_n^*))Q(x_2(P_n^*))}{\max_{x'\in\mathcal{X}}Q(T(P_n^*)|x')}\cdot\frac{1}{\ln 2}\end{aligned} \tag{30}$$

$$\begin{aligned}&\leq -\frac{1}{(n+1)^{|\mathcal{X}|}}2^{-nD(P_n^*||Q_{x_1(P_n^*)})}Q(x_1(P_n^*)) \\ &\quad\cdot\frac{2^{-nD_n^*}Q(x_2(P_n^*))}{(n+1)^{|\mathcal{X}|}2^{-nD(P_n^*||Q_{x_1(P_n^*)})}}\cdot\frac{1}{\ln 2}\end{aligned} \tag{31}$$

$$= -\frac{Q(x_1(P_n^*))Q(x_2(P_n^*))}{(n+1)^{2|\mathcal{X}|}\ln 2}2^{-nD_n^*}. \tag{32}$$

As we have now shown that mutual information is upper and lower bounded by expressions of the form $H(X)-K_n\cdot 2^{-nD_n^*}$ for some subexponential sequence $K_n$, it remains to be shown that this exponent approaches the minimum Chernoff information as $n\to\infty$.

First, it can be shown using standard continuity arguments that

$$\lim_{n\to\infty}\inf_{P\in\mathcal{P}_n} D(P||Q_{x_2(P)}) = \inf_{P\in\mathcal{P}} D(P||Q_{x_2(P)}) \tag{33}$$

since $D(P||Q_{x_2(P)})$ is a continuous function of $P$. Finally, we arrive at the desired result using Lemma 2.

## V. Proof for Maximal Leakage ($\alpha = \infty$)

While the lower bound on $I_\infty^S(X;Y^n)$ can be proven directly, due to space constraints we will instead note that the desired bound can be obtained from (62) to follow by letting $\alpha \to \infty$. For the upper bound, for fixed $n$, let

$$D_x = \{P \in \mathcal{P} | Q(T(P)|x) > Q(T(P)|x') \ \forall x' \neq x\} \quad (34)$$

$$\bar{D}_x = \{P \in \mathcal{P} | Q(T(P)|x) \geq Q(T(P)|x') \ \forall x' \in \mathcal{X}\} \quad (35)$$

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

$$Q(y^n|x) = 2^{-n(D(P||Q_x)+H(P))} \ \forall y^n \in T(P). \quad (36)$$

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 $P_n \to P$. Then $P_n \in D_{x_b}$ eventually and

$$I_\infty^S(X;Y^n) \leq \log \sum_{x \in \mathcal{X}} \sum_{P \in \bar{D}_x \cap \mathcal{P}_n} Q(T(P)|x) \quad (37)$$

$$= \log \big[ |\mathcal{X}| - \sum_{x \in \mathcal{X}} \sum_{P \in \mathcal{P}_n \setminus \bar{D}_x} Q(T(P)|x) \big] \quad (38)$$

$$\leq \log \big[ |\mathcal{X}| - \sum_{P \in \mathcal{P}_n \setminus \bar{D}_{x_a}} Q(T(P)|x_a) \big] \quad (39)$$

$$\leq \log \big[ |\mathcal{X}| - Q(T(P_n)|x_a) \big], \quad (40)$$

eventually. Thus for sufficiently large $n$,

$$I_\infty^S(X;Y^n)$$

$$\leq \log \big[ |\mathcal{X}| - \frac{1}{(n+1)^{|\mathcal{X}|}} 2^{-nD(P_n||Q_{x_a})} \big] \quad (41)$$

$$\leq \log |\mathcal{X}| - \frac{1}{|\mathcal{X}|(n+1)^{|\mathcal{X}|}} 2^{-nD(P_n||Q_{x_a})} \quad (42)$$

Thus,

$$\limsup_{n \to \infty} -\frac{1}{n} \log \big( |\mathcal{X}| - I_\infty^S(X;Y^n) \big)$$

$$\leq \lim_{n \to \infty} D(P_n||Q_{x_a}) = D(P||Q_{x_a}). \quad (43)$$

Since $x_a \neq x_b$ and $P$ were arbitrary, the result follows by Lemma 2.

## VI. Proof for ($\alpha \in (1, \infty)$)

To lower bound $I_\alpha^S(X;Y^n)$, we use the $D_x$ sets defined in the previous proof:

$$I_\alpha^S(X;Y^n) \equiv \frac{\alpha}{\alpha - 1} \log \sum_{y^n \in \mathcal{Y}^n} \Big( \sum_{x \in \mathcal{X}} Q(x) Q(y^n|x)^\alpha \Big)^{1/\alpha} \quad (44)$$

$$= \frac{\alpha}{\alpha - 1} \log \sum_{P \in \mathcal{P}_n} \Big( \sum_{x \in \mathcal{X}} Q(x) Q(T(P)|x)^\alpha \Big)^{1/\alpha} \quad (45)$$

$$\geq \frac{\alpha}{\alpha - 1} \log \sum_{x \in \mathcal{X}} \sum_{P \in D_x \cap \mathcal{P}_n} \Big( \sum_{x' \in \mathcal{X}} Q(x') Q(T(P)|x')^\alpha \Big)^{1/\alpha} \quad (46)$$

$$\geq \frac{\alpha}{\alpha - 1} \log \sum_{x \in \mathcal{X}} Q(x)^{1/\alpha} \sum_{P \in D_x \cap \mathcal{P}_n} Q(T(P)|x) \quad (47)$$

$$= \frac{\alpha}{\alpha - 1} \log \sum_{x \in \mathcal{X}} Q(x)^{1/\alpha} \Big( 1 - \sum_{P \in \mathcal{P}_n \setminus D_x} Q(T(P)|x) \Big) \quad (48)$$

$$= \frac{\alpha}{\alpha - 1} \log \Big( \sum_{x \in \mathcal{X}} Q(x)^{1/\alpha} - \sum_{x \in \mathcal{X}} \sum_{P \in \mathcal{P}_n \setminus D_x} Q(x)^{1/\alpha} Q(T(P)|x) \Big) \quad (49)$$

Letting

$$R = \frac{\sum_{x \in \mathcal{X}} \sum_{P \in \mathcal{P}_n \setminus D_x} Q(x)^{1/\alpha} Q(T(P)|x)}{\sum_{x \in \mathcal{X}} Q(x)^{1/\alpha}}, \quad (50)$$

we have

$$I_\alpha^S(X;Y^n) \geq \frac{\alpha}{\alpha - 1} \log \big\{ \big( \sum_{x \in \mathcal{X}} Q(x)^{1/\alpha} \big)(1 - R) \big\} \quad (51)$$

$$= H_{1/\alpha}(X) + \frac{\alpha}{\alpha - 1} \log(1 - R). \quad (52)$$

Note that

$$\ln(1 - \epsilon) = -\sum_{i=1}^\infty \frac{\epsilon^i}{i} \quad (53)$$

$$\geq -\epsilon - \frac{\epsilon}{2} (\sum_{i=1}^\infty \epsilon^i) = -\epsilon - \frac{\epsilon^2}{2(1 - \epsilon)} \quad (54)$$

for $0 < \epsilon < 1$. Hence,

$$I_\alpha^S(X;Y^n) \geq H_{1/\alpha}(X) + \frac{\alpha}{(\alpha - 1)\ln 2} (-R - \frac{R^2}{2(1 - R)}). \quad (55)$$

Next we derive an upper bound for $R$.

$$R \leq \frac{\sum_{x \in \mathcal{X}} Q(x)^{1/\alpha} (n+1)^{|\mathcal{X}|} \cdot \max_{P \in \mathcal{P}_n \setminus D_x} Q(T(P)|x)}{\sum_{x \in \mathcal{X}} Q(x)^{1/\alpha}} \quad (56)$$

$$\leq \frac{\sum_{x \in \mathcal{X}} Q(x)^{1/\alpha} (n+1)^{|\mathcal{X}|} \cdot \max_{x' \in \mathcal{X}} \max_{P \in \mathcal{P}_n \setminus D_{x'}} Q(T(P)|x')}{\sum_{x \in \mathcal{X}} Q(x)^{1/\alpha}} \quad (57)$$

$$= (n+1)^{|\mathcal{X}|} \cdot \max_{x \in \mathcal{X}} \max_{P \in \mathcal{P}_n \setminus D_x} Q(T(P)|x) \quad (58)$$

$$\leq (n+1)^{|\mathcal{X}|} \cdot 2^{-n(\min_{x \in \mathcal{X}} \min_{P \in \mathcal{P}_n \setminus D_x} D(P||Q_x))} \quad (59)$$

$$\leq (n+1)^{|\mathcal{X}|} \cdot 2^{-n(\min_{x \neq x'} \inf_{P \in \bar{D}_{x'}} D(P||Q_x))} \quad (60)$$

$$= (n+1)^{|\mathcal{X}|} \cdot 2^{-n \cdot \min_{x \neq x'} \mathcal{C}(Q_x||Q_{x'})} \equiv R_{upper} \quad (61)$$

where we have used Lemma 2. Note that $R_{upper}$ is independent of $Q(x)$ and $\alpha$. Then,

$$I_\alpha^S(X;Y^n) \geq H_{1/\alpha}(X) - \frac{\alpha}{(\alpha - 1)\ln 2} (R + \frac{R^2}{2(1 - R)})$$

$$\geq H_{1/\alpha}(X) - \frac{\alpha}{(\alpha - 1)\ln 2} (R_{upper} + \frac{R_{upper}^2}{2(1 - R_{upper})}) \quad (62)$$

As a result, we also have the lower bound for maximal leakage simply by taking limits for $\alpha \to \infty$ on both sides.

For the upper bound, for convenience, let

$$F(x,P) = Q(x)Q(T(P)|x)^{\alpha}. \tag{63}$$

Then 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 $F(x,P)^{1-1/\alpha} = \max_{x' \in \mathcal{X}} F(x',P)^{1-1/\alpha}$. 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 $P^*$. Note that $P_n \in E_{x_b}^{(n)}$ eventually. Then

$$I_\alpha^S(X;Y^n) = \frac{\alpha}{\alpha-1}\log \sum_{x\in\mathcal{X}} \sum_{P\in E_x^{(n)}} \Big(\sum_{x'\in\mathcal{X}} F(x',P)\Big)^{1/\alpha} \tag{64}$$

$$= \frac{\alpha}{\alpha-1}\log \sum_{x\in\mathcal{X}} \sum_{P\in E_x^{(n)}} F(x,P)^{1/\alpha}\Big(1+\sum_{x'\neq x}\frac{F(x',P)}{F(x,P)}\Big)^{1/\alpha} \tag{65}$$

Using the Taylor series expansion of $(1+x)^{1/\alpha}$ and discarding $x^2$ and higher order terms (since $\frac{1}{\alpha} < 1$), we have

$$\leq \frac{\alpha}{\alpha-1}\log \sum_{x\in\mathcal{X}} \sum_{P\in E_x^{(n)}} F(x,P)^{1/\alpha}\Big(1+\frac{1}{\alpha}\sum_{x'\neq x}\frac{F(x',P)}{F(x,P)}\Big) \tag{66}$$

$$\leq \frac{\alpha}{\alpha-1}\log \sum_{x\in\mathcal{X}} \sum_{P\in E_x^{(n)}} \Big(F(x,P)^{1/\alpha} + F(x,P)^{1/\alpha-1}\sum_{x'\neq x} F(x',P)\Big), \tag{67}$$

where we have used the fact that $\alpha > 1$. For the remainder of the proof, we redefine $x_k(P)$ so that they are ordered by $F(x,P)$ instead of relative entropy. Then

$$= \frac{\alpha}{\alpha-1}\log \sum_{x\in\mathcal{X}} \Big(\sum_{P\in E_x^{(n)}} F(x,P)^{1/\alpha} + \sum_{P\notin E_x^{(n)}} F(x_1(P),P)^{1/\alpha-1}F(x,P)\Big) \tag{68}$$

$$= \frac{\alpha}{\alpha-1}\log \sum_{x\in\mathcal{X}} \Big(\sum_{P\in E_x^{(n)}} F(x,P)^{1/\alpha} + \sum_{P\notin E_x^{(n)}} F(x_1(P),P)^{1/\alpha-1}F(x,P) + \sum_{P\notin E_x^{(n)}} F(x,P)^{1/\alpha} - \sum_{P\notin E_x^{(n)}} F(x,P)^{1/\alpha}\Big) \tag{69}$$

$$= \frac{\alpha}{\alpha-1}\log \sum_{x\in\mathcal{X}} \Big(\sum_{P\in\mathcal{P}_n} F(x,P)^{1/\alpha} + \sum_{P\notin E_x^{(n)}} \big(F(x_1(P),P)^{1/\alpha-1} - F(x,P)^{1/\alpha-1}\big)F(x,P)\Big) \tag{70}$$

Using $\ln(1+x) \leq x$ and noting that the summand of the sum over $P \notin E_x^{(n)}$ is nonpositive,

$$\leq H_{1/\alpha}(X) + \frac{\alpha}{(\alpha-1)\ln 2}\frac{1}{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}} \sum_{x\in\mathcal{X}}\sum_{P\notin E_x^{(n)}} \cdot (F(x_1(P),P)^{1/\alpha-1} - F(x,P)^{1/\alpha-1})F(x,P)) \tag{71}$$

$$\leq H_{1/\alpha}(X) + \frac{\alpha}{(\alpha-1)\ln 2}\frac{1}{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}} \cdot (F(x_1(P_n),P_n)^{1/\alpha-1} - F(x_a,P_n)^{1/\alpha-1})F(x_a,P_n)). \tag{72}$$

Note that eventually $x_1(P_n) = x_b$ and $F(x_b,P_n)^{1/\alpha-1} < \frac{1}{2}F(x_a,P_n)^{1/\alpha-1}$. Thus, eventually,

$$\leq H_{1/\alpha}(X) - \frac{1}{2}\frac{\alpha}{(\alpha-1)\ln 2}\frac{1}{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}}F(x_a,P_n)^{1/\alpha} \tag{73}$$

$$\leq H_{1/\alpha}(X) - \frac{\alpha}{2(\alpha-1)\ln 2}\frac{1}{\sum_{x\in\mathcal{X}} Q(x)^{1/\alpha}}Q_{\min}(X)^{1/\alpha} \cdot \frac{1}{(n+1)^{|\mathcal{X}|}}2^{-nD(P_n||Q_{x_a})} \tag{74}$$

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

$$\limsup_{n\to\infty} -\frac{1}{n}\log\big(H_{1/\alpha}(X) - I_\alpha^S(X;Y^n)\big) \leq \lim_{n\to\infty} D(P_n||Q_{x_a}) = D(P^*||Q_{x_a}). \tag{75}$$

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

$$\limsup_{n\to\infty} -\frac{1}{n}\log\big(H_{1/\alpha}(X) - I_\alpha^S(X;Y^n)\big) \leq \min_{x\neq x'}\inf_{P\in D_x} D(P||Q_{x'}) = \min_{x\neq x'}\mathscr{C}(Q_x||Q_{x'}). \tag{76}$$

## VII. Acknowledgment

This research was supported by the US National Science Foundation under grant CCF-1704443.

## References

[1] P. C. Kocher, "Timing Attacks on Implementations of Di e-Hellman, RSA, DSS, and Other Systems," p. 10.

[2] C. Wampler, S. Uluagac, and R. Beyah, "Information Leakage in Encrypted IP Video Traffic," in *2015 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2015, pp. 1–7.

[3] Y. Zhu, Y. Lu, and A. Vikram, "On Privacy of Encrypted Speech Communications," *IEEE Transactions on Dependable and Secure Computing*, 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." [Online]. Available: arXiv:1603.01887

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

[7] I. Issa, A. B. Wagner, and S. Kamath, "An operational measure of information leakage," *IEEE Trans. Inf. Theory*, to appear.

[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)*, 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)*, 2017, pp. 769–773.
[10] I. Issa, S. Kamath, and A. B. Wagner, "An operational measure of information leakage," in *Proc. Conf. Inf. Sci. and Sys. (CISS)*, 2016, pp. 234–239.
[11] J. Liao, O. Kosut, L. Sankar, and F. P. Calmon, "A Tunable Measure for Information Leakage," *arXiv:1806.03332 [cs, math]*, Jun. 2018, arXiv: 1806.03332. [Online]. Available: http://arxiv.org/abs/1806.03332
[12] D. M. Smith and G. Smith, "Tight Bounds on Information Leakage from Repeated Independent Runs," in *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, Aug. 2017, pp. 318–327, iSSN: 2374-8303.
[13] R. Sibson, "Information radius," *Zeitschrift for Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 14, no. 2, pp. 149–160, 1969. [Online]. Available: http://link.springer.com/10.1007/BF00537520
[14] S. Verdú, "$\alpha$-mutual information," in *Proc. Inf. Theory and Appl. (ITA) Workshop*, 2015.
[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed., 2006.
[16] Y. Polyanskiy and S. Verdú, "Arimoto channel coding converse and Rényi divergence," in *Proc. Ann. Allerton Conf. on Comm., Control, and Computing*, 2010, pp. 1327–1333.