A Bound For Multiparty Secret Key Agreement And Implications For A Problem Of Secure Computing

Himanshu Tyagi[1] and Shun Watanabe[2]

[1] Information Theory and Applications (ITA) Center, University of California, San Diego, La Jolla, CA 92093, USA.
htyagi@eng.ucsd.edu

[2] Department of Information Science and Intelligent Systems, University of Tokushima, Tokushima 770-8506, Japan, and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA.
shun-wata@is.tokushima-u.ac.jp

Abstract. We consider secret key agreement by multiple parties observing correlated data and communicating interactively over an insecure communication channel. Our main contribution is a *single-shot* upper bound on the length of the secret keys that can be generated, without making any assumptions on the distribution of the underlying data. Heuristically, we bound the secret key length in terms of "how far" is the joint distribution of the initial observations of the parties and the eavesdropper from a distribution that renders the observations of the parties conditionally independent across some partition, when conditioned on the eavesdropper's side information. The closeness of the two distributions is measured in terms of the exponent of the probability of error of type II for a binary hypothesis testing problem, thus bringing out a structural connection between secret key agreement and binary hypothesis testing. When the underlying data consists of an independent and identically distributed sequence, an application of our bound recovers several known upper bounds for the asymptotic rate of a secret key that can be generated, without requiring the agreement error probability or the security index to vanish to 0 asymptotically.

Also, we consider the following problem of secure function computation with trusted parties: Multiple parties observing correlated data seek to compute a function of their collective data. To this end, they communicate interactively over an insecure communication channel. It is required that the value of the function be concealed from an eavesdropper with access to the communication. When is such a secure computation of a given function feasible? Using the aforementioned upper bound, we derive a necessary condition for the existence of a communication protocol that allows the parties to reliably recover the value of a given function, while keeping this value concealed from an eavesdropper with access to (only) the communication.

Keywords: secret key agreement, single shot bound, secure computing

1 Introduction

A uniformly distributed random string that is shared by legitimate parties and remains concealed from eavesdroppers is a cherished resource in cryptography. It can be used to authenticate or secure the communication between the parties, or as a password granting access to one or more members of a group. It was pointed out first by Bennett, Brassard, and Robert [3] that parties observing correlated data and with access to an authenticated, error-free, albeit insecure, communication channel can harness the correlation in their observations to share a (almost) uniform random string that is concealed from an eavesdropper observing the communication as well as some correlated side information. Such a shared random string, termed a *secret key* (SK), is secure in the sense of *information theoretic security*, without making any assumptions on the computation capabilities of the eavesdropper.[3]

For two parties, the problem of SK agreement from correlated observations is well-studied. The problem was introduced by Maurer [20] and Ahlswede and Csiszár [1], who considered the case where the correlated observations of the two parties are long sequences, generated by an *independent and identically distributed* (IID) random process. However, in certain applications it is of interest to consider observations arising from a single realization of correlated *random variables* (RVs).[4] For instance, in applications such as biometric and hardware authentication (cf. [23, 14]), the correlated observations consist of different versions of the biometric and hardware signatures, respectively, recorded at the registration and the authentication stages. To this end, Renner and Wolf [27] derived bounds on the length of a SK that can be generated by two parties observing a single realization of correlated RVs, using one-side communication.

The problem of SK agreement with multiple parties, for the IID setup, was introduced in [13] (also, see [7] for an early formulation). In this work, we consider the SK agreement problem for multiple parties observing a single realization of correlated RVs.

Our main contributions are summarized below.

1.1 Main contributions

We derive a single-shot upper bound on the length of SKs that can be generated by multiple parties observing correlated data, using interactive public communication. Unlike the single-shot upper bound in [27], which is restricted to two parties with one-way communication, we allow arbitrary interactive communication between multiple parties.[5] Asymptotically our bound is tight – its

[3] While the SK is information theoretically secure, the security of the cryptographic protocols using it might be based on computation complexity.

[4] This model is sometimes referred to as the *single-shot* model to distinguish it from the IID case.

[5] A comparison between a restriction of our bound to one-way communication and the bound in [27] is unavailable, since the latter involves auxiliary RVs and therefore, is difficult to evaluate.

application to the IID case recovers some previously known (tight) bounds on the asymptotic SK rates. In fact, we strengthen the previously known asymptotic results since we do not require the probability of error in SK agreement or the security index to be asymptotically 0.[6]

For the heuristic idea underlying our upper bound, consider the two party case when the eavesdropper observes only the communication between the legitimate parties (no side-information). Clearly, if the observations of the legitimate parties are independent, a SK cannot be generated. We upper bound the length of SKs that can be generated in terms of "how far" is the joint distribution of the observations of the parties and from a distribution that renders their observations independent. Specifically, for this special case, we show

$$S_\epsilon\left(X_1, X_2\right) \leq -\log \beta_{\epsilon+\eta}\big(\mathrm{P}_{X_1X_2}, \mathrm{P}_{X_1} \times \mathrm{P}_{X_2}\big) + 2\log(1/\eta),$$

where $S_\epsilon\left(X_1, X_2\right)$ is the maximum length of a SK (for a given security index ϵ). Here the distance between $\mathrm{P}_{X_1X_2}$ and $\mathrm{P}_{X_1} \times \mathrm{P}_{X_2}$ is measured by β_ϵ, which is the optimal probability of error of type II for testing the null hypothesis $\mathrm{P}_{X_1X_2}$ with the alternative $\mathrm{P}_{X_1} \times \mathrm{P}_{X_2}$, given that the probability of error of type I is smaller than ϵ. Similarly, in the general case, our main result in Theorem 1 bounds the secret key length in terms of the distance between the joint distribution of the observations of the parties and the eavesdropper and a distribution that renders the observations of the parties conditionally independent across some partition, when conditioned on the eavesdropper's side information.

Our approach brings out a structural connection between SK agreement and binary hypothesis testing. This is in the spirit of [24], where a connection between channel coding and binary hypothesis testing was used to establish an upper bound on the rate of good channel codes (see, also, [35, 16]). Also, our upper bound is reminiscent of the *measure of entanglement* for a quantum state proposed in [34], namely the minimum distance between the density matrix of the state and that of a disentangled state. This measure of entanglement was shown to be an upper bound on the entanglement of distillation in [34], where the latter is the largest proportion of maximally entangled states that can be distilled using a purification process [4].

As an application, we relate our result to the following problem of *secure function computation with trusted parties* introduced in [33] (for an early version of the problem, see [22]): Multiple parties observing correlated data seek to compute a function of their collective data. To this end, they communicate interactively over a public communication channel, which is assumed to be authenticated and error-free. It is required that the value of the function be concealed from an eavesdropper with access to the communication. When is such a secure computation of a given function feasible?[7] Using our aforementioned upper bound, we derive a necessary condition for the existence of a communication

[6] Such bounds that do not require the probability of error to vanish to 0 are called *strong converse* bounds [12].

[7] In contrast to the traditional definition of secure computing [37], the legitimate parties are trusted and allowed to get any information about each other's data.

protocol that allows the parties to reliably recover the value of a given function, while keeping this value concealed from an eavesdropper with access to (only) the communication.

1.2 Outline of paper

The next section contains formal descriptions of our model, the allowed interactive communication, and a SK, along with a definition of the SK capacity. Also, we review some basic notions in binary hypothesis testing that will be used in this paper. Our main result is Theorem 1 in Section 3; implications of this main result are presented as corollaries. In Section 4, we show that our new upper bound is asymptotically tight and leads to a strong converse for the SK capacity. Implications for the secure computing problem with trusted parties, along with illustrative examples, are given in Section 5. The final section contains a discussion of our results.

1.3 Notations

For brevity, we use abbreviations SK, RV, and IID for secret key, random variable, and independent and identically distributed, respectively; a plural form will be indicated by appending an 's' to the abbreviation. The RVs are denoted by capital letters and the corresponding range sets are denoted by calligraphic letters. The distribution of a RV U is given by P_U. The set of all parties $\{1, ..., m\}$ is denoted by $\mathcal{M}$. For a collection of RVs $\{U_1, .., U_m\}$ and a subset A of $\mathcal{M}$, U_A denotes the RVs $\{U_i, \, i \in A\}$. For a RV U, U^n denotes n IID repetitions of the RV U. Similarly, P^n denotes the distribution corresponding to the n IID repetitions generated from P. All logarithms in this paper are to the base 2.

2 Preliminaries

We consider the problem of SK agreement using interactive public communication by m (trusted) parties. The ith party observes a discrete RV X_i taking values in a finite set $\mathcal{X}_i$, $1 \leq i \leq m$.[8] Upon making these observations, the parties communicate interactively over a public communication channel that is accessible by an eavesdropper, who additionally observes a RV Z such that the RVs $(X_{\mathcal{M}}, Z)$ have a distribution $\mathrm{P}_{X_{\mathcal{M}}Z}$. We assume that the communication is error-free and each party receives the communication from every other party. Furthermore, we assume that the public communication is authenticated and the eavesdropper cannot tamper with it. Specifically, the communication is sent over r rounds of interaction. In the jth round of communication, $1 \leq j \leq r$, the ith party sends F_{ij}, which is a function of its observation X_i, a *locally generated* randomness[9] U_i and the previously observed communication

$$F_{11}, ..., F_{m1}, F_{12}, ..., F_{m2}, ..., F_{1j}, ..., F_{(i-1)j}.$$

[8] Our main theorem remains valid for RVs taking countably many values.

[9] The RVs $U_1, ..., U_m$ are mutually independent and independent jointly of $(X_{\mathcal{M}}, Z)$.

The overall interactive communication $F_{11}, ..., F_{m1}, ..., F_{1r}, ..., F_{mr}$ is denoted by $\mathbf{F}$.

Using the interactive communication $\mathbf{F}$ and their local observations, the parties agree on a SK. In the next section, we formally explain this notion.

2.1 Secret keys

A SK is a collection of RVs $K_1, ..., K_m$, where the ith party gets K_i, that agree with probability close to 1 and are concealed, in effect, from an eavesdropper. Formally, the ith party computes a function K_i of $(U_i, X_i, \mathbf{F})$. Traditionally, the RVs $K_1, ..., K_m$ with a common range $\mathcal{K}$ constitute an (ϵ, δ)-SK if the following two conditions are satisfied (for alternative definitions of secrecy, see [20, 11, 13])

$$\mathrm{P}\left(K_1 = \cdots = K_m\right) \geq 1 - \epsilon, \tag{1}$$

$$\frac{1}{2}\left\|\mathrm{P}_{K_1\mathbf{F}Z} - \mathrm{P}_{\mathtt{unif}} \times \mathrm{P}_{\mathbf{F}Z}\right\| \leq \delta, \tag{2}$$

where $\| \cdot \|$ is the variational distance and $\mathrm{P}_{\mathtt{unif}}$ is the uniform distribution on $\mathcal{K}$. The first condition above represents the reliable *recovery* of the SK and the second condition guarantees *security*. In this work, we use the following alternative definition of a SK, which conveniently combines the recoverability and the security conditions (cf. [25]): The RVs $K_1, ..., K_m$ above constitute an ϵ-SK with common range $\mathcal{K}$ if

$$\frac{1}{2}\left\|\mathrm{P}_{K_{\mathcal{M}}\mathbf{F}Z} - \mathrm{P}^{(\mathcal{M})}_{\mathtt{unif}} \times \mathrm{P}_{\mathbf{F}Z}\right\| \leq \epsilon, \tag{3}$$

where

$$\mathrm{P}^{(\mathcal{M})}_{\mathtt{unif}}\left(k_{\mathcal{M}}\right) = \frac{\mathbb{1}(k_1 = \cdots = k_m)}{|\mathcal{K}|}.$$

In fact, the two definitions above are closely related.

Proposition 1. *Given $0 \leq \epsilon, \delta \leq 1$, if $K_{\mathcal{M}}$ constitute an (ϵ, δ)-SK under (1) and (2), then they constitute an $(\epsilon + \delta)$-SK under (3).*

Conversely, if $K_{\mathcal{M}}$ constitute an ϵ-SK under (3), then they constitute an (ϵ, ϵ)-SK under (1) and (2).

Note that a SK generation protocol that satisfies (3) *universally composable-emulates* an ideal SK generation protocol (see [6] for a definition).[10] Therefore, by the composition theorem in [6], the complex cryptographic protocols using such SKs instead of perfect SKs are secure.[11]

We are interested in characterizing the maximum length $\log |\mathcal{K}|$ of an ϵ-SK.

[10] The emulation is with emulation slack ϵ, for an environment of unbounded computational complexity.

[11] A perfect SK refers to unbiased shared bits that are independent of eavesdropper's observations.

Definition 1. *Given* $0 \leq \epsilon < 1$*, denote by* $S_\epsilon\left(X_1, ..., X_m \mid Z\right)$ *the maximum length* $\log|\mathcal{K}|$ *of an* ϵ*-SK* $K_{\mathcal{M}}$ *with common range* $\mathcal{K}$*.*

Next, we define the concept of SK capacity [20, 1, 13].

Definition 2. *Given* $0 < \epsilon < 1$*, the* ϵ*-SK capacity* $C(\epsilon)$ *is defined as follows:*

$$C(\epsilon) := \liminf_{n\to\infty} \frac{1}{n} S_\epsilon(X_1^n, ..., X_m^n \mid Z^n),$$

where the RVs $\{X_{\mathcal{M}t}, Z_t\}$ are IID for $1 \leq t \leq n$, with a common distribution $\mathrm{P}_{X_{\mathcal{M}}Z}$.

The SK capacity C is defined as the limit

$$C := \lim_{\epsilon\to 0} C(\epsilon).$$

For the case when the eavesdropper does not observe any side information, i.e., $Z =$ *constant*, the SK capacity for two parties was characterized by Maurer [20] and Ahlswede and Csiszár [1]. Later, the SK capacity for a multiterminal model, with Z =constant was characterized by Csiszár and Narayan [13]. The general problem of characterizing the SK capacity for arbitrary Z remains open. Several upper bounds for SK capacity are known [20, 1, 21, 26, 13, 15], which are tight for special cases.

In this paper, we present a single-shot upper bound on $S_\epsilon\left(X_1, ..., X_m \mid Z\right)$. As a consequence, we obtain an upper bound on $C(\epsilon)$. In fact, for the case Z= constant, this upper bound coincides with C, thus establishing that

$$C = C(\epsilon), \quad \forall\, 0 < \epsilon < 1.$$

This is a strengthening of the result in [32], where a *strong converse* was established for (ϵ, δ_n)-SKs under (1) and (2), with $\delta_n \to 0$ as $n \to 0$.

Our upper bound is based on relating the SK agreement problem to a binary hypothesis testing problem; in the next section we review some basic concepts in hypothesis testing that will be used.

2.2 Hypothesis testing

Consider a binary hypothesis testing problem with null hypothesis P and alternative hypothesis Q, where P and Q are distributions on the same alphabet $\mathcal{X}$. Upon observing a value $x \in \mathcal{X}$, the observer needs to decide if the value was generated by the distribution P or the distribution Q. To this end, the observer applies a stochastic test T, which is a conditional distribution on $\{0, 1\}$ given an observation $x \in \mathcal{X}$. When $x \in \mathcal{X}$ is observed, the test T chooses the null hypothesis with probability $\mathrm{T}(0|x)$ and the alternative hypothesis with probability $T(1|x) = 1 - T(0|x)$. For $0 \leq \epsilon < 1$, denote by $\beta_\epsilon(\mathrm{P}, \mathrm{Q})$ the infimum of the probability of error of type II given that the probability of error of type I is less than ϵ, i.e.,

$$\beta_\epsilon(\mathrm{P}, \mathrm{Q}) := \inf_{\mathrm{T}\,:\,\mathrm{P}[\mathrm{T}]\geq 1-\epsilon} \mathrm{Q}[\mathrm{T}], \tag{4}$$

where

$$\mathrm{P}[\mathrm{T}] = \sum_x \mathrm{P}(x)\mathrm{T}(0|x),$$
$$\mathrm{Q}[\mathrm{T}] = \sum_x \mathrm{Q}(x)\mathrm{T}(0|x).$$

We close this section by noting two important properties of the quantity $\beta_\epsilon(\mathrm{P},\mathrm{Q})$.

1. **Data Processing Inequality.** Let W be a stochastic mapping from $\mathcal{X}$ to $\mathcal{Y}$, i.e., for each $x \in \mathcal{X}$, $\mathrm{W}(\cdot \mid x)$ is a distribution on $\mathcal{Y}$. Then, with $\mathrm{PW}(y) = \sum_x \mathrm{P}(x)\mathrm{W}(y|x)$ and $\mathrm{QW}(y) = \sum_x \mathrm{Q}(x)\mathrm{W}(y|x)$, we have
$$\beta_\epsilon(\mathrm{P},\mathrm{Q}) \le \beta_\epsilon(\mathrm{PW},\mathrm{QW}). \tag{5}$$
In other words, if we add extra noise to the observations, then β_ϵ can only increase.
2. **Stein's Lemma.** (cf. [19, Theorem 3.3]) For every $0 < \epsilon < 1$, we have
$$\lim_{n\to\infty} -\frac{1}{n}\log\beta_\epsilon(\mathrm{P}^n,\mathrm{Q}^n) = D(\mathrm{P}\|\mathrm{Q}), \tag{6}$$
where $D(\mathrm{P}\|\mathrm{Q})$ is the Kullback-Leibler divergence given by
$$D(\mathrm{P}\|\mathrm{Q}) = \sum_{x\in\mathcal{X}} \mathrm{P}(x)\log\frac{\mathrm{P}(x)}{\mathrm{Q}(x)},$$
with the convention $0\log(0/0) = 0$.

3 Main result: Upper bound on the length of a multiparty secret key

In this section, we present a new methodology for proving converse results for the multiparty SK agreement problem. Our main result is an upper bound on the length $\log|\mathcal{K}|$ of a SK generated by multiple parties, using interactive public communication.

Consider a (nontrivial) partition $\pi = \{\pi_1, ..., \pi_l\}$ of the set $\mathcal{M}$. Heuristically, if the underlying distribution of the observations $\mathrm{P}_{X_\mathcal{M}Z}$ is such that $X_\mathcal{M}$ are conditionally independent across the partition π given Z, the length of a SK that can be generated is 0. Our approach is to bound the length of a generated SK in terms of "how far" is the distribution $\mathrm{P}_{X_\mathcal{M}Z}$ from another distribution $\mathrm{Q}^\pi_{X_\mathcal{M}Z}$ that renders $X_\mathcal{M}$ conditionally independent across the partition π given Z – the closeness of the two distributions is measured by $\beta_\epsilon\big(\mathrm{P}_{X_\mathcal{M}Z},\mathrm{Q}^\pi_{X_\mathcal{M}Z}\big)$.

Specifically, for a partition π with $|\pi| \ge 2$ parts, let $\mathcal{Q}(\pi)$ be the set of all distributions $\mathrm{Q}^\pi_{X_\mathcal{M}Z}$ that factorize as follows:

$$\mathrm{Q}^\pi_{X_\mathcal{M}|Z}(x_1,\dots,x_m|z) = \prod_{i=1}^{|\pi|}\mathrm{Q}^\pi_{X_{\pi_i}|Z}(x_{\pi_i}|z). \tag{7}$$

Our main result is given below.

Theorem 1 (Single-Shot Converse). *Given $0 \leq \epsilon < 1$, $0 < \eta < 1-\epsilon$, and a partition π of $\mathcal{M}$. It holds that*

$$S_\epsilon\left(X_1, ..., X_m \mid Z\right) \leq \frac{1}{|\pi|-1}\left[-\log \beta_{\epsilon+\eta}\big(\mathrm{P}_{X_\mathcal{M}Z}, \mathrm{Q}^\pi_{X_\mathcal{M}Z}\big) + |\pi|\log(1/\eta)\right] \quad (8)$$

for all $\mathrm{Q}^\pi_{X_\mathcal{M}Z} \in \mathcal{Q}(\pi)$.

To prove Theorem 1, we first relate the SK length to the exponent of the probability of error of type II in a binary hypothesis testing problem where an observer of $(K_\mathcal{M}, \mathbf{F}, Z)$ seeks to find out if the underlying distribution was $\mathrm{P}_{X_\mathcal{M}Z}$ or $\mathrm{Q}^\pi_{X_\mathcal{M}Z}$. This result is stated next.

Lemma 1. *For an ϵ-SK $K_\mathcal{M}$ with a common range $\mathcal{K}$ generated using an interactive communication $\mathbf{F}$, let $W_{K_\mathcal{M}\mathbf{F}|X_\mathcal{M}Z}$ be the resulting conditional distribution on $(K_\mathcal{M}, \mathbf{F})$ given $(X_\mathcal{M}, Z)$. Then, for every $0 < \eta < 1-\epsilon$ and every $\mathrm{Q}^\pi_{X_\mathcal{M}Z} \in \mathcal{Q}(\pi)$, we have*

$$\log|\mathcal{K}| \leq \frac{1}{|\pi|-1}\left[-\log \beta_{\epsilon+\eta}\big(\mathrm{P}_{K_\mathcal{M}\mathbf{F}Z}, \mathrm{Q}^\pi_{K_\mathcal{M}\mathbf{F}Z}\big) + |\pi|\log(1/\eta)\right], \quad (9)$$

where $\mathrm{P}_{K_\mathcal{M}\mathbf{F}Z}$ is the marginal of $(K_\mathcal{M}, \mathbf{F}, Z)$ for the joint distribution

$$\mathrm{P}_{K_\mathcal{M}\mathbf{F}X_\mathcal{M}Z} = W_{K_\mathcal{M}\mathbf{F}|X_\mathcal{M}Z}\,\mathrm{P}_{X_\mathcal{M}Z},$$

and $\mathrm{Q}^\pi_{K_\mathcal{M}\mathbf{F}Z}$ is the corresponding marginal for the joint distribution

$$\mathrm{Q}^\pi_{K_\mathcal{M}\mathbf{F}X_\mathcal{M}Z} = W_{K_\mathcal{M}\mathbf{F}|X_\mathcal{M}Z}\,\mathrm{Q}^\pi_{X_\mathcal{M}Z}.$$

Also, we need the following basic property of interactive communication which was pointed out in [32].

Lemma 2. *Given $\mathrm{Q}^\pi_{X_\mathcal{M}Z} \in \mathcal{Q}(\pi)$ and an interactive communication $\mathbf{F}$, the following holds:*

$$\mathrm{Q}^\pi_{X_\mathcal{M}|\mathbf{F}Z}(x_\mathcal{M}|\mathbf{f}, z) = \prod_{i=1}^{|\pi|} \mathrm{Q}^\pi_{X_{\pi_i}|\mathbf{F}Z}(x_{\pi_i}|\mathbf{f}, z),$$

i.e., conditionally independent observations remain so when conditioned additionally on an interactive communication.

Proof of Lemma 1. We establish (9) by constructing a test for the hypothesis testing problem with null hypothesis $\mathrm{P} = \mathrm{P}_{K_\mathcal{M}\mathbf{F}Z}$ and alternative hypothesis $\mathrm{Q} = \mathrm{Q}^\pi_{K_\mathcal{M}\mathbf{F}Z}$. Specifically, we use a deterministic test[12] with the following acceptance region (for the null hypothesis)[13]:

$$\mathcal{A} := \left\{(k_\mathcal{M}, \mathbf{f}, z) : \log\frac{\mathrm{P}^{(\mathcal{M})}_{\text{unif}}(k_\mathcal{M})}{\mathrm{Q}^\pi_{K_\mathcal{M}|\mathbf{F}Z}(k_\mathcal{M}|\mathbf{f}, z)} \geq \lambda_\pi\right\},$$

[12] In fact, we use a simple threshold test on the log-likelihood ratio but with $\mathrm{P}^{(\mathcal{M})}_{\mathtt{unif}} \times \mathrm{P}_{\mathbf{F}Z}$ in place of $\mathrm{P}_{K_\mathcal{M}\mathbf{F}Z}$, since the two distributions are close to each other by the security condition (3).

[13] The values $(k_\mathcal{M}, \mathbf{f}, z)$ with $\mathrm{Q}^\pi_{K_\mathcal{M}|\mathbf{F}Z}(k_\mathcal{M}|\mathbf{f}, z) = 0$ are included in $\mathcal{A}$.

where

$$\lambda_\pi = (|\pi| - 1)\log|\mathcal{K}| - |\pi|\log(1/\eta).$$

For this test, the probability of error of type II is bounded above as

$$\begin{aligned}
\mathrm{Q}^\pi_{K_\mathcal{M}\mathbf{F}Z}(\mathcal{A}) &= \sum_{\mathbf{f},z}\mathrm{Q}^\pi_{\mathbf{F}Z}(\mathbf{f},z)\sum_{\substack{k_\mathcal{M}:\\(k_\mathcal{M},\mathbf{f},z)\in\mathcal{A}}}\mathrm{Q}^\pi_{K_\mathcal{M}|\mathbf{F}Z}(k_\mathcal{M}|\mathbf{f},z)\\
&\le 2^{-\lambda_\pi}\sum_{\mathbf{f},z}\mathrm{Q}^\pi_{\mathbf{F}Z}(\mathbf{f},z)\sum_{k_\mathcal{M}}\mathrm{P}^{(\mathcal{M})}_{\mathrm{unif}}(k_\mathcal{M})\\
&= |\mathcal{K}|^{1-|\pi|}\eta^{-|\pi|}.
\end{aligned}\tag{10}$$

On the other hand, the probability of error of type I is bounded above as

$$\begin{aligned}
\mathrm{P}_{K_\mathcal{M}\mathbf{F}Z}(\mathcal{A}^c) &\le \frac{1}{2}\left\|\mathrm{P}_{K_\mathcal{M}\mathbf{F}Z} - \mathrm{P}^{(\mathcal{M})}_{\mathrm{unif}}\times\mathrm{P}_{\mathbf{F}Z}\right\| + \mathrm{P}^{(\mathcal{M})}_{\mathrm{unif}}\times\mathrm{P}_{Z\mathbf{F}}(\mathcal{A}^c)\\
&\le \epsilon + \mathrm{P}^{(\mathcal{M})}_{\mathrm{unif}}\times\mathrm{P}_{\mathbf{F}Z}(\mathcal{A}^c),
\end{aligned}\tag{11}$$

where the first inequality follows from the definition of variational distance, and the second is a consequence of the security condition (3) satisfied by the ϵ-SK $K_\mathcal{M}$. The second term above can be expressed as follows:

$$\begin{aligned}
\mathrm{P}^{(\mathcal{M})}_{\mathrm{unif}}\times\mathrm{P}_{\mathbf{F}Z}(\mathcal{A}^c) &= \sum_{\mathbf{f},z}\mathrm{P}_{\mathbf{F}Z}(\mathbf{f},z)\frac{1}{|\mathcal{K}|}\sum_k \mathbb{1}\left((\mathbf{k},\mathbf{f},z)\in\mathcal{A}^c\right)\\
&= \sum_{\mathbf{f},z}\mathrm{P}_{\mathbf{F}Z}(\mathbf{f},z)\frac{1}{|\mathcal{K}|}\sum_k \mathbb{1}\left(\mathrm{Q}^\pi_{K_\mathcal{M}|\mathbf{F}Z}(\mathbf{k}|\mathbf{f},z)|\mathcal{K}|^{|\pi|}\eta^{|\pi|} > 1\right),
\end{aligned}\tag{12}$$

where $\mathbf{k} = (k,\ldots,k)$. The inner sum can be further upper bounded as

$$\begin{aligned}
\sum_k \mathbb{1}\left(\mathrm{Q}^\pi_{K_\mathcal{M}|\mathbf{F}Z}(\mathbf{k}|\mathbf{f},z)|\mathcal{K}|^{|\pi|}\eta^{|\pi|} > 1\right) &\le \sum_k\left(\mathrm{Q}^\pi_{K_\mathcal{M}|\mathbf{F}Z}(\mathbf{k}|\mathbf{f},z)|\mathcal{K}|^{|\pi|}\eta^{|\pi|}\right)^{\frac{1}{|\pi|}}\\
&= |\mathcal{K}|\eta\sum_k \mathrm{Q}^\pi_{K_\mathcal{M}|\mathbf{F}Z}(\mathbf{k}|\mathbf{f},z)^{\frac{1}{|\pi|}}\\
&= |\mathcal{K}|\eta\sum_k\prod_{i=1}^{|\pi|}\mathrm{Q}^\pi_{K_{\pi_i}|\mathbf{F}Z}(\mathbf{k}|\mathbf{f},z)^{\frac{1}{|\pi|}},
\end{aligned}\tag{13}$$

where the previous equality uses Lemma 2 and the fact that given $\mathbf{F}$, K_{π_i} is a function of (X_{π_i}, U_{π_i}). Next, an application of Hölder's inequality to the sum on the right-side of (13) yields

$$\begin{aligned}
\sum_k\prod_{i=1}^{|\pi|}\mathrm{Q}^\pi_{K_{\pi_i}|\mathbf{F}Z}(\mathbf{k}|\mathbf{f},z)^{\frac{1}{|\pi|}} &\le \prod_{i=1}^{|\pi|}\left(\sum_k \mathrm{Q}^\pi_{K_{\pi_i}|\mathbf{F}Z}(\mathbf{k}|\mathbf{f},z)\right)^{\frac{1}{|\pi|}}\\
&\le \prod_{i=1}^{|\pi|}\left(\sum_{k_\pi}\mathrm{Q}^\pi_{K_{\pi_i}|\mathbf{F}Z}(k_{\pi_i}|\mathbf{f},z)\right)^{\frac{1}{|\pi|}}\\
&= 1.
\end{aligned}\tag{14}$$

Upon combining (12)-(14) we obtain

$$\mathrm{P}_{\mathrm{unif}}^{(\mathcal{M})} \times \mathrm{P}_{\mathbf{F}Z}(\mathcal{A}^c) \leq \eta,$$

which along with (11) gives

$$\mathrm{P}_{K_{\mathcal{M}}\mathbf{F}Z}\left(\mathcal{A}^c\right) \leq \epsilon + \eta. \tag{15}$$

It follows from (15) and (10) that

$$\beta_{\epsilon+\eta}\big(\mathrm{P}_{K_{\mathcal{M}}\mathbf{F}Z}, \mathrm{Q}^{\pi}_{K_{\mathcal{M}}\mathbf{F}Z}\big) \leq |\mathcal{K}|^{1-|\pi|}\eta^{-|\pi|},$$

which completes the proof. □

Proof of Theorem 1. Using the data processing inequality (5) with $\mathrm{P} = \mathrm{P}_{X_{\mathcal{M}}Z}$, $\mathrm{Q} = \mathrm{Q}^{\pi}_{X_{\mathcal{M}}Z}$, and $W = W_{K_{\mathcal{M}}\mathbf{F}|X_{\mathcal{M}}Z}$, we get

$$\beta_{\epsilon+\eta}\big(\mathrm{P}_{X_{\mathcal{M}}Z}, \mathrm{Q}^{\pi}_{X_{\mathcal{M}}Z}\big) \leq \beta_{\epsilon+\eta}\big(\mathrm{P}_{K_{\mathcal{M}}\mathbf{F}Z}, \mathrm{Q}^{\pi}_{K_{\mathcal{M}}\mathbf{F}Z}\big),$$

which along with Lemma 1 gives Theorem 1. □

We close this section with a simple extension of the bound of Theorem 1. Consider a RV $\overline{Z}$ such that $X_{\mathcal{M}} — Z — \overline{Z}$ is a Markov chain. Then, $S_\epsilon\left(X_1, ..., X_m \mid Z\right)$ cannot decrease if the eavesdropper observes $\overline{Z}$ instead of Z, i.e.,

$$S_\epsilon\left(X_1, ..., X_m \mid Z\right) \leq S_\epsilon\left(X_1, ..., X_m \mid \overline{Z}\right).$$

This observation and Theorem 1 give the following result.

Corollary 1. *Given $0 \leq \epsilon < 1$, $0 < \eta < 1 - \epsilon$, a partition π of $\mathcal{M}$ and a RV $\overline{Z}$ such that $X_{\mathcal{M}} — Z — \overline{Z}$ is a Markov chain. It holds that*

$$S_\epsilon\left(X_1, ..., X_m \mid Z\right) \leq \frac{1}{|\pi| - 1}\Big[- \log \beta_{\epsilon+\eta}\big(\mathrm{P}_{X_{\mathcal{M}}\overline{Z}}, \mathrm{Q}^{\pi}_{X_{\mathcal{M}}\overline{Z}}\big) + |\pi| \log(1/\eta)\Big],$$

for all $\mathrm{Q}^{\pi}_{X_{\mathcal{M}}\overline{Z}}$ satisfying $\mathrm{Q}^{\pi}_{X_{\mathcal{M}}|\overline{Z}} = \prod_{i=1}^{|\pi|} \mathrm{Q}^{\pi}_{X_{\pi_i}|\overline{Z}}$.

4 Asymptotic tightness of the upper bound

In this section, we show that our upper bound on $S_\epsilon\left(X_1, ..., X_m \mid Z\right)$ in Theorem 1 is asymptotically tight. Moreover, it extends some previously known upper bounds on C to upper bounds on $C(\epsilon)$, for all $0 < \epsilon < 1$.

First, consider the case where the eavesdropper gets no side information, i.e., $Z =$ constant. With this simplification, the SK capacity C for multiple parties was characterized by Csiszár and Narayan [13]. Furthermore, they introduced the remarkable expression on the right-side of (16) below as an upper bound for C, and showed its tightness for $m = 2, 3$. Later, the tightness of the upper bound for arbitrary m was shown in [9]; we summarize these developments in the result below.

Theorem 2. *[13, 9] The SK capacity C for the case when eavesdropper's side information $Z =$ constant is given by*

$$C = \min_{\pi} \frac{1}{|\pi| - 1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \middle\| \prod_{i=1}^{|\pi|} \mathrm{P}_{X_{\pi_i}}\right), \tag{16}$$

where the min *is over all partitions π of $\mathcal{M}$.*

This generalized the classic result of Maurer [20] and Ahlswede and Csiszár [1], which established that for two parties, $C = D\left(\mathrm{P}_{X_1X_2} \| \mathrm{P}_{X_1} \times \mathrm{P}_{X_2}\right)$, which is the same as Shannon's mutual information between X_1 and X_2.

The converse part of Theorem 2 relied critically on the fact that $\epsilon \to 0$ as $n \to 0$. Below we strengthen the converse and show that the upper bound for SK rates implied by Theorem 2 holds even when ϵ is fixed. Specifically, for $0 < \epsilon < 1$ and $Z =$ constant, an application of Theorem 1 to the IID rvs $X_{\mathcal{M}}^n$, with $\mathrm{Q}^{\pi}_{X_{\mathcal{M}}^n} = \prod_{i=1}^{|\pi|} \mathrm{P}^n_{X_{\pi_i}}$, yields

$$S_\epsilon\left(X_1^n, ..., X_m^n\right) \leq \frac{1}{|\pi| - 1}\left[-\log \beta_{\epsilon+\eta}\left(\mathrm{P}^n_{X_{\mathcal{M}}}, \prod_{i=1}^{|\pi|} \mathrm{P}^n_{X_{\pi_i}}\right) + |\pi| \log(1/\eta)\right],$$

where $\eta < 1 - \epsilon$. Therefore, using Stein's Lemma (see (6)) we get

$$\begin{aligned} C(\epsilon) &\leq \frac{1}{|\pi| - 1} \liminf_{n \to \infty} -\frac{1}{n} \log \beta_{\epsilon+\eta}\left(\mathrm{P}^n_{X_{\mathcal{M}}}, \prod_{i=1}^{|\pi|} \mathrm{P}^n_{X_{\pi_i}}\right) \\ &= \frac{1}{|\pi| - 1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \middle\| \prod_{i=1}^{|\pi|} \mathrm{P}_{X_{\pi_i}}\right). \end{aligned}$$

Thus, we have established the following *strong converse* for the SK capacity when $Z =$ constant.

Corollary 2 (Strong Converse). *For every $0 < \epsilon < 1$, the ϵ-SK capacity when $Z =$ constant is given by*

$$C(\epsilon) = C = \min_{\pi} \frac{1}{|\pi| - 1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \middle\| \prod_{i=1}^{|\pi|} \mathrm{P}_{X_{\pi_i}}\right).$$

Next, we consider the general case for two parties, where the eavesdropper's side information Z may not be constant. Applying Corollary 1 with

$$\mathrm{Q}^{\pi}_{X_1^n X_2^n \overline{Z}^n} = \mathrm{P}^n_{X_1|\overline{Z}} \mathrm{P}^n_{X_2|\overline{Z}} \mathrm{P}^n_{\overline{Z}}$$

and following the steps above, we get the *intrinsic conditional information* bound of [21], without requiring the ϵ to vanish to 0.[14]

[14] This bound is a stepping stone for other, often tighter, bounds [26, 15].

Corollary 3. *For every $0 < \epsilon < 1$, the ϵ-SK capacity for two parties ($m = 2$) is bounded above as*[15]

$$C(\epsilon) \leq \min_{\mathrm{P}_{\bar{Z}|Z}} I(X_1 \wedge X_2|\bar{Z}).$$

5 Implications for secure computing with trusted parties

In this section, we present a connection of our result to a problem of secure function computation with trusted parties, where the parties seek to compute a function of their observations using a communication that does not reveal the value of the function by itself (without the observations at the terminals). This is in contrast to the traditional definition of secure computing [37] where the communication is secure but the parties are required not to get any more information than the computed function value. This problem was introduced in [33] where a matching necessary and sufficient condition was given for the feasibility of secure computing in the asymptotic case with IID observations. Here, using Theorem 1, we derive a necessary condition for the feasibility of such secure computing for general observations (not necessarily IID).

5.1 Problem Formulation

Consider $m \geq 2$ parties observing RVs $X_1, ..., X_m$ taking values in finite sets $\mathcal{X}_1, ..., \mathcal{X}_m$, respectively. Upon making these observations, the parties communicate interactively in order to *securely compute* a function $g : \mathcal{X}_1 \times ... \times \mathcal{X}_m \to \mathcal{G}$ in the following sense: The ith party forms an estimate $G_{(i)}$ of the function based on its observation X_i, local randomization U_i and interactive communication $\mathbf{F}$, i.e., $G_{(i)} = G_{(i)}(U_i, X_i, \mathbf{F})$. For $0 \leq \epsilon, \delta < 1$, a function g is (ϵ, δ)-*securely computable* if there exists a protocol satisfying

$$\mathrm{P}\left(G = G_{(1)} = ... = G_{(m)}\right) \geq 1 - \epsilon, \tag{17}$$

$$\frac{1}{2} \left\| \mathrm{P}_{G\mathbf{F}} - \mathrm{P}_G \times \mathrm{P}_{\mathbf{F}} \right\| \quad \leq \delta, \tag{18}$$

where $G = g\left(X_{\mathcal{M}}\right)$. The first condition captures the reliability of computation and the second condition ensures the security of the protocol. Heuristically, for security we require that an observer of (only) $\mathbf{F}$ must not get to know the computed value of the function. We seek to characterize the (ϵ, δ)-securely computable functions g.

In [33], an asymptotic version of this problem was addressed. The parties observe $X_1^n, ..., X_m^n$ and seek to compute $G_t = g\left(X_{1t}, ..., X_{mt}\right)$ for each $t \in \{1, ..., n\}$; consequently, the RVs $\{G_t, 1 \leq t \leq n\}$ are IID. A function g is securely computable if the parties can form estimates $G_{(1)}^{(n)}, ..., G_{(m)}^{(n)}$ such that

$$\mathrm{P}\left(G^n = G_{(1)}^{(n)} = ... = G_{(m)}^{(n)}\right) \geq 1 - \epsilon_n, \quad \tfrac{1}{2} \left\| \mathrm{P}_{G^n\mathbf{F}} - \mathrm{P}_{G^n} \times \mathrm{P}_{\mathbf{F}Z} \right\| \leq \epsilon_n,$$

[15] The min instead of inf is justified by the support lemma [12] (see also [10]).

where $\lim_{n\to\infty} \epsilon_n = 0$. The following characterization of securely computable functions g is known.

Theorem 3. *[33] For the asymptotic case described above, a function g is securely computable if $H(G) < C$, where $H(G)$ is the entropy of the RV $G = g(X_1, ..., X_m)$ and C is the SK capacity.*

Conversely, if a function g is securely computable, then $H(G) \leq C$.

Heuristically, the necessary condition above follows upon observing that if the parties can securely compute the function g, then they can extract a SK of rate $H(G)$ from RVs G^n. Therefore, $H(G)$ must be necessarily less than the maximum rate of a SK that can be generated, namely the SK capacity C.

In the next section, this heuristic is applied to obtain a necessary condition for a function g to be (ϵ, δ)-securely computable for general observations.

5.2 A necessary condition for functions to be securely computable

We present a necessary condition for a function g to be (ϵ, δ)-securely computable. The following definition is required.

Definition 3. *Denote by $\mathcal{P}(\mathcal{X})$ the set $\left\{\mathrm{P} : \mathrm{P}\left(x\right) \geq 0 \; \forall x, \text{ and } \sum_x \mathrm{P}\left(x\right) \leq 1\right\}$. For $\mathrm{P}_X \in \mathcal{P}(\mathcal{X})$, the min-entropy of P_X is given by*

$$H_{\min}\left(\mathrm{P}_X\right) = -\log \max_x \mathrm{P}_X\left(x\right).$$

The ϵ-smooth min-entropy of P_X (cf. [5, 25, 27]) is defined as

$$H_{\min}^{\epsilon}(\mathrm{P}_X) := \max_{\substack{\mathrm{P}\in\mathcal{P}(\mathcal{X}): \\ \frac{1}{2}\|\mathrm{P}_X - \mathrm{P}\| \leq \epsilon}} H_{\min}(\mathrm{P}).$$

Corollary 4. *For $0 \leq \epsilon, \delta < 1$ with $\epsilon + \delta < 1$, if a function g is (ϵ, δ)-securely computable, then*

$$H_{\min}^{\xi}(\mathrm{P}_G) \leq \frac{1}{|\pi| - 1}\left[-\log \beta_\mu\big(\mathrm{P}_{X_\mathcal{M}Z}, \mathrm{Q}^{\pi}_{X_\mathcal{M}Z}\big) + |\pi| \log(1/\eta)\right] + 2\log(1/2\zeta) + 1, \quad \forall\, \mathrm{Q}^{\pi}_{X_\mathcal{M}Z} \in \mathcal{Q}(\pi), \tag{19}$$

for every $\mu := \epsilon + \delta + 2\xi + \zeta + \eta$ with $\xi, \zeta, \eta > 0$ such that $\mu < 1$, and for every partition π of $\mathcal{M}$.

The proof of Corollary 4 is based on extracting an ϵ-SK from the RV G that the parties share. We need the following version of the *Leftover-Hash Lemma*, which is a significant extension of the original result of Impagliazzo-Levin-Luby in [17] (see, also, [2]).

Lemma 3. *(cf. [25, 27]) For $0 \leq \epsilon < 1$ and a RV X taking values in $\mathcal{X}$, there exists*[16] *$K : \mathcal{X} \to \mathcal{K}$ such that the RV $K = K(X)$ satisfies*

$$\frac{1}{2}\left\|\mathrm{P}_K - \mathrm{P}_{\mathrm{unif}}\right\| \leq 2\epsilon + \frac{1}{2}\sqrt{|\mathcal{K}| 2^{-H_{\min}^{\epsilon}(\mathrm{P}_X)}}, \tag{20}$$

where $\mathrm{P}_{\mathrm{unif}}$ is the uniform distribution on $\mathcal{K}$.

[16] A randomly chosen function from a 2-universal hash family suffices.

Proof of Corollary 4. Lemma 3 with $X = G$ and condition (18) imply that there exists $K = K(G)$ with

$$\begin{aligned}
&\frac{1}{2}\left\|\mathrm{P}_{K(G)\mathbf{F}} - \mathrm{P}_{\mathrm{unif}} \times \mathrm{P}_{\mathbf{F}}\right\| \\
&\leq \frac{1}{2}\left\|\mathrm{P}_{K(G)\mathbf{F}} - \mathrm{P}_{K(G)} \times \mathrm{P}_{\mathbf{F}}\right\| + \frac{1}{2}\left\|\mathrm{P}_{K(G)} \times \mathrm{P}_{\mathbf{F}} - \mathrm{P}_{\mathrm{unif}} \times \mathrm{P}_{\mathbf{F}}\right\| \\
&\leq \frac{1}{2}\left\|\mathrm{P}_{G\mathbf{F}} - \mathrm{P}_{G} \times \mathrm{P}_{\mathbf{F}}\right\| + \frac{1}{2}\left\|\mathrm{P}_{K(G)} - \mathrm{P}_{\mathrm{unif}}\right\| \\
&\leq \delta + 2\xi + \frac{1}{2}\sqrt{|\mathcal{K}| 2^{-H_{\min}^{\xi}(\mathrm{P}_G)}}.
\end{aligned}$$

Thus, in the view of Proposition 1, for $|\mathcal{K}| = \lfloor 2^{H_{\min}^{\xi}(\mathrm{P}_G)} 4\zeta^2 \rfloor$, the RV K constitutes[17] an $(\epsilon + \delta + 2\xi + \zeta)$-SK. An application of Theorem 1 gives (19). □

5.3 Illustrative Examples

Example 1. **(Computing functions of independent observations using a perfect SK).** Suppose the ith party observes U_i, where the RVs $U_1, ..., U_m$ are mutually independent. Furthermore, all parties share a κ-bit perfect SK K which is independent of $U_{\mathcal{M}}$. How many bits κ are required to (ϵ, δ)-securely compute a function $g(U_1, ..., U_m)$?

Note that the data observed by the ith party is given by $X_i = (U_i, K)$. A simple calculation shows that for every partition π of $\mathcal{M}$,

$$\beta_\epsilon\left(\mathrm{P}_{X_{\mathcal{M}}}, \prod_{i=1}^{|\pi|} \mathrm{P}_{X_{\pi_i}}\right) \geq (1-\epsilon)\kappa^{1-|\pi|},$$

and therefore, by Corollary 4 a necessary condition for g to be (ϵ, δ)-securely computable is

$$H_{\min}^{\xi}(\mathrm{P}_G) \leq \kappa + \frac{1}{|\pi| - 1}\left(|\pi| \log(1/\eta) + \log(1/(1-\mu))\right) + 2\log(1/2\zeta) + 1, \quad (21)$$

for every $\xi, \zeta, \eta > 0$ satisfying $\mu = \epsilon + \delta + 2\xi + \zeta + \eta < 1$.

For the special case when $U_i = B_i^n$, a sequence of independent, unbiased bits, and

$$g\left(B_1^n, ..., B_m^n\right) = B_{11} \oplus ... \oplus B_{m1}, ..., B_{1n} \oplus ... \oplus B_{mn},$$

i.e., the parties seek to compute the (element-wise) parities of the bit sequences, it holds that $H_{\min}^{\xi}(\mathrm{P}_G) \geq n$. Therefore, (ϵ, δ)-secure computing is feasible only if $n \leq \kappa + O(1)$. We remark that this necessary condition is also (almost) sufficient. Indeed, if $n \leq \kappa$, all but the mth party can reveal all their bits $B_1^n, \ldots, B_{m-1}^n$ and the mth party can send back $B_1^n \oplus \ldots \oplus B_m^n \oplus K_n$, where K_n denotes any n out of κ bits of K. Clearly, this results in a secure computation of g.

[17] Strictly speaking, the estimates $K_1, ..., K_m$ of K formed by different parties constitute the $(\epsilon + \delta + 2\xi + \zeta)$-SK in the sense of (3).

Example 2. **(Secure transmission).** Two parties sharing a κ-bit perfect SK K seek to exchange a message M securely.[18] To this end, they communicate interactively using a communication $\mathbf{F}$, and based on this communication the second party forms an estimate $\hat{M}$ of the first party's message M. This protocol accomplishes (ϵ, δ)-secure transmission if

$$\mathrm{P}\left(M = \hat{M}\right) \geq 1 - \epsilon, \quad \tfrac{1}{2}\left\|\mathrm{P}_{M\mathbf{F}} - \mathrm{P}_M \times \mathrm{P}_{\mathbf{F}}\right\| \leq \delta.$$

The classic result of Shannon [30] implies that $(0, 0)$-secure transmission is feasible only if κ is at least $\log \|M\|$, where $\|M\|$ denotes the size of the message space.[19] But, can we relax this constraint for $\epsilon, \delta > 0$? In this example, we will give a necessary condition for the feasibility of (ϵ, δ)-secure transmission by relating it to the previous example.

Specifically, let the observations of the two parties consist of $X_1 = (M, K)$, $X_2 = K$. Then, (ϵ, δ)-secure transmission of M is tantamount to securely computing the function $g(X_1, X_2) = M$. Therefore, using (21), (ϵ, δ)-secure transmission of M is feasible only if

$$H^{\xi}_{\min}(\mathrm{P}_M) \leq \kappa + 2\log(1/\eta) + \log(1/(1-\mu)) + 2\log(1/2\zeta) + 1, \qquad (22)$$

for every $\xi, \zeta, \eta > 0$ satisfying $\mu = \epsilon + \delta + 2\xi + \zeta + \eta < 1$.

Condition (22) brings out a trade-off between κ and $\epsilon + \delta$ (cf. [18, Problems 2.12 and 2.13]). For an illustration, consider a message M consisting of a RV Y taking values in a set $\mathcal{Y} = \{0, 1\}^n \cup \{0, 1\}^{2n}$ and with the following distribution:

$$\mathrm{P}_Y(y) = \begin{cases} \frac{1}{2} \cdot \frac{1}{2^n} & y \in \{0,1\}^n \\ \frac{1}{2} \cdot \frac{1}{2^{2n}} & y \in \{0,1\}^{2n} \end{cases}.$$

For $\epsilon + \delta = 0$, we know that secure transmission will require κ to be more than the *worst-case message length* $2n$. But perhaps by allowing $\epsilon + \delta$ to be greater than 0, we can make do with fewer SK bits; for instance, perhaps κ equal to $H(M) = (3/2)n + 1$ will suffice (note that the *average message length* equals $(3/2)n$). The necessary condition above says that this is not possible if $\epsilon + \delta < 1/2$. Indeed, since $H^{\xi}_{\min}(\mathrm{P}_Y) \geq 2n$ for $\xi = 1/4$, we get from (22) that the message $M = Y$ can be (ϵ, δ)-securely transmitted only if $2n \leq \kappa + O(1)$, where the constant depends on ϵ and δ.

6 Discussion

The evaluation of the upper bound in Theorem 1 relies on the computation of $\beta_\epsilon(\mathrm{P}, \mathrm{Q})$. The latter is given by a linear program (see (4)), solving which has a polynomial complexity in the size of the observation space. Also, weaker bounds

[18] A message M is a RV with known distribution P_M.

[19] This is a slight generalization of Shannon's original result; see [18, Theorem 2.7] for a proof.

than (8) can be obtained by using upper bounds on $-\log\beta_\epsilon(\mathrm{P},\mathrm{Q})$; the following is easy to show:

$$-\log\beta_\epsilon(\mathrm{P},\mathrm{Q}) \leq \inf_\gamma \gamma - \log\left(\mathrm{P}\left(\log\frac{\mathrm{P}(X)}{\mathrm{Q}(X)} \leq \gamma\right) - \epsilon\right).$$

In particular, using $\gamma = D_\alpha(\mathrm{P},\mathrm{Q}) + \frac{1}{1-\alpha}\log(1-\epsilon-\epsilon')$, where $D_\alpha(\mathrm{P},\mathrm{Q})$ is the Rényi's divergence of order $\alpha > 1$ [29] given by

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

it can be shown that

$$-\log\beta_\epsilon(\mathrm{P},\mathrm{Q}) \leq D_\alpha(\mathrm{P},\mathrm{Q}) + \frac{1}{1-\alpha}\log(1-\epsilon-\epsilon') - \log(\epsilon').$$

In general, this bound is not tight, but it can lead to an upper bound on SK length that is easier to evaluate than the original bound (8) and can also be used to prove Stein's lemma (see (6)). Tighter bounds are available when P and Q correspond to IID RVs or a Markov chain [36].

Finally, we remark that we did not present any general protocols for multiparty SK agreement or for secure function computation with trusted parties. For the SK agreement problem, it is possible to mimic the approach in [20, 1, 13, 27] to obtain protocols that first use communication for *information reconciliation* and then extract SKs using *privacy amplification*. The challenge in the multiparty setup is to identify the appropriate *information to be reconciled*. The task is perhaps even more daunting for the secure function computation with trusted parties where, at the outset, the communication must be selected to be almost independent of the computed function value. A sufficient condition for the existence of such communication can be derived based on the approach in [8] (cf. [28]). Specifically, the sufficient condition will guarantee the existence of random (noninteractive) communication that is almost independent of the function value and at the same time allows each party to recover the collective data of all the parties. But it is unclear if the resulting sufficient condition matches the necessary condition in Corollary 4. In particular, we cannot verify or contradict the following intriguing observations made in [13] and [33] (see, also, [31]), respectively:

1. A largest rate SK can be generated by recovering the collective data of all the parties $X_\mathcal{M}^n$, locally, at each party.[20]
2. Every securely computable function can be computed by first recovering the entire data at each terminal, using a communication that does not give away the value of g.

Examining if these asymptotic principles hold in the general single-shot setting is an interesting future research direction.

[20] Recovering $X_\mathcal{M}^n$ at a party is referred to as the party attaining *omniscience* [13].

Acknowledgment

The authors would like to thank Prakash Narayan for helpful comments and discussions. Also, thanks are due to Jonathan Katz for comments that helped us to improve the presentation.

References

1. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography–part i: Secret sharing. IEEE Trans. Inf. Theory **39**(4) (July 1993) 1121–1132
2. Bennett, C.H., Brassard, G., Crépeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inf. Theory **41**(6) (November 1995) 1915–1923
3. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM J. Comput. **17**(2) (1988) 210–229
4. Bennett, C.H., DiVincenzo, D.P., Smolin, J.A., Wootters, W.K.: Mixed-state entanglement and quantum error correction. Phys. Rev. A **54** (November 1996) 3824–3851
5. Cachin, C.: Smooth entropy and Rényi entropy. EUROCRYPT, LNCS **1233** (1997) 193–208
6. Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols. Proc. Annual Symposium on Foundations of Computer Science (also, see Cryptology ePrint Archive, Report 2000/067) (2001) 136–145
7. Cerf, N., Massar, S., Schneider, S.: Multipartite classical and quantum secrecy monotones. Physical Review A **66**(4) (October 2002) 042309
8. Chan, C.: Agreement of a restricted secret key. Proc. IEEE International Symposium on Information Theory (July 2012) 1782–1786
9. Chan, C., Zheng, L.: Mutual dependence for secret key agreement. Proc. Annual Conference on Information Sciences and Systems (CISS) (2010)
10. Christandl, M., Renner, R., Wolf, S.: A property of the intrinsic mutual information. Proc. IEEE International Symposium on Information Theory (June 2003) 258
11. Csiszár, I.: Almost independence and secrecy capacity. Prob. Pered. Inform. **32**(1) (1996) 48–57
12. Csiszár, I., Körner, J.: Information theory: Coding theorems for discrete memoryless channels. 2nd edition. Cambridge University Press (2011)
13. Csiszár, I., Narayan, P.: Secrecy capacities for multiple terminals. IEEE Trans. Inf. Theory **50**(12) (December 2004) 3047–3061
14. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM Journal on Computing **38**(1) (2008) 97–139
15. Gohari, A.A., Anantharam, V.: Information-theoretic key agreement of multiple terminals?part i. IEEE Trans. Inf. Theory **56**(8) (August 2010) 3973 – 3996
16. Hayashi, M., Nagaoka, H.: General formulas for capacity of classical-quantum channels. IEEE Trans. Inf. Theory **49**(7) (July 2003) 1753–1768
17. Impagliazzo, R., Levin, L.A., Luby, M.: Pseudo-random generation from one-way functions. Proc. Annual Symposium on Theory of Computing (1989) 12–24
18. Katz, J., Lindell, Y.: Introduction to Modern Cryptography. Chapman & Hall/CRC (2007)

19. Kullback, S.: Information Theory and Statistics. Dover Publications (1968)
20. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory **39**(3) (May 1993) 733–742
21. Maurer, U.M., Wolf, S.: Unconditionally secure key agreement and the intrinsic conditional information. IEEE Trans. Inf. Theory **45**(2) (March 1999) 499–514
22. Orlitsky, A., Gamal, A.E.: Communication with secrecy constraints. STOC (1984) 217–224
23. Pappu, R.S.: Physical one-way functions. Ph. D. Dissertation, Massachussetts Institute of Technology (2001)
24. Polyanskiy, Y., Poor, H.V., Verdú, S.: Channel coding rate in the finite blocklength regime. IEEE Trans. Inf. Theory **56**(5) (May 2010) 2307–2359
25. Renner, R.: Security of quantum key distribution. Ph. D. Dissertation, ETH Zurich (2005)
26. Renner, R., Wolf, S.: New bounds in secret-key agreement: The gap between formation and secrecy extraction. EUROCRYPT, LNCS **2656** (2003) 562–577
27. Renner, R., Wolf, S.: Simple and tight bounds for information reconciliation and privacy amplification. ASIACRYPT, LNCS **3788** (2005) 199–216
28. Renner, R., Wolf, S., Wullschleger, J.: Trade-offs in information-theoretic multiparty one-way key agreement. ICITS, LNCS **4883** (2007) 65–75
29. Rényi, A.: On measures of entropy and information. Proc. Fourth Berkeley Symposium on Mathematics Statistics and Probability, Vol. 1 (Univ. of Calif. Press) (1961) 547–561
30. Shannon, C.E.: Communication theory of secrecy systems. Bell System Technical Journal **28** (1949) 656–715
31. Tyagi, H.: Common randomness principles of secrecy. Ph. D. Dissertation, Univeristy of Maryland, College Park (2013)
32. Tyagi, H., Narayan, P.: How many queries will resolve common randomness? IEEE Trans. Inf. Theory **59**(9) (September 2013) 5363–5378
33. Tyagi, H., Narayan, P., Gupta, P.: When is a function securely computable? IEEE Trans. Inf. Theory **57**(10) (October 2011) 6337–6350
34. Vedral, V., Plenio, M.B.: Entanglement measures and purification procedures. Phys. Rev. A **57** (March 1998) 1619–1633
35. Wang, L., Renner, R.: One-shot classical-quantum capacity and hypothesis testing. Phys. Rev. Lett. **108**(20) (May 2012) 200501
36. Watanabe, S., Hayashi, M.: Finite-length analysis on tail probability and simple hypothesis testing for Markov chain. arXiv:1401.3801.
37. Yao, A.C.: Protocols for secure computations. Proc. Annual Symposium on Foundations of Computer Science (1982) 160–164