Impossibility Bounds for Secure Computing

Himanshu Tyagi* Shun Watanabe†

***Abstract*—We derive impossibility (converse) bounds for the efficiency of implementing information theoretically secure oblivious transfer and bit commitment using correlated observations. Our approach is based on relating these problems to that of testing if the observations of the parties are conditionally independent given the adversary's observation. The resulting bounds strengthen and improve upon several previously known results.**

I. Introduction

A folklore heuristic in certain information theory circles [1] states that information theoretic security is feasible because of the advantage that the legitimate parties have over the eavesdropper owing to the residual correlation in their observations, when conditioned on eavesdropper's observation. This simple heuristic is vindicated partly by the asymptotic results in *secret key* (SK) agreement with public communication [17], [2], [6], [7] which show that no positive rate SK can be generated if the observations of the legitimate parties are independent given the observation of the eavesdropper. However, is there a concrete, more direct realization of this heuristic principle? And does it extend to the other canonical problems of cryptography such as secure computing?

In a recent result [29], we provided one such realization for the SK agreement problem. Specifically, we reduced[1] the binary hypothesis testing problem of testing conditional independence of the observations of legitimate parties given the eavesdropper's observation to that of SK agreement – given a SK agreement protocol, one can derive a test for the checking if the observations of the legitimate parties are conditionally independent given the eavesdropper's observation. This in turn led to a bound on the length of a SK that can be generated, which we term the *conditional independence testing* bound.

In this paper, we show a similar connection between conditional independence testing and secure computing. In particular, we reduce the conditional independence testing problem above to two fundamental primitives in information theoretically secure computing [36], namely *oblivious transfer* (OT) [21], [8] and *bit commitment* (BC) [5]. This brings out an explicit connection between the residual correlation mentioned above and these two secure computing primitives. Our reduction proof, illustrated in Fig. 1, is divided into two steps. First, we reduce SK agreement to BC and OT, and then use the reduction of conditional independence testing to SK agreement derived in [29]. As a consequence, we get bounds on the efficiency of implementing these secure computing primitives from correlated observations.

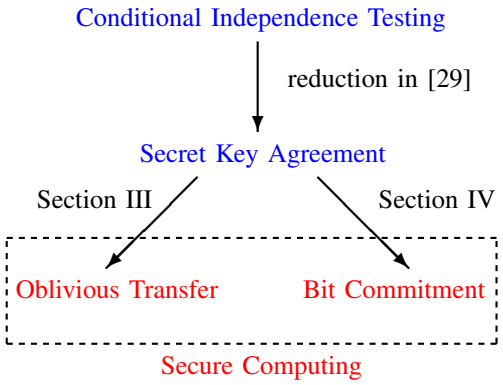

Fig. 1: Depiction of our reduction arguments.

Our single-shot bounds apply to all discrete random variables, and they strengthen and improve some previously known asymptotic bounds. Specifically, it follows from our bounds that an upper bound of Ahlswede and Csiszár [3][2] on OT capacity holds even when the asymptotic perfect OT conditions are dropped and a strong converse holds for the BC capacity established in [33]. To further illustrate the tightness of our bounds, consider the problem of constructing (string) BC of length l from OT of length n. As a simple consequence of our bound, we roughly get (see Example 1 below for details)

$$l \le n + \log(1/(1-\epsilon-\delta_1-\delta_2))$$

for security parameters $\epsilon, \delta_1, \delta_2$, a marked improvement over the previously known bound [22, Corollary 2]

$$l \le \frac{n + h(\delta_1) + h(\epsilon+\delta_2)}{1-\epsilon-\delta_1-\delta_2}, \tag{1}$$

where $h(\cdot)$ is the binary entropy.

The rest of the paper is organized as follows. The next section reviews a basic property of interactive communication, the SK agreement problem, binary hypothesis testing, and the conditional independence testing bound, all of which will be instrumental in our proofs. In the subsequent two sections, we present impossibility or converse bounds for OT and BC.

*Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore, Karnataka 560012, India. Email: htyagi@ece.iisc.ernet.in
†Department of Computer and Information Sciences, Tokyo University of Agriculture and Technology, Tokyo 184-8588, Japan. Email: shunwata@cc.tuat.ac.jp

[1]A *reduction* is a construction of complex protocols from one or more simpler protocols. Such constructions are ubiquitous in cryptography (*cf.* [11]) and form the basis of computational security proofs.

[2]The asymptotic bound in [3] is a special case of a more general asymptotic bound in [23]. It is not clear if our approach can derive a single-shot version of the general bound in [23].

We conclude the paper with a brief discussion in Section V. Due to lack of space, some of the technical proofs have been omitted and can be found in [30].

II. Preliminaries

We start by reviewing some basic notions and results that will be instrumental in our proofs. Some of the observations are new and complete proofs are available in the extended version of this conference paper [30].

A. Interactive communication

An interactive communication $\mathbf{F}$ for two parties consists of stochastic[3] functions $F_1 = F_1(X)$, $F_2 = F_2(Y, F_1)$, $F_3 = F_3(X, F_1, F_2)$, and so on. We begin by noting a simple property of interactive communication, namely that conditionally independent random variables remain so when conditioned additionally on an interactive communication.

Lemma 1 (**Interactive communication property).** ($cf.$ [26]) *Given $\mathrm{Q}_{X_1X_2|Z} = \mathrm{Q}_{X_1|Z}\mathrm{Q}_{X_2|Z}$ and an interactive communication $\mathbf{F}$, the following holds:*

$$\mathrm{Q}_{X_1X_2|\mathbf{F}Z}\left(x_1, x_2|f, z\right) = \mathrm{Q}_{X_1|\mathbf{F}Z}\left(x_1|f, z\right)\mathrm{Q}_{X_2|\mathbf{F}Z}\left(x_2|f, z\right).$$

B. Secret keys using interactive communication

Two parties, with the first observing the random variable X_1 and the second X_2, seek to generate a SK using an interactive public communication $\mathbf{F}$ such that the key remains concealed from an eavesdropper with access to Z and $\mathbf{F}$. To that end, using the communication $\mathbf{F}$ and their local observations, the first and the second party compute, respectively, random functions K_1 and K_2 of $(X_1, \mathbf{F})$ and $(X_2, \mathbf{F})$, with a common range $\mathcal{K}$.

Definition 1. Given $0 \leq \epsilon < 1$, the random variables K_1, K_2 as above, taking values in a common set $\mathcal{K}$, constitute an ϵ-*secret key* (ϵ-SK) if

$$\left\|\mathrm{P}_{K_1K_2\mathbf{F}Z} - \mathrm{P}^{(2)}_{\mathtt{unif}} \times \mathrm{P}_{\mathbf{F}Z}\right\| \leq \epsilon, \tag{2}$$

where $\|\mathrm{P} - \mathrm{Q}\| = \frac{1}{2}\sum_x |\mathrm{P}(x) - \mathrm{Q}(x)|$ is the total variation distance and

$$\mathrm{P}^{(2)}_{\mathtt{unif}}(k_1, k_2) = \frac{1}{|\mathcal{K}|}\mathbb{1}(k_1 = k_2).$$

The maximum length of ϵ-SK is denoted by $S_\epsilon(X_1, X_2|Z)$

C. Binary hypothesis testing

In order to state the required upper bound on $S_\epsilon(X_1, X_2|Z)$, we need a concept from binary 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, $i.e.$,

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

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

We note 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 $x \in \mathcal{X}$, $W(\cdot \mid x)$ is a distribution on $\mathcal{Y}$. Then,
$$\beta_\epsilon(\mathrm{P}, \mathrm{Q}) \leq \beta_\epsilon(\mathrm{P} \circ W, \mathrm{Q} \circ W), \tag{3}$$
where $(\mathrm{P} \circ W)(y) = \sum_x \mathrm{P}\,(x)\,W(y \mid x)$.
2) **Stein's Lemma.** ($cf.$ [16, Theorem 3.3]) For every $0 < \epsilon < 1$, we have
$$\lim_{n\to\infty} -\frac{1}{n}\log \beta_\epsilon(\mathrm{P}^n, \mathrm{Q}^n) = D(\mathrm{P}\|\mathrm{Q}),$$
where $D(\mathrm{P}\|\mathrm{Q})$ is the Kullback-Leibler divergence.

D. The conditional independence testing bound

Our approach for deriving an upper bound entails reducing secure computing to SK agreement and using the *conditional independence testing* upper bound on the maximum length of an ϵ-*SK*, which was derived in [29], [30]. The general upper bound in [29], [30] is a single-shot upper bound on the SK length for a multiparty SK agreement problem, derived by reducing SK agreement to binary hypothesis testing. Here, we recall a specialization to the two party case.

Theorem 2 (**Conditional independence testing bound).** [29], [30] *Given $0 \leq \epsilon < 1$, $0 < \eta < 1 - \epsilon$, the following bound holds:*

$$S_\epsilon\left(X_1, X_2 \mid Z\right) \leq -\log \beta_{\epsilon+\eta}\big(\mathrm{P}_{X_1X_2Z}, \mathrm{Q}_{X_1|Z}\mathrm{Q}_{X_2|Z}\mathrm{Q}_Z\big) + 2\log(1/\eta),$$

for all joint distributions Q on $\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Z}$ that render X_1 and X_2 conditionally independent given Z.

III. Oblivious transfer

We present bounds on the efficiency of implementing information theoretically secure one-of-two OT using correlated randomness. The first party observes K_0 and K_1, distributed uniformly over $\{0, 1\}^l$, and the second party observes a random bit B. The random variables K_0, K_1, and B are mutually independent. Furthermore, party i observes the random variable X_i, $i = 1, 2$, where random variables (X_1, X_2) are independent jointly of (K_0, K_1, B). The second party seeks to compute K_B without giving away B to the first party. At the same time, the first party does not want to give away $K_{\overline{B}}$ to the second party.

Definition 2. (**Oblivious transfer)** An $(\epsilon, \delta_1, \delta_2)$-OT of length l consists of an interactive communication protocol $\mathbf{F}$ and

[3]Local randomness is assumed to be independent of any other randomness in the model.

$\hat{K} = \hat{K}(X_2, B, \mathbf{F})$ such that the following conditions hold[4]:

$$\mathbb{P}\left(K_B \neq \hat{K}\right) \leq \epsilon, \tag{4}$$

$$\left\|\mathrm{P}_{K_{\overline{B}} X_2 B \mathbf{F}} - \mathrm{P}_{K_{\overline{B}}} \times \mathrm{P}_{X_2 B \mathbf{F}}\right\| \leq \delta_1, \tag{5}$$

$$\|\mathrm{P}_{B K_0 K_1 X_1 \mathbf{F}} - \mathrm{P}_B \times \mathrm{P}_{K_0 K_1 X_1 \mathbf{F}}\| \leq \delta_2, \tag{6}$$

where $\overline{B} = 1 \oplus B$. The first condition above denotes the reliability of OT, while the second and the third conditions ensure security for party 1 and 2, respectively. Denote by $O_{\epsilon,\delta_1,\delta_2}(X_1, X_2)$ the largest length l of an $(\epsilon, \delta_1, \delta_2)$-OT.

When the underlying observations X_1, X_2 consist of n-length IID sequences X_1^n, X_2^n with common distribution $\mathrm{P}_{X_1 X_2}$, it is known that $O_{\epsilon,\delta_1,\delta_2}(X_1, X_2)$ may grow linearly with n ($cf.$ [18], [3]); the largest rate of growth is called the OT capacity.

Definition 3 (OT capacity). For $0 < \epsilon < 1$, the ϵ-OT capacity of (X_1, X_2) is defined as

$$C_\epsilon(X_1, X_2) = \lim_{\delta_1,\delta_2 \to 0} \liminf_n \frac{1}{n} O_{\epsilon,\delta_1,\delta_2}(X_1^n, X_2^n),$$

. The OT capacity is defined as

$$C(X_1, X_2) = \lim_{\epsilon \to 0} C_\epsilon(X_1, X_2).$$

The main result of this section is an upper bound on $O_{\epsilon,\delta_1,\delta_2}(X_1, X_2)$. Consequently, we recover the upper bound on $C(X_1, X_2)$ due to Ahlswede and Csiszár derived in [3]. In fact, we show that the upper bound is "strong" and applies to $C_\epsilon(X_1, X_2)$ for every $0 < \epsilon < 1$.

To state this result, and the result of the next section, we need the notions of *maximum common function* and *minimum sufficient statistic*; their role in bounding the performance of secure computing protocols was first highlighted in [35]. Specifically, for random variables X_1, X_2, denote by $\mathrm{mcf}(X_1, X_2)$ the maximum common function of X_1 and X_2 [10] (see, also, [27]). Also, denote by $\mathrm{mss}(X_2|X_1)$ the minimum sufficient statistic for X_2 given X_1, $i.e.$, the minimal function $g(X_1)$ such that the Markov chain X_1—$g(X_1)$—X_2 holds. Specifically, $\mathrm{mss}(X_2|X_1)$ is given by the function resulting from the following equivalence relation on $\mathcal{X}_1$ ($cf.$ [9], [15], [25]):

$$x_1 \sim x_1' \Leftrightarrow \mathrm{P}_{X_2|X_1}(x_2|x_1) = \mathrm{P}_{X_2|X_1}(x_2|x_1'), \quad \text{for all } x_2 \in \mathcal{X}_2.$$

Theorem 3 (Single-shot bound for OT length). *For random variables X_1, X_2, $V_0 = \mathrm{mcf}(X_1, X_2)$ and $V_1 = \mathrm{mss}(X_2|X_1)$, the following inequalities hold:*

$$O_{\epsilon,\delta_1,\delta_2}(X_1, X_2) \leq -\log \beta_\eta\left(\mathrm{P}_{X_1 X_2 V_0}, \mathrm{P}_{X_1|V_0} \mathrm{P}_{X_2|V_0} \mathrm{P}_{V_0}\right) + 2\log(1/\xi), \tag{7}$$

$$O_{\epsilon,\delta_1,\delta_2}(X_1, X_2) \leq -\log \beta_\eta\left(\mathrm{P}_{V_1 V_1 X_2}, \mathrm{P}_{V_1|X_2} \mathrm{P}_{V_1|X_2} \mathrm{P}_{X_2}\right) + 2\log(1/\xi), \tag{8}$$

for all $\xi > 0$ with $\eta = \epsilon + \delta_1 + 2\delta_2 + \xi < 1$.

Corollary 4 (Strong bound for OT capacity). *For $0 < \epsilon < 1$, the ϵ-OT capacity of (X_1, X_2) satisfies*

$$C_\epsilon(X_1, X_2) \leq \min\{I(X_1 \wedge X_2|V_0),\, H(V_1|X_2)\},$$

where $V_0 = \mathrm{mcf}(X_1, X_2)$ and $V_1 = \mathrm{mss}(X_2|X_1)$.

The proof of Theorem 3 entails reducing two SK agreement problems to OT[5]. The bound (7) is obtained by recovering K_B as a SK, while (8) is obtained by recovering $K_{\overline{B}}$ as a SK; we note these two reductions as separate lemmas below.

Lemma 5 (Reduction 1 of SK agreement to OT). *Consider SK agreement for two parties observing X_1 and X_2, respectively, with the eavesdropper observing $V_0 = \mathrm{mcf}(X_1, X_2)$. Given an $(\epsilon, \delta_1, \delta_2)$-OT of length l, there exists a protocol for generating an $(\epsilon + \delta_1 + 2\delta_2)$-SK of length l. In particular,*

$$O_{\epsilon,\delta_1,\delta_2}(X_1, X_2) \leq S_{\epsilon+\delta_1+2\delta_2}(X_1, X_2|V_0).$$

Lemma 6 (Reduction 2 of SK agreement to OT). *Consider two party SK agreement where the first party observes X_1, the second party observes $(V_1, X_2) = (\mathrm{mss}(X_2|X_1), X_2)$ and the eavesdropper observes X_2. Given an $(\epsilon, \delta_1, \delta_2)$-OT of length l, there exists a protocol for generating an $(\epsilon + \delta_1 + 2\delta_2)$-SK of length l. In particular,*

$$O_{\epsilon,\delta_1,\delta_2}(X_1, X_2) \leq S_{\epsilon+\delta_1+2\delta_2}(X_1, (V_1, X_2)|X_2).$$

Remarks. (i) Underlying the proof of $C(X_1, X_2) \leq I(X_1 \wedge X_2)$ in [3] was a reduction of SK agreement to OT, which is extended in our proof of (7). In contrast, the proof of the bound $C(X_1, X_2) \leq H(X_1|X_2)$ in [3] relied on manipulations of entropy terms. We give an alternative reduction argument to prove (8).

(ii) In general, our bounds are stronger than those presented in [32]. For instance, the latter is loose when the observations consist of mixtures of IID random variables. Further, while both (8) and [32, Theorem 5] (specialized to OT) suffice to obtain the second bound in Corollary 4, in contrast to (7), [32, Theorem 2] does not yield the first bound in Corollary 4.

(iii) For simplicity of presentation, we did not allow local randomization in the formulation above. However, it can be easily included as a part of X_1 and X_2 by replacing X_i with (X_i, U_i), $i = 1, 2$, where $U_1, U_2, (X_1, X_2)$ are mutually independent. Since our proofs are based on reduction of SK agreement to OT, by noting that $\mathrm{mss}(X_2, U_2|X_1, U_1) = \mathrm{mss}(X_2|X_1)$ and that the availability of local randomness does not change our upper bound on SK length in Theorem 2, the results above remain valid even when local randomness is available.

(iv) An $(\epsilon, \delta_1, \delta_2)$-OT capacity can be defined, without requiring δ_{1n}, δ_{2n} to go to 0 as in the definition of $C_\epsilon(X_1, X_2)$. The problem of characterizing $(\epsilon, \delta_1, \delta_2)$-OT capacity for all $0 < \epsilon, \delta_1, \delta_2 < 1$ remains open.

[4]Strictly speaking, OT refers to the problem where the strings K_0, K_1 and the bit B are fixed. The randomized version here is sometimes referred as *oblivious key transfer* (see [4], [34]) and is equivalent to OT.

[5]A reduction of SK to OT in a computational security setup appeared in [11].

Theorem 3 follows from Theorem 2, along with the Markov relation X_1—V_1—X_2 and the data processing inequality (3); the corollary follows by Stein's Lemma (see Section II-C).

IV. Bit commitment

Two parties observing correlated observations X_1 and X_2 want to implement information theoretically secure BC using interactive public communication, *i.e.*, the first party seeks to report to the second the results of a series of coin tosses that it conducted at its end in such a manner that, at a later stage, the second party can detect if the first party was lying [5]. Formally, a BC protocol consists of two phases: the *commit phase* and the *reveal phase*. In the commit phase, the first party generates a random string K, distributed uniformly over $\{0,1\}^l$ and independent jointly of (X_1, X_2). Furthermore, the two parties communicate interactively with each other. In the reveal phase, the first party "reveals" its data, *i.e.*, it sends X_1' and K', claiming these were its initial choices of X_1 and K, respectively. Subsequently, the second party applies a (randomized) test function $T = T(K', X_1', X_2, \mathbf{F})$, where $T = 0$ and $T = 1$, respectively, indicate $K' = K$ and $K' \neq K$.

Definition 4 (Bit commitment). An $(\epsilon, \delta_1, \delta_2)$-BC of length l consists of a secret $K \sim \mathtt{unif}\{0,1\}^l$, an interactive communication $\mathbf{F}$ (sent during the commit phase), and a $\{0,1\}$-valued randomized test function $T = T(K', X_1', X_2, \mathbf{F})$ such that the following hold:

$$\mathbb{P}\left(T(K, X_1, X_2, \mathbf{F}) \neq 0\right) \leq \epsilon, \tag{9}$$

$$\|\mathrm{P}_{KX_2\mathbf{F}} - \mathrm{P}_K \times \mathrm{P}_{X_2\mathbf{F}}\| \leq \delta_1, \tag{10}$$

$$\mathbb{P}\left(T(K', X_1', X_2, \mathbf{F}) = 0, K' \neq K\right) \leq \delta_2, \tag{11}$$

where random variables X_1', K' are arbitrary. The first condition above is the *soundness condition*, which captures the reliability of BC. The next condition is the *hiding condition*, which ensures that the second party cannot ascertain the secret in the commit phase. Finally, the *binding condition* in (11) restricts the probability with which the first party can cheat in the reveal phase. Denote by $B_{\epsilon,\delta_1,\delta_2}(X_1, X_2)$ the largest length l of an $(\epsilon, \delta_1, \delta_2)$-BC.

For n-length IID sequences X_1^n, X_2^n generated from $\mathrm{P}_{X_1X_2}$, the largest rate of $B_{\epsilon,\delta_1,\delta_2}(X_1^n, X_2^n)$ is called the BC capacity.

Definition 5 (BC capacity). For $0 < \epsilon, \delta_1, \delta_2 < 1$, the $(\epsilon, \delta_1, \delta_2)$-BC capacity of (X_1, X_2) is defined as

$$C_{\epsilon,\delta_1,\delta_2}(X_1, X_2) = \liminf_n \frac{1}{n} B_{\epsilon,\delta_1,\delta_2}(X_1^n, X_2^n).$$

The BC capacity is defined as

$$C(X_1, X_2) = \lim_{\epsilon,\delta_1,\delta_2 \to 0} C_{\epsilon,\delta_1,\delta_2}(X_1, X_2).$$

The following result of Winters, Nascimento, and Imai [33] (see, also, [24, Chapter 8]) gives a simple formula for $C(X_1, X_2)$.

Theorem 7. [33] *For random variables X_1, X_2, let $V_1 = \mathrm{mss}(X_2|X_1)$. The BC capacity is given by*

$$C(X_1, X_2) = H(V_1 \mid X_2).$$

The main result of this section is an upper bound on $B_{\epsilon,\delta_1,\delta_2}(X_1, X_2)$, which in turn leads to a strong converse for BC capacity.

Theorem 8 (Single-shot bound for BC length). *Given $0 < \epsilon, \delta_1, \delta_2$, $\epsilon + \delta_1 + \delta_2 < 1$, for random variables X_1, X_2 and $V_1 = \mathrm{mss}(X_1|X_2)$, the following inequality holds:*

$$B_{\epsilon,\delta_1,\delta_2}(X_1, X_2) \leq -\log \beta_\eta \left(\mathrm{P}_{V_1V_1X_2}, \mathrm{P}_{V_1|X_2}\mathrm{P}_{V_1|X_2}\mathrm{P}_{X_2}\right) + 2\log(1/\xi),$$

for all ξ with $\eta = \epsilon + \delta_1 + \delta_2 + \xi$.

Corollary 9 (Strong converse for BC capacity). *For $0 < \epsilon, \delta_1, \delta_2$, $\epsilon + \delta_1 + \delta_2 < 1$, the $(\epsilon, \delta_1, \delta_2)$-BC capacity satisfies*

$$C_{\epsilon,\delta_1,\delta_2}(X_1, X_2) \leq H(V_1 \mid X_2),$$

where $V_1 = \mathrm{mss}(X_2|X_1)$.

Theorem 8 is obtained by a reduction of SK agreement to BC, which is along the lines of [33], [14], [22]; the following lemma captures the resulting bound.

Lemma 10 (Reduction of SK to BC). *For $0 < \epsilon, \delta_1, \delta_2$, $\epsilon + \delta_1 + \delta_2 < 1$, it holds that*

$$B_{\epsilon,\delta_1,\delta_2}(X_1, X_2) \leq S_{\epsilon+\delta_1+\delta_2}(X_1, (V_1, X_2) \mid X_2),$$

where $V_1 = \mathrm{mss}(X_2|X_1)$.

Remarks. (i) While local randomization was not allowed in the foregoing discussion, as before (see Remark (iii) following Lemma 6) our results do not change with the availability of local randomness.

(ii) For $\epsilon, \delta_1, \delta_2 > 0$, $\epsilon + \delta_1 + \delta_2 < 1$, the following bound on $B_{\epsilon,\delta_1,\delta_2}(X_1, X_2)$ was derived in [22, Lemma 4]:

$$B_{\epsilon,\delta_1,\delta_2}(X_1, X_2) \leq \frac{H(V_1|X_2) + h(\delta_1) + h(\epsilon + \delta_2)}{1 - \epsilon - \delta_1 - \delta_2},$$

where $h(\cdot)$ is the binary entropy function. However, this bound is weaker than Theorem 8, in general, and is not sufficient for deriving Corollary 9.

Theorem 8 follows by using Lemma 10 with Theorem 2, along with the Markov relation X_1—V_1—X_2 and the data processing inequality (3); Corollary 9 follows by Stein's Lemma (see Section II-C).

We conclude this section by observing a simple application of Theorem 8 in bouding the efficiency of reduction of BC to OT. For a detailed discussion, see [22].

Example 1 (Reduction of BC to OT). Suppose two parties have at their disposal an OT of length n. Using this as a resource, what is the length l of $(\epsilon, \delta_1, \delta_2)$-BC that can be constructed?

Denoting by K_0, K_1 the OT strings, and by B the OT bit of second party, let $X_1 = (K_0, K_1)$ and $X_2 = (B, K_B)$. Note

that (see [30, Section II.B]) when the condition

$$\log \frac{\mathrm{P}(X)}{\mathrm{Q}(X)} = D(\mathrm{P}\|\mathrm{Q}) \tag{12}$$

is satisfied with probability 1 under P, we have

$$-\log \beta_\epsilon(\mathrm{P},\mathrm{Q}) \leq D(\mathrm{P}\|\mathrm{Q}) + \log(1/(1-\epsilon)). \tag{13}$$

Therefore, since (12) holds with $\mathrm{P} = \mathrm{P}_{X_1X_1X_2}$ and $\mathrm{Q} = \mathrm{P}_{X_1|X_2}\mathrm{P}_{X_1X_2}$, and $D(\mathrm{P}_{X_1X_1X_2}\|\mathrm{P}_{X_1|X_2}\mathrm{P}_{X_1X_2}) = n$, by Theorem 8 and (13)

$$l \leq n + \log(1/(1-\epsilon-\delta_1-\delta_2-\eta)) + 2\log(1/\eta),$$

where $0 < \eta < 1-\epsilon-\delta_1-\delta_2$, which is stronger than the multiplicative loss bound (1) derived in [22, Corollary 2] (fixing $n = n' = 1$ in that bound).

V. Discussion

We derived the impossibility bounds for OT and BC by first reducing SK agreement to these secure computing problem and then using the conditional independence testing bound for secret key agreement. In spirit, the conditional independence testing bound can be regarded as a multiterminal variant of the *meta-converse* of Polyanskiy, Poor, and Verdú [20], [19] (see, also, [12], [31]). But there is another crucial difference: the former allows interactive communication. The admissibility of interactive communication makes this bound useful in cryptography where interaction is natural to consider, and it is foreseeable that other applications of this bound in information theoretic secrecy will emerge; an instance arises in [13]. In fact, this bound can find applications in problems involving interactive communication without any secrecy requirements. For instance, it is used in [28] to derive a lower bound for length of interactive communication needed for two parties to exchange their correlated data.

References

[1] Discussions in 2353, A.V. Williams building, University of Maryland, College Park.

[2] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–part i: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[3] ——, "On oblivious transfer capacity," *Information Theory, Combinatorics, and Search Theory*, pp. 145–166, 2013.

[4] D. Beaver, "Precomputing oblivious transfer," in *Advances in Cryptology - CRYPTO*, 1995, pp. 97–109.

[5] M. Blum, "Coin flipping by telephone a protocol for solving impossible problems," *SIGACT News*, vol. 15, no. 1, pp. 23–27, Jan. 1983.

[6] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, December 2004.

[7] ——, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, June 2008.

[8] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Communications of ACM*, vol. 28, no. 6, pp. 637–647, Jun. 1985.

[9] M. Fitzi, S. Wolf, and J. Wullschleger, "Pseudo-signatures, broadcast, and multi-party computation from correlated randomness," in *Advances in Cryptology - CRYPTO*, 2004, pp. 562–578.

[10] P. Gács and J. Körner, "Common information is far less than mutual information," *Problems of Control and Information Theory*, vol. 2, no. 2, pp. 149–162, 1973.

[11] Y. Gertner, S. Kannan, T. Malkin, O. Reingold, and M. Viswanathan, "The relationship between public key encryption and oblivious transfer," in *Proc. Annual Symposium on Foundations of Computer Science (FOCS)*, 2000, pp. 325–335.

[12] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1753–1768, July 2003.

[13] M. Hayashi, H. Tyagi, and S. Watanabe, "Strong converse for a degraded wiretap channel via active hypothesis testing," *Proc. Conference on Communication, Control, and Computing (Allerton)*, 2014.

[14] H. Imai, K. Morozov, A. C. Nascimento, and A. Winter, "Efficient protocols achieving the commitment capacity of noisy correlations," in *Proc. IEEE International Symposium on Information Theory*, 2006, pp. 1432–1436.

[15] S. Kamath and V. Ananthram, "A new dual to the Gács-Körner common information defined via the Gray-Wyner system," *Proc. Conference on Communication, Control, and Computing (Allerton)*, pp. 1340–1346, 2010.

[16] S. Kullback, *Information Theory and Statistics*. Dover Publications, 1968.

[17] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[18] A. C. A. Nascimento and A. Winter, "On the oblivious-transfer capacity of noisy resources," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2572–2581, 2008.

[19] Y. Polyanskiy, "Channel coding: non-asymptotic fundamental limits," *Ph. D. Dissertation, Princeton University*, 2010.

[20] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[21] M. O. Rabin, "How to exchange secrets with oblivious transfer," Cryptology ePrint Archive, Report 2005/187, 2005, http://eprint.iacr.org/.

[22] S. Ranellucci, A. Tapp, S. Winkler, and J. Wullschleger, "On the efficiency of bit commitment reductions," in *Proc. ASIACRYPT*, 2011, pp. 520–537.

[23] K. S. Rao and V. M. Prabhakaran, "A new upperbound for the oblivious transfer capacity of discrete memoryless channels," in *Proc. IEEE Information Theory Workshop*, 2014, pp. 35–39.

[24] P. Tuyls, B. Škorić, and T. Kevenaar (Eds), *Security with Noisy Data*. Springer, 2007.

[25] H. Tyagi, "Common information and secret key capacity," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5627–5640, 2013.

[26] H. Tyagi and P. Narayan, "How many queries will resolve common randomness?" *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5363–5378, September 2013.

[27] H. Tyagi, P. Narayan, and P. Gupta, "When is a function securely computable?" in *Proc. IEEE International Symposium on Information Theory*, 2011, pp. 2876–2880.

[28] H. Tyagi, P. Viswanath, and S. Watanabe, "Interactive communication for data exchange," *to appear, IEEE International Symposium on Information Theory*, 2015.

[29] H. Tyagi and S. Watanabe, "A bound for multiparty secret key agreement and implications for a problem of secure computing," in *Proc. EUROCRYPT*, 2014, pp. 369–386.

[30] ——, "Converses for secret key agreement and secure computing," *CoRR*, vol. abs/1404.5715, 2014.

[31] L. Wang and R. Renner, "One-shot classical-quantum capacity and hypothesis testing," *Phys. Rev. Lett.*, vol. 108, no. 20, p. 200501, May 2012.

[32] S. Winkler and J. Wullschleger, "On the efficiency of classical and quantum secure function evaluation," *arXiv:1205.5136*, 2012.

[33] A. Winter, A. C. A. Nascimento, and H. Imai, "Commitment capacity of discrete memoryless channels," in *Proc. Cryptography and Coding*, 2003, pp. 35–51.

[34] S. Wolf and J. Wullschleger, "Oblivious transfer is symmetric," in *Proc. EUROCRYPT*, 2006, pp. 222–232.

[35] ——, "New monotones and lower bounds in unconditional two-party computation," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2792–2797, June 2008.

[36] A. C. Yao, "Protocols for secure computations," in *Proc. Annual Symposium on Foundations of Computer Science (FOCS)*, 1982, pp. 160–164.