Common Randomness for Secure Computing

Prakash Narayan* Himanshu Tyagi† Shun Watanabe‡

***Abstract*—We revisit A.C. Yao's classic problem of secure function computation by interactive communication, in an information theoretic setting. Our approach, based on examining the underlying common randomness, provides a new proof of the characterization of a securely computable function by deterministic protocols. This approach also yields a characterization of the minimum communication needed for secure computability.**

***Key words*: Common randomness, maximum common function, recoverability, secure computing, security.**

I. Introduction

Terminals 1 and 2 observe, respectively, the finite-valued random variables (rvs) X_1 and X_2. They seek to compute a given function $G = g(X_1, X_2)$ using an interactive communication protocol in such a manner that each terminal should glean no information about the other terminal's observation than can be obtained from its own observation and the function value. This basic problem of secure computing, introduced in the seminal work of Yao [23], has been studied extensively in cryptography for both computational as well as information theoretic secrecy criteria (cf. [18], [5], [4], [6], [3], [11]).

When the terminals communicate, they generate *common randomness* (CR) [1], namely shared bits known to both parties. Even in an ideal world where an oracle reveals the value of G to both terminals and no information is exchanged between them, the two parties acquire not only G but the *maximum common function* V of the rvs (X_1, G) and (X_2, G). We shall term this the *oracle CR*. Heuristically, a secure protocol is one that reveals no more than the oracle CR to the two terminals. In this work, restricting ourselves to deterministic protocols that do not use local randomness, we provide a simple proof of this heuristic statement: the CR generated by any perfectly information theoretically secure protocol is exactly the oracle CR and no more. This provides a characterization of the CR that is generated in securely computing a function.

Clearly, if the oracle CR V is an interactive function of X_1 and X_2, then the two terminals can securely compute G by simply revealing the oracle CR interactively; in fact, this observation holds in a more general and abstract setting (see [14] for details). On the other hand, our result above implies that if G is securely computable then the corresponding oracle CR is an interactive function. Thus, a function is securely computable if and only if its oracle CR is an interactive function. This characterization of securely computable functions was first discovered by [3] and [11] (see also [13] for statistically secure setting). We provide a simple and operational proof of this fundamental result by a different approach, as our first contribution. It also clarifies how exactly the property of interactive communication comes into play.

Another consequence of our characterization of the CR generated in secure computing is a bound for the "size" of secure interactive communication needed for the purpose, which is our second contribution. Specifically, a basic property of interactive communication noted in [15], [1], implies that the entropy of an interactive communication $\mathbf{F}$ that computes a function G must satisfy

$$H(\mathbf{F}) \geq H(G|X_1) + H(G|X_2).$$

Furthermore, when the rvs X_1 and X_2 are independent, the minimum such communication needed to securely compute G coincides with the oracle CR, and

$$H(\mathbf{F}) = H(V) = H(G|X_1) + H(G|X_2).$$

See [11], [8] for related results of a similar spirit.

The next section contains a formal description of secure computation. Section III contains our main results, followed by a discussion in the final section of our continuing work.

II. Secure Computation

We begin with a formal description of secure computation. Terminals 1 and 2 observe, respectively, rvs X_1 and X_2 taking values in finite sets $\mathcal{X}_1$ and $\mathcal{X}_2$, and with known joint probability mass function (pmf) $\mathrm{P}_{X_1X_2}$. An *interactive communication* protocol entails the terminals communicating with each other alternatingly, with a message from each terminal being allowed to depend on its local observation and all previous exchanges. We assume without loss of generality that the communication of the terminals takes place in consecutive time slots in r rounds. The resulting interactive communication is described in terms of the mappings

$$f_{11}, f_{12}, f_{21}, f_{22}, \ldots, f_{r1}, f_{r2}, \tag{1}$$

with f_{ti} corresponding to a message in round t from terminal i, $1 \leq t \leq r$, $i = 1, 2$; in general, f_{ti} is allowed to yield any function of X_i and all the previous communication. The corresponding rvs representing the interactive communication are depicted collectively as

$$\mathbf{F} = (F_{11}, F_{12}, F_{21}, F_{22}, \ldots, F_{r1}, F_{r2}),$$

*Department of Electrical and Computer Engineering, and the Institute for Systems Research, University of Maryland, College Park, MD 20742, USA. Email: prakash@umd.edu.

†Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 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.

where $\mathbf{F} = \mathbf{F}(X_1, X_2)$.

For a given mapping $g : \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{Z}$, terminals 1 and 2, observing X_1 and X_2, seek to compute the function $G \triangleq g(X_1, X_2)$ of their collective data (X_1, X_2) using interactive communication, in such a way that each terminal gleans no more information about the other terminal's observation than can be obtained from its own observation and the function value. We require *exact recovery* and *perfect security*, i.e., that there exist an interactive communication $\mathbf{F}$ and local estimates $G_i = g_i(X_i, \mathbf{F})$, $i = 1, 2$, such that

$$P(G_1 = G_2 = G) = 1, \tag{2}$$

and

$$H(X_i|X_{i^c}, G) = H(X_i|X_{i^c}, \mathbf{F}), \quad i = 1, 2, \tag{3}$$

where i^c denotes $\{1, 2\}\backslash\{i\}$. Note that under the exact recoverability condition (2), the security condition (3) becomes

$$I(X_i \wedge \mathbf{F}|X_{i^c}, G) = H(\mathbf{F}|X_{i^c}, G) = 0, \quad i = 1, 2. \tag{4}$$

A function G is called *securely computable* if there exists an interactive communication $\mathbf{F}$ that satisfies (2) and (4). Our main result characterizes the CR that is generated in securely computing such a function. The concept of CR introduced in [1] and the related notion of *maximum common function* introduced in [10] are defined below.

Definition 1 (Common Randomness). An rv $L = L(X_1, X_2)$ is (exact) CR for the terminals 1 and 2 using communication $\mathbf{F}$, if there exist local estimates

$$L_i = L_i(X_i, \mathbf{F}), \ i = 1, 2$$

satisfying

$$P(L_1 = L_2 = L) = 1.$$

Definition 2 (Maximum Common Function). A maximum common function of finite-valued rvs A_1 and A_2 with joint pmf $\mathrm{P}_{A_1A_2}$, denoted by $\mathtt{mcf}(A_1, A_2)$, is a "common function" of A_1 and of A_2, i.e., there exist functions $\alpha(A_1)$ and $\beta(A_2)$ such that $P(\alpha(A_1) = \beta(A_2)) = 1$; and such that every common function of A_1 and A_2 is a function of $\mathtt{mcf}(A_1, A_2)$.

Loosely speaking, the rv $\mathtt{mcf}(A_1, A_2)$ represents the maximum CR shared by two terminals with access to the rvs A_1 and A_2, *without communication* between themselves.

The characterization of securely computable functions that we provide in the next section is in terms of the operational definition of `mcf` above. On the other hand, the characterization of a securely computable function in [3], [11] is intrinsically in terms of a constructive characterization of `mcf` in [10]; thus, the two characterizations are equivalent.

III. Main Results

Consider an oracle model in which the value of function $G = g(X_1, X_2)$ is gifted to both terminals (but no communication between them is allowed). Then,

$$V \triangleq \mathtt{mcf}((X_1, G), (X_2, G)), \tag{5}$$

termed the *oracle CR*, is the maximum CR shared by the oracle-aided terminals.

Note that the *oracle CR*, too, is a function of (X_1, X_2). We begin by showing that when the terminals compute G by any[1] communication $\mathbf{F}$, they compute, in effect, the oracle CR. Furthermore, the security of each computation implies the other.

Lemma 1 (Equivalence of computing G and oracle CR). *A function $G = g(X_1, X_2)$ is securely computable by any communication $\mathbf{F}$ iff $V = \mathtt{mcf}((X_1, G), (X_2, G))$ is securely computable by $\mathbf{F}$.*

Proof: For *any* communication $\mathbf{F}$, it holds by the definition of V that

$$\begin{aligned} H(V|X_i, \mathbf{F}) &\le H(X_i, G|X_i, \mathbf{F}) \\ &= H(G|X_i, \mathbf{F}) \\ &\le H(V|X_i, \mathbf{F}), \end{aligned}$$

upon noting that G is a function of V. Therefore,

$$H(V|X_i, \mathbf{F}) = H(G|X_i, \mathbf{F}), \quad i = 1, 2,$$

Similarly, for $i = 1, 2$,

$$\begin{aligned} I(X_i \wedge \mathbf{F}|X_{i^c}, V) &= I(X_i \wedge \mathbf{F}|X_{i^c}, V, G) \\ &= I(X_i \wedge \mathbf{F}|X_{i^c}, G). \end{aligned}$$

Thus, the recoverability condition (2) and the security condition (4) apply identically to V and G, for any communication $\mathbf{F}$. ∎

The rvs A_1 and A_2 will be said to be *equivalent*, denoted $A_1 \equiv A_2$, if $H(A_1|A_2) = H(A_2|A_1) = 0$, i.e., in essence, the rvs A_1 and A_2 are the same.

The oracle CR V has the following simple and useful invariance property.

Lemma 2 (Invariance of oracle CR). *Given a function $G = g(X_1, X_2)$, the oracle CR $V = \mathtt{mcf}((X_1, G), (X_2, G))$ satisfies*

$$V \equiv \mathtt{mcf}((X_1, V), (X_2, V)).$$

Proof: Since G is a function of V,

$$\mathtt{mcf}((X_1, V), (X_2, V)) \equiv \mathtt{mcf}((X_1, V, G), (X_2, V, G)),$$

and since V is a common function of (X_1, G) and of (X_2, G),

$$\begin{aligned} \mathtt{mcf}((X_1, V, G), (X_2, V, G)) &\equiv \mathtt{mcf}((X_1, G), (X_2, G)) \\ &\equiv V. \end{aligned}$$

∎

Given any communication $\mathbf{F}$, let $\hat{V}$ denote the maximum CR that the two terminals can generate using $\mathbf{F}$, *i.e.*,

$$\hat{V} \triangleq \mathtt{mcf}((X_1, \mathbf{F}), (X_2, \mathbf{F})).$$

Since G is recoverable from $(X_1, \mathbf{F})$ and $(X_2, \mathbf{F})$, the CR $\hat{V}$ must contain the oracle CR V. Our first main result shows

[1] By "any," we mean hereafter "not necessarily interactive."

that the security condition renders $\hat{V}$ to be exactly the oracle CR.

Theorem 3. *If G is securely computable by any communication $\mathbf{F}$, then $\hat{V}$ is equivalent to the oracle CR V.*

Proof: By Lemma 1, the secure computability of G by $\mathbf{F}$ is tantamount to that of V by $\mathbf{F}$. Then the recoverability condition (2) and the security condition (4) yield

$$\begin{aligned}\mathtt{mcf}((X_1,\mathbf{F}),(X_2,\mathbf{F})) &\equiv \mathtt{mcf}((X_1,\mathbf{F},V),(X_2,\mathbf{F},V))\\ &\equiv \mathtt{mcf}((X_1,V),(X_2,V))\\ &\equiv V,\end{aligned}$$

where the last step uses Lemma 2. ∎

The result above provides an exact characterization of the CR that is generated by any communication $\mathbf{F}$ that securely computes G – it is exactly the oracle CR. In fact, the assertions above hold for *any* communication $\mathbf{F} = \mathbf{F}(X_1, X_2)$.

As a simple consequence of Theorem 3 above, we obtain a characterization of securely computable functions and show that only "trivial" functions are securely computable by *interactive* communication $\mathbf{F}$. For this purpose, we define the notion of an *interactive function*.

Definition 3 (Interactive Function). A rv $A = a(X_1, X_2)$ is an interactive function (under $\mathrm{P}_{X_1X_2}$) if there exists interactive communication $\mathbf{F} = \mathbf{F}(X_1, X_2)$ such that $A \equiv \mathbf{F}$.

Thus, an interactive function is one which, with probability 1, induces the same partition as an interactive communication. This property depends both on the structure of the function as well as the support of the pmf $\mathrm{P}_{X_1X_2}$. For instance, the function a defined in Table I is not an interactive function if $\mathrm{P}_{X_1X_2}$ has full support, but it is an interactive function if $\mathrm{P}_{X_1X_2}(2,2) = 0$.

TABLE I: $a(x_1, x_2)$

$x_1 \backslash x_2$	0	1	2
0	a	a	b
1	d	e	b
2	d	c	c

Corollary 4 (Characterization of securely computable functions). *A function $G = g(X_1, X_2)$ is securely computable by interactive communication if and only if $V = \mathtt{mcf}((X_1, G), (X_2, G))$ is an interactive function.*

Remark. Note that while the joint pmf $\mathrm{P}_{X_1X_2}$ is fixed, the characterization of securely computable functions above depends only on its support.

Proof: If V is an interactive function, then choosing $\mathbf{F} = V$ trivially enables the secure computability of V, and, with V as in (5), that of G by Lemma 1.

Next, suppose that G is securely computable by interactive communication $\mathbf{F}$. By Theorem 3, it suffices to show that $\hat{V}$ is an interactive function. Observe that

$$\begin{aligned}\hat{V} &= \mathtt{mcf}((X_1,\mathbf{F}),(X_2,\mathbf{F}))\\ &\equiv \big(\mathbf{F}, \mathtt{mcf}((X_1,\mathbf{F}),(X_2,\mathbf{F}))\big)\\ &\equiv (\mathbf{F}, \alpha(X_1,\mathbf{F}))\\ &\equiv (\mathbf{F}, \beta(X_2,\mathbf{F})),\end{aligned}$$

for some mappings α and β. Clearly if $\mathbf{F}$ is interactive communication, then $\hat{V}$ is an interactive function. ∎

Remark. The fact that G is computed by *interactive* communication is used only in Corollary 4. All the earlier claims hold for any $\mathbf{F}$.

We close this section with a comparison of the set $\mathcal{G}_{\mathtt{int}} = \mathcal{G}_{\mathtt{int}}(\mathrm{P}_{X_1X_2})$ of interactive functions and the set $\mathcal{G}_{\mathtt{sec}} = \mathcal{G}_{\mathtt{sec}}(\mathrm{P}_{X_1X_2})$ of securely computable functions by interactive communication. Clearly, $\mathcal{G}_{\mathtt{int}} \subset \mathcal{G}_{\mathtt{sec}}$. Corollary 4 yields a characterization of $\mathcal{G}_{\mathtt{sec}}$ in terms of $\mathcal{G}_{\mathtt{int}}$. In fact, for the case of independent X_1 and X_2, $\mathcal{G}_{\mathtt{int}}$ can be characterized using $\mathcal{G}_{\mathtt{sec}}$; we provide such a characterization below.

First, for any pmf $\mathrm{P}_{X_1X_2}$, the following fundamental property holds for any interactive function $\mathbf{F}$ (see [15], [1]):

$$I(X_1 \wedge X_2|\mathbf{F}) \le I(X_1 \wedge X_2). \tag{6}$$

Indeed, it follows by (1) that

$$\begin{aligned}I(X_1 \wedge X_2) &= I(X_1, F_{11} \wedge X_2)\\ &\ge I(X_1 \wedge X_2|F_{11})\\ &= I(X_1 \wedge X_2, F_{12}|F_{11})\\ &\ge I(X_1 \wedge X_2|F_{11}, F_{12}),\end{aligned}$$

and the claimed property is obtained by iterating. A simple manipulation yields the equivalent form

$$H(\mathbf{F}) \ge H(\mathbf{F}|X_1) + H(\mathbf{F}|X_2). \tag{7}$$

In particular, for independent X_1 and X_2, an interactive function $\mathbf{F}$ satisfies

$$H(\mathbf{F}) = H(\mathbf{F}|X_1) + H(\mathbf{F}|X_2). \tag{8}$$

Let $\mathcal{G}_{\mathtt{rec}} = \mathcal{G}_{\mathtt{rec}}(\mathrm{P}_{X_1X_2})$ be the set of all functions satisfying (8)[2].

In general, the property (7) does not suffice for characterizing the set $\mathcal{G}_{\mathtt{int}}$. However, for independent X_1 and X_2, the set $\mathcal{G}_{\mathtt{sec}}$ and (8) characterize $\mathcal{G}_{\mathtt{int}}$ as follows:

Proposition 5. *For independent rvs X_1 and X_2, a function g is interactive if and only if g is securely computable by interactive communication and satisfies property* (8)*, i.e.,*

$$\mathcal{G}_{\mathtt{int}} = \mathcal{G}_{\mathtt{sec}} \cap \mathcal{G}_{\mathtt{rec}}.$$

Proof: As noted above, any interactive function g is securely computable by interactive communication and satisfies (8).

For the converse, suppose that G is securely computable by

[2]For independent X_1 and X_2, (8) is tantamount to the function table being partitioned into *rectangles*.

interactive communication and satisfies (8). By Corollary 4, the corresponding oracle CR $V = \mathtt{mcf}\left((X_1, G), (X_2, G)\right)$ is an interactive function. Therefore, (8) holds with V in place of $\mathbf{F}$, *i.e.*,

$$\begin{aligned} H(V) &= H(V|X_1) + H(V|X_2) \\ &= H(G|X_1) + H(G|X_2), \end{aligned}$$

where the previous equality holds since G is a function of V and V is a function of (X_1, G) as well as (X_2, G). But by (8), the right-side above further equals $H(G)$ and it follows that

$$H(G) = H(V). \tag{9}$$

Since $H(G, V) = H(V) + H(G|V) = H(G) + H(V|G)$ and $H(G|V) = 0$, by (9) $H(V|G) = 0$. Hence, the function G, too, is interactive. ∎

Note that, for independent binary rvs X_1 and X_2, the function $g(X_1, X_2) = X_1 \oplus X_2$ is securely computable by Corollary 4 since the corresponding oracle CR $V = (X_1, X_2)$ is an interactive function. However, g does not satisfy (8) and, therefore, is not an interactive function. On the other hand, the function a given in Table I does satisfy (8), but it is not an interactive function for independent X_1 and X_2. Therefore, it is not securely computable.

IV. On Communication Complexity

We now turn to the problem of determining the communication complexity of protocols that securely compute a given function. Specifically, what is the minimum number of bits of communication needed to securely compute G? If G is securely computable, the associated oracle CR V is an interactive function by Corollary 4 and constitutes an interactive communication for securely computing G. Thus, the minimum entropy of a communication that securely computes G securely is bounded above by $H(V)$. In fact, entropy of any interactive communication that securely computes G is bounded above by $H(V)$. Indeed, by condition (4) $\mathbf{F}$ is a function of (X_1, G) and of (X_2, G), and thus of the oracle CR V. Hence, we necessarily have that

$$H(\mathbf{F}) \leq H(V).$$

In order to obtain a lower bound the number of bits that must be communicated to securely compute G, we seek a lower bound for the entropy $H(\mathbf{F})$ of an interactive communication $\mathbf{F}$ that securely computes G.

The following lower bound for $H(\mathbf{F})$, which constitutes our second main result, is an immediate consequence of (7) upon using the recoverability condition (2). Further, it yields as a byproduct a new lower bound for the "worst-case communication complexity."

Proposition 6. *If G is recoverable from interactive communication $\mathbf{F}$, then*

$$H(\mathbf{F}) \geq H(G|X_1) + H(G|X_2).$$

For independent X_1, X_2, if G is securely computable by interactive communication $\mathbf{F}$, then

$$H(\mathbf{F}) = H(V) = H(G|X_1) + H(G|X_2). \tag{10}$$

Corollary 7. *The worst-case communication complexity is bounded below as*

$$\begin{aligned} &\max_{\mathrm{P}_{X_1X_2}} \min_{\mathbf{F}} H\left(\mathbf{F}\left(X_1, X_2\right)\right) \\ &\qquad \geq \max_{\mathrm{P}_{X_1X_2}} \left[H\left(G|X_1\right) + H\left(G|X_2\right)\right]. \end{aligned}$$

Proof: Observe that by the recoverability condition (2),

$$\begin{aligned} &H(\mathbf{F}|X_1) + H(\mathbf{F}|X_2) \\ &= H(\mathbf{F}, G|X_1) + H(\mathbf{F}, G|X_2) \\ &= H(G|X_1) + H(G|X_2) + H(\mathbf{F}|X_1, G) + H(\mathbf{F}|X_2, G). \end{aligned} \tag{11}$$

Thus, the first assertion of the proposition follows by (7).

If X_1 and X_2 are independent, then (7) holds with equality and, consequently, $H(\mathbf{F})$ equals the right side of (11). Furthermore, if G is securely computable by $\mathbf{F}$, then the last two terms on the right side of (11) are zero, so that $H(\mathbf{F})$ equals the right side of (10). Since G is securely computable by interactive communication $\mathbf{F}$, by Corollary 4 the oracle CR V is an interactive communication by which, too, G is securely computable. Hence, $H(V)$ also equals the right side of (10), completing the proof of the proposition. The corollary is immediate. ∎

Remark. Note that for independent X_1 and X_2, for an interactive communication $\mathbf{F}$, we have by (8) and (11) that

$$\begin{aligned} H(\mathbf{F}) = H(G|X_1) + H(G|X_2) \\ + I(\mathbf{F} \wedge X_2|X_1, G) + I(\mathbf{F} \wedge X_1|X_2, G), \end{aligned}$$

since $H(\mathbf{F}|X_1, X_2) = 0$. Therefore, minimizing the entropy rate of communication $\mathbf{F}$ is tantamount to minimizing the cumulative leakage $I(\mathbf{F} \wedge X_2|X_1, G) + I(\mathbf{F} \wedge X_1|X_2, G)$.

V. Looking Ahead at Multiple Terminals

In a multiterminal setting, terminals $1, \ldots, m$, $m \geq 2$, observe, respectively, rvs $X_1, \ldots, X_m$ with known joint pmf $\mathrm{P}_{X_1,\ldots,X_m}$, and wish to compute a function $G = g(X_1, \ldots, X_m)$. For local estimates $G_i = G_i(X_i, \mathbf{F})$, $i = 1, \ldots, m$, the recoverability condition, analogous to (2), is

$$P(G_i = G,\ i = 1, \ldots, m) = 1.$$

A (strong) security condition (cf. (3)) is

$$H(X_B|X_{B^c}, G) = H(X_B|X_{B^c}, \mathbf{F}) \quad \forall B \in \mathcal{B}, \tag{12}$$

where

$$\mathcal{B} = \left\{B \subsetneq \mathcal{M}, B \neq \emptyset\right\}.$$

With the oracle CR defined as[3]

$$V = \mathtt{mcf}((X_i, G),\ i = 1, \ldots, m),$$

expected generalizations of Theorem 3 and Corollary 4 are immediate.

The counterpart of (7) for $m \geq 2$ is

$$H(\mathbf{F}) \geq \max_{\lambda} \sum_{B \in \mathcal{B}} \lambda_B H(\mathbf{F}|X_{B^c}),$$

with equality when $X_1, \ldots, X_m$ are mutually independent, where the maximum is taken over the "fractional partitions":

$$\lambda = \left\{ 0 \leq \lambda_B \leq 1, B \in \mathcal{B},\ \text{s.t.} \sum_{B \in \mathcal{B}: B \ni i} \lambda_B = 1\ \forall i \in \mathcal{M} \right\}$$

(see [7] and also [12]). Using this bound, the generalization of Proposition 6 follows.

A criticism of the security condition in (12) is that it is unduly restrictive, as it entails concealment for *every subset* of terminals from a coalition of *all* the remaining terminals. In fact, it is known that, for $m \geq 3$, certain nontrivial functions are securely computable if a majority of the terminals are "honest" (see [2], [19][4]). This motivates a relaxed definition of security, where concealment is sought from only coalitions of a limited size, leading to a new class of problems.

Finally, the available resources at each terminal can include local randomization, described by rvs $U_1, \ldots, U_m$, which are independent of $X_1, \ldots, X_m$. The rvs $U_1, \ldots, U_m$ themselves may be correlated or not. For $m = 2$, the availability of independent rvs U_1, U_2 at the terminals does not lead to a new problem [3], [11]. However, conclusive answers are still elusive regarding the class of securely computable functions for correlated rvs U_1, U_2 (e.g. see [9], [22], [17]). For $m \geq 3$, the above-mentioned results involving an honest majority rely on mutually independent rvs $U_1, \ldots, U_m$. Hence, the role of local randomization, in general, is yet to be understood fully, despite important advances [16], [21] that are based on approaches different from ours. The potential usefulness of our method in this context is under study.

ACKNOWLEDGEMENT

This work was supported in part by the U.S. National Science Foundation under Grant CCF1117546.

REFERENCES

[1] 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.

[2] D. Beaver, "Multiparty protocols tolerating half faulty processors," *CRYPTO, LNCS*, vol. 435, pp. 560–572, 1989.

[3] ——, "Perfect privacy for two party protocols," *Technical Report TR-11-89, Harvard University*, 1989.

[3]For finite-valued rvs $A_1, \ldots, A_m$, the rv $\mathtt{mcf}(A_1, \ldots, A_m)$ is defined recursively by $\mathtt{mcf}(A_1, \ldots, A_m) = \mathtt{mcf}(\mathtt{mcf}(A_1, \ldots, A_{m-1}), A_m)$, with $\mathtt{mcf}(A_1, A_2)$ as in Definition 2 (see [20]).

[4]In fact, this result holds even for active adversaries. In a "pairwise communication" model, the same result holds if two-thirds of the terminals are honest [4], [6].

[4] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distribution computation," *STOC*, pp. 1–10, 1988.

[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] D. Chaum, C. Crépeau, and I. Damgård, "Multiparty unconditionally secure protocols," *STOC*, pp. 11–19, 1988.

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

[8] D. Data, M. M. Prabhakaran, and V. M. Prabhakara, "On the communication complexity of secure computation," *CRYPTO, LNCS*, vol. 8617, pp. 199–216, 2014.

[9] Y. Dodis and S. Micali, "Lower bound for oblivious transfer reductions," *EUROCRYPT, LNCS*, vol. 1592, pp. 42–55, 1999.

[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] E. Kushilevitz, "Privacy and communication complexity," *SIAM Journal on Math*, vol. 5, no. 2, pp. 273–284, 1992.

[12] M. Madiman and P. Tetali, "Information inequalities for joint distributions, with interpretations and applications," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2699–2713, June 2010.

[13] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Complexity of multiparty computation problems: The case of 2-party symmetric secure function evaluation," *TCC, LNCS*, vol. 5444, pp. 256–273, 2009.

[14] ——, "A unified characterization of completeness and triviality for secure function evaluation," *INDOCRYPTO, LNCS*, vol. 7668, pp. 40–59, 2012.

[15] 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.

[16] V. M. Prabhakaran and M. M. Prabhakaran, "On secure multiparty sampling for more than two parties," in *Information Theory Workshop, 2012. Proceedings of the 2012 IEEE*, Sept. 2012, pp. 99–103.

[17] ——, "Assisted common information with an application to secure two-party samplign," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3413–3434, June 2014.

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

[19] T. Rabin and M. Ben-Or, "Verifiable secret sharing and multiparty protocols with honest majority," *STOC*, pp. 73–85, 1989.

[20] H. Tyagi, P. Narayan, and P. Gupta, "When is a function securely computable?" *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6337–6350, October 2011.

[21] Y. Wang, P. Ishwar, and S. Rane, "Information-theoretically secure three-party computation with one corrupted party," *Proc. IEEE International Symposium on Information Theory*, pp. 3160–3164, July 2013.

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

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