MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

An Elementary Completeness Proof for Secure Two-Party Computation Primitives

Wang, Y.; Ishwar, P.; Rane, S.

TR2014-092 November 2014

Abstract

In the secure two-party computation problem, two parties wish to compute a (possibly randomized) function of their inputs via an interactive protocol, while ensuring that neither party learns more than what can be inferred from only their own input and output. For semi-honest parties and information-theoretic security guarantees, it is well-known that, if only noise-less communication is available, only a limited set of functions can be securely computed; however, if interaction is also allowed over general communication primitives (multi-input/output channels), there are 'complete' primitives that enable any function to be securely computed. The general set of complete primitives was characterized recently by Maji, Prabhakaran, and Rosulek leveraging an earlier specialized characterization by Kilian. Our contribution in this paper is a simple, self-contained, alternative derivation using elementary information-theoretic tools.

IEEE Information Theory Workshop (ITW)

An Elementary Completeness Proof for Secure Two-Party Computation Primitives

Ye Wang
Mitsubishi Electric Research Laboratories
Cambridge, MA, USA
Email: yewang@merl.com

Prakash Ishwar
Boston University
Boston, MA, USA
Email: pi@bu.edu

Shantanu Rane
Mitsubishi Electric Research Laboratories
Cambridge, MA, USA
Email: rane@merl.com

***Abstract*—In the secure two-party computation problem, two parties wish to compute a (possibly randomized) function of their inputs via an interactive protocol, while ensuring that neither party learns more than what can be inferred from only their own input and output. For semi-honest parties and information-theoretic security guarantees, it is well-known that, if only noiseless communication is available, only a limited set of functions can be securely computed; however, if interaction is also allowed over general communication primitives (multi-input/output channels), there are "complete" primitives that enable any function to be securely computed. The general set of complete primitives was characterized recently by Maji, Prabhakaran, and Rosulek leveraging an earlier specialized characterization by Kilian. Our contribution in this paper is a simple, self-contained, alternative derivation using elementary information-theoretic tools.**

I. Introduction

We consider the problem of secure two-party computation, where two parties named Alice and Bob wish to correctly and privately compute outputs from their initial individual inputs, according to a (potentially randomized) function. Correctness means that the outputs should have the appropriate conditional distribution (corresponding to the desired function) with respect to the inputs. Privacy means that neither party should learn anything about the other party's input and output besides what can be inferred from only their own input and output. The aim is to construct an interactive protocol that computes the desired function while satisfying these security goals. We restrict our attention to passive ("honest but curious") parties who will faithfully execute a given protocol, but attempt to extract additional information from their views of the execution. However, we require information-theoretic privacy, providing unconditional security guarantees against adversaries with even unbounded computational power.

We focus on the *feasibility* of constructing protocols for general secure computation when the parties are allowed unlimited interaction via noise-free communication as well as via a given set of communication *primitives*[1], which are general memoryless two-way channels where each party may have an input and an output. In the "from scratch" scenario, where only noise-free communication is allowed and no additional primitives are available, it is well-known that not all functions can be securely computed by two parties (see [1] for example). However, given the availability of certain *complete* primitives, protocols can be constructed to perform any general computation. Oblivious transfer[2] is a complete primitive [2], as is any primitive that enables secure computation of oblivious transfer as the desired function [3]. Identifying complete primitives (and proposing efficient constructions) has been an active area of research with several works characterizing the complete primitives within specific subclasses: one-way channels (primitives with one input and one output) [4], [5], [6], joint sources (primitives with no inputs) [6], and primitives with only one output or a common output [7]. Recently, a general characterization of all complete primitives for the passive secure two-party computation problem was given in [8] by leveraging the specialized results of [7].

Our main contribution is a simple, self-contained, alternative derivation of the general characterization of complete primitives using elementary information-theoretic tools, which contrast with the detailed combinatorial analysis of protocol structure given by [7] and leveraged by [8]. Our converse proof is based on considering the subclass of secure two-party *sampling* problems, where Alice and Bob have no initial inputs and only wish to generate outputs according to a desired joint distribution. This proof technique also clarifies a subtlety: that a set of primitives that are each individually incomplete cannot provide completeness when available together. Further, we observe that the secure sampling problems exhibit a zero-one law, in the sense that any set of primitives is either complete or "useless", i.e., allowing only a set of "trivial" distributions to be sampled. The trivial distributions are those that can be securely sampled from scratch, and were characterized in [9] as those for which the mutual information is equal to the common information[3].

II. Problem Formulation

A. Secure Two-Party Computation Protocols

Alice and Bob respectively start with inputs Q and T with joint distribution $P_{Q,T}$ over the finite alphabet $\mathcal{Q} \times \mathcal{T}$. They wish to securely compute the (in general randomized)

[1]Primitives and functions are the same class of mathematical objects (random channels where each party has an input and output), but we use "primitives" to refer to the channels available for implementing a protocol, while "function" refers to the secure computation objective of the protocol.

[2]Oblivious transfer is the channel where Alice has a two-bit input and no output, and Bob's binary input selects one of Alice's bits to be his output.

[3]This property is equivalent for the Wyner [10] and Gács-Körner [11] notions of common information.

function $P_{X,Y|Q,T}$. To realize this goal, they execute a two-party computation protocol at the end of which Alice outputs $\hat{X} \in \mathcal{X}$ and Bob outputs $\hat{Y} \in \mathcal{Y}$.

A protocol may involve multiple rounds of local computation interspersed with rounds of interaction via error-free communication or through one of the available communication primitives. A *communication primitive* is a channel with input (A, B) in the finite alphabet $\mathcal{A} \times \mathcal{B}$, output (U, V) in the finite alphabet $\mathcal{U} \times \mathcal{V}$, and a conditional distribution $P_{U,V|A,B}$. Each primitive usage is "memoryless", and Alice controls input A and receives output U, while Bob controls input B and receives output V. After the protocol terminates, Alice and Bob generate their respective outputs via deterministic functions of their respective *views* of the protocol. A party's view consists of its initial input, local computations, messages sent/received, and inputs/outputs to/from the used primitives.

For simplicity, we only consider protocols that terminate in a fixed (deterministic) number of rounds n, but do not put a bound on n. A protocol consists of a sequence of steps that governs how the views of the parties can evolve during the protocol's execution. The initial views of Alice and Bob are their respective inputs and denoted by $(R_0, S_0) := (Q, T)$. Let $(R_1, S_1), \ldots, (R_n, S_n)$ denote the sequence of their evolving views over n rounds. In each round t of the protocol, the evolution of views from (R_{t-1}, S_{t-1}) to (R_t, S_t) occurs via one of three possible structured mechanisms: local computation, error-free message passing, or primitive usage (if available).

- (Local computation) $R_t = (R_{t-1}, A)$ and $S_t = (S_{t-1}, B)$, where $A \leftrightarrow R_{t-1} \leftrightarrow S_{t-1} \leftrightarrow B$ is a Markov chain.
- (Message passing) $R_t = (R_{t-1}, g(S_{t-1}))$ and $S_t = (S_{t-1}, f(R_{t-1}))$, where f and g are some deterministic functions.
- (Primitive usage) $R_t = (R_{t-1}, U)$ and $S_t = (S_{t-1}, V)$, where (U, V) are the outputs of one of the given communication primitives, with inputs $A = f(R_{t-1})$ and $B = g(S_{t-1})$ generated via some deterministic functions f and g, and $P_{U,V|A,B}$ corresponds to the distribution governing the primitive used. The memoryless behavior of the primitives implies that $(U, V) \leftrightarrow (A, B) \leftrightarrow (R_{t-1}, S_{t-1})$ is a Markov chain.

After n rounds, outputs are generated deterministically from the final views, that is, $\hat{X} = \phi(R_n)$ and $\hat{Y} = \psi(S_n)$, for some functions ϕ and ψ.

B. Security Definitions

A protocol for computing $P_{X,Y|Q,T}$ is called *ϵ-correct* if and only if the following maximal variational distance does not exceed ϵ:

$$\max_{P_{Q,T}} d(P_{\hat{X},\hat{Y}|Q,T} P_{Q,T}, P_{X,Y|Q,T} P_{Q,T}) \leq \epsilon,$$

where the variational distance is given by $d(P_{\hat{Z}}, P_Z) := \frac{1}{2} \sum_z |P_{\hat{Z}}(z) - P_Z(z)|$. A protocol is *$\delta$-private* if and only if the maximal information leakage of the final views satisfies

$$\max_{P_{Q,T}} I(R_n; \hat{Y}, T|\hat{X}, Q) + I(S_n; \hat{X}, Q|\hat{Y}, T) \leq \delta.$$

We will say that a protocol is (ϵ, δ)-secure if and only if it is ϵ-correct and δ-private. A function $P_{X,Y|Q,T}$ is said to be *securely computable* given a set of primitives if and only if for all $\epsilon, \delta > 0$, there exists a protocol for computing $P_{X,Y|Q,T}$ using the given primitives that is (ϵ, δ)-secure. A primitive is said to be *complete* if and only if any function is securely computable given that primitive. A *set* of primitives is said to *incomplete* if and only if some functions cannot be securely computed via any protocols using that set of primitives. Note that an incomplete set must be comprised of primitives that are each individually incomplete. The reverse implication is not immediately obvious but turns out to be true (see Theorem 1).

C. Secure Two-Party Sampling

The secure two-party *sampling* problem is the special case where Alice and Bob have no inputs and the goal simplifies to generating outputs with the joint distribution $P_{X,Y}$. Their initial views are constant $R_0 = S_0 = 0$ and the conditions for ϵ-correctness and δ-privacy simplify to $d(P_{\hat{X},\hat{Y}}, P_{X,Y}) \leq \epsilon$ and $I(R_n; \hat{Y}|\hat{X}) + I(S_n; \hat{X}|\hat{Y}) \leq \delta$, respectively.

The distributions that can be securely sampled via protocols that use only error-free communication (and no other primitives) will be called *trivial*, since they can always be securely sampled regardless of the other primitives available. A set of primitives is said to be *useless for sampling* if only the trivial distributions can be securely sampled using that set of primitives. Since secure sampling is a special case of secure computation, a complete primitive allows any distribution to be securely sampled. Hence, a set of primitives is incomplete (for general computation) if it is useless for sampling.

III. Characterization Results

A. Preliminaries

Common information plays a key role in the characterizations of both the secure sampling and computation problems. There are two related (and somewhat complementary) notions of common information, one introduced by Wyner [10] and the other introduced by Gács-Körner [11]. We will review only the Wyner common information here to allow us to quickly state our results, and leave Gács-Körner common information and other related concepts to be reviewed later in Section IV.

The Wyner common information of two random variables (X, Y) is given by

$$C(X;Y) := \min_{Z: I(X;Y|Z)=0} I(X, Y; Z),$$

where the minimum can be attained by a $Z \in \mathcal{Z}$ with $|\mathcal{Z}| \leq |\mathcal{X} \times \mathcal{Y}|$ [10]. This quantity characterizes the solution of the Gray-Wyner source coding problem. Note that, in general, $C(X;Y) \geq I(X;Y)$ [10].

It follows from the results of [9] and the continuity of Wyner common information (see Lemma 4 in Section IV), that the trivial distributions, i.e., those which can be securely sampled from scratch, are precisely those where $C(X;Y) = I(X;Y)$ (see Lemma 1 in Section IV for equivalent conditions). We will hence use the terms *trivial* (and *non-trivial*) to refer to

joint distributions $P_{X,Y}$ which do (and, respectively, do not) satisfy $C(X;Y) = I(X;Y)$.

B. Main Results

The main theorem characterizes the complete primitives and notes that incomplete primitives are useless for sampling.

Theorem 1. *A primitive $P_{U,V|A,B}$ is complete if and only if there exist random variables $A \in \mathcal{A}$, $B \in \mathcal{B}$, and Z such that $A \leftrightarrow Z \leftrightarrow B$ is a Markov chain and $C(Z,A,U;Z,B,V) > I(Z,A,U;Z,B,V)$, where $(U,V,A,B,Z) \sim P_{U,V|A,B}P_{A,B,Z}$. Further, any set of incomplete primitives is useless for sampling.*

An interpretation of a complete primitive is that its usage can produce resultant views (Z,A,U) and (Z,B,V) with a non-trivial distribution, while starting from prior views (Z,A) and (Z,B) that have a trivial distribution.

The following corollary characterizes the feasibility of secure sampling, which exhibits a zero-one law: any set of primitives is either complete or useless for sampling.

Corollary 1. *Given any set of primitives, if at least one is complete (see conditions in Theorem 1), then any distribution $P_{X,Y}$ can be securely sampled. Otherwise, only the trivial distributions, where $C(X;Y) = I(X;Y)$, can be securely sampled.*

IV. Properties of Common Information

This section reviews key concepts and results needed to establish our main results. They are, however, also of independent interest.

The *graphical representation* of $P_{X,Y}$ is the bipartite graph with an edge between $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ if and only if $P_{X,Y}(x,y) > 0$. The *common part* of two random variables (X,Y), denoted by $W_{X,Y}$, is the (unique) label of the connected component of the graphical representation of $P_{X,Y}$ in which (X,Y) falls. Note that $W_{X,Y}$ is a deterministic function of X alone and also a deterministic function of Y alone.

The Gács-Körner common information of two random variables (X,Y) is given by $K(X;Y) := H(W_{X,Y})$ [11]. The operational significance of $K(X;Y)$ is that it is the maximum number of common bits per symbol that can be independently extracted from X and Y. Note that, in general, $K(X;Y) \leq I(X;Y)$ [11].

While it may be tedious, in general, to solve the optimization problem that defines Wyner common information, one can conveniently check if it is equal to its lower bound by using its well-known relationship to Gács-Körner common information and other properties given in the following lemma (see [12]).

Lemma 1. [12] *For any random variables (X,Y), the following are equivalent:*

1) $C(X;Y) = I(X;Y)$,
2) $K(X;Y) = I(X;Y)$,
3) *There exists Z such that $Z \leftrightarrow X \leftrightarrow Y$, $Z \leftrightarrow Y \leftrightarrow X$, and $X \leftrightarrow Z \leftrightarrow Y$ are all Markov chains,*
4) *$X \leftrightarrow W_{X,Y} \leftrightarrow Y$ is a Markov chain, where $W_{X,Y}$ is the common part of (X,Y).*

One can also determine whether common information is equal to mutual information by checking if conditional entropy is positive after "removing redundancies" from the random variables. To *remove redundancy* from X with respect to $P_{X,Y}$, first partition the support of P_X into equivalence classes using $P_{Y|X=x} = P_{Y|X=x'}$ as the equivalence rule for $x, x' \in \mathcal{X}$, then uniquely label these classes and define $\tilde{X}$ as the label of the class in which X falls. Similarly, $\tilde{Y}$ can be defined as Y with redundancies removed. Note that, by construction, $X \leftrightarrow \tilde{X} \leftrightarrow \tilde{Y} \leftrightarrow Y$ is a Markov chain.

Lemma 2. *For any random variables (X,Y), the following are equivalent:*

1) $C(X;Y) = I(X;Y) = K(X;Y)$,
2) $H(\tilde{X}|\tilde{Y}) = 0$,
3) $H(\tilde{Y}|\tilde{X}) = 0$,

where $(\tilde{X},\tilde{Y})$ are (X,Y) with redundancies removed.

Proof: This lemma can be shown to follow from the monotone region results of [13]. We, however, provide a simpler, self-contained proof here. Any $x, x' \in \mathcal{X}$ with $P_{Y|X=x} = P_{Y|X=x'}$ are clearly in the same connected component of the graphical representation of $P_{X,Y}$. If $X \leftrightarrow W_{X,Y} \leftrightarrow Y$ is a Markov chain, then for any symbols $x, x' \in \mathcal{X}$ attached to the same connected component, $P_{Y|X=x} = P_{Y|X=x'}$. Thus, given condition 1, we find that $W_{X,Y}$, $\tilde{X}$, and $\tilde{Y}$ (via similar arguments) are equivalent, that is, $W_{X,Y} = f(\tilde{X}) = g(\tilde{Y})$ for some bijective functions f and g. Hence, it follows that condition 1 implies condition 2 and 3. Given condition 2, $\tilde{X}$ is a function of $\tilde{Y}$, and hence a function of Y. By construction, $\tilde{X}$ is a function of X, and $X \leftrightarrow \tilde{X} \leftrightarrow \tilde{Y} \leftrightarrow Y$ is a Markov chain. Hence, $X \leftrightarrow \tilde{X} \leftrightarrow Y$, $\tilde{X} \leftrightarrow X \leftrightarrow Y$, and $\tilde{X} \leftrightarrow Y \leftrightarrow X$ are all Markov chains and condition 1 holds by Lemma 1. Similarly, condition 3 also implies condition 1. ■

Another useful property for checking whether the Wyner common information is close to the mutual information is given in the next lemma from [9].

Lemma 3. [9] *For any random variables (X,Y), $C(X;Y) - I(X;Y) \leq \delta$ if and only if there exist Z such that $X \leftrightarrow Z \leftrightarrow Y$ is a Markov chain, and $I(Z;X|Y) + I(Z;Y|X) \leq \delta$.*

Wyner common information is a uniformly continuous functional of $P_{X,Y}$ for all $P_{X,Y}$ as established in the next lemma. The Gács-Körner common information, in contrast, is discontinuous.

Lemma 4. *If $P_{X,Y}, P_{\hat{X},\hat{Y}}$ are joint distributions over the same finite alphabet $\mathcal{X} \times \mathcal{Y}$ with variational distance $d(P_{\hat{X},\hat{Y}}, P_{X,Y}) \leq \epsilon$, then $|C(X;Y) - C(\hat{X};\hat{Y})| \leq \alpha(\epsilon)$, for some function α where $\alpha(\epsilon) \longrightarrow 0$ as $\epsilon \longrightarrow 0$.*

Proof: One can construct random variables $(X,Y) \sim P_{X,Y}$ and $(\hat{X},\hat{Y}) \sim P_{\hat{X},\hat{Y}}$ such that $\Pr\big((\hat{X},\hat{Y}) \neq (X,Y)\big) = d(P_{\hat{X},\hat{Y}}, P_{X,Y})$ [14]. Let Z be the random variable such that $C(X;Y) = I(X,Y;Z)$ and $X \leftrightarrow Z \leftrightarrow Y$ is a Markov chain.

Next, let

$$\hat{Z} := \begin{cases} (Z, \perp, \perp), & \text{when } (\hat{X}, \hat{Y}) = (X, Y), \\ (\perp, \hat{X}, \hat{Y}), & \text{when } (\hat{X}, \hat{Y}) \neq (X, Y), \end{cases}$$

where $\perp$ is a constant symbol not in the alphabets $\mathcal{X}$, $\mathcal{Y}$, or $\mathcal{Z}$. By construction, $\hat{X} \leftrightarrow \hat{Z} \leftrightarrow \hat{Y}$ is a Markov chain, and $\Pr\left((\hat{X}, \hat{Y}, \hat{Z}) \neq (X, Y, (Z, \perp, \perp))\right) \leq \epsilon$. Thus,

$$\begin{aligned} C(\hat{X}; \hat{Y}) \leq I(\hat{X}, \hat{Y}; \hat{Z}) &\leq I(X, Y; Z) + \alpha(\epsilon) \\ &= C(X; Y) + \alpha(\epsilon) \end{aligned}$$

for some $\alpha(\epsilon)$ with $\alpha(\epsilon) \longrightarrow 0$ as $\epsilon \longrightarrow 0$, where the second inequality follows due to the uniform continuity of entropy [14]. Symmetrically, we can argue that $C(X; Y) \leq C(\hat{X}; \hat{Y}) + \alpha(\epsilon)$, and hence $|C(X; Y) - C(\hat{X}; \hat{Y})| \leq \alpha(\epsilon)$. ■

V. Proof of Theorem 1

A. Converse Result

We will show that, given any set of primitives that each fail to satisfy the completeness conditions, only trivial distributions can be securely sampled, and hence the primitives are incomplete and useless. The first part of our converse proof is closely related to the method of monotones – functionals that are monotonic over the sequence of views – introduced in [15]. Specifically, we will show that the distributions of the views P_{R_t, S_t} will remain trivial throughout the execution of the protocol. Then, we will argue that given final views (R_n, S_n) with a trivial distribution, only "almost trivial" (in the sense of Wyner common information being close to mutual information) outputs can be securely produced by a δ-private protocol. This result, in conjunction with the continuity of Wyner common information (see Lemma 4), implies that only trivial distributions can be securely sampled.

The next two lemmas establish that if we start with views (R_{t-1}, S_{t-1}) that have a trivial distribution, then the views (R_t, S_t), after respectively local computation and message passing, must also have a trivial distribution. Due to space constraints, and since they can be shown to follow from related results in [15], we will omit the proofs of these two lemmas.

Lemma 5. *Let $C(R; S) = I(R; S)$. If $A \leftrightarrow R \leftrightarrow S \leftrightarrow B$ is a Markov chain then $C(A, R; B, S) = I(A, R; B, S)$.*

Lemma 6. *Let $C(R; S) = I(R; S)$. If f, g are deterministic functions then $C(R, g(S); S, f(R)) = I(R, g(S); S, f(R))$.*

The next lemma establishes that if we start from views (R_{t-1}, S_{t-1}) with a trivial distribution, then using a primitive that does not meet the completeness conditions, with any inputs $A = f(R_{t-1})$ and $B = g(S_{t-1})$, results in views $(R_t, S_t) := ((R_{t-1}, U), (S_{t-1}, V))$ that also have a trivial distribution.

Lemma 7. *If a primitive does not meet the completeness conditions of Theorem 1, then for all random variables (R, S) such that $C(R; S) = I(R; S)$ and functions $f : \mathcal{R} \to \mathcal{A}$, $g : \mathcal{S} \to \mathcal{B}$, we have that $C(R, U; S, V) = I(R, U; S, V)$, where $A = f(R)$, $B = g(R)$, and $(U, V) \sim P_{U,V|A,B}$.*

Proof: Let $W_{R,S}$ be the common part of (R, S). By Lemma 1, $(A, R) \leftrightarrow W_{R,S} \leftrightarrow (B, S)$ is a Markov chain. Since the primitive does not meet the completeness conditions, we have that $C(W_{R,S}, A, U; W_{R,S}, B, V) = I(W_{R,S}, A, U; W_{R,S}, B, V)$. Since $(U, V) \leftrightarrow (A, B) \leftrightarrow (R, S, W_{R,S})$ is a Markov chain, $R \leftrightarrow (W_{R,S}, A, U) \leftrightarrow (W_{R,S}, B, V) \leftrightarrow S$ is also a Markov chain. Thus, by Lemma 5, we have that $C(R, U; S, V) = C(R, W_{R,S}, A, U; S, W_{R,S}, B, V) = I(R, W_{R,S}, A, U; S, W_{R,S}, B, V) = I(R, U; S, V)$. ■

Combining Lemmas 5, 6, and 7, and noting that the initial views $(R_0, S_0) := (0, 0)$ are trivial, we can conclude that the final views (R_n, S_n) also have a trivial distribution.

The next lemma establishes that for any δ-private protocol, if the final views have a trivial distribution, then the outputs must satisfy $C(\hat{X}; \hat{Y}) - I(\hat{X}; \hat{Y}) \leq \delta$.

Lemma 8. *Let $C(R; S) = I(R; S)$. If (ϕ, ψ) are deterministic functions such that $I(R; \psi(S)|\phi(R)) + I(S; \phi(R)|\psi(S)) \leq \delta$ then $C(\phi(R); \psi(S)) - I(\phi(R); \psi(S)) \leq \delta$.*

Proof: Let $W_{R,S}$ be the common part of (R, S). Since ϕ and ψ are deterministic functions, it follows that $\phi(R) \leftrightarrow W_{R,S} \leftrightarrow \psi(S)$ is a Markov chain. Using the property that $W_{R,S}$ is a function of R,

$$\begin{aligned} &I(W_{R,S}; \psi(S)|\phi(R)) \\ &\quad = H(\psi(S)|\phi(R)) - H(\psi(S)|\phi(R), W_{R,S}) \\ &\quad \leq H(\psi(S)|\phi(R)) - H(\psi(S)|\phi(R), R) \\ &\quad = I(R; \psi(S)|\phi(R)). \end{aligned}$$

Similarly, $I(W_{R,S}; \phi(R)|\psi(S)) \leq I(S; \phi(R)|\psi(S))$ follows. Thus, $I(W_{R,S}; \psi(S)|\phi(R)) + I(W_{R,S}; \phi(R)|\psi(S)) \leq \delta$, and hence, $C(\phi(R); \psi(S)) - I(\phi(R); \psi(S)) \leq \delta$ by Lemma 3. ■

Thus, if $P_{X,Y}$ can be securely sampled given a set of primitives that do not satisfy the completeness conditions, then for any $\epsilon, \delta > 0$ there exists $P_{\hat{X},\hat{Y}}$ such that $d(P_{\hat{X},\hat{Y}}, P_{X,Y}) \leq \epsilon$ and $C(\hat{X}; \hat{Y}) - I(\hat{X}; \hat{Y}) \leq \delta$. Finally, due to the continuity of Wyner common information (see Lemma 4) and entropy, it follows that $P_{X,Y}$ must be trivial.

B. Achievability Sketch

Due to space restrictions and since the essential techniques are well-known in the literature, we will only sketch the overall scheme for securely computing any function given a primitive satisfying the completeness conditions. Also, we aim only to describe a general but straight-forward approach to show feasibility. Of course, more complex approaches or specialized methods exploiting the structure of particular problem instances may yield more efficient schemes. The overall achievability argument follows these high-level steps:

1) Given a primitive satisfying the completeness conditions, we can construct a protocol which can simulate a source primitive $P_{U,V}$ that has a non-trivial distribution.
2) The simulated source primitive with a non-trivial distribution can be converted into a binary erasure source via the methods of [6].

3) Continuing with the methods of [6], the binary erasure source can be used to perform oblivious transfers.
4) Using the methods of [2], general secure computation can be performed via the oblivious transfers.

We further explain these steps below.

Step 1) Let $(A, B, Z) \sim P_{A,B,Z}$ be the random variables such that the primitive satisfies the completeness conditions. To simulate a source primitive (one with no inputs) with a non-trivial distribution, the parties perform the following:

- Alice generates $(A, Z) \sim P_{A,Z}$ independently from her and Bob's current views.
- Alice sends Z to Bob via error-free communication.
- Bob generates $B \sim P_{B|Z}$ that is conditionally independent from his and Alice's current views given Z. Note that, since $A \leftrightarrow Z \leftrightarrow B$ is a Markov chain, this generation procedure results in $(A, B, Z) \sim P_{A,B,Z}$.
- Alice and Bob interact via the primitive using inputs $A = f(R)$ and $B = g(S)$, and receiving outputs U and V, respectively.

This procedure results in Alice and Bob respectively holding (Z, A, U) and (Z, B, V) that have the non-trivial distribution $P_{(Z,A,U),(Z,B,V)}$ and are independent from their views prior to executing this procedure. Thus, any protocol that requires a source primitive with a non-trivial distribution can equivalently substitute the primitive $P_{U,V|A,B}$ by using this technique. Repeating this procedure generates an iid sequence of sample pairs from the non-trivial distribution $P_{(Z,A,U),(Z,B,V)}$.

Step 2) The methods of [6] require a source primitive $P_{U,V}$ with $H(\tilde{U}|\tilde{V}) > 0$ where $(\tilde{U}, \tilde{V})$ are the random variables (U, V) with redundancies removed. However, by Lemma 2, this is equivalent to requiring a source primitive with a non-trivial distribution. Due to the properties of distributions with $H(\tilde{U}|\tilde{V}) > 0$, sample pairs from this non-trivial source can be selectively discarded, leaving behind sample pairs that essentially have a binary erasure source distribution, where Alice's sample is a uniform bit and Bob's sample is either equal to Alice's or an erasure symbol (see [6] for details).

Step 3) Using these binary erasure source sample pairs, one can perform oblivious transfer, that is, to essentially simulate the primitive $P_{U,V|A,B}$ where $A := (A_0, A_1)$, $A_0, A_1, B \in \{0, 1\}$, and $(U, V) := (0, A_B)$ (see [6]). Bob first chooses two sample pairs of the binary erasure source for which there is exactly one erasure, and then instructs Alice to respectively exclusive-or her two input bits (A_0, A_1) with the two corresponding bits she has from her half of the erasure source such that the non-erased bit is aligned with the input that Bob wants (according to B). By sending the result to Bob over the error-free channel, he can recover A_B, while Alice's other bit is masked due to the erasure.

Step 4) Using the methods of [2], the ability to perform oblivious transfers can be leveraged to compute any secure computation. For approximating $P_{X,Y|Q,T}P_{Q,T}$ within any variational distance $\epsilon > 0$, the outputs $(\hat{X}, \hat{Y})$ could be computed from a boolean circuit with a uniformly random sequence of bits as input. Each party first independently generates a uniformly random sequence of bits. Using these as shares of the input sequence, the parties then apply the methods of [2] for securely evaluating the circuit to generate their respective outputs.

Note that evaluating the circuit in the last step requires a fixed number of oblivious transfers; however, the number that can actually be performed depends on the random number of binary erasure sample pairs extracted in the second step. With a protocol of fixed length (and hence fixed primitive usages), the situation of insufficient erasure samples can be handled as an error event leading to a constant output, and its effect can be made asymptotically small and hence within any ϵ approximation error. This approach also has the benefit of yielding constructions that are perfectly private ($\delta = 0$).

REFERENCES

[1] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," in *Proc. ACM Symp. on Theory of Computing*, Chicago, IL, 1988, pp. 1–10.

[2] J. Kilian, "Founding cryptography on oblivious transfer," in *Proc. ACM Symp. on Theory of Computing*, Chicago, IL, 1988, pp. 20–31.

[3] C. Crépeau and J. Kilian, "Achieving oblivious transfer using weakened security assumptions," in *Proc. IEEE Symp. on the Foundations of Computer Science*, 1988, pp. 42–52.

[4] C. Crépeau, "Efficient cryptographic protocols based on noisy channels," in *Advances in Cryptology – EUROCRYPT*, ser. Lecture Notes in Computer Science, vol. 1233. Springer-Verlag, 1997, pp. 306–317.

[5] C. Crépeau, K. Morozov, and S. Wolf, "Efficient unconditional oblivious transfer from almost any noisy channel," in *Proc. Conf. on Security in Communication Networks*, ser. Lecture Notes in Computer Science, vol. 3352. Springer-Verlag, 2004, pp. 47–59.

[6] A. Nascimento and A. Winter, "On the oblivious transfer capacity of noisy resources," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2572–2581, Jun. 2008.

[7] J. Kilian, "More general completeness theorems for secure two-party computation," in *Proc. ACM Symp. on Theory of Computing*, Portland, OR, 2000, pp. 316–324.

[8] H. Maji, M. Prabhakaran, and M. Rosulek, "A unified characterization of completeness and triviality for secure function evaluation," in *Proc. Intl. Conf. on Cryptology in India*, ser. Lecture Notes in Computer Science, vol. 7668. Springer-Verlag, 2012, pp. 40–59.

[9] Y. Wang and P. Ishwar, "On unconditionally secure multi-party sampling from scratch," in *Proc. IEEE Intl. Symp. on Information Theory*, Saint Petersburg, Russia, Jun. 2011.

[10] A. Wyner, "The common information of two dependent random variables," *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 163–179, Mar. 1975.

[11] 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.

[12] R. Ahlswede and J. Körner, "On common information and related characteristics of correlated information sources," in *Proc. Prague Conf. on Information Theory*, 1974.

[13] V. Prabhakaran and M. Prabhakaran, "Assisted common information with an application to secure two-party sampling," *to appear in IEEE Transactions on Information Theory*, available at arxiv.org/abs/1206.1282.

[14] Z. Zhang, "Estimating mutual information via Kolmogorov distance," *IEEE Transactions on Information Theory*, vol. 53, no. 7, pp. 3280–3282, Sep. 2007.

[15] S. Wolf and J. Wullschleger, "New monotones and lower bounds in unconditional two-party computation," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2792–2797, Jun. 2008.