Information-Theoretically Secure Three-party Computation with One Active Adversary

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

TR2012-045 June 2012

Abstract

A special three-party secure computation problem is studied in which one of three pairwise interacting parties is required to compute a function of the sequences held by the other two when one of the three parties may arbitrarily deviate from the computation protocol (active behavioral model). For this problem, information-theoretic conditions for secure computation are developed within the real versus ideal model simulation paradigm. Conditions for the passive behavioral model are also provided. A pure one-time-pad based protocol for securely computing the Hamming distance between binary sequences is developed and is shown, using the information-theoretic security conditions, to be secure under both the active and passive behavioral models. In contrast, the general techniques of [1] and [2] require at least four parties when dealing with the active behavioral model. In particular, for the three-party problem considered herein, the BGW protocol that securely computes the squared l2 distance between sequences under the passive behavioral model is demonstrated to be insecure under the active behavioral model, even for binary sequences when the squared l2 distance coincides with the Hamming distance.

Cornell University Library

Information-Theoretically Secure Three-Party Computation with One Active Adversary

Ye Wang, *Member, IEEE,* Prakash Ishwar, *Senior Member, IEEE,* Shantanu Rane, *Member, IEEE*

Abstract

A special three-party secure computation problem is studied in which one of three pairwise interacting parties is required to compute a function of the sequences held by the other two when one of the three parties may arbitrarily deviate from the computation protocol (active behavioral model). For this problem, information-theoretic conditions for secure computation are developed within the real versus ideal model simulation paradigm. Conditions for the passive behavioral model are also provided. A pure one-time-pad based protocol for securely computing the Hamming distance between binary sequences is developed and is shown, using the information-theoretic security conditions, to be secure under both the active and passive behavioral models. In contrast, the general techniques of [1] and [2] require at least four parties when dealing with the active behavioral model. In particular, for the three-party problem considered herein, the BGW protocol that securely computes the squared ℓ_2 distance between sequences under the passive behavioral model is demonstrated to be insecure under the active behavioral model, even for binary sequences when the squared ℓ_2 distance coincides with the Hamming distance.

Index Terms

Secure Multiparty Computation, Active Adversaries, Ideal/Real Models, Information-Theoretic Privacy, Hamming Distance, Quadratic Distance, BGW Protocol.

I. Introduction

We consider a special secure three-party computation problem under the active behavioral model for adversaries. In our problem setup, Alice has a sequence of random variables $X^n := X_1, \ldots, X_n$, with $X_i \in \mathcal{X}$, Bob has a sequence of random variables $Y^n := Y_1, \ldots, Y_n$, with $Y_i \in \mathcal{Y}$, and Charlie wants to compute a function $f(X^n, Y^n)$. The objective is to construct protocols that securely compute $f(X^n, Y^n)$ under the active behavioral model where one of the parties may arbitrarily deviate from the protocol.

The formulation of security for the active behavioral model requires careful consideration of the notions of correctness and privacy due to the possibility that a party may arbitrarily deviate from the protocol. Of course, a party can always corrupt the computation by simply changing its input data. This, however, cannot be considered as a security-weakness since such an attack can also be mounted against a trusted genie that facilitates the computation by receiving all inputs, performing all computations, and delivering the results to the designated parties. A deviating party's ability to influence the computation should, ideally, not exceed what could be done against a trusted genie. Therefore, in the active behavioral model a protocol is said to be secure if it adequately *simulates* the presence of a trusted genie that facilitates the computation. This is made precise through the real versus ideal model simulation paradigm for secure multiparty computation [3]. In contrast, in the passive behavioral model, where it is assumed that all parties will adhere to the protocol, to assess the security of a protocol, one only needs to check that the protocol correctly computes the function while revealing no more information than what can be inherently inferred from the result of the computation.

A motivating application for our special three-party computation problem is secure, privacy-preserving authentication amongst three parties. In this application, Alice wishes to authenticate herself to Charlie, and Bob is an authentication authority holding a registered biometric measurement. Alice should be authenticated if the biometric that she produces (her sequence X^n which represent features extracted from a sensor measurement) is sufficiently close (with respect to an appropriate distance measure represented by $f(X^n, Y^n)$) to the registered biometric held by Bob (his sequence Y^n). However, the authentication process should be performed privately, ensuring that no

Y. Wang and P. Ishwar are with the Department of Electrical and Computer Engineering, Boston Unversity, Boston, MA, 02215 USA e-mail: {yw,pi}@bu.edu.

S. Rane are with the Mitsubish Electric Research Laboratories, Cambridge, MA 02139 USA e-mail: rane@merl.com.

information is revealed between Alice and Bob, and that Charlie only learns how close Alice's biometric is to the registered one held by Bob. Consideration of the active behavioral model is relevant in this application since an unauthorized and malicious Alice may attempt to deviate from the protocol in order to increase her chances of being falsely authenticated by attempting to influence the computation output produced by Charlie or to learn some information about Bob's sequence.

We make three contributions in this work:

(i) For our three-party computation problem with one active adversary, in Section II we develop information-theoretic security conditions that are equivalent to the security definition based on the real versus ideal model simulation paradigm [3]. This may be viewed as extending the results in [4] from two to three parties. We also provide information-theoretic security conditions for passive parties.

(ii) In Section III we develop a pure one-time-pad based protocol **HamDist** for securely computing the Hamming distance between binary sequences:

$$\mathcal{X} = \mathcal{Y} = \{0, 1\}, \quad f(X^n, Y^n) = \sum_{i=1}^{n} (X_i \oplus Y_i),$$

where $\oplus$ denotes binary exclusive-or. We show that **HamDist** is secure under both the active and the passive behavioral models using the corresponding information-theoretic security conditions from Section II. This is interesting because under the active behavioral model, even with only up to one corrupt party, not all functions can be securely computed. Moreover, the general active party techniques of [1] and [2] are not applicable to our problem because they require at least four parties under the active behavioral model.

(iii) In Section IV we show that the **BGW** protocol for computing the quadratic distance (squared ℓ_2 norm)[1] between integer sequences,

$$\mathcal{X} = \mathcal{Y} = \mathbb{Z}_s, \quad f(X^n, Y^n) = \sum_{i=1}^{n} (X_i - Y_i)^2,$$

where $\mathbb{Z}_s = \{0, 1, \ldots, s-1\}$, is not secure under the active behavioral model. We leave open the question whether there exists any three-party protocol for computing the quadratic distance under the active behavioral model.

II. Information-Theoretic Conditions for Security Against One Active Party

In this section, we will first provide an overview of the real versus ideal model simulation paradigm for secure computation and then state and prove information-theoretic conditions for our secure computation problem for the active behavioral model. We also state information-theoretic conditions for secure computation under the passive behavioral model. For convenience, we will denote the sequences X^n and Y^n by X and Y respectively.

A. Real versus Ideal Model Simulation Paradigm for Secure Three-Party Computation

A protocol Π for three-party computation is a triple of algorithms (A, B, C) that are intended to be executed by Alice, Bob, and Charlie respectively. Each algorithm is a set of instructions that are intended to be executed by its respective party. This includes instructions for processing inputs (X for Alice and Y for Bob), generating local randomness, performing intermediate local computations, sending messages to and receiving and processing messages from other parties, and producing local outputs. The outputs produced by Alice, Bob, and Charlie will be denoted by U, V, and W respectively. A protocol Π is regarded as the "real model" for three-party computation and is illustrated in Figure 1(a).

In the "ideal model" for three-party computation, in addition to the three parties, there is a fourth party: a trusted genie that facilitates the computation. An ideal model protocol $\overline{\Pi}_I$ for three-party computation is a triple of algorithms $(\overline{A}_I, \overline{B}_I, \overline{C}_I)$ that have a very specific structure. Alice's algorithm $\overline{A}_I$ consists solely of an independent random functionality that takes as an input only X and outputs U_I and $\overline{X}_I$, and can be modeled as a conditional distribution $P_{U_I, \overline{X}_I | X}$. Likewise, Bob's algorithm $\overline{B}_I$ is an independent random functionality that takes as an input

[1]The Hamming distance coincides with the quadratic distance for binary sequences.

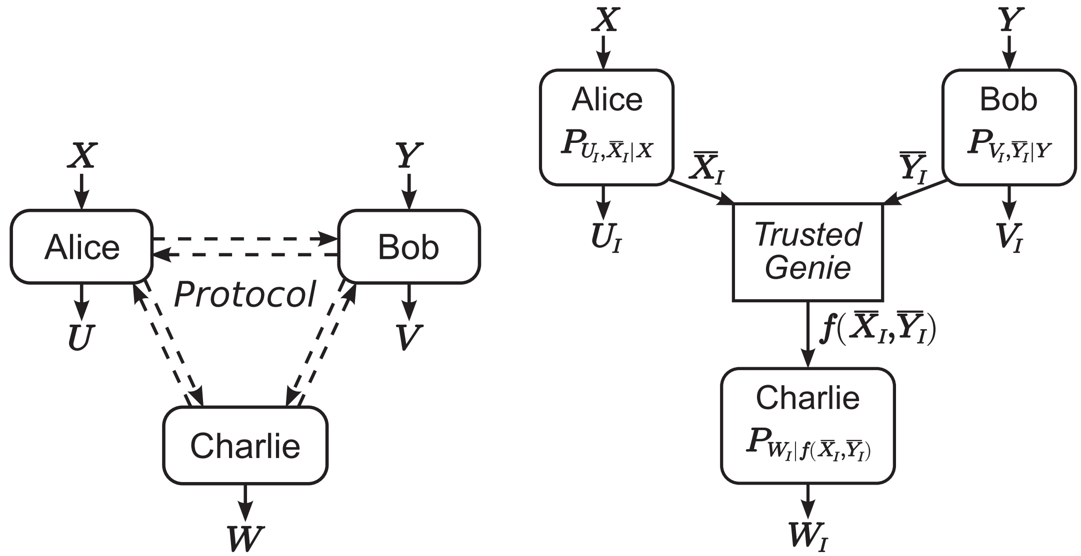

Fig. 1. A protocol is secure if any attack against it in the real model (a) can be equivalently mounted against the trusted genie in the ideal model (b).

only Y and outputs V_I and $\overline{Y}_I$, and can be modeled as a conditional distribution $P_{V_I,\overline{Y}_I|Y}$. The random variables $\overline{X}_I$ and $\overline{Y}_I$ represent the inputs that Alice and Bob give to the trusted genie, and U_I and V_I respectively represent Alice and Bob's outputs. The trusted genie receives $(\overline{X}_I,\overline{Y}_I)$ from Alice and Bob, computes $f(\overline{X}_I,\overline{Y}_I)$ and sends this to Charlie. If either Alice or Bob refuse to send their input to the trusted genie or send an invalid input, e.g., inputs not belonging to the proper alphabets $\mathcal{X}$ or $\mathcal{Y}$, then the genie will assume a default input. Charlie's algorithm $\overline{C}_I$ is a random functionality that takes $f(\overline{X}_I,\overline{Y}_I)$ as input and produces W_I as output, and can be modeled as a conditional distribution $P_{W_I|f(\overline{X}_I,\overline{Y}_I)}$. The ideal model for three-party computation and is illustrated in Figure 1(b).

Definition 1 (Honest Ideal Model Protocol): The ideal model protocol $\Pi_I = (A_I, B_I, C_I)$ is called "honest" if Alice's and Bob's outputs are null, the inputs to the trusted genie are Alice's and Bob's inputs, and Charlie's output is the input that he receives from the trusted genie. Specifically,

$$U_I = V_I = \emptyset, \overline{X}_I = X, \overline{Y}_I = Y, W_I = f(\overline{X}_I,\overline{Y}_I) = f(X,Y).$$

In our problem, at most one party may actively deviate from the protocol, and no collusions form between any parties. This motivates the following definition that captures the active behavioral model of interest.

Definition 2 (Admissible Deviation): A protocol $\overline{\Pi} = (\overline{A},\overline{B},\overline{C})$ is an admissible deviation of $\Pi = (A,B,C)$ if at most one of $(\overline{A},\overline{B},\overline{C})$ differs from (A,B,C).

In the real versus ideal model simulation paradigm, a real model protocol is considered to be secure if it can adequately simulate the presence of the trusted genie in the ideal model. Specifically, a real model protocol is secure if it can be shown that for every attack against the protocol – captured through the above notion of an admissible deviation of a protocol – a statistically equivalent attack can be mounted against the honest ideal model protocol in the ideal model. The following definition makes precise this notion of security under the active behavioral model.

Definition 3 (Security Against Active Behavior): A three-party protocol $\Pi = (A,B,C)$ securely computes $f(X,Y)$ under the active behavioral model if, for every real model protocol $\overline{\Pi} = (\overline{A},\overline{B},\overline{C})$ that is an admissible deviation of Π and for any distribution $P_{X,Y}$ on inputs $(X,Y) \sim P_{X,Y}$, there exists an ideal model protocol $\overline{\Pi}_I = (\overline{A}_I,\overline{B}_I,\overline{C}_I)$ that is an admissible deviation of the honest ideal model protocol $\Pi_I = (A_I,B_I,C_I)$, where the same players are honest, such that

$$P_{U,V,W|X,Y} = P_{U_I,V_I,W_I|X,Y}, \tag{1}$$

where (U, V, W) are the outputs of the protocol $\overline{\Pi}$ in the real model with inputs (X, Y) and (U_I, V_I, W_I) are the outputs of the protocol $\overline{\Pi}_I$ in the ideal model with inputs (X, Y).

Contained within the above definition of security is the requirement that a secure protocol must ensure that Charlie will correctly compute the function if none of the parties deviate from the protocol. This correctness condition is captured since no deviation is an admissible deviation and corresponds to the honest ideal model protocol, which results in the correct computation of the function. Privacy requirements against a deviating party are also contained within this security definition, since the deviating party may include arbitrary additional information in its output. The above security definition prevents this additional output information from containing any information that could not be obtained by the party deviating in the ideal model.

B. Active Behavior Security Characterization via Information-Theoretic Conditions

In the following theorem we establish information-theoretic conditions that are equivalent to the security conditions for the active behavioral model given by Definition 3. These conditions provide a way to test whether a given protocol is secure under the active behavioral model directly in the real model without explicit reference to an ideal model or a trusted genie. In contrast, Definition 3 needs to refer to an ideal model to establish security against active adversarial behavior.

Theorem 1: A real-model three-party protocol $\Pi = (A, B, C)$ securely computes $f(X, Y)$ under the active behavioral model if, and only if, for every real model protocol $\overline{\Pi} = (\overline{A}, \overline{B}, \overline{C})$ that is an admissible deviation of Π and for any distribution $P_{X,Y}$ on inputs $(X, Y) \sim P_{X,Y}$, the algorithms $(\overline{A}, \overline{B}, \overline{C})$ respectively produce outputs (U, V, W), such that the following conditions are satisfied:

- *(Correctness)* If none of the players deviate from the protocol, that is $\overline{\Pi} = \Pi$, then Charlie's output W satisfies
$$\Pr[(U, V, W) = (\emptyset, \emptyset, f(X, Y))] = 1.$$
- *(Security against Alice)* If Bob and Charlie follow the protocol, that is $(B, C) = (\overline{B}, \overline{C})$, then there exists random variable $\overline{X}$ such that
$$I(U, \overline{X}; Y|X) = 0, \tag{2}$$
$$\Pr[(V, W) = (\emptyset, f(\overline{X}, Y))] = 1. \tag{3}$$
- *(Security against Bob)* If Alice and Charlie follow the protocol, that is $(A, C) = (\overline{A}, \overline{C})$, then there exists random variable $\overline{Y}$ such that
$$I(V, \overline{Y}; X|Y) = 0, \tag{4}$$
$$\Pr[(U, W) = (\emptyset, f(X, \overline{Y}))] = 1. \tag{5}$$
- *(Security against Charlie)* If Alice and Bob follow the protocol, that is $(A, B) = (\overline{A}, \overline{B})$, then
$$I(W; X, Y|f(X, Y)) = 0, \tag{6}$$
$$\Pr[(U, V) = (\emptyset, \emptyset)] = 1. \tag{7}$$

Proof: In order to prove the equivalence of the information-theoretic conditions with respect to the ideal vs real model definition, we must show that the conditions are both necessary and sufficient.

(Necessity) First, we show that the conditions are necessary, that is, if the protocol Π securely computes $f(X, Y)$ then the information-theoretic conditions must hold. Consider any real model protocol $\overline{\Pi} = (\overline{A}, \overline{B}, \overline{C})$ that is an admissible deviation of Π. Since the protocol is secure, there must exist an ideal model protocol $\overline{\Pi}_I = (\overline{A}_I, \overline{B}_I, \overline{C}_I)$ that is an admissible deviation of the honest ideal model protocol $\Pi_I = (A_I, B_I, C_I)$, where the same players are honest, such that
$$P_{U,V,W|X,Y} = P_{U_I,V_I,W_I|X,Y},$$
where (U, V, W) are the outputs of the protocol $\overline{\Pi}$ in the real model with inputs (X, Y) and (U_I, V_I, W_I) are the outputs of the protocol $\overline{\Pi}_I$ in the ideal model with inputs (X, Y).

In the case that all of the players are honest, that is $\overline{\Pi} = \Pi$, then the corresponding ideal model protocol $\overline{\Pi}_I$ is the same as Π_I, and thus the ideal model outputs U_I and V_I are null and $W_I = f(X,Y)$ with probability one. Since $P_{U,V,W|X,Y} = P_{U_I,V_I,W_I|X,Y}$, we have that

$$\Pr[(U,V,W) = (\emptyset,\emptyset,f(X,Y))] = 1.$$

Now we consider the case that Alice is dishonest and Bob and Charlie are honest. In the ideal model, we have that

$$I(U_I,\overline{X}_I;Y|X) = 0,$$

since U_I and $\overline{X}_I$ are generated only from X, and also by the structure of the ideal model and the honesty of Bob and Charlie,

$$\Pr[W_I = f(\overline{X}_I,Y)] = 1,$$

while V_I is null. Since $P_{U,V,W|X,Y} = P_{U_I,V_I,W_I|X,Y}$, we have that V is identically distributed as V_I and hence is also null, and we can define random variable $\overline{X}$ that is distributed according to

$$P_{\overline{X}|X,Y,U,V,W} := P_{\overline{X}_I|X,Y,U_I,V_I,W_I},$$

such that

$$I(U,\overline{X};Y|X) = 0,$$

and

$$\Pr[W = f(\overline{X},Y)] = 1.$$

The argument for the case that Bob is dishonest is symmetric to the case of a dishonest Alice. This leaves the case for the when Charlie is dishonest. In the ideal model, Charlie's output satisfies

$$I(W_I;X,Y|f(X,Y)) = 0,$$

since W_I is only generated from $f(X_I,Y_I)$, and that $(X_I,Y_I) = (X,Y)$, since Alice and Bob are honest. Also, since Alice and Bob are honest, their outputs U_I and V_I are null. Since $P_{U,V,W|X,Y} = P_{U_I,V_I,W_I|X,Y}$, we must also have that

$$\begin{aligned} I(W;X,Y|f(X,Y)) &= 0, \\ \Pr[(U,V) = (\emptyset,\emptyset)] &= 1. \end{aligned}$$

(Sufficiency) Now, we must show that the conditions are sufficient, that is, if the information-theoretic conditions hold then the protocol is secure. Consider any real model protocol $\overline{\Pi} = (\overline{A},\overline{B},\overline{C})$ that is an admissible deviation of Π and assume that the information theoretic conditions hold. We must now construct an ideal model protocol $\overline{\Pi}_I = (\overline{A}_I,\overline{B}_I,\overline{C}_I)$ that is an admissible deviation of the honest ideal model protocol $\Pi_I = (A_I,B_I,C_I)$, where the same players are honest, such that

$$P_{U,V,W|X,Y} = P_{U_I,V_I,W_I|X,Y},$$

where (U,V,W) are the outputs of the protocol $\overline{\Pi}$ in the real model with inputs (X,Y) and (U_I,V_I,W_I) are the outputs of the protocol $\overline{\Pi}_I$ in the ideal model with inputs (X,Y).

In the case that all of the players are honest, the information theoretic conditions state that U and V are null and that $W = f(X,Y)$ with probability one. The honest ideal model protocol also produces null outputs for Alice and Bob, that is U_I and V_I are null, and Charlie's output $W_I = f(X,Y)$. Thus, we have that

$$P_{U,V,W|X,Y} = P_{U_I,V_I,W_I|X,Y}.$$

In the case that Alice is dishonest, we must construct an ideal model protocol, with an honest Bob and Charlie, that produce statistically equivalent outputs. Let Alice's ideal model algorithm $\overline{A}_I$ be defined by the conditional distribution

$$P_{U_I,\overline{X}_I|X} := P_{U,\overline{X}|X},$$

which governs how Alice generates U_I and $\overline{X}_I$ based on only X. Since Bob and Charlie are honest, that is $\overline{B}_I = B_I$ and $\overline{C}_I = C_I$, with probability one their outputs are given by

$$V_I = \emptyset \text{ and } W_I = f(\overline{X}_I, Y).$$

Considering the conditional distribution of U_I and W_I given X and Y, we have that

$$\begin{aligned} P_{U_I,W_I|X,Y} &= \sum_{\overline{x}} P_{U_I,W_I,\overline{X}_I|X,Y} \\ &= \sum_{\overline{x}} P_{U_I,\overline{X}_I|X,Y} P_{W_I|X,Y,U_I,\overline{X}_I} \\ &= \sum_{\overline{x}} P_{U_I,\overline{X}_I|X} P_{W_I|Y,\overline{X}_I}, \end{aligned}$$

since U_I and $\overline{X}_I$ are only generated from X and $W_I = f(\overline{X}_I, Y)$, and hence

$$P_{W_I|Y,\overline{X}_I}(w|y,\overline{x}) = \mathbf{1}_{\{f(\overline{x},y)\}}(w) = \begin{cases} 1, & \text{if } w = f(\overline{x}, y), \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

Likewise, we can manipulate the conditional distribution of U and W given X and Y, using the conditions given by (2) and (3),

$$\begin{aligned} P_{U,W|X,Y} &= \sum_{\overline{x}} P_{U,W,\overline{X}|X,Y} \\ &= \sum_{\overline{x}} P_{U,\overline{X}|X,Y} P_{W|X,Y,U,\overline{X}} \\ &= \sum_{\overline{x}} P_{U,\overline{X}|X} P_{W|Y,\overline{X}}. \end{aligned}$$

Since $P_{U_I,\overline{X}_I|X} = P_{U,\overline{X}|X}$ by design and $P_{W|Y,\overline{X}} = P_{W_I|Y,\overline{X}_I}$ due to (3) and (8), we have that $P_{U,W|X,Y} = P_{U_I,W_I|X,Y}$. Since both V_I and V are null, we have that $P_{U,V,W|X,Y} = P_{U_I,V_I,W_I|X,Y}$.

The argument for the case that Bob is dishonest is symmetric to the case of a dishonest Alice. This leaves the case for the when Charlie is dishonest. Let Charlie's ideal model algorithm $\overline{C}_I$ be defined by the following conditional distribution that governs how Charlie generates W_I based on only $f(\overline{X}_I, \overline{Y}_I)$

$$P_{W_I|f(\overline{X}_I,\overline{Y}_I)} := P_{W|f(X,Y)} = P_{W|f(X,Y),X,Y},$$

due to the (7). Note that since Alice and Bob are honest, $(\overline{X}_I, \overline{Y}_I) = (X, Y)$, and U_I and V_I are null. Considering the conditional distribution of W_I given X, Y,

$$\begin{aligned} P_{W_I|X,Y} &= \sum_{f} P_{W_I,f(\overline{X}_I,\overline{Y}_I)|X,Y} \\ &= \sum_{f} P_{W_I|f(\overline{X}_I,\overline{Y}_I),X,Y} P_{f(\overline{X}_I,\overline{Y}_I)|X,Y} \\ &= \sum_{f} P_{W_I|f(\overline{X}_I,\overline{Y}_I)} P_{f(X,Y)|X,Y} \\ &= \sum_{f} P_{W|f(X,Y),X,Y} P_{f(X,Y)|X,Y} \\ &= \sum_{f} P_{W,f(X,Y)|X,Y} = P_{W|X,Y}. \end{aligned}$$

Thus since $P_{W|X,Y} = P_{W_I|X,Y}$ and both (U, V) and (U_I, V_I) are null, we have that $P_{U,V,W|X,Y} = P_{U_I,V_I,W_I|X,Y}$.

■

C. Passive Behavioral Model

When all parties correctly follow a protocol, they are said to be behaving passively. When parties are passive, they may still attempt to learn as much new information as they can from the messages that they receive from other parties during the execution of the protocol. Hence, the passive behavioral model is also referred to as the "honest-but-curious" model. A protocol is secure against passive behavior if it produces correct computation results and reveals no more information to any party than what any party can infer from its own inputs and its own computation results. Thus, security against passive behavior is a statement about the correctness and the information leakage properties of a protocol. In contrast to the security definition for the active behavioral model, security under the passive behavioral model can be directly stated in terms of information-theoretic conditions as follows.

Definition 4 (Security Against Passive Behavior): A three-party protocol $\Pi = (A, B, C)$ securely computes $f(X, Y)$ under the passive behavioral model (with no collusions) if after Alice, Bob, and Charlie execute the protocol, the following conditions are satisfied:

- *(Correctness)* Charlie correctly computes the function and Alice and Bob output nothing, that is,

$$\Pr[(U, V, W) = (\emptyset, \emptyset, f(X, Y))] = 1.$$

- *(Privacy against Alice)* The view of Alice, denoted by M_1 and consisting of all of the local randomness generated, local computation performed, and messages sent and received by Alice, does not reveal any more information about Bob's input Y and Charlie's output $f(X, Y)$ other than what can be inferred from her input X, that is,

$$I(M_1; Y, f(X, Y)|X) = 0.$$

- *(Privacy against Bob)* The view of Bob, denoted by M_2 and consisting of all of the local randomness generated, local computation performed, and messages sent and received by Bob, does not reveal any more information about Alice's input X and Charlie's output $f(X, Y)$ other than what can be inferred from his input Y, that is,

$$I(M_2; X, f(X, Y)|Y) = 0.$$

- *(Privacy against Charlie)* The view of Charlie, denoted by M_3 and consisting of all of the local randomness generated, local computation performed, and messages sent and received by Charlie, does not reveal any more information about Alice and Bob's inputs (X, Y) other than what can be inferred from his output $f(X, Y)$, that is,

$$I(M_3; X, Y|f(X, Y)) = 0.$$

In general, security of a protocol under the active behavioral model does not necessarily imply security of a protocol under the passive behavioral model [5]. This may seem counterintuitive at first since possible attacks by active parties are surely expected to subsume the possible "passive attacks". This can be resolved by observing that the definition of security under the active behavioral model compares admissible deviations (active attacks) in the real model to possible active attacks in the ideal model. This comparison to a benchmark involving active attacks in the ideal model potentially results in more permissive privacy conditions than the information leakage conditions required in the passive behavioral model. To illustrate this difference, consider the following two-party example (from [5]): Alice and Bob each have a bit and Bob wishes to compute the Boolean AND of the bits, while Alice computes nothing. A protocol where Alice simply gives Bob her bit and he computes his desired function is clearly insecure under the passive behavioral model since Alice directly reveals her bit, whereas the AND function should only reveal her bit if Bob's bit is one. However, this protocol would be secure in the active behavioral model since a deviating Bob, in the ideal model, could change his input to one to always reveal the value of Alice's bit from the trusted genie in the ideal model.

III. A Secure Protocol for Hamming Distance

In this section, we present and analyze a pure one-time-pad based protocol **HamDist** that securely computes the Hamming distance for binary sequences under both the passive and the active behavioral models. The security of this protocol will be proved using the information-theoretic conditions for security under the active behavioral model from Theorem 1 and the information theoretic conditions for security under the passive behavioral model in Definition 4.

Protocol **HamDist**:

1) Alice randomly generates the binary string $R_1, \ldots, R_n \sim$ iid Bernoulli$(1/2)$ and independently of (X^n, Y^n). Alice also randomly chooses π, a permutation of $\{1, \ldots, n\}$, uniformly and independently of (X^n, Y^n, R^n).
2) Alice sends R^n and π to Bob.
3) Alice sends $\pi(X^n \oplus R^n)$ to Charlie, where $X^n \oplus R^n$ denotes the bitwise exclusive-or of the binary strings X^n and R^n and $\pi(\cdot)$ denotes the application of the permutation π.
4) Bob computes and sends $\pi(Y^n \oplus R^n)$ to Charlie.
5) Charlie combines the messages from Alice and Bob to obtain
$$\pi(X^n \oplus Y^n) = \pi(X^n \oplus R^n) \oplus \pi(Y^n \oplus R^n),$$
and outputs the Hamming weight of the vector $\pi(X^n \oplus Y^n)$.
6) Alice and Bob do not produce outputs.

During the execution of the protocol, if any party fails to send a message or sends a malformed message to another party, a default message is assumed by the receiving party. Also, any extraneous messages are simply ignored. For example, in second step, Bob expects to receive an n-bit binary string and a permutation of $\{1, \ldots, n\}$ from Alice. If Alice does not send a message or sends a malformed binary string, then Bob interprets it as if Alice sent the all-zero binary string. If Alice does not send a message or sends an invalid permutation, then Bob interprets it as if Alice sent the identity permutation $(1, \ldots, n)$. Likewise, in other parts of the protocol, a malformed or missing binary string is interpreted as the all-zero binary string. The specific default message assumed in the case of invalid or unsent messages is unimportant and could be replaced with any other fixed message.

Before we prove that the **HamDist** protocol is secure in the active behavioral model, we first establish two lemmas that will be used in the proof.

Lemma 1: For random variables A, B, X, Y, the Markov chain $A - B - (X, Y)$ holds if and only if the Markov chains $A - B - X$ and $A - (B, X) - Y$ (or by symmetry $A - B - Y$ and $A - (B, Y) - X$) both hold.

Proof: The lemma follows from following identity
$$I(A; X, Y|B) = I(A; X|B) + I(A; Y|B, X),$$
since the conditional mutual information on the left hand side is equal to zero if and only if the Markov chain $A - B - (X, Y)$ holds, and the conditional mutual informations on the right hand side are equal to zero if and only if the Markov chains $A - B - X$ and $A - (B, X) - Y$ both hold. ■

Lemma 2: If the random variables A, B, X, Y satisfy the Markov chains $A - B - X$ and $A - (B, X) - Y$, then $A - B - Y$ also forms a Markov chain.

Proof: The given Markov chains imply, by Lemma 1, that $A - B - (X, Y)$ forms a Markov chain, which also implies, by symmetry, that $A - B - Y$ forms a Markov chain. ■

Theorem 2: Protocol **HamDist** is secure under the active behavioral model for any distribution P_{X^n, Y^n}.

Proof: (Correctness) The protocol is correct since the Hamming weight of any permutation of the vector $X^n \oplus Y^n$ is the Hamming distance between X^n and Y^n. Hence,
$$\Pr[W = f(X^n, Y^n)] = 1.$$
Also, Alice and Bob produce null outputs as specified by the protocol.

Since any unsent or invalid messages are interpreted by the receiver as some default message as described earlier, we can assume, without loss of generality, that the arbitrarily modified algorithms send well-formed messages belonging to the appropriate message alphabet.

(Security against Alice) Let $B_A \in \{0,1\}^n$ denote the n-bit string (corresponding to R^n) and $\overline{\pi} \in \mathcal{P}(\{1,\ldots,n\})$ denote the permutation of $\{1,\ldots,n\}$ that Alice sends to Bob. Let $C_A \in \{0,1\}^n$ denote the n-bit string that Alice sends to Charlie. Let $\overline{X}^n = B_A \oplus \overline{\pi}^{-1}(C_A)$, where $\overline{\pi}^{-1}(\cdot)$ denotes the inverse application of the permutation $\overline{\pi}$.

Since Alice does not receive any messages, B_A, C_A, $\overline{\pi}$, and U can only be generated from X^n and since $\overline{X}^n$ is a function of B_A, C_A and $\overline{\pi}$, we have that $Y^n - X^n - (B_A, C_A, \overline{\pi}, U) - (\overline{X}^n, U)$ forms a Markov chain, hence

$$I(U, \overline{X}^n; Y^n | X^n) = 0.$$

Since Bob and Charlie are following the protocol, the messages from Alice and Bob's input Y^n are ultimately combined by Charlie to form the vector

$$\overline{\pi}(Y^n \oplus B_A) \oplus C_A = \overline{\pi}(Y^n \oplus B_A) \oplus \overline{\pi}(\overline{X}^n \oplus B_A) = \overline{\pi}(Y^n \oplus \overline{X}^n),$$

from which he computes the Hamming weight to produce his output $W = f(\overline{X}^n, Y^n)$. Bob, following the protocol, does not produce an output, hence V is null.

(Security against Bob) Bob receives the random binary string R^n and random permutation π from Alice. Let $C_B \in \{0,1\}^n$ denote the n-bit string that Bob sends to Charlie. Let $\overline{Y}^n = \pi^{-1}(C_B) \oplus R^n$.

The message C_B can only be generated from R^n, π, and Y^n, thus $C_B - (R^n, \pi, Y^n) - X^n$ forms a Markov chain. Since (R^n, π) is independent of (X^n, Y^n), we have that $(R^n, \pi) - Y^n - X^n$ trivially forms a Markov chain. These two Markov chains imply that $(C_B, R^n, \pi) - Y^n - X^n$ forms a Markov chain by Lemma 1. Since $\overline{Y}^n$ is a function of (C_B, R^n, π) and V can only be generated from Y^n, R^n, π, C_B, and $\overline{Y}^n$, we have that $(V, \overline{Y}^n) - (C_B, R^n, \pi, Y^n) - Y^n - X^n$ forms a Markov chain, hence

$$I(V, \overline{Y}^n; X^n | Y^n) = 0.$$

Since Alice and Charlie are following the protocol, the message from Bob and Alice's input X^n are ultimately combined by Charlie to form the vector

$$\pi(X^n \oplus R^n) \oplus C_B = \pi(X^n \oplus R^n) \oplus \pi(\overline{Y}^n \oplus R^n) = \pi(X^n \oplus \overline{Y}^n),$$

from which he computes the Hamming weight to produce his output $W = f(X^n, \overline{Y}^n)$. Alice, following the protocol, does not produce an output, hence U is null.

(Security against Charlie) Charlie receives $\pi(X^n \oplus R^n)$ from Alice and $\pi(Y^n \oplus R^n)$ from Bob. Charlie's output W can only be generated from $\pi(X^n \oplus R^n)$ and $\pi(Y^n \oplus R^n)$ thus $W - (\pi(X^n \oplus R^n), \pi(Y^n \oplus R^n)) - (X^n, Y^n)$ forms a Markov chain. Since $\pi(X^n \oplus Y^n)$ and $f(X^n, Y^n)$ are functions of $\pi(X^n \oplus R^n)$ and $\pi(Y^n \oplus R^n)$, we have that

$$(X^n, Y^n) - (\pi(X^n \oplus R^n), \pi(Y^n \oplus R^n), \pi(X^n \oplus Y^n), f(X^n, Y^n)) - W \tag{9}$$

also forms a Markov chain. The Markov chain

$$(X^n, Y^n) - f(X^n, Y^n) - (\pi(X^n \oplus R^n), \pi(Y^n \oplus R^n), \pi(X^n \oplus Y^n)) \tag{10}$$

holds due to the following

$$\begin{aligned}
&I(\pi(X^n \oplus R^n), \pi(Y^n \oplus R^n), \pi(X^n \oplus Y^n); X^n, Y^n | f(X^n, Y^n)) \\
&\overset{(a)}{=} I(\pi(X^n \oplus Y^n), \pi(Y^n \oplus R^n); X^n, Y^n | f(X^n, Y^n)) && (11) \\
&\overset{(b)}{=} H(X^n, Y^n | f(X^n, Y^n)) && (12) \\
&\quad - H(X^n, Y^n | \pi(X^n \oplus Y^n), \pi(Y^n \oplus R^n), f(X^n, Y^n)) \\
&\overset{(c)}{=} H(X^n, Y^n | f(X^n, Y^n)) && (13) \\
&\quad - H(X^n, Y^n | \pi(X^n \oplus Y^n), f(X^n, Y^n)) \\
&\overset{(d)}{=} H(X^n, Y^n | f(X^n, Y^n)) - H(X^n, Y^n | f(X^n, Y^n)) = 0,
\end{aligned}$$

where (a) holds since $\pi(X^n \oplus R^n)$ is a function of $\pi(X^n \oplus Y^n)$ and $\pi(Y^n \oplus R^n)$, (b) is by the definition of conditional mutual information, (c) is due to the independence of R^n, and (d) holds since the random permutation of the XOR of the sequences does not reveal any more information about the sequences than the Hamming distance. Thus, by Lemma 2 and the Markov chains in (9) and (10), we have that $(X^n, Y^n) - f(X^n, Y^n) - W$ forms a Markov chain, and hence

$$I(W; X^n, Y^n | f(X^n, Y^n)) = 0.$$

Also, since Alice and Bob follow the protocol, their outputs, U and V, are null. ■

As previously discussed, security of a protocol under the active behavioral model does not necessarily imply security of a protocol under the passive behavioral model [5]. Thus, we must also show the the **HamDist** protocol is secure in the passive behavioral model.

Theorem 3: Protocol **HamDist** is secure under the passive behavioral model for any distribution P_{X^n,Y^n}.

Proof: (Correctness) The protocol is correct according to the same argument as for the active behavioral model.

(Privacy against Alice) The protocol is private against Alice since she does not even receive any messages and hence no information from other parties. Formally,

$$\begin{aligned} &I(M_1; Y^n, f(X^n, Y^n)|X^n) \\ &\quad = I(\pi, R^n, \pi(X^n \oplus R^n); Y^n, f(X^n, Y^n)|X^n) \\ &\quad = I(\pi, R^n; Y^n, f(X^n, Y^n)|X^n) = 0, \end{aligned}$$

since $\pi(X^n \oplus R^n)$ is a function of (π, R^n, X^n), and (π, R^n) are independent of X^n and Y^n.

(Privacy against Bob) The protocol is private against Bob since the only message from Alice that he receives are independent of X^n, Y^n, W. Formally,

$$\begin{aligned} &I(M_2; X^n, f(X^n, Y^n)|Y^n) \\ &\quad = I(\pi, R^n, \pi(Y^n) \oplus R^n; X^n, f(X^n, Y^n)|Y^n) \\ &\quad = I(\pi, R^n; X^n, f(X^n, Y^n)|Y^n) = 0, \end{aligned}$$

since π, R^n are independent of X^n and Y^n.

(Privacy against Charlie) The protocol is private against Charlie since the messages that he receives from Alice and Bob are only sufficient to reveal a permutation of the bitwise exclusive-or of X^n and Y^n, $\pi(X^n \oplus Y^n)$, which reveals no more information about X^n and Y^n than the Hamming distance. Formally,

$$\begin{aligned} &I(M_3; X^n, Y^n | f(X^n, Y^n)) \\ &\quad = I(\pi(X^n \oplus R^n), \pi(Y^n \oplus R^n); X^n, Y^n | f(X^n, Y^n)) \\ &\quad = I(\pi(X^n \oplus Y^n), \pi(Y^n \oplus R^n); X^n, Y^n | f(X^n, Y^n)) = 0, \end{aligned}$$

for the same reasons as in (11). ■

IV. Inadequacy of BGW for Quadratic Distance

Under the passive behavioral model (with no collusions), any function can be securely computed amongst three parties. The general passive party techniques of [1] provide a method to construct secure protocols. In this section, we will briefly present and analyze the **BGW** protocol [1] that securely computes the quadratic distance under the passive behavioral model. Since quadratic distance coincides with Hamming distance for binary sequences, the same protocol can also be used to compute the Hamming distance for binary sequences. The passive-party techniques of [1] exploit the homomorphic properties of the polynomial secret-sharing scheme of [6]. The resulting protocol is secure for passive parties but is not guaranteed to be secure for active parties.

We will show that the **BGW** protocol is insecure under the active behavioral model for three-party quadratic (and Hamming) distance computation. This will provide further insight into the notion of security under the active behavioral model. Since we are dealing with three parties, the active-party techniques of [1] are not applicable since they require at least four parties to be involved in the computation.

In the following protocol, the non-negative integers $\mathbb{Z}_s = \{0, 1, \ldots, s-1\}$ are assumed to be embedded in a finite field $\mathbb{Z}_N$ of prime order $N > n(s-1)^2$ with field arithmetic defined as modular arithmetic with respect to N. This ensures that $\mathbb{Z}_N$ is large enough to simulate the necessary integer arithmetic for computing the quadratic distance between length-n sequences while avoiding overflow (modulo) effects.

Protocol **BGW** for computing the quadratic distance between two length-n strings in $\mathbb{Z}_s^n$ comprises the following steps:

1) Alice randomly chooses $\alpha_1, \ldots, \alpha_n \sim$ iid Unif($\mathbb{Z}_N$) independently of (X^n, Y^n). For each $i \in \{1, \ldots, n\}$, Alice creates the polynomial $p_i : \mathbb{Z}_N \to \mathbb{Z}_N$, via
$$p_i(j) = \alpha_i j + X_i.$$
Alice sends to Bob (player $j = 2$) the values $\{p_1(2), \ldots, p_n(2)\}$, and sends to Charlie (player $j = 3$) the values $\{p_1(3), \ldots, p_n(3)\}$, while keeping the values $\{p_1(1), \ldots, p_n(1)\}$ for herself.
2) Bob performs an analogous step. First, he randomly chooses $\beta_1, \ldots, \beta_n \sim$ iid Unif($\mathbb{Z}_N$) independently of (X^n, Y^n). For each $i \in \{1, \ldots, n\}$, Bob creates the polynomial $q_i : \mathbb{Z}_N \to \mathbb{Z}_N$, via
$$q_i(j) = \beta_i j + Y_i.$$
Bob sends to Alice (player $j = 1$) the values $\{q_1(1), \ldots, q_n(1)\}$, and sends to Charlie (player $j = 3$) the values $\{q_1(3), \ldots, q_n(3)\}$, while keeping the values $\{q_1(2), \ldots, q_n(2)\}$ for himself.
3) Alice, Bob, and Charlie now each individually compute samples of the polynomial $r : \mathbb{Z}_N \to \mathbb{Z}_N$ defined by
$$r(j) = \sum_{i=1}^{n} \left[p_i^2(j) + q_i^2(j) - 2p_i(j)q_i(j)\right].$$
Alice computes $r(1)$ via the above equation from the values available to her, $\{p_i(1), q_i(1)\}_{i=1}^n$. Likewise, Bob and Charlie compute $r(2)$ and $r(3)$, respectively.
4) Alice and Bob transmit $r(1)$ and $r(2)$, respectively, to Charlie.
5) Charlie reconstructs the degree-two polynomial r via interpolation from the three points $r(1)$, $r(2)$, and $r(3)$. Charlie evaluates $r(0)$ in order to get
$$\begin{aligned} r(0) &= \sum_{i=1}^{n} \left[p_i^2(0) + q_i^2(0) - 2p_i(0)q_i(0)\right] \\ &= \sum_{i=1}^{n} \left[X_i^2 + Y_i^2 - 2X_iY_i\right] \\ &= f(X^n, Y^n). \end{aligned}$$

The **BGW** protocol securely computes the quadratic distance under the passive behavioral model [1]. However, it is not secure under the active behavioral model – neither for quadratic distance nor for Hamming distance computation. In the following discussion, this insecurity is illustrated by demonstrating a simple attack that is able to influence the computation beyond what can be done against a trusted genie.

Quadratic Distance: Consider the computation of quadratic distance (where $s > 2$), that is, Alice and Bob have integer sequences $X^n, Y^n \in \{0, \ldots, s-1\}^n$ and Charlie wishes to compute
$$f(X^n, Y^n) = \sum_{i=1}^{n} (X_i - Y_i)^2.$$
The range of this function $\mathcal{R}(f)$ is a proper subset of $Z_{n(s-1)^2}$ since each function value is a sum of n numbers from the set $\{x^2 : x \in Z_s\}$. The finite field $\mathbb{Z}_N$ used by this protocol must have prime size $N > n(s-1)^2$ in order to simulate integer arithmetic as finite-field arithmetic. Hence, $\mathcal{R}(f)$ must be a proper subset of $\mathbb{Z}_N$ and the rest of $\mathbb{Z}_N$ would be invalid outputs for the function computation. In the ideal model, for any attack by Alice (or symmetrically by Bob), the output of Charlie would still remain in range $\mathcal{R}(f)$, since Alice can only affect it by

changing her input, and an invalid output by Charlie is impossible. However, in the real model, Alice can launch a simple attack, where she simply randomly chooses the final message $r(1)$ that she sends to Charlie independently and uniformly over Z_N. This would cause Charlie's output to uniformly take values over the entire finite-field Z_N, including invalid values, due to the polynomial interpolation used to recover the function computation result. For fixed values of $r(2)$ and $r(3)$, each (possibly modified) value for $r(1)$ corresponds to a unique polynomial interpolation result, since three samples uniquely determine a degree-two (parabolic) polynomial. Thus, due to this one-to-one relationship, a uniform distribution on $r(1)$ induces a uniform distribution on the function computation result. Thus, the protocol is insecure since there exists an attack in the real model (against the protocol) that cannot be equivalently mounted in the ideal model. In addition to the possibility that an attack against the protocol could create invalid output, the distribution of the valid outputs also becomes uniform, which cannot, in general, happen in an attack against a trusted genie. The next example illustrates this issue further.

Hamming Distance: Consider the computation of Hamming distance when Alice and Bob's binary sequences are independent sequences of iid Bernoulli$(1/2)$ bits. In the ideal model, for any attack by Alice (or symmetrically by Bob), the exclusive-or of her string and Bob's will be an iid Bernoulli$(1/2)$ sequence since his string is iid Bernoulli$(1/2)$ and independent of Alice's modified input. This means that for any attack by Alice against a trusted genie, Charlie's output would always be distributed over $\{0, 1, \ldots, n\}$ as a binomial distribution with parameters n and $p = 1/2$. For the protocol in the real model, if $N = n + 1$ is prime, then Z_N can be used and does not contain any invalid outputs. In the real model, Alice can launch a simple attack (as in Example 1), where she simply randomly chooses the final message $r(1)$ that she sends to Charlie independently and uniformly over Z_N, causing Charlie's output to be uniformly distributed over Z_N. Thus, the protocol is insecure since there exists an attack in the real model (against the protocol) that influences the computation output in a manner that cannot be replicated by an attack against a trusted genie.

Even though this simple attack does not enable Alice to choose Charlie's output with certainty, her ability to affect the distribution of that output can have a profound impact in certain applications. Consider the application of secure authentication described earlier. The model of Alice and Bob's sequences as independent binary strings reflects when an illegitimate Alice is attempting to falsely authenticate herself. Imagine that the system was designed allow authentication of Alice if her string was ninety percent similar to Bob's, i.e., the Hamming distance is within $n/10$. Against the trusted genie of the ideal model, any attack from Alice still results in a binomial distribution in the output computed by Charlie, which has an exponentially decaying tail probability for large n and hence a negligible chance for Alice to falsely authenticate herself. However, against the protocol in the real model, if Alice uses this simple attack to cause the output of Charlie to be uniformly distributed, then she has ten percent chance of being falsely authenticated.

V. Concluding Remarks and Future Work

In this paper, we studied a special three-party secure computation problem and provided information-theoretic conditions for security under the active behavioral model. These conditions are equivalent to the formulation of security based on the notion of simulating a trusted genie. We used these conditions to prove the security of the **HamDist** protocol which securely computes the Hamming distance between binary sequences. We also use these conditions to analyze the security of the **BGW** protocol, which securely computes the quadratic distance under the passive behavioral model, but is insecure for the active behavioral model. Information-theoretic conditions similar to those in Theorem 1 can be developed for the general three-party computation problem in which each party has an input and each party is required to compute a potentially different function of the inputs held by all the parties. Another direction for extending this work is to relax the requirement for exactly matching the statistical properties of the ideal model. For instance, requiring that the distributions in equation (1) be only ϵ-close with respect to some measure of distributional closeness as in [7]. An open question is whether there exist protocols that can securely compute (under the active behavioral model) the Hamming distance for non-binary sequences and the quadratic distance.

References

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

[2] D. Chaum, C. Crépeau, and I. Damgård, "Multi-party unconditionally secure protocols," in *Proceedings of the ACM Symposium on Theory of Computing*, Chicago, IL, 1988, pp. 11–19.
[3] O. Goldreich, *Foundations of Cryptography*. Cambridge University Press, 2004, vol. II: Basic Applications.
[4] C. Crépeau, G. Savvides, C. Schaffner, and J. Wullschleger, "Information-theoretic conditions for two-party secure function evaluation," in *Advances in Cryptology – EUROCRYPT*, ser. Lecture Notes in Computer Science, vol. 4004. Springer-Verlag, 2006, pp. 538–554.
[5] J. Wullschleger, "Oblivious-transfer amplification," Ph.D. dissertation, Swiss Federal Institute of Technology, Zürich, 2008.
[6] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 637–647, 1985.
[7] C. Crépeau and J. Wullschleger, "Statistical security conditions for two-party secure function evaluation," in *Proceedings of the 3rd International Conference on Information Theoretic Security*, ser. Lecture Notes in Computer Science, vol. 5155. Springer-Verlag, 2008, pp. 86–99.