Statistical Security Conditions for Two-Party Secure Function Evaluation

Claude Crépeau[1] and Jürg Wullschleger[2]

[1] McGill University, Montréal, QC, Canada
crepeau@cs.mcgill.ca
[2] University of Bristol, Bristol, United Kingdom
j.wullschleger@bristol.ac.uk

Abstract. To simplify proofs in information-theoretic security, the standard security definition of two-party secure function evaluation based on the real/ideal model paradigm is often replaced by an information-theoretic security definition. At EUROCRYPT 2006, we showed that most of these definitions had some weaknesses, and presented new information-theoretic conditions that were equivalent to a simulation-based definition in the real/ideal model. However, there we only considered the perfect case, where the protocol is not allowed to make any error, which has only limited applications.

We generalize these results to the statistical case, where the protocol is allowed to make errors with a small probability. Our results are based on a new measure of information that we call the *statistical information*, which may be of independent interest.

Keywords: Secure function evaluation, information-theoretic security, security definition, oblivious transfer.

1 Introduction

Secure function evaluation [1] allows two (or more) parties to jointly compute a function in a secure way, which means that no player may get additional information about the other players' inputs or outputs, other than what may be deduced from their own input and output. A computationally secure solution to this problem has been given in [2]. Schemes ensuring unconditional security were subsequently provided in [3] and independently in [4].

Oblivious transfer [5,6,7] is a simple primitive of central interest in secure function evaluation. It allows a sender to send one of n binary strings of length k to a receiver. The primitive allows the receiver to receive the string of his choice while concealing this choice from a (possibly dishonest) sender. On the other hand, a dishonest receiver cannot obtain information about more than one of the strings, including partial joint information on two or more strings. It has since been proved that oblivious transfer is in fact sufficient by itself to securely compute any function [8,9]. More completeness results followed in [10,11,12,13].

R. Safavi-Naini (Ed.): ICITS 2008, LNCS 5155, pp. 86–99, 2008.

1.1 Security Definitions

Formal security definitions for secure function evaluation have been proposed in [14] and [15]. Both definitions were inspired by the *simulation paradigm* used in [16] to define zero-knowledge proofs of knowledge. These definitions require that for any adversary, there exists a simulated adversary in an ideal setting (which is secure by definition) that achieves the same. That protocols which satisfy these definitions are *sequentially composable* has been proved in [17]. See also [18].

Later, a stronger notion of security, called *universal composability*, has been defined in [19] and independently in [20]. It guarantees that protocols are securely composable in any way.

Even though simulation-based security definitions are widely accepted as being the right definition of security today, ad-hoc definitions are still widely used due to their simplicity. Unfortunately, as we showed in [21], many of these definitions proposed for various specific scenarios have turned out to be deficient. We proposed in [21] simple information-theoretic conditions for the security of function evaluation, and proved that they are equivalent to the standard definition in the real/ideal model. However, these conditions could only be applied in the perfect case, when the protocol does not have any failure probability and does not leak any information, and therefore had only a very limited range of applications. For the special case of *randomized oblivious transfer*, these conditions have been generalized in [22] to the statistical case, where the protocol is allowed to make errors with a small probability.

1.2 Information Measures

The *Shannon mutual information* has been introduced in [23], and is one of the most important tools in information theory, as a measure of *how many bits of information* one random variable has over the other. The mutual information tells us for example how many bits can be transmitted over a noisy channel.

In information-theoretic cryptography, the mutual information has also been used in security definitions, to express that an adversary obtains almost no information about some secret, i.e., that two random variables are *almost independent*. But since in cryptography we are not interested in *how many bits* the adversary gets, but in the *probability* that he gets *any* information at all, the mutual information is not a good measure for that task.

1.3 Contribution

First, we propose a new measure of information that we call the *statistical information*, which is better suited to express security conditions than the mutual information. The difference between the statistical and the mutual information is the distance measure they are based on: while the mutual information is based on the relative entropy, the statistical information is based on the statistical distance.

Then we will generalize the results from [21] and [22]. We present necessary and sufficient information theoretic conditions for any two-party secure function evaluation in the statistical case, and apply them to oblivious transfer. The statistical information plays a very important role to state these conditions.

1.4 Related Work

Recently, Fehr and Schaffner showed in [24] that similar results also hold in the quantum setting. They presented security conditions for quantum protocols where the honest players have classical input and output, and showed that any quantum protocol that satisfies these conditions can be used as a sub-protocol in a classical protocol.

1.5 Preliminaries

For a random variable X, we denote its distribution by P_X and its domain by $\mathcal{X}$. $P_{Y|X} = P_{XY}/P_X$ denotes a conditional probability distribution, which models a probabilistic function that takes x as input and outputs y, distributed according to $P_{Y|X=x}$.

Definition 1. *The* statistical distance *between two distributions P_X and $P_{X'}$ over $\mathcal{X}$ is defined as $\delta(P_X, P_{X'}) = \frac{1}{2}\sum_{x\in\mathcal{X}} |P_X(x) - P_{X'}(x)|$.*

If $\delta(P_X, P_{X'}) \le \varepsilon$, we may also write $P_X \equiv_\varepsilon P_{X'}$ or $X \equiv_\varepsilon X'$. We will need the following basic properties of δ.

Lemma 1 (Triangle Inequality). *For any distributions P_X, $P_{X'}$ and $P_{X''}$, we have*

$$\delta(P_X, P_{X''}) \le \delta(P_X, P_{X'}) + \delta(P_{X'}, P_{X''}) \ .$$

Lemma 2 (Data Processing). *For any distributions P_{XY} and $P_{X'Y'}$, we have*

$$\delta(P_X, P_{X'}) \le \delta(P_{XY}, P_{X'Y'}) \ .$$

Lemma 3. *For any distributions P_X and $P_{X'}$, and any conditional distribution $P_{Y|X}$, we have*

$$\delta(P_X, P_{X'}) = \delta(P_X P_{Y|X}, P_{X'} P_{Y|X}) \ .$$

Lemma 4. *For any distributions P_X and $P_{X'}$ we have $\delta(P_X, P_Y) \le \varepsilon$, if and only if there exist events $\mathcal{E}_X$ and $\mathcal{E}_Y$ with $\Pr[\mathcal{E}_X] = \Pr[\mathcal{E}_Y] = 1 - \varepsilon$ and $P_{X|\mathcal{E}_X} = P_{Y|\mathcal{E}_Y}$.*

2 Statistical Information

In this section, we introduce the *statistical information* $\mathrm{I_S}$. While the mutual information uses relative entropy as the underlying distance measure, we will use the statistical distance. Its value tells us how close the distribution of three random variables X, Y and Z is to a *Markov-chain.*

Definition 2. *The* statistical information of X and Y given Z *is defined as* $\mathrm{I_S}(X;Y \mid Z) := \delta(P_{XYZ}, P_Z P_{X|Z} P_{Y|Z})$.

Obviously, this measure is non-negative and symmetric in X and Y. We will now show more properties of $\mathrm{I_S}$, which are related to similar properties of the mutual information.

Lemma 5 (Chain rule). *For all P_{WXYZ}, we have*

$$\mathrm{I_S}(WX; Y \mid Z) \leq \mathrm{I_S}(W; Y \mid Z) + \mathrm{I_S}(X; Y \mid WZ)$$

Proof. We have

$$\mathrm{I_S}(X; Y \mid WZ) = \delta(P_{WXYZ}, P_{WYZ}P_{X|WZ}) \; .$$

From Lemma 3 follows that

$$\begin{aligned} \delta(P_{WYZ}P_{X|WZ}, P_Z P_{W|Z} P_{Y|Z} P_{X|WZ}) &= \delta(P_{WYZ}, P_Z P_{W|Z} P_{Y|Z}) \\ &= \mathrm{I_S}(W; Y \mid Z) \; . \end{aligned}$$

Using Lemma 1 and $P_{WX|Z} = P_{W|Z}P_{X|WZ}$, we get

$$\delta(P_{WXYZ}, P_Z P_{WX|Z} P_{Y|Z}) \leq \mathrm{I_S}(W; Y \mid Z) + \mathrm{I_S}(X; Y \mid WZ) \; . \qquad \square$$

Lemma 6 (Monotonicity). *For all P_{WXYZ}, we have*

$$\mathrm{I_S}(W; Y \mid Z) \leq \mathrm{I_S}(WX; Y \mid Z) \; .$$

Proof. Using Lemma 2, we get

$$\begin{aligned} \mathrm{I_S}(WX; Y \mid Z) &= \delta(P_{WXYZ}, P_Z P_{W|Z} P_{X|WZ} P_{Y|Z}) \\ &\geq \delta(P_{WYZ}, P_Z P_{W|Z} P_{Y|Z}) \\ &= \mathrm{I_S}(W; Y \mid Z) \; . \end{aligned} \qquad \square$$

Note that there exist P_{XYZ} and $Q_{ZX}Q_{Y|Z}$, where

$$\delta(P_{XYZ}, Q_{ZX}Q_{Y|Z}) < \delta(P_{XYZ}, P_Z P_{X|Z} P_{Y|Z}),$$

so $P_Z P_{X|Z} P_{Y|Z}$ is not always the closest Markov-chain to P_{XYZ}. Luckily, as the following two lemmas show, $P_Z P_{X|Z} P_{Y|Z}$ is only by a factor of 4 away from the optimal Markov-chain, which is sufficient for our applications[1].

Lemma 7. *For all probability distributions P_{XYZ}, we have*

$$\mathrm{I_S}(X; Y \mid Z) \leq 2 \cdot \min_{Q_{Y|Z}} \delta(P_{XYZ}, P_{XZ}Q_{Y|Z}) \; .$$

[1] An alternative definition for $\mathrm{I_S}$ would be to take the distance to the closest Markov-chain. However, we think that this would make the definition much more complicated, at almost no benefit.

Proof. Let $Q_{Y|Z}$ be the conditional probability distribution that minimizes the expression, and let $\varepsilon := \delta(P_{XYZ}, P_{XZ}Q_{Y|Z})$. We have

$$P_{XZ}Q_{Y|Z} = P_Z Q_{Y|Z} P_{X|Z} \; .$$

Let $Q'_{YZ} := P_Z Q_{Y|Z}$. From Lemma 2 follows that $\delta(P_{YZ}, Q'_{YZ}) \leq \varepsilon$ and from Lemma 3 that $\delta(P_{YZ}P_{X|Z}, Q'_{YZ}P_{X|Z}) \leq \varepsilon$. From Lemma 1 follows then that

$$\delta(P_{XYZ}, P_{XZ}P_{Y|Z}) \leq 2\varepsilon \; . \qquad \square$$

Lemma 8. *For all probability distributions P_{XYZ}, we have*

$$\mathrm{I_S}(X;Y \mid Z) \leq 4 \cdot \min_{Q_{XZ}, Q_{Y|Z}} \delta(P_{XYZ}, Q_{XZ}Q_{Y|Z}) \; .$$

Proof. Let Q_{XZ} and $Q_{Y|Z}$ be the conditional probability distributions that minimize the expression, and let $\varepsilon := \delta(P_{XYZ}, Q_{XZ}Q_{Y|Z})$. From Lemma 2 follows that $\delta(P_{XZ}, Q_{XZ}) \leq \varepsilon$ and from Lemma 3 that $\delta(P_{XZ}Q_{Y|Z}, Q_{XZ}Q_{Y|Z}) \leq \varepsilon$. From Lemma 1 follows that $\delta(P_{XYZ}, P_{XZ}Q_{Y|Z}) \leq 2\varepsilon$. The statement follows by applying Lemma 7. □

Lemma 9. *For all P_{WXYZ}, we have*

$$\mathrm{I_S}(X;Y \mid WZ) \leq 2 \cdot \mathrm{I_S}(WX;Y \mid Z) \; .$$

Proof. From Lemma 7 follows that

$$\begin{aligned} \mathrm{I_S}(X;Y \mid WZ) &\leq 2 \cdot \min_{Q_{Y|WZ}} \delta(P_{WXYZ}, P_{WXZ}Q_{Y|WZ}) \\ &\leq 2 \cdot \delta(P_{WXYZ}, P_{WXZ}P_{Y|Z}) \\ &= 2 \cdot \mathrm{I_S}(WX;Y \mid Z) \; . \end{aligned} \qquad \square$$

2.1 Relation between I and $\mathrm{I_S}$

Since we would like to use $\mathrm{I_S}$ in situations where previously the Shannon mutual information I has been used, it is important to know how these two measures relate to each other. Using Pinsker's inequality (see, for example, Lemma 16.3.1 in [25]) and Jensen's inequality, it is easy to show that

$$\mathrm{I_S}(X;Y \mid Z) \leq \sqrt{\mathrm{I}(X;Y \mid Z)} \; .$$

The other direction can be shown using Lemma 12.6.1 from [25]. We get that for $\mathrm{I_S}(X;Y \mid Z) \leq \frac{1}{4}$,

$$\mathrm{I}(X;Y \mid Z) \leq -2 \cdot \mathrm{I_S}(X;Y \mid Z) \log \frac{2 \cdot \mathrm{I_S}(X;Y \mid Z)}{|\mathcal{X}| \cdot |\mathcal{Y}| \cdot |\mathcal{Z}|} \; .$$

3 Two-Party Secure Function Evaluation

3.1 Definition of Security in the Real/Ideal Paradigm

We will now give a definition of secure function evaluation based on the real/ideal model paradigm. We use the same definitions as [21], which are based on Definition 7.2.10 of [18] (see also [17]).

Let $x \in \mathcal{X}$ denote the input of the first party, $y \in \mathcal{Y}$ the input of the second party and $z \in \{0,1\}^*$ an additional auxiliary input available to both parties, that is ignored by all honest parties. A *g-hybrid protocol* is a pair of (randomized) algorithms $\Pi = (A_1, A_2)$ which can interact by exchanging messages and which additionally have access to the functionality g. A pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ is called *admissible* for protocol Π if either $\overline{A}_1 = A_1$ or $\overline{A}_2 = A_2$, i.e., if at least one of the parties is honest and uses the algorithm defined by the protocol Π. The joint execution of Π under $\overline{A}$ on input pair $(x,y) \in \mathcal{X} \times \mathcal{Y}$ and auxiliary input $z \in \{0,1\}^*$ in the real model, denoted by

$$\textsc{real}^g_{\Pi,\overline{A}(z)}(x,y) \ ,$$

is defined as the output pair resulting from the interaction between $\overline{A}_1(x,z)$ and $\overline{A}_2(y,z)$ using the functionality g.

The *ideal model* defines the optimal setting where the players have access to an ideal functionality f they wish to compute. The trivial f-hybrid protocol $B = (B_1, B_2)$ is defined as the protocol where both parties send their inputs x and y unchanged to the functionality f and output the values u and v received from f unchanged. Let $\overline{B} = (\overline{B}_1, \overline{B}_2)$ be an admissible pair of algorithms for B. The joint execution of f under $\overline{B}$ in the ideal model on input pair $(x,y) \in \mathcal{X} \times \mathcal{Y}$ and auxiliary input $z \in \{0,1\}^*$, denoted by

$$\textsc{ideal}_{f,\overline{B}(z)}(x,y) \ ,$$

is defined as the output pair resulting from the interaction between $\overline{B}_1(x,z)$ and $\overline{B}_2(y,z)$ using the functionality f.

We say that a protocol securely computes a functionality, if anything an adversary can do in the real model can be simulated in the ideal model.

Definition 3 (Statistical Security). *A g-hybrid protocol Π* securely computes f with an error of at most ε *if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible in the real model for the protocol Π, there exists a pair of algorithms $\overline{B} = (\overline{B}_1, \overline{B}_2)$ that is admissible in the ideal model for protocol B (and where the same players are honest), such that for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $z \in \{0,1\}^*$, we have*

$$\textsc{ideal}_{f,\overline{B}(z)}(x,y) \equiv_\varepsilon \textsc{real}^g_{\Pi,\overline{A}(z)}(x,y) \ .$$

A very important property of the above definition is that it implies *sequential composition*, see [17]. Note that in contrast to [17] or [18], we do not require the simulation to be efficiently computable.

The following lemma formalizes the idea already mentioned in [21], namely that if a protocol is secure against adversaries without auxiliary input, then it is also secure against adversaries with auxiliary input. To avoid that the ideal adversary with auxiliary input gets infinitely big, we have to additionally require that there exists an explicit construction of the ideal adversary without auxiliary input.

Lemma 10. *If a g-hybrid protocol Π securely computes f with an error ε against adversaries with constant auxiliary input and the construction of the ideal adversary is explicit, then it securely computes f with an error of at most ε.*

Proof. If both players are honest the auxiliary input is ignored and the lemma holds. Let player i be malicious and denote by $\overline{A}_i$ the algorithm used. For a fixed $z \in \{0,1\}^*$, let $\overline{A}_i^z$ be equal to $\overline{A}_i$, but with the auxiliary input z hard-wired into it. Since Π securely computes f with an error ε against adversaries with constant auxiliary input, there exists an algorithm $\overline{B}_i^z$, such that for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, we have

$$\text{IDEAL}_{f,\overline{B}^z}(x,y) \equiv_\varepsilon \text{REAL}^g_{\Pi,\overline{A}^z}(x,y) \ .$$

Now, we let $\overline{B}_i$ be the concatenation of all $\overline{B}_i^z$, i.e., on auxiliary input z the adversary $\overline{B}_i$ behaves as $\overline{B}_i^z$. Note that since we have an explicit construction of $\overline{B}_i^z$, $\overline{B}_i$ has a finite description. Obviously, we have for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $z \in \{0,1\}^*$ that

$$\text{IDEAL}_{f,\overline{B}(z)}(x,y) \equiv_\varepsilon \text{REAL}^g_{\Pi,\overline{A}(z)}(x,y) \ .$$

Hence, Π securely computes f with an error of at most ε. □

Therefore, to show the security of a protocol in our model, the auxiliary input can be omitted, which we will do for the rest of this paper.

3.2 Information-Theoretic Conditions for Security

We will now state our main results, which are information-theoretic conditions for the *statistical* security of a protocol *without the use of an ideal model.*

First of all, we will slightly change our notation. Let X and Y be random variables denoting the player's inputs, distributed according to a distribution P_{XY} unknown to the players, and let U and V be random variables denoting the outputs of the two parties, i.e., for specific inputs (x,y) we have

$$(U,V) = \text{REAL}^g_{\Pi,\overline{A}}(x,y) \ , \quad (\underline{U},\underline{V}) = \text{IDEAL}_{f,\overline{B}}(x,y) \ .$$

The security condition of Definition 3 can be expressed as

$$P_{\underline{UV}|X=x,Y=y} \equiv_\varepsilon P_{UV|X=x,Y=y} \ .$$

To simplify the statement of the following theorem, we will assume that the ideal functionality f is deterministic. It can be generalized to probabilistic functionalities without any problems.

The conditions for the security for player 1 must ensure that there exists an ideal adversary that achieves almost the same as the real adversary. We achieve this by requiring that there exists a virtual input value Y' that the adversary could have created (this is ensured by $\mathrm{I_S}(X; Y' \mid Y) \approx 0$), and a virtual output value V' that, together with U, could be the output of the ideal functionality, given X and Y' as input (this is ensured by $\Pr[(U, V') = f(X, Y')] \approx 1$). The protocol is secure if the adversary's output V could have been calculated by him from Y, Y' and V', which is ensured by $\mathrm{I_S}(UX; V \mid YY'V') \approx 0$.

Theorem 1. *A protocol Π* securely computes the deterministic functionality f with an error of at most 3ε, *if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible in the real model for the protocol Π and for any input (X, Y) distributed according to P_{XY} over $\mathcal{X} \times \mathcal{Y}$, $\overline{A}$ produces outputs (U, V) distributed according to $P_{UV|XY}$, such that the following conditions are satisfied:*

- (Correctness) *If both players are honest, we have*

$$\Pr[(U, V) = f(X, Y)] \geq 1 - \varepsilon \ .$$

- (Security for Player 1) *If player* 1 *is honest then there exist random variables Y' and V' distributed according to $P_{Y'V'|XYUV}$ such that*

$$\Pr[(U, V') = f(X, Y')] \geq 1 - \varepsilon \ ,$$

$$\mathrm{I_S}(X; Y' \mid Y) \leq \varepsilon$$

and

$$\mathrm{I_S}(UX; V \mid YY'V') \leq \varepsilon \ .$$

- (Security for Player 2) *If player* 2 *is honest then there exist random variables X' and U' distributed according to $P_{X'U'|XYUV}$ such that*

$$\Pr[(U', V) = f(X', Y)] \geq 1 - \varepsilon \ ,$$

$$\mathrm{I_S}(Y; X' \mid X) \leq \varepsilon$$

and

$$\mathrm{I_S}(VY; U \mid XX'U') \leq \varepsilon \ .$$

Both $P_{Y'V'|XYUV}$ and $P_{X'U'|XYUV}$ should have explicit constructions.

Proof. If both players are honest, the correctness condition implies

$$P_{UV|X=x,Y=y} \equiv_{\varepsilon} P_{\underline{UV}|X=x,Y=y} \ ,$$

for all x and y. If both players are malicious nothing needs to be shown.

Without loss of generality, let player 1 be honest and player 2 be malicious. Let us for the moment assume that the input distribution P_{XY} is fixed and known to the adversary, so the joint distribution in the real model is

$$P_{XYUV} = P_{XY} P_{UV|XY} \ .$$

We will define an admissible protocol $\overline{B} = (B_1, \overline{B}_2)$ in the ideal model that produces almost the same output distribution as the protocol Π in the real model. On input y, let $\overline{B}_2$ choose his input $\underline{y}'$ according to $P_{Y'|Y=y}$, which we model by the channel $P_{\underline{Y}'|Y}$. After receiving $\underline{v}'$ from the ideal functionality f, let $\overline{B}_2$ choose his output $\underline{v}$ according to $P_{V|Y=y,Y'=\underline{y}',V'=\underline{v}'}$, which we model by the channel $P_{\underline{V}|Y\underline{Y}'\underline{V}'}$. The distribution of the input/output in the ideal model is given by

$$P_{XY\underline{UV}} = P_{XY} \sum_{\underline{y}',\underline{v}'} P_{\underline{Y}'|Y} P_{\underline{UV}'|X\underline{Y}'} P_{\underline{V}|Y\underline{Y}'\underline{V}'} \ ,$$

where $(\underline{U}, \underline{V}') = f(X, \underline{Y}')$.

In the real model, it follows from $\mathrm{I_S}(X; Y' \mid Y) \leq \varepsilon$ that

$$P_{XY} P_{Y'|XY} \equiv_\varepsilon P_{XY} P_{Y'|Y} \ ,$$

from $\mathrm{I_S}(UX; V \mid YY'V') \leq \varepsilon$ that

$$P_{XY} P_{UY'V'|XY} P_{V|XYUY'V'} \equiv_\varepsilon P_{XY} P_{UY'V'|XY} P_{V|YY'V'} \ ,$$

and from $\Pr[(U, V') = f(X, Y')] \geq 1 - \varepsilon$ and Lemma 4 that

$$P_{XY} P_{Y'|XY} P_{\underline{UV}'|X\underline{Y}'} \equiv_\varepsilon P_{XY} P_{Y'|XY} P_{UV'|XYY'} \ .$$

We have

$$\begin{aligned} P_{XY\underline{UV}} &= P_{XY} \sum_{\underline{y}',\underline{v}'} P_{\underline{Y}'|Y} P_{\underline{UV}'|X\underline{Y}'} P_{\underline{V}|Y\underline{Y}'\underline{V}'} \\ &\equiv_\varepsilon P_{XY} \sum_{y',v'} P_{Y'|XY} P_{\underline{UV}'|X\underline{Y}'} P_{\underline{V}|Y\underline{Y}'\underline{V}'} \\ &\equiv_\varepsilon P_{XY} \sum_{y',v'} P_{Y'|XY} P_{UV'|XYY'} P_{\underline{V}|Y\underline{Y}'\underline{V}'} \\ &\equiv_\varepsilon P_{XY} \sum_{y',v'} P_{Y'|XY} P_{UV'|XYY'} P_{V|XYUY'V'} \\ &= P_{XYUV} \ . \end{aligned}$$

Therefore, given P_{XY}, we are able to construct an adversary in the ideal model that simulates the output of the real protocol with an error of at most 3ε. However, we have to show that a *fixed* adversary in the ideal model works for *every* input $(x, y) \in \mathcal{X} \times \mathcal{Y}$.[2]

Given P_{XY}, let e be the average error of the simulation, and let e_{xy} be the error if the input is (x, y). We have $e = \sum_{x,y} P_{XY}(x, y) \cdot e_{xy}$. Let $h(P_{XY}) \to P'_{XY}$ a function that maps from the space of all distribution over $\mathcal{X} \times \mathcal{Y}$ to itself, where

$$P'_{XY}(x, y) := P_{XY}(x, y) \cdot \frac{e_{xy} + 1}{e + 1} \ .$$

[2] This part is missing in [21], but there the problem can be solved easily by fixing P_{XY} to the uniform distribution. But in our case, this would give us an error bound that would depend on the dimension of the input, which would be quite weak.

h is a continuous[3] function from a non-empty, compact, convex set $S \subset \mathbb{R}^{|\mathcal{X}\times\mathcal{Y}|}$ into itself, so by Brouwer's Fixed Point Theorem h must have a fixed point distribution Q_{XY}. (A constructive proof of Brower's Fixed Point Theorem can be found in [26].) So we have for all (x, y) that

$$Q_{XY}(x, y) = Q_{XY}(x, y) \cdot \frac{e_{xy} + 1}{e + 1}$$

and $Q_{XY}(x, y) > 0$, and hence $e_{xy} = e$. Therefore, by taking the adversary in the ideal model for the input distribution Q_{XY}, the output will have the same error e for all inputs. Since $e \leq 3\varepsilon$, we get for all x and y

$$P_{\underline{UV}|X=x,Y=y} \equiv_{3\varepsilon} P_{UV|X=x,Y=y} \ ,$$

which implies that the protocol is secure with an error of at most 3ε. □

Theorem 2 now shows that our conditions are not only sufficient but also necessary.

Theorem 2. *If a protocol Π securely computes the deterministic functionality f with an error of at most ε, then for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible in the real model for the protocol Π and for any input (X, Y) distributed according to P_{XY} over $\mathcal{X} \times \mathcal{Y}$, $\overline{A}$ produces outputs (U, V) distributed according to $P_{UV|XY}$, such that the following conditions are satisfied:*

- (Correctness) *If both players are honest, we have*

$$\Pr[(U, V) = f(X, Y)] \geq 1 - \varepsilon \ .$$

- (Security for Player 1) *If player 1 is honest then there exist random variables Y' and V' distributed according to $P_{Y'V'|UVXY}$ such that*

$$\Pr[(U, V') = f(X, Y')] \geq 1 - \varepsilon \ ,$$

$$\mathrm{I}_{\mathrm{S}}(X; Y' \mid Y) = 0$$

and

$$\mathrm{I}_{\mathrm{S}}(UX; V \mid YY'V') \leq 4\varepsilon \ .$$

- (Security for Player 2) *If player 2 is honest then there exist random variables X' and U' distributed according to $P_{X'U'|UVXY}$ such that*

$$\Pr[(U', V) = f(X', Y)] \geq 1 - \varepsilon \ ,$$

$$\mathrm{I}_{\mathrm{S}}(Y; X' \mid X) = 0$$

and

$$\mathrm{I}_{\mathrm{S}}(VY; U \mid XX'U') \leq 4\varepsilon \ .$$

[3] We can assume that $P_{Y'V'|XYUV}$ is a continuous function of P_{XY}.

Proof. There exists an admissible pair of algorithms $\overline{B} = (\overline{B}_1, \overline{B}_2)$ for the ideal model such that for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, we have

$$P_{\underline{UV}|X=x,Y=y} =_\varepsilon P_{UV|X=x,Y=y} \ .$$

If both players are honest we have $\overline{B} = B$. B_1 and B_2 forward their inputs (X, Y) unchanged to the trusted third party, get back $(\underline{U}', \underline{V}') := f(X, Y)$ and output $(\underline{U}, \underline{V}) = (\underline{U}', \underline{V}') = f(X, Y)$. It follows that $\Pr[(U, V) = f(X, Y)] \geq 1 - \varepsilon$.

Without loss of generality, let player 1 be honest and player 2 be malicious. Let us look at the execution of $\overline{B} = (B_1, \overline{B}_2)$, and let P_{XY} be an arbitrary input distribution. The malicious $\overline{B}_2$ can be modeled by the two conditional probability distributions $P_{\underline{Y}'\underline{S}|Y}$ computing the input to the ideal functionality f and some internal data $\underline{S}$, and $P_{\underline{V}|\underline{V}'\underline{S}}$ computing the output. We get

$$\begin{aligned} P_{XY\underline{UVY}'\underline{V}'} &= \sum_s P_{XY} P_{\underline{Y}'\underline{S}|Y} P_{\underline{UV}'|X\underline{Y}'} P_{\underline{V}|\underline{V}'\underline{S}} && (1) \\ &= P_{XY} P_{\underline{Y}'|Y} P_{\underline{UV}'|X\underline{Y}'} \sum_s P_{\underline{S}|Y\underline{Y}'} P_{\underline{V}|\underline{V}'\underline{S}} && (2) \\ &= P_{XY} P_{\underline{Y}'|Y} P_{\underline{UV}'|X\underline{Y}'} P_{\underline{V}|Y\underline{V}'\underline{Y}'} \ , && (3) \end{aligned}$$

where $(\underline{U}, \underline{V}') = f(X, \underline{Y}')$.

Let $P_{Y'V'|UVXY} := P_{\underline{Y}'\underline{V}'|\underline{UV}XY}$. From $P_{\underline{Y}'\underline{V}'|\underline{UV}XY} = P_{\underline{Y}'|Y} P_{\underline{V}'|\underline{UV}XY\underline{Y}'}$ follows that

$$\mathrm{I_S}(X; Y' \mid Y) = 0 \ .$$

From $P_{\underline{UV}XY} \equiv_\varepsilon P_{UVXY}$ and Lemma 3 follows that

$$P_{XYUVY'V'} \equiv_\varepsilon P_{XY\underline{UVY}'\underline{V}'} \ .$$

Since $P_{XY\underline{UVY}'\underline{V}'} = P_{XY\underline{UV}'\underline{Y}'} P_{\underline{V}|Y\underline{V}'\underline{Y}'}$, it follows from Lemma 8 that

$$\mathrm{I_S}(UX; V \mid YY'V') \leq 4\varepsilon \ ,$$

and from Lemma 2 follows $P_{XY'UV'} \equiv_\varepsilon P_{X\underline{Y}'\underline{UV}'}$, and therefore

$$\Pr[(U, V') = f(X, Y')] \geq 1 - \varepsilon \ . \qquad \square$$

3.3 Oblivious Transfer

We now apply Theorem 1 to 1-out-of-n string oblivious transfer, or $\binom{n}{1}$-OT^k for short. The ideal functionality f_{OT} is defined as $f_{\mathrm{OT}}(X, C) := (\perp, X_C)$, where $\perp$ denotes a constant random variable, $X = (X_0, \ldots, X_{n-1})$, $X_i \in \{0, 1\}^k$ for $i \in \{0, \ldots, n-1\}$, and $C \in \{0, \ldots, n-1\}$.

Theorem 3. *A protocol Π securely computes $\binom{n}{1}$-OT^k with an error of at most 6ε if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible for protocol Π and for any input (X, C), $\overline{A}$ produces outputs (U, V) such that the following conditions are satisfied:*

- (Correctness) *If both players are honest, then $U = \perp$ and*

$$\Pr[V = X_C] \geq 1 - \varepsilon \ .$$

- (Security for Player 1) *If player 1 is honest, then we have $U = \perp$ and there exists a random variable C' distributed according to $P_{C'|XCV}$, such that*

$$\mathrm{I_S}(X; C' \mid C) \leq \varepsilon \ , \ \textit{and} \ \mathrm{I_S}(X; V \mid CC'X_{C'}) \leq \varepsilon \ .$$

- (Security for Player 2) *If player 2 is honest, we have $V \in \{0,1\}^k$ and*

$$\mathrm{I_S}(C; U \mid X) \leq \varepsilon \ .$$

Proof. We need to show that these conditions imply the conditions of Theorem 1 for $\varepsilon' := 2\varepsilon$. For correctness and the security for player 1 this is trivial.

For the security for player 2, we choose $X' = (X'_0, \ldots, X'_{n-1})$ as follows: for all values i, let X'_i be chosen according to the distribution $P_{V|XU,C=i}$ except for X'_C. We set $X'_C = V$. Note that all X'_i, $0 \leq i \leq n-1$, have distribution $P_{V|XU,C=i}$. Thus X' does not depend on C given XU, and we have $\mathrm{I_S}(C; X' \mid XU) = 0$. From Lemma 5 follows that

$$\mathrm{I_S}(C; X'U \mid X) \leq \mathrm{I_S}(C; U \mid X) + \mathrm{I_S}(C; X' \mid XU) \leq \varepsilon \ .$$

Lemmas 6 implies that $\mathrm{I_S}(C; X' \mid X) \leq \varepsilon$ and, since V is a function of X' and C, it follows from Lemma 9 that

$$\mathrm{I_S}(VC; U \mid XX') = \mathrm{I_S}(C; U \mid XX') \leq 2 \cdot \mathrm{I_S}(C; X'U \mid X) \leq 2\varepsilon \ .$$

The statements follows by applying Theorem 1. □

Furthermore, note that using Lemmas 5 and 6, we get

$$\begin{aligned} \mathrm{I_S}(C; U \mid X) &\leq \mathrm{I_S}(C; X'U \mid X) \\ &\leq \mathrm{I_S}(C; X' \mid X) + \mathrm{I_S}(C; U \mid XX') \\ &\leq \mathrm{I_S}(C; X' \mid X) + \mathrm{I_S}(VC; U \mid XX') \ , \end{aligned}$$

from which it is easy to show that the conditions of Theorem 1 also imply the conditions in Theorem 3.

References

1. Yao, A.C.: Protocols for secure computations. In: Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 1982), pp. 160–164 (1982)
2. Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game. In: Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC 1987), pp. 218–229. ACM Press, New York (1987)

3. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC 1988), pp. 1–10. ACM Press, New York (1988)
4. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols (extended abstract). In: Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC 1988), pp. 11–19. ACM Press, New York (1988)
5. Wiesner, S.: Conjugate coding. SIGACT News 15(1), 78–88 (1983)
6. Rabin, M.O.: How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory (1981)
7. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. Commun. ACM 28(6), 637–647 (1985)
8. Goldreich, O., Vainish, R.: How to solve any protocol problem - an efficiency improvement. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 73–86. Springer, Heidelberg (1988)
9. Kilian, J.: Founding cryptography on oblivious transfer. In: Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC 1988), pp. 20–31. ACM Press, New York (1988)
10. Crépeau, C.: Verifiable disclosure of secrets and applications. In: Quisquater, J.-J., Vandewalle, J. (eds.) EUROCRYPT 1989. LNCS, vol. 434, pp. 181–191. Springer, Heidelberg (1990)
11. Goldwasser, S., Levin, L.A.: Fair computation of general functions in presence of immoral majority. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 77–93. Springer, Heidelberg (1991)
12. Crépeau, C., van de Graaf, J., Tapp, A.: Committed oblivious transfer and private multi-party computation. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 110–123. Springer, Heidelberg (1995)
13. Kilian, J.: More general completeness theorems for secure two-party computation. In: Proceedings of the 32th Annual ACM Symposium on Theory of Computing (STOC 2000), pp. 316–324. ACM Press, New York (2000)
14. Micali, S., Rogaway, P.: Secure computation (abstract). In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 392–404. Springer, Heidelberg (1992)
15. Beaver, D.: Foundations of secure interactive computing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 377–391. Springer, Heidelberg (1992)
16. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof systems. SIAM J. Comput. 18(1), 186–208 (1989)
17. Canetti, R.: Security and composition of multiparty cryptographic protocols. Journal of Cryptology 13(1), 143–202 (2000)
18. Goldreich, O.: Foundations of Cryptography. Basic Applications, vol. II. Cambridge University Press, Cambridge (2004)
19. Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: Proceedings of the 42th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2001), pp. 136–145 (2001), http://eprint.iacr.org/2000/067
20. Backes, M., Pfitzmann, B., Waidner, M.: A universally composable cryptographic library (2003), http://eprint.iacr.org/2003/015
21. Crépeau, C., Savvides, G., Schaffner, C., Wullschleger, J.: Information-theoretic conditions for two-party secure function evaluation. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 538–554. Springer, Heidelberg (2006), http://eprint.iacr.org/2006/183

22. Wullschleger, J.: Oblivious-Transfer Amplification. PhD thesis, ETH Zurich, Switzerland (2007)
23. Shannon, C.E.: A mathematical theory of communication. Bell System Tech. Journal 27, 379–423 (1948)
24. Fehr, S., Schaffner, C.: Composing quantum protocols in a classical environment (2008), http://arxiv.org/abs/0804.1059
25. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley-Interscience, Chichester (1991)
26. Kellogg, R.B., Li, T.Y., Yorke, J.: A constructive proof of the brouwer fixed-point theorem and computational results. SIAM Journal on Numerical Analysis 13(4), 473–483 (1976)