# Information-Theoretic Conditions for Two-Party Secure Function Evaluation*

Claude Crépeau[1] **, George Savvides[1] *,
Christian Schaffner[2] ***, and Jürg Wullschleger[3] †

[1] McGill University, Montréal, QC, Canada. {crepeau,gsavvi1}@cs.mcgill.ca
[2] BRICS, University of Århus, Denmark. chris@brics.dk
[3] ETH Zürich, Switzerland. wjuerg@inf.ethz.ch

**Abstract** Definitions of unconditionally secure function evaluation based on the simulation paradigm for the real/ideal model have the disadvantage of being overly complicated to work with in practice. On the other hand, the simpler information-theoretic definitions proposed for various specific scenarios have often turned out to be deficient. Motivated by this unsatisfactory situation, we present a simple information-theoretic definition of two-party secure function evaluation for the general case and prove its equivalence to the standard, simulation-based definition in the real/ideal model.

## 1 Introduction

### 1.1 Secure Function Evaluation

Secure function evaluation is a cryptographic task originally introduced by Yao in [31]. In essence, this task enables a set of mutually distrustful parties without access to a trusted intermediary to jointly compute the output of a function $f$ without any party revealing any information about its input or output to the other parties beyond what these parties can infer from their own inputs and outputs. Goldreich, Micali and Wigderson [22] showed how to achieve this for any function $f$ in a computationally secure way. Schemes ensuring unconditional security were subsequently provided by Ben-Or, Goldwasser and Wigderson [3] and independently by Chaum, Crépeau and Damgård [12].

Micali and Rogaway [26] and Beaver [2] proposed formal security definitions for secure function evaluation. Both definitions were inspired by the simulation paradigm used by Goldwasser, Micali and Rackoff [23] to define zero-knowledge proofs of knowledge. In a nutshell, to each *real* protocol computing $f$ we associate a two-step procedure in an *ideal* model, where each party simply forwards

* This is the full version of a paper published at EUROCRYPT 2006 [16].
** Supported in part by NSERC, MITACS, and CIAR.
*** Supported by the EC-Integrated Project SECOQC, No: FP6-2002-IST-1-506813.
† Supported by Canada's NSERC, Québec's FQRNT, and Switzerland's SNF.

its input to a trusted party which in turn computes $f$ and distributes the corresponding outputs to the parties. The real protocol is deemed secure if any adversary attacking the protocol has a counterpart in the ideal model that achieves a similar result simply by processing the input prior to forwarding it to the trusted party, and then by processing the output it receives from it. In other words, a protocol is secure if any attack can be simulated in the much more restrictive ideal model. Such protocols secure in the real/ideal model paradigm were later shown to be *sequentially composable*, in the sense that the composition of two or more secure protocols is itself a secure protocol. The sequential composability of secure protocols was further explored by Canetti [9,10] and Goldreich [21].

Canetti [11] also defined *universal composability*, an even stronger security requirement that guarantees that protocols satisfying it can be securely composed *concurrently* in any environment. A similar security definition was provided independently by Backes, Pfitzmann and Waidner [1]. Unfortunately, however appealing the properties of these security definitions may be, they are too strong to allow even basic tasks such as bit commitment to be realized without further assumptions. For this reason, we will limit ourselves to the simpler definition based on the real/ideal model, as given by Goldreich [21].

### 1.2 Oblivious Transfer

*1-out-of-n string oblivious transfer*, denoted $\binom{n}{1}$-$\mathrm{OT}^k$, is a primitive that allows a sender Alice to send one of $n$ binary strings of length $k$ to a receiver Bob. The primitive allows Bob to receive the string of his choice while concealing this choice from (possibly dishonest) Alice. On the other hand, the primitive guarantees that (any dishonest) Bob cannot obtain information about more than one of the strings, including partial joint information on two or more strings.

The first variant of oblivious transfer was introduced by Wiesner [29]. Independently, Rabin re-introduced oblivious transfer in [28] and demonstrated its potential as a cryptographic tool. Its applicability to multi-party computation was shown by Even, Goldreich and Lempel in [20]. It has since been proved that oblivious transfer is in fact sufficient by itself to securely compute any function [24]. More completeness results followed in [14], [15] and [25].

### 1.3 Contributions

The motivation behind our work was to come up with a *general, information-theoretic* security definition to replace the various ad-hoc definitions proposed in the past that are only applicable to specific cryptographic primitives and in restricted contexts. We start by reviewing some of these definitions and point out their shortcomings, as well as subtle flaws that some of them contain. As our starting point for deriving our general definition we use the real/ideal model paradigm of Micali and Rogaway [26] and Beaver [2] and the associated security definition for the case of computationally-bounded parties as it appears in Goldreich [21]. We then adapt the model and the definition so as to allow both parties to be *arbitrary channels* in a non-computational setting. We distill the

relevant security properties of the ideal model into a set of information-theoretic conditions, which become the basis of our new definition. We prove that despite its apparent simplicity, our definition is in fact *equivalent* to the definition based on the real/ideal model paradigm. We subsequently turn our attention to the important special case of oblivious transfer. We show that in this case, the resulting security requirements can be significantly simplified. Moreover, our analysis allows us to easily demonstrate that in the case of a dishonest sender, privacy alone implies security. To further illustrate the usefulness of our definition, we conclude by providing a simple information-theoretic proof of security for the protocol presented in [30] that optimally inverts $\binom{2}{1}$-OT.

### 1.4 Shortcomings of Previously Proposed Security Definitions for Oblivious Transfer

We revisit some information-theoretic definitions for oblivious transfer that appear in the literature and list some of their shortcomings. These examples demonstrate that coming up with the 'right' information-theoretic security definition is a delicate task. This is in fact the main reason why have aimed for a definition which is *provably equivalent* to the standard simulation-based definition using the real/ideal model paradigm.

**Random Inputs** In [19], only oblivious transfer with random inputs is considered, thereby restricting the scope of the proposed definitions to only a few special cases.

**Problems with the Security for the Receiver** In [5,27], the definition of security for requires that the sender's view be independent of the receiver's input. This is overly restrictive: in the most general case we assume that there is a known dependency between the inputs. In this case, the sender's view (which includes his own input) will inevitably be correlated with the receiver's input and so no protocol will satisfy the definition above. In general, one can only expect the two variables to be independent *given the sender's input.*

**Problems with the Security for the Sender** The security for the sender is more difficult to correctly formalize. In addition to problems analogous to the ones presented above for the definition of security for the receiver ([5,27]), there are several commonly encountered difficulties:

- In [6,17] a dishonest receiver is only allowed to change his input in a *deterministic* way. Specifically, the random variable $C'$ indicating the receiver's *effective input* (i.e., the bit he eventually obtains) must be a deterministic function of the input $C$, in contrast to the ideal model where $C'$ can be chosen probabilistically by the dishonest receiver.

– In [7] the random variable $C'$ may depend on the honest sender's input, which is impossible in the ideal model. Furthermore, the view $V$ of the dishonest receiver is required to be independent of the honest sender's input $X$ conditioned on the original input $C$ and the receiver's output $X_{C'}$, *but not on* $C'$. This definition can thus also be overly restrictive in some scenarios. Consider for example the case where the sender's input $X$ is uniformly distributed in $\{00, 01, 10\}$ while the receiver simply replaces his input $C$ with $C'$ chosen uniformly at random from $\{0, 1\}$ and then acts honestly. Let $V$ be the view of the receiver. This clearly permissible behavior is disallowed as $\mathrm{I}(X; V \mid C, X_{C'}) > 0$.

**Abort** In [6,17,7], the honest player is allowed to abort the protocol. However, it is possible that the dishonest player gets some information *before* the honest player aborts, or that the fact of aborting itself provides information about the honest player's inputs.

**Setup stage** An alternative definition is given in [18] in the context of the bounded-storage model. However, this definition is overly complicated and requires a special *setup stage*, which is in general not present in OT protocols.

### 1.5 Preliminaries

Let $X$, $Y$, and $Z$ be three random variables. We will often use expressions of the form

$$\mathrm{I}(X; Y \mid Z) = 0 \ ,$$

where I is the conditional mutual Shannon information. This means that $X$ *and* $Y$ *are independent, given* $Z$. The same condition can also be expressed by saying that $X$*,* $Y$ *and* $Z$ *form a Markov-chain*,

$$X \leftrightarrow Z \leftrightarrow Y \ ,$$

or by

$$P_{Y|ZX} = P_{Y|Z} \ .$$

By the *chain rule* for mutual information we have

$$\mathrm{I}(X; YW \mid Z) = \mathrm{I}(X; W \mid Z) + \mathrm{I}(X; Y \mid WZ) \ .$$

The *information processing inequality* says that local computation cannot increase mutual information. In other words, for any probabilistic $f$ we have

$$\mathrm{I}(X; Y \mid Z) \geq \mathrm{I}(f(X); Y \mid Z) \ .$$

The *statistical distance* or *variational distance* between the distributions of two random variables $X$ and $Y$ over the same domain $\mathcal{V}$ is defined as

$$\delta(X, Y) = \frac{1}{2} \sum_{v \in \mathcal{V}} \big| \Pr[X = v] - \Pr[Y = v] \big| .$$

We also use the notation $X \equiv_\varepsilon Y$ for $\delta(X,Y) \leq \varepsilon$. If $X$ and $Y$ have the *same* distribution, i.e., $\delta(X,Y) = 0$, we write $X \equiv Y$. The statistical distance can alternatively be expressed as:

$$\delta(X,Y) = \max_S \left(\Pr[X \in S] - \Pr[Y \in S]\right) \ .$$

From this expression it is easy to see that the optimal algorithm distinguishing the two distributions can succeed with probability exactly $\frac{1}{2} + \delta(X,Y)$. Another important property of the statistical distance is that for any random variables $X$ and $Y$, there exists a random variable $\tilde{X}$ with the same distribution as $Y$ satisfying $\Pr[\tilde{X} \neq X] = \delta(X,Y)$.

## 2 Defining Secure Function Evaluation using the Real/Ideal Model Paradigm

In this section we provide a simulation-based definition of secure function evaluation for the real/ideal model paradigm. Our definition is based on Definition 7.2.10 of Goldreich [21] (see also [10]).

### 2.1 The information-theoretic context

Goldreich's definition assumes a computational model where all participants are polynomial-time algorithms. In order to bring this model in line with our information-theoretic context we allow the parties in both the real and the ideal model to be *arbitrary channels*. Indeed, as one would naturally expect, our information-theoretic definitions establish certain constraints and relations between several variables such as the two parties' inputs and outputs. These relations imply the existence of *channels* that can sample one variable given others as inputs. However, as is typically the case with information theory, there is no guarantee that there exists a circuit or algorithm (much less an efficient one) that can simulate such channels. Consequently, as it is not possible to demonstrate that our definitions imply that any *algorithmic* adversary in the real model can be converted to an algorithmic adversary in the ideal model, we assume the parties in both models are arbitrary channels.

While we will not be concerned with issues of computational efficiency in this paper, we would like to point out that efficiency is not necessarily irrelevant in an information-theoretic context, unless of course every participant has unlimited computational power. Indeed, from the study of zero-knowledge interactive proof systems [23] we learned that "perfect zero-knowledge" is a more powerful and more restrictive notion than "zero-information" because it imposes additional computational conditions, including the existence of an *efficient* simulator. This is important when the participants are computationally bounded, as it might well be the case that an attack in the ideal model is prohibitively more expensive than an attack in the real model. Consequently, even though such attacks in the ideal model may always be possible in theory (in which case the protocol would

satisfy the information-theoretic security requirements), they might not always be feasible in practice and thus the computational security requirements would not be met.

We remark that by introducing additional constraints regarding computability and efficiency to our definitions, one could guarantee that algorithmic real adversaries have algorithmic ideal counterparts (of comparable complexity, even). However, as such constraints are alien to the information-theoretic setting, they would make our definitions unwieldy and would detract from their essence. We thus refrain from further consideration of such constraints in the present paper.

**The updated model** The model we will be using differs from that of Definition 7.2.10 of Goldreich [21] in the following ways:

(i) We allow the parties in both the real and ideal model to be *arbitrary channels* (as opposed to being polynomially-bounded algorithms).
(ii) We require that the output distributions of the ideal and the real model be either *perfectly indistinguishable* or *statistically indistinguishable* (as opposed to computationally indistinguishable).
(iii) We allow both honest players to have an output.

The motivation behind Modification (i) was explained above. Modification (ii) is just a consequence of (i) while (iii) simplifies the model by making it symmetric and generalizes it to allow functions such as coin flipping by telephone [4] where both players have an output, but which can be implemented without allowing either party to abort the protocol. In Section 7 we also discuss the model of Definition 7.2.6 of [21], i.e., the model where the first party is allowed to abort the protocol after receiving its result but before the second party receives its own.

### 2.2 The definition

We use the following notation: $x \in \mathcal{X}$ denotes the input of the first party, $y \in \mathcal{Y}$ the input of the second party and $z \in \{0,1\}^*$ represents an additional auxiliary input available to both parties but assumed to be 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 $g$[4]. More precisely, for a (randomized) function $g : \mathcal{X} \times \mathcal{Y} \to \mathcal{U} \times \mathcal{V}$ the two parties can send $x$ and $y$ to a trusted party and receive $u$ and $v$, respectively, where $(u, v) = g(x, y)$. Note that a default value is used if a player refuses to send a value. A pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ is called *admissible* for protocol $\Pi$ 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 $\Pi$.

[4] Note that $g$ is in general different from $f$. It should generally be thought of as some trusted cryptographic primitive which the protocol uses as a black box.

**Definition 1 (Real Model).** *Let $\Pi = (A_1, A_2)$ be a $g$-hybrid protocol and let $\overline{A} = (\overline{A}_1, \overline{A}_2)$ be an admissible pair of algorithms for the protocol $\Pi$. The joint execution of $\Pi$ 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*

$$\text{REAL}^g_{\Pi,\overline{A}(z)}(x, y) \ ,$$

*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 scenario where the players have access to an ideal functionality $f$ corresponding to the function they wish to compute. A malicious player may therefore only change (1) his input to the functionality and (2) the output he obtains from the functionality.

**Definition 2 (Ideal Model).** *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*

$$\text{IDEAL}_{f,\overline{B}(z)}(x, y) \ ,$$

*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 $f$.*

Any admissible pair of algorithms $\overline{B}$ in the ideal model can be expressed in the following way: the first party receives input $(x, z)$ and the second party receives input $(y, z)$. The two parties produce $(x', z_1) = \overline{B_1^{\text{in}}}(x, z)$ and $(y', z_2) = \overline{B_2^{\text{in}}}(y, z)$, from which $x'$ and $y'$ are inputs to a trusted third party, and $z_1$ and $z_2$ are some auxiliary output. The trusted party computes $(u', v') = f(x', y')$ and sends $u'$ to the first party and $v'$ to the second party. The two parties are now given the outputs $v'$ and $u'$ and the auxiliary inputs $z_1$ and $z_2$, respectively. The first party outputs $u = \overline{B_1^{\text{out}}}(u', z_1)$ while the second party outputs $v = \overline{B_2^{\text{out}}}(v', z_2)$. Note that if the first party is honest, we have $B_1^{\text{in}}(x, z) = (x, \perp)$ and $B_1^{\text{out}}(u', z_1) = u'$ and similarly for the second party.

Now, to show that a $g$-hybrid protocol $\Pi$ securely computes a functionality $f$, we have to show that anything an adversary can do in the real model can also be done in the ideal model.

**Definition 3 (Perfect Security).** *A $g$-hybrid protocol $\Pi$* securely computes $f$ perfectly *if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible in the real model for the protocol $\Pi$, 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*

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

It is sometimes not possible to achieve perfect security. The following definition captures the situation where the simulation has a (small) error $\varepsilon$, defined as the maximal statistical distance between the output distributions in the real and ideal model.

**Definition 4 (Statistical Security).** *A $g$-hybrid protocol $\Pi$* securely computes *$f$* with an error of at most $\varepsilon$ *if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible in the real model for the protocol $\Pi$, 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*

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

The statistical distance is used because it has nice properties and intuitively measures the error of a computation: a protocol $\Pi$ which securely computes $f$ with an error of at most $\varepsilon$, computes $f$ *perfectly* with probability at least $1-\varepsilon$.

A very important property of the above definitions is that they imply *sequential composition*. The following theorem has been proven in [10].

**Theorem 1.** *If an $h$-hybrid protocol $\Gamma$ securely computes $g$ with an error of at most $\gamma$ and a $g$-hybrid protocol $\Pi$ securely computes $f$ with an error of at most $\pi$, then the composed protocol $\Pi^\Gamma$, namely the protocol $\Pi$ where every call to $g$ is replaced by $\Gamma$, is an $h$-hybrid protocol that securely computes $f$ with an error of at most $\pi + t\gamma$, where $t$ is the number of calls of $\Pi$ to $g$.*

The following lemma shows that any protocol that is secure without auxiliary input, is also secure with auxiliary input.

**Lemma 1.** *If a $g$-hybrid protocol $\Pi$* securely computes *$f$* with an error $\varepsilon$ *with constant auxiliary input, then it securely computes $f$ with an error of at most $\varepsilon$.*

*Proof.* If both players are honest the auxiliary input is ignored and the lemma holds. Let player $i$ be malicious, and let him use the algorithm $\overline{A}_i$. Let $\overline{A}_i^z$ be equal to $\overline{A}_i$, but with the auxiliary input $z$ hard-wired into it. Since $\Pi$ securely computes $f$ with an error $\varepsilon$ with constant auxiliary input, there exists an algorithm $\overline{B}_i^z$, such that for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, 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. the the adversary that behaves as $\overline{B}_i^z$ on auxiliary input $z$. (Note that our computation model allows us to do that.) Obviously, we have for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $z \in \{0,1\}^*$, we have

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

Hence, $\Pi$ securely computes $f$ with an error of at most $\varepsilon$. □

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

## 3 Secure Function Evaluation from an Information-Theoretic Point of View

In this section, we adopt an information-theoretic view of the security definition. We change our notation slightly to make it more suitable to the information-theoretic domain. We let $X$, $Y$ and $Z$ be random variables denoting the inputs, distributed according to an unknown distribution. Likewise, we let $U$ and $V$ be random variables denoting the outputs of the two parties. Hence, for specific inputs $x, y, z$ we have

$$(U, V) = \text{REAL}^{g}_{\Pi,\overline{A}(z)}(x, y)$$

and

$$(\underline{U}, \underline{V}) = \text{IDEAL}_{f,\overline{B}(z)}(x, y) \ .$$

Note that the condition of Definition 3, namely that for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $z \in \{0,1\}^*$, we have

$$\text{IDEAL}_{f,\overline{B}(z)}(x, y) \equiv \text{REAL}^{g}_{\Pi,\overline{A}(z)}(x, y) \ ,$$

can equivalently be expressed as

$$P_{\underline{UV}|XYZ} = P_{UV|XYZ}.$$

We now state our main theorem. It gives an information-theoretic condition for the security of a real protocol, *without the use of an ideal model*. Intuitively, the security condition for player 1 (and its counterpart for player 2) expresses what a malicious player could do in the ideal model, namely, producing a value $Y'$ (only based on $Y$ and $Z$), send it to the ideal functionality, receive $V'$, and then calculate a value $V$ (only based on $Z$, $Y$, $Y'$ and $V'$). The condition $\text{I}(X; Y' \mid ZY) = 0$ ensures that $Y'$ is only based on $Z$ and $Y$, and not on $X$. The condition

$$P_{UV'|XY'YZ}(u, v' \mid x, y', y, z) = \Pr[(u, v') = f(x, y')]$$

ensures that the distributions of $U$ and $V'$ are the same as those of the outputs of $f$ on input $X$ and $Y'$. Finally, $\text{I}(UX; V \mid ZYY'V') = 0$ ensures that $V$ is only based on $Z$, $Y$, $Y'$ and $V'$, and not on $X$ and $U$.

**Theorem 2.** *A $g$-hybrid protocol $\Pi$* securely computes *$f$* with an error of at most *$\varepsilon$ if and only if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible in the real model for the protocol $\Pi$ and for all inputs $(X, Y)$ and auxiliary input $Z$, $\overline{A}$ produces outputs $(U, V)$, such that the following conditions are satisfied: There exists an event $\mathcal{E}$ with $\Pr[\mathcal{E}] \geq 1 - \varepsilon$, such that*

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

$$P_{UV|XYZ,\mathcal{E}}(u, v \mid x, y, z) = \Pr[(u, v) = f(x, y)] \ .$$

– (Security for Player 1) *If player* 1 *is honest, then there exist random variables* $Y'$ *and* $V'$ *such that we have*

$$\mathrm{I}(X; Y' \mid ZY, \mathcal{E}) = 0 \ ,$$

$$P_{UV'|XY'YZ,\mathcal{E}}(u, v' \mid x, y', y, z) = \Pr[(u, v') = f(x, y')] \ ,$$

*and*

$$\mathrm{I}(UX; V \mid ZYY'V', \mathcal{E}) = 0 \ .$$

– (Security for Player 2) *If player* 2 *is honest, then there exist random variables* $X'$ *and* $U'$*, such that we have*

$$\mathrm{I}(Y; X' \mid ZX, \mathcal{E}) = 0 \ ,$$

$$P_{U'V|X'YXZ,\mathcal{E}}(u', v \mid x', y, x, z) = \Pr[(u', v) = f(x', y)] \ ,$$

*and*

$$\mathrm{I}(VY; U \mid ZXX'U', \mathcal{E}) = 0 \ .$$

*Proof.* Let us first assume that the protocol $\Pi$ securely computes $f$ with an error of at most $\varepsilon$. Then there exists an admissible pair of algorithms $\overline{B} = (\overline{B}_1, \overline{B}_2)$ for the ideal model such that for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $z \in \{0,1\}^*$, we have

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

or equivalently, for all $x, y, z$, we have $\delta((\underline{U}, \underline{V}), (U, V)) \leq \varepsilon$, from which follows that there exists an event $\mathcal{E}$ with $\Pr[\mathcal{E}] = \varepsilon$, such that

$$P_{\underline{UV}|X=x,Y=y,Z=z,\mathcal{E}} = P_{UV|X=x,Y=y,Z=z,\mathcal{E}} \ .$$

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 $(\underline{U}, \underline{V}) = (\underline{U}', \underline{V}')$. Therefore, we have

$$P_{\underline{UV}|XYZ}(u, v \mid x, y, z) = \Pr[(u, v) = f(x, y)] \ ,$$

from which follows that

$$P_{UV|XYZ,\mathcal{E}}(u, v \mid x, y, z) = \Pr[(u, v) = f(x, y)] \ .$$

Without loss of generality, let player 1 be honest and player 2 be malicious. Let us look at the execution of $\overline{B} = (B_1, \overline{B}_2)$. The malicious $\overline{B}_2$ can be modeled by the two conditional probability distributions $P_{\underline{Y}'\underline{S}|YZ}$ computing the input to the ideal functionality and some internal data $\underline{S}$, and $P_{\underline{V}|\underline{V}'\underline{S}}$ computing the output. Note that we can write $P_{\underline{Y}'\underline{S}|YZ} = P_{\underline{Y}'|YZ} P_{\underline{S}|YZ\underline{Y}'}$, i.e., we can say that $\underline{Y}'$ is computed from $Y$ and $Z$, and that $\underline{S}$ is computed from $Y$, $Z$, and $\underline{Y}'$. Clearly, we have

$$\mathrm{I}(X; \underline{Y}' \mid ZY) = 0 \ .$$

The honest $B_1$ always sends $X$ to the trusted party, which computes $(\underline{U}', \underline{V}') = f(X, \underline{Y}')$ and sends the results to $B_1$ and $\overline{B}_2$. Since $B_1$ always outputs $\underline{U} = \underline{U}'$, we have

$$P_{\underline{U}\underline{V}'|X\underline{Y}'YZ}(u, v' \mid x, y', y, z) = \Pr[(u, v') = f(x, y')] \ .$$

$\overline{B}_2$'s output $\underline{V}$ only depends on $\underline{V}'$ and $\underline{S}$, which only depends on $Y$, $Z$ and $\underline{Y}'$. It follows that

$$\mathrm{I}(\underline{U}X; \underline{V} \mid ZY\underline{Y}'\underline{V}') = 0 \ .$$

Since

$$P_{\underline{U}\underline{V}|X=x,Y=y,Z=z,\mathcal{E}} = P_{UV|X=x,Y=y,Z=z,\mathcal{E}} \ ,$$

there must exist random variables satisfying the same properties, for the output of protocol $\Pi$ in the real model, if the event $\mathcal{E}$ occurs. Consequently, there must exist random variables $Y'$ and $V'$, such that

$$\mathrm{I}(X; Y' \mid ZY, \mathcal{E}) = 0 \ ,$$

$$P_{UV'|XY'YZ,\mathcal{E}}(u, v' \mid x, y', y, z) = \Pr[(u, v') = f(x, y')] \ ,$$

and

$$\mathrm{I}(UX; V \mid ZYY'V', \mathcal{E}) = 0 \ .$$

Now assume that the conditions of Theorem 2 hold. If both players are honest, the correctness condition implies $P_{UV|XYZ,\mathcal{E}} = P_{\underline{U}\underline{V}|XYZ,\mathcal{E}}$. If both players are malicious nothing needs to be shown. Without loss of generality, let player 1 be honest and player 2 be malicious. We will define an admissible protocol $\overline{B} = (B_1, \overline{B}_2)$ in the ideal model that produces the same distribution as the protocol $\Pi$ in the real model. Let $\overline{B}_2$ choose his input $\underline{Y}'$ according to $P_{\underline{Y}'|YZ} := P_{Y'|YZ}$, set $\underline{S} := YZ\underline{Y}'$ and let him choose his output $\underline{V}$ according to $P_{\underline{V}|YZ\underline{Y}'\underline{V}'} := P_{V|YZY'V'}$. The conditional distribution of the output in the ideal model is given by

$$P_{\underline{U}\underline{V}|XYZ} = \sum_{y',v'} P_{\underline{Y}'|YZ} P_{\underline{U}\underline{V}'|X\underline{Y}'} P_{\underline{V}|YZ\underline{Y}'\underline{V}'} \ ,$$

where

$$P_{\underline{U}\underline{V}'|X\underline{Y}'}(u, v' \mid x, y') = \Pr[(u, v') = f(x, y')] \ .$$

From $\mathrm{I}(X; Y' \mid ZY, \mathcal{E}) = 0$ and $\mathrm{I}(UX; V \mid ZYY'V', \mathcal{E}) = 0$ it follows that $P_{Y'|XYZ,\mathcal{E}} = P_{Y'|YZ,\mathcal{E}}$ and $P_{V|XYZY'UV',\mathcal{E}} = P_{V|YZY'V',\mathcal{E}}$. Furthermore, we have $P_{UV'|XY'YZ,\mathcal{E}} = P_{\underline{U}\underline{V}'|X\underline{Y}',\mathcal{E}}$. As for the conditional distribution of the output in the real model, we have:

$$\begin{aligned}
P_{UV|XYZ,\mathcal{E}} &= \sum_{y',v'} P_{Y'UV'|XYZ,\mathcal{E}} P_{V|XYZY'UV',\mathcal{E}} \\
&= \sum_{y',v'} P_{Y'|XYZ,\mathcal{E}} P_{UV'|XYZY',\mathcal{E}} P_{V|YZY'V',\mathcal{E}} \\
&= \sum_{y',v'} P_{\underline{Y}'|YZ,\mathcal{E}} P_{\underline{U}\underline{V}'|X\underline{Y}',\mathcal{E}} P_{\underline{V}|YZ\underline{Y}'\underline{V}',\mathcal{E}} \\
&= P_{\underline{U}\underline{V}|XYZ,\mathcal{E}} \ .
\end{aligned}$$

Therefore, for any admissible $\overline{A}$ in the real model there exists an admissible $\overline{B}$ in the ideal model such that

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

implying that the protocol is secure with an error of at most $\varepsilon$. □

Note that the expression

$$P_{UV'|XY'YZ}(u,v' \mid x,y',y,z) = \Pr[(u,v') = f(x,y')]$$

can be replaced by $(U,V') = f(X,Y')$ if $f$ is deterministic. This yields the following corollary for deterministic functionalities.

**Corollary 1.** *A protocol $\Pi$* securely computes the deterministic functionality $f$ with an error of at most $\varepsilon$, *if and only if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible in the real model for the protocol $\Pi$ and for all inputs $(X,Y)$ and auxiliary input $Z$, $\overline{A}$ produces outputs $(U,V)$, such that the following conditions are satisfied: There exists an event $\mathcal{E}$ with $\Pr[\mathcal{E}] \geq 1-\varepsilon$, such that*

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

$$\Pr[(U,V) = f(X,Y) \mid \mathcal{E}] = 1 \ .$$

- (Security for Player 1) *If player 1 is honest then there exists a random variable $Y'$ such that for $V'$ defined by $(U,V') = f(X,Y')$, it holds that*

$$\mathrm{I}(X;Y' \mid ZY,\mathcal{E}) = 0 \ , \qquad \textit{and} \qquad \mathrm{I}(UX;V \mid ZYY'V',\mathcal{E}) = 0 \ .$$

- (Security for Player 2) *If player 2 is honest then there exists a random variable $X'$ such that for $U'$ defined by $(U',V) = f(X',Y)$, it holds that*

$$\mathrm{I}(Y;X' \mid ZX,\mathcal{E}) = 0 \ , \qquad \textit{and} \qquad \mathrm{I}(VY;U \mid ZXX'U',\mathcal{E}) = 0 \ .$$

Note that we require the conditions of Theorem 2 and Corollary 1 to hold for all distributions of the inputs $(X,Y)$. In particular, they have to hold for any input distribution $P_{XY|Z=z}$, i.e., given the event that the auxiliary input $Z$ equals $z$. Since all the requirements are conditioned on $Z$, it is sufficient to show that the conditions are met for all distributions $P_{XY}$, ignoring $Z$ in all the expressions.

In information theory, the distance between distributions is sometimes expressed using bounds on entropy and mutual information instead of statistical distance. The following inequalities translate such bounds into bounds on statistical distance. Let $U$ be uniformly distributed over the set $\mathcal{X}$.

$$\delta(P_{XYZ}, P_Z P_{X|Z} P_{Y|Z}) \leq \frac{1}{2}\sqrt{2\ln 2\, \mathrm{I}(X;Y \mid Z)}$$

$$\delta(P_X, P_U) \leq \frac{1}{2}\sqrt{2\ln 2(\log|\mathcal{X}| - \mathrm{H}(X))}$$

The first inequality can easily be proved from [13], Lemma 16.3.1 while the second inequality was proved in [8], Lemma 3.4.

## 4 Oblivious Transfer

We now apply our security definition to 1-out-of-$n$ string oblivious transfer, or $\binom{n}{1}$-OT$^k$ for short. The ideal functionality $f_{\mathrm{OT}}$ 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 $\Pi$ securely computes $\binom{n}{1}$-OT$^k$ perfectly if and only if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible for protocol $\Pi$ and for all inputs $(X, C)$ and auxiliary input $Z$, $\overline{A}$ produces outputs $(U, V)$ such that the following conditions are satisfied:*

- (Correctness) *If both players are honest, then $(U, V) = (\perp, X_C)$.*
- (Security for Player 1) *If player 1 is honest, then we have $U = \perp$ and there exists a random variable $C'$, such that*

$$\mathrm{I}(X; C' \mid ZC) = 0 \,, \qquad \textit{and} \qquad \mathrm{I}(X; V \mid ZCC'X_{C'}) = 0 \,.$$

- (Security for Player 2) *If player 2 is honest, then we have*

$$\mathrm{I}(C; U \mid ZX) = 0 \,.$$

*Proof.* We only need to show that the security condition for player 2 is equivalent to the one in Corollary 1:

$$\mathrm{I}(C; X' \mid ZX) + \mathrm{I}(X'_C C; U \mid ZXX') = 0$$

Since $X'_C$ is a function of $C$ and $X'$,

$$\mathrm{I}(X'_C C; U \mid ZXX') = 0 \text{ is equivalent to } \mathrm{I}(C; U \mid ZXX') = 0 \,.$$

From the chain rule it follows that

$$\begin{aligned} \mathrm{I}(C; X' \mid ZX) + \mathrm{I}(C; U \mid ZXX') &= \mathrm{I}(C; X'U \mid ZX) \\ &= \mathrm{I}(C; U \mid ZX) + \mathrm{I}(C; X' \mid ZXU) \,. \end{aligned}$$

Now choose $X' = (X'_0, \ldots, X'_{n-1})$ as follows: for all values $i$, let $X'_i$ be chosen according to the distribution $P_{V|ZXU,C=i}$ except for $X'_C$. We set $X'_C = V$. Note that all $X'_i$, $0 \le i \le n-1$, have distribution $P_{V|ZXU,C=i}$. Thus $X'$ does not depend on $C$ given $ZXU$, we have $V = X'_C$ and $\mathrm{I}(C; X' \mid ZXU) = 0$. So there always exists a suitable $X'$ [5], and the condition simplifies to $\mathrm{I}(C; U \mid ZX) = 0$. □

[5] Note that these values $X'$ are not necessarily known to a malicious player 1.

*Proof.* We only need to show that the security condition for player 2, i.e, where player 1 is honest and player 2 may be malicious, is equivalent to the one in Corollary 1.

Let us first assume that the protocol $\Pi$ securely computes $f$. Then there exists an admissible pair of algorithms $\overline{B} = (\overline{B}_1, \overline{B}_2)$ for the ideal model such that for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $z \in \{0,1\}^*$, we have

$$\text{IDEAL}_{f,\overline{B}(z)}(x,y) \equiv \text{REAL}^{g}_{\Pi,\overline{A}(z)}(x,y) \ ,$$

or equivalently,

$$P_{\underline{UV}|XYZ} = P_{UV|XYZ}.$$

The malicious $\overline{B}_2$ can be modeled by the conditional probability distributions $P_{\underline{UX}'|XZ} = P_{\underline{U}|XZ} P_{\underline{X}'|XZ\underline{U}}$ computing the input to the ideal functionality $\underline{X}'$ and the output $\underline{U}$. Clearly, we have

$$\mathrm{I}(C; \underline{U} \mid ZX) = 0 \ .$$

Since the probability distributions $P_{UV|XCZ}$ and $P_{\underline{UV}|XCZ}$ are identical, we also have

$$\mathrm{I}(C; U \mid ZX) = 0 \ .$$

Now assume that the conditions of Theorem 2 hold. We will define an admissible protocol $\overline{B} = (B_1, \overline{B}_2)$ in the ideal model that produces the same distribution as the protocol $\Pi$ in the real model. Let $\overline{B}_2$ choose his input output $\underline{U}$ according to $P_{\underline{U}|XZ} := P_{U|XZ}$, and he chooses input $\underline{X}'_i$ according to $P_{\underline{X}'_i|XZ\underline{U}} := P_{V|XZU,C=i}$. Note that since we have $\underline{V} = \underline{X}'_C$, this implies that

$$\sum_{\underline{x}'} P_{\underline{X}'|XZ\underline{U}} P_{V|\underline{X}'C} = P_{V|XZUC} \ .$$

From $\mathrm{I}(C; U \mid ZX) = 0$ follows that $P_{U|XZC} = P_{U|XZ}$. Hence, we have

$$\begin{aligned} P_{\underline{UV}|XCZ} &= \sum_{x'} P_{\underline{U}|XZ} P_{\underline{X}'|XZ\underline{U}} P_{V|\underline{X}'C} \\ &= P_{U|XZ} \sum_{x'} P_{\underline{X}|XZ\underline{U}} P_{V|\underline{X}'C} \\ &= P_{U|XZC} P_{V|XZUC} \\ &= P_{UV|XCZ} \ . \end{aligned}$$

Therefore, for any admissible $\overline{A}$ in the real model there exists an admissible $\overline{B}$ in the ideal model such that

$$\text{IDEAL}_{f,\overline{B}(z)}(x,y) \equiv \text{REAL}^{g}_{\Pi,\overline{A}(z)}(x,y) \ ,$$

implying that the protocol is perfectly secure. □

The interpretation of these properties of oblivious transfer is quite intuitive: If player 1 is honest, then she can be confident that anything player 2 can do is basically equivalent to choosing a choice bit $C'$ which is possibly different from $C$. On the other hand, if player 2 is honest, he can be certain that player 1 does not get to know his input $C$. Theorem 3 shows that in the case of a dishonest sender in $\binom{n}{1}$-$\mathrm{OT}^k$, *privacy alone implies security.* There *always* exists an input $X'$ that a dishonest sender can use in the ideal model to obtain the same results.

## 5 Rabin OT

The ideal functionality $f$ is defined as

$$f(X) := (\perp, V) \,,$$

where $\perp$ denotes a constant random variable, $X \in \{0,1\}^k$, and $V = (W, C) \in \{0,1\}^k \times \{0,1\}$, where $\mathrm{H}(C \mid X) = 1$ and $W = X$ if $C = 1$ and $W = \perp$ if $C = 0$.

**Theorem 4.** *A protocol $\Pi$ securely computes Rabin-OT perfectly if and only if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible for protocol $\Pi$ and for all inputs $X$ and auxiliary input $Z$, $\overline{A}$ produces outputs $(U, V)$ such that the following conditions are satisfied:*

- (Correctness) *If both players are honest, then $(U, V) = f(X)$.*
- (Security for Player 1) *If player 1 is honest, then we have $U = \perp$ and there exists a random variable $C'$, such that*

$$\mathrm{H}(C' \mid XZ) = 1 \,, \qquad \textit{and} \qquad \mathrm{I}(X; V \mid Z, C' = 0) = 0 \,.$$

- (Security for Player 2) *If player 2 is honest, then we have*

$$\mathrm{H}(C \mid XUZ) = 1 \,.$$

*Proof.* Security for Player 1: The condition of Theorem 2 tells us that $U = \perp$ and there must exist $V' = (W', C')$, such that $\mathrm{H}(C' \mid XZ) = 1$, and $W' = X$ if $C' = 1$ and $W' = \perp$ if $C' = 0$, and

$$\mathrm{I}(X; V \mid ZW'C') = 0 \,.$$

Now, if $C' = 1$, that condition always holds, since $W' = X$. For $C' = 0$, $W'$ is a constant and we get

$$\mathrm{I}(X; V \mid Z, C' = 0) = 0 \,.$$

Security for Player 2: Player 1 does not have any output and player 2 does not have any input. The conditions of Theorem 2 tell us that there must exist a $X'$, such that $\mathrm{H}(C \mid XX'Z) = 1$, and $W = X$ if $C = 1$ and $W = \perp$ if $C = 0$, and

$$\mathrm{I}(WC; U \mid ZXX') = 0 \,. \tag{1}$$

We choose $X' := W$, if $C = 1$, and sample $X'$ according to the distribution $P_{W|XUZ,C=1}$, if $C = 0$. We have $P_{X'|XUZC} = P_{X'|XUZ}$, from which follows that

$$\mathrm{I}(X'; C \mid XUZ) = 0 \,,$$

and therefore

$$\mathrm{H}(C \mid XX'UZ) = \mathrm{H}(C \mid XUZ) \,.$$

It follows that

$$\mathrm{H}(C \mid XX'Z) \geq \mathrm{H}(C \mid XX'UZ) = \mathrm{H}(C \mid XUZ) = 1.$$

Condition (1) is equivalent to

$$\mathrm{I}(C; U \mid ZXX') = 0 \qquad \text{and} \qquad \mathrm{I}(W; U \mid ZXX'C) = 0 \,.$$

Since $I(C; U \mid ZXX') = \mathrm{H}(C \mid XX'Z) - \mathrm{H}(C \mid XX'UZ) = \mathrm{H}(C \mid XX'Z) - \mathrm{H}(C \mid XUZ) \geq 0$, the first condition is implied by $\mathrm{H}(C \mid XUZ) = 1$. The second condition always holds for our choice of $X'$, because in the case $C = 1$, we have set $X' = W$ and for $C = 0$, $W$ is constant. □

## 6 An Example

In this section we show how the result from Section 4 can be used to prove the security of a protocol. Our example will be the protocol from [30], where one instance of $\binom{2}{1}$-OT is implemented using one instance of $\binom{2}{1}$-TO, which is an instance of $\binom{2}{1}$-OT in the opposite direction.

**Protocol 1 ([30])** *Let player 1 have input $X = (X_0, X_1) \in \{0,1\} \times \{0,1\}$, and player 2 have input $C \in \{0,1\}$.*

1. *Player 2 chooses $R \in \{0,1\}$ at random.*
2. *The two players execute $\binom{2}{1}$-TO, where player 1 inputs $\underline{C} = X_0 \oplus X_1$, and player 2 inputs $\underline{X}_0 = R$ and $\underline{X}_1 = R \oplus C$.*
3. *Player 1 receives $A = \underline{X}_C$ and sends $M = X_0 \oplus A$ to the player 2.*
4. *Player 1 outputs $V := R \oplus M$.*

**Theorem 5.** *Protocol 1 perfectly securely reduces $\binom{2}{1}$-OT to one realization of $\binom{2}{1}$-TO.*

*Proof.* If both parties are honest, the protocol is correct because we have

$$R \oplus M = R \oplus X_0 \oplus (X_0 \oplus X_1)C \oplus R = X_C \,.$$

Let player 1 be honest, and let $C' := \underline{X}_0 \oplus \underline{X}_1$. Using the data processing inequality,

$$\mathrm{I}(X_0X_1; C' \mid ZC) \leq \mathrm{I}(X_0X_1; \underline{X}_0\underline{X}_1 \mid ZC) \leq \mathrm{I}(X_0X_1; ZC \mid ZC) = 0 \,.$$

Since $M = X_0 \oplus (X_0 \oplus X_1)(\underline{X}_0 \oplus \underline{X}_1) \oplus \underline{X}_0 = X_{C'} \oplus \underline{X}_0$, the values $\underline{X}_0\underline{X}_1 M$, $\underline{X}_0 C' M$, and $\underline{X}_0 C' X_{C'}$ contain the same information. Thus, using the data processing inequality,

$$\begin{aligned} \mathrm{I}(X_0X_1; V \mid ZCC'X_{C'}) &\leq \mathrm{I}(X_0X_1; CZ\underline{X}_0\underline{X}_1 M \mid ZCC'X_{C'}) \\ &= \mathrm{I}(X_0X_1; CZ\underline{X}_0 C'X_{C'} \mid ZCC'X_{C'}) = 0 \,. \end{aligned}$$

Now let player 2 be honest. Since $A = R \oplus C\underline{C}$ and $R$ is uniform, we have

$$\mathrm{I}(C; U \mid ZX_0X_1) \leq \mathrm{I}(C; X_0X_1ZA \mid ZX_0X_1) = \mathrm{I}(C; A \mid ZX_0X_1) = 0 \,.$$

Thus, the protocol is secure. □

## 7 Secure Two-Party Computation with Abort

In this section we will briefly discuss the model of Definition 7.2.6 of [21] where the first party is allowed to abort the protocol right after receiving its output but before the second party has received its own. The *ideal model with abort for player* 1 is similar to the ideal model from Definition 2, the only difference being that player 1 is given the option of aborting the computation by sending a bit $C$ to the trusted party after having received his output. The trusted party sends to player 2 the corresponding output if $C = 1$, and $\perp$ if $C = 0$. An honest player always sends $C = 1$. The real model and the definition of security are identical to the definition without abort. We call a protocol that satisfies this definition *secure with abort for player* 1.

**Theorem 6.** *A $g$-hybrid protocol $\Pi$* securely computes *$f$* perfectly with abort for player 1*, if and only if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible in the real model for the protocol $\Pi$, and for all inputs $(X, Y)$ and auxiliary input $Z$, $\overline{A}$ produces outputs $(U, V)$, such that the following conditions are satisfied:*

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

$$P_{UV|XYZ}(u, v \mid x, y, z) = \Pr[(u, v) = f(x, y)] \,.$$

- (Security for Player 1) *If player* 1 *is honest, then there exist random variables $Y'$ and $V'$, such that we have*

$$\mathrm{I}(X; Y' \mid ZY) = 0 \,,$$

$$P_{UV'|XY'YZ}(u, v' \mid x, y', y, z) = \Pr[(u, v') = f(x, y')] \,,$$

*and*

$$\mathrm{I}(UX; V \mid ZYY'V') = 0 \,.$$

– (Security for Player 2) *If player* 2 *is honest, then there exist random variables* $X', C$ *and* $U', V'$*, such that we have*

$$\mathrm{I}(Y; X' \mid ZX) = 0 \,,$$

$$P_{U'V'|X'YXZ}(u', v' \mid x', y, x, z) = \Pr[(u', v') = f(x', y)] \,,$$

$$\mathrm{I}(V'Y; UC \mid ZXX'U') = 0 \,,$$

*and* $V = V'$ *if* $C = 1$ *and* $V = \perp$ *if* $C = 0$*.*

*Proof.* The proof is identical to that of Theorem 2 for the case where player 1 is honest. We therefore only examine the case where player 2 is honest and player 1 is malicious.

Let us assume that the protocol $\Pi$ securely computes $f$. Consequently, there exists an admissible pair of algorithms $\overline{B} = (\overline{B}_1, B_2)$ such that for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, and $z \in \{0,1\}^*$ we have $P_{UV|XYZ} = P_{\underline{UV}|XYZ}$.

The malicious $\overline{B}_1$ can be modeled by the two conditional probability distributions $P_{\underline{X}'\underline{S}|XZ}$ computing the input to the ideal functionality and some internal data $\underline{S}$, and $P_{\underline{UC}|\underline{U}'\underline{S}}$ computing the output $\underline{U}$ and the bit $\underline{C}$. Note that we can write $P_{\underline{X}'\underline{S}|XZ} = P_{\underline{X}'|XZ} P_{\underline{S}|XZ\underline{X}'}$. Clearly, we have

$$\mathrm{I}(Y; \underline{X}' \mid ZX) = 0 \,.$$

The ideal functionality computes $\underline{U}', \underline{V}'$ such that

$$P_{\underline{U}'\underline{V}'|\underline{X}'YXZ}(u', v' \mid x', y, x, z) = \Pr[(u', v') = f(x', y)] \,.$$

$B_1$ gets back $\underline{U}'$ from the ideal functionality. Based on $X, Z, \underline{X}', \underline{U}'$ he decides to send $\underline{C}$ to the functionality and outputs $\underline{U}$. Hence, we have

$$\mathrm{I}(\underline{V}'Y; \underline{UC} \mid XZ\underline{X}'\underline{U}') = 0 \,.$$

If $C = 1$, the functionality sends $\underline{V} = \underline{V}'$ to $B_2$, if $C = 0$ it sends $\underline{V} = \perp$. $B_2$ outputs $\underline{V}$ unchanged. As $P_{UV|XYZ} = P_{\underline{UV}|XYZ}$ it must be the case that the same conditions hold in the real model, which implies the security condition for player 2.

Now let the conditions of Theorem 6 hold. We define an admissible protocol $\overline{B} = (\overline{B}_1, B_2)$ in the ideal model that produces the same distribution as the protocol $\Pi$ in the real model. Let $\overline{B}_1$ choose input $\underline{X}'$ according to $P_{\underline{X}'|XZ} := P_{X'|XZ}$, and $(\underline{U}, \underline{C})$ according to $P_{\underline{UC}|XZ\underline{X}'\underline{U}'} := P_{UC|XZX'U'}$. The conditional distribution of the output in the ideal model is given by

$$P_{\underline{UV}|XYZ} = \sum_{x', c, u', v'} P_{\underline{X}'|XZ} P_{\underline{U}'\underline{V}'|\underline{X}'Y} P_{\underline{UC}|XZ\underline{X}'\underline{U}'} P_{\underline{V}|\underline{V}'\underline{C}} \,,$$

where

$$P_{\underline{U}'\underline{V}'|\underline{X}'Y}(u', v' \mid x', y) = \Pr[(u', v') = f(x', y)] \,.$$

From $\mathrm{I}(Y; X' \mid ZX) = 0$ and $\mathrm{I}(V'Y; UC \mid XZX'U') = 0$ it follows that $P_{X'|XYZ} = P_{X'|XZ}$ and $P_{UC|XZX'U'V'Y} = P_{UC|XZX'U'}$. Furthermore, we have $P_{U'V'|X'YXZ} = P_{\underline{U}'\underline{V}'|\underline{X}'Y}$ and $P_{V|V'C} = P_{\underline{V}|\underline{V}'\underline{C}}$. We get for the conditional distribution of the output in the real model

$$\begin{aligned}
P_{UV|XYZ} &= \sum_{x',c,u',v'} P_{X'|XYZ} P_{U'V'|XYZX'} P_{UCV|XYZX'U'V'} \\
&= \sum_{x',c,u',v'} P_{X'|XZ} P_{\underline{U}'\underline{V}'|\underline{X}'Y} P_{UC|XYZX'U'V'} P_{V|XYZX'U'V'CU} \\
&= \sum_{x',c,u',v'} P_{X'|XZ} P_{\underline{U}'\underline{V}'|\underline{X}'Y} P_{UC|XZX'U'} P_{V|V'C} \\
&= \sum_{x',c,u',v'} P_{\underline{X}'|XZ} P_{\underline{U}'\underline{V}'|\underline{X}'Y} P_{\underline{UC}|XZ\underline{X}'\underline{U}'} P_{\underline{V}|\underline{V}'\underline{C}} \\
&= P_{\underline{UV}|XYZ} \ .
\end{aligned}$$

Therefore for any admissible $\overline{A}$ in the real model there exists an admissible $\overline{B}$ in the ideal model such that

$$\textsc{ideal}_{f,\overline{B}(z)}(x,y) \equiv \textsc{real}^{g}_{\Pi,\overline{A}(z)}(x,y) \ ,$$

which means that the protocol is perfectly secure with abort for player 1. □

## 8 Randomized Variants of Oblivious Transfer

Many information-theoretic constructions for $\binom{n}{1}$-$\mathrm{OT}^k$ implicitly build on randomized variants of $\binom{n}{1}$-$\mathrm{OT}^k$, such as *sender-randomized 1-out-of-n string OT*, $\binom{n}{1}$-$\mathrm{ROT}^k$, or *1-out-of-n string oblivious key*, $\binom{n}{1}$-$\mathrm{ROTR}^k$. In $\binom{n}{1}$-$\mathrm{ROT}^k$, instead of $X$ being given to player 1 as *input*, it is randomly generated in the course of the protocol and becomes part of player 1's *output*. In $\binom{n}{1}$-$\mathrm{ROTR}^k$, the players have no input and both $X$ and $C$ are randomized outputs.

The reductions of $\binom{n}{1}$-$\mathrm{OT}^k$ to $\binom{n}{1}$-$\mathrm{ROT}^k$ and $\binom{n}{1}$-$\mathrm{ROT}^k$ to $\binom{n}{1}$-$\mathrm{ROTR}^k$ are well known. We will state formal security requirements for $\binom{n}{1}$-$\mathrm{ROT}^k$ and $\binom{n}{1}$-$\mathrm{ROTR}^k$ and proof that they are sufficient to implement secure $\binom{n}{1}$-$\mathrm{OT}^k$. Note that unlike in the previous sections, these requirements are *not* linked to any ideal functionalities.

### 8.1 Reducing OT to Sender-Randomized OT

In a protocol $\Pi$ for $\binom{n}{1}$-$\mathrm{ROT}^k$, honest player 1 has no input and outputs $U = (U_0, \ldots, U_{n-1})$ where $U_i \in \{0,1\}^k$ for $i \in \{0, \ldots, n-1\}$, whereas honest player 2 has input $C \in \{0, \ldots, n-1\}$ and output $V = U_C$.

**Definition 5.** *A protocol $\Pi$* securely computes $\binom{n}{1}$-ROT$^k$*, if and only if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible for protocol $\Pi$ and for all inputs $C$ for player 2 and auxiliary input $Z$, $\overline{A}$ produces outputs $(U, V)$ such that the following conditions are satisfied:*

- (Correctness) *If both players are honest, then $U = (U_0, \ldots, U_{n-1})$ and $V = U_C$.*
- (Security for Player 1) *If player 1 is honest, then there exists a random variable $C' \in \{0, \ldots, n-1\}$, such that $U = (U_0, \ldots, U_{n-1})$ and*

$$P_{U_0 \cdots U_{C'-1}, U_{C'+1} \cdots U_{n-1} | ZCC'U_{C'}V}$$

  *is uniformly distributed.*
- (Security for Player 2) *If player 2 is honest, then we have* $\mathrm{I}(C; U \mid Z) = 0$.

A protocol implementing $\binom{n}{1}$-ROT$^k$ can be used to build secure $\binom{n}{1}$-OT$^k$ using the following reduction:

**Protocol 2 (Reduction of $\binom{n}{1}$-OT$^k$ to $\binom{n}{1}$-ROT$^k$)** *Let player 1 have input $X = (X_0, \ldots X_{n-1})$, and player 2 have input $C \in \{0, \ldots, n-1\}$.*

1. *The two players execute $\binom{n}{1}$-ROT$^k$, where player 2 inputs $C$. Player 1 gets $U^* = (U_0^*, \ldots U_{n-1}^*)$, player 2 gets $U_C^*$.*
2. *For all $i \in \{0, \ldots n-1\}$, player 1 sends to player 2 $S_i := X_i \oplus U_i^*$.*
3. *Player 1 outputs $\perp$ and player 2 outputs $V := S_C \oplus U_C^*$.*

**Theorem 7.** *Protocol 2 securely reduces $\binom{n}{1}$-OT$^k$ to $\binom{n}{1}$-ROT$^k$.*

*Proof.* We superscript the random variables used in $\binom{n}{1}$-ROT$^k$ with $*$, e.g. $Z^*$ is the auxiliary input to $\binom{n}{1}$-ROT$^k$, whereas $Z$ is the auxiliary input to $\binom{n}{1}$-OT$^k$.

If both players are honest, then we have $U = \perp$ and $V = S_C \oplus U_C^* = X_C \oplus U_C^* \oplus U_C^* = X_C$, from which correctness follows.

If player 1 is honest, there exists a random variable $C'^*$ such that player 1 gets $U^* = (U_0^*, \ldots, U_{n-1}^*)$ and

$$P_{U_0^* \cdots U_{C'^*-1}^*, U_{C'^*+1}^* \cdots U_{n-1}^* | Z^* C'^* V^* U_{C'^*}^*}$$

is uniformly distributed for $Z^* := (Z, C)$. We set $C' := C'^*$ and have

$$\mathrm{I}(X; V^* C' U^* \mid ZC) = 0, \tag{2}$$

since honest player 1 is not using his knowledge of $X$ in $\binom{n}{1}$-ROT$^k$. This implies

$$\mathrm{I}(X; C' \mid ZC) = 0, \tag{3}$$

and

$$\mathrm{I}(X; V^* U_{C'}^* \mid ZCC' X_{C'}) = 0. \tag{4}$$

Dishonest player 2's output $V$ is computed based on $Z, C, V^*$ and

$$S = (S_0, \ldots, S_{n-1}) = (X_0 \oplus U_0^*, \ldots, X_{n-1} \oplus U_{n-1}^*).$$

Because of (2),

$$P_{U_0^* \cdots U_{C'-1}^*, U_{C'+1}^* \cdots U_{n-1}^* | ZCC' X_{C'} V^* U_{C'}^*}$$

is uniformly distributed. So, all $S_i$ except $S_{C'}$ are independent of $X_i$ given $ZCC'X_{C'}V^*U_{C'}^*$, and it holds that $S_{C'} = X_{C'} \oplus U_{C'}^*$. Therefore, we have

$$\mathrm{I}(X; S_0, \ldots, S_{n-1} \mid ZCC'X_{C'}V^*U_{C'}^*) = 0.$$

Combining this with (4) using the chain rule yields $\mathrm{I}(X; V^*S \mid ZCC'X_{C'}) = 0$ and hence

$$\mathrm{I}(X; V \mid ZCC'X_{C'}) = 0.$$

The security for player 1 follows together with (3).

If player 2 is honest, we have $\mathrm{I}(C; U^* \mid Z^*) = 0$ for $Z^* = (X, Z)$. Dishonest player 1's output $U$ is computed based on $U^*, Z$ and $X$, from which it follows that $\mathrm{I}(C; U \mid ZX) = 0$. □

### 8.2 Reducing Sender-Randomized OT to (Fully) Randomized OT

In a protocol $\Pi$ for $\binom{n}{1}$-ROTR$^k$, honest player 1 has no input and outputs $U = (U_0, \ldots, U_{n-1})$ where $U_i \in \{0,1\}^k$ for $i \in \{0, \ldots, n-1\}$, and honest player 2 has no input and outputs $V = (C, U_C)$, where $C \in \{0, \ldots, n-1\}$.

**Definition 6.** *A protocol $\Pi$* securely computes *$\binom{n}{1}$-ROTR$^k$, if for every pair of algorithms $\overline{A} = (\overline{A}_1, \overline{A}_2)$ that is admissible for protocol $\Pi$ and for all auxiliary input $Z$, $\overline{A}$ produces outputs $(U, V)$ such that the following conditions are satisfied:*

- (Correctness) *If both players are honest, then $U = (U_0, \ldots, U_{n-1})$ and $V = (U_C, C)$.*
- (Security for Player 1) *If player 1 is honest, then there exists a random variable $C' \in \{0, \ldots, n-1\}$, such that $U = (U_0, \ldots, U_{n-1})$ and*

  $$P_{U_0 \cdots U_{C'-1}, U_{C'+1} \cdots U_{n-1} | ZC' U_{C'} V}$$

  *is uniformly distributed.*
- (Security for Player 2) *If player 2 is honest, then $P_{C|ZU}$ is uniformly distributed.*

We want to show that the requirements for $\binom{n}{1}$-ROTR$^k$ are sufficient to implement $\binom{n}{1}$-OT$^k$. However, since we have already shown how to implement $\binom{n}{1}$-OT$^k$ from $\binom{n}{1}$-ROT$^k$, we only need to show that a protocol implementing $\binom{n}{1}$-ROTR$^k$ can be used to build secure $\binom{n}{1}$-ROT$^k$. This is achieved by the following reduction:

**Protocol 3 (Reduction of $\binom{n}{1}$-ROT$^k$ to $\binom{n}{1}$-ROTR$^k$)** *Let player 2 have input $C \in \{0, \ldots, n-1\}$. Player 1 has no input.*

1. *The two players execute $\binom{n}{1}$-ROTR$^k$. Player 1 gets $U^* = (U_0^*, \ldots U_{n-1}^*)$, player 2 gets $(U_{C^*}^*, C^*)$.*
2. *Player 2 sends to player 1 $M := (C^* - C) \mod n$.*
3. *Player 1 outputs $U = (U_M^*, \ldots U_{(M+n) \mod n}^*)$ and player 2 outputs $V := U_{C^*}^*$.*

**Theorem 8.** *Protocol 3 securely reduces $\binom{n}{1}$-ROT$^k$ to $\binom{n}{1}$-ROTR$^k$.*

*Proof.* We superscript the random variables used in $\binom{n}{1}$-ROTR$^k$ with $*$, e.g. $Z^*$ is the auxiliary input to $\binom{n}{1}$-ROTR$^k$, whereas $Z$ is the auxiliary input to $\binom{n}{1}$-ROT$^k$.

If both players are honest, then we have $U = (U_M^*, \ldots U_{(M+n) \mod n}^*)$ and $V = U_{C^*}^* = U_{(C^*-M) \mod n} = U_C$, from which correctness follows.

If player 1 is honest, there exists a random variable $C'^*$ such that player 1 gets $U^* = (U_0^*, \ldots, U_{n-1}^*)$ and

$$P_{U_0^* \cdots U_{C'^*-1}^*, U_{C'^*+1}^* \cdots U_{n-1}^* | Z^* C'^* V^* U_{C'^*}^*}$$

is uniformly distributed for $Z^* := (Z, C)$. We set $C' := (C'^* - M) \mod n$. Since $U_i = U_{(i+M) \mod n}^*$, and hence $U_{C'} = U_{C'^*}^*$, we have

$$P_{U_0 \cdots U_{C'-1}, U_{C'+1} \cdots U_{n-1} | Z C C' V U_{C'}}.$$

is uniformly distributed as well. If player 2 is honest, $P_{C^* | Z^* U^*}$ is uniformly distributed. Since $M = (C^* - C) \mod n$, $M$ is independent of $C$, given $Z^*$ and $U^*$. We can choose $Z^* := Z$ and get that $\mathrm{I}(C; U \mid Z) = 0$. □

## 9 Conclusion and Open Problems

We have shown that various information-theoretic security definitions for oblivious transfer used in the past contain subtle flaws. We propose a new information-theoretic security definition which is provably equivalent to the security definition based on the real/ideal model paradigm. This not only provides a solid security foundation for most protocols in the literature, which turn out to meet our requirements, but also shows that they are in fact sequentially composable.

An interesting open problem is to generalize our model to various quantum settings, for example to the scenario where two players connected by a quantum channel wish to securely implement a classical functionality.

## 10 Acknowledgments

We thank Abdul Ahsan, Serge Fehr and Stefan Wolf for many helpful discussions and the anonymous referees for their comments.

## References


1. M. Backes, B. Pfitzmann, and M. Waidner. A universally composable cryptographic library. Cryptology ePrint Archive, Report 2003/015, 2003.
2. D. Beaver. Foundations of secure interactive computing. In *Advances in Cryptology: CRYPTO '91*, pages 377–391, London, UK, 1992. Springer-Verlag.
3. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 1–10. Springer-Verlag, 1988.
4. Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 15(1):23–27, 1983.
5. C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson. New results on unconditionally secure distributed oblivious transfer. In *SAC '02: Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography*, pages 291–309, London, UK, 2003. Springer-Verlag.
6. G. Brassard, C. Crépeau, and M. Santha. Oblivious transfers and intersecting codes. *IEEETIT: IEEE Transactions on Information Theory*, 42, 1996.
7. G. Brassard, C. Crépeau, and S. Wolf. Oblivious transfers and privacy amplification. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(4):219–237, 2003.
8. C. Cachin. *Entropy Measures and Unconditional Security in Cryptography*. PhD thesis, No. 12187, ETH Zurich, Switzerland, 1997.
9. R. Canetti. *Studies in Secure Multiparty Computation and Applications*. PhD thesis, Weizmann Instituite of Science, Israel, 1996.
10. R. Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, 2000.
11. R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. Cryptology ePrint Archive, Report 2000/067, 2000.
12. D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 11–19. ACM Press, 1988.
13. T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley-Interscience, New York, USA, 1991.
14. C. Crépeau. Verifiable disclosure of secrets and applications (abstract). In *Advances in Cryptology: EUROCRYPT '89*, Lecture Notes in Computer Science, pages 181 – 191. Springer-Verlag, 1990.
15. C. Crépeau, J. van de Graaf, and A. Tapp. Committed oblivious transfer and private multi-party computation. In *Advances in Cryptology: CRYPTO '95*, Lecture Notes in Computer Science, pages 110–123, 1995.
16. Claude Crépeau, George Savvides, Christian Schaffner, and Jürg Wullschleger. Information-theoretic conditions for two-party secure function evaluation. In *Advances in Cryptology: EUROCRYPT '06*, Lecture Notes in Computer Science, pages 538–554. Springer-Verlag, 2006.
17. P. D'Arco and D. R. Stinson. Generalized zig-zag functions and oblivious transfer reductions. In *SAC '01: Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, pages 87–102, London, UK, 2001. Springer-Verlag.
18. Y. Ding, D. Harnik, A. Rosen, and R. Shaltiel. Constant-round oblivious transfer in the bounded storage model. In *In Theory of Cryptography — TCC '04*, volume 2951. Springer-Verlag, 2004.

19. Y. Dodis and S.Micali. Lower bounds for oblivious transfer reductions. In *Advances in Cryptology: EUROCRYPT '97*, 1999.
20. S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, 1985.
21. O. Goldreich. *Foundations of Cryptography*, volume II: Basic Applications. Cambridge University Press, 2004.
22. O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC '87)*, pages 218–229. ACM Press, 1987.
23. S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.
24. J. Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 20–31, 1988.
25. J. Kilian. More general completeness theorems for secure two-party computation. In *STOC*, pages 316–324, 2000.
26. S. Micali and P. Rogaway. Secure computation (abstract). In *Advances in Cryptology: CRYPTO '91*, pages 392–404, London, UK, 1992. Springer-Verlag.
27. V. Nikov, S. Nikova, B. Preneel, and J. Vandewalle. On unconditionally secure distributed oblivious transfer. In *Progress in Cryptology - INDOCRYPT 2002*, pages 395–408, 2002.
28. M. O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.
29. S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.
30. S. Wolf and J. Wullschleger. Oblivious transfer is symmetric. In *Advances in Cryptology: EUROCRYPT '06*, Lecture Notes in Computer Science. Springer-Verlag, 2006.
31. A. C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science (FOCS '82)*, pages 160–164, 1982.