entropy

MDPI

Article

On the Composability of Statistically Secure Random Oblivious Transfer

Rafael Dowsley [1,*], Jörn Müller-Quade [2,*] and Anderson C. A. Nascimento [3,*]

1 Department of Computer Science, Bar-Ilan University, Ramat Gan 5290002, Israel
2 Institute of Theoretical Informatics, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany
3 School of Engineering & Technology, University of Washington Tacoma, Tacoma, WA 98402, USA
* Correspondence: rafael@dowsley.net (R.D.); mueller-quade@kit.edu (J.M.-Q.); andclay@uw.edu (A.C.A.N.)

Received: 11 December 2019; Accepted: 10 January 2020; Published: 16 January 2020

check for updates

Abstract: We show that random oblivious transfer protocols that are statistically secure according to a definition based on a list of information-theoretical properties are also statistically universally composable. That is, they are simulatable secure with an unlimited adversary, an unlimited simulator, and an unlimited environment machine. Our result implies that several previous oblivious transfer protocols in the literature that were proven secure under weaker, non-composable definitions of security can actually be used in arbitrary statistically secure applications without lowering the security.

Keywords: random oblivious transfer; unconditional security; universal composability

1. Introduction

Oblivious transfer (OT) [1] is a primitive of central importance in modern cryptography and implies secure computation [2,3]. Several flavors of OT were proposed, but they are all equivalent [4]. In this work, we focus on the so-called one-out-of-two random oblivious transfer. This is a two-party primitive in which a sender (Alice) gets two uniformly random bits b_0, b_1 and a receiver (Bob) gets a uniformly random choice bit c and b_c. Bob remains ignorant about $b_{\overline{c}}$. On the other hand, Alice cannot learn the choice bit c.

Many OT protocols are known, based on various assumptions (both computational and physical) and achieving diverse notions of security. However, weaker security notions do not guarantee security when multiple copies of the protocol are executed, or when the OT protocols are used as building blocks within other protocols. This is an unsatisfactory state of affairs, as the major utility of OT is in the modular designing of larger protocols. Following the simulation paradigm used in [5] to define the seminal notion of zero-knowledge proofs of knowledge, many simulation-based definitions of security for multi-party protocols were proposed (e.g., [2,6]) and they guarantee that the protocols are sequentially composable [7]; however, this paradigm of security does not guarantee general composability of the protocols. UC-security [8] emerges as a very desirable notion of security for OT since it guarantees that the security of the protocol holds even when the OT scheme is concurrently composed with an arbitrary set of protocols. UC-security is a very powerful notion of security that allows to fully enjoy the nice properties of OT within other protocols.

Some questions about the equivalence of list-based and composable security notions in the case of statistically secure protocols were studied [9,10]. In general, these security notions are not equivalent [10]. Therefore, it is an interesting question to study if there are restricted scenarios where this equivalence holds.

Our Results: In this paper, we show that random OT protocols that are based on certain stateless two-party functionalities and that match a certain list of information-theoretical security properties (i.e., statistical equalities involving the statistical information) are not only secure in a simulation-based way, but are actually UC-secure with an unlimited adversary, an unlimited simulator, and an unlimited environment machine. Note that Random OT can be straightforwardly used to obtain OT for arbitrary inputs in a secure and composable way [11,12]. Note also that most OT protocols based on two-party stateless functionalities already internally run a random OT protocol and then use derandomization techniques to obtain OT for arbitrary inputs. We think that this approach is interesting because, in this scenario, a protocol designer can worry only about meeting the list-based security notion and the protocol inherits the UC-security. The setting studied in this paper covers the case of statistically secure protocols based on noisy channels, cryptogates, and pre-distributed correlated data. As a consequence of our result, several previously proposed protocols implementing oblivious transfer that were proven secure in weaker models automatically have their security upgraded to a simulation-based, composable one for free [11,13–26].

Related Work

OT can be constructed based both on generic computational assumptions such as the existence of enhanced trapdoor permutations [27,28] and on the computational hardness of many specific problems such as factoring [1], Diffie–Hellman [29,30], Learning with Errors (LWE) [31], variants of Learning Parity with Noise (LPN) [32], and McEliece assumptions [33,34]. However, the focus of this work is on statistically secure OT. When aiming for statistical security, OT can be based on noisy channels [13–21], cryptogates [22,23], pre-distributed correlated data [11,18,24], the bounded storage model [35–38], and on hardware tokens [25,26].

Canetti and Fischlin [39] showed that OT cannot be UC-realized in the plain model, thus additional setup assumptions are required. UC-secure OT protocols were initially constructed in the common reference string (CRS) model [31,40,41]. In the CRS model there exists an honestly generated random string that is available to the parties (the simulator can generate its own string as long as it looks indistinguishable from the honestly generated one). In the public key infrastructure model, Damgård and Nielsen [42] proposed an OT protocol that is UC-secure against adaptive adversaries under the assumption that threshold homomorphic encryption exists. Katz [43] proved that two-party and multi-party computation are possible assuming a tamper-proof hardware.

The question about the equivalence of list-based and composable security definitions for statistically secure protocols was previously addressed in [9,10], where it was proven that the equivalence does not hold in general. In [44], it was proven that perfectly secure OT protocols according to a list of properties are *sequentially* composable, this result being extended to statistical security in [45].

It was shown that, for statistically secure commitment schemes based on two-party stateless primitives, a list-based security definition actually implies UC-security [46]. While this result implies the possibility of building UC-secure OT protocols based on these commitment protocols, this is not the most efficient way of obtaining OT and it does not prove any additional security property about the existing OT protocols.

Even if the resources available to the parties to implement OT are asymmetric, Wolf and Wullschleger [12] showed a very simple way to reverse the OT's direction (indeed, all complete two-party functionalities are reversible, as proved recently by Khurana et al. [47]).

2. Preliminaries

2.1. Notation

Domains of random variables are denoted by calligraphic letters, the random variables by uppercase letters, and the realizations by lowercase letters. For random variables X over $\mathcal{X}$ and Y over $\mathcal{Y}$, $P_X : \mathcal{X} \rightarrow [0,1]$ with $\sum_{x\in\mathcal{X}} P_X(x) = 1$ denotes the probability distribution of X, $P_X(x) := \sum_{y\in\mathcal{Y}} P_{XY}(x,y)$ the marginal probability distribution, and $P_{X|Y}(x|y) := P_{XY}(x,y)/P_Y(y)$

the conditional probability distribution if $P_Y(y) \neq 0$. The statistical distance $\delta(P_X, P_Y)$ between P_X and P_Y with alphabet $\mathcal{X}$ is given by

$$\delta(P_X, P_Y) = \max_{\mathcal{S}\subseteq\mathcal{X}} \left| \sum_{x\in\mathcal{S}} P_X(x) - P_Y(x) \right|.$$

We say P_X and P_Y are ε-close if $\delta(P_X, P_Y) \leq \varepsilon$. Following Crépeau and Wullschleger [45], let the statistical information of X and Y given Z be defined as

$$\mathrm{I_S}(X; Y|Z) = \delta(P_{XYZ}, P_Z P_{X|Z} P_{Y|Z}).$$

2.2. The UC Framework

Here, we briefly review the main concepts of the UC framework, for more details please refer to the original work of Canetti [8]. In the UC framework, the security of a protocol to carry out a certain task is ensured in three phases:

1. One formalizes the framework, i.e., the process of executing a protocol in the presence of an adversary and an environment machine.
2. One formalizes an ideal protocol for carrying out the task in an ideal protocol using a "trusted party". In the ideal protocol, the trusted party captures the requirements of the desired task and the parties do not communicate among themselves.
3. One proves that the real protocol emulates the ideal protocol, i.e., for every adversary in the real model, there exists an ideal adversary (also known as the simulator) in the ideal model such that no environment machine can distinguish if it is interacting with the real or the ideal world.

The environment in the UC framework represents all activity external to the running protocol, thus it provides inputs to the parties running the protocol and receives the outputs that the parties generate during the execution of the protocol. As stated above, the environment also tries to distinguish between attacks on real executions of the protocol and simulated attacks against the ideal functionality. If no environment can distinguish the two situations, the real protocol emulates the ideal functionality. Proving that a protocol is secure in the UC framework provides the following benefits:

1. The ideal functionality describes intuitively the desired properties of the protocol.
2. The protocols are secure under composition.
3. The security is retained when the protocol is used as a sub-protocol to replace an ideal functionality that it emulates.

2.2.1. The Ideal World

An ideal functionality $\mathcal{F}$ represents the desired properties of a given task. Conceptually, $\mathcal{F}$ is treated as a local subroutine by the several parties that use it, and thus the communication between the parties and $\mathcal{F}$ is supposedly secure (i.e., messages are sent by input and output tapes). The ideal protocol also involves a simulator $\mathcal{S}$, an environment $\mathcal{Z}$ on input z, and a set of dummy parties that interacts as defined below. Whenever a dummy party is activated with input x, it writes x onto the input tape of $\mathcal{F}$. Whenever the dummy party is activated with value x on its subroutine output tape, it writes x on subroutine output tape of $\mathcal{Z}$. The simulator $\mathcal{S}$ has no access to the contents of messages sent between dummy parties and $\mathcal{F}$, and it should send corruption messages directly to $\mathcal{F}$, which is responsible for determining the effects of corrupting any dummy party. The ideal functionality receives messages from the dummy parties by reading its input tape and sends messages to them by writing to their subroutine output tape. In the ideal protocol, there is no communication among the parties. The environment $\mathcal{Z}$ can set the inputs to the parties and read their outputs, but cannot see the communication with the ideal functionality.

2.2.2. The Real World

In the real world, the protocol π is executed by parties $\mathcal{P}_1, \ldots, \mathcal{P}_n$ with some adversary $\mathcal{A}$ and an environment machine $\mathcal{Z}$ with input z. $\mathcal{Z}$ can set the inputs for the parties and see their outputs, but not the communication among the parties. The parties can invoke subroutines, pass inputs to them, and receive outputs from them. They can also write messages on the incoming communication tape of the adversary. These messages may specify the identity of the final destination of the message. $\mathcal{A}$ can send messages to any party ($\mathcal{A}$ delivers the message). In addition, they may use the ideal functionalities that are provided to the real protocol. $\mathcal{A}$ can communicate with $\mathcal{Z}$ and the ideal functionalities that are provided to the real protocol. $\mathcal{A}$ also controls the corrupt parties (the environment always knows which parties are corrupted).

2.2.3. The Adversarial Model

The network is asynchronous without guaranteed delivery of messages. The communication is public, but authenticated (i.e., the adversary cannot modify the messages). The adversary controls the corrupted parties. Any number of parties can be corrupted, but we consider static corruptions, i.e., the corruptions happen before the beginning of the protocol. Finally, the adversary, the environment, and the simulator are allowed unbounded complexity. This assumption on the computational power of the simulator somehow weakens our result as the composition theorem cannot be applied several times if the real adversary were restricted to polynomial time, because the "is at least as secure as" relation can no longer be proven to be transitive. However, arbitrary composition is allowed when considering statistically secure protocols and this situation is common in the literature when proving general results on the composability of statistically secure protocols [9,10,44,45].

2.2.4. Realizing an Ideal Functionality

A protocol π statistically UC-realizes an ideal functionality $\mathcal{F}$ if for any real-life adversary $\mathcal{A}$ there exists a simulator $\mathcal{S}$ such that no environment $\mathcal{Z}$, on any input z, can tell with non-negligible probability whether it is interacting with $\mathcal{A}$ and parties running π in the real-life process, or it is interacting with $\mathcal{S}$ and $\mathcal{F}$ in the ideal protocol. This means that, from the point of view of the environment, running protocol π is statistically indistinguishable from the ideal world with $\mathcal{F}$.

2.2.5. The Oblivious Transfer Functionality

We present in Figure 1 the one-out-of-two bit random oblivious transfer functionality $\mathcal{F}_{\mathsf{ROT}}$. The sender is denoted by Alice and the receiver by Bob.

Functionality $\mathcal{F}_{\mathsf{ROT}}$

$\mathcal{F}_{\mathsf{ROT}}$ interacts with Alice and Bob.

Alice's Check-in: Upon receiving (DISTRIBUTE, sid, …) from Alice, if Alice is honest, sample uniformly random $b_0, b_1 \in \{0,1\}$; otherwise, set the bits b_0, b_1 as specified in Alice's message. Record (sid, b_0, b_1) and ignore future (DISTRIBUTE, sid, …) from Alice.

Bob's Check-in: Upon receiving (DISTRIBUTE, sid, …) from Bob, if Bob is honest, sample a uniformly random $c \in \{0,1\}$; otherwise, set the bit c as specified in Bob's message. Record (sid, c) and ignore future (DISTRIBUTE, sid, …) from Bob.

Distribution: Upon having recorded values b_0, b_1, and c for some sid, send (OUTPUT, sid) to $\mathcal{S}$. Upon an answer (OUTPUT, sid) from $\mathcal{S}$, deliver (OUTPUT, b_0, b_1) to Alice and (OUTPUT, c, b_c) to Bob.

Figure 1. The one-out-of-two bit random oblivious transfer functionality.

2.3. Setup Assumption

In this work, we consider the scenario in which Alice and Bob have access to the functionality $\mathcal{F}_{P_{V,W|X,Y}}$ that given inputs $x \in \mathcal{X}$ from Alice and $y \in \mathcal{Y}$ from Bob samples the outputs $v \in \mathcal{V}$ and $w \in \mathcal{W}$ according to the conditional probability distribution $P_{V,W|X,Y}$, and gives the outputs v and w to Alice and Bob, respectively. The functionality $\mathcal{F}_{P_{V,W|X,Y}}$ is described in Figure 2. We remark that this functionality captures several cryptographic primitives that have been previously used for obtaining secure oblivious transfer, including noisy channels and pre-distributed correlated data. Similar cryptographic primitives have appeared in the literature under a different terminology [48,49].

Functionality $\mathcal{F}_{P_{V,W|X,Y}}$

$\mathcal{F}_{P_{V,W|X,Y}}$ interacts with Alice and Bob and is parameterized by the conditional probability distribution $P_{V,W|X,Y}$.

Alice's Input: Upon receiving (INPUT, sid, x) from Alice, if $x \in \mathcal{X}$, then record (sid, x). Ignore future messages (INPUT, sid, ...) from Alice.

Bob's Input: Upon receiving (INPUT, sid, y) from Bob, if $y \in \mathcal{Y}$, then record (sid, y). Ignore future messages (INPUT, sid, ...) from Bob.

Output: Upon obtained valid inputs from Alice and Bob for some sid, pick v, w according to $P_{V,W|X,Y}$ and output (OUTPUT, sid, v) to Alice and (OUTPUT, sid, w) to Bob.

Figure 2. The functionality, given valid inputs, samples outputs according to the conditional probability distribution and delivers the outputs to Alice and Bob.

3. Random Oblivious Transfer Based on Statistically Secure Two Party Stateless Functionalities

In this section, we define a list-based security model for random OT protocols that achieve statistical security by using $\mathcal{F}_{P_{V,W|X,Y}}$ as a setup assumption. Alice and Bob have two resources available between them:

- a bidirectional authenticated noiseless channel denoted as $\mathcal{F}_{\mathsf{AUTH}}$, and
- the functionality $\mathcal{F}_{P_{V,W|X,Y}}$.

We stress we are not describing a specific protocol in this section. Rather, we are providing a general framework and security definitions that encompasses any protocol that implements OT based on two-party stateless functionalities and has statistical security. In the following, we model the probabilistic choices of Alice by a random variable $\mathsf{coins}_{\mathsf{Alice}}$ and those of Bob by a random variable $\mathsf{coins}_{\mathsf{Bob}}$, so that we can use deterministic functions in the protocol. As usual, we assume that the noiseless messages exchanged by the players and their personal randomness are taken from $\{0,1\}^*$. We now describe a generic protocol π that is general enough to captures any protocol implementing OT based on two-party stateless functionalities with statistical security.

Protocol π

Alice and Bob interact and in the end of the execution Alice gets (b_0, b_1) and Bob gets (c, b_c), for $b_0, b_1, c \in \{0,1\}$ picked uniformly at random. The security parameter is n, and determines how many times the parties can use the functionality $\mathcal{F}_{P_{V,W|X,Y}}$: in the ith round, Alice and Bob input symbols x_i and y_i to the functionality $\mathcal{F}_{P_{V,W|X,Y}}$, which generates the outputs v_i and w_i according to $P_{V,W|X,Y}$ and delivers them to Alice and Bob, respectively. Let x^i, y^i, v^i, and w^i denote the vectors of these variables until ith round. The parties can use $\mathcal{F}_{\mathsf{AUTH}}$ at any moment. Let trans denote all the noiseless messages exchanged between the players.

We call the view of Bob all the data in his possession, i.e. $y^n, w^n, c, \mathsf{coins}_{\mathsf{Bob}}$, and trans, and denote it by $\mathsf{view}_{\mathsf{Bob}}$. $\mathsf{view}_{\mathsf{Alice}}$ is defined similarly. We denote the output of the (possibly malicious) parties Alice and Bob by $\mathsf{output}_{\mathsf{Alice}}$ and $\mathsf{output}_{\mathsf{Bob}}$, respectively. The list-based definition of security that is henceforth considered in this paper follows the lines of Crépeau and Wullschleger [45]. The protocol is said to be secure if there exists an ϵ that is a negligible function of the security parameter n and is such that the following properties are satisfied:

Correctness

If both parties are honest, then $\mathsf{output}_{\mathsf{Alice}} = (b_0, b_1)$ and $\mathsf{output}_{\mathsf{Bob}} = (c, d)$ for $d \in \{0, 1\}$ and uniformly random $b_0, b_1, c \in \{0, 1\}$. Additionally,

$$\Pr[D = B_C] \geq 1 - \epsilon.$$

Security for Alice

If Alice is honest, then $\mathsf{output}_{\mathsf{Alice}} = (b_0, b_1)$ for uniformly random $b_0, b_1 \in \{0, 1\}$ and there exists a random variable C such that

$$I_S(B_0, B_1; C) \leq \epsilon$$

and

$$I_S(B_0, B_1; \mathsf{output}_{\mathsf{Bob}} | C, B_C) \leq \epsilon.$$

Security for Bob

If Bob is honest, then $\mathsf{output}_{\mathsf{Bob}} = (c, d)$ for $d \in \{0, 1\}$ and uniformly random $c \in \{0, 1\}$; and

$$I_S(C; \mathsf{output}_{\mathsf{Alice}}) \leq \epsilon.$$

4. UC-Security Implication

In this section, we address the question of whether random OT protocols that are secure according to the definitions of Section 3 also enjoy statistical UC-security. We show that this is indeed the case. Intuitively, this follows from the fact that the security in those protocols is based on the correlated randomness that is provided by the functionality $\mathcal{F}_{P_{V,W|X,Y}}$ to Alice and Bob. Since in the ideal world the simulator controls $\mathcal{F}_{P_{V,W|X,Y}}$, it can leverage this knowledge in order to extract the outputs of the corrupted parties and forward them to the random oblivious transfer functionality $\mathcal{F}_{\mathsf{ROT}}$, thus allowing the ideal execution to be indistinguishable from the real execution from the environment's point of view. First, we prove some lemmas that are used below to prove the main result of this work.

We first show that, in any random OT protocol that is secure according to the definitions of Section 3, if Bob is honest, then given Alice's input to and output from the functionality $\mathcal{F}_{P_{V,W|X,Y}}$ and all the noiseless communication exchanged by Alice and Bob through $\mathcal{F}_{\mathsf{AUTH}}$, it is possible to extract both outputs that Bob would get with $c = 0$ and $c = 1$ in the random OT protocol.

Lemma 1. *Let π be a random OT protocol that is secure according to the definitions of Section 3 and let* Bob *be honest. Given* Alice*'s input to and output from $\mathcal{F}_{P_{V,W|X,Y}}$ and all the noiseless communication exchanged by* Alice *and* Bob *through $\mathcal{F}_{\mathsf{AUTH}}$ during the execution of π, with overwhelming probability, it is possible to extract the output that* Bob *would get both in the case that $c = 0$ and $c = 1$.*

Proof. Let us consider an execution of the protocol π in which Bob has random coins $\mathsf{coins}_{\mathsf{Bob}}$ and gets $\mathsf{output}_{\mathsf{Bob}} = (c, d)$ for $d \in \{0, 1\}$ and uniformly random $c \in \{0, 1\}$ (as the protocol is secure according to the definitions of Section 3). Denote by m the set of messages exchanged between Alice and $\mathcal{F}_{P_{V,W|X,Y}}$ concatenated with the noiseless messages between Bob and Alice. We claim that there should exist $\overline{\mathsf{coins}_{\mathsf{Bob}}} \neq \mathsf{coins}_{\mathsf{Bob}}$ so that, for the same m, if Bob executed the protocol with $\overline{\mathsf{coins}_{\mathsf{Bob}}}$ he should have been able with overwhelming probability to get $\overline{\mathsf{output}_{\mathsf{Bob}}} = (\overline{c}, \overline{d})$ with $\overline{c} \neq c$ and $\overline{d} \in \{0,1\}$. If that were not the case, Alice would know that Bob is unable to obtain a valid output $\overline{d}$ when the choice bit is $\overline{c}$, thus gaining knowledge on the choice bit and breaking the protocol security. Given that

$$I_S(\mathsf{output}_{\mathsf{Alice}}; C) \leq \epsilon,$$

we get

$$\delta(P_{\mathsf{output}_{\mathsf{Alice}}C}, P_{\mathsf{output}_{\mathsf{Alice}}}P_C) \leq \epsilon,$$

and so there are events $\mathcal{E}_1$ and $\mathcal{E}_2$ such that

$$\Pr[\mathcal{E}_1] = \Pr[\mathcal{E}_2] = 1 - \epsilon \text{ and}$$

$$P_{\mathsf{output}_{\mathsf{Alice}}C|\mathcal{E}_1} = P_{\mathsf{output}_{\mathsf{Alice}}|\mathcal{E}_2}P_{C|\mathcal{E}_2}.$$

Therefore, if $\mathcal{E}_1$ and $\mathcal{E}_2$ happen, then $\mathsf{output}_{\mathsf{Alice}}$ does not provide information about C and $\overline{\mathsf{coins}_{\mathsf{Bob}}}$ should exist. Thus, given m we are left with an extraction procedure. One just computes $\mathsf{coins}_{\mathsf{Bob}}$ and $\overline{\mathsf{coins}_{\mathsf{Bob}}}$ that for this m produce outputs $\mathsf{output}_{\mathsf{Bob}}$ and $\overline{\mathsf{output}_{\mathsf{Bob}}}$, respectively, and simulates the protocol execution for each specified Bob's randomness. □

We now prove that, given access to the messages that Bob exchanges with Alice and $\mathcal{F}_{P_{V,W|X,Y}}$, there is a point in the protocol execution in which it is possible to extract the choice bit c and still equivocate b_0, b_1 to any value, i.e., it is possible to find an Alice's view that is compatible with the current view of Bob and the new values of b_0 and b_1.

Lemma 2. *Let π be a random OT protocol that is secure according to the definitions of Section 3 and let* Alice *be honest. Given access to all messages that* Bob*'s exchanges with $\mathcal{F}_{P_{V,W|X,Y}}$ and all the noiseless communication exchanged by* Alice *and* Bob *through $\mathcal{F}_{\mathsf{AUTH}}$ during the execution of π, with overwhelming probability it is possible to extract the choice bit c at some point of the execution of the protocol π. Additionally, at this point, it is still possible to change b_0 and b_1 to any desired values.*

Proof. We first prove that there is a point in the protocol execution where we can extract the choice bit given the messages that Bob exchanged with Alice and the functionality $\mathcal{F}_{P_{V,W|X,Y}}$. Let m denote these messages in a given protocol execution. Let $\mathcal{M}(0)$ denote the set of messages that allow Bob to obtain the bit b_0 with overwhelming probability (the probability taken over $\mathsf{coins}_{\mathsf{Alice}}$, $\mathsf{coins}_{\mathsf{Bob}}$ and the randomness of $\mathcal{F}_{P_{V,W|X,Y}}$). Let $\mathcal{M}(1)$ be defined similarly for b_1. From the security for Alice, we have that

$$I_S(B_0, B_1; C) \leq \epsilon$$

and

$$I_S(B_0, B_1; \mathsf{output}_{\mathsf{Bob}}|C, B_C) \leq \epsilon,$$

and so we get that m with overwhelming probability (over $\mathsf{coins}_{\mathsf{Alice}}$ and the randomness of $\mathcal{F}_{P_{V,W|X,Y}}$) cannot be in both $\mathcal{M}(0)$ and $\mathcal{M}(1)$, since this fact would imply that the resulting protocol would be insecure for Alice. This fact gives us a procedure for obtaining the choice bit c given m. We just check if m is in $\mathcal{M}(0)$ or $\mathcal{M}(1)$.

We now turn to the equivocation property. From the previous reasoning, we know that there should exist a point in the protocol where Bob sends a message to Alice that fixes the choice bit (i.e., the choice bit can be extracted from his messages from/to Alice and $\mathcal{F}_{P_{V,W|X,Y}}$). Let i be the index of such message. Suppose the ith message is the very last one in the protocol. Then, Bob has all the information necessary to compute his output even before sending the ith message. As the choice bit is only fixed in the next message, Bob should be able to compute both b_0 and b_1, breaking Alice's security. Thus, the ith message should not be the last one. The same reasoning implies that, from Bob's point of view, none of Alice's outputs b_0 and b_1 can be fixed before the ith message: (1) if both b_0 and b_1 are fixed from Bob's point of view before the ith message, then he could obtain both b_0 and b_1 and break the security according to the definitions of Section 3; and (2) if only b_i is fixed, then Bob can still change his choice to $c = 1 - i$ and obtain both b_0 and b_1, thus breaking the security definition of Section 3. Therefore, we should have that, when the ith message is sent by Bob, Alice's outputs b_0 and b_1 are still equivocable. □

We now use two lemmas to prove our main result:

Theorem 1. *Any random OT protocol based on $\mathcal{F}_{\mathsf{AUTH}}$ and $\mathcal{F}_{P_{V,W|X,Y}}$ that is secure according to the definitions of Section 3 also UC-realizes $\mathcal{F}_{\mathsf{ROT}}$.*

Proof. We construct the simulator $\mathcal{S}$ as follows. $\mathcal{S}$ runs a simulated copy of $\mathcal{A}$ in a black-box way, plays the role of the ideal functionality $\mathcal{F}_{P_{V,W|X,Y}}$, and simulates a copy of the hybrid interaction of π for the simulated adversary $\mathcal{A}$. In addition, $\mathcal{S}$ forwards the messages between $\mathcal{Z}$ and $\mathcal{A}$. Below, we describe the procedures of the simulator in each occasion:

Only Alice **is corrupted:** $\mathcal{S}$ samples the randomness $\mathsf{coins}_{\mathsf{Bob}}$ of the simulated Bob and proceeds with the simulated execution of the protocol π by producing his noiseless messages as well as his inputs $y_i \in \mathcal{Y}$ to $\mathcal{F}_{P_{V,W|X,Y}}$. Additionally, once the inputs $x_i \in \mathcal{X}$ and $y_i \in \mathcal{Y}$ to $\mathcal{F}_{P_{V,W|X,Y}}$ are fixed, $\mathcal{S}$ simulates the outputs of the functionality $\mathcal{F}_{P_{V,W|X,Y}}$ and sends v_i to $\mathcal{A}$. As $\mathcal{S}$ plays the role of $\mathcal{F}_{P_{V,W|X,Y}}$, when the execution is done, $\mathcal{S}$ extracts the output bits b_0, b_1 of the corrupted Alice using the result of lemma 1 and forwards b_0, b_1 to $\mathcal{F}_{\mathsf{ROT}}$. $\mathcal{S}$ then allows $\mathcal{F}_{\mathsf{ROT}}$ to deliver the output.

Only Bob **is corrupted:** $\mathcal{S}$ samples the randomness $\mathsf{coins}_{\mathsf{Alice}}$ of the simulated Alice and proceeds with the simulated execution of the protocol π by producing her noiseless messages as well as her inputs $x_i \in \mathcal{X}$ to $\mathcal{F}_{P_{V,W|X,Y}}$. Additionally, once the inputs $x_i \in \mathcal{X}$ and $y_i \in \mathcal{Y}$ to $\mathcal{F}_{P_{V,W|X,Y}}$ are fixed, $\mathcal{S}$ simulates the outputs of the functionality $\mathcal{F}_{P_{V,W|X,Y}}$, and sends w_i to $\mathcal{A}$. Then, using the result of lemma 2, $\mathcal{S}$ extracts the choice bit c of the corrupted Bob, inputs c to $\mathcal{F}_{\mathsf{ROT}}$, receives b_c, and finishes the simulated protocol execution in such way that the received bit in the hybrid interaction b'_c is equal to the received bit in the ideal protocol b_c with overwhelming probability.

Neither party is corrupted: $\mathcal{S}$ samples the randomness $\mathsf{coins}_{\mathsf{Alice}}$ and $\mathsf{coins}_{\mathsf{Bob}}$ and proceeds with the simulated execution of the protocol π by simulating the noiseless messages as well as the inputs/outputs of $\mathcal{F}_{P_{V,W|X,Y}}$, and reveals the noiseless messages to $\mathcal{A}$. If the simulated Bob would output $b'_{c'}$ in the hybrid interaction, then $\mathcal{S}$ allows $\mathcal{F}_{\mathsf{ROT}}$ to output the bit b_c.

Both parties are corrupted: $\mathcal{S}$ just simulates $\mathcal{F}_{P_{V,W|X,Y}}$.

We analyze below the probabilities of the events that can result in different views for the environment $\mathcal{Z}$ between the real world execution with the protocol π and the adversary $\mathcal{A}$, and the ideal world execution with functionality $\mathcal{F}_{\mathsf{ROT}}$ and the simulator $\mathcal{S}$:

- When only Alice is corrupted, $\mathcal{Z}$'s view in the real and ideal worlds are equal if: (1) $\mathcal{S}$ succeeds to extract both of Alice's outputs bits b_0, b_1 to forward to $\mathcal{F}_{\mathsf{ROT}}$; and (2) $\mathcal{A}$ does not learn the choice bit c' in the simulated protocol execution. By Lemma 1, the extraction works with overwhelming probability. By the security definitions of Section 3, with overwhelming probability $\mathcal{A}$ does not learn c'.
- When only Bob is corrupted, $\mathcal{Z}$'s view in the real and ideal worlds are equal if: (1) $\mathcal{S}$ succeeds to extract the bit c and finish the protocol in such way that the received bit b'_c in the simulated protocol execution is equal to b_c; and (2) $\mathcal{A}$ cannot learn $b'_{\bar{c}}$ in the simulated protocol execution. By Lemma 2, the first condition is satisfied with overwhelming probability. By the security definitions of Section 3, with overwhelming probability $\mathcal{A}$ cannot learn $b'_{\bar{c}}$
- When neither party is corrupted, $\mathcal{S}$'s procedures statistically emulate the hybrid execution for the adversary $\mathcal{A}$, as $\mathcal{A}$ cannot learn b'_0, b'_1, c' from the noiseless messages alone.
- When both parties are corrupted, $\mathcal{S}$'s procedures perfectly emulate the hybrid execution for the adversary $\mathcal{A}$.

We conclude that, since all events that can result in different views have negligible probabilities, the protocol π UC-realizes $\mathcal{F}_{\mathsf{ROT}}$. $\square$

5. Conclusions

In this paper, we prove that random oblivious transfer protocols based on two-party stateless functionalities matching a list of security properties are universally composable when unbounded simulators are allowed. As previously commented, this assumption on the simulator gives us secure universal composability with other statistically secure protocols. The restriction to random oblivious transfer protocols is not restrictive (since random OT can be used to obtain OT for arbitrary inputs [11], proving the composability of such reduction is straightforward [12]). Most of the OT protocols based on two-party stateless functionalities are in fact designed to initially run an internal random OT protocol and then derandomize the values. In this case, the universally composability implication can be applied directly to the inner random OT protocol. However, it is an interesting problem to generalize the results presented here to arbitrary OT. Our result immediately implies that several previously proposed OT protocols can have their security upgraded for free [11,13–26].

Finally, we note that, in the case that the extraction (Lemma 1) and equivocability (Lemma 2) procedures can be executed in polynomial time (such as in [11,24]), we achieve fully-fledged UC-security—obtaining secure composability even with protocols that are only computationally secure.

Author Contributions: The three authors contributed equally to all parts of this work. All authors have read and agreed to the published version of the manuscript.

Funding: Rafael Dowsley is supported by the BIU Center for Research in Applied Cryptography and Cyber Security in conjunction with the Israel National Cyber Bureau in the Prime Minister's Office.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rabin, M.O. *How to Exchange Secrets by Oblivious Transfer*; Technical Report Technical Memo TR-81; Aiken Computation Laboratory, Harvard University: Cambridge, MA, USA, 1981.
2. Goldreich, O.; Micali, S.; Wigderson, A. How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority. In Proceedings of the 19th Annual ACM Symposium on Theory of Computing, New York, NY, USA, 25–27 May 1987; Aho, A., Ed.; ACM Press: New York, NY, USA, 1987; pp. 218–229.
3. Kilian, J. Founding Cryptography on Oblivious Transfer. In Proceedings of the 20th Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, 2–4 May 1988; ACM Press: New York, NY, USA, 1988; pp. 20–31.
4. Crépeau, C. Equivalence Between Two Flavours of Oblivious Transfers. In Proceedings of the Advances in Cryptology–CRYPTO'87, Santa Barbara, CA, USA, 21–25 August 1988; Lecture Notes in Computer Science; Pomerance, C., Ed.; Springer: Berlin/Heidelberg, Germany, 1988; Volume 293, pp. 350–354.
5. Goldwasser, S.; Micali, S.; Rackoff, C. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.* **1989**, *18*, 186–208. [CrossRef]
6. Beaver, D. Foundations of Secure Interactive Computing. In Proceedings of the Advances in Cryptology—CRYPTO'91, Santa Barbara, CA, USA, 16–20 August 1992; Lecture Notes in Computer Science; Feigenbaum, J., Ed.; Springer: Berlin/Heidelberg, Germany, 1992; Volume 576, pp. 377–391.
7. Canetti, R. Security and Composition of Multiparty Cryptographic Protocols. *J. Cryptol.* **2000**, *13*, 143–202. [CrossRef]
8. Canetti, R. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, Newport Beach, CA, USA, 8–11 October 2001; IEEE Computer Society Press: Washington, DC, USA, 2001; pp. 136–145.
9. Kushilevitz, E.; Lindell, Y.; Rabin, T. Information-theoretically secure protocols and security under composition. In Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, 21–23 May 2006; Kleinberg, J.M., Ed.; ACM Press: New York, NY, USA, 2006; pp. 109–118.

10. Backes, M.; Müller-Quade, J.; Unruh, D. On the Necessity of Rewinding in Secure Multiparty Computation. In Proceedings of the TCC 2007: 4th Theory of Cryptography Conference, Amsterdam, The Netherlands, 21–24 February 2007; Lecture Notes in Computer Science; Vadhan, S.P., Ed.; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4392, pp. 157–173.
11. Beaver, D. Commodity-Based Cryptography (Extended Abstract). In Proceedings of the 29th Annual ACM Symposium on Theory of Computing, El Paso, TX, USA, 4–6 May 1997; ACM Press: New York, NY, USA, 1997; pp. 446–455.
12. Wolf, S.; Wullschleger, J. Oblivious Transfer Is Symmetric. In Proceedings of the Advances in Cryptology—EUROCRYPT 2006, St. Petersburg, Russia, 28 May–1 June 2006; Lecture Notes in Computer Science; Vaudenay, S., Ed.; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4004, pp. 222–232.
13. Crépeau, C.; Kilian, J. Achieving Oblivious Transfer Using Weakened Security Assumptions (Extended Abstract). In Proceedings of the 29th Annual Symposium on Foundations of Computer Science, White Plains, NY, USA, 24–26 October 1988; IEEE Computer Society Press: Washington, DC, USA, 1988; pp. 42–52.
14. Crépeau, C. Efficient Cryptographic Protocols Based on Noisy Channels. In Proceedings of the Advances in Cryptology—EUROCRYPT'97, Konstanz, Germany, 11–15 May 1997; Lecture Notes in Computer Science; Fumy, W., Ed. Springer: Berlin/Heidelberg, Germany, 1997; Volume 1233, pp. 306–317.
15. Damgård, I.; Kilian, J.; Salvail, L. On the (Im)possibility of Basing Oblivious Transfer and Bit Commitment on Weakened Security Assumptions. In Proceedings of the Advances in Cryptology—EUROCRYPT'99, Prague, Czech Republic, 2–6 May 1999; Lecture Notes in Computer Science; Stern, J., Ed.; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1592, pp. 56–73.
16. Stebila, D.; Wolf, S. Efficient oblivious transfer from any non-trivial binary-symmetric channel. In Proceedings of the IEEE International Symposium on Information Theory, Lausanne, Switzerland, 30 June–5 July 2002; p. 293. [CrossRef]
17. Crépeau, C.; Morozov, K.; Wolf, S. Efficient Unconditional Oblivious Transfer from Almost Any Noisy Channel. In Proceedings of the SCN 04: 4th International Conference on Security in Communication Networks, Amalfi, Italy, 8–10 September 2004; Lecture Notes in Computer Science; Blundo, C., Cimato, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3352, pp. 47–59.
18. Nascimento, A.C.A.; Winter, A. On the Oblivious-Transfer Capacity of Noisy Resources. *IEEE Trans. Inf. Theory* **2008**, *54*, 2572–2581. [CrossRef]
19. Pinto, A.C.B.; Dowsley, R.; Morozov, K.; Nascimento, A.C.A. Achieving Oblivious Transfer Capacity of Generalized Erasure Channels in the Malicious Model. *IEEE Trans. Inf. Theory* **2011**, *57*, 5566–5571. [CrossRef]
20. Ahlswede, R.; Csiszár, I. On Oblivious Transfer Capacity. In *Information Theory, Combinatorics, and Search Theory*; Lecture Notes in Computer Science; Aydinian, H., Cicalese, F., Deppe, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; Volume 7777, pp. 145–166. [CrossRef]
21. Dowsley, R.; Nascimento, A.C.A. On the Oblivious Transfer Capacity of Generalized Erasure Channels Against Malicious Adversaries: The Case of Low Erasure Probability. *IEEE Trans. Inf. Theory* **2017**, *63*, 6819–6826. [CrossRef]
22. Kilian, J. More general completeness theorems for secure two-party computation. In Proceedings of the 32nd Annual ACM Symposium on Theory of Computing, Portland, OR, USA, 21–23 May 2000; ACM Press: New York, NY, USA, 2000; pp. 316–324.
23. Beimel, A.; Malkin, T.; Micali, S. The All-or-Nothing Nature of Two-Party Secure Computation. In Proceedings of the Advances in Cryptology—CRYPTO'99, Santa Barbara, CA, USA, 15–19 August 1999; Lecture Notes in Computer Science; Wiener, M.J., Ed.; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1666, pp. 80–97.
24. Rivest, R.L. Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer. Available online: http://people.csail.mit.edu/rivest/Rivest-commitment.pdf (accessed on 1 October 2019).
25. Döttling, N.; Kraschewski, D.; Müller-Quade, J. Unconditional and Composable Security Using a Single Stateful Tamper-Proof Hardware Token. In Proceedings of the TCC 2011: 8th Theory of Cryptography Conference, Providence, RI, USA, 28–30 March 2011; Lecture Notes in Computer Science; Ishai, Y., Ed.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6597, pp. 164–181.

26. Dowsley, R.; Müller-Quade, J.; Nilges, T. Weakening the Isolation Assumption of Tamper-Proof Hardware Tokens. In Proceedings of the ICITS 15: 8th International Conference on Information Theoretic Security, Lugano, Switzerland, 2–5 May 2015; Lecture Notes in Computer Science; Lehmann, A., Wolf, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9063, pp. 197–213. [CrossRef]
27. Even, S.; Goldreich, O.; Lempel, A. A Randomized Protocol for Signing Contracts. *Commun. ACM* **1985**, *28*, 637–647. [CrossRef]
28. Goldreich, O. *Foundations of Cryptography: Basic Applications*; Cambridge University Press: Cambridge, UK, 2004; Volume 2.
29. Bellare, M.; Micali, S. Non-Interactive Oblivious Transfer and Spplications. In Proceedings of the Advances in Cryptology—CRYPTO'89, Santa Barbara, CA, USA, 20–24 August 1989; Lecture Notes in Computer Science; Brassard, G., Ed.; Springer: Berlin/Heidelberg, Germany, 1990; Volume 435, pp. 547–557.
30. Naor, M.; Pinkas, B. Efficient Oblivious Transfer Protocols. In Proceedings of the 12th Annual ACM-SIAM Symposium on Discrete Algorithms, Washington, DC, USA, 7–9 January 2001; Kosaraju, S.R., Ed.; ACM-SIAM: New York, NY, USA, 2001; pp. 448–457.
31. Peikert, C.; Vaikuntanathan, V.; Waters, B. A Framework for Efficient and Composable Oblivious Transfer. In Proceedings of the Advances in Cryptology—CRYPTO 2008, Santa Barbara, CA, USA, 17–21 August 2008; Lecture Notes in Computer Science; Wagner, D., Ed.; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5157, pp. 554–571.
32. David, B.; Dowsley, R.; Nascimento, A.C.A. Universally Composable Oblivious Transfer Based on a Variant of LPN. In Proceedings of the CANS 14: 13th International Conference on Cryptology and Network Security, Heraklion, Crete, Greece, 22–24 October 2014; Lecture Notes in Computer Science; Gritzalis, D., Kiayias, A., Askoxylakis, I.G., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8813, pp. 143–158. [CrossRef]
33. Dowsley, R.; van de Graaf, J.; Müller-Quade, J.; Nascimento, A.C.A. Oblivious Transfer Based on the McEliece Assumptions. In Proceedings of the ICITS 08: 3rd International Conference on Information Theoretic Security, Calgary, AB, Canada, 10–13 August 2008; Lecture Notes in Computer Science; Safavi-Naini, R., Ed.; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5155, pp. 107–117. [CrossRef]
34. Dowsley, R.; van de Graaf, J.; Müller-Quade, J.; Nascimento, A.C.A. Oblivious Transfer Based on the McEliece Assumptions. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2012**, *E95-A*, 567–575. [CrossRef]
35. Cachin, C.; Crépeau, C.; Marcil, J. Oblivious Transfer with a Memory-Bounded Receiver. In Proceedings of the 39th Annual Symposium on Foundations of Computer Science, Palo Alto, CA, USA, 8–11 November 1998; IEEE Computer Society Press: Washington, DC, USA, 1998; pp. 493–502.
36. Dowsley, R.; Lacerda, F.; Nascimento, A.C.A. Oblivious transfer in the bounded storage model with errors. In Proceedings of the 2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, 29 June–4 July 2014; pp. 1623–1627. [CrossRef]
37. Ding, Y.Z.; Harnik, D.; Rosen, A.; Shaltiel, R. Constant-Round Oblivious Transfer in the Bounded Storage Model. In Proceedings of the TCC 2004: 1st Theory of Cryptography Conference, Cambridge, MA, USA, 19–21 February 2004; Lecture Notes in Computer Science; Naor, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 2951, pp. 446–472.
38. Dowsley, R.; Lacerda, F.; Nascimento, A.C.A. Commitment and Oblivious Transfer in the Bounded Storage Model With Errors. *IEEE Trans. Inf. Theory* **2018**, *64*, 5970–5984. [CrossRef]
39. Canetti, R.; Fischlin, M. Universally Composable Commitments. In Proceedings of the Advances in Cryptology—CRYPTO 2001, Santa Barbara, CA, USA, 19–23 August 2001; Lecture Notes in Computer Science; Kilian, J., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2139, pp. 19–40.
40. Canetti, R.; Lindell, Y.; Ostrovsky, R.; Sahai, A. Universally composable two-party and multi-party secure computation. In Proceedings of the 34th Annual ACM Symposium on Theory of Computing, Montreal, QC, Canada, 19–21 May 2002; ACM Press: New York, NY, USA, 2002; pp. 494–503.
41. Garay, J.A. Efficient and Universally Composable Committed Oblivious Transfer and Applications. In Proceedings of the TCC 2004: 1st Theory of Cryptography Conference, Cambridge, MA, USA, 19–21 February 2004; Lecture Notes in Computer Science; Naor, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 2951, pp. 297–316.

42. Damgård, I.; Nielsen, J.B. Universally Composable Efficient Multiparty Computation from Threshold Homomorphic Encryption. In Proceedings of the Advances in Cryptology–CRYPTO 2003, Santa Barbara, CA, USA, 17–21 August 2003; Lecture Notes in Computer Science; Boneh, D., Ed.; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2729, pp. 247–264.
43. Katz, J. Universally Composable Multi-party Computation Using Tamper-Proof Hardware. In Proceedings of the Advances in Cryptology—EUROCRYPT 2007, Barcelona, Spain, 20–24 May 2007; Lecture Notes in Computer Science; Naor, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4515, pp. 115–128.
44. Crépeau, C.; Savvides, G.; Schaffner, C.; Wullschleger, J. Information-Theoretic Conditions for Two-Party Secure Function Evaluation. In Proceedings of the Advances in Cryptology—EUROCRYPT 2006, St. Petersburg, Russia, 28 May–1 June 2006; Lecture Notes in Computer Science; Vaudenay, S., Ed.; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4004, pp. 538–554.
45. Crépeau, C.; Wullschleger, J. Statistical Security Conditions for Two-Party Secure Function Evaluation. In Proceedings of the ICITS 08: 3rd International Conference on Information Theoretic Security, Calgary, AB, Canada, 10–13 August 2008; Lecture Notes in Computer Science; Safavi-Naini, R., Ed.; Springer: Berlin/Heidelberg, Germany , 2008; Volume 5155, pp. 86–99. [CrossRef]
46. Dowsley, R.; van de Graaf, J.; Müller-Quade, J.; Nascimento, A.C.A. On the Composability of Statistically Secure Bit Commitments. *J. Internet Technol.* **2013**, *14*, 509–516.
47. Khurana, D.; Kraschewski, D.; Maji, H.K.; Prabhakaran, M.; Sahai, A. All Complete Functionalities are Reversible. In Proceedings of the Advances in Cryptology–EUROCRYPT 2016, Part II, Vienna, Austria, 8–12 May 2016; Lecture Notes in Computer Science; Fischlin, M., Coron, J.S., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9666, pp. 213–242. [CrossRef]
48. Maji, H.K.; Prabhakaran, M.; Rosulek, M. A unified characterization of completeness and triviality for secure function evaluation. In Proceedings of the International Conference on Cryptology in India, Kolkata, India, 9–12 December 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 40–59.
49. Kraschewski, D.; Maji, H.K.; Prabhakaran, M.; Sahai, A. A full characterization of completeness for two-party randomized function evaluation. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, 11–15 May 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 659–676.