New Perspectives on Weak Oblivious Transfer

Ueli Maurer
Department of Computer Science
ETH Zurich
Switzerland
Email: maurer@inf.ethz.ch

João Ribeiro
ETH Zurich
Switzerland
Email: ljoao@student.ethz.ch

***Abstract*—In this paper we provide a generalization of weak oblivious transfer through the constructive cryptography framework. This generalization requires the global order of the inputs and outputs from and to two parties called Alice and Bob to be completely defined, a subtlety which has been overlooked by previous work on the subject. We provide evidence that the order of inputs and outputs in weak oblivious transfer matters. In particular, it may influence the kind and strength of symmetry results which can be obtained about such resources.**

I. Introduction

A. Setting and previous work

1-2 Oblivious Transfer (1-2-OT) is a cryptographic primitive which receives two secret bits from Alice, one selection bit from Bob, and outputs the selected bit to Bob. It is guaranteed that Bob does not learn the secret bit he did not select and that Alice does not learn Bob's selection bit. This resource is fundamental in cryptography in the sense that one can base many important primitives on 1-2-OT. This includes, for example, several resources in secure multi-party computation.

It is known that 1-2-OT cannot be constructed only from a noiseless channel. As a result there have been many efforts to construct 1-2-OT from other kinds of weaker resources. For example, 1-2-OT can be constructed from all-or-nothing oblivious transfer (OT) (see [1]) and from several types of noisy channels (see [2], [5] and [6]). The analysis of the intermediate steps in such constructions has led to the definition and study of weaker notions of 1-2-OT (so-called weak oblivious transfer), where additional information may be leaked to Alice and Bob. Two important variants of weak oblivious transfer were proposed and studied in [5], [6], and [9].

The question of whether 1-2-OT can be reversed (i.e. Alice takes the role of Bob, and vice-versa) was first stated, motivated and answered in [8], where it was proved that one can obtain reversed 1-2-OT from several instances of 1-2-OT and a clear channel. Later, it was proved in [7] that one instance of 1-2-OT and a clear channel suffice to reverse 1-2-OT.

The constructive cryptography framework, where cryptographic protocols are seen as constructions of resources from other resources, was first developed in [3] and in [4]. The definition of what constitutes a valid construction depends on which parties can be dishonest and on which kind of security we are aiming to achieve.

B. Contributions

In Section III we propose a generalization of weak oblivious transfer (called $\mathbf{FOT}$) through the constructive cryptography framework. For ease of presentation, we focus on a subclass of $\mathbf{FOT}$ which is still quite general. For example, it captures (p,q,ε)-$\mathbf{WOT}$ (as defined in [5] and [6]) as a specification, i.e. a set of resources. We also show that it captures Crépeau's reduction of 1-2-OT to OT presented in [1] (when it is seen in a non-asymptotic manner) as a different instantiation from (p,q,ε)-$\mathbf{WOT}$.

In Section IV we discuss symmetry statements for our generalization of weak oblivious transfer. While [6] and [9] also propose generalized versions of weak oblivious transfer, these are not adequate for reasoning about more precise symmetry statements. In particular, previous definitions do not pay much attention to the order of the inputs and outputs to and from Alice and Bob. We formalize symmetry for weak oblivious transfer as a constructive statement and provide partial symmetry results for some instantiations of our generalization of weak oblivious transfer, including a symmetry result which requires no clear channel. This latter result is based on a simple idea which also yields an amplification method for weak oblivious transfer in a previously unexplored setting. Furthermore, we provide evidence that the order of inputs and outputs influences the kind of symmetry results we are able to prove about an instantiation of weak oblivious transfer.

II. Preliminaries

A. Notation

We denote a random variable by an upper-case letter X, its probability function by P_X and an element of the domain of the random variable X by a lower-case x. We also denote that r was uniformly sampled from a set $\mathcal{X}$ by $r \in_R \mathcal{X}$. Also, probability distributions are denoted by lower-case Greek letters such as ρ. Given n independent random variables $U_1,\dots,U_n$ uniformly distributed over $\{0,1\}$, we define $F(n,k)=\Pr\left[\sum_{i=1}^{n} U_i \geq k\right]$.

978-1-5090-1805-5/16/$31.00 ©2016 IEEE

B. Constructive Cryptography

In this paper we use the constructive cryptography framework (see [3] and [4]) to formulate our results. This framework deals with systems which, at the highest level of abstraction, are objects with interfaces. Systems can be composed by connecting some of their interfaces.

Systems can be separated into three types: converters, distinguishers and resources. Resources are denoted by boldfaced upper-case letters such as $\mathbf{R}$. In this paper we consider only resources with two interfaces: a left interface, which we call Alice's interface, and a right interface, which we call Bob's interface. We can also use two such resources $\mathbf{R}$ and $\mathbf{S}$ in parallel, which results in a resource $\mathbf{R}||\mathbf{S}$, which again has two interfaces. Each of those two interfaces gives access to an interface of $\mathbf{R}$ and an interface of $\mathbf{S}$. We define by $\mathbf{R}^k$ the resource which consists of the parallel composition of k copies of resource $\mathbf{R}$. We study situations where one of Alice and Bob is dishonest, but not both. A specification is a set of resources.

Converters are systems which have an inner interface and an outer interface. They are denoted by lower-case Greek letters such as α, β and π. We denote the set of all converters by Σ. A converter α can be connected to a resource $\mathbf{R}$ by connecting its inner interface to either the left or the right interface of $\mathbf{R}$. If α is connected to the left interface of $\mathbf{R}$ we denote the resulting (2-interface) system by $\alpha\mathbf{R}$, where the new left interface is the outer interface of α and the new right interface is still the right interface of $\mathbf{R}$. If α is connected to the right interface of $\mathbf{R}$, we denote the resulting system by $\mathbf{R}\alpha$.

Distinguishers are systems which connect to all interfaces of a resource $\mathbf{R}$ and output a bit B at a separate interface. The interaction between $\mathbf{D}$ and $\mathbf{R}$ specifies a random experiment and the probability that $\mathbf{D}$ outputs 1 when interacting with $\mathbf{R}$ is denoted by $P^{\mathbf{DR}}[B=1]$. The distinguishing advantage of $\mathbf{D}$ in distinguishing between resources $\mathbf{R}$ and $\mathbf{S}$ is

$$\Delta^{\mathbf{D}}(\mathbf{R},\mathbf{S}) := \left|P^{\mathbf{DR}}[B=1] - P^{\mathbf{DS}}[B=1]\right|.$$

We denote the set of all distinguishers by $\mathcal{D}$ and define

$$\Delta^{\mathcal{D}}(\mathbf{R},\mathbf{S}) := \sup_{\mathbf{D}\in\mathcal{D}} \Delta^{\mathbf{D}}(\mathbf{R},\mathbf{S}).$$

Note that $\Delta^{\mathcal{D}}$ is a pseudo-metric. We denote the statement $\Delta^{\mathcal{D}}(\mathbf{R},\mathbf{S}) = 0$ by $\mathbf{R} \equiv \mathbf{S}$. It is known that deterministic distinguishers are optimal. Furthermore, for a resource S we define the specification $\mathbf{S}_d$ as

$$\mathbf{S}_d := \{\mathbf{R} : \Delta^{\mathcal{D}}(\mathbf{R},\mathbf{S}) \leq d\}.$$

Definition 1. A resource $\mathbf{S}$ is constructed from resource $\mathbf{R}$, denoted $\mathbf{R} \rightarrow \mathbf{S}$, if there exist converters $\pi_1, \pi_2, \sigma_1, \sigma_2 \in \Sigma$ such that

$$\begin{aligned} \pi_1\mathbf{R}\pi_2 &\equiv \mathbf{S} \\ \mathbf{R}\pi_2 &\equiv \sigma_1\mathbf{S} \\ \pi_1\mathbf{R} &\equiv \mathbf{S}\sigma_2. \end{aligned} \tag{1}$$

The converters σ_1 and σ_2 may also be called simulators.

In this paper we make heavy use of two resources. The first is a perfect communication channel between Alice and Bob that we denote by $\mathbf{C}$. The second is a resource for all or nothing oblivious transfer with probability p, which we denote by p-$\mathbf{OT}$. When $p = 1/2$ we denote the corresponding resource by $\mathbf{OT}$ for convenience. In p-$\mathbf{OT}$, Alice inputs a bit B at the left interface and Bob receives $B' \in \{0,1,?\}$ from the right interface. Furthermore, $P_{B'}[B' = B] = p$ and $P_{B'}[B' =?] = 1-p$.

III. Generalizing weak oblivious transfer – constructively

In this section we describe a resource we name $\mathbf{FOT}$ (for *faulty oblivious transfer*) which is a generalized form of weak oblivious transfer. This resource allows to capture, as special cases, existing notions of weak oblivious transfer (see [5], [6] and [9]). We focus on one particular instantiation of $\mathbf{FOT}$, which we denote by ρ-$\mathbf{FOT}$. For example, ρ-$\mathbf{FOT}$ already captures (p,q,ε)-$\mathbf{WOT}$ as defined in [5] and [6]. Furthermore, we show that Crépeau's protocol from [1] is captured by a different instantiation of ρ-$\mathbf{FOT}$. We highlight the fact that each instantiation of $\mathbf{FOT}$ must specify the global chronological order of inputs and outputs. This subtlety becomes relevant, for example, when studying symmetry in Section IV.

Suppose that Alice has secret bits X_0 and X_1 and Bob has a selection bit S. Furthermore, consider random variables D and E over $\{0,1\}$ and a random variable C over $\{0,1,2\}$ distributed according to a joint probability distribution $\rho := P_{CDE}$. Note that we do not assume anything regarding the correlation between C, D and E.

Consider the following set of actions of ρ-$\mathbf{FOT}$.

1) Bob receives C.
2) Bob inputs his selection bit S.
3) Alice receives V, where
$$V = \begin{cases} ? & \text{if } D = 0 \\ S & \text{if } D = 1 \end{cases} \tag{2}$$
4) Alice inputs X_0 and X_1.
5) Bob receives Y, where
$$Y = \begin{cases} ? & \text{if } C = 0 \\ \overline{X_S} & \text{if } C = 1 \\ (\overline{X_S}, X_{1-S}) & \text{if } C = 2 \end{cases} \tag{3}$$
where $\overline{X_S} = E \oplus X_S$.

Intuitively, D models Alice's ability to learn Bob's selection bit, C models Bob's ability to learn one, both or none of Alice's secret bits, and E models a possible transmission error. We can then define instantiations of ρ-$\mathbf{FOT}$ by simply providing a valid order of the above actions and the joint probability distribution of C, D, and E. For our set of actions it suffices to fix the relative order of actions 1 and 2 and of actions 3 and 4 to define a full order of the actions. For Alice's interface, $\uparrow$ means "3 before 4" and, for Bob's interface, "1

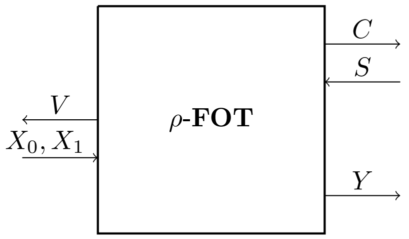

Fig. 1. A graphical representation of the ρ-$\mathbf{FOT}^{\uparrow\uparrow}$ resource. Note the order imposed on the inputs and outputs. The arrows are ordered from top to bottom by a chronological order which applies to both interfaces.

before 2”. The reversed arrow $\downarrow$ means the opposite statement for each interface. We can fix an order by specifying the arrows for Alice and Bob. Given $O \in \{\uparrow\uparrow, \uparrow\downarrow, \downarrow\uparrow, \downarrow\downarrow\}$ and a joint probability distribution ρ we define the resource ρ-$\mathbf{FOT}^O$ as ρ-$\mathbf{FOT}$ with the order induced by O and where C, D and E have joint probability distribution ρ. If $O =\uparrow\uparrow$ we may write ρ-$\mathbf{FOT}$ for convenience. Note that this yields an avenue for defining notions of $\mathbf{FOT}$ which are more general or with a completely different set of actions in a natural way. Nevertheless, we stick to ρ-$\mathbf{FOT}^O$ for ease of presentation because it is already quite general and because it serves the purposes of the paper.

One can show that Crépeau's protocol for reducing 1-2-$\mathbf{OT}$ to $\mathbf{OT}$ (see [1] for a detailed explanation of the protocol) is captured by ρ-$\mathbf{FOT}$.

Most of the results in this paper do not depend on the correlation between C, D and E but only on their marginal distributions. Thus we can define useful specifications for ρ-$\mathbf{FOT}$ in a very natural way.

Definition 2. Given a tuple $(\alpha, \beta, \gamma, \delta)$ with $\alpha, \beta, \gamma \in [0, 1]$, $\delta \in [0, 1/2]$ and $\beta + \gamma \leq 1$ and an order O, we define the specification $(\alpha, \beta, \gamma, \delta)$-$\mathbf{FOT}^O$ as the set of all resources ρ-$\mathbf{FOT}^O$ such that $P_D(1) = \alpha$, $P_E(1) = \delta$ and

$$P_C(c) = \begin{cases} \gamma & \text{if } c = 0 \\ 1 - \beta - \gamma & \text{if } c = 1 \\ \beta & \text{if } c = 2 \end{cases} \tag{4}$$

In this paper we mainly work with specifications $(\alpha, \beta, \gamma, \delta)$-$\mathbf{FOT}^{\uparrow\uparrow}$, which we denote by $(\alpha, \beta, \gamma, \delta)$-$\mathbf{FOT}$ for convenience. Note that when $\delta = 0$ and at least one of α, β, γ is 0 or 1 then the specification $(\alpha, \beta, \gamma, \delta)$-$\mathbf{FOT}$ contains only one resource. In this case we may identify the specification and the resource contained in the specification.

It is easy to see now that (p, q, ε)-$\mathbf{WOT}$ can be seen as the union of all specifications $(\alpha, \beta, 0, \delta)$-$\mathbf{FOT}^{\downarrow\downarrow}$ such that $\alpha \leq p$, $\beta \leq q$ and $\delta \leq \varepsilon$.

If we assume that we have access to a limited number k of $\mathbf{OT}$ calls, then Crépeau's protocol allows us to obtain a particular instance of ρ-$\mathbf{FOT}$.

Theorem 1.

$$\mathbf{OT}^k||\mathbf{C} \to (0, \beta, \gamma, 0)\text{-}\mathbf{FOT}.$$

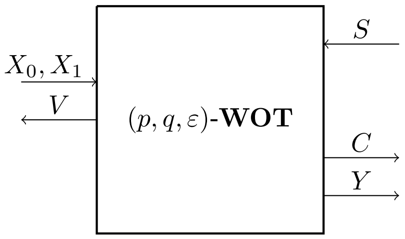

Fig. 2. A graphical representation of an element of (p, q, ε)-$\mathbf{WOT}$. Note that this is an instance of ρ-$\mathbf{FOT}^{\downarrow\downarrow}$ with $P_C(0) = 0$.

where $\beta = F(k, 3k/4)$ *and* $\gamma = F(k, 5k/8)$.

Proof Sketch: The high-level intuition for this result comes from the fact that Bob learns how many secret bits he will receive (but not their values) when he receives bits $c_1, \ldots, c_k$ from Alice through the k $\mathbf{OT}$ resources. For example, if $|\{i : c_i \neq ?\}| \geq 3k/4$ then Bob can learn both bits. Bob only learns the values of the secret bits he is supposed to receive *after* inputting his selection bit. On the other hand, Alice learns no information about Bob's selection bit. It is then easy to see that $(0, \beta, \gamma, 0)$-$\mathbf{FOT}$ is securely constructed with

$$\beta = \Pr[|\{i : c'_i \neq ?\}| \geq 3k/4] = F(k, 3k/4)$$

and

$$\gamma = \Pr[|\{i : c'_i \neq ?\}| < 3k/8] = F(k, 5k/8).$$

■

IV. Symmetry

The question of whether oblivious transfer can be reversed is well motivated (for example by differences in computational power between Alice and Bob) and has received some attention in the past. It was first stated and answered by Crépeau and Sántha in [8]. Later, Wolf and Wullschleger showed that one can obtain reversed 1-2-$\mathbf{OT}$ from a single instance of 1-2-$\mathbf{OT}$ and a clear channel in [7]. It is then natural to ask whether one can reverse weak oblivious transfer from a single instance of weak oblivious transfer and a clear channel, and what kind of properties influence symmetry results.

In this section we present partial symmetry results for certain subclasses of $\mathbf{FOT}$. It is clear that the subtleties outlined earlier show up here in a fundamental way. In fact, when reversing a certain resource we may want some particular chronological order of inputs and outputs to hold for the reversed resource (for example, we may want the reversed resource to keep the same order as the original resource). Our general $\mathbf{FOT}$ resource and the constructive cryptography framework allow us to reason about these fine-grained symmetry questions. We refer to the reversed versions of ρ-$\mathbf{FOT}^O$ and $\mathbf{OT}$ as ρ-$\mathbf{TOF}^O$ and $\mathbf{TO}$, respectively. Thus, ρ-$\mathbf{TOF}^O$ and $\mathbf{TO}$ are the same as ρ-$\mathbf{FOT}^O$ and $\mathbf{OT}$ but with their left and right interfaces swapped. We can then define specifications $(\alpha, \beta, \gamma, \delta)$-$\mathbf{TOF}^O$ in the same way as for $\mathbf{FOT}$. Therefore, precise symmetry statements for ρ-$\mathbf{FOT}$ can be seen as constructive statements from $(\alpha, \beta, \gamma, \delta)$-$\mathbf{FOT}^{O}$ to $(\alpha', \beta', \gamma', \delta')$-$\mathbf{TOF}^{O'}$, where O and O' need not coincide.

A. Symmetry without a clear channel and an application to weak oblivious transfer amplification

In this subsection we show that we can obtain symmetry results with a single instance of ρ-$\mathbf{FOT}^{\downarrow\downarrow}$ and without using a clear channel.

Lemma 2. *For any $p \in (0,1)$ we have*

$$p\text{-}\mathbf{TO} \rightarrow (p,0,1,0)\text{-}\mathbf{FOT}^{\downarrow\downarrow}$$

and

$$\rho\text{-}\mathbf{FOT}^{\downarrow\downarrow} \rightarrow p\text{-}\mathbf{TO},$$

whenever C, D, and E are independent and $P_D(1) = p$.

Proof Sketch: To prove the first statement, note that a converter for Bob can always output $C = 0$ and $Y = ?$ and the converter for Alice can disregard all input at the outer interface and simply output V. To prove the second statement, note that a converter for Bob can input his secret bit as a selection bit. Then a converter for Alice can input random secret bits. In both cases the simulators are straightforward. ■

We also have the following lemma.

Lemma 3. *For any ρ-$\mathbf{FOT}^{\downarrow\downarrow} \in (\alpha, \beta, \gamma, 0)$-$\mathbf{FOT}$ and independent random variables C and D we have*

$$\rho\text{-}\mathbf{FOT}^{\downarrow\downarrow} \rightarrow (1-\gamma)\text{-}\mathbf{OT}.$$

Proof Sketch: We can define a converter for Alice which sets $X_0 = X_1 = b$, where b is Alice's secret bit. The converter for Bob can input a random selection bit S and output ? if $Y = ?$ or X_S otherwise. The corresponding simulators are straightforward. ■

As a corollary of Lemma 2 and Lemma 3 we obtain a partial symmetry result which does not require a clear channel.

Theorem 4. *For any ρ-$\mathbf{FOT}^{\downarrow\downarrow} \in (\alpha, \beta, \gamma, 0)$-$\mathbf{FOT}$ and independent random variables C and D we have*

$$\rho\text{-}\mathbf{FOT}^{\downarrow\downarrow} \rightarrow (1-\gamma, 0, 1, 0)\text{-}\mathbf{TOF}^{\downarrow\downarrow}.$$

While this result is to be seen as an example of a difference between weak and regular oblivious transfer, the simple ideas used to prove it can be applied to make progress in other questions. A natural question which can be posed is the following: From which instances of weak oblivious transfer can we obtain unconditionally secure 1-2-$\mathbf{OT}$? This has been studied extensively in [5] and [9]. In particular, the following impossibility theorem is proved in [5].

Theorem 5 (Impossibility Theorem from [5])**.** *Whenever $p + q + 2\varepsilon \geq 1$ there is $\mathbf{R} \in (p,q,\varepsilon)$-$\mathbf{WOT}$ such that for some $d > 0$ we have $\mathbf{R}^k \not\rightarrow$ 1-2-$\mathbf{OT}_d$ for every integer k.*

In [5] and [9] the authors focus on parameters which satisfy $p + q + 2\varepsilon < 1$, but one can ask the following: What happens when we go beyond the impossibility bound? Obviously, reduction methods in this case must exploit something other than the parameters (p,q,ε). We claim that the ideas from Lemma 2 provide a first stepping stone towards understanding weak oblivious transfer amplification beyond this bound. In fact, we have the following result.

Theorem 6. *For any (p,q,ε) with $p > 0$, an integer s and $\mathbf{R} \in (p,q,\varepsilon)$-$\mathbf{WOT}$ with C, D, and E independent and $P_D(1) \in (0,1)$ we have $\mathbf{R}^k \rightarrow$ 1-2-$\mathbf{OT}_{2^{-s}}$ for $k = O(\text{poly}(s))$.*

Proof Sketch: Note that if $p' := P_D(1)$ then we can construct p'-$\mathbf{TO}$ from R by Lemma 2. We can then apply Crépeau's construction from [1] to construct $S' \in$ 1-2-$\mathbf{TO}_{2^{-s}}$ using $O(\text{poly}(s))$ many copies of p'-$\mathbf{TO}$. Using the protocol from [7] for reversing 1-2-$\mathbf{OT}$ (described in the next subsection) we construct $S \in$ 1-2-$\mathbf{OT}_{2^{-s}}$ from S'. ■

This result can also be easily generalized to the case where not all instances of (p,q,ε)-$\mathbf{WOT}$ we are using have the same p' but are guaranteed to have $p' \in [a,b] \subset (0,1)$.

Some open questions naturally arise: can we extend this reduction method so that we can reduce 1-2-$\mathbf{OT}$ to instances of (p,q,ε)-$\mathbf{WOT}$ where C, D and E are almost independent in some sense? Can we get a similar result when $p = 0$?

B. Symmetry with a clear channel

Wolf and Wullschleger [7] presented a protocol for reversing 1-2-$\mathbf{OT}$, based on one instance of 1-2-$\mathbf{OT}$ and a clear channel, which is perfectly secure and optimal (as it needs only one bit of communication between Alice and Bob). We describe it below. Alice has a selection bit S and Bob has secret bits X_0 and X_1.

1) Alice generates $r \in_R \{0,1\}$ and inputs $(r, r \oplus S)$ to 1-2-$\mathbf{OT}$.
2) Bob inputs $X_0 \oplus X_1$ as his selection bit and receives output a. Then Bob computes $m = X_0 \oplus a$ and sends m to Alice through a clear channel.
3) Alice receives m and computes $X_S = m \oplus r$.

We make use of their protocol in the following theorem.

Theorem 7. *For any $p \in [0,1]$,*

$$(p,0,0,0)\text{-}\mathbf{FOT}||\mathbf{C} \rightarrow (0,p,0,0)\text{-}\mathbf{TOF}.$$

Furthermore, for any $q \in [0,1]$,

$$(0,q,0,0)\text{-}\mathbf{FOT}||\mathbf{C} \rightarrow (q,0,0,0)\text{-}\mathbf{TOF}.$$

Proof: The first claim follows from a direct application of Wolf and Wullschleger's protocol.

In order to prove the second claim we slightly adapt Wolf and Wullschleger's protocol. The main observation behind our adaptation of the protocol is the fact that when Alice learns that $C = 2$ she can afterwards input a random selection bit, as she will receive both secret bits regardless. This means that we can define a converter π_2 that is able to correctly compute V before asking for Bob's secret bits.

Defining a converter π_1 and a simulator σ_1 for Alice is straightforward as it is again a direct application of Wolf and

```
CONVERTER $\pi_2$
receive $C$ at inner interface
if $C = 1$ then
    output $V =?$ at outer interface
    on input $(X_0, X_1)$ at outer interface, input $X_0 \oplus X_1$ at inner interface
    receive $a \in \{r, r \oplus s\}$ at inner interface
else
    generate $r \in_R \{0,1\}$
    input $r$ at inner interface
    on output $(b_0, b_1)$ at inner interface compute $s = b_0 \oplus b_1$
    output $V = s$ at outer interface
    on input $(X_0, X_1)$ at outer interface, set $a = b_{X_0 \oplus X_1}$
end if
compute $m = X_0 \oplus a$
input $m$ at the clear channel at inner interface
```

Fig. 3. Converter π_2 for Theorem 7.

```
SIMULATOR $\sigma_2$
receive $V$ at inner interface
if $V \neq ?$ then
    output $C = 2$ at outer interface
else
    output $C = 1$ at outer interface
end if
receive $a$ at outer interface
generate $r \in_R \{0,1\}$
if $C = 1$ then
    output $r$ at outer interface
else
    output $(r, r \oplus V)$ at outer interface
end if
receive $m$ at outer interface
if $C = 1$ then
    compute $X_0 = m \oplus r$ and $X_1 = X_0 \oplus a$
    input $(X_0, X_1)$ at inner interface
else
    compute $X_V = m \oplus r$
    generate $r' \in_R \{0,1\}$
    input $(r', X_V)$ at inner interface
end if
```

Fig. 4. Simulator σ_2 for Theorem 7.

Wullschleger's protocol. We show how to define a converter π_2 and a simulator σ_2 for Bob only. Refer to Figure 3 for π_2 and to Figure 4 for σ_2.

For defining σ_2, note that if $C = 1$ then Bob should choose $a = X_0 \oplus X_1$ and thus σ_2 can recover X_0 and X_1 at a later stage. Furthermore, if $C = 2$ then Bob can choose a random a. Nevertheless, it should be the case that $m \oplus r = b_S$, where S is Alice's selection bit. This is so because if $X_0 \oplus X_1 = 0$ then $m = X_0 \oplus r$ and then $m \oplus r = X_0 = X_S$. Moreover, if $X_0 \oplus X_1 = 1$ then $m = X_0 \oplus r \oplus S$ and so $m \oplus r = X_0 \oplus S = b_S$. Since we know S in this case we know how to input the secret bits into $\mathbf{TOF}$. Thus σ_2 is a valid simulator. ■

C. Other orders and instantiations

Although we can easily obtain partial symmetry results for ρ-$\mathbf{FOT}$ based on Wolf and Wullschleger's protocol, the reality is very different when we consider other instantiations of $\mathbf{FOT}$. In fact, if we consider ρ-$\mathbf{FOT}^{\downarrow\downarrow}$ then Wolf and Wullschleger's protocol fails. This failure is due to the fact that Alice and Bob only learn leaked information *after* inputting their secret bits and selection bit, respectively. Recall that in ρ-$\mathbf{FOT}$ Alice learns leaked information *before* inputting her secret bits. When we try to apply Wolf and Wullschleger's protocol to ρ-$\mathbf{FOT}^{\downarrow\downarrow}$ and we attempt to devise a simulator for Bob, we run into some problems. We receive a bit b from Bob, which should satisfy $b = X_0 \oplus X_1$ if Bob is honest. Furthermore, we should simulate outputting both secret bits from Alice (r and $r \oplus S$) with probability p. The problem we are faced with now is that to simulate outputting r and $r \oplus S$ we must know S, but we first need to input X_0 and X_1 to the reversed $\mathbf{FOT}$ to obtain S with probability p.

This property seems to be a fundamental barrier to proving symmetry results for a large class of $\mathbf{FOT}$ instantiations that are similar to ρ-$\mathbf{FOT}^{\downarrow\downarrow}$ (in the sense that the left interface only leaks information after receiving the secret bits). This is not an issue when dealing with ρ-$\mathbf{FOT}$ because we learn S before inputting X_0 and X_1. Thus, the order of inputs and outputs in weak oblivious transfer seems to have an important effect on the kind of properties we can prove about such resources.

ACKNOWLEDGMENT

João Ribeiro is supported by an Excellence Scholarship awarded by ETH Zurich.

REFERENCES

[1] C. Crépeau, Equivalence between two flavours of oblivious transfers, *Advances in Cryptology–CRYPTO 87*, Springer-Verlag, pp. 350–354, 1988.

[2] C. Crépeau and J. Kilian, Achieving oblivious transfer using weakened security assumptions, *29th Annual Symposium on Foundations of Computer Science*, pp. 42–52, 1988.

[3] U. Maurer and R. Renner, Abstract Cryptography, *The Second Symposium in Innovations in Computer Science, ICS 2011*, Tsinghua University Press, pp. 1–21, 2011.

[4] U. Maurer, Constructive cryptography – A new paradigm for security definitions and proofs, *Theory of Security and Applications (TOSCA 2011)*, Lecture Notes in Computer Science, Springer-Verlag, vol. 6993, pp. 33–56, 2011.

[5] I. Damgård, J. Kilian and L. Salvail, On the (im) possibility of basing oblivious transfer and bit commitment on weakened security assumptions, *Advances in Cryptology–EUROCRYPT 99*, Springer-Verlag, pp. 56–73, 1999.

[6] I. Damgård, S. Fehr, K. Morozov and L. Salvail, Unfair noisy channels and oblivious transfer, Springer-Verlag, pp. 355–373, 2004.

[7] S. Wolf and J. Wullschleger, Oblivious transfer is symmetric, *Advances in Cryptology–EUROCRYPT 06*, Springer-Verlag, pp. 222-232, 2006.

[8] C. Crépeau and M. Sántha, *Advances in Cryptology– EUROCRYPT 91*, Springer-Verlag, pp. 106–113, 1991.

[9] J. Wullschleger, Oblivious-transfer amplification, *Advances in Cryptology–EUROCRYPT 07*, Springer-Verlag, pp. 555–572, 2007.