New Impossibility Results for Concurrent Composition and a Non-Interactive Completeness Theorem for Secure Computation

Shweta Agrawal * Vipul Goyal † Abhishek Jain ‡ Manoj Prabhakaran § Amit Sahai ¶

Abstract

We consider the *client-server* setting for the concurrent composition of secure protocols: in this setting, a single server interacts with multiple clients concurrently, executing with each client a specified protocol where only the client should receive any nontrivial output. Such a setting is easily motivated from an application standpoint. There are important special cases for which positive results are known – such as concurrent zero knowledge protocols – and it has been an open question explicitly asked, for instance, by Lindell [J. Cryptology'08] – whether other natural functionalities such as Oblivious Transfer (OT) are possible in this setting.

In this work:

- We resolve this open question by showing that unfortunately, even in this very limited concurrency setting, **broad new impossibility results** hold, ruling out not only OT, but in fact all nontrivial asymmetric functionalities. Our new negative results hold even if the inputs of all honest parties are fixed in advance, and the adversary receives no auxiliary information.
- Along the way, we establish a new **unconditional completeness result** for asymmetric functionalities, where we characterize functionalities that are *non-interactively complete* secure against active adversaries. When we say that a functionality $\mathcal{F}$ is non-interactively complete, we mean that every other asymmetric functionality can be realized by parallel invocations of several copies of $\mathcal{F}$, with no other communication in any direction. Our result subsumes a completeness result of Kilian [STOC'00] that uses protocols which require additional interaction in both directions.

*UCLA. Email: shweta@cs.ucla.edu. Research supported in part from a DARPA/ONR PROCEED award, NSF grants 1136174, 1118096, 1065276, 0916574 and 0830803, a Xerox Faculty Research Award, a Google Faculty Research Award, an equipment grant from Intel, and an Okawa Foundation Research Grant. This material is based upon work supported by the Defense Advanced Research Projects Agency through the U.S. Office of Naval Research under Contract N00014-11-1-0389. The views expressed are those of the author and do not reflect the official policy or position of theDepartment of Defense or the U.S. Government.

†MSR, India. Email: vipul@microsoft.com

‡UCLA. Email: abhishek@cs.ucla.edu

§UIUC. Email: mmp@uiuc.edu Supported by NSF grant CNS 07-47027.

¶UCLA. Email: sahai@cs.ucla.edu. Research supported in part from a DARPA/ONR PROCEED award, NSF grants 1136174, 1118096, 1065276, 0916574 and 0830803, a Xerox Faculty Research Award, a Google Faculty Research Award, an equipment grant from Intel, and an Okawa Foundation Research Grant. This material is based upon work supported by the Defense Advanced Research Projects Agency through the U.S. Office of Naval Research under Contract N00014-11-1-0389. The views expressed are those of the author and do not reflect the official policy or position of theDepartment of Defense or the U.S. Government.

1 Introduction

Consider the following scenario: Goldman Sachs, which has collected in-depth market research and analysis on various companies, wishes to offer a paid service to high-profile investors who are interested in using this market research. For this purpose, it has set up a large server to which potential clients can connect in order to obtain answers to queries of an authorized kind (for which they have paid). Potential investors, however, are wary of Goldman Sachs learning about their business plans, and would want to hide the queries from Goldman Sachs – indeed, Goldman Sachs should learn nothing at all except that the client performed an authorized query. On the other hand, Goldman Sachs would like to ensure that in one session, a client can only learn the answer to a single query of a kind that it is authorized to ask. In particular, it would like to ensure that multiple clients who may connect to the server simultaneously, cannot perform a *coordinated attack* to learn more information than what each of them paid for (or even carry out an unauthorized query).

Can we satisfy these requirements? While well-known two-party computation protocols (e.g., [Yao86, GMW87]) offer remarkably powerful simulation-based security guarantees, these guarantees hold only in the stand-alone model, where only one protocol execution takes place. Our scenario is slightly more complex, as it has some mild concurrency in that multiple clients may interact with the server concurrently. At the same time, we are making the plausible assumption that the server is programmed only to interact with clients using the prescribed protocol, and we do not seek to guarantee security of any other protocols that the clients may be engaged in while they are communicating with the server[1]. Arguably, such a *client-server* setting (formally, asymmetric functionalities in a "fixed-role concurrent self composition" setting) is of great practical relevance. But apart from the practical significance, from a theoretical point of view, it is an important question as to whether restricting to such a model of concurrent executions of a single protocol, allows us to recover strong security guarantees for two-party computation (at least for some functionalities).

In this work, we consider secure computation in the client-server setting, and show that, even in this highly restricted concurrency setting, broad impossibility results for secure computation hold.

- We establish **new and broad impossibility results** for achieving security under fixed-roles concurrent self composition, ruling out *all finite functionalities* (except "trivial" ones which have universally composable protocols), including many natural functionalities such as oblivious transfer. Our results hold even if the inputs to the parties in all sessions are fixed before the protocols commence.
- Along the way, we establish a new **unconditional completeness result** for asymmetric functionalities, where we characterize functionalities that are *non-interactively complete*[2] for secure computation against active adversaries. This subsumes a result of Kilian [Kil00] that used a protocol which had additional interaction and, for its security, relied on the properties of a Nash equilibrium of a zero-sum game.

Background: Security under Concurrent Composition. With the proliferation of the network setting, in particular the *Internet*, the last decade has seen a push towards constructing protocols that have strong concurrent composability guarantees. For example, we could require security under *concurrent self-composition* (which is the focus of this work): a protocol should remain secure even when there are multiple copies executing concurrently. The framework of universal composability (UC) [Can01] was introduced to capture the more general setting of *concurrent general composition*, where a protocol may be executed concurrently with not only several copies of itself but also with other arbitrary protocols.

General positive results for UC secure computation have been obtained based on various *trusted* setup assumptions such as a common random string [CF01, CLOS02, BCNP04, CPS07, Kat07, LPV09]. Whether a given set of players is actually willing to trust an external entity, however, is debatable. Indeed a driving goal in cryptographic research is to eliminate the need to trust other parties. Ideally, we would like to achieve security under concurrent composition in the *plain model* (which is the main focus of this work).

[1] If we did consider the security of other protocols that the clients were engaged in, then known sweeping impossibility results would apply. See further details below.

[2] We say that a functionality $\mathcal{F}$ is non-interactively complete if every other asymmetric functionality can be realized by parallel invocations of several copies of $\mathcal{F}$, with no other communication in any direction.

The Dark Side of Concurrency. Unfortunately, in the plain model, by and large, most of the results have been negative.[3] UC secure protocols for most functionalities of interest were ruled out in [CF01, CKL03, PR08]. (Recently, these were extended to various public key models in [KL11].) These impossibility results were extended to the setting of general composition by Lindell [Lin03] who proved that security under concurrent general composition implies UC security. Later, Lindell [Lin04] established broad negative results even for the setting of concurrent self-composition by showing equivalence of concurrent self-composition and general composition for functionalities where each party can "communicate" to the other party via its output (referred to as *bit transmitting functionalities*). Barak et al. [BPS06] (and more recently, [Goy11]) obtained negative results for very specific functions in the "static-input" setting (i.e., where the inputs of honest parties are fixed in advance for all the protocol sessions).

On the positive side, there has been much success in obtaining construction for zero-knowledge and related functionalities, with security in similar models (e.g., [DNS98, RK99, KP01, PRS02, BPS06, Lin08]). Very recently, Goyal [Goy11] has been able to obtain positive results for a large class of functionalities in this setting with the restriction that an honest party uses the *same*, static input in all of the sessions. However these results do not translate to the more general setting where the server may choose different inputs in different sessions. Indeed, in a scenario such as the one discussed earlier, if the server is required to use the same static input in all sessions, it will have to allow all clients the same level of access, and further use its *entire* database in every computation (which may be impractical).

Our Question: Static-Input, Fixed-Roles Concurrent Self-Composition? In this work, we study the (im)possibility of achieving secure two-party computation with respect to a very weak notion of concurrency as occurs in the *client-server* setting: one server interacts with many clients using the same protocol, always playing the same role, while each (honest) client interacts only with the server. Further, the functionalities being computed are *asymmetric*, in that only the client gets any output.[4]

The adversarial model is that either the clients or the server may be adversarial – this is referred to as the *fixed roles* setting in the literature [Lin04].[5,6] We note that this is a very natural setting and captures several important functionalities such as **oblivious transfer**. However, despite extensive prior work on concurrent security, this setting has remained largely unstudied for general secure two-party computation (with the exception of [BPS06, Goy11] as discussed above). Indeed, concurrent security of oblivious transfer under (unbounded) concurrent composition was left was an explicit open problem by Lindell (see [Lin08, pg. 6]).

The importance of the above question stems from the fact that if the answer is positive, then it would enable security of many application scenarios, such as the one discussed at the beginning. On the other hand, if the answer is negative, then the situation would indeed be quite stark, and reaffirm the need for relaxing the standard security definitions. The recent positive results of Goyal [Goy11] may give hope that the answer is positive. Unfortunately, in this work, we show that the latter case holds.

We now proceed to describe our results.

1.1 Our Results

We obtain negative results regarding two-party computation with security under concurrent self-composition in the *fixed-roles* setting, along with positive results on UC-secure reductions that were used to get the negative results. (These are formally stated in Section 6.)

[3] We remark that several works have obtained positive results for "non-standard" simulation-based security, in which the simulator, for example, has access to super-polynomial computational power [Pas03, PS04, BS05, MPR06, GJO10, CLP10, GGJS12]. In this work, we will focus on security w.r.t. standard (polynomial time) simulation.

[4] Functionalities in which both parties receive output (which is not entirely a function of their local input) are more "complex" and already ruled out by Lindell [Lin04], when the inputs could be adaptively chosen.

[5] One could consider the corruption model where one or more clients and the server are corrupted. We note that if communication pattern is "bipartite" (i.e., honest clients do not talk to each other), then this is also covered in the fixed roles setting.

[6] Note that in the setting of *inter-changeable roles* (i.e., where parties may assume different roles in different protocol executions), essentially all non-trivial functionalities allow bit-transmission, and hence the negative results of Lindell [Lin04] are applicable.

- We give a **full-characterization** of security under concurrent self-composition for deterministic *asymmetric* finite functionalities (in which only one party receives output). (Theorem 5.) Specifically, we prove that no *non-trivial* deterministic asymmetric finite functionality can be computed securely under concurrent self composition, while *trivial* ones can be computed UC securely against active adversaries. (A deterministic asymmetric functionality is said to be non-trivial if there does not exist a single input for the receiver that "dominates" all other inputs.) Our results are *unconditional* and hold in the *static-input* setting, and thus also rule out the more general case where a party may choose its input in a session *adaptively*, based on the outcomes of the previous sessions. Further, our results are "robust" in the sense that the impossibility is not because honest parties could choose their inputs by reacting to signals sent by corrupt parties over subliminal channels.

  In particular, our results rule out concurrent security of 1-out-of-2 oblivious transfer and thus settle the open question of Lindell [Lin08]. Furthermore, to the best of our knowledge, these are the first broad impossibility results in the *static-input* setting. (In contrast, prior works which considered static inputs [BPS06, Goy11] only ruled out very specific functionalities.)

- To prove the above, we first construct a new UC-secure *asynchronous non-interactive* protocol for 1-out-of-2 oblivious transfer ($\mathcal{F}_{\mathsf{OT}}$) using any given non-trivial deterministic asymmetric functionality $\mathcal{F}$, thereby subsuming a result of Kilian [Kil00]. By a non-interactive protocol we mean that the only step in the protocol is to invoke, in parallel, several copies of the given functionality $\mathcal{F}$; we say that the protocol is asynchronous if it remains secure even if the adversary can adaptively schedule the different invocations of $\mathcal{F}$. (Theorem 3.)

  - Combining the above protocol with a UC-secure non-interactive protocol from [IPS08, Full version] for any asymmetric functionality $\mathcal{F}$ given $\mathcal{F}_{\mathsf{OT}}$, we obtain a full characterization of completeness among deterministic asymmetric functionalities with respect to non-interactive reductions. (Theorem 7.)

- We further devise a *composition theorem* for static-input fixed-role concurrent security. (Theorem 1.) This theorem holds only for asynchronous non-interactive protocols. Given this theorem and our asynchronous non-interactive OT protocol, we complete the proof of our main result by establishing the impossibility of static-input, fixed-role concurrently secure protocols for $\mathcal{F}_{\mathsf{OT}}$. (Theorem 2.)

  Independent Work. Independent of our work, exciting results concerning the impossibility of concurrently secure computation have been obtained recently by Garg et al. [GKOV12]. We refer the reader to [GKOV12] for more details.

1.2 Our Techniques

Asynchronous Non-Interactive Protocol for $\mathcal{F}_{\mathsf{OT}}$. As mentioned above, the first ingredient in our main result, and a contribution of independent interest, is an asynchronous non-interactive protocol for $\mathcal{F}_{\mathsf{OT}}$ given any non-trivial deterministic asymmetric functionality $\mathcal{F}$. To obtain the impossibility result in the static-input setting it is vital that this protocol is non-interactive *and asynchronous*.

Let $\mathcal{F}$ be a *non-trivial* asymmetric functionality that takes inputs x and y from Alice and Bob respectively, and outputs $f(x, y)$ to Bob. The intuitive reason why such a functionality $\mathcal{F}$ can yield $\mathcal{F}_{\mathsf{OT}}$ is that Bob has no input which will let it learn Alice's input to $\mathcal{F}$ exactly (up to equivalent inputs), where as Alice does not learn anything about Bob's input to $\mathcal{F}$. In particular, one can find two inputs $\hat{y}^0$ and $\hat{y}^1$ for Bob, such that if Alice chooses her input x at random, the only way Bob can learn $f(x, \hat{y}^0)$ with full certainty is if he chooses $\hat{y}^0$ as his input; similarly, unless he deterministically chooses $\hat{y}^1$ as his input, Bob will be left with some entropy regarding $f(x, \hat{y}^1)$. Thus Bob can choose to learn at most one of $f(x, \hat{y}^0)$ and $f(x, \hat{y}^1)$ exactly. There are two main challenges in turning this idea into an implementation of $\mathcal{F}_{\mathsf{OT}}$:

– Bob learns some information about $f(x, \hat{y}^0)$ when he uses $\hat{y}^1$ as an input, and vice versa, whereas in $\mathcal{F}_{\mathsf{OT}}$, he should not learn any information about one of Alice's two inputs (and learn the other one completely).

– Alice and Bob may deviate from the prescribed distributions when choosing their inputs to $\mathcal{F}$. In particular, any solution to the above issue should work even if Bob uses an input other than $\hat{y}^0$ and $\hat{y}^1$.

Kilian [Kil00] handles the issue of active adversaries using properties of a Nash equilibrium of an appropriate zero-sum game. However, this approach (apart from being not asynchronous) appears suitable only for constructing an erasure channel, and does not permit Bob to use an input. (Converting the erasure channel to $\mathcal{F}_{\mathsf{OT}}$ requires interaction.) The way [KM11] handles active corruption using cut-and-choose checks is highly interactive and again inadequate for our purposes.

One natural approach one could consider is to use an extractor to amplify the uncertainty Bob has about $f(x, \hat{y}^0)$ or $f(x, \hat{y}^1)$ from many invocations of $\mathcal{F}$ (with x independently randomly chosen each time). That is, if Bob has some uncertainty about at least one of the strings, R^0 and R^1 where R^0 (respectively, R^1) is defined as the string of outputs Bob would have received if he chose $\hat{y}^0$ (respectively, $\hat{y}^1$) as his input in all invocations of $\mathcal{F}$, then Alice can choose two seeds for a strong extractor and obtain two masks r_0 and r_1 as the strings extracted from R^0 and R^1 respectively, using these seeds. Unfortunately, *this is not secure in an asynchronous protocol*. Alice must transmit the extractor seeds she picked to Bob (for which she can use instances of $\mathcal{F}$). However, in an asynchronous non-interactive protocol, a corrupt Bob can *first receive the extractor seeds* before picking its inputs for the other instances of $\mathcal{F}$; hence the seeds are not independent of the information Bob obtains about R^0 and R^1, and the guarantees of extraction no more hold.

We get around this by avoiding using *the full power of extractors*, and in fact using a deterministic function in its place. For instance, when f is a boolean function, consider defining r_0 as simply the XOR of all the bits in R^0 (and similarly r_1). Since Alice picks her input x to $\mathcal{F}$ independently for each invocation, this still guarantees that if Bob has uncertainty about sufficiently many bits in R^0, then he has almost no information about r_0.

But using a linear function in place of the extractor will not suffice when Bob can use inputs other than $\hat{y}^0$ and $\hat{y}^1$. In particular, for boolean functions again, if there is an input $\hat{y}^2$ such that $f(x, \hat{y}^2) = f(x, \hat{y}^0) \oplus f(x, \hat{y}^1)$, then using this input in all invocations, Bob can learn $R^0 \oplus R^1$, and $r_0 \oplus r_1$. Our solution to this is to use a simple "quadratic" function, after appropriately mapping Bobs outputs to a field. This lets us ensure that one of the two "extracted" strings r_0 and r_1 remains almost uniformly random, even given the other string.

Impossibility for $\mathcal{F}_{\mathsf{OT}}$. As the next step towards our final impossibility result, we rule out a protocol for concurrent OT even for the case where both parties have fixed roles. The basic idea behind this impossibility result builds on the techniques from [BPS06, Goy11]. The proof proceeds in the following steps. Suppose, towards contradiction, we are given a protocol Π_{OT} that securely realizes OT in our setting.

1. First, we will construct an instance of the *chosen protocol attack* for this protocol. More precisely, we will construct a protocol $\widehat{\Pi_{\mathsf{OT}}}$ such that the protocols Π_{OT} and $\widehat{\Pi_{\mathsf{OT}}}$ are *insecure* when executed concurrently. We will have three parties in the system: Alice and Eve running Π_{OT} (as sender and receiver respectively); Eve and David running $\widehat{\Pi_{\mathsf{OT}}}$ (as sender and receiver respectively). In our chosen protocol attack, Eve will be the corrupted party acting as man-in-the-middle between Alice and David and violating security of Π_{OT} (see Section 4 for more details of this step).

2. Next, we will use *one time programs* (OTPs) [GKR08, GIS$^+$10] to eliminate David. In more detail, Eve simply gets a set of one-time programs implementing the next message function of David.

3. To execute these one-time programs, the (possibly adversarial) Eve is required to carry out a number of oblivious transfer invocations. In these invocations, Alice can be given the required key and can act as the sender. Fortunately, oblivious transfer is exactly the functionality that Π_{OT} provides! So these OT invocations can be executed using the protocol Π_{OT}.

4. Thus, now there are only Alice and Eve running a number of concurrent executions of Π_{OT}. Hence, the chosen protocol attack we started with can now be carried out in our setting of concurrent self-composition with static-inputs and fixed-roles.

More details are provided in Section 4.

2 Preliminaries

Below we present some of the important definitions we need. Throughout this paper, we denote the security parameter by κ.

2.1 Notation

The following standard notation will be used throughout the paper. We say that a function $f : \mathbb{R}^+ \to \mathbb{R}^+$ is negligible if for all $d > d_0$ we have $f(\lambda) < 1/\lambda^d$ for sufficiently large λ. We write $f(\lambda) < \text{negl}(\lambda)$. For two distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ over some set Ω we define the statistical distance $\text{SD}(\mathcal{D}_1, \mathcal{D}_2)$ as

$$\text{SD}(\mathcal{D}_1, \mathcal{D}_2) := \frac{1}{2} \sum_{x \in \Omega} \left| \Pr_{\mathcal{D}_1}[x] - \Pr_{\mathcal{D}_2}[x] \right|$$

We say that two distribution ensembles $\mathcal{D}_1(\lambda)$ and $\mathcal{D}_2(\lambda)$ are statistically close or statistically indistinguishable if $\text{SD}\big(\mathcal{D}_1(\lambda), \mathcal{D}_2(\lambda)\big)$ is a negligible function of λ.

Similarly, we say that $\mathcal{D}_1(\lambda)$ and $\mathcal{D}_2(\lambda)$ are computationally indistinguishable (denoted as $\mathcal{D}_1 \stackrel{c}{\equiv} \mathcal{D}_1$) if for every probabilistic polynomial time distinguisher Dist, we have that $|\Pr(\mathsf{Dist}(\mathcal{D}_1(\lambda)) = 1) - \Pr(\mathsf{Dist}(\mathcal{D}_2(\lambda)) = 1)| = \mu(\lambda)$ where $\mu(\cdot)$ is some negligible function of λ.

2.2 Real and Ideal models.

IDEAL MODEL. An ideal execution with an adversary who controls P_2 proceeds as follows (when the adversary controls P_1, the roles are simply reversed):

Inputs: P_1 and P_2 obtain a vector of m inputs (where m denotes the number of sessions that P_1 and P_2 will execute), denoted $\vec{x}$ and $\vec{y}$ respectively.

Session initiation: The adversary initiates a new session by sending a $\mathsf{start\text{-}session}$ message to the trusted party. The trusted party then sends $(\mathsf{start\text{-}session}, i)$ to P_1, where i is the index of the session.

Honest party sends input to trusted party: Upon receiving $(\mathsf{start\text{-}session}, i)$ from the trusted party, honest party P_1 sends (i, x_i) to the trusted party, where x_i denotes P_1's input for session i.

Adversary sends input to trusted party and receives output: Whenever the adversary wishes, it may send a message (i, y_i') to the trusted party for any y_i' of its choice. Upon sending this pair, it receives back $(i, f_2(x_i, y_i'))$ where x_i is the input value that P_1 previously sent to the trusted party for session i. The only limitation is that for any i, the trusted party accepts at most one pair indexed by i from the adversary.

Adversary instructs trusted party to answer honest party: When the adversary sends a message of the type $(\mathsf{send\text{-}output}, i)$ to the trusted party, the trusted party sends $(i, f_1(x_i, y_i'))$ to P_i, where x_i and y_i' denote the respective inputs sent by P_1 and adversary for session i.

Outputs: The honest party P_1 always outputs the values $f_1(x_i, y_i')$ that it obtained from the trusted party. The adversary may output an arbitrary (probabilistic polynomial-time computable) function of its auxiliary input z, input vector $\vec{y}$ and the outputs obtained from the trusted party.

Let $\mathcal{S}$ be a non-uniform probabilistic polynomial-time machine (representing the ideal-model adversary). Then, the $\mathsf{ideal\ execution}$ of a function $\mathcal{F}$ with security parameter κ, input vectors $\vec{x}$, $\vec{y}$ and auxiliary input z to $\mathcal{S}$, denoted $ideal_{\mathcal{F},\mathcal{S}}(\kappa, \vec{x}, \vec{y}, z)$, is defined as the output pair of the honest party and $\mathcal{S}$ from the above ideal execution.

REAL MODEL. We now consider the real model in which a real two-party protocol is executed (and there exists no trusted third party). Let $\mathcal{F}$ be as above and let Π be a two-party protocol for computing $\mathcal{F}$. Let $\mathcal{A}$ denote a non-uniform probabilistic polynomial-time adversary that controls either P_1 or P_2. Then, the real concurrent execution of Π with security parameter κ, input vectors $\vec{x}$, $\vec{y}$ and auxiliary input z to $\mathcal{A}$, denoted $real_{\Pi,\mathcal{A}}(\kappa, \vec{x}, \vec{y}, z)$, is defined as the output pair of the honest party and $\mathcal{A}$, resulting from the following real-world process. The parties run concurrent executions of the protocol Π, where the honest party follows the instructions of Π in all executions. The honest party initiates a new session i with input x_i whenever it receives a start-session message from $\mathcal{A}$. The scheduling of all messages throughout the executions is controlled by the adversary. That is, the execution proceeds as follows: the adversary sends a message of the form (i, msg) to the honest party. The honest party then adds msg to its view of session i and replies according to the instructions of Π and this view.

2.3 One Time Programs

A one-time program (OTP) [GKR08, GIS+10] for a function f allows a party to evaluate f on a single input x chosen by the party dynamically. Thus, a one-time program guarantees that no efficient adversary, after evaluating the one-time program on some input x, can learn anything beyond $(x, f(x))$. In particular he gains no information about $f(y)$ for any $y \neq x$ outside of the information provided by $f(x)$. OTPs are *non interactive*; an OTP corresponding to some function f, $\mathsf{OTP\text{-}msg}_f$ given to a user by some environment (or user) U allows the user to evaluate f *once* on some input of its choice, with no further interaction with U. It is shown in [GKR08, GIS+10] that OTPs cannot be implemented by software alone. Thus, an OTP is typically implemented as a software plus hardware package, where the hardware is assumed to be secure (that is, can only be accessed in a black box way via its interface), and the software can be read and tampered with. The secure hardware devices that are used are called *one time memory* devices (OTM).

An OTM is a memory device initialized by two keys k_0, k_1 which takes as input a single bit b, outputs k_b and then "self destructs". OTMs were inspired by the oblivious transfer protocol, and indeed, for our purposes, we will find it necessary to use oblivious transfer in place of one time memory tokens. This approach is not new and has been used in previous works as well [GIS+10]. Thus, for our setting, we will define one-time programs in the $\mathcal{F}_{\mathsf{OT}}$-hybrid model directly for ease of use. We state this definition in terms of an *asynchronous, non-interactive* protocol (as defined above) for an asymmetric "one-time program functionality" $\mathcal{F}_{\mathsf{OTP}}$, which accepts a circuit f from the party P_1 and an input x from the party P_2, and returns $f(x)$ to P_2 (and notifies P_1) (see Figure 1). The protocol is required to be secure only against corruption of P_2. Note that the requirement of being non-interactive makes this non-trivial (i.e., P_2 cannot send its input to P_1 and have it evaluated).

Ideal Functionality of One Time Program

In Figure 1, we describe the ideal functionality of a One Time Program.

Functionality $\mathcal{F}^{\mathsf{OTP}}$

Create Upon receiving $(\mathsf{sid}, \mathsf{create}, P_1, P_2, f)$ from P_1 (with a fresh session ID sid), where f is a circuit for a function, do:

1. Send $(\mathsf{sid}, \mathsf{create}, P_1, P_2, \mathsf{size}(f))$ to P_2, where the size outputs the size of the circuit and the number of input wires it has.
2. Store (sid, P_2, f).

Execute Upon receiving $(\mathsf{sid}, \mathsf{run}, x)$ from P_2, find the stored tuple (sid, P_2, f) (if no such tuple exists, do nothing). Send $(\mathsf{sid}, \mathsf{value}, f(x))$ to P_2 and delete tuple (sid, P_2, f). (If x is not of the right size, define $f(x) = \perp$.) Send $(\mathsf{sid}, \mathsf{evaluated})$ to P_1.

Figure 1: Ideal functionality for One-time Program.

Definition 1 (One-Time Program)**.** (Adapted from [GKR08, GIS$^+$10]) A *one-time program (OTP) scheme* is an asynchronous two-party non-interactive protocol $\Pi^{\mathcal{F}_{\mathsf{OT}}}$ (in the $\mathcal{F}_{\mathsf{OT}}$-hybrid model) that UC-securely realizes $\mathcal{F}_{\mathsf{OTP}}$ (as defined in Figure 1) when the adversary is allowed to corrupt only P_2.

In other words, if $\Pi^{\mathcal{F}_{\mathsf{OT}}}$ is a one-time program scheme, then for every probabilistic polynomial time adversary $\mathcal{A}$ corrupting P_2, and adaptively scheduling the $\mathcal{F}_{\mathsf{OT}}$ sessions in the real-model execution of Π, there exists a probabilistic polynomial time ideal-world adversary $\mathsf{Sim}_{\mathsf{OTP}}$ (the simulator), such that for every environment $\mathcal{Z}$, it holds that $\mathsf{Ideal}^{f}_{\mathsf{Sim}_{\mathsf{OTP}},\mathcal{Z}} \stackrel{c}{\equiv} \mathsf{Real}^{\Pi}_{\mathcal{A},\mathcal{Z}}$, where $\mathsf{Ideal}^{f}_{\mathsf{Sim}_{\mathsf{OTP}},\mathcal{Z}}$ and $\mathsf{Real}^{\Pi}_{\mathcal{A},\mathcal{Z}}$ denote the outputs produced by $\mathsf{Sim}_{\mathsf{OTP}}$ and $\mathcal{A}$ respectively.

We shall refer to an execution of an OTP scheme with input f for P_1 as an *OTP for* f.

We note that OTPs exist if a (standalone secure) Oblivious Transfer protocol exists [GIS$^+$10], which in turn exists if a concurrent secure OT protocol exists. Thus, for proving the impossibility of concurrent secure OT protocols, we can assume the existence of OTPs "for free."

Intuitively, this means that for every probabilistic polynomial time algorithm $\mathcal{A}$ given access to a one-time program (or non interactive protocol Π) for some function f, there exists another probabilistic polynomial time algorithm $\mathsf{Sim}_{\mathsf{OTP}}$ which is given one time black box access to f, i.e. it can request to see the value $f(x)$ for any x of its choice, such that (for any f) the output distributions of $\mathsf{Sim}_{\mathsf{OTP}}$ (denoted by $\mathsf{Ideal}^{f}_{\mathsf{Sim}_{\mathsf{OTP}}}$) and $\mathcal{A}$ (denoted by $\mathsf{Real}^{\Pi}_{\mathcal{A}}$) are computationally indistinguishable, even to a machine that knows f.

According to our definition above, in an OTP protocol all communication is via asynchronous, parallel invocations of $\mathcal{F}_{\mathsf{OT}}$. However, to reflect the structure of OTPs as originally defined in [GKR08, GIS$^+$10] we shall consider the protocol to consist of some $\mathcal{F}_{\mathsf{OT}}$ instances invoked to simply communicate a message $\mathsf{OTP\text{-}msg}$ (which, w.l.o.g, an adversary would schedule first) and several other OT instances whose outputs we shall refer to as keys. (The reader may consider the OTP-msg to be empty, without any harm.)

Properties of OTPs: OTPs can be seen as providing a stronger privacy guarantee than garbled circuits. The garbled circuit construction works against honest-but-curious adversaries, but in our case we will need to consider malicious adversaries. More precisely, the garbled circuit simulator generates a dummy garbled circuit for circuit C, after the input x is specified, i.e. only after it knows the circuit's output $C(x)$. On the contrary, in our setting, we will need the simulator to construct the garbled circuit *before* he knows which input the adversary will choose to run it on. Garbled circuit simulators cannot handle this but OTP simulators can. We note that Barak et al. [BPS06] handle this by augmenting the garbled circuit construction with a *masking* technique, in which the desired output of the garbled circuit is masked with a random value in a way that allows the simulator to produce the garbled circuit for some random output (prior to knowing the desired output of the circuit), and provide keys/inputs *after* knowing the circuit output, in a manner that the input masks and output mask cancel each other out. Goyal [Goy11] instead used one-time programs that offer a cleaner abstraction to handle this issue directly. Hence we will find it more convenient to work directly with one-time programs.

OTP simulator : In the real world, the output of the adversary $\mathcal{A}$ consists of a one time program $\mathsf{OTP\text{-}msg}^{\mathsf{Real}}$ for a function f of circuit size ℓ (say), as well as one input to $\mathsf{OTP\text{-}msg}^{\mathsf{Real}}$, denoted by $\mathsf{keys}^{\mathsf{Real}} = \{\mathsf{key}_1^{\mathsf{Real}}, \ldots \mathsf{key}_k^{\mathsf{Real}}\}$ (for k input wires). Thus, $\mathsf{Real}^{\Pi}_{\mathcal{A},\mathcal{Z}} = \{\mathsf{OTP\text{-}msg}^{\mathsf{Real}}, \mathsf{keys}^{\mathsf{Real}}\}$.

We describe how our OTP simulator (denoted by $\mathsf{Sim}_{\mathsf{OTP}}$) interacts with some environment (or user), say U.

1. U gives $\mathsf{Sim}_{\mathsf{OTP}}$ a circuit size ℓ, $\mathsf{Sim}_{\mathsf{OTP}}$ returns a one time program $\mathsf{OTP\text{-}msg}^{\mathsf{Ideal}}$ for circuit size ℓ.
2. Let us assume that $\mathsf{OTP\text{-}msg}^{\mathsf{Ideal}}$ has k input wires, and denote these inputs by $\mathsf{key}_1^{\mathsf{Ideal}}, \ldots, \mathsf{key}_k^{\mathsf{Ideal}}$. U may query $\mathsf{Sim}_{\mathsf{OTP}}$ for the inputs to be provided to $\mathsf{OTP\text{-}msg}^{\mathsf{Ideal}}$. Then, $\mathsf{Sim}_{\mathsf{OTP}}$ returns inputs $\{\mathsf{key}_1^{\mathsf{Ideal}}, \ldots, \mathsf{key}_t^{\mathsf{Ideal}}\}$ for the first t bits, for some $t < k$ (we refer to the inputs as keys since they are similar to the keys that are input to garbled circuits).
3. After returning t inputs, $\mathsf{Sim}_{\mathsf{OTP}}$ produces a value, say x, and queries U for $f(x)$, i.e. the desired output of $\mathsf{OTP\text{-}msg}^{\mathsf{Ideal}}$ on x.

4. U provides the output, at which point $\mathsf{Sim}_{\mathsf{OTP}}$ returns the values for the remaining input wires $\{\mathsf{key}_{t+1}^{\mathsf{Ideal}}, \ldots, \mathsf{key}_{k}^{\mathsf{Ideal}}\}$. We will denote $\mathsf{keys}^{\mathsf{Ideal}} = \{\mathsf{key}_{1}^{\mathsf{Ideal}}, \ldots, \mathsf{key}_{k}^{\mathsf{Ideal}}\}$.

5. Output $\mathsf{Ideal}^{f}_{\mathsf{Sim}_{\mathsf{OTP}}} = \{\mathsf{OTP\text{-}msg}^{\mathsf{Ideal}}, \mathsf{keys}^{\mathsf{Ideal}}\} \stackrel{c}{\equiv} \{\mathsf{OTP\text{-}msg}^{\mathsf{Real}}, \mathsf{keys}^{\mathsf{Real}}\} = \mathsf{Real}^{\Pi}_{\mathcal{A},\mathcal{Z}}$.

Secure Computation Under Concurrent Self-Composition. In this section, we present the definition for concurrently secure two-party computation.

The definition we give below is an adaptation of the definition of security under concurrent self-composition from [Lin04], but with two further restrictions to the model — *fixed-roles* and *static-inputs* — i.e., there are only two parties engaged in multiple executions of a given protocol, with each playing the same "role" in all the sessions, and the inputs of the honest parties for each session is fixed in advance. (Recall that since the focus in this work is on obtaining impossibility results, our results are stronger by adding these restrictions.) Some parts of the definition below have been taken almost verbatim from [Lin04].

A two-party functionality[7] $\mathcal{F}$ with input domains X and Y for the two parties is defined by two functions $f_1 : X \times Y \to Z_A$ and $f_2 : X \times Y \to Z_B$, where Z_A, Z_B are the output domains. For most part we shall consider the input and output domains to be finite sets. Such functionalities are called *finite functionalities*. (Again, since our focus is on impossibility results, it is more interesting to show impossibility of finite functionalities than of infinite functionalities.)

We will denote the two parties that wish to jointly instantiate $\mathcal{F}$ as Alice and Bob (or sometimes P_1 and P_2). If Alice's input is $x \in X$ and Bob's input is $y \in Y$, then the functionality would output $f_1(x, y)$ to Alice and $f_2(x, y)$ to Bob (unless aborted by a corrupt party). A functionality is called *asymmetric* if only Bob receives any output; more precisely, in an asymmetric functionality f_1 is the constant function (Alice does receive this fixed output to indicate the termination of execution). An asymmetric functionality will be defined using a single function $f : X \times Y \to Z$.

In this work, we consider a malicious, static adversary. The scheduling of the messages across the concurrent executions is controlled by the adversary. The security of a protocol is analyzed by comparing what an adversary can do in the protocol to what it can do in an ideal scenario, where a trusted party computes the function output on the inputs of the parties. We do not require fairness (i.e., our impossibility is not a consequence of requiring fairness) and hence in the ideal model, we allow a corrupt party to receive its output in a session and then optionally block the output from being delivered to the honest party, in that session. Unlike in the case of stand-alone computation, in the setting of concurrent executions, the trusted party computes the functionality many times, each time upon different inputs. In Section 2.2 we present further details of the real and ideal model executions, following the description in [Lin04].

The output pair of the ideal-model adversary $\mathcal{S}$ and the honest party (or both parties, when neither corrupt) in an ideal-model execution of a functionality $\mathcal{F}$ with security parameter κ, input vectors $\vec{x}$, $\vec{y}$ and auxiliary input z to $\mathcal{S}$, will be denoted as $\text{IDEAL}_{\mathcal{F},\mathcal{S}}(\kappa, \vec{x}, \vec{y}, z)$. Similarly, the output pair of the real-model adversary $\mathcal{A}$ and the honest party (or parties) in a real-model concurrent execution of a protocol Π with security parameter κ, input vectors $\vec{x}$, $\vec{y}$ and auxiliary input z to $\mathcal{A}$ will be denoted by $\text{REAL}_{\Pi,\mathcal{A}}(\kappa, \vec{x}, \vec{y}, z)$.

Definition 2 (Security under Concurrent Self-Composition)**.** A protocol Π is said to *securely realize* a functionality $\mathcal{F}$ *under concurrent composition* if for every real model non-uniform probabilistic polynomial-time adversary $\mathcal{A}$, there exists an ideal-model non-uniform probabilistic expected polynomial-time adversary $\mathcal{S}$, such that for all polynomials $m = m(\kappa)$, every $z \in \{0,1\}^*$, every pair of input vectors $\vec{x} \in X^m$, $\vec{y} \in Y^m$,

$$\{\text{IDEAL}_{\mathcal{F},\mathcal{S}}(\kappa, \vec{x}, \vec{y}, z)\}_{\kappa\in\mathbb{N}} \stackrel{c}{\equiv} \{\text{REAL}_{\Pi,\mathcal{A}}(\kappa, \vec{x}, \vec{y}, z)\}_{\kappa\in\mathbb{N}}$$

We shall also consider a few *stronger* security definitions, that we achieve in our positive results (used in proving the main negative result). Firstly, we can require the above to hold even with probabilistic *expected*

[7] All functionalities considered in this paper are (unfair) secure function evaluation (SFE) functionalities. For simplicity we shall not explicitly qualify them as SFE or non-reactive.

polynomial time adversaries in the real-model. Secondly, we could in fact allow the real-model adversary to be computationally unbounded, and allow the ideal-model adversary to be unbounded too.[8] Also, we shall consider Universally Composable (UC) security [Can01, Can05]. We shall not present the details of the UC security definition (which has several slight variants, with essentially the same properties), but remark that it implies concurrent self-composition and more.

Finally, sometimes we permit the real model protocols to invoke ideal functionalities as sub-protocols (denoted like $\Pi^{\mathcal{F}}$, where $\mathcal{F}$ is the ideal functionality invoked by the parties in Π). In all the instances we do this, we can actually consider UC-security of the protocol; however this definition can be easily generalized to security under concurrent self-composition too, and would be useful in stating a composition theorem (without involving UC-security).

Non-Interactive Protocols and Asynchronous Non-Interactive Protocols. A two-party protocol $\Pi^{\mathcal{F}}$ (i.e., in the $\mathcal{F}$-hybrid model) is called a *non-interactive protocol* if the protocol has the following structure: the two parties carry out local computation; then together they invoke one or more *parallel, synchronized* sessions of $\mathcal{F}$; then they carry out more local computation and produce outputs. By synchronized sessions we mean that even corrupt players can invoke these sessions only in parallel.[9] We shall also require that all copies of $\mathcal{F}$ are invoked with the same fixed roles for the two parties.

A two-party protocol $\Pi^{\mathcal{F}}$ is called an *asynchronous non-interactive protocol* if the protocol has the above structure, but the parallel sessions of $\mathcal{F}$ are parallel but asynchronous. By this we mean that a corrupt player can invoke these sessions in arbitrary order, choosing the inputs for each session based on the outputs from prior sessions; the honest players have to choose their inputs *a priori* and remain oblivious to the order in which the sessions are invoked.

One Time programs. A one-time program (OTP) [GKR08, GIS$^+$10] for a function f allows a party to evaluate f on a single input x chosen by the party dynamically. As introduced in [GKR08, GIS$^+$10], an OTP is implemented as a package consisting of some software and hardware tokens (specifically *one time memory* tokens), that essentially provided the party with *asynchronous* access to several oblivious transfer invocations. We shall treat OTPs as an *asynchronous non-interactive protocol* in the OT-hybrid model (as was done in [GIS$^+$10]), that securely realizes an asymmetric "one-time program functionality" $\mathcal{F}_{\mathsf{OTP}}$ against corruption of the receiver alone. (See in Section 2.3 for a discussion.) $\mathcal{F}_{\mathsf{OTP}}$ accepts a circuit f from the party P_1 and an input x from the party P_2, and returns $f(x)$ to P_2 (and notifies P_1) (see Figure 1 in Section 2.3).

Definition 3 (One-Time Program)**.** (Adapted from [GKR08, GIS$^+$10]) A *one-time program (OTP) scheme* is an asynchronous two-party non-interactive protocol $\Pi^{\mathcal{F}_{\mathsf{OT}}}$ (in the $\mathcal{F}_{\mathsf{OT}}$-hybrid model) that UC-securely realizes $\mathcal{F}_{\mathsf{OTP}}$ (as defined in Figure 1) when the adversary is allowed to corrupt only P_2.

We shall refer to the collection of inputs P_1 provides to the $\mathcal{F}_{\mathsf{OT}}$ instances in an execution of $\Pi^{\mathcal{F}_{\mathsf{OT}}}$ when its input is a circuit f, as an *OTP for* f.

We note that OTPs exist if a (standalone secure) Oblivious Transfer protocol exists [GIS$^+$10], which in turn exists if a concurrent secure OT protocol exists. Thus, for proving the impossibility of concurrent secure OT protocols, we can assume the existence of OTPs "for free."

Our use of OTP parallels the use of garbled circuits in the impossibility result in [BPS06]. Following [Goy11], we use OTPs instead of garbled circuits, since they have stronger security properties (namely, security against an actively corrupt receiver), and allows one to simplify the construction in [BPS06].

[8] This is not a strengthening of the security definition, as the ideal-model is more relaxed now; however, the protocols we shall consider will satisfy this definition in addition to the other definitions.

[9] A more accurate notation for such a protocol that invokes at most t sessions of $\mathcal{F}$, would be $\Pi^{\mathcal{F}^t}$, where $\mathcal{F}^t$ stands for a non-reactive functionality implementing t independent copies of f. For simplicity we do not use this notation.

3 A Non-Interactive Protocol for OT from Any Non-Trivial Asymmetric SFE

The goal of this section is to obtain an asynchronous, non-interactive protocol for $\mathcal{F}_{\mathsf{OT}}$ in the $\mathcal{F}$-hybrid model, for *any* finite deterministic "non-trivial" asymmetric functionality $\mathcal{F}$. For our purposes, we define a *trivial* asymmetric functionality as follows. (As elsewhere in this paper, we consider only deterministic functionalities.)

Definition 4 (Dominating input.)**.** In an asymmetric functionality defined by a function $f : X \times Y \to Z$, an input $y \in Y$ for the receiver is said to *dominate* another input $y' \in Y$ if $\forall x_1, x_2 \in X$, $f(x_1, y) = f(x_2, y) \implies f(x_1, y') = f(x_2, y')$.

Definition 5 (Trivial functionality.)**.** An asymmetric functionality is called *trivial* if there exists an input for Bob that dominates all of its other inputs in the functionality.

Background. In [Kil00] Kilian presented an elegant protocol to show that any non-trivial asymmetric functionality is complete for security against active adversaries. The protocol, which constructs an erasure channel from a non-trivial asymmetric functionality $\mathcal{F}$, achieves security against active adversaries by using an input distribution to $\mathcal{F}$ derived from the Nash equilibrium of a zero-sum game defined using $\mathcal{F}$. Kilian shows that an adversary deviating from the prescribed distribution cannot change the erasure probability in the protocol. This rather enigmatic protocol does invoke $\mathcal{F}$ with fixed roles, but is not useful for showing impossibility of concurrent secure protocol for $\mathcal{F}$, because it is modestly interactive (two steps which should occur one after the other) and more importantly, because it yields only an erasure channel and not a $\binom{2}{1}$-OT.[10] The only known substitute for this protocol, by [KM11], is much more interactive, involving several rounds of communication in both directions, apart from the invocation of $\mathcal{F}$. Our challenge is to devise an *asynchronous non-interactive* protocol which uses $\mathcal{F}$ with fixed-roles and directly yields $\binom{2}{1}$-OT. Being non-interactive and asynchronous requires that all the sessions are invoked together by an honest party, but the adversary is allowed to schedule them adaptively, and base its inputs for later sessions based on the outputs from earlier sessions (rushing adversary). As mentioned in Section 1.2, this rules out some standard techniques like privacy amplification (using extractors), since the adversary can learn the seed used for extraction *before* it extracts partial information about a string to which the extraction will be applied.

We present a new and simple non-interactive OT protocol which uses a simple non-linear "extraction" strategy that does not require a seed, but is sufficient to amplify the uncertainty about certain values into almost zero information about at least one of two extracted values. Our protocol is in fact UC-secure (in the PPT as well as information theoretic settings) and is asynchronous.

3.1 The New Protocol

Our asynchronous non-interactive protocol UC-securely realizes the $\binom{2}{1}$-OT functionality $\mathcal{F}_{\mathsf{OT}}$ in the $\mathcal{F}$-hybrid model, where $\mathcal{F}$ is a finite[11] asymmetric functionality defined by a function $f : X \times Y \to Z$, and $\mathcal{F}$ is *not trivial*. Note that (since domination is transitive) this means that there are at least *two inputs* in Y — denoted by $\hat{y}^0$ and $\hat{y}^1$ — which are not dominated by any other input $y \in Y$.

To define the protocol, first we pick a prime number $p \geq \min\{|X|, |Z|\}$. Then we can define two maps to relabel the columns corresponding to $\hat{y}^0$ and $\hat{y}^1$ in the function table of f using elements in $\mathbb{Z}_p$ – i.e., two injective functions $N_0 : Z_0 \to \mathbb{Z}_p$, $N_1 : Z_1 \to \mathbb{Z}_p$, where $Z_b = \{f(x, \hat{y}^b) | x \in X\}$ – such that there exist $\hat{x}^0, \hat{x}^1 \in X$ satisfying the following.

$$\begin{bmatrix} N_0\big(f(\hat{x}^0, \hat{y}^0)\big) & N_1\big(f(\hat{x}^0, \hat{y}^1)\big) \\ N_0\big(f(\hat{x}^1, \hat{y}^0)\big) & N_1\big(f(\hat{x}^1, \hat{y}^1)\big) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

We claim that this is possible as follows.

[10] Our impossibility result in Section 4 holds only for $\binom{2}{1}$-OT, and not for erasure channels. Indeed, using techniques in [Goy11, GJO10], it would be possible to construct concurrent secure protocols for an asymmteric functionality like erasure channels, in which Bob does not have any input.

[11] For simplicity, following [Kil00], we require $|X|, |Y|$ to be constant. But the security of the protocol presented here only requires $|X|$ to be $\mathsf{poly}(\kappa)$ where κ is the security parameter. Alternatively, if $|Y|$ is $\mathsf{poly}(\kappa)$, we can have the protocol use a uniform distribution over a subset of X of size at most $2|Y|$, restricted to which the functionality is still non-trivial.

Claim 6. If $f : X \times Y \to Z$ is a function with two inputs $\hat{y}^0, \hat{y}^1 \in Y$ which are not dominated by any other input in Y, for any number $p \geq \min\{|X|, |Z|\}$, there exist two injective functions $N_0 : Z_0 \to \mathbb{Z}_p$, $N_1 : Z_1 \to \mathbb{Z}_p$, where $Z_b = \{f(x, \hat{y}^b) | x \in X\}$, such that there exist $\hat{x}^0, \hat{x}^1 \in X$ satisfying the following:

$$\begin{bmatrix} N_0\big(f(\hat{x}^0, \hat{y}^0)\big) & N_1\big(f(\hat{x}^0, \hat{y}^1)\big) \\ N_0\big(f(\hat{x}^1, \hat{y}^0)\big) & N_1\big(f(\hat{x}^1, \hat{y}^1)\big) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Proof. Define N_0 and N_1 as follows. Since $\hat{y}^0$ does not dominate $\hat{y}^1$, there are $x_1, x_2 \in X$ such that $f(x_1, \hat{y}^0) = f(x_2, \hat{y}^0) = \alpha$ (say), but $f(x_1, \hat{y}^1) \neq f(x_2, \hat{y}^1)$; we let $N_0 : \alpha \mapsto 0$. Symmetrically, there are $x_3, x_4 \in X$ such that $f(x_3, \hat{y}^0) \neq f(x_4, \hat{y}^0)$ but $f(x_3, \hat{y}^1) = f(x_4, \hat{y}^1) = \beta$,say; we let $N_1 : \beta \mapsto 0$. Now, since $f(x_1, \hat{y}^1) \neq f(x_2, \hat{y}^1)$, w.l.o.g assume that $f(x_1, \hat{y}^1) \neq \beta$ (swapping x_1 and x_2 if necessary), and then let $N_1 : f(x_1, \hat{y}^1) \mapsto 1$. Similarly, since $f(x_3, \hat{y}^0) \neq f(x_4, \hat{y}^0)$, w.l.o.g assume that $f(x_3, \hat{y}^0) \neq \alpha$ (swapping x_3 and x_4 if necessary), and then let $N_0 : f(x_3, \hat{y}^0) \mapsto 1$. (Then we can extend N_0 and N_1 arbitrarily as injective mappings from Z_0 and Z_1 (resp.) to $\mathbb{Z}_p$, since than $p \geq |Z_0|$ and $p \geq |Z_1|$.) We can then set $\hat{x}^0$ to be x_1 and $\hat{x}^1$ to be x_3. □

To illustrate this for the case of boolean functions ($p = |Z| = 2$), we note that for a non-trivial boolean functionality, the function table of f, restricted to the two columns corresponding to $\hat{y}^0$ and $\hat{y}^1$ must have one of the following minors (possibly with the columns reordered, in the last case): $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$ $\left[\begin{smallmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \end{smallmatrix}\right]$. In the first two cases N_0, N_1 can be the identity map and in the last case exactly one of N_0, N_1 would be the identity.

The protocol is now defined as follows, in terms of the inputs $\hat{y}^0, \hat{y}^1 \in Y$, $\hat{x}^0, \hat{x}^1 \in X$ and the functions N_0, N_1 as identified above.

Alice's program: Alice's input is two bits s_0, s_1.

1. Alice carries out the following computations:
   - For $i = 1$ to 2κ, pick $x_i \leftarrow X$.
   - For each i, let $R_i^0 = N_0(f(x_i, \hat{y}^0))$ and $R_i^1 = N_1(f(x_i, \hat{y}^1))$.
   - Let $r_0 = \sum_{i=1}^{\kappa} R_i^0 R_{\kappa+i}^0$, and $r_1 = \sum_{i=1}^{\kappa} R_i^1 R_{\kappa+i}^1$.
   - Let $m_0 = s_0 + r_0$ and $m_1 = s_1 + r_1$ (interpreting bits s_0, s_1 as elements in $\{0, 1\} \subseteq \mathbb{Z}_p$).
2. Alice invokes, in parallel, several copies of $\mathcal{F}$ with the following inputs:
   - Sessions $i = 1$ to 2κ with inputs x_i.
   - $2\lceil \log p \rceil$ more sessions to "communicate" the bits of (m_0, m_1): in a session to send a bit 0, use input $\hat{x}^0$, and in a session to send a bit 1, use input $\hat{x}^1$.
3. If all $\mathcal{F}$ sessions are completed, then Alice completes the protocol (i.e., outputs an acknowledgment).

Bob's program: Bob's input is a choice bit b.

1. Bob invokes the same copies of $\mathcal{F}$ as Alice with the following inputs:
   - In each of the 2κ sessions numbered $i = 1$ to 2κ, use input $\hat{y}^b$, and obtain R_i^b.
   - In each of the sessions used for communication, use input $\hat{y}^0$; obtain all bits of (m_0, m_1).
2. If all sessions of $\mathcal{F}$ are completed, compute $r_b = \sum_{i=1}^{\kappa} R_i^b R_{\kappa+i}^b$, and $s_b = m_b - r_b$. Then, if $s_b = 0$ output 0, otherwise output 1.

Intuition. The protocol is easily seen to be correct. Also, security when Alice is corrupt is easy to argue as $\mathcal{F}$ does not give any output to Alice. (The simulator can extract Alice's inputs by considering what Bob would output when his input is $b = 0$ and $b = 1$.) The interesting case is when Bob is corrupt.

Note that in the protocol, all the instances of $\mathcal{F}$ are invoked in parallel by the honest parties, but a rushing adversary that corrupts Bob can dynamically schedule the sessions and also choose its inputs for these sessions adaptively, based on the outputs received thus far. The main idea behind showing security against Bob is that one of r_0 and r_1 appears completely random to Bob (even given the other one), no matter how he chooses his inputs y_i. For this we define a pair of $\mathcal{F}$ sessions $(i, \kappa + i)$ to be a "0-undetermined pair" if $R_i^0 R_{\kappa+i}^0$ is not completely determined by the view of the adversary in those sessions, combined with $R_i^1 R_{\kappa+i}^1$; simiarly we define the pair to be a "1-undetermined pair" if $R_i^1 R_{\kappa+i}^1$ is not completely determined by the view of the adversary in those sessions, combined with $R_i^0 R_{\kappa+i}^0$. Then, as shown in Claim 7, there will be a constant probability that any pair will be either 0-undetermined or 1-undetermined.

Note that for any input y that the adversary chooses in the first session out of a pair, it does not dominate at least one of $\hat{y}^0$ and $\hat{y}^1$. With constant probability the adversary will be left with some uncertainty about either $f(x, \hat{y}^0)$ or $f(x, \hat{y}^1)$, where x stands for Alice's input in this session. Suppose $f(x, \hat{y}^0)$ is not fully determined. Now, with a further constant probability Alice's input in the other session in the pair would be $x' = \hat{x}^1$. Then, even if Bob learns x' exactly, he remains uncertain of $f(x, \hat{y}^0).f(x', \hat{y}^0) = f(x, \hat{y}^0) \cdot 1$. This uncertainty remains even if Bob learns $f(x, \hat{y}^1).f(x', \hat{y}^1) = f(x, \hat{y}^1) \cdot 0$, as it is independent of x. This slight uncertainty about a term in r_0 or r_1 gets amplified by addition in $\mathbb{Z}_p$.

To complete the intuitive argument of security, we need to also consider how the simulator for Bob can extract his input bit b. The simulator would let Bob schedule several sessions, until a constant fraction of the pairs $(i, \kappa+i)$ have had both sessions completed. At this point Bob would have already accumulated sufficient uncertainty about one of r_0 and r_1, say $r_{\overline{b}}$, that will remain no matter what he learns from the remaining sessions. Further, not having invoked the remaining sessions will ensure that at this point he still has no information about the other element r_b. So, at this point, the simulator will send $b = 1 - \overline{b}$ to the ideal $\mathcal{F}_{\mathsf{OT}}$ and learn what r_b should be, and can henceforth "pretend" that it was always using that value of r_b. Pretending thus (i.e., sampling Alice's inputs for the remaining sessions according to the right conditional distribution) can be efficiently done by rejection sampling (since p is a constant).

Formal Proof. Note that in the protocol, all the instances of $\mathcal{F}$ are invoked in parallel by the honest parties, but a rushing adversary that corrupts Bob can dynamically schedule the sessions and also choose its inputs for these sessions adaptively, based on the outputs received thus far.

When Both Parties are Honest. Correctness when both parties are honest follows from the fact that an honest Bob can exactly compute r_b by using inputs as prescribed by the protocol.

When Alice is Corrupt. Security when Alice is corrupt easily follows from the fact that $\mathcal{F}$ does not give any output to Alice. We consider an efficient simulator which waits for Alice to invoke all the sessions of $\mathcal{F}$, and based on Alice's inputs to instances of $\mathcal{F}$, computes both (r_0, m_0) and (r_1, m_1). Then, for $j = 0, 1$ it computes the number $s_j = m_j - r_j$ and sets the bit $s'_j = 0$ if $s_j = 0$, and $s'_j = 1$ otherwise. The simulator sends (s'_0, s'_1) to the ideal $\mathcal{F}_{\mathsf{OT}}$ functionality, to complete the simulation. It is easy to verify that this is a perfect simulation.

When Bob is Corrupt. The main idea behind showing security against Bob is that one of r_0 and r_1 appears completely random to Bob (even given the other one), no matter how he chooses his inputs y_i. For this we define a pair of $\mathcal{F}$ sessions $(i, \kappa + i)$ to be a "0-undetermined pair" if $R_i^0 R_{\kappa+i}^0$ is not completely determined by the view of the adversary in those sessions, combined with $R_i^1 R_{\kappa+i}^1$; simiarly we define the pair to be a "1-undetermined pair" if $R_i^1 R_{\kappa+i}^1$ is not completely determined by the view of the adversary in those sessions, combined with $R_i^0 R_{\kappa+i}^0$. As shown below, given the way we have defined R_i^0 and R_i^1 (and N_0 and N_1), there will be a constant probability that any pair will be either 0-undetermined or 1-undetermined.

Claim 7. There is a constant $\epsilon > 0$,[12] such that, for any pair of sessions $(i, \kappa + i)$, for any adversarial strategy of scheduling them and choosing y_i and $y_{\kappa+i}$, with probability at least ϵ the pair will be either 0-undetermined or 1-undetermined.

Proof. W.l.o.g, we can assume that the adversary schedules session i first (the other case being symmetric). Suppose it uses input $y_i = y$ for this session. Note that y does not dominate at least one of $\hat{y}^0$ and $\hat{y}^1$ (if $y \notin \{\hat{y}^0, \hat{y}^1\}$, it dominates neither).

Suppose y does not dominate $\hat{y}^0$. That is, there exists some $x, x' \in X$ such that $f(x, y) = f(x', y)$ but $f(x, \hat{y}^0) \neq f(x', \hat{y}^0)$. With probability $2/|X|$, the input $x_i \in \{x, x'\}$. Further, independently, with probability $1/|X|$, $x_{\kappa+i} = \hat{x}^1$. Thus with probability $2/|X|^2$, we will have $R_i^0 R_{\kappa+i}^0 = f(x_i, \hat{y}^0).1 = f(x_i, \hat{y}^0)$ and $R_i^1 R_{\kappa+i}^1 = f(x_i, \hat{y}^1).0 = 0$. In this case, the adversary cannot determine $R_i^0 R_{\kappa+i}^0$ (which could be either $f(x, \hat{y}^0)$ or $f(x', \hat{y}^0)$), given $f(x_i, y)$, $f(x_{\kappa+i}, y')$ for any y' (or even $x_{\kappa+i}$ itself) and $R_i^1 R_{\kappa+i}^1 = 0$.

Similarly, if y does not dominate $\hat{y}^1$, then with probability at least $2/|X|^2$, $R_i^1 R_{\kappa+i}^1$ cannot be completely determined from $f(x_i, y)$, $x_{\kappa+i}$ and $R_i^0 R_{\kappa+i}^0 = 0$.

Thus, in either case, with probability at least $2/|X|^2$, the pair becomes either 0-undetermined or 1-undetermined. □

This slight uncertainty about a term in r_0 or r_1 gets amplified by addition in $\mathbb{Z}_p$ (see Lemma 8). To formalize the intuition into a proof of security, we need to build an appropriate simulator, that works even when Bob can schedule the $\mathcal{F}$ sessions in arbitrary order. We divide the invocations of $\mathcal{F}$ into the following imaginary phases:

- Communication Phase: W.l.o.g, we assume that Bob first schedules all the communication sessions, and uses input $\hat{y}^0$ in them. (Any other strategy is "dominated" by this, in that it can be simulated by an adversary as above.)
- Phase 1: This phase starts when Bob invokes one of the 2κ sessions numbered 1 to 2κ, and lasts until, for $c_1\kappa$ values of $i \in [\kappa]$, both sessions i and $\kappa + i$ have been invoked (where c_1 is a constant to be determined).
- Phase 2: This phase consists of the rest of the invocations of $\mathcal{F}$.

The simulator will behave differently based on which phase it is in, as follows:

- Communication Phase: Randomly pick $m_0, m_1 \leftarrow \mathbb{Z}_p$, and faithfully simulate all the communication sessions using these.
- Phase 1: In Phase 1, to simulate a new session i, accept y_i from Bob and return $f(x_i, y_i)$ for a uniformly random input x_i.
- Input Extraction: At the end of Phase 1, the simulator asserts that $c_2\kappa$ of these pairs are either 0-undetermined or 1-undetermined (for a constant c_2, also to be determined), and else aborts the simulation. (This, as we shall argue, happens with negligible probability.) Then, for $\bar{b} \in \{0, 1\}$, at least $(c_2/2)\kappa$ pairs are $\bar{b}$-undetermined. Simulator sends $b = 1 - \bar{b}$ to $\mathcal{F}_{\mathsf{OT}}$ and gets back $s_b \in \{0, 1\}$.
- Phase 2: Now the simulator will sample x_i for the remaining sessions uniformly at random, but conditioned on $r_b = m_b - s_b$, where $r_b = \sum_{i=1}^{\kappa} R_i^b R_{\kappa+i}^b$. This can be done efficiently by rejection sampling. (The simulator can abort after κ unsuccessful trials.)

[12] Recall that we treat $|X|, |Y|$ as constants. All the positive constants in this analysis are $\Omega(\mathsf{poly}(1/|X|))$.

We shall argue that, for a suitable choice of the constants c_1, c_2, for any input (s_0, s_1) for Alice, the above simulation is good – i.e., indistinguishable from an actual execution of the protocol.

The analysis rests on the following observations about the real execution:

1. (r_0, r_1) are almost (i.e., up to negligible statistical distance) uniformly distributed over $\mathbb{Z}_p \times \mathbb{Z}_p$.
2. Conditioned on any value of (r_0, r_1), x_i in the sessions invoked by the adversary in Phase 1 are almost uniformly random.[13]
3. Let $(\bar{b}, b)$ be defined after Phase 1 the same way it is defined by the simulator. Then, $r_{\bar{b}}$ is almost uniform even conditioned on r_b and the view of the adversary in Phase 1 and Phase 2.

Given the above three observations, it is immediate that the simulation is good. In the rest of the proof we prove the above three observations.

To prove the first item note that except with negligible probability, for $N = \Theta(\kappa)$ values of $i \in [\kappa]$, $x_i = \hat{x}^0$ and for another N values of i, $x_i = \hat{x}^1$. We will condition on this event happening, and let S_0 be the set of first N indices i with $x_i = \hat{x}^1$; similarly let S_1 be the set of first N indices i with $x_i = \hat{x}^0$. Note that then $r_0 = u_0 + v_0$ where $u_0 := \sum_{i \in S_0} N_0\big(f(x_{\kappa+i}, \hat{y}^0)\big)$ and v_0 is indepedent of u_0; similarly $r_1 = u_1 + v_1$ where $u_1 := \sum_{i \in S_1} N_1\big(f(x_{\kappa+i}, \hat{y}^1)\big)$ and v_1 is indepedent of u_1. (v_0 and v_1 are correlated.) To show that (r_0, r_1) is almost uniformly distributed in $\mathbb{Z}_p \times \mathbb{Z}_p$, it is enough to show that (u_0, u_1) are distributed that way. Firstly, since S_0 and S_1 are disjoint, they are independent of each other. To see that they are almost uniform, we rely on Lemma 8, using distributions D_0 and D_1 defined as the distribution of $N_0\big(f(x, \hat{y}^0)\big)$ and $N_1\big(f(x, \hat{y}^1)\big)$ respectively, for uniform $x \leftarrow X$.

To prove the second item, for ease of analysis, we shall consider a stronger adversary for Phase 1, which learns the value of x_i in each session it invokes in Phase 1. W.l.o.g we may assume that it first invokes the sessions $i = 1$ to κ, and then adaptively invokes sessions $i \in T \subseteq [\kappa + 1, 2\kappa]$ where $|T| = c_1\kappa$. There is a constant c such that, except for a negligibly probable event — which we shall condition on not occuring — there are at least $c\kappa$ values of $i \in [\kappa]$ for which $x_i = \hat{x}^0$ and $c\kappa$ values of $i \in [\kappa]$ for which $x_i = \hat{x}^1$. We shall set c_1 so that $c > c_1$. Then there are sets $S_0, S_1 \subseteq [\kappa + 1, 2\kappa] \backslash T$, with $|S_0| = |S_1| = (c - c_1)\kappa$ such that for $i \in S_0$, $x_i = \hat{x}^1$ and for $i \in S_1$, $x_i = \hat{x}^0$. Using S_0, S_1 to define u_0, u_1 as before, similar to the argument above, we have $r_b = u_b + v_b$, where (u_0, u_1) is almost uniform over $\mathbb{Z}_p \times \mathbb{Z}_p$ and (almost) independent of v_b and the x_i values revealed to the adversary in Phase 1.

Finally, to prove the third item, we return to the normal adversary (who does not learn x_i exactly, but only $f(x_i, y_i)$ for a y_i that it adaptively chooses). By Claim 7, except with negligible probability, out of the $c_1\kappa$ pairs that have both sessions invoked, at least $(c_2/2)\kappa$ pairs are $\bar{b}$-undetermined. The distribution from which an undetermined value for the pair $(i, \kappa + i)$ is sampled is decided by $(x_i, y_i, x_{\kappa+i}, y_{\kappa+i})$. Hence there are only a constant number of such distributions. Let D be the most frequent of these distributions among the $\bar{b}$-undetermined $(c_2/2)\kappa$ pairs. Let $W \subseteq [\kappa]$ be such that for $i \in W$, the pair $(i, \kappa + i)$ is $\bar{b}$-undetermined and is associated with the distribution D. Then $|W| = \Theta(\kappa)$. We can consider revealing $(x_j, x_{\kappa+j})$ for all $j \notin W$, as well as the adversary's view (i.e., $f(x_i, y_i), f(x_{\kappa+i}, y_{\kappa+i})$) and $R_i^b R_{\kappa+i}^b$ for all $i \in W$ (since the definition of being undetermined allows conditioning on the last two). Then by Lemma 8, similar to above arguments, $r_{\bar{b}}$ is still uniform conditioned on r_b and the view of the adversary (which are subsumed by $(x_j, x_{\kappa+j})$ for $j \notin W$, and $R_i^b R_{\kappa+i}^b$ for $i \in W$).

Lemma 8. *Let p be a fixed prime number. Let D be a distribution over $\mathbb{Z}_p$, such that for some constant $\epsilon > 0$, for all $z \in \mathbb{Z}_p$, $\Pr_{a \leftarrow D}[a = z] < 1 - \epsilon$. For any positive integer N, let $a_1, \cdots, a_N$ be i.i.d random variables sampled according to D. Then the statistical distance between the distribution of $\sum_{i=1}^{N} a_i$ (summation in $\mathbb{Z}_p$) and the uniform distribution over $\mathbb{Z}_p$ is negligible in N.*

[13] Note that *which* sessions are invoked can depend on (r_0, r_1), but for any such choice of sessions, the *values* of x_i in those sessions will be (almost) independent of (r_0, r_1).

Proof. We give an elementary argument to prove this lemma. First, for simplicity, consider the case that each a_i has a support of size two. W.l.o.g, we can assume that one of the values in the support is 0. This is because, otherwise we can simply consider the summation of $a'_i = a_i - z^*$, where z^* is an element in the support of a_i, and the statistical distance of $\sum_i a_i$ from the uniform distribution is the same as that of $\sum_i a'_i$.

Then, let a_i be z with probability δ and 0 with probability $1-\delta$, where δ is bounded away from 0 and 1. For any value $w \in \mathbb{Z}_p$, consider $\Pr\left[\sum_i a_i = w\right]$. Let $u = wz^{-1}$ ($u \in \mathbb{Z}_p$ will be treated as an integer in $\{0, \cdots, p-1\}$). Then

$$\begin{aligned} \Pr\left[\sum_i a_i = w\right] &= \sum_{t \geq 0} \binom{N}{tp+u} \delta^{tp+u}(1-\delta)^{N-(tp+u)} \\ \Pr\left[\sum_i a_i = 0\right] &= \sum_{t \geq 0} \binom{N}{tp} \delta^{tp}(1-\delta)^{N-tp}. \end{aligned} \tag{1}$$

We argue that, for any $w \in \mathbb{Z}_p$, the above two summations are close to each other.[14] For this we show that, for all values of u, $\sum_{t \geq 0} \binom{N}{tp+u} \delta^{tp+u}(1-\delta)^{N-(tp+u)} = \frac{1}{p} \pm (1-\alpha)^N$ for some constant $0 < \alpha < 1$.

Let $S_k = ((1-\delta) + \delta\omega^k)^N$ where $\omega = e^{i2\pi/p}$, is a p^{th} root of unity. Using the binomial expansion of S_k and the fact that $\sum_{k=0}^{p-1} \omega^k = 0$, we get

$$\sum_{t \geq 0} \binom{N}{tp+u} \delta^{tp+u}(1-\delta)^{N-(tp+u)} = \frac{1}{p} \sum_{k=0}^{p-1} \omega^{-ku} S_k.$$

Now, $\sum_{k=0}^{p-1} \omega^{-ku} S_k = 1 + \sum_{k=1}^{p-1} \omega^{-ku} S_k$, because $S_0 = 1$. Further, for $0 < k \leq p-1$, $|(1-\delta) + \delta\omega^k| \leq 1 - \alpha$, where we take $\alpha = 1 - |(1-\delta) + \delta\omega|$. Since p is a constant and δ is also a constant with $0 < \delta < 1$, α is a constant with $0 < \alpha < 1$. Then,

$$\begin{aligned} \sum_{k=1}^{p-1} \omega^{ku} S_k &\leq \sum_{k=1}^{p-1} |\omega^{ku} S_k| \\ &= \sum_{k=1}^{p-1} |S_k| \leq (p-1)(1-\alpha)^N < p(1-\alpha)^N. \end{aligned}$$

Thus indeed,

$$\sum_{t \geq 0} \binom{N}{tp+u} \delta^{tp+u}(1-\delta)^{N-(tp+u)} = \frac{1}{p} \pm (1-\alpha)^N$$

Since this holds for all values of u, including $u = 0$, the difference between the two probabilities in (1) is at most $2(1-\alpha)^N$, which is negligible in N.

This proves the lemma when D has a support of size 2. For the general case, when D has a larger support, let z_0, z_1 be two elements with the most weight according to D. Then, we note that there would be a constant $\gamma > 0$ such that, except with negligible probability, for at least γN values of $i \in [N]$, $a_i \in \{z_0, z_1\}$. So we can condition on this event occurring. Conditioned on this, $\sum_i a_i$ is distributed as $v + \sum_{i=1}^{\gamma N} u_i$ where u_i are i.i.d according to D restricted to $\{z_0, z_1\}$, and v is independent of u. By appealing to the case of binary support, we conclude that $\sum_i a_i$ is almost uniformly random. □

Going Beyond Finite Functionalities. We note that if $|Y|$ is $\mathsf{poly}(\kappa)$, then we can have the above protocol use a uniform distribution over a subset of X of size at most $2|Y|$, restricted to which the functionality is still non-trivial.

[14] We thank Hemanta Maji for spotting a flaw in an earlier argument, and suggesting a new argument.

Thus, we note that our protocol can be easily made to work for infinite functionalities f for which there exists a bounded-size subset of X, restricted to which f is non-trivial.

In order to extend our results to all non-trivial infinite functionalities, we can further build upon the above idea. We note in our OT protocol presented in Section 3, if we can somehow "restrict" Bob to using non-dominating inputs $\hat{y}^0$ and $\hat{y}^1$ (more generally, a bounded-size subset), then we would only require Alice to sample her inputs in the protocol from a bounded-size subset of domain X. In this case, our protocol can easily handle asymmetric infinite functionalities.

Then, we note that our impossibility results for static-input fixed-roles concurrent self composition can be easily extended to rule out all non-trivial asymmetric infinite functionalities in the following manner:

- First, towards a contradiction, given a static-input fixed-roles concurrently secure protocol Π for a non-trivial asymmetric infinite functionality f, we can "compile" it using stand-alone zero knowledge proof system to obtain a static-input fixed-roles concurrently secure protocol Π^* for functionality f^*, where f^* is the same as f, except that Bob's input domain Y^* is bounded-size. Very roughly, the compiled protocol Π^* works as follows: with each outgoing message m in Π, Bob now additionally gives a zero-knowledge proof to prove that the message was computed using an input in Y^*.
- Now, combining Π^* with our asynchronous non-interactive OT protocol for f^* and the composition theorem in Section 5, we can obtain a static-input fixed-roles concurrently secure protocol for OT. Combining this with the impossibility result for OT in Section 4, we obtain a contradiction.

Remark. We note that a downside of the above approach is that it requires computational assumptions (in particular, one-way functions for zero-knowledge proofs). This is in contrast to the case of asymmetric finite functionalities where we obtained an unconditional (non-interactive) completeness result.

4 Impossibility of Concurrent Oblivious Transfer

In this section, we will prove the impossibility of $\binom{2}{1}$-OT secure under concurrent self-composition in the static-input, fixed-roles setting. To show this, we proceed as follows. First, we note that for any functionality to be secure, it must hold that for *every* input to the functionality, a real world attack, successful with non-negligible probability (say) ϵ, implies an ideal world attack that succeeds with probability at least $\epsilon - \text{negl}$. Now, suppose towards contradiction, we are given a protocol Π_{OT} that securely realizes the OT functionality $\mathcal{F}_{\mathsf{OT}}$ under static-input, fixed-roles concurrent self-composition. We will exhibit a set of inputs (for sender and receiver) and a real-world adversarial receiver that is able to perform a concurrent attack and manages to learn a secret value, called secretwith probability 1. We will then prove that if there exists an adversarial receiver in the ideal world that is able to learn secret with high enough probability, then we can break the stand-alone security of Π_{OT} against a cheating sender, thus arriving at a contradiction.

The high level structure of our proof is as follows:

1. First, we will construct an instance of the *chosen protocol attack* for the OT functionality. More precisely, let Π_{OT} be a secure protocol that implements the OT functionality. Then we will construct a protocol $\widehat{\Pi_{\mathsf{OT}}}$ such that the protocols Π_{OT} and $\widehat{\Pi_{\mathsf{OT}}}$ are *insecure* when executed concurrently.
2. Next, we will use *one time programs* (OTPs) to transform the above concurrent protocol executions of Π_{OT} and $\widehat{\Pi_{\mathsf{OT}}}$ into self composition of OT protocol Π_{OT}.
3. This will provide us with particular inputs to the OT functionality, such that when a malicious receiver Bob engages in concurrent executions of Π_{OT} with an honest sender Alice (with these inputs), he will be able to output secret with probability 1. This will give us a real world attack.
4. We will then show the infeasibility of an adversarial receiver in the ideal world that successfully outputs secret with probability at least $1 - \text{negl}$. In particular, we will show that such an adversarial receiver can be used to used to construct a stand-alone cheating sender for Π_{OT}.

4.1 Chosen Protocol Attack

Let Π_{OT} be a protocol that securely realizes the OT functionality. To fix notation, let us consider two parties Alice and Bob that are executing an instance of Π_{OT}. Say that Alice's input bits are denoted by s_0 and s_1 and Bob's input bit is b. Upon successful completion of the protocol, Bob obtains s_b. Next, let $\widehat{\Pi_{\mathsf{OT}}}$ be a slightly modified version of Π_{OT} where the receiver Bob also has both of Alice's inputs, s_0 and s_1 in addition to his bit b. In $\widehat{\Pi_{\mathsf{OT}}}$, Bob and Alice run an execution of Π_{OT} with inputs b and s_0, s_1 respectively. Upon receiving an output s^*, Bob checks whether $s^* = s_b$. If so, he sends $\mathsf{secret} = s_{\bar{b}}$ to Alice.

Now, consider the following scenario involving three parties Alice, Eve and David. Alice holds input bits s_0, s_1, while David holds s_0, s_1, as well as a random input bit b. Alice plays the sender with receiver Eve in an execution of Π_{OT}, and Eve plays sender with receiver David in an execution of $\widehat{\Pi_{\mathsf{OT}}}$. It is clear that a malicious Eve can launch "man-in-the-middle" attack, playing simultaneously with Alice and David, and by merely forwarding Alice's message to David and David's back to Alice, she can learn the value $\mathsf{secret} = s_{\bar{b}}$. However, note that if the execution of Π_{OT} is replaced with an ideal call to the OT functionality, then the attack does not carry through. (To avoid repetition, we skip proof details here and instead present them later more formally).

4.2 Converting $\widehat{\Pi_{\mathsf{OT}}}$ to Π_{OT}

Note that the above attack is valid in the setting of concurrent general composition. However, we are interested in the setting of concurrent self composition, where only Π_{OT} is executed concurrently. Towards this end, in this section, we will convert the protocol $\widehat{\Pi_{\mathsf{OT}}}$ into a series of OT calls which can be implemented by Π_{OT}. Since Π_{OT} executed concurrently with $\widehat{\Pi_{\mathsf{OT}}}$ is insecure, this will allow us to show that Π_{OT} is insecure under concurrent self composition.

To begin, we transform the protocol $\widehat{\Pi_{\mathsf{OT}}}$ run by Eve (as sender) and David into a sequence of calls made by Eve to an ideal reactive functionality (with inputs fixed in advance). As in [BPS06], it is natural to instantiate this ideal functionality by the *next message function* $\mathcal{F}^{\mathsf{David}}$ of David's strategy in protocol $\widehat{\Pi_{\mathsf{OT}}}$. Then Eve can simulate the interaction with David by invoking $\mathcal{F}^{\mathsf{David}}$ each time she expects a message from David.

More precisely, the inputs to $\mathcal{F}^{\mathsf{David}}$ will be the bits s_0 and s_1, a random bit b, a message from Eve denoted by e_i, and a state state_{i-1} (since $\mathcal{F}^{\mathsf{David}}$ is a reactive functionality, it needs to know state_{i-1} in order to compute state_i), and the output of $\mathcal{F}^{\mathsf{David}}$ will be David's i^{th} message in $\widehat{\Pi_{\mathsf{OT}}}$ and state_i. By doing this, Eve can, as before, play the receiver in an execution of Π_{OT} with Alice as the sender (with inputs s_0, s_1) and carry out the man in the middle attack by invoking $\mathcal{F}^{\mathsf{David}}$. We will denote the real world attacker played by Eve as above, by $\hat{\mathcal{E}}^{\mathsf{real}}$.

As the next step, we will to replace the ideal calls to $\mathcal{F}^{\mathsf{David}}$ made by $\hat{\mathcal{E}}^{\mathsf{real}}$ by a series of OTs executed between Alice and $\hat{\mathcal{E}}^{\mathsf{real}}$. Let n denote the number of messages that David sends in protocol $\widehat{\Pi_{\mathsf{OT}}}$. Then, consider the one time programs $\mathsf{OTP\text{-}msg}_1, \ldots, \mathsf{OTP\text{-}msg}_n$ where $\mathsf{OTP\text{-}msg}_i$ computes the i^{th} next message function of David. We will provide Alice with all the keys $\{\mathsf{keys}_i\}_{i=1}^n$ to the OTPs. Then, to evaluate the i^{th} OTP, $\hat{\mathcal{E}}^{\mathsf{real}}$ executes (multiple sessions of) Π_{OT} with Alice to obtain the keys corresponding to her input.

Also note that OTPs are *stateless* by definition, but David's next message functionality is *stateful*, i.e. David's $(i+1)^{th}$ message depends on the previous i messages. Looking ahead, we will require that the OTPs only be invoked by the ideal world attacker in consecutive order. We ensure this by allowing each $\mathsf{OTP\text{-}msg}_i$ to pass its private state to $\mathsf{OTP\text{-}msg}_{i+1}$ using standard techniques (as used in [BPS06, Goy11]). Specifically, we will add to the (fixed) inputs of $\mathsf{OTP\text{-}msg}_i$ a key K for an authenticated encryption scheme. Now, $\mathsf{OTP\text{-}msg}_i$ outputs not only David's next message d_i, but also an authenticated encryption of its resultant state, denoted by $\tau_i = \mathsf{Enc}_K(\mathsf{state}_i)$. As input, $\mathsf{OTP\text{-}msg}_i$ requests not only message e_i, but also a valid authenticated encryption τ_{i-1} such that $\mathsf{Dec}_K(\tau_{i-1}) = \mathsf{state}_{i-1}$. This forces the functionality $\mathcal{F}^{\mathsf{David}}$ implemented by OTPs, to be invoked in proper order. For the rest of the article, we will assume that any OTPs we use are made "stateful" in this way.

Note that there are two kinds of executions of Π_{OT} being carried out between Alice and $\hat{\mathcal{E}}^{\mathsf{real}}$: the "main" OT execution where Alice uses inputs s_0, s_1, and the additional OT executions that allow Eve to obtain keys for the one time programs. For clarity of exposition, we will refer to the "main" execution as $\Pi_{\mathsf{OT}}^{\mathsf{main}}$ and each of the remaining ones as $\Pi_{\mathsf{OT}}^{\mathsf{David}}$.

4.3 Attack in the real world

Now, we will describe the explicit execution of OTs between Alice and $\hat{\mathcal{E}}^{\mathsf{real}}$, where $\hat{\mathcal{E}}^{\mathsf{real}}$ recovers $\mathsf{secret} = s_{\bar{b}}$. The protocol is as follows:

Alice's program: Alice is given input bits s_0, s_1 for $\Pi_{\mathsf{OT}}^{\mathsf{main}}$ and all the one time program keys $\{\mathsf{keys}_i\}_{i=1}^n$ for $\mathsf{OTP\text{-}msg}_1, \ldots, \mathsf{OTP\text{-}msg}_n$

Alice behaves honestly according to the protocol Π_{OT} and responds honestly to all OT invocations made by $\hat{\mathcal{E}}^{\mathsf{real}}$.

$\hat{\mathcal{E}}^{\mathsf{real}}$**'s program:** $\hat{\mathcal{E}}^{\mathsf{real}}$ is given input bit $\hat{b}$ for $\Pi_{\mathsf{OT}}^{\mathsf{main}}$ and the one time programs $\{\mathsf{OTP\text{-}msg}_i\}_{i=1}^n$ where $\mathsf{OTP\text{-}msg}_i$ computes the i^{th} next message function of David. Let s_0, s_1 and b denote the fixed inputs (hardwired) in the OTPs such that $\mathsf{secret} = s_{\bar{b}}$.

For $i = 1, \ldots, n$, do:

1. Upon receiving i^{th} message from Alice in $\Pi_{\mathsf{OT}}^{\mathsf{main}}$, say a_i, suspend (temporarily) the ongoing $\Pi_{\mathsf{OT}}^{\mathsf{main}}$ session and start a new $\Pi_{\mathsf{OT}}^{\mathsf{David}}$ session with Alice to compute the i^{th} message that David would have sent in response had he received a_i from Eve. Depending on a_i, retrieve the corresponding keys keys_i from Alice to input to $\mathsf{OTP\text{-}msg}_i$. End the $\Pi_{\mathsf{OT}}^{\mathsf{David}}$ protocol.
2. Run $\mathsf{OTP\text{-}msg}_i$ with keys keys_i and obtain output d_i.
3. If $i \leq n-1$, resume the suspended $\Pi_{\mathsf{OT}}^{\mathsf{main}}$ protocol and send d_i back to Alice as response. Otherwise, output the value secret received from $\mathsf{OTP\text{-}msg}_n$.

Thus, using a sequence of OT executions, a dishonest $\hat{\mathcal{E}}^{\mathsf{real}}$ is able to recover $\mathsf{secret} = s_{\bar{b}}$ with probability 1.

4.4 Infeasibility of Ideal world attacker

In this section, we will prove the infeasibility of an ideal world adversarial receiver that succeeds in outputting secret with the same probability as $\hat{\mathcal{E}}^{\mathsf{real}}$. Towards a contradiction, let us assume that there exists an ideal world attacker $\hat{\mathcal{E}}^{\mathsf{ideal}}$ that successfully outputs secret with probability at least $1 - \mathsf{negl}$. $\hat{\mathcal{E}}^{\mathsf{ideal}}$ has oracle access to the ideal OT functionality $\mathcal{F}_{\mathsf{OT}}$, which for notational clarity we will (as before) divide into two kinds of OTs – $\mathcal{F}_{\mathsf{OT}}^{\mathsf{Main}}$ and $\mathcal{F}_{\mathsf{OT}}^{\mathsf{David}}$. Then, we have two possible cases:

Case 1: With probability at least $\frac{1}{2} + \mathsf{non} - \mathsf{negl}$, $\hat{\mathcal{E}}^{\mathsf{ideal}}$ queries $\mathcal{F}_{\mathsf{OT}}^{\mathsf{Main}}$ for the same bit as is built into the David OTP (since David was a receiver in the OT protocol, he has a random input bit which is built into the OTPs implementing his messages). In this case, we construct a stand-alone cheating sender $\hat{\mathcal{S}}$ that executes OT protocol Π_{OT} with an honest receiver $\mathcal{R}$, and uses $\hat{\mathcal{E}}^{\mathsf{ideal}}$ to learn $\mathcal{R}$'s secret input bit b with probability at least $\frac{1}{2} + \mathsf{non} - \mathsf{negl}$. This will imply that Π_{OT} is standalone insecure, a contradiction.

Case 2: With probability at most $\frac{1}{2} + \mathsf{negl}$, $\hat{\mathcal{E}}^{\mathsf{ideal}}$ queries the same bit as in the OTPs. That is, with probability $\frac{1}{2} - \mathsf{negl}$, $\hat{\mathcal{E}}^{\mathsf{ideal}}$ queries different bit. In this case, we will show via an information theoretic argument, that with probability at least $\frac{1}{4} - \mathsf{negl}$, $\hat{\mathcal{E}}^{\mathsf{ideal}}$ cannot output secret. Since by assumption $\hat{\mathcal{E}}^{\mathsf{ideal}}$ succeeds with probability at least $1 - \mathsf{negl}$, this is a contradiction.

These cases are analyzed below.

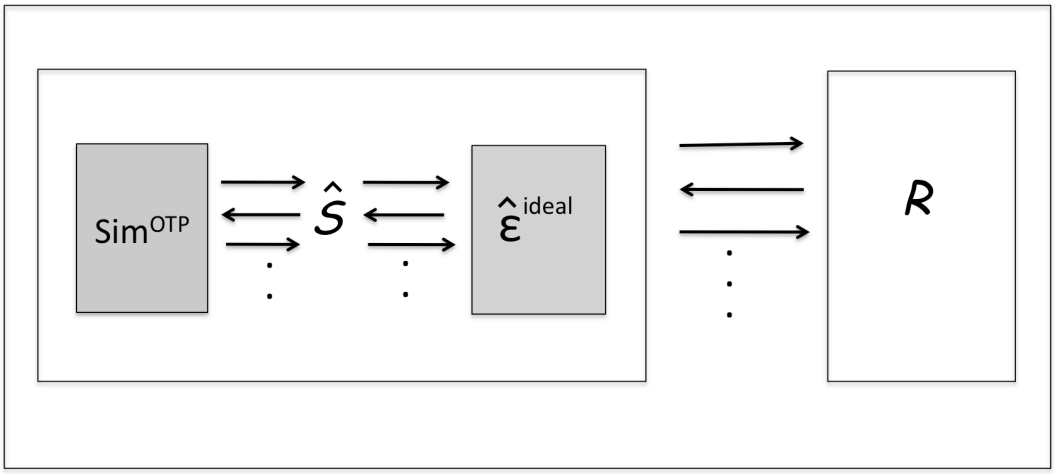

Figure 2: Stand-alone Cheating Sender $\hat{\mathcal{S}}$.

Case 1: Lets say that $\hat{\mathcal{E}}^{\mathsf{ideal}}$ queries the same bit as in the OTP with probability at least $\frac{1}{2} + \mathsf{non} - \mathsf{negl}$. In this case, we will construct a stand-alone cheating sender $\hat{\mathcal{S}}$ that uses such a $\hat{\mathcal{E}}^{\mathsf{ideal}}$ to learn $\mathcal{R}$'s secret bit with probability at least $\frac{1}{2} + \mathsf{non} - \mathsf{negl}$. The interaction is captured in Figure Figure 2.

Note that in order for $\hat{\mathcal{S}}$ to successfully run $\hat{\mathcal{E}}^{\mathsf{ideal}}$, $\hat{\mathcal{S}}$ will need to provide inputs to $\hat{\mathcal{E}}^{\mathsf{ideal}}$ and answer its queries to $\mathcal{F}_{\mathsf{OT}}$. Note that $\hat{\mathcal{E}}^{\mathsf{ideal}}$ may query the ideal OT functionality $\mathcal{F}_{\mathsf{OT}}^{\mathsf{Main}}$ or the ideal David OT functionality $\mathcal{F}_{\mathsf{OT}}^{\mathsf{David}}$. For all of these tasks, $\hat{\mathcal{S}}$ makes use of the one time program simulator $\mathsf{Sim}_{\mathsf{OTP}}$.

The cheating sender $\hat{\mathcal{S}}$ works as follows:

$\hat{\mathcal{S}}$'s program:

1. $\hat{\mathcal{S}}$ runs $\hat{\mathcal{E}}^{\mathsf{ideal}}$: $\hat{\mathcal{S}}$ provides as inputs to $\hat{\mathcal{E}}^{\mathsf{ideal}}$ the (simulated) one time programs $\mathsf{OTP\text{-}msg}_1, \ldots, \mathsf{OTP\text{-}msg}_n$ computed by the OTP simulator $\mathsf{Sim}_{\mathsf{OTP}}$ where $\mathsf{OTP\text{-}msg}_i$ corresponds to the i^{th} next message function of David as described before.

2. If $\hat{\mathcal{E}}^{\mathsf{ideal}}$ makes queries to $\mathcal{F}_{\mathsf{OT}}^{\mathsf{David}}$, $\hat{\mathcal{S}}$ needs to return keys for the OTPs $\mathsf{OTP\text{-}msg}_1, \ldots, \mathsf{OTP\text{-}msg}_n$. Consider the queries made by $\hat{\mathcal{E}}^{\mathsf{ideal}}$ for $\mathsf{OTP\text{-}msg}_i$ w.l.o.g for some $i \in [n]$.

   - $\hat{\mathcal{E}}^{\mathsf{ideal}}$ wishes to obtain keys keys_i corresponding to $\mathsf{OTP\text{-}msg}_i$. Let us assume that $\mathsf{OTP\text{-}msg}_i$ has k input wires. $\hat{\mathcal{E}}^{\mathsf{ideal}}$ begins to query $\hat{\mathcal{S}}$ for the keys (one query per input wire). $\hat{\mathcal{S}}$ forwards each query to $\mathsf{Sim}_{\mathsf{OTP}}$ and receives some key in response which it forwards back to $\hat{\mathcal{E}}^{\mathsf{ideal}}$.
   - At some point, after returning t keys (for some $t < k$) for $\mathsf{OTP\text{-}msg}_i$, $\mathsf{Sim}_{\mathsf{OTP}}$ makes its one-time input query with some value x and requests the value $\mathcal{F}_i^{\mathsf{David}}(x)$.
   - $\hat{\mathcal{S}}$ parses this query as a message $\mathsf{msg}_i^{\hat{\mathcal{S}}}$ and sends it to $\mathcal{R}$.
   - In response, $\mathcal{R}$ sends some message $\mathsf{msg}_i^{\mathcal{R}}$ back to $\hat{\mathcal{S}}$. Upon receiving $\mathsf{msg}_i^{\mathcal{R}}$, $\hat{\mathcal{S}}$ provides $\mathsf{msg}_i^{\mathcal{R}}$ as a response to $\mathsf{Sim}_{\mathsf{OTP}}$. Upon receiving this, $\mathsf{Sim}_{\mathsf{OTP}}$ resumes answering $\mathcal{F}_{\mathsf{OT}}^{\mathsf{David}}$ queries by returning keys back to $\hat{\mathcal{S}}$ for $\mathsf{OTP\text{-}msg}_i$, which $\hat{\mathcal{S}}$ forwards to $\hat{\mathcal{E}}^{\mathsf{ideal}}$. Let us denote all the keys returned by $\mathsf{Sim}_{\mathsf{OTP}}$ for $\mathsf{OTP\text{-}msg}_i$ as keys_i. Then, we have that $\mathsf{OTP\text{-}msg}_i(\mathsf{keys}_i) = \mathsf{msg}_i^{\mathcal{R}}$.

3. If $\hat{\mathcal{E}}^{\mathsf{ideal}}$ makes a query to $\mathcal{F}_{\mathsf{OT}}^{\mathsf{Main}}$ with input bit b, $\hat{\mathcal{S}}$ outputs this bit b and halts.

It follows from the description of $\hat{\mathcal{S}}$ that $\hat{\mathcal{S}}$ successfully mirrors its interaction with $\mathcal{R}$ by the interaction between $\hat{\mathcal{E}}^{\mathsf{ideal}}$ and $\{\mathsf{OTP\text{-}msg}\}_{i=1}^{n}$. In particular, the secret bit b in the simulated OTPs correspond to the input bit b of the receiver $\mathcal{R}$. Then, since (by our assumption) $\hat{\mathcal{E}}^{\mathsf{ideal}}$ queries the same bit b as in the OTPs with probability at least $\frac{1}{2} + \mathsf{non} - \mathsf{negl}$, Claim 9 follows.

Claim 9. $\hat{\mathcal{S}}$ successfully outputs $\mathcal{R}$'s secret bit with probability at least $\frac{1}{2} + \mathsf{non} - \mathsf{negl}$.

Case 2: Consider the case where $\hat{\mathcal{E}}^{\mathsf{ideal}}$ queries the same bit as in the OTP with probability $\leq \frac{1}{2} + \mathsf{negl}$. This implies that with probability $\geq \frac{1}{2} - \mathsf{negl}$, $\hat{\mathcal{E}}^{\mathsf{ideal}}$ queries different bit. Then, $\hat{\mathcal{E}}^{\mathsf{ideal}}$ received a different bit from $\mathcal{F}_{\mathsf{OT}}^{\mathsf{Main}}$ than what it needs in order to learn secret. In this case, $\hat{\mathcal{E}}^{\mathsf{ideal}}$ *fails* to guess s_b correctly with probability at least $\frac{1}{4} - \mathsf{negl}$ and hence cannot output secret with probability at least $\frac{1}{4} - \mathsf{negl}$. Since we assume that $\hat{\mathcal{E}}^{\mathsf{ideal}}$ succeeds with probability at least $1 - \mathsf{negl}$, this is a contradiction.

5 A Composition Theorem for Static-Input Fixed-Role Concurrent Security

In this section, we give a composition theorem for static-input fixed-role concurrent (self-composition) security. Very roughly, the composition theorem says the following: suppose we are given an asynchronous non-interactive protocol $\Pi^{\mathcal{F}}$ that realizes functionality $\mathcal{G}$ with static-input fixed-role concurrent security in the $\mathcal{F}$-hybrid model. Then, replacing each ideal invocation of $\mathcal{F}$ in $\Pi^{\mathcal{F}}$ with a static-input fixed-role concurrently secure protocol for $\mathcal{F}$ yields a (real-world) protocol that realizes $\mathcal{G}$ with the same security.

More formally, the composition theorem is stated as follows:

Theorem 1. *Suppose $\Pi^{\mathcal{F}}$ is an asynchronous, non-interactive protocol that securely realizes $\mathcal{G}$ under concurrent self-composition in the static-input, fixed-role setting, and is secure against expected PPT adversaries. Also, suppose ρ is a protocol (in the plain model) that securely realizes $\mathcal{F}$ under concurrent self-composition in the static-input, fixed-role setting. Then Π^{ρ} securely realizes $\mathcal{G}$ under concurrent self-composition in the static-input, fixed-role setting.*

Proof. Let $\mathcal{A}$ denote a non-uniform probabilistic polynomial-time real-world adversary for protocol Π^{ρ} in the static-input fixed-role concurrent setting. For any such $\mathcal{A}$, we will construct a non-uniform probabilistic (expected) polynomial-time ideal-world adversary $\mathcal{S}$ that satisfies Definition 2. We will construct $\mathcal{S}$ by the following series of steps:

Step 1: Given $\mathcal{A}$, we will first construct a real-world adversary $\mathcal{A}'$ for protocol ρ in the static-input fixed-role concurrent setting.

Step 2: Next, given $\mathcal{A}'$, by static-input fixed-role concurrent security of ρ, we will obtain a simulator $\mathcal{S}'$ for ρ.

Step 3: Now, given $\mathcal{S}'$, we can easily obtain an (hybrid-world) adversary $\mathcal{A}^{\mathcal{F}}$ for $\Pi^{\mathcal{F}}$ in the static-input fixed-role concurrent setting.

Step 4: Finally, given $\mathcal{A}^{\mathcal{F}}$, by relying on the static-input fixed-role concurrent security of the asynchronous non-interactive protocol $\Pi^{\mathcal{F}}$, we obtain our final simulator $\mathcal{S}$.

Before we proceed to elaborate on these steps, we first setup some notation. We model Π^{ρ} (as well as ρ) as a two-party protocol between Alice and Bob. Let m denote the total number of concurrent executions of Π^{ρ} that $\mathcal{A}$ participates in. We will denote these sessions by $\mathsf{s}_1, \ldots, \mathsf{s}_m$. Note that since we are in the fixed-roles setting, $\mathcal{A}$ corrupts parties with the same role (i.e., either Alice or Bob) in all the executions of Π^{ρ}. For simplicity of exposition, we denote the honest party in session s_i by a unique identifier P_i. In reality, the machines P_i may not be unique and more than one P_i may in fact refer to a single honest party; thus capturing the scenario where $\mathcal{A}$ engages in more than one protocol session with an honest party. We further note that since we are in the static-input setting, the inputs of $P_1, \ldots, P_m$ are fixed prior to any protocol execution. Let k denote the number of invocations

of $\mathcal{F}$ in the asynchronous non-interactive protocol $\Pi^{\mathcal{F}}$. Then, note that a session s_i of Π^{ρ} consists of k executions of ρ, denoted $\mathsf{s}_{i,1}, \ldots, \mathsf{s}_{i,k}$. Thus, m sessions of Π^{ρ} consist of $m \cdot k$ sessions of ρ.

We now proceed to explain Steps 1 to 4 in more detail.

Step 1: Given adversary $\mathcal{A}$, we construct a real-world adversary $\mathcal{A}'$ for ρ in the following manner. $\mathcal{A}'$ starts by internally running $\mathcal{A}$. If $\mathcal{A}$ wishes to corrupt all parties playing the role of Alice (resp., Bob) in the m sessions of Π^{ρ}, then $\mathcal{A}'$ corrupts Alice (resp., Bob) in all the $m \cdot k$ sessions of ρ. Whenever $\mathcal{A}$ wishes to schedule a new session $s_{i,j}$ of ρ in session i of Π^{ρ}, $\mathcal{A}'$ schedules a new session of ρ with party P_i. $\mathcal{A}'$ simply forwards the messages of ρ between P_i and $\mathcal{A}$. Finally, $\mathcal{A}$ stops and outputs its view. $\mathcal{A}'$ outputs the same view and halts.

It follows from the above description that if $\mathcal{A}$ is a non-uniform probabilistic polynomial-time real-world adversary for m sessions of Π^{ρ} in the static-input fixed-roles concurrent setting, then $\mathcal{A}'$ is a non-uniform probabilistic polynomial-time real-world adversary for $m \cdot k$ sessions of ρ in the static-input fixed-roles concurrent setting. Note that the view output by $\mathcal{A}'$ is identical to that output by $\mathcal{A}$.

Step 2: Next, since ρ realizes $\mathcal{F}$ in the static-input fixed-roles concurrent setting, given $\mathcal{A}'$, we immediately obtain an non-uniform probabilistic (expected) polynomial-time ideal-world adversary $\mathcal{S}'$ that corrupts the same parties as $\mathcal{A}'$ does and outputs a view (computationally) indistinguishable from that output by $\mathcal{A}'$.

Step 3: Now, given $\mathcal{S}'$, we construct a (hybrid-world) adversary $\mathcal{A}^{\mathcal{F}}$ for protocol $\Pi^{\mathcal{F}}$ in the following manner. $\mathcal{A}^{\mathcal{F}}$ starts by internally running $\mathcal{S}'$. If If $\mathcal{S}'$ wishes to corrupt all parties playing the role of Alice (resp., Bob) in the $m \cdot k$ ideal-world sessions with $\mathcal{F}$, then $\mathcal{A}^{\mathcal{F}}$ corrupts Alice (resp., Bob) in all the m sessions of Π^{ρ}. Now, consider any $i \in [m]$. Whenever $\mathcal{S}'$ issues a query to functionality $\mathcal{F}$ for a session $\mathsf{s}_{i,j}$ such that it has never previously queried $\mathcal{F}$ for a session $\mathsf{s}_{i,j'}$ (where $j' \neq j$), $\mathcal{A}^{\mathcal{F}}$ initiates the session s_i of $\Pi^{\mathcal{F}}$ with party P_i and forwards the query of $\mathcal{S}'$ to $\mathcal{F}$ and returns $\mathcal{F}$'s response to $\mathcal{S}'$. Any future queries of $\mathcal{S}'$ for session $s_{i,j'}$ are simply forwarded by $\mathcal{A}^{\mathcal{F}}$ to $\mathcal{F}$ and the response is returned to $\mathcal{S}'$. This completes the description of $\mathcal{A}^{\mathcal{F}}$.

It follows immediately from the above description that if $\mathcal{S}'$ runs in (expected) polynomial-time, then $\mathcal{A}^{\mathcal{F}}$ runs in (expected) polynomial time as well, and outputs a view identical to that output by $\mathcal{S}'$. Further, note that by definition, $\mathcal{S}'$ makes $m \cdot k$ total ideal invocations of $\mathcal{F}$. However, these invocations of $\mathcal{F}$ may be in *any arbitrary order*. Specifically, the k invocations $\mathsf{s}_{i,1}, \ldots, \mathsf{s}_{i,k}$ of $\mathcal{F}$ corresponding to a single session s_i of $\Pi^{\mathcal{F}}$ may *not* be in parallel. Therefore, the resultant adversary $\mathcal{A}^{\mathcal{F}}$ is asynchronous in that it may make the k queries to $\mathcal{F}$ for a single session of $\Pi^{\mathcal{F}}$ in any arbitrary order.

Step 4: Finally, since $\Pi^{\mathcal{F}}$ realizes $\mathcal{G}$ in $\mathcal{F}$-hybrid model in the static-input fixed-roles concurrent setting, and since $\Pi^{\mathcal{F}}$ is asynchronous, given adversary $\mathcal{A}^{\mathcal{F}}$, we obtain an ideal-world adversary $\mathcal{S}$ that only interacts with $\mathcal{G}$ and outputs a view indistinguishable from that output by $\mathcal{A}^{\mathcal{F}}$. This is our final simulator. (Note that since $\mathcal{A}^{\mathcal{F}}$ may be expected polynomial-time, we require that $\Pi^{\mathcal{F}}$ is secure against expected polynomial-time adversaries.) □

6 Putting it All Together

In this section we summarize our results. All functionalities referred to below are 2-party finite deterministic non-reactive functionalities. For brevity and clarity we drop these qualifiers. In Section 4 we showed the following impossibility.

Theorem 2. *There does not exist a protocol that securely realizes $\mathcal{F}_{\mathsf{OT}}$ under concurrent self-composition even in the static-input, fixed-role setting.*

In Section 3 we gave a new asynchronous, non-interactive protocol for OT using any non-trivial asymmetric functionality:

Theorem 3. *For any non-trivial asymmetric functionality $\mathcal{F}$, there exists an asynchronous, non-interactive protocol $\Pi^{\mathcal{F}}$ that UC-securely realizes $\mathcal{F}_{\mathsf{OT}}$. This protocol is also secure against computationally unbounded adversaries and expected PPT adversaries.*

In Section 5, we prove the following composition theorem for security under concurrent self-composition in the static-input, fixed-role setting.

Theorem 4. *Suppose $\Pi^{\mathcal{F}}$ is an asynchronous, non-interactive protocol that securely realizes $\mathcal{G}$ under concurrent self-composition in the static-input, fixed-role setting, and is secure against expected PPT adversaries. Also, suppose ρ is a protocol (in the plain model) that securely realizes $\mathcal{F}$ under concurrent self-composition in the static-input, fixed-role setting. Then Π^{ρ} securely realizes $\mathcal{G}$ under concurrent self-composition in the static-input, fixed-role setting.*

Since UC-security implies security under concurrent self-composition in the static-input, fixed-role setting, by composing the OT protocol in Theorem 3 with a hypothetical protocol for any non-trivial asymmetric functionality $\mathcal{F}$ (using Theorem 1), we will obtain a protocol for $\mathcal{F}_{\mathsf{OT}}$, contradicting Theorem 2. This gives our main impossibility result:

Theorem 5. *For any non-trivial asymmetric functionality $\mathcal{F}$, there does not exist a protocol (in the plain model) that securely realizes $\mathcal{F}$ under self-composition even in the static-input, fixed-role setting. (On the other hand, every trivial asymmetric functionality has a UC-secure protocol.)*

Another consequence of the protocol in Theorem 3 is to give a characterization of functionalities that are *non-interactively complete* against active adversaries. This is because $\mathcal{F}_{\mathsf{OT}}$ itself has this property, as was shown by the following non-interactive (but not asynchronous) protocol from [IPS08].

Theorem 6. *[IPS08, Full version] For any asymmetric functionality $\mathcal{G}$, there exists a non-interactive protocol $\Phi^{\mathcal{F}_{\mathsf{OT}}}$ that UC-securely realizes $\mathcal{G}$. This protocol is also secure against computationally unbounded adversaries and expected PPT adversaries.*

Since the protocols in our positive results above are UC-secure, by the UC theorem their composition is secure. Further, composing a non-interactive protocol in $\mathcal{F}_{\mathsf{OT}}$-hybrid with a non-interactive protocol for $\mathcal{F}_{\mathsf{OT}}$ in $\mathcal{F}$-hybrid gives a non-interactive protocol in $\mathcal{F}$-hybrid. This gives us the following characterization:

Theorem 7. *In the class of asymmetric functionalities, every non-trivial functionality is non-interactively complete with respect to UC security (against active adversaries).*

That is, for any two asymmetric functionalities $\mathcal{F}$, $\mathcal{G}$, if $\mathcal{F}$ is non-trivial, then there exists a non-interactive protocol $\Psi^{\mathcal{F}}$ that UC-securely realizes $\mathcal{G}$. This protocol is also secure against computationally unbounded adversaries and expected PPT adversaries.

Theorem 5 and Theorem 7 are the main results in this work. In addition, the protocol in Theorem 3 is of independent interest.

References

[BCNP04] Boaz Barak, Ran Canetti, Jesper Buus Nielsen, and Rafael Pass. Universally composable protocols with relaxed set-up assumptions. In *FOCS*, pages 186–195, 2004.

[BPS06] Boaz Barak, Manoj Prabhakaran, and Amit Sahai. Concurrent non-malleable zero knowledge. In *FOCS*, pages 345–354, 2006.

[BS05] Boaz Barak and Amit Sahai. How to play almost any mental game over the net - concurrent composition via super-polynomial simulation. In *FOCS*, pages 543–552, 2005.

[Can01] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS*, pages 136–147, 2001.

[Can05] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. http://eprint.iacr.org/2000/067, 2005.

[CF01] Ran Canetti and Marc Fischlin. Universally composable commitments. In *CRYPTO*, pages 19–40, 2001.

[CKL03] Ran Canetti, Eyal Kushilevitz, and Yehuda Lindell. On the limitations of universally composable two-party computation without set-up assumptions. In *EUROCRYPT*, pages 68–86, 2003.

[CLOS02] Ran Canetti, Yehuda Lindell, Rafail Ostrovsky, and Amit Sahai. Universally composable two-party and multi-party secure computation. In *STOC*, pages 494–503, 2002.

[CLP10] Ran Canetti, Huijia Lin, and Rafael Pass. Adaptive hardness and composable security in the plain model from standard assumptions. In *FOCS*, pages 541–550, 2010.

[CPS07] Ran Canetti, Rafael Pass, and Abhi Shelat. Cryptography from sunspots: How to use an imperfect reference string. In *FOCS*, pages 249–259, 2007.

[DNS98] Cynthia Dwork, Moni Naor, and Amit Sahai. Concurrent zero-knowledge. In *STOC*, pages 409–418, 1998.

[GGJS12] Sanjam Garg, Vipul Goyal, Abhishek Jain, and Amit Sahai. Concurrently secure computation in constant rounds. In *EUROCRYPT*, 2012.

[GIS+10] Vipul Goyal, Yuval Ishai, Amit Sahai, Ramarathnam Venkatesan, and Akshay Wadia. Founding cryptography on tamper-proof hardware tokens. In *TCC*, pages 308–326, 2010.

[GJO10] Vipul Goyal, Abhishek Jain, and Rafail Ostrovsky. Password-authenticated session-key generation on the internet in the plain model. In *CRYPTO*, pages 277–294, 2010.

[GKOV12] Sanjam Garg, Abishek Kumarasubramanian, Rafail Ostrovsky, and Ivan Visconti. Impossibility results for static input secure computation. In *CRYPTO*, 2012.

[GKR08] Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum. One-time programs. In *Proceedings of the 28th Annual conference on Cryptology: Advances in Cryptology*, CRYPTO 2008, pages 39–56, 2008.

[GMW87] O. Goldreich, S. Micali, and A. Wigderson. How to play ANY mental game. In *STOC*, pages 218–229, 1987.

[Goy11] Vipul Goyal. Positive results for concurrently secure computation in the plain model. *IACR Cryptology ePrint Archive*, 2011:602, 2011.

[IPS08] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In *CRYPTO*, pages 572–591, 2008. Preliminary full version on http://www.cs.uiuc.edu/~mmp/.

[Kat07] J. Katz. Universally composable multi-party computation using tamper-proof hardware. In *Advances in Cryptology — Eurocrypt 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 115–128. Springer, 2007.

[Kil00] Joe Kilian. More general completeness theorems for secure two-party computation. In *STOC*, pages 316–324, 2000.

[KL11] Dafna Kidron and Yehuda Lindell. Impossibility results for universal composability in public-key models and with fixed inputs. *J. Cryptology*, 24(3):517–544, 2011.

[KM11] Daniel Kraschewski and Jörn Müller-Quade. Completeness theorems with constructive proofs for finite deterministic 2-party functions. In *TCC*, pages 364–381, 2011.

[KP01] Joe Kilian and Erez Petrank. Concurrent and resettable zero-knowledge in poly-logarithm rounds. In *STOC*, pages 560–569, 2001. Preliminary full version published as cryptology ePrint report 2000/013.

[Lin03] Yehuda Lindell. General composition and universal composability in secure multi-party computation. In *FOCS*, pages 394–403, 2003.

[Lin04] Yehuda Lindell. Lower bounds for concurrent self composition. In *TCC*, pages 203–222, 2004.

[Lin08] Yehuda Lindell. Lower bounds and impossibility results for concurrent self composition. *J. Cryptology*, 21(2):200–249, 2008.

[LPV09] Huijia Lin, Rafael Pass, and Muthuramakrishnan Venkitasubramaniam. A unified framework for concurrent security: universal composability from stand-alone non-malleability. In *STOC*, pages 179–188. ACM, 2009.

[MPR06] Silvio Micali, Rafael Pass, and Alon Rosen. Input-indistinguishable computation. In *FOCS*, pages 367–378, 2006.

[Pas03] Rafael Pass. Simulation in quasi-polynomial time, and its application to protocol composition. In *EUROCRYPT*, pages 160–176, 2003.

[PR08] Manoj Prabhakaran and Mike Rosulek. Cryptographic complexity of multi-party computation problems: Classifications and separations. In *CRYPTO*, pages 262–279, 2008.

[PRS02] Manoj Prabhakaran, Alon Rosen, and Amit Sahai. Concurrent zero knowledge with logarithmic round-complexity. In *FOCS*, pages 366–375, 2002.

[PS04] Manoj Prabhakaran and Amit Sahai. New notions of security: achieving universal composability without trusted setup. In *STOC*, pages 242–251, 2004.

[RK99] Ransom Richardson and Joe Kilian. On the concurrent composition of zero-knowledge proofs. In *EUROCRYPT*, pages 415–431, 1999.

[Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets. In *FOCS*, pages 162–167, 1986.