Universally Composable Secure Computation with Corrupted Tokens

Nishanth Chandran[1], Wutichai Chongchitmate[2⋆], Rafail Ostrovsky[3⋆⋆], and Ivan Visconti[4⋆⋆⋆]

[1] Microsoft Research India, India
nichandr@microsoft.com
[2] Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, Thailand
wutichai.ch@chula.ac.th
[3] Department of Computer Science and Department of Mathematics, University of California, Los Angeles CA, USA
rafail@cs.ucla.edu
[4] DIEM, University of Salerno, Italy
visconti@unisa.it

Abstract. We introduce the *corrupted token model*. This model generalizes the *tamper-proof token model* proposed by Katz (EUROCRYPT '07) relaxing the trust assumption on the honest behavior of tokens. Our model is motivated by the real-world practice of outsourcing hardware production to possibly corrupted manufacturers. We capture the malicious behavior of token manufacturers by allowing the adversary to corrupt the tokens of honest players at the time of their creation.
We show that under minimal complexity assumptions, i.e., the existence of one-way functions, it is possible to UC-securely realize (a variant of) the tamper-proof token functionality of Katz in the corrupted token model with n stateless tokens assuming that the adversary corrupts at most $n-1$ of them (for any $n > 0$). We apply this result to existing multi-party protocols in Katz's model to achieve UC-secure MPC in the corrupted token model assuming only the existence of one-way functions. Finally, we show how to obtain the above results using tokens of small size that take only short inputs. The technique in this result can also be used to improve the assumption of UC-secure hardware obfuscation recently proposed by Nayak *et al.* (NDSS '17). While their construction requires the existence of collision-resistant hash functions, we can obtain

⋆ Work done while the author was at Department of Computer Science, University of California, Los Angeles.

⋆⋆ Research supported in part by NSF-BSF grant 1619348, DARPA SafeWare subcontract to Galois Inc., DARPA SPAWAR contract N66001-15-C-4065, US-Israel BSF grant 2012366, JP Morgan Faculty Award, OKAWA Foundation Research Award, IBM Faculty Research Award, Xerox Faculty Research Award, B. John Garrick Foundation Award, Teradata Research Award, and Lockheed-Martin Corporation Research Award. The views expressed are those of the authors and do not reflect position of the Department of Defense or the U.S. Government.

⋆⋆⋆ Work done in part while the author was visiting UCLA.

the same result from only one-way functions. Moreover using our main result we can improve the trust assumption on the tokens as well.

1 Introduction

UC-secure MPC. Secure multi-party computation [27] (MPC) allows mutually distrustful parties to jointly compute a function f, while preserving the privacy of their inputs/outputs. Canetti [8] introduced the notion of universal composability (UC) to model secure MPC in an environment where multiple concurrent executions of different protocols take place. Unfortunately UC security is significantly harder to achieve than plain secure computation. In fact, in the plain model (i.e., without trusted set-up assumptions, physical assumptions, superpolynomial-time simulation and so on) most functionalities can not be UC-realized [11, 13]. Impossibility results exist even for the basic case of self-concurrent composition with static inputs [4, 1, 25].

In light of these impossibility results, various trust assumptions have been studied in order to obtain UC-secure constructions. Among these, one of the most studied is that of tamper-proof hardware tokens. Hofheinz *et al.* [32], considered the notion of "tamper-proof devices" in the form of signature cards in order to realize UC-secure protocols. They show how to construct UC-secure commitment and zero-knowledge arguments using tamper-proof signature cards as the setup assumption. The more general formalization of tamper-proof hardware tokens was given by Katz [35]. Katz's tamper-proof token functionality abstractly captures a physical tamper-proof hardware token that is created and sent by a sender to a receiver. The receiver can use the token to execute the program stored in it multiple times as a black-box, on inputs of his choice. Tokens can be either *stateful* (i.e., they retain an updatable memory between executions; this is a stronger trust assumption because it additionally assumes a tamper-proof updatable memory) or *stateless* (i.e., all executions start with the same configuration). Motivated by the practical relevance of the model, as well as the challenging open questions on the feasibility of protocols in this model, UC-security with tamper-proof tokens has been widely explored with a focus on the more challenging case of stateless tokens [14, 36, 29, 17, 15, 20, 31, 39, 5].

Token manufacturing. Assuming that tokens are honestly generated is clearly a very demanding assumption that essentially requires honest players to rely on the honesty of a token manufacturer that they trust. Hence, while the tamper-proof token model works as a physical assumption in theory, in practice it degenerates into a model where the security of an honest player depends on the honest behavior of an external player chosen by the honest player[5]. All prior works that consider hardware-based security critically rely on the honest player being able to reliably construct tamper-proof tokens. An attempt to relax this assumption was

[5] A similar question for the case of Common Reference String (CRS) generation was answered in the multi-string model [30]

done in [23] focusing only on the set intersection functionality, without considering UC security. More recently, [2] considered the problem of outsourcing circuit fabrication where a given circuit is compiled into smaller components, each of which can be outsourced to a possibly malicious manufacturer. The components (both honestly and maliciously manufactured) are then re-assembled honestly to get a "secure hardware token". Their (stand-alone) security model only allows an adversary black-box access to the rebuilt circuit, and not the individual components and additionally also requires one "small" tamper-proof token that can be generated honestly in a trusted manner. In contrast, we do not wish to make any assumptions on small trusted components and consider composability. The above state of affairs brings us to the following natural question.

"Can we obtain UC-secure hardware-based security in a world where most hardware token manufacturers may be corrupt?"

1.1 Our Results

We resolve the above open problem in the positive under minimal complexity assumptions. We now discuss all our contributions in detail.

The corrupted token model. We consider the concrete scenario where the sender of a token does not have the ability to physically create a tamper-proof token, but instead has to rely on possibly untrusted manufacturers. In case a manufacturer is corrupted (and may be colluding with other parties), the program embedded in the token may be leaked, or replaced in its entirety. In other words, tokens in this model can be tampered arbitrarily at the time of creation.

To model security, we define a functionality for UC security allowing the design of protocols that make use of tokens generated by potentially adversarial manufacturers. In turn, we propose a new model extending the stateless version of Katz's tamper-proof token model in [35], that we call *corrupted token model*. In our new model, the adversary is allowed to corrupt tokens when they are created by honest parties. The attack happens during the token creation phase, and the adversary learns all information that the honest player wanted to store in the token. Moreover the adversary is allowed to replace the token with a different token of its choice, including even a stateful one.

The corrupted token model abstractly represents the process of outsourcing the production of hardware tokens to possibly corrupted manufacturers. This is the reason why we allow corruption to occur only at the time the tokens are created. Our model also allows adaptive corruption of the manufacturers, in the sense that the adversary may choose to corrupt the next request of token generation of an honest player depending on what has been learnt so far. Finally, the adversary can freely decide the content of corrupted tokens and can even make it stateful. This is similar to dealing with a real-world hardware Trojan as described in [21, 38] with a few key differences. In the model of [21], there exists an incorruptible "master circuit," whose role is to manage communication between tokens honestly. The model of [38] also has a "controller" circuit, whose role is similar to the master circuit in [21], but is allowed to be compromised. On

the other hand, our model does not have a token with a specific role and allows any token to be corrupted. Both [21] and [38] do not consider UC security and additionally the construction of [38] is based on variants of ElGamal public-key encryption and Schnorr signature scheme, whose security are based on hardness of elliptic curve Diffie-Hellman and discrete logarithm, respectively. Our construction is UC-secure and is based on the minimal assumption of OWFs.

Katz's token functionality in the corrupted token model. We construct a protocol in the corrupted token model using n tokens that UC-realizes a stronger variant of Katz's tamper-proof token functionality. We call such a variant the *tamper-proof token with abort* functionality. The difference between the tamper-proof token with abort functionality and the original Katz's tamper-proof token functionality is that our variant allows the adversary to learn that a token has been sent (even between honest parties), and can choose to abort and prevent the delivery of that token. This captures the realistic scenario where an adversary physically prevents token delivery and thus stops the protocol that relies on tokens. Still the adversary learns nothing about the program in the uncorrupted token generated by the honest party. The need for abort in the functionality is unavoidable as seen through the following reasoning. Suppose the tamper-proof token functionality (without abort) can be realized by n corruptible tokens. Then, the adversary in the corrupted token model corrupts all but one of the tokens and replaces them with corrupted tokens that do nothing. Now, if the tamper-proof token functionality without abort is realized with the remaining (uncorrupted) token, then this token must hold the complete program and secrets of the honest party (so that it can carry out the computation by itself). However, in an alternate corruption strategy, this token is also susceptible to corruption, and if the adversary had instead corrupted only this token, she would have learnt all secrets of the original honest token in Katz's model resulting in the insecurity of the protocol. Hence, the functionality must allow for aborts.

It is easy to see that this argument extends to the case of any dishonest majority (i.e., even with only $\lfloor n/2 + 1 \rfloor$ corrupted tokens). Our protocol UC-realizes the tamper-proof token with abort functionality assuming that the adversary corrupts at most $n - 1$ tokens where n is the number of token creations invoked by an honest party. We remark that, if we were willing to make the assumption that a majority of token manufacturers were honest, then we can avoid aborting the protocol when the adversary corrupts a (minority) fraction of the tokens.

The notion of token transfer across the environment in various sessions in the Global-UC (GUC) framework has been studied recently by Hazay *et al.* [31]. Obtaining GUC security is more challenging and we leave the question of GUC security in the corrupted token model to future research. Still, we stress that in many natural scenarios, UC security already suffices and achieves a very strong level of security under composition with any other protocol as long as there is a way to avoid the *sharing of the same setup among sessions.*

A compiler to reduce trust in tokens. As our main result, we show how to transform any protocol in Katz's tamper-proof token model into a protocol in our

corrupted token model thereby improving the trust assumption of several hardware token-based protocols. Indeed the transformed protocol remains secure even when $n-1$ out of the n tokens created by honest parties are corrupted at the time of creation. Our transformation preserves UC security and only assumes the existence of one-way functions (OWF). We focus on stateless tokens since this is the milder physical assumption and is the most challenging case. We remark here that requiring one token to be uncorrupted is unavoidable. To see this, suppose for the sake of contradiction, there is a protocol UC-realizing a tamper-proof token functionality using n corruptible tokens that remains secure even when an adversary corrupts all n tokens. Now suppose an adversary in the secure computation protocol corrupts all but one of the parties and corrupts all the tokens manufactured by this party. Now, if the resulting protocol still remains secure, then this would give us a UC-secure MPC protocol (secure against all-but-one corruption) with no trusted setup, as all "trusted" components created by the honest party are corrupted (in more detail, generating and sending a token could then be replaced by sending a message with the description of the program of the token). This contradicts known impossibility results [11, 13]. Hence, we must assume that at least one hardware token created by every honest party is uncorrupted. Additionally, the existence of OWFs is the minimal assumption that one can hope for since, as argued in [29], any unbounded adversary can query a stateless tokens exponentially many times to learn the programs embedded.

Our transformation can be applied to existing protocols in the Katz's token model to obtain new results in the corrupted token model. For instance, starting with the recent UC-secure MPC constructions in the tamper-proof token model based on OWFs [31], we get the same results in the corrupted token model assuming only OWFs.

Other results and sub-protocols. As an additional result, we improve the result of [39] by removing the need of collision-resistant hash functions, and apply our transformation to obtain an obfuscation protocol in the corrupted token model based solely on OWFs. Moreover, as a building block for our constructions, we present a simultaneous resettable zero-knowledge (sim-res ZK) argument and UC-secure MPC for any well-formed functionality in the correlated randomness (CR) model assuming OWFs only. In the CR model, each party has access to a private, input-independent, honestly generated, string before the execution of the protocol by the correlated randomness functionality. These protocols may be of independent interest. We stress that correlated randomness is not required as a setup for our construction achieving UC security in the corrupted token model and is only used as an intermediate building block.

1.2 High-Level Overview of Our Constructions

Realizing Katz's token functionality. We begin by describing how to UC-realize Katz's token functionality in the $(n, n-1)$-token-corruptible hybrid model, (i.e., the model where n tokens are generated by an honest player and at most $n-1$ are corrupted by the adversary at the time of token generation). We refer to

the final protocol that realizes Katz's functionality as Π. Protocol Π will make use of a UC-secure n-party protocol Π' and a sim-res ZK argument Π_{rsZK} with straight-line simulator, both in the CR model[6]. At a very high level, we construct Π as follows. Given a description of the program P for Katz's tamper-proof token (such a description is specified by the protocol in Katz's model) we first create n shares of the description of P using an n-out-of-n threshold secret sharing scheme. Then n tokens are created as follows. The program of the i-th token includes: 1) the i-th share; 2) commitments of all shares; 3) decommitment information for the i-th share; 4) correlated randomness to run the n-party UC-secure MPC in the CR model; 5) correlated randomness to run a simultaneous resettable ZK in the CR model; 6) seed for a PRF; and 7) random tape for commitment of the seed.

When a user must query a Katz token implementing program P on input x, he/she must first send each token this input value (a dishonest user may send different values to different tokens). We shall refer to the "version" that the i^{th} token receives by x_i. When queried with an input x_i, the i-th token first commits to its input (i.e., x_i) and to its seed for the PRF (see point 6 above). The randomness used for the first commitment comes from evaluating the PRF using the above seed and the input x_i while the randomness for the second commitment is the string stored in the token (see point 7 above). These commitments provided by all the tokens together is called the determining message. For the remaining execution of Π, each token obtains the random tape needed by Π' and Π_{rsZK} by computing the PRF on the determining message (and a unique ID value) using its seed. The tokens will execute an n-party UC-secure MPC protocol in the CR model, Π' (see point 4 above). More specifically, the i-th token, if honest, will run the code of the i-th player of Π' on input the following pair: the received input (i.e., x_i) and the i-th share of P (see step 1 above). Π' will securely compute the functionality that reconstructs P from the shares that are part of the inputs of the players and then executes P on input x. The reconstruction aborts if $x \neq x_i$ for some i. Each Π' message m sent by the i^{th} token is followed by a simultaneous resettable ZK argument of knowledge (see step 5 above) proving that the message m is computed correctly according to the committed PRF seed and the i-th committed share (see step 2 and 3 above) of P.

The resettable soundness of the ZK argument guarantees that a corrupted token cannot deviate from the underlying MPC protocol Π' even when the adversary can execute any tokens any number of times on any inputs of his choice (even after resetting the state of the honest token several times). Moreover, the security of Π' guarantees that the adversary corrupting all but one token does not learn anything about the inputs of uncorrupted tokens other than x_i he chooses and the output. This means the adversary only learns at most $n - 1$

[6] The correlated randomness is the key that allows us to avoid the impossibility of resettably-secure computation in the standard model proven in [25]. However, we stress that correlated randomness is not required by our main theorem for UC security with tamper-proof stateless corruptible tokens from OWFs.

shares of the program P, and thus learns nothing about P by the security of the secret sharing scheme.

Since tokens are stateless, we employ the technique in [39] to encrypt the state of the token and output it along with the message. Each subsequent invocation of the token requires an encrypted previous state as additional input. A symmetric key encryption scheme is used to prevent the adversary to learn or modify states of uncorrupted tokens. This allows us to construct a simulator that simulates both the MPC and ZK messages using their simulators.

Simultaneous resettable ZK argument in the CR model. The above discussion assumed the existence of a sim-res ZK argument Π_{srZK} with straight-line simulator in the CR model. We obtain this result in 2 steps starting from a 3-round public-coin ZK argument Σ, in the CRS model with straight-line simulation based on OWFs (such as the one in [37]).

First, we add the argument of knowledge (AoK) property with straight-line witness extractor to Σ in the CR model. For this, we use a technique similar to the one used in [24] where a prover encrypts a witness, sends the encryption as a message, and then uses Σ to prove that it is the encryption of the right witness. To avoid the use of stronger assumptions than OWFs, we replace a public-key encryption scheme in [24] with a secret-key encryption scheme and a commitment scheme. The commitment of a secret key and its corresponding decommitment information are given to the prover while only the commitment is given to the verifier as part of their correlated randomness. The resulting protocol is still 3-round, public-coin and with straight-line simulation.

In the second step, we add a simultaneous resettable witness indistinguishability (sim-res WI) argument of knowledge from OWFs to construct a simultaneous resettable zero-knowledge argument in the CR model with straight-line simulation. To prevent a malicious prover from resetting, the verifier uses a PRF applied to the statement and the prover's message to generate a string c to play in the second round of Σ instead of uniformly sampling her message. Then, to prevent a malicious verifier from resetting, the verifier runs the prover of the sim-res WI to prove that c is generated honestly or that a given long string d is an output of a PRG on input a short seed. Since d is uniformly chosen as part of the correlated randomness, the verifier cannot maliciously manipulate c. Resettable soundness can then be shown through a hybrid experiment where d is generated from the PRG similarly to [19].

UC-secure n-party computation in the CR model. Our main result also assumed Π', i.e., a UC-secure n-party computation protocol in the CR model for any well-formed functionality. We next outline how we construct Π' based on OWFs.

First, we consider UC-secure MPC in the OT-hybrid model against a malicious adversary corrupting all but one party such as the one in [34]. Since OT can be generated using correlated randomness [6], we focus towards obtaining a UC-secure MPC in the CR model. However, we face a new challenge. Since our final protocol can be executed on polynomially many inputs, where the polynomial is not apriori known to the correlated randomness generator, we must be

able to produce "different" randomness for any input on which the protocol is generated. This would require a stronger version of the OT extension technique from [7] that allows the extension to super-polynomial number of OTs. This is similar in spirit to constructing a PRF that can generate "super-polynomial" randomness from a short seed (even though it will only be evaluated on polynomially many inputs). In particular, we modify the technique in [7] to construct UC-secure unbounded number of OTs from a small number of OTs distributed as setup in the CR model. We do this as follows. In the OT extension protocol in [7], a sender uses a circuit that first computes a PRG that takes a small input and outputs a large random string and then uses the string to obtain a large number of OTs. The circuit is then garbled using Yao's garbled circuit and sent to a receiver. The receiver then uses a small number of OTs to obtain a garbled input correspond to its small random seed. In our approach, the sender uses a PRF that allows us to generate super-polynomial number of such random strings. While a computationally bounded sender cannot compute a garbled circuit of super-polynomial size, it only needs to send a smaller subcircuit to compute the ith string in each execution. This garbled circuit is of polynomial size as in Beaver's version, computing only the required amount of OTs at a time. This is repeated to give an (apriori) unbounded number of OTs. Composing the UC-secure unbounded number of OTs in the CR model and a UC-secure MPC in the OT-hybrid model, we get UC-secure MPC in the CR model.

Getting rid of correlated randomness. While the building blocks Π' and Π_{rsZK} are in the CR model, our main protocol Π is not. Both subprotocols will be run by n tokens created by a single honest party to emulate the token functionality of a single well-formed token in Katz's model. Therefore, in Π, the party requesting the creation of a token can generate and give the correlated randomness to n different manufacturers. Hence, the correlated randomness is not a setup of our main result, and is computed by an honest player in our protocol to run subprotocols that need it. An adversary can replace the correlated randomness in $n-1$ of those tokens arbitrarily, and still our protocol is secure because Π' and Π_{rsZK} are secure with respect to such behavior. In fact, as a further optimization, if we wish to create tokens that are completely independent of each other, then the honest player in our protocol can create tokens that will only contain private keys to encryption and MAC schemes – the correlated randomness and shares of program required by the token can then be provided as encrypted and MACed input by the honest player to the token when they need to be used.

Reducing the token size. In order to ensure that the queries to tokens are short and the size of each token is small, we consider a technique used in [39] where a large input is fed into a token in blocks of small size. To ensure the consistency of the input, in [39] a Merkle's tree based on CRHFs is used to commit to the input beforehand. We improve on this technique by replacing the Merkle's tree with a new construction based on OWFs. At a very high level, we require the user to "commit" to his/her input by feeding the input bit-by-bit into to the token. The token will produce an authentication tag for every bit of the input

sequentially, such that the final authentication tag will act as a "commitment" to the user's input. This result is of independent interest as an improvement on the assumption of [39]. We generalize the technique of "bounded-size" tokens to our corrupted token protocol. We first give a variant of corrupted token functionality where the token size is independent of program P and the token can only accept queries of (apriori) fixed, constant size. We then construct a protocol that UC-realizes the corrupted token functionality in the corrupted "bounded-size" token hybrid model using the above technique. Finally, we combine this protocol with our main result to give a protocol that UC-realizes 'standard' tamper-proof token functionality in the corrupted "bounded-size" token hybrid model.

2 Preliminaries

A polynomial-time relation R is a relation for which it is possible to verify in time polynomial in $|x|$ whether $R(x, w) = 1$. Let us consider an $\mathcal{NP}$-language L and denote by R_L the corresponding polynomial-time relation such that $x \in L$ if and only if there exists w such that $R_L(x, w) = 1$. We will call such a w a *valid witness for* $x \in L$. Let λ denote the security parameter. A *negligible* function $\nu(\lambda)$ is a non-negative function such that for any constant $c < 0$ and for all sufficiently large λ, $\nu(\lambda) < \lambda^c$. We will denote by $\Pr_r[X]$ the probability of an event X over coins r, and $\Pr[X]$ when r is not specified. The abbreviation "PPT" stands for probabilistic polynomial time. For a randomized algorithm A, let $A(x; r)$ denote running A on an input x with random coins r. If r is chosen uniformly at random with an output y, we denote $y \leftarrow A(x)$. For a pair of interactive Turing machines (P, V), let $\langle P, V\rangle(x)$ denote V's output after interacting with P upon common input x. We say V accepts if $\langle P, V\rangle(x) = 1$ and rejects if $\langle P, V\rangle(x) = 0$. We denote by $\mathtt{view}^{P(w)}_{V(x,z)}$ the view (i.e., its private coins and the received messages) of V during an interaction with $P(w)$ on common input x and auxiliary input z. We will use the standard notion of computational indistinguishability [28].

2.1 Building Blocks

The main building blocks of our construction include simultaneous resettable ZK arguments and MPC in the CR model. Please see the full version of this paper [9] for various definitions related to interactive argument systems, zero-knowledge arguments of knowledge, witness indistinguishability and resettability in the CR model, adapted from their counterparts [12, 22, 3] in the plain model. We also present other standard definitions of commitments, secret sharing schemes and pseudorandom functions that we make use of in our construction.

2.2 UC Security in the Correlated Randomness (CR) Model

The correlated randomness (CR) model is an extension of the CRS model where each party has access to a string generated by a trusted third party. Unlike in the CRS model, the strings for parties may be different, but possibly correlated.

and unlike in the augmented CRS model of [10], honest parties can access their strings privately. Thus, it can be considered as a variant of the key registration (KR) model of [10].

Our CR model is defined to be consistent with the one of [33], taking into account the UC setting. A protocol ϕ in the CR model is defined with the corresponding correlated randomness functionality $\mathcal{F}_{corr}^{\phi}$, which generates a correlated random string for each party in the protocol ϕ independently of the parties' input. Each party can access its string (but not other parties' random strings) by invoking $\mathcal{F}_{corr}^{\phi}$. In the security proof, the ideal world simulator is allowed to obtain the correlated random strings associated to all parties, thereby having an advantage over the real-world adversary.

Let ϕ be n-party protocol in the CR model. Let $\mathcal{D}$ be a distribution on $S_1 \times \ldots \times S_n$ where S_i is the set of possible random strings for party P_i. The correlated randomness functionality $\mathcal{F}_{corr}^{\phi}$ is defined in Figure 1.

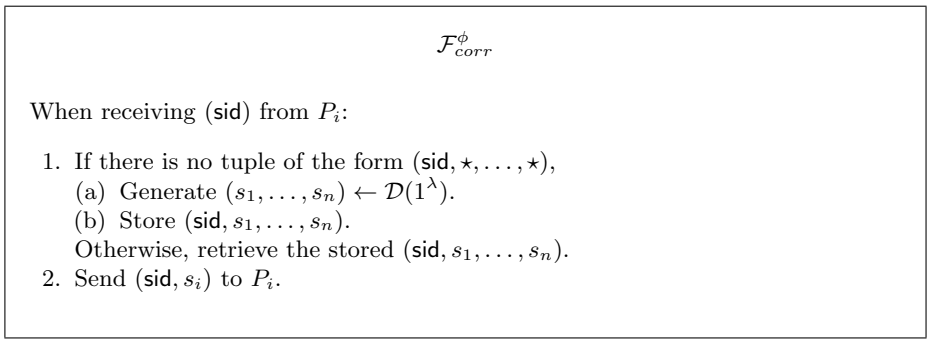

Fig. 1. Correlated Randomness Functionality $\mathcal{F}_{corr}^{\phi}$

Definition 1. *Let $\mathcal{F}$ be an ideal functionality and let ϕ be a multi-party protocol. Then the protocol ϕ UC realizes $\mathcal{F}$ in $\mathcal{F}_{corr}^{\phi}$-hybrid model if $\forall$ PPT hybrid model adversary $\mathcal{A}$, $\exists$ a uniform PPT simulator $\mathcal{S}$ such that for every non-uniform environment $\mathcal{Z}$, the following two ensembles are computationally indistinguishable*

$$\{\mathsf{View}_{\phi,\mathcal{A},\mathcal{Z}}^{\mathcal{F}_{corr}^{\phi}}(\lambda)\}_{\lambda\in\mathbb{N}} \approx^{c} \{\mathsf{View}_{\mathcal{F},\mathcal{S},\mathcal{Z}}(\lambda)\}_{\lambda\in\mathbb{N}}.$$

3 Simultaneous Resettable ZK from OWFs

In this section, we construct a simultaneous resettable ZK argument in the correlated randomness model with straight-line simulation. The security of our construction relies only on the existence of OWFs. The main building block for our construction is a 3-round public-coin ZK argument system in the CRS model

with straight-line simulation based on OWFs (such as in [37]). Using this public-coin argument system, we first construct a zero-knowledge *argument of knowledge* (ZKAoK) in the CR model with straight-line simulation and extraction. We then use this ZKAoK protocol to construct a simultaneously resettable zero-knowledge protocol in the correlated randomness model, based only on OWFs. We do so, in the following way: As part of the correlated randomness, the prover is given the commitment t, to the seed of a PRF, s, as well as a long random string d. The verifier is given the decommitment information (s and randomness) to this commitment t as well as d. Now, we have the verifier prove, using a simultaneous resettable WI (srWI) argument (based on OWFs [16]), that: either the verifier's random message c in the ZKAoK protocol is the output of a PRF (using seed s) on input the transcript so far, or that d is the output of a PRG on input a short string. The prover verifies the srWI argument and if this is successful, will execute the remainder of the ZKAoK taking c as the verifier's message. More details follow.

3.1 ZKAoK in the Correlated Randomness Model from OWFs

We first show how to convert a 3-round public-coin ZK argument system in the CRS model with straight-line simulation (based on OWFs) into one that is also an argument of knowledge (with straight-line simulation and straight-line witness extractor) in the CR model. Let $\Pi_{ZK} = (K, P, V)$ be the ZK argument in the CRS model with a straight-line simulator $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ (e.g. [37]). Let $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a CPA-secure secret key encryption scheme. Define (K', P', V') in the CR model as in Figure 2.

Lemma 1. *Π_{ZKAoK} is ZKAoK with straight-line simulator and witness extractor in the correlated randomness model.*

For a proof of the above lemma, please see the full version of this paper [9]. Note that if the protocol Π_{ZK} is 3-round and public-coin, the resulting protocol Π_{ZKAoK} is also 3-round and public-coin.

3.2 Simultaneous resettable ZK in the CR model from OWFs

We now construct a simultaneous resettable ZK argument system in the correlated randomness model based on OWFs. Let $\Pi_{ZKAoK} = (K_{ZKAoK}, P_{ZKAoK}, V_{ZKAoK})$ be a 3-round ZK argument of knowledge protocol in the CR model with transcript (m_1, c, m_2) where $c \in \{0,1\}^\lambda$ is chosen uniformly at random, a straight-line simulator $\mathcal{S}_{ZKAoK} = (\mathcal{S}_1, \mathcal{S}_2)$, and a straight-line witness extractor $\mathcal{E}_{ZKAoK} = (\mathcal{E}_1, \mathcal{E}_2)$ from Lemma 1. Let (P_{WI}, V_{WI}) be a srWI argument (e.g. [16]). Let $\{f_s\}_s$ be a family of pseudorandom functions such that for $s \in \{0,1\}^{\ell_0(\lambda)}$, f_s outputs $c \in \{0,1\}^\lambda$. Let $f : \{0,1\}^{\ell_1(\lambda)} \to \{0,1\}^{\ell_2(\lambda)}$ be a PRG. We define Π_{srZK} as in Figure 3.

The proof of resettable soundness goes as follows. We first consider the experiment with an imaginary protocol Π_F where a truly random function is used

$$\Pi_{ZKAoK} = (K', P', V')$$

$K'(1^\lambda)$:

1. $\sigma \leftarrow K(1^\lambda)$, $sk \leftarrow \mathsf{KeyGen}(1^\lambda)$. Let $k = \mathsf{com}(sk)$ and γ_0 be the decommitment information.
2. K' outputs $s_P = (\sigma, sk, k, \gamma_0)$ and $s_V = (\sigma, k)$.

Execution phase: P' on input (x, w) and private string s_P; V' on input x and private string s_V

1. P' parses $s_P = (\sigma, sk, k, \gamma_0)$, computes $e \leftarrow \mathsf{Enc}(sk, w)$ and sends e to V'.
2. V' parses $s_V = (\sigma, k)$.
3. P' and V' run $\langle P(w'), V\rangle(\sigma, x')$ where $x' = (x, e, k)$ and $w' = (w, sk, \gamma_0)$ to prove that there exists w, sk, γ_0 such that $(x, w) \in R_L$ and $w = \mathsf{Dec}(sk, e)$ and k can be decommitted to sk using γ_0.
4. V' outputs the output of V.

Fig. 2. ZKAoK argument protocol Π_{ZKAoK} in the correlated randomness model

instead of the PRF, and the verifier uses an alternate witness for the sim-res WI. We will show that Π_F is resettably sound by contradiction. Finally, we show that the probability that any resetting adversary can prove a false theorem in Π_{srZK} is negligibly close to that of Π_F through a series of hybrids. This implies that Π_{srZK} is also resettably-sound.

Lemma 2. *The protocol Π_{srZK} in the CR model is resettably-sound.*

Lemma 3. *Protocol Π_{srZK} is resettable ZK in the CR model with a straight-line simulator.*

For proofs of the above lemmas, please see the full version of this paper [9]. Lemmas 2 and 3 together gives us the following theorem:

Theorem 4. *Assuming the existence of OWFs, there exists a simultaneous resettable ZK argument protocol in the CR model with a straight-line simulator.*[7]

4 MPC in the Correlated Randomness Model

In this section, we construct a UC-secure MPC protocol in the CR model based on OWFs. The key ingredients are an MPC protocol in the OT-hybrid model UC-secure against an adversary corrupting all but one party, and a protocol UC-realizing unbounded number of OTs in the CR model. In [34], Ishai, Prabhakaran

[7] Our ZK argument protocol also has a straight-line witness extractor, but it is not necessary for our applications.

$$\Pi_{srZK} = (K, P, V)$$

$K(1^\lambda)$:

1. $(\sigma_P, \sigma_V) \leftarrow K_{ZKAoK}(1^\lambda)$, $s \leftarrow U_{\ell_0(\lambda)}$, $d \leftarrow U_{\ell_2(\lambda)}$. Let $t = \mathsf{com}(s)$ and γ be the decommitment information.
2. K outputs $s_P = (\sigma_P, t, d)$ and $s_V = (\sigma_V, s, \gamma, t, d)$.

Execution phase: P on input (x, w) and private string s_P; V on input x and private string s_V

1. P parses $s_P = (\sigma_P, t, d)$, runs $P_{ZKAoK}(x, w, \sigma_P)$ to compute m_1, and sends m_1 to V.
2. V parses $s_V = (\sigma_V, s, \gamma, t, d)$, runs $V_{ZKAoK}(x, \sigma_V)$ to sends $c = f_s(x||m_1)$ on behalf of V_{ZKAoK} to P (running P_{ZKAoK}), and runs $P_{WI}(y, (s, \gamma))$, with $y = (t, c, d, x, m_1)$, proving to P running $V_{WI}(y)$ that one of the following statements hold
   - there exists s' and γ such that t can be decommitted to s' using γ and $c = f_{s'}(x||m_1)$.
   - there exists d' such that $d = f(d')$.
3. If V_{WI} accepts, P continues running $P_{ZKAoK}(x, w, \sigma_P)$ to compute m_2 and send it to V.
4. V runs V_{ZKAoK} on (m_1, c, m_2) and outputs the output of V_{ZKAoK}.

Fig. 3. Simultaneous resettable ZK argument protocol Π_{srZK} in the CR model

and Sahai introduce the IPS compiler which combines an MPC with an honest majority and a protocol secure against semi-honest adversary in the OT-hybrid model to get a protocol UC-secure against malicious adversaries in the setting of no honest majority. One of their main applications, by applying the compiler to a variant of the protocol in [18], gives an MPC protocol in the OT-hybrid model that is UC-secure against a malicious adversary corrupting all but one party, assuming only a PRG. Unlike their main result, however, this MPC protocol requires a large number of OTs, proportional to the circuit size.

To address the number of OTs required, we then construct a UC-secure protocol for unbounded number of OTs in the CR model. The first attempt is to use Beaver's OT extension [7] from a bounded number of OTs which can be generated using correlated randomness [6]. The problem with this approach is that we can only get polynomial number (in the number of original OTs) of OTs for some fixed polynomial known in advance. However, in our protocol, we would require (an apriori) unknown number of OTs to be generated from the initial OTs – this is because the number of OTs needed depends on the number of times the hardware token is executed.

To get around this problem, we do as follows. We have the sender construct a super-polynomial size Yao's garbled circuit that computes the OTs. Of course, the sender cannot compute this entire garbled circuit. So, instead of sending the garbled circuit to the receiver, the sender commits to the first layer of the garbled circuit and the seed for the PRF that is used to generate the rest of the garbled circuit. When the receiver queries for the ith OT, the sender sends a section of the garbled circuit that suffices to compute the output followed by the ZK argument that it is consistent with committed values. However, this section of the circuit is now of polynomial size. This technique is similar in spirit to the GGM [26] technique for constructing a PRF. We now present more details.

4.1 Beaver's OT Extension

Before we construct a UC-secure protocol computing unbounded number of OTs, we first recall Beaver's construction [7]. Beaver considers two notions of OT.

- $\frac{1}{2}$OT: the sender S has x_0 and x_1. At the end of the protocol, the receiver learns (b, x_b) for a random bit b, the sender learns nothing about b.
- $\binom{2}{1}$OT: the sender has x_0 and x_1, the receiver has a bit b. At the end of the protocol, the receiver learns x_b, the sender learns nothing about b.

In [6], Beaver shows that $O(n)$ instances of $\binom{2}{1}$OT can be generated from $O(n^2)$ instances of $\frac{1}{2}$OT. In [7], the sender constructs a garbled circuit that takes a short input for a PRG, then expands it to a long string. Each bit of the string is used to select one of each pair of the sender's inputs. In order to get a garbled input corresponding to the receiver's seed and the garbled circuit, the sender and the receiver only need to perform a small number of OTs for each bit of the short input. This OT extension technique extends λ $\binom{2}{1}$OTs to $poly(\lambda)$ $\frac{1}{2}$OTs. This small number of OTs can be precomputed [6] as part of the correlated randomness. While this OT extension results in $\frac{1}{2}$OT, smaller number (but still polynomial) of $\binom{2}{1}$OT can be generated using the same number of starting OTs.

4.2 Unbounded Number of OTs

We now construct a UC-secure protocol computing unbounded number of OTs in the correlated randomness model assuming only OWFs. We consider the following modification to the OT extension above. Instead of a PRG, we use a PRF to generate a pseudorandom r_i for any $i \in \{0,1\}^\lambda$ using seed s_1 given to the sender on input $s_2||i$ where s_2 plays the same role as the seed in Beaver's extension protocol. Each r_i can be used to select the sender's input in the same way as in Beaver's protocol. However, the entire circuit (for all i) will have exponential size. To get around this problem, for each i, the sender only sends a garbled circuit corresponding to a subcircuit that suffices to compute an output based on the sender's ith input and r_i. We also use UC-secure ZK argument and commitment to ensure that malicious parties cannot deviate from the protocol. Since the whole garbled circuit is fixed given the committed values, the

sender cannot change the circuit and still successfully provide the ZK argument. Sender security is proved by arguing that the receiver does not learn more than the intended output by the property of the garbled circuits.

$$\mathsf{OT}^{\mathsf{unbounded}} = (K, S, R)$$

$K(1^\lambda)$:

1. $(\sigma_S, \sigma_R) \leftarrow K_0(1^\lambda)$, $\sigma_{ZK} \leftarrow K_{ZK}(1^\lambda)$, $s_1, s_2, s_3 \leftarrow S$. For $i = 1, 2, 3$, let $(c_i, \gamma_i) \leftarrow \mathsf{com}(s_i)$ with decommitment information $\gamma_i \in \{0,1\}^{\ell(\lambda)}$.
2. K outputs $s_S = (\sigma_S, \sigma_{ZK}, s_1, \gamma_1, s_3, \gamma_3, c_2)$ and $s_R = (\sigma_R, \sigma_{ZK}, s_2, \gamma_2, c_1, c_3)$.

Before 1st Execution phase: S on private string s_S; R on private string s_R

1. S parses $s_S = (\sigma_S, \sigma_{ZK}, s_1, \gamma_1, s_3, \gamma_3, c_2)$. Let $C(s, i) = C_{X,s_1,c_2}(s, i)$ be a circuit that outputs $(r_1, \ldots, r_n) = F_{s_1}(s||i)$. Let $(G, \pi) = \mathsf{GC}(C; f_{s_3}(0))$.
2. R parses $s_R = (\sigma_R, \sigma_{ZK}, s_2, \gamma_2, c_1, c_3)$. R runs $R_0(s_2, \sigma_R)$ to query $\pi(s_2)$ from S running $S_0(\pi, \sigma_S)$. R records the output $\overline{s}$.
3. R runs $P_{ZK}(\sigma_{ZK}, (s_2, \gamma_2))$ to prove to S running $V_{ZK}(\sigma_{ZK})$ that c_2 can be decommitted to s_2 using γ_2 and R queries for s_2. If V_{ZK} rejects, S aborts.

ith Execution phase: S on input $X_i = \{x_0^{i,j}, x_1^{i,j}\}_{j\in[n]}$, where $x_b^{i,j} \in \{0,1\}$ and private string s_S; R on private string s_R

1. S parses $s_S = (\sigma_S, \sigma_{ZK}, s_1, \gamma_1, s_3, \gamma_3, c_2)$. Let $C_i(s) = C_{i,X,s_1,c_2}(s)$ be a circuit that first computes $r = C(s, i)$, and if $r = (r_1, \ldots, r_n) \neq \perp$, outputs $((r_1, x_{r_1}^{i,1}), \ldots, (r_n, x_{r_n}^{i,n}))$; otherwise, outputs $\perp$. S computes $(G_i, \pi) = \mathsf{GC}(C_i; f_{s_3}(0), f_{s_3}(i))$ such that $f_{s_3}(0)$ is used for input wires (for consistency of π) and $f_{s_3}(i)$ is used for the rest. S sends G_i to R
2. R parses $s_R = (\sigma_R, \sigma_{ZK}, s_2, \gamma_2, c_1, c_3)$; S runs $P_{ZK}(\sigma_{ZK}, (s_1, s_3, \gamma_1, \gamma_3)))$ to prove to R running $V_{ZK}(\sigma_{ZK})$ that G_i is generated using s_1 and s_3, which decommitted to c_1 and c_3 using γ_1 and γ_3, respectively. R aborts if V_{ZK} rejects.
3. R outputs $\mathsf{GE}(G_i, \overline{s})$.

Fig. 4. UC-Secure Unbounded OT Protocol

Let $\mathcal{G} = (\mathsf{GC}, \mathsf{GE})$ be Yao's garbling circuit scheme where each gate and wire are encrypted. For a circuit C, let $(G, \pi) \leftarrow \mathsf{GC}(C)$ consist of a garbled circuit C and garbled input function π such that $\pi(i, x)$ is a garbled input for ith position input $x \in \{0,1\}$. Let $\mathsf{OT}_0 = (K_0, S_0, R_0)$ be a protocol for λ $\binom{2}{1}$OTs in the CR model. Let $\{f_s\}_{s\in\mathcal{S}}$ be a family of PRFs with seed space $\mathcal{S}$ and $f_s : \{0,1\}^{2\lambda} \to \{0,1\}^{p_1(\lambda)}$ for some polynomial p_1. The unbounded OT protocol construction, $\mathsf{OT}^{\mathsf{unbounded}}$, is provided in Figure 4. Each execution of $\mathsf{OT}^{\mathsf{unbounded}}$ gives $n = p_1(\lambda)$ $\frac{1}{2}$OTs similar to Beaver's, which can be turned into

$p_2(\lambda)$ $\binom{2}{1}$OT for a smaller polynomial p_2. A computational-bounded receiver can execute $\mathsf{OT}^{\mathsf{unbounded}}$ polynomially many times for any polynomial not known at construction time (as long as the polynomial is smaller than 2^λ).

Theorem 5. *Assuming OWFs, the protocol in Figure 4 is a UC-secure protocol computing unbounded number of OTs in the CR model.*

For a proof of the above theorem, please see the full version of this paper [9].

4.3 MPC in the OT-hybrid Model

Ishai *et al.* [34], construct a compiler that turns an MPC protocol that is secure against adversary corrupting less than half of the parties (honest majority) into a UC-secure MPC protocol in the OT-hybrid model. They apply this transformation to a variant of the MPC protocol from [18] to obtain the following:

Theorem 6 (Theorem 3 in [34]). *Assuming a PRG, for any $n \geq 2$, $\exists$ an n-party constant-round MPC protocol in the OT-hybrid model that is UC-secure against an active adversary adaptively corrupting at most $n-1$ parties.*

Combining this theorem with our UC-secure protocol for unbounded number of OTs in the CR model, we get the following corollary.

Corollary 1. *Assuming OWFs, for any $n \geq 2$, there exists an n-party constant-round MPC protocol in the CR model that is UC-secure against an active adversary adaptively corrupting at most $n-1$ parties.*

5 Corrupted Token Model

We consider a generalization of the Katz's tamper-proof token model [35] where tokens can be corrupted by adversaries even when they are created by honest parties. Our model is inspired by the real world application where honest users cannot create tokens themselves. They instead rely on a number of manufacturers, some of whom could be malicious. Thus, the secrets embedded in the token description can be revealed to the adversary. Furthermore, the adversary can replace the tokens with ones of its choice.

5.1 Katz's Stateless Tamper-Proof Token Functionality $\mathcal{F}_{\mathsf{token}}$

Our model is based on the stateless version of Katz's tamper-proof token model [35]. In this model, each user can create a stateless token by sending its description to $\mathcal{F}_{\mathsf{token}}$. The token is tamper-proof in the sense that the receiver can only access it through $\mathcal{F}_{\mathsf{token}}$ functionality in a black-box manner. We consider the case of stateless tokens where the tokens do not keep information between each access and use the same random tape. Hence, without loss of generality, we can assume that the function computed by the token is deterministic. In this case, we may represent the function with a circuit.

Our protocol will UC-realize a variant of $\mathcal{F}_{\mathsf{token}}$, called $\mathcal{F}_{\mathsf{token}}^{\mathsf{abort}}$, in which the adversary is notified whenever a party creates a token and can choose to interrupt its delivery. The receiver will not receive the token, but will be notified with the special message $\mathsf{interrupted}$. In such a case, the receiver aborts the protocol. This (otherwise unavoidable) change can be avoided by restricting the adversary to corrupt less than half of the corruptible tokens, which will allow the receiver to compute the output using the remaining uncorrupted tokens, but will weaken the threshold of corruptions tolerated. For formal descriptions of the two functionalities, please see the full version of this paper [9].

5.2 Corruptible Tamper-Proof Token Functionality $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$

We generalize the tamper-proof token model to accommodate such a scenario by allowing an adversary to corrupt each token upon its creation. We define corruptible tamper-proof token functionality $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$ in Figure 5 by modifying $\mathcal{F}_{\mathsf{token}}$ as follows. Every time a user sends create command to the functionality $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$, it first notifies the adversary and waits for one of two possible responses. The adversary may choose to learn the description of the token, and replace it with another (possibly stateful) token of its choice. We call the token chosen by the adversary a *corrupted* token. Alternately, the adversary may ignore the creation of that token, and therefore, that token creation is completed successfully and in this case, the adversary will not learn the description of the token. After uncorrupted tokens are created, they are tamper-proof in the same sense as in Katz's model. The stateful program for the corrupted token can be represented by a Turing machine.

In the case that the adversary chooses not to corrupt any token created by honest users, our model is identical to the model of Katz. Thus, our model generalizes the standard tamper-proof token model. We show that we can achieve UC-secure 2PC/MPC in the corrupted token model allowing the adversary to corrupt one party and all but one token generated by every honest party.

6 A Compiler to the Corrupted Token Model

6.1 Protocol for Corruptible Tokens

In this section, we describe a multi-party protocol that the n corruptible tokens will run in order to emulate the Katz' stateless token functionality.

Let $(K_{srZK}, P_{srZK}, V_{srZK})$ be a simultaneous resettable ZK argument in the correlated randomness model with straight-line simulator. Let $\mathcal{S} = (\mathsf{share}, \mathsf{recon})$ be an n out of n secret sharing scheme. Let Γ_0 be a UC-secure MPC protocol in the CR model for functionality $\mathcal{F}$ described in Figure 6.

We define a multi-party protocol $\Gamma = \Gamma(\Pi)$ on input $(x_1, \ldots, x_n)$ to compute $\Pi(x)$ when $x = x_i$ for all $i \in [n]$ in Figure 7.

$\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$

Upon receiving $(\mathsf{create}, \mathsf{sid}, P_j, \Pi)$ from P_i with $i \neq j$:

1. If there is no tuple of the form $(\mathsf{sid}, P_i, P_j, \star, \star)$, store $(\mathsf{sid}, P_i, P_j, \Pi, \mathsf{creating})$.
2. Send $(\mathsf{create}, \mathsf{sid}, P_i, P_j)$ to Adv.

Upon receiving $(\mathsf{corrupt}, \mathsf{sid}, P_i, P_j)$ from Adv:

1. Find the stored tuple $(\mathsf{sid}, P_j, P_i, \Pi, \mathsf{creating})$. If no such tuple exists, abort.
2. Send Π to Adv.

Upon receiving $(\mathsf{replace}, \mathsf{sid}, P_i, P_j, \Pi^*, \mathsf{state}_0)$ from Adv:

1. Find and remove the unique stored tuple $(\mathsf{sid}, P_j, P_i, \Pi, \mathsf{creating})$. If no such tuple exists, abort.
2. Store $(\mathsf{sid}, P_i, P_j, \Pi^*, \mathsf{state}_0)$, send $(\mathsf{done}, \mathsf{sid})$ to P_i, send $(\mathsf{create}, \mathsf{sid}, P_i)$ to P_j.

Upon receiving $(\mathsf{notcorrupt}, \mathsf{sid}, P_i, P_j)$ from Adv:

1. Find and remove the unique stored tuple $(\mathsf{sid}, P_j, P_i, \Pi, \mathsf{creating})$. If no such tuple exists, abort.
2. Store $(\mathsf{sid}, P_i, P_j, \Pi, \bot)$, send $(\mathsf{done}, \mathsf{sid})$ to P_i and send $(\mathsf{create}, \mathsf{sid}, P_i)$ to P_j.

Upon receiving $(\mathsf{execute}, \mathsf{sid}, P_i, \mathit{inp})$ from P_j with $i \neq j$:

1. Find the stored tuple $(\mathsf{sid}, P_i, P_j, \Pi, \mathsf{state})$. If no such tuple exists, abort.
2. Run $\Pi(\mathsf{state}, \mathit{inp})$ and let $(\mathsf{state}', \mathit{out})$ be the output. If $\mathsf{state} \neq \bot$, set $\mathsf{state} = \mathsf{state}'$.
3. Send $(\mathsf{sid}, \mathit{out})$ to P_j.

Upon receiving $(\mathsf{read}, \mathsf{sid}, P_i, P_j)$ from Adv:

1. Find the unique stored tuple $(\mathsf{sid}, P_j, P_i, P, \mathsf{state})$. If no such tuple exists, abort.
2. Send $(\mathsf{sid}, \mathsf{state})$ to Adv.

Fig. 5. Token Functionality $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$

6.2 Realizing a Tamper-Proof Token with Corruptible Tokens

Now we are ready to describe our protocol realizing the tamper-proof token with n corruptible tokens. To compute Π, the corruptible tokens are given the setup parameters for the MPC protocol $\Gamma(\Pi)$. Up on execution with input x_i, they will run $\Gamma(\Pi)$ to compute $\Pi(x)$ only if $x = x_i$ for all $i \in [n]$. We let Γ_i be the Turing machine computing messages Party P_i in Γ sends to other P_j, $j \in [n] \setminus \{i\}$ in each round of Γ. Since our token are stateless, Γ_i takes as input a state state_{k-1} which stores internal memory of P_i in round $k-1$ together with

$\mathcal{F}$

On input $((\Pi_1, x_1), \ldots, (\Pi_n, x_n))$

1. If $x_i \neq x_j$ for some $i \neq j$, output $\perp$. Otherwise, let x be the common input.
2. $\Pi = \mathsf{recon}(\Pi_1, \ldots, \Pi_n)$.
3. Output $\Pi(x)$.

Fig. 6. Function $\mathcal{F}$

$\Gamma(\Pi)$

Setup:

1. Let $(\Pi_1, \ldots, \Pi_n) \leftarrow \mathsf{share}(\Pi)$. Let $c_i = \mathsf{com}(\Pi_i)$ with decommitment information d_i for $i \in [n]$.
2. For $i \neq j \in [n]$, let $(\sigma_{i,j,P}, \sigma_{i,j,V}) \leftarrow K_{srZK}(1^\lambda)$ be the correlated randomness for the simultaneous resettable ZK argument with prover P_i and verifier P_j.
3. Let $(\sigma_1, \ldots, \sigma_n) \leftarrow \mathsf{SetUp}_{\Gamma_0}(1^\lambda)$ be the correlated randomness for Γ_0.
4. For $i \in [n]$, send $\Sigma_i = (\Pi_i, \sigma_i, c_i, d_i, \{c_j, \sigma_{i,j,P}, \sigma_{j,i,V}\}_{j \in [n] \setminus \{i\}})$ to Party P_i.

Execution: Party P_i on input x_i, correlated string Σ_i and a random tape $R_i = (s_i, r_i)$

1. For each $i \in [n]$, P_i commits to its input x_i and its PRF seed s_i using randomness $r_{i,x} = PRF_{s_i}(x_i)$ and r_i, respectively. P_i sends its *determining message* $M_i = (\mathsf{com}(x_i; r_{i,x}) || \mathsf{com}(s_i; r_i))$ *to all* P_j, $j \neq i$.
2. *For each* $i \in [n]$, P_i *computes* $R'_i = PRF_{s_i}(M_1 || \ldots || M_n)$ *consisting of* $R'_i[0]$ *for running* Γ_0 *and* $R'_i[1]$ *for running* (P_{srZK}, V_{srZK}).
3. *For each* $i \in [n]$, P_i *executes as the* i*th party in* Γ_0 *where* P_i *follows* k*th round message* $m_{i,k}$ *by running* P_{srZK} *to prove that there exists* $\alpha_i = (x_i, s_i)$ *and* Π_i *such that*
   (a) $M_i = (M_i[0], M_i[1])$ *where* $M_i[0]$ *can be decommitted to* x_i *and* $M_i[1]$ *can be decommitted to* s_i*;*
   (b) c_i *can be decommitted to* Π_i*;*
   (c) $m_{i,k}$ *is correctly computed using* $R'_i[0]$ *in* Γ_0 *with* (Π_i, x_i) *as an input where* $R'_i = PRF_{s_i}(M_1 || \ldots || M_n)$.

Fig. 7. Multi-party protocol $\Gamma(\Pi)$ computing Π

in which consists of all incoming messages P_i receives in round $k-1$. Γ_i outputs a new state state_k and outgoing messages for round k.

Formally, $\Gamma_i(\mathsf{state}_{k-1}, in_{k-1}) = (\mathsf{state}_k, out_k)$ where state_k is the internal state of P_i in round k and

- $in_{k-1} = \{m_{j,i,k-1}\}_{j\in[n]\setminus\{i\}}$ where $m_{j,i,k-1}$ is the incoming message from Party P_j to Party P_i in round $k-1$. $m_{j,i,k-1} = \perp$ if P_i does not receive a message from P_j in round $k-1$.
- $out_k = \{m_{i,j,k}\}_{j\in[n]\setminus\{i\}}$ where $m_{i,j,k}$ is the outgoing message from Party P_i to Party P_j in round k. $m_{i,j,k} = \perp$ if Party P_i does not send a message to Party P_j in round k.
- Let $\mathsf{state}_0 = \perp$ and in_0 be P_i's input for Γ.
- If P_i terminates at the end of round t, $\Gamma_i(\mathsf{state}_t, in_t) = (\mathsf{done}, output)$ where $output$ is P_i's output for Γ.

In order to protect Γ_i's state state_k when a token is sent to a malicious party, we use a symmetric key encryption scheme with a secret key embedded in the token to encrypt a state state before outputting. Let $\mathbb{S} = (\mathsf{SetUp}, \mathsf{Enc}, \mathsf{Dec})$ be a symmetric key encryption scheme. Let $\overline{\mathsf{state}}$ denote an encryption of state using $\mathbb{S}$. Let s_i consists of all information embedded in the ith token. Formally, we define $T_i = T(s_i)$ in Figure 8.

On input $(\mathsf{Initialize}, x_i)$

1. Parse $s_i = (i, sk_i, R_i, \Pi_i, \sigma_i, c_i, d_i, \{c_j, \sigma_{i,j,P}, \sigma_{j,i,V}\}_{j\in[n]\setminus\{i\}})$.
2. Initiate Γ_i on setup parameters $(\Pi_i, \sigma_i, c_i, d_i, \{c_j, \sigma_{i,j,P}, \sigma_{j,i,V})\}_{j\in[n]\setminus\{i\}})$, random tape R_i
3. Let $\Gamma_i(\perp, x_i) = (\mathsf{state}, out)$.
4. Output $(\mathsf{Enc}(sk_i, \mathsf{state}), out)$.

On input $(\overline{\mathsf{state}}, in)$

1. Parse $s_i = (i, sk_i, R_i, \Pi_i, \sigma_i, c_i, d_i, \{c_j, \sigma_{i,j,P}, \sigma_{j,i,V}\}_{j\in[n]\setminus\{i\}})$.
2. Initiate Γ_i on setup parameters $(\Pi_i, \sigma_i, c_i, d_i, \{c_j, \sigma_{i,j,P}, \sigma_{j,i,V})\}_{j\in[n]\setminus\{i\}})$, random tape R_i.
3. Decrypt $\mathsf{state} = \mathsf{Dec}(sk_i, \overline{\mathsf{state}})$, abort if fail.
4. Let $\Gamma_i(\mathsf{state}, in) = (\mathsf{state}', out)$
5. Output $(\mathsf{Enc}(sk_i, \mathsf{state}'), out)$.

Fig. 8. Token $T_i = T(s_i)$

Finally, protocol Λ in $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$-hybrid model realizing $\mathcal{F}_{\mathsf{token}}^{\mathsf{abort}}$ is in Figure 9.

6.3 Proof of Security

Let $\mathcal{S}_{srZK} = (\mathcal{S}_1, \mathcal{S}_2)$ be the straight-line simulator for the simultaneous resettable ZK, and Sim_{MPC} be the UC simulator for the UC-secure MPC.

Let Adv be an adversary corrupting up to $n-1$ tokens. Let n_c be the number of corrupted tokens, and $n_h = n - n_c$ be the number of honest (uncorrupted)

Λ

To create a token running Π for P_j, P_i does the following:

1. Generate the setup parameters for $\Gamma(\Pi)$: $(\Pi_k, \sigma_k, c_k, d_k, \{c_l, \sigma_{k,l,P}, \sigma_{l,k,V})\}_{l\in[n]})$ for $k \in [n]$ as defined in Figure 7.
2. Generate secret keys for decrypting share/state $sk_k \leftarrow \mathsf{KeyGen}(1^\lambda)$ for all $k \in [n]$.
3. Let $s_k = (k, sk_k, R_k, \Pi_k, \sigma_k, c_k, d_k, \{c_l, \sigma_{k,l,P}, \sigma_{l,k,V}\}_{l\in[n]})$.
4. Send $(\mathsf{create}, \mathsf{sid}_k, P_j, T_k)$ to $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$ where $T_k = T(s_k)$ for $k \in [n]$.

To execute a token running Π sent by P_i, P_j does the following:

1. For $k \in [n]$, initialize T_k by sending $(\mathsf{execute}, \mathsf{sid}_k, S, (\mathsf{initialize}, inp))$ to $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$ to compute $T_k(\mathsf{initialize}, inp) = (\overline{\mathsf{state}}_k, out_k)$.
2. While $\overline{\mathsf{state}}_k \neq \mathsf{done}$ for all $k \in [n]$, for $k \in [n]$
   (a) Parse $out_k = \{m_{k,l}\}_{l\neq k}$. Let $in_k = \{m_{l,k}\}_{l\neq k}$.
   (b) Send $(\mathsf{execute}, \mathsf{sid}_k, P_i, (\overline{\mathsf{state}}_k, in_k))$ to $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$ to compute $T_k(\overline{\mathsf{state}}_k, in_k) = (\overline{\mathsf{state}}'_k, out'_k)$.
   (c) Replace $\overline{\mathsf{state}}_k$ by $\overline{\mathsf{state}}'_k$ and out_k by out'_k.
3. Let $out = out_k$ for $k \in [n]$ such that $\overline{\mathsf{state}}_k = \mathsf{done}$.

Fig. 9. Protocol Λ in $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$-hybrid model UC realizing $\mathcal{F}_{\mathsf{token}}^{\mathsf{abort}}$

tokens. We construct a UC simulator Sim in Figure 10 internally running Adv such that any environment $\mathcal{E}$ cannot distinguish between interacting with Adv running Λ in the real world and interacting with Sim running $\mathcal{F}_{\mathsf{token}}^{\mathsf{abort}}$ in the ideal world. Now consider the series of hybrids:

Hybrid H_0: This hybrid is the real world execution.

Hybrid H_1: This hybrid is similar to H_0 except that every message to $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$ goes to Sim, and Sim acts honestly on behalf of $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$ while recording the messages. This hybrid is identical to H_0.

Let t be the maximum number of call from Adv to execute uncorrupted tokens. Let Hybrid $H_{2.0} = H_1$. For $k = 1, \ldots, t$

Hybrid $H_{2.k}$: This hybrid is similar to $H_{2.(k-1)}$ except that Sim records and replaces the kth encrypted state $\overline{\mathsf{state}}$ from uncorrupted T_l with $\overline{\mathsf{state}}^* = \mathsf{Enc}(sk_l, 0^{|\mathsf{state}|})$ before sending it to Adv and replaces $\overline{\mathsf{state}}^*$ with $\overline{\mathsf{state}}$ before applying T_l. Hybrid $H_{2.(k-1)}$ and $H_{2.k}$ are indistinguishable by the security of the symmetric key encryption $\mathbb{S}$.

Let Hybrid $H_{3.0} = H_{2.t}$. For $k = 1, \ldots, n_h \cdot n_c$,

Sim

Whenever Sim receives $(\mathsf{create}, \mathsf{sid}, P_i, P_j)$ from $\mathcal{F}_{\mathsf{token}}^{\mathsf{abort}}$, Sim does the followings:

1. For each $k \in [n]$, send $(\mathsf{create}, \mathsf{sid}_k, P_i, P_j)$ to Adv.
2. If Adv replies with $(\mathsf{corrupt}, \mathsf{sid}_k, P_i, P_j)$ for any $k \in [n]$ or P_j is corrupted,
   (a) Follow the protocol of Λ for creating a token, except that Sim uses zero string $0^{|\Pi|}$ instead of the actual token Π to create secret shares $\Pi_1, \ldots, \Pi_n$, and uses $\mathcal{S}_1$ to generate $(\sigma_{i,j,P}, \sigma_{i,j,V}, \tau_{i,j})$ instead of K_{srZK} and Sim_{MPC} to generate σ_i instead of $\mathsf{SetUp}_{\Gamma_0}$ for the setup parameters of Γ for the corruptible tokens. Sim stores the secret shares for later comparison.
   (b) Send T_k to Adv for each k Adv chose to corrupt.
   (c) Store $(\mathsf{replace}, \mathsf{sid}_k, P_i, P_j, T'_k, \mathsf{state}_k)$ from Adv.
   (d) Send $(\mathsf{interrupt}, \mathsf{sid}, P_i, P_j)$ to $\mathcal{F}_{\mathsf{token}}^{\mathsf{abort}}$.
3. Otherwise, send $(\mathsf{notinterrupt}, \mathsf{sid}, P_i, P_j)$ to $\mathcal{F}_{\mathsf{token}}^{\mathsf{abort}}$.

Whenever Adv runs the protocol for execution that involves both corrupted and uncorrupted tokens, Sim does the following:

1. Sim generates the Γ messages for uncorrupted T_k using $\mathcal{S}_2(\tau_k)$ and Sim_{MPC} as follows:
   (a) Sim generates and commits to α_k honestly as in Γ.
   (b) Sim runs Sim_{MPC} to generate messages for Γ_0.
   (c) Sim For each message generated by Sim_{MPC}, runs $\mathcal{S}_2(\tau_k)$ to generate messages for the following sim-res ZK argument.
   (d) When Sim_{MPC} queries the functionality of the function F on input $((\Pi'_1, x'_1), \ldots, (\Pi'_n, x'_n))$, if x'_k's are all equal to x', send $(\mathsf{execute}, \mathsf{sid}, P_i, x)$ to $\mathcal{F}_{\mathsf{token}}^{\mathsf{abort}}$ and passes the output to Sim_{MPC}. Otherwise, Sim aborts.
2. Sim records and replaces every encrypted state $\overline{\mathsf{state}}$ from uncorrupted T_k with $\overline{\mathsf{state}}^* = \mathsf{Enc}(sk_l, 0^{|\mathsf{state}|})$ before sending it to Adv and replaces $\overline{\mathsf{state}}^*$ with $\overline{\mathsf{state}}$ before applying T_k.
3. Sim records all inputs/outputs to the tokens. If Adv queries with the same input (state and incoming messages), Sim returns the recorded output (new state and outgoing messages).

Fig. 10. UC Simulator Sim for Λ

Hybrid $H_{3.k}$: This hybrid is similar to $H_{3.(k-1)}$ except that Sim uses $\mathcal{S}_1$ to generate $(\sigma_{i,j,P}, \sigma_{i,j,V}, \tau_{i,j})$ instead of K_{srZK} for honest token i and corrupted token j with $k = i(n_c - 1) + j$, and runs $\mathcal{S}_2(\tau_{i,j})$ to generate the sim-res ZK messages for token i by feeding the sim-res ZK messages from corrupted tokens. Sim records the transcript leading to each sim-res ZK session. By the GUC-security of the rZK, this hybrid is indistinguishable from H_1.

Lemma 7. *Hybrid $H_{3.(k-1)}$ and $H_{3.k}$ are indistinguishable.*

Proof. Suppose there exists a poly-time D that can distinguish $H_3.(k-1)$ and $H_3.k$ with non-negligible probability. We construct a distinguisher D' that can distinguish an interaction of P_{srZK} with a resetting verifier V^*_{srZK} and $\mathcal{S}_2(\tau_{i,j})$ for the sim-res ZK as follows. Given setup strings for the sim-res ZK, D' generates the setup for other pairs of tokens and the inputs for $\Gamma(\Pi)$. D' then runs $H_3.(k-1)$ or $H_3.k$ until Adv queries the honest token to prove a statement x using the sim-res ZK. D' runs the interaction and passes the messages from and to Adv as V^*_{srZK}'s messages. When V^*_{srZK} resets P_{srZK} or $\mathcal{S}_2(\tau_{i,j})$, D' queries the token using the saved state of the earlier round in the sim-res ZK. Finally, D' outputs the output of D. □

Claim. Fix a combined determining message $M = M_1||\ldots||M_n$, any polynomial-time resetting machine Adv can find only one transcript of Γ_0 in $\Gamma(\Pi)$ that every following sim-res ZK argument convinces the verifier to accept.

Proof. Suppose not. Let $tr = (\ldots, m_{i,k})$ and $tr' = (\ldots, m'_{i,k})$ be the partial transcripts of Γ_0 generated by Adv up to the differing messages $m_{i,k}, m'_{i,k}$ with accepting sim-res ZK argument. Note that we cannot have both $(c_i, M_i, M, tr), (c_i, M_i, M, tr') \in R_{rsZK}$. Otherwise, either M_i or c_i can be decommitted to two different values, and thus can be reduced to the security of the commitment scheme. Hence, either $(c_i, M_i, M, tr) \notin R_{rsZK}$ or $(c_i, M_i, M, tr') \notin R_{rsZK}$. Thus, we can construct a resetting prover P^*_{srZK} that can prove a false statement. □

Let Hybrid $H_{4.0} = H_{3.(n_h \cdot n_c)}$. Let m be the number of distinct sessions of Γ_0 based on combined determining message $M_1||\ldots||M_n$ generated through Adv querying the tokens. For $k = 1, \ldots, m$,

Hybrid $H_{4.k}$: This hybrid is similar to $H_{4.(k-1)}$ except that Sim runs Sim_{MPC} to generate the MPC messages for uncorrupted tokens by feeding the MPC messages from corrupted tokens in the execution of $\Gamma(\Pi)$ following kth combined determining message.

Lemma 8. *Hybrid $H_{4.(k-1)}$ and $H_{4.k}$ are indistinguishable.*

Proof. Suppose there exists a poly-time D that can distinguish $H_{4.(k-1)}$ and $H_{4.k}$ with non-negligible probability. We construct a distinguisher D' for Sim_{MPC} as follows. Given the correlated randomness for the MPC, D' generates the rest of the setup parameters for $\Sigma(\Pi)$ as in the experiment. D' then passes the MPC messages from Adv to D followed by the srZK messages from Sim_{ZK}. Since the accepting transcript is unique by the claim above, Adv cannot change the messages. D' outputs the output of D. □

Let Hybrid $H_{5.0} = H_{4.m}$. For $k = 1, \ldots, n$,

Hybrid $H_{5.k}$: This hybrid is similar to $H_{5.(k-1)}$ except that if the kth token is uncorrupted, Sim replaces the PRF in $\Gamma(\Pi)$ with truly random function F.

Lemma 9. *Hybrid $H_{5.(k-1)}$ and $H_{5.k}$ are indistinguishable.*

Proof. Suppose there exists a PPT distinguisher D that can distinguish $H_{5.(k-1)}$ and $H_{5.k}$ with non-negligible probability p. We construct a PPT D' that given function f, it runs $H_{5.(k-1)}$ and outputs the output of D when PRF_{s_i} is replaced by f. By the property of the PRF, p is negligible. □

Let Hybrid $H_{6.0} = H_{5.n}$. For $k = 1, \ldots, n$,

Hybrid $H_{6.k}$: This hybrid is similar to $H_{6.(k-1)}$ except that if the kth token is uncorrupted, Sim replaces the second half of the determining message M_i in $\Gamma(\Pi)$ with $\mathsf{com}(0^{|s_i|}; r_i)$ where s_i is the PRF seed in $\Gamma(\Pi)$.

Lemma 10. *Hybrid $H_{6.(k-1)}$ and $H_{6.k}$ are indistinguishable.*

Proof. Suppose there exists a PPT distinguisher D that can distinguish $H_{6.(k-1)}$ and $H_{6.k}$ with non-negligible probability p. We construct a PPT D' that given a commitment C of s_i or $0^{|s_i|}$, it runs $H_{6.(k-1)}$ or $H_{6.k}$ and outputs the output of D when the second half of M_i is replaced by C. Since s_i is not used as a witness nor as a PRF seed in $H_{6.(k-1)}$ or $H_{6.k}$, D' can generate the input for D. By the hiding property of com, p is negligible. □

Hybrid H_7: This is similar to $H_{6.n}$ except that Sim checks if inputs x_k, $k \in [n]$, are the same. If not, Sim records x_k's and replaces outputs of $\Gamma(\Pi)$ by $\perp$.

Lemma 11. *Hybrid $H_{6.n}$ and H_7 are indistinguishable.*

Proof. By the binding of com, Adv cannot find x'_k that $\mathsf{com}(x_k; r)$ (where r is an output of the truly random function f) decommitted to x_k except with negligible probability. In this case, by the soundness of rsZK, the output of $\Gamma(\Pi)$ is $\perp$. □

Hybrid H_8: This hybrid is similar to H_7 except that Sim passes token creation request from honest parties to $\mathcal{F}_{\mathsf{token}}^{\mathsf{abort}}$ and uses it to compute the output for Sim_{MPC}.

Lemma 12. *Hybrid H_7 and H_8 are indistinguishable.*

Proof. Note that if Adv generates messages for the MPC honestly using the same input x_i and the share Π_i given in the setup, then the output from $\mathcal{F}_{\mathsf{token}}^{\mathsf{abort}}$ must be the same as the output of the MPC by the correctness of the MPC. Suppose there exists a poly-time D that can distinguish H_3 and H_4 with non-negligible probability p. There must be at least one MPC message m^* from Adv that is not generated honestly. Thus, we construct a resetting prover P^*_{srZK} for the sim-res ZK argument following m^* by randomly choosing a Γ_0 message and passing the following prover messages to V. When Adv sends a different message using the same token state, P^*_{srZK} resets the verifier. It has at least $1/T$ probability of choosing m^* where T is the number of Γ_0 messages sent by Adv. Thus, it has at least p/T probability of proving a false statement, contradicting the resettable soundness of the sim-res ZK. □

Hybrid H_9: This hybrid is similar to H_8 except that Sim generates secret share of zero string $0^{|\Pi|}$ instead of the one received from an honest party.

Lemma 13. *Hybrid H_8 and H_9 are indistinguishable.*

Proof. Suppose there exists a poly-time D that can distinguish H_8 and H_9 with non-negligible probability. We construct a distinguisher D' for the secret sharing scheme $\mathcal{S}$ as follows. D' runs the experiment for D until it is given Adv shares consisting of less than n shares. D' then continues the experiment and D distinguishes between H_8 and H_9. Using the result of D, D' can distinguish between less than n shares of 0 and some program Π, contradicting the security of $\mathcal{S}$. □

Let Hybrid $H_{10.0} = H_9$. For $k = 1, \ldots, n$,

Hybrid $H_{10.k}$: This hybrid is similar to $H_{10.(k-1)}$ except that if the kth token is uncorrupted, Sim replaces the second half of the determining message M_i in $\Gamma(\Pi)$ with $\mathsf{com}(s_i; r_i)$ where s_i is the PRF seed in R_i. Hybrid $H_{10.(k-1)}$ and $H_{10.k}$ are indistinguishable by similar argument as Lemma 10.

Let Hybrid $H_{11.0} = H_{10.n}$. For $k = 1, \ldots, n$,

Hybrid $H_{11.k}$: This hybrid is similar to $H_{11.(k-1)}$ except that if the kth token is uncorrupted, Sim replaces the truly random function F in $\Gamma(\Pi)$ with PRF_{s_i}. Hybrid $H_{10.(k-1)}$ and $H_{10.k}$ are indistinguishable by similar argument as Lemma 9. This hybrid is the ideal world execution.

Using these, we prove our main theorem below.

Theorem 14. *Assuming an existence of OWFs, there exists a protocol with n corruptible tokens in $\mathcal{F}_{\mathsf{token}}^{\mathsf{corruptible}}$-hybrid model UC-realizing $\mathcal{F}_{\mathsf{token}}^{\mathsf{abort}}$.*

7 RAM Obfuscation and Tokens with Bounded Memory

RAM obfuscation. We now describe how to obtain program obfuscation with stateless hardware tokens solely from OWFs. This improves the assumption from the work of Nayak *et al.* [39], who additionally also assumed collision-resistant hash functions. At a very high level, the protocol of Nayak *et al.* makes use of OWFs and CRHFs. First, they make use of CRHFs for the authenticated ORAM structure. We observe that we can replace the authenticated ORAM used in Nayak *et al.* with an authenticated ORAM based on OWF (that can be built from the work of Ostrovsky and Goldreich, Ostrovsky). Next, in order to obtain a single starting seed for randomness that depends on the specific execution of the program and input, Nayak *et al.* require the user to first feed in a hash of the input to the token and then use this hash to derive all randomness (along with a unique program id). This gives them a unique execution id. We derive a unique value based on the input and program by having the user feed the input one-by-one to the token. Upon receiving one input, the token will authenticate it

and provide an authentication tag (this process is deterministic) that will then allow the user to input the next input. This process continues until the last input is inserted into the token, upon which the authentication tag produced at this stage is a unique id that can be used (in combination with the program id) to derive all randomness needed by the token for program execution. This process is similar in spirit to the GGM construction of deriving a PRF from a PRG.

7.1 High level description of the protocol

Program Authentication. At a high level, the program creation by the sender works as follows. Let the program to be obfuscated be $\mathsf{RAM} := (\mathsf{cpustate}, \mathsf{mem})$ where mem is a list of program instructions and $\mathsf{cpustate}$ is the initial cpu state. Let the program comprise of t instructions. The sender first creates the token containing a hardwired secret key K where $K := (K_e, K_{\text{prf}})$. K_e is used as the encryption key for encrypting state, K_{prf} is used as the key to a pseudorandom function used by the token to generate all randomness needed for executing the ORAM, creating ciphertexts, and so on. The sender creates a unique execution identity $\mathsf{id}_{\text{exec}}$, which is unique for every program created. The sender then encrypts $\mathsf{mem}||\mathsf{id}_{\text{exec}}||\mathsf{id}_{\text{instr}}$ (one instruction at a time) to obtain $\overline{\mathsf{mem}}$ ($\overline{\mathsf{mem}}_i$ denotes the ciphertext obtained upon encrypting $\mathsf{mem}_i||\mathsf{id}_{\text{exec}}||i$). The sender also computes a "tag" of the start ciphertext, $\overline{\mathsf{mem}}_1$, as $\tau_1 = \mathsf{PRF}_{K_{\text{prf}}}(\mathtt{start}, \overline{\mathsf{mem}}_1)$. The sender creates an encrypted program header $\overline{\mathsf{Header}} := \mathsf{Enc}_{K_e}(\mathsf{cpustate}, \mathsf{id}_{\text{exec}}, t)$. The receiver is sent $\overline{\mathsf{mem}}, \overline{\mathsf{mem}}_1^*$ and $\overline{\mathsf{Header}}$ as the obfuscated program.

Program Feed. At a very high level, the receiver will feed in the program, one instruction at a time, to the token, as follows:

1. As the first message, the token receives $(\mathtt{programauth}, 1, \overline{\mathsf{mem}}_1, \tau_1, \overline{\mathsf{mem}}_2, \overline{\mathsf{Header}})$. It will check that $\mathsf{PRF}_{K_{\text{prf}}}(\mathtt{start}, \overline{\mathsf{mem}}_1, \overline{\mathsf{Header}}) = \tau_1$ and output $\perp$ otherwise. Similarly, for all $2 \leq i < t-1$, it receives $(\mathtt{programauth}, i, \tau_{i-1}, \overline{\mathsf{mem}}_i, \tau_i, \overline{\mathsf{mem}}_{i+1}, \overline{\mathsf{Header}})$. It will check that $\mathsf{PRF}_{K_{\text{prf}}}(\tau_{i-1}, \overline{\mathsf{mem}}_i, \overline{\mathsf{Header}}) = \tau_i$ and output $\perp$ otherwise.
2. Next, it decrypts $\overline{\mathsf{mem}}_i$ and $\overline{\mathsf{mem}}_{i+1}$ to get mem_i and mem_{i+1}, and $\mathsf{id}_{\text{exec}}$ as well as decrypt $\overline{\mathsf{Header}}$ to get $\mathsf{id}_{\text{exec}}$ and t. It will check that $\mathsf{id}_{\text{instr}} = i$ and $i+1$ respectively (also that these values are $\leq t$) and that the two $\mathsf{id}_{\text{exec}}$ values are the same and equal to the $\mathsf{id}_{\text{exec}}$ value in $\overline{\mathsf{Header}}$. If these checks do not pass, it will respond with $\perp$. If the checks pass, the token will output $\tau_{i+1} = \mathsf{PRF}_{K_{\text{prf}}}(\tau_i, \overline{\mathsf{mem}}_{i+1}, \overline{\mathsf{Header}})$.

Input Feed. Let the input to the program be denoted by $x_1, \cdots, x_n$. The receiver will send the following instructions, step-by-step, for every input, to the token.

1. On input, $(\mathtt{inputauth}, 1, \tau_{t-1}, \overline{\mathsf{mem}}_t, \tau_t, x_1, n, \overline{\mathsf{Header}})$, it checks that $\mathsf{PRF}_{K_{\text{prf}}}(\tau_{t-1}, \overline{\mathsf{mem}}_t, \overline{\mathsf{Header}}) = \tau_t$, that $\overline{\mathsf{mem}}_t$ is the t^{th} program instruction (by decrypting $\overline{\mathsf{mem}}_t$ to get $\mathsf{id}_{\text{instr}}$ and $\overline{\mathsf{Header}}$ to get t and comparing) and output $\perp$ otherwise. It outputs $\tau_{t+1} = \mathsf{PRF}_{K_{\text{prf}}}(\tau_t, 1, x_1, n, \overline{\mathsf{Header}})$.

2. On input, $(\texttt{inputauth}, j, \tau_{t+j-2}, x_{j-1}, \tau_{t+j-1}, x_j, n, \overline{\mathsf{Header}})$, for $2 \leq j \leq n$, it checks that $\mathsf{PRF}_{K_{\text{prf}}}(\tau_{t+j-2}, j-1, x_{j-1}, n, \overline{\mathsf{Header}}) = \tau_{t+j-1}$ and outputs $\perp$ otherwise. It then outputs $\tau_{t+j} = \mathsf{PRF}_{K_{\text{prf}}}(\tau_{t+j-1}, j, x_j, n, \overline{\mathsf{Header}})$.

Program/Input ORAM Insertion. Once the program and input authentication is done, the program and input, henceforth collectively referred to as memory, must be inserted into the Authenticated Oblivious RAM structure. There are t program instructions and n inputs that must be inserted. Let $\ell = t + n$ be the total memory requirement of the program (we can assume this without loss of generality as any additional memory needed by the program can be thought of as dummy program instructions). First, a set of ℓ "zeroes" are inserted into the ORAM structure (i.e., the values of memory in all locations is set to 0)[8]. The insertion of a set of ℓ "zeroes" into the ORAM structure is done as follows:

1. For every memory location $1 \leq i \leq \ell$, the user prepares the message $(\texttt{ORAMsetup}, i, \ell, \tau_{i-1}^{\text{oraminit}}, n, x_n, \overline{\mathsf{Header}}, \tau_i^{\text{oraminit}}, \tau_\ell)$ and gives it to the token, with $\tau_1^{\text{oraminit}} = \tau_\ell$ and $\tau_0^{\text{oraminit}} = \tau_{\ell-1}$. The token checks that $\mathsf{PRF}_{K_{\text{prf}}}(\tau_0^{\text{oraminit}}, n, x_n, n, \overline{\mathsf{Header}}) = \tau_1^{\text{oraminit}}$ (for $i = 1$) and $\mathsf{PRF}_{K_{\text{prf}}}(\text{ORAMsetup}, i, \ell, \overline{\mathsf{Header}}, \tau_{i-1}^{\text{oraminit}}, \tau_\ell) = \tau_i^{\text{oraminit}}$ (for all other i) and outputs $\perp$ otherwise.
2. Otherwise, the token derives a key for the ORAM structure − this ORAM key is derived as $K_{\text{oram}} = \mathsf{PRF}_{K_{\text{prf}}}(\texttt{ORAMKey}, \tau_\ell)$.
   (a) It creates an ORAM initialization structure (that is, creates an initial random mapping of all virtual addresses to their real address); this initialization is done using randomness from the ORAM key K_{oram}.
   (b) In this map let address a_j have been mapped to address i. In this case, the token creates an authenticated encryption of $(a_j, 0)$ (again using keys and randomness derived from K_{oram}) to be inserted into the ORAM structure at virtual address i.
   (c) The token then outputs $\tau_{i+1}^{\text{oraminit}} = \mathsf{PRF}_{K_{\text{prf}}}(\text{ORAMsetup}, i, \ell, \overline{\mathsf{Header}}, \tau_i^{\text{oraminit}}, \tau_\ell)$.

Once all ℓ memory locations have been inserted with 0 values, the user then inserts the real input and program into the ORAM structure. This is done as follows: in the reverse order, starting with the n^{th} input to the first input, and then the t^{th} to the first program instruction. We now describe this process at a high level. For ease of exposition, we shall assume that every ORAM operation is a single step denoted as $\mathsf{oram}_{\sigma, K_{\text{oram}}}(i, v_i, \texttt{read/write}, \perp / v_i^*)$ (this can be easily extended to the case when the ORAM read/write is a set of operations, similar to Nayak *et al.* [39]). The protocol is as follows:

1. The user will insert the i^{th} memory location ($\ell \geq i \geq 1$, which is either an input or a program instruction) by sending the message $(\text{MemORAMInsert}, i, \ell, \tau_{2\ell-i}^{\text{oraminit}}, n, x_n, n, \overline{\mathsf{Header}}, \tau_{2\ell-i+1}^{\text{oraminit}}, \tau_i, \tau_{i-1}, w_i)$,

[8] Whenever, the state of the program (ORAM or otherwise) needs to be modified, this is done by appending encrypted `state` with $\overline{\mathsf{Header}}$ and then authenticating, similar to Nayak *et al.* [39]

where $w_i = (i-t, x_{i-t}, n)$ if the i^{th} location has an input (i.e., $\ell \geq i \geq t+1$) and $w_i = \overline{\mathsf{mem}}_i$ if the i^{th} location has a program instruction (i.e., $t \geq i \geq 1$).

2. If the i^{th} location has an input:
   (a) The token will check that $\tau_i = \mathsf{PRF}_{K_{\text{prf}}}(\tau_{i-1}, i-t, x_{i-t}, n, \overline{\mathsf{Header}})$ and that $\tau^{\text{oraminit}}_{2\ell-i+1} = \mathsf{PRF}_{K_{\text{prf}}}(\text{ORAMsetup}, i, \ell, \overline{\mathsf{Header}}, \tau^{\text{oraminit}}_{2\ell-i}, \tau_\ell)$.
   (b) The token will then execute the ORAM instruction $\mathsf{oram}_{\sigma,K_{\text{oram}}}(i, 0, \texttt{write}, x_{i-t})$.
   (c) The token then outputs $\tau^{\text{oraminit}}_{2\ell-i+2} = \mathsf{PRF}_{K_{\text{prf}}}(\text{ORAMsetup}, i-1, \ell, \overline{\mathsf{Header}}, \tau^{\text{oraminit}}_{2\ell-i+1}, \tau_\ell)$.
3. If the i^{th} location has a program instruction:
   (a) The token will check that $\tau_i = \mathsf{PRF}_{K_{\text{prf}}}(\tau_{i-1}, \overline{\mathsf{mem}}_i, \overline{\mathsf{Header}})$ and that $\tau^{\text{oraminit}}_{2\ell-i+1} = \mathsf{PRF}_{K_{\text{prf}}}(\text{ORAMsetup}, i, \ell, \overline{\mathsf{Header}}, \tau^{\text{oraminit}}_{2\ell-i}, \tau_\ell)$.
   (b) The token decrypts $\overline{\mathsf{mem}}_i$ to get $\mathsf{mem}_i||\mathsf{id}_{\text{exec}}||i$ and executes the ORAM instruction $\mathsf{oram}_{\sigma,K_{\text{oram}}}(i, 0, \texttt{write}, \mathsf{mem}_i||\mathsf{id}_{\text{exec}}||i)$.
   (c) The token then outputs $\tau^{\text{oraminit}}_{2\ell-i+2} = \mathsf{PRF}_{K_{\text{prf}}}(\text{ORAMsetup}, i-1, \ell, \overline{\mathsf{Header}}, \tau^{\text{oraminit}}_{2\ell-i+1}, \tau_\ell)$.

Program Execution. The program execution is similar to Nayak *et al.* [39].

8 Tokens with Small Memory

We consider a variant of $\mathcal{F}^{\mathsf{corruptible}}_{\mathsf{token}}$ in Figure 5, called $\mathcal{F}^{\mathsf{corruptible,short},L_1,L_2}_{\mathsf{token}}$ where create and execute only take Π and *inp* of short size. We also allow a token sender to send a message along with the token created through the functionality. This allows the adversary to intercept the message when it chooses to corrupt a token without neither sender nor receiver knowledge. This is unavoidable as we represent a token in the standard corruptible model with both a token and an additional auxiliary string from the sender. We use $\mathcal{F}^{\mathsf{corruptible,short}}_{\mathsf{token}}$ when L_1 and L_2 are clear from the context.

In theory, we would like L_1 and L_2 be of constant size in security parameter. Though [39] suggests using logarithmic size in practice for better performance. We define an implementation Token of $\mathcal{F}^{\mathsf{corruptible}}_{\mathsf{token}}$ in $\mathcal{F}^{\mathsf{corruptible,short}}_{\mathsf{token}}$-hybrid model and prove the following theorem in the full version of this paper [9].

Theorem 15. *The protocol* Token *UC-realizes* $\mathcal{F}^{\mathsf{corruptible}}_{\mathsf{token}}$ *in* $\mathcal{F}^{\mathsf{corruptible,short}}_{\mathsf{token}}$*-hybrid model.*

Combining the above result with the result in Section 6 gives:

Corollary 2. *Assuming OWFs, there exists a protocol that UC realizes* $\mathcal{F}^{\mathsf{abort}}_{\mathsf{token}}$ *functionality in* $\mathcal{F}^{\mathsf{corruptible,short}}_{\mathsf{token}}$*-hybrid model using n corruptible tokens with short inputs and small size against an adversary corrupting up to* $n-1$ *tokens.*

References

1. S. Agrawal, V. Goyal, A. Jain, M. Prabhakaran, and A. Sahai. New impossibility results for concurrent composition and a non-interactive completeness theorem for secure computation. In *CRYPTO 2012* , pages 443–460, 2012.
2. G. Ateniese, A. Kiayias, B. Magri, Y. Tselekounis, and D. Venturi. Secure outsourcing of circuit manufacturing. In *ProvSec* 2018.
3. B. Barak, O. Goldreich, S. Goldwasser, and Y. Lindell. Resettably-sound zero-knowledge and its applications. In *FOCS '02*, pages 116–125, 2001.
4. B. Barak, M. Prabhakaran, and A. Sahai. Concurrent non-malleable zero knowledge. In *FOCS '06*, pages 345–354, 2006.
5. S. Badrinarayanan, A. Jain, R. Ostrovsky, and I. Visconti. Non-interactive secure computation from one-way functions. In *ASIACRYPT 2018*, volume 11274 of *LNCS*, pages 118–138. Springer, 2018.
6. D. Beaver. Precomputing oblivious transfer. *CRYPTO '95*, pages 97–109, 1995.
7. D. Beaver. Correlated pseudorandomness and the complexity of private computations. In *STOC '96*, pages 479–488. ACM, 1996.
8. R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS '01*, pages 136–145. IEEE, 2001.
9. N. Chandran, W. Chongchitmate, R. Ostrovsky, and I. Visconti. Universally composable secure computation with corrupted tokens. In *Cryptology ePrint Archive*, Report 2017/1092. 2017.
10. R. Canetti, Y. Dodis, R. Pass, and S. Walfish. Universally composable security with global setup. In *TCC '07*, pages 61–85. Springer, 2007.
11. R. Canetti and M. Fischlin. Universally composable commitments. In *Crypto '01*, pages 19–40. Springer, 2001.
12. R. Canetti, O. Goldreich, S. Goldwasser, and S. Micali. Resettable zero-knowledge (extended abstract). In *STOC '00*, pages 235–244, 2000.
13. R. Canetti, E. Kushilevitz, and Y. Lindell. On the limitations of universally composable two-party computation without set-up assumptions. *Journal of Cryptology*, 19(2):135–167, 2006.
14. N. Chandran, V. Goyal, and A. Sahai. New constructions for uc secure computation using tamper-proof hardware. In *Eurocrypt '08*, pages 545–562. 2008.
15. S. G. Choi, J. Katz, D. Schröder, A. Yerukhimovich, and H.-S. Zhou. (efficient) universally composable oblivious transfer using a minimal number of stateless tokens. In *TCC '14*, pages 638–662. Springer, 2014.
16. K.-M. Chung, R. Ostrovsky, R. Pass, and I. Visconti. Simultaneous resettability from one-way functions. In *FOCS '13*, pages 60–69. IEEE, 2013.
17. D. Dachman-Soled, T. Malkin, M. Raykova, and M. Venkitasubramaniam. Adaptive and concurrent secure computation from new adaptive, non-malleable commitments. In *ASIACRYPT '13*, pages 316–336. Springer, 2013.
18. I. Damgård and Y. Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. In *CRYPTO '05*, pages 378–394. Springer, 2005.
19. A. De Santis, G. Di Crescenzo, R. Ostrovsky, G. Persiano, and A. Sahai. Robust non-interactive zero knowledge. In *CRYPTO '01*, pages 566–598. Springer, 2001.
20. N. Döttling, D. Kraschewski, J. Müller-Quade, and T. Nilges. General statistically secure computation with bounded-resettable hardware tokens. In *TCC (1)*, pages 319–344, 2015.
21. S. Dziembowski, S. Faust, and F.-X. Standaert. Private circuits iii: Hardware trojan-resilience via testing amplification. In *CCS '16*, pages 142–153. ACM, 2016.

22. U. Feige and A. Shamir. Witness indistinguishable and witness hiding protocols. In *STOC '90*, pages 416–426, 1990.
23. M. Fischlin, B. Pinkas, A. Sadeghi, T. Schneider, and I. Visconti. Secure set intersection with untrusted hardware tokens. In *Topics in Cryptology - CT-RSA 2011*, volume 6558 of *LNCS*, pages 1–16. Springer, 2011.
24. J. A. Garay, P. MacKenzie, and K. Yang. Strengthening zero-knowledge protocols using signatures. In *Eurocrypt '03*, volume 2656, pages 177–194. Springer, 2003.
25. S. Garg, A. Kumarasubramanian, R. Ostrovsky, and I. Visconti. Impossibility results for static input secure computation. In *CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 424–442. Springer, 2012.
26. O. Goldreich, S. Goldwasser, and S. Micali. How to Construct Random Functions In *Journal of the ACM*, 33(4):792-807, 1986.
27. O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In *STOC '87*, pages 218–229, 1987.
28. S. Goldwasser and S. Micali. Probabilistic encryption. *J. Comput. Syst. Sci.*, 28(2):270–299, 1984.
29. V. Goyal, Y. Ishai, A. Sahai, R. Venkatesan, and A. Wadia. Founding cryptography on tamper-proof hardware tokens. In *TCC '10*, pages 308–326. 2010.
30. J. Groth and R. Ostrovsky. Cryptography in the multi-string model. In *CRYPTO '07*, pages 323–341, 2007. Springer-Verlag.
31. C. Hazay, A. Polychroniadou, and M. Venkitasubramaniam. Composable security in the tamper-proof hardware model under minimal complexity. In *TCC '16*, pages 367–399. Springer, 2016.
32. D. Hofheinz, J. Müller-Quade, and D. Unruh. Universally composable zero-knowledge arguments and commitments from signature cards. In *5th Central European Conference on Cryptology*, 2005.
33. Y. Ishai, E. Kushilevitz, S. Meldgaard, C. Orlandi, and A. Paskin-Cherniavsky. On the power of correlated randomness in secure computation. In *TCC'13*, pages 600–620. Springer, 2013.
34. Y. Ishai, M. Prabhakaran, and A. Sahai. Founding cryptography on oblivious transfer–efficiently. *CRYPTO '08*, 5157:572–592, 2008.
35. J. Katz. Universally composable multi-party computation using tamper-proof hardware. In *EUROCRYPT '07*, pages 115–128. Springer, 2007.
36. H. Lin, R. Pass, and M. Venkitasubramaniam. A unified framework for concurrent security: universal composability from stand-alone non-malleability. In *STOC '09*, pages 179–188. ACM, 2009.
37. P. MacKenzie and K. Yang. On simulation-sound trapdoor commitments. In *EUROCRYPT '04*, pages 382–400. Springer, 2004.
38. V. Mavroudis, A. Cerulli, P. Svenda, D. Cvrcek, D. Klinec and G. Danezis. A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components. In *CCS '17*, pages 1583–1600. ACM, 2017.
39. K. Nayak, C. W. Fletcher, L. Ren, N. Chandran, S. Lokam, E. Shi, and V. Goyal. Hop: Hardware makes obfuscation practical. In *NDSS '17*, 2017.