Reusing Tamper-Proof Hardware in UC-Secure Protocols

Jeremias Mechler[1](✉), Jörn Müller-Quade[1], and Tobias Nilges[2]

[1] Karlsruhe Institute of Technology, Karlsruhe, Germany
jeremias.mechler@kit.edu
[2] Aarhus University, Aarhus, Denmark

Abstract. Universally composable protocols provide security even in highly complex environments like the Internet. Without setup assumptions, however, UC-secure realizations of cryptographic tasks are impossible. Tamper-proof hardware tokens, e.g. smart cards and USB tokens, can be used for this purpose. Apart from the fact that they are widely available, they are also cheap to manufacture and well understood.

Currently considered protocols, however, suffer from two major drawbacks that impede their practical realization:

– The functionality of the tokens is protocol-specific, i.e. each protocol requires a token functionality tailored to its need.
– Different protocols cannot reuse the same token even if they require the same functionality from the token, because this would render the protocols insecure in current models of tamper-proof hardware.

In this paper we address these problems. First and foremost, we propose formalizations of tamper-proof hardware as an *untrusted* and *global* setup assumption. Modeling the token as a global setup naturally allows to reuse the tokens for arbitrary protocols. Concerning a versatile token functionality we choose a simple *signature* functionality, i.e. the tokens can be instantiated with currently available signature cards. Based on this we present solutions for a large class of cryptographic tasks.

Keywords: Universal Composability · Tamper-proof hardware
Unique signatures · Global setup

1 Introduction

In 2001, Canetti [5] proposed the *Universal Composability (UC)* framework. Protocols proven secure in this framework have strong security guarantees for protocol composition, i.e. the parallel or interleaved execution of protocols. Subsequently, it was shown that it is not possible to construct protocols in this strict framework without additional assumptions [7]. Typical setup assumptions like a common reference string or a public key infrastructure assume a *trusted* setup.

T. Nilges—Supported by the European Union's Horizon 2020 research and innovation programme under grant agreement #669255 (MPCPRO).

Katz [33] on the other hand put forward the idea that protocol parties create and exchange *untrusted* tamper-proof hardware tokens, i.e. the tokens may be programmed maliciously by the sending party.

Katz' proposal spawned a line of research that focuses mainly on the feasibility of UC-secure two-party computation. First, stateful tamper-proof hardware was considered [14,17,24,26,33,38], then weaker models of tamper-proof hardware, where the hardware token cannot reliably keep a state, i.e. the receiver can reset the token [11,12,15,18–20,25–28,34].

Common to all of the aforementioned results is the fact that each protocol requires a token functionality that is tailored to the protocol. From a practical point of view it seems unlikely that these tokens will ever be produced by hardware vendors, and software implementations on standard smart cards are far too inefficient. Another negative side effect of protocol-specific tokens is that users need to keep at least one token for each application, which is prohibitive in practice.

We would therefore like to be able to use widely available standard hardware for our protocols. Examples are signature cards, where the token functionality is a simple signature functionality. The signing key is securely stored inside the tamper-proof hardware, while the verification key can be requested from the card. These cards are not required to keep an internal state (the keys can be hardwired). As an alternative several works in the literature discuss bit-oblivious transfer (OT) tokens as a very simple and cheap functionality [2,26,31]. However, there are no standardized implementations of such tokens, while signature tokens are standardized and already deployed.

As it turns out, even if there were protocols that use a signature card as a setup assumption, it would not be possible to use the same token in a different protocol. This is due to the current definitions of tamper-proof hardware in the UC model. To the best of our knowledge, reusing tamper-proof hardware was only considered by Hofheinz et al. [29], who introduce the concept of *catalysts*. In their model, they show that the setup can be used for multiple protocols, unlike a normal UC setup, but they assume a *trusted* setup.

A recent line of research, e.g. [4,8,10], has focused on efficient protocols based on a *globally available setup*. This stronger notion of UC security, called *Generalized UC (GUC)*, was introduced by Canetti et al. [6] and captures the fact that protocols are often more efficient if they can use the same setup. Indeed, a globally available token in the sense of GUC would naturally allow different protocols to use the same token. We note that the work of Chandran et al. [11] and subsequent works following the approach of requiring only black-box access to the token during simulation (e.g. [12,26]) might in principle be suitable for reuse, however none of these works consider this scenario and the problem of highly protocol-specific token functionalities is prevalent in all of these works.

1.1 Our Contribution

We apply the GUC methodology to resettable tamper-proof hardware and define the first global setup that is *untrusted*, in contrast to *trusted and incorruptible* setups like a global random oracle [8], key registration with knowledge [6] or trusted processors [40].

We present two models for reusable tamper-proof hardware:

- The first model is inspired by the work of [29] and generalizes their approach from trusted signature cards to generic and untrusted resettable tokens. It is also designed to model real world restrictions regarding concurrent access to e.g. a smart card. A real world analogy is an ATM that seizes the card for the duration of the cash withdrawal. During that time, the card cannot be used to sign a document. We want to highlight that this only limits the access to the tokens for a short time, it is still possible to run several protocols requiring the same token in an interleaved manner.
- The second model is a GUC definition of a resettable tamper-proof hardware token following the approach of [8], which is meant to give a GUC definition of reusable tamper-proof hardware. In particular, this means that there are no restrictions at all regarding access to the token.

We also consider a peculiarity of real world signature cards that is typically ignored in idealized descriptions. Most signature cards outsource some of the hashing of the message, which is usually needed in order to generate a signature, to the client. This is done to make the signature generation more efficient. We formally capture this in a new definition of signatures where the signing process is partitioned into a preprocessing and the actual signing. As we will show, cards that do outsource the hashing—even if only in part—cannot be used in all scenarios. Nevertheless, we show that a wide range of cryptographic functionalities can be realized, even if the card enforces preprocessing.

- UC-secure commitments in both models, even with outsourced hashing by the signature card. This means that all currently available signature cards can in principle be used with our protocols.
- UC-secure non-interactive secure computation (NISC) in the GUC model. Here it is essential that the hashing is performed on the card, i.e. not all signature cards are suitable for these protocols. This result establishes the minimal interaction required for (one-sided) two-party computation.

We show that the number of tokens sent is optimal, and that stateful tokens do not yield any advantage in the setting of globally available or reusable tokens.

1.2 Our Techniques

Modelling reusable hardware tokens. In the definition of the "realistic" model, a protocol is allowed to send a `seize` command to the token functionality, which will block all requests by other protocols to the token until it is released again via `release`. We have to make sure that messages cannot be exchanged between different protocols, thus the receiving party (of the signature, i.e. the sender of the signature card) has to choose a nonce. This nonce has to be included in the signature, thereby binding the message to a protocol instance. This obviously requires interaction, so non-interactive primitives cannot be realized in this model.

In order to explore the full feasibility of functionalities with reusable tokens and obtain more round-efficient protocols, we therefore propose a more idealized model following [8]. The simulator is given access to all "illegitimate" queries that are made to the token, so that all queries concerning a protocol (identified by a process ID PID), even from other protocols, can be observed. Essentially, this turns the token into a full-blown GUC functionality and removes the additional interaction from the protocols.

Commitments from signature cards. Concerning our protocols in the above described models, one of the main difficulties when trying to achieve UC security with hardware tokens is to make sure that the tokens cannot behave maliciously. In our case, this would mean that we have to verify that the signature was created correctly. Usually, e.g. in [20, 29], this is done via zero-knowledge proofs of knowledge, but the generic constructions that are available are highly inefficient. Instead, similar to Choi et al. [12], we use unique signatures. Unique signatures allow verification of the signature, but they also guarantee that the signature is subliminal-free, i.e. a malicious token cannot tunnel messages through the signatures.

Based on tokens with this unique signature functionality, we construct a straight-line extractable commitment. The main idea is to send the message to the token and obtain a signature on it. The simulator can observe this message and extract it. Due to the aforementioned partitioning of the signature algorithm on current smart cards, however, the simulator might only learn a hash value, which makes extraction impossible. We thus modify this approach and make it work in our setting. Basically, we keep the intermediate values sent to the token in the execution and use them as a seed for a PRG, which can in turn be used to mask the actual message. Since the simulator observes this seed, it can extract the message. However, the token can still abort depending on the input, so we also have to use randomness extraction on the seed, otherwise the sender of the token might learn some bits of the seed.

Using the straight-line-extractable commitment as a building block, we modify the UC commitment of [8] so that it works with signature cards.

Non-interactive witness-extractable arguments. A witness-extractable argument is basically a witness-indistinguishable argument of knowledge (WIAoK) with a straight-line extraction procedure. We construct such a non-interactive witness-extractable argument for later use in non-interactive secure computation (NISC). Our approach follows roughly the construction of Pass [39], albeit not in the random oracle model. [39] modify a traditional WIAoK by replacing the commitments with straight-line extractable ones. Further, they replace the application of a hash function to the transcript (i.e. the Fiat-Shamir heuristic) with queries to a random oracle. For our construction, we can basically use our previously constructed straight-line extractable commitments, but we also replace the queries to the random oracle by calls to the signature token, i.e. we can use the EUF-CMA security of the signature to ensure the soundness of the proof.

As hinted at above, this protocol requires the ideal model, since using a nonce would already require interaction. Also, there is a subtle technical issue when one tries to use signatures with preprocessing instead of the random oracle. In the reduction to the EUF-CMA security (where the reduction uses the signing oracle to simulate the token), it is essential that the commitments contain an (encoded) valid signature *before* they are sent to the token. However, if we use preprocessing, the preprocessed value does not provide the reduction with the commitments, which could in turn be extracted to reveal the valid signature and break the EUF-CMA security. Instead, it only obtains a useless preprocessed value, and once the reduction obtains the complete commitments via the non-interactive proof from the adversary, a valid call to the signature card on these commitments means that the adversary has a valid way to obtain a signature and the reduction does not go through. If the protocol were interactive, this would not be an issue, because we could force the adversary to first send the commitments and then provide a signature in a next step. But since the protocol is non-interactive, this does not work and we cannot use signature cards with preprocessing for this protocol. We believe this to be an interesting insight, since it highlights one of the differences in feasibility between idealized and practically available hardware.

1.3 Related Work

In an independent and concurrent work, using an analogous approach based on [8], Hazay et al. [27] recently introduced a GUC-variant of tamper-proof hardware to deal with the problem of adversarial token transfers in the multi-party case. This problem is equivalent to the problem of allowing the parties to reuse the token in different protocols without compromising security. Apart from using completely different techniques, however, [27] are only interested in the general feasibility of round-efficient protocols. In contrast, we would like to minimize the number of tokens that are sent. Additionally, [27] only consider the somewhat idealized GUC token functionality, and do not investigate a more realistic approach (cf. Sect. 3). This is an important aspect, in particular since our results indicate that some of the protocols in the idealized model cannot be realized in our more natural token model that is compatible with existing signature cards. Thus, from a more practical point of view, even the feasibility of generic 2PC is not conclusively resolved from existing results.

Table 1 gives a concise overview of our result compared with previous solutions based on resettable hardware that make black-box use of the token program in the UC security proof. Other approaches as shown in e.g. [17,18,20] are more efficient, but require the token code and therefore cannot be reused.

Generally, physically uncloneable functions (PUFs) also provide a fixed functionality, which has (assumed) statistical security. One could thus imagine using PUFs to realize reusable tokens. However, in the context of transferable setups

Table 1. Comparison of our result with existing solutions based on resettable hardware that technically allow reusing the tokens. All results mentioned above allow UC-secure 2PC, either directly or via generic completeness results.

	# Tokens	Rounds	Assumption	Token func.
[11]	2 (bidir.)	$\Theta(\kappa)$	eTDP	Specific for com.
[26]	$\Theta(\kappa)$ (bidir.)	$\Theta(1)$	CRHF[a]	Specific for OT
[12]	2 (bidir.)	$\Theta(1)$	VRF[b]	Specific for OT
[27]	$\Theta(\kappa^2)$ (bidir.)	$\Theta(1)$	OWF	Specific for OT
Ours (Sect. 3)	2 (bidir.)	$\Theta(1)$	Unique Sign.[c]	Generic
Ours (Sect. 4)	2 (bidir.)	$\Theta(1)$	Unique Sign./DDH[d]	Generic

[a] A protocol based on OWF is also shown, but the round complexity increases to $\Theta(\kappa/\log(\kappa))$. Additionally, it was shown by Hazay et al. [27] that there is a subtle error in the proof of the protocol.
[b] Verifiable random functions (VRFs) are only known from specific number-theoretic assumptions [32,35,37]. They also present a protocol with similar properties based on a CRHF, but the number of OTs is bounded in this case.
[c]Unique signatures are only known from specific number-theoretic assumptions and closely related to VRFs. These are required for our protocols.
[d]DDH is necessary for the NISC protocol.

(i.e. setups that do not disclose whether they have been passed on), Boureanu et al. [4] show that neither OT nor key exchange can be realized, and PUFs fall into the category of transferable setups. Tamper-proof hardware as defined in this paper on the other hand is not a transferable setup according to their definitions, so their impossibilities do not apply.

2 Preliminaries

2.1 UC Framework

We show our results in the generalized UC framework (GUC) of Canetti et al. [6]. Let us first briefly describe the basic UC framework [5], and then highlight the changes required for GUC. In UC, the security of a *real* protocol π is shown by comparing it to an *ideal* functionality $\mathcal{F}$. The ideal functionality is incorruptible and secure by definition. The protocol π is said to realize $\mathcal{F}$, if for any adversary $\mathcal{A}$ in the real protocol, there exists a simulator $\mathcal{S}$ in the ideal model that mimics the behavior of $\mathcal{A}$ in such a way that any environment $\mathcal{Z}$, which is plugged either to the ideal or the real model, cannot distinguish both.

In UC, the environment $\mathcal{Z}$ cannot run several protocols that share a state, e.g. via the same setup. In GUC, this restriction is removed. In particular, $\mathcal{Z}$ can query the setup independently of the current protocol execution, i.e. the simulator will not observe this query.

We will realize a UC-secure commitment. The ideal functionality $\mathcal{F}_{\mathrm{COM}}$ is defined in Fig. 1.

Functionality $\mathcal{F}_{\mathrm{COM}}$

Implicitly parametrized by a domain of secrets S.

Commit phase:

1. Await an input $(\texttt{commit}, s)$ with $s \in S$ from the sender. Store s, send $(\texttt{committed})$ to the adversary and ignore any further `commit`-messages.
2. Await a message $(\texttt{notify})$ from the adversary. Then send $(\texttt{committed})$ to the receiver.

Unveil phase:

3. Await an input $(\texttt{unveil}, \hat{s})$ with $\hat{s} \in S$ from the sender. Then, store $\hat{s}$ and send $(\texttt{opened})$ to the adversary.
4. Await a message $(\texttt{output})$ from the adversary. Then, if $\hat{s} = s$, send $(\texttt{opened}, \hat{s})$ to the receiver; otherwise, send a special reject message $\perp$.

Fig. 1. Ideal functionality for commitments.

2.2 Commitments

We need several types of commitment schemes. A commitment is a (possibly interactive) protocol between two parties and consists of two phases. In the commit phase, the sender commits to a value and sends the commitment to the receiver. The receiver must not learn the underlying value before the unveil phase, where the sender sends the unveil information to the receiver. The receiver can check the correctness of the commitment. A commitment must thus provide two security properties: a hiding property that prevents the receiver from extracting the input of the sender out of the commitment value, and a binding property that ensures that the sender cannot unveil a value other than the one he committed to.

Definition 1. *A* commitment scheme COM *between a sender* S *and a receiver* R *consists of two PPT algorithms* Commit *and* Open *with the following functionality.*

– Commit *takes as input a message s and computes a commitment c and unveil information d.*
– Open *takes as input a commitment c, unveil information d and a message s and outputs a bit $b \in \{0,1\}$.*

We require the commitment scheme to be correct, i.e. for all s:

$$\mathsf{Open}(\mathsf{Commit}(s), d, s) = 1$$

We assume the standard notions of statistical binding and computational hiding.

Further, we need extractable commitments. Extractabilty is a stronger form of the binding property which states that the sender is not only bound to one input, but that there also exists an (efficient) extraction algorithm that extracts this value. Our definition of extractable commitments is derived from Pass and Wee [41].

Definition 2. *We say that* $\mathsf{COM} = (\mathsf{Commit}, \mathsf{Open})$ *is* extractable*, if there exists an (expected) PPT algorithm* Ext *that, given black-box access to any malicious PPT algorithm* $\mathcal{A}_{\mathsf{S}}$*, outputs a pair* $(\hat{s}, \tau)$ *such that*

- *(simulation)* τ *is identically distributed to the view of* $\mathcal{A}_{\mathsf{S}}$ *at the end of interacting with an honest receiver* R *in the commit phase,*
- *(extraction) the probability that* τ *is accepting and* $\hat{s} = \perp$ *is negligible, and*
- *(binding) if* $\hat{s} \neq \perp$*, then it is infeasible to open* τ *to any value other than* $\hat{s}$*.*

Extractable commitments can be constructed from any commitment scheme via additional interaction, see e.g. [23,41]. The definition of extractable commitments implicitly allows the extractor to rewind the adversarial sender to extract the input. In some scenarios, especially in the context of concurrently secure protocols, it is necessary that the extractor can extract the input without rewinding. This is obviously impossible in the plain model, as a malicious receiver could employ the same strategy to extract the sender's input. Thus, some form of setup (e.g. tamper-proof hardware) is necessary to obtain straight-line extractable commitments.

Definition 3. *We say that* $\mathsf{COM} = (\mathsf{Commit}, \mathsf{Open})$ *is* straight-line extractable *if in addition to Definition 2, the extractor does not use rewinding.*

Another tool that we need is a trapdoor commitment scheme, where the sender can equivocate a commitment if he knows a trapdoor. We adapt a definition from Canetti et al. [8].

Definition 4. *A* trapdoor commitment scheme TCOM *between a sender* S *and a receiver* R *consists of five PPT algorithms* KeyGen, TVer, Commit, Equiv *and* Open *with the following functionality.*

- KeyGen *takes as input the security parameter and creates a key pair* $(\mathsf{pk}, \mathsf{sk})$*, where* sk *serves as the trapdoor.*
- TVer *takes as input* pk *and* sk *and outputs* 1 *iff* sk *is a valid trapdoor for* pk.
- Commit *takes as input a message* s *and computes a commitment* c *and unveil information* d*.*
- Equiv *takes as input the trapdoor* sk*, message* s'*, commitment* c*, unveil information* d *and outputs an unveil information* d' *for* s'*.*
- Open *takes as input a commitment* c*, unveil information* d *and a message* s *and outputs a bit* $b \in \{0, 1\}$*.*

The algorithm Equiv *has to satisfy the following condition. For every PPT algorithm* $\mathcal{A}_{\mathsf{R}}$*, the following distributions are computationally indistinguishable.*

– (pk, c, d, s), *where* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{A}_{\mathsf{R}}(1^\kappa)$ *such that* $\mathsf{TVer}(\mathsf{pk}, \mathsf{sk}) = 1$ *and* $(c, d) \leftarrow \mathsf{Commit}(\mathsf{pk}, s)$
– (pk, c', d', s), *where* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{A}_{\mathsf{R}}(1^\kappa)$ *such that* $\mathsf{TVer}(\mathsf{pk}, \mathsf{sk}) = 1$, $(c', z) \leftarrow \mathsf{Commit}(\mathsf{pk}, \cdot)$ *and* $d' \leftarrow \mathsf{Equiv}(\mathsf{sk}, s, c', z)$

For example, the commitment scheme by Pedersen [42] satisfies the above definition.

2.3 Witness-Indistinguishability

We construct a witness-indistiguishable argument of knowledge in this paper.

Definition 5. *A* witness-indistinguishable argument of knowledge system *for a language* $\mathcal{L} \in \mathcal{NP}$ *with witness relation* $\mathcal{R}_\mathcal{L}$ *consists of a pair of PPT algorithms* (P, V) *such that the following conditions hold.*

– *Completeness: For every* $(x, w) \in \mathcal{R}_\mathcal{L}$,

$$\Pr[\langle \mathsf{P}(w), \mathsf{V}\rangle(x) = 1] = 1.$$

– *Soundness: For every* $x \notin \mathcal{L}$ *and every malicious PPT prover* P^*,

$$\Pr[\langle \mathsf{P}^*, \mathsf{V}\rangle(x) = 1] \le \mathsf{negl}(|x|).$$

– *Witness-indistinguishability: For every* $w_1 \neq w_2$ *such that* $(x, w_1) \in \mathcal{R}_\mathcal{L}$, $(x, w_2) \in \mathcal{R}_\mathcal{L}$ *and every PPT verifier* V^*, *the distributions* $\{\langle \mathsf{P}(w_1), \mathsf{V}^*\rangle(x)\}$ *and* $\{\langle \mathsf{P}(w_2), \mathsf{V}^*\rangle(x)\}$ *are computationally indistinguishable.*
– *Proof of Knowledge: There exists an (expected) PPT algorithm* Ext *such that for every* $x \in \mathcal{L}$ *and every PPT algorithm* P^*, *there exists a negligible function* $\nu(\kappa)$ *such that* $\Pr[\mathsf{Ext}(x, \mathsf{P}^*) \in w_\mathcal{L}(x)] > \Pr[\langle \mathsf{P}^*, \mathsf{V}\rangle(x) = 1] - \nu(\kappa)$.

Witness-indistinguishable arguments/proofs of knowledge are also sometimes referred to as *witness-extractable*. Similar to the case of extractable commitments, one can also require the extractor to be straight-line, i.e. the extractor may not rewind the prover. Again, this requires an additional setup assumption and is not possible in the plain model.

Definition 6. *We say that a witness-indistinguishable argument/proof system is* straight-line witness-extractable *if in addition to Definition 5, the extractor does not use rewinding.*

2.4 Digital Signatures

A property of some digital signature schemes is the uniqueness of the signatures. Our definition is taken from Lysyanskaya [35]. Such schemes are known only from specific number theoretic assumptions.

Definition 7. *A* digital signature scheme SIG *consists of three PPT algorithms* KeyGen, Sign *and* Verify.

– $\mathsf{KeyGen}(1^\kappa)$ *takes as input the security parameter* κ *and generates a key pair consisting of a verification key* vk *and a signature key* sgk*.*
– $\mathsf{Sign}(\mathsf{sgk}, m)$ *takes as input a signature key* sgk *and a message* m*, and outputs a signature* σ *on* m*.*
– $\mathsf{Verify}(\mathsf{vk}, m, \sigma)$ *takes as input a verification key* vk*, a message* m *and a presumed signature* σ *on this message. It outputs 1 if the signature is correct and 0 otherwise.*

We require correctness, i.e. for all m *and* $(\mathsf{vk}, \mathsf{sgk}) \leftarrow \mathsf{KeyGen}(1^\kappa)$*:*

$$\mathsf{Verify}(\mathsf{vk}, m, \mathsf{Sign}(\mathsf{sgk}, m)) = 1.$$

A signature scheme is called unique *if the following property holds: There exists no tuple* $(\mathsf{vk}, m, \sigma_1, \sigma_2)$ *such that* $\mathsf{SIG.Verify}(\mathsf{vk}, m, \sigma_1) = 1$ *and* $\mathsf{SIG.Verify}(\mathsf{vk}, m, \sigma_2) = 1$ *with* $\sigma_1 \neq \sigma_2$*.*

We point out that in the above definition, vk, σ_1, and σ_2 need not be created honestly by the respective algorithms, but may be arbitrary strings.

3 Real Signature Tokens

It is our objective to instantiate the token functionality with a signature scheme. In order to allow currently available signature tokens to be used with our protocol, our formalization of a generalized signature scheme must take the peculiarities of real tokens into account.

One of the most important aspects regarding signature tokens is the fact that most tokens split the actual signing process into two parts: the first step is a (deterministic) preprocessing that usually computes a digest of the message. To improve efficiency, some tokens require this step to be done on the host system, at least in part. In a second step, this digest is signed on the token using the encapsulated signing key. In our case, this means that the *adversary contributes to computing the signature.* This has severe implications regarding the extraction in UC-secure protocols, because it is usually assumed that the simulator can extract the input from observing the query to the token.

To illustrate the problem, imagine a signature token that executes textbook RSA, and requires the host to compute the hash. A malicious host can *blind* his real input due to the homomorphic properties of RSA. Let (e, N) be the verification key and d the signature key for the RSA function. The adversary chooses a message m and computes the hash value $h(m)$ under the hash function h. Instead of sending $h(m)$ directly to the signature token, he chooses a random r, computes $h(m)' = h(m) \cdot r^e \mod N$ and sends $h(m)'$ to the token. The signature token computes $\sigma' = (h(m) \cdot r^e)^d = h(m)^d \cdot r \mod N$ and sends it to the adversary, who can multiply σ' by r^{-1} and obtain a valid signature σ on m. Obviously, demanding EUF-CMA for the signature scheme is not enough, because the signature is valid and the simulator is not able to extract m.

The protocols of [29] will be rendered insecure if the tokens perform *any kind* of preprocessing outside of the token, so the protocols cannot be realized with most of the currently available signature tokens (even if they are trusted). We aim to find an exact definition of the requirements, so that tokens which outsource part of the preprocessing can still be used in protocols. The following definition of a signature scheme with preprocessing thus covers a large class of currently available signature tokens and corresponding standards.

Definition 8. *(Digital signatures with preprocessing). A signature scheme* SIG *with preprocessing consists of five PPT algorithms* KeyGen, PreSg, Sign, Vfy *and* Verify.

- $\mathsf{KeyGen}(1^\kappa)$ *takes as input the security parameter* κ *and generates a key pair consisting of a verification key* vk *and a signature key* sgk.
- $\mathsf{PreSg}(\mathsf{vk}, m)$ *takes as input the verification key* vk*, the message* m *and outputs a deterministically preprocessed message* p *with* $|p| = n$.
- $\mathsf{Sign}(\mathsf{sgk}, p)$ *takes as input a signing key* sgk *and a preprocessed message* p *of fixed length* n*. It outputs a signature* σ *on the preprocessed message* p.
- $\mathsf{Vfy}(\mathsf{vk}, p, \sigma)$ *takes as input a verification key* vk*, a preprocessed message* p *and a presumed signature* σ *on this message. It outputs 1 if the signature is correct and 0 otherwise.*
- $\mathsf{Verify}(\mathsf{vk}, m, \sigma)$ *takes as input a verification key* vk*, a message* m *and a presumed signature* σ *on this message. It computes* $p \leftarrow \mathsf{PreSg}(\mathsf{vk}, m)$ *and then checks if* $\mathsf{Vfy}(\mathsf{vk}, p, \sigma) = 1$*. It outputs 1 if the check is passed and 0 otherwise.*

We assume that the scheme is correct, i.e. it must hold for all messages m *that*

$$\forall \kappa \in \mathbb{N}\ \forall (\mathsf{vk}, \mathsf{sgk}) \leftarrow \mathsf{KeyGen}(1^\kappa) : \mathsf{Verify}(\mathsf{vk}, m, \mathsf{Sign}(\mathsf{sgk}, \mathsf{PreSg}(\mathsf{vk}, m))) = 1.$$

Additionally, we require uniqueness according to Definition 7.

Existential unforgeability can be defined analogously to the definition for normal signature schemes. However, the EUF-CMA property has to hold for both $\mathsf{KeyGen}, \mathsf{Sign}$ and Vfy and $\mathsf{KeyGen}, \mathsf{Sign}$ and Verify. The PreSg algorithm is typically realized as a collision-resistant hash function.

All protocols in the following sections can be instantiated with currently available signature tokens that adhere the definition above. Tokens that completely outsource the computation of the message digest to the host do not satisfy this definition (because KeyGen, Sign and Vfy are not EUF-CMA secure).

The full version of this paper [36] contains an analysis for generic preprocessings, in the following we assume for simplicity that PreSg is the identity function.

3.1 Model

Our definition of reusable resettable tamper-proof hardware is defined analogously to normal resettable tamper-proof hardware tokens as in [20,26], but we add a mechanism that allows a protocol party to seize the hardware token. This approach is inspired by the work of Hofheinz et al. [29], with the difference that we consider untrusted tokens instead of a trusted signature token. While the token is seized, no other (sub-)protocol can use it. An adversarial sender can still store a malicious functionality in the wrapper, and an adversarial receiver is allowed to reset the program. The formal description of the wrapper $\mathcal{F}_{\text{wrap}}^{\text{ru-strict}}$ is given in Fig. 2.

We assume that the token receiver can verify that it obtained the correct token, e.g. by requesting some token identifier from the sender.

For completeness, we add the definition of a catalyst introduced by Hofheinz et al. [29].

Definition 9. *Let Π be a protocol realising the functionalities $\mathcal{F}$ and $\mathcal{C}$ in the $\mathcal{C}$-hybrid model. We say that $\mathcal{C}$ is used as a* catalyst *if Π realises $\mathcal{C}$ by simply relaying all requests and the respective answers directly to the ideal functionality $\mathcal{C}$.*

Functionality $\mathcal{F}_{\text{wrap}}^{\text{ru-strict}}$

Implicitly parametrized by a security parameter κ.

Creation:

1. Await an input ($\texttt{create}, \mathsf{M}, t$) from the token issuer, where M is a deterministic Turing machine and $t \in \mathbb{N}$. Store (M, t) and send ($\texttt{created}$) to the adversary. Ignore all further `create`-messages.
2. Await a message (`delivery`) from the adversary. Then, send (`ready`) to the token receiver.

Execution:

3. Await an input ($\texttt{run}, w, sid$) from the receiver. If no `create`-message has been sent, return a special symbol $\bot$. Otherwise, if $seized = sid$, run M on w from its most recent state. When M halts without generating output or t steps have passed, send $\bot$ to the receiver; otherwise store the current state of M and send the output of M to the receiver.
4. Await an input ($\texttt{seize}, sid$) from the receiver. If $seized = \bot$, set $seized = sid$.
5. Await an input (`release`) from the receiver. Set $seized = \bot$.

Reset (adversarial receiver only):

6. Upon receiving a message (`reset`) from a corrupted token receiver, reset M to its initial state.

Fig. 2. The wrapper functionality by which we model reusable resettable tamper-proof hardware. The runtime bound t is merely needed to prevent malicious token senders from providing a perpetually running program code M; it will be omitted throughout the rest of the paper.

In other words, the environment (and therefore other protocols) have access to the catalyst $\mathcal{C}$ while it is used in the protocol Π. In particular, this implies that the catalyst $\mathcal{C}$ cannot be simulated for a protocol. All in all, this notion is very similar to Definition 10.

3.2 UC-Secure Commitments

Straight-Line Extractable Commitment
We need a straight-line extractable commitment scheme in the $\mathcal{F}_{\text{wrap}}^{\text{ru-strict}}$-hybrid model to achieve two-party computation. We enhance a protocol due to Hofheinz et al. [29] which assumes trusted signature tokens as a setup such that it remains secure even with maliciously created signature tokens. Towards this goal, we adapt the idea of Choi et al. [12] to use unique signatures to our scenario. This is necessary, because verifying the functionality of an untrusted token is difficult. A unique signature scheme allows this verification very efficiently (compared to other measures such as typically inefficient ZK proofs). Additionally, it prevents the token from channeling information to the receiver of the signatures via subliminal channels.

Our protocol proceeds as follows. As a global setup, we assume that the commitment receiver has created a token containing a digital signature functionality, i.e. basically serving as a signature oracle. In a first step, the commitment receiver sends a nonce N to the sender such that the sender cannot use messages from other protocols involving the hardware token. The sender then draws a random value x. It ignores the precomputation step and sets the result p_x of this step to be x concatenated with the nonce N. The value p_x is sent to the token, which returns a signature. From the value p_x the sender derives the randomness for a one-time pad otp and randomness r for a commitment. Using r the sender commits to x, which will allow the extractor to verify if he correctly extracted the commitment. The sender also commits to the signature, x and N in a separate extractable commitment. To commit to the actual input s, the sender uses otp. Care has to be taken because a maliciously programmed signature card might leak some information about p_x to the receiver. Thus, the sender applies a 2-universal hash function before using it and sends all commitments and the blinded message to the receiver. To unveil, the sender has to send its inputs and random coins to the receiver, who can then validate the correctness of the commitments. A formal description of the protocol is shown in Fig. 3. We abuse the notation in that we define $(c, d) \leftarrow \mathsf{COM.Commit}(x)$ to denote that the commitment c was created with randomness d.

Theorem 1. *The protocol $\Pi_{\text{COM}}^{\text{se}}$ in Fig. 3 is a straight-line extractable commitment scheme as per Definition 3 in the $\mathcal{F}_{\text{wrap}}^{\text{ru-strict}}$-hybrid model, given that unique signatures exist, using $\mathcal{F}_{\text{wrap}}^{\text{ru-strict}}$ as a catalyst.*

Very briefly, extractability follows from the fact that the extractor can see all messages that were sent to the token, including the seed for the PRG that allows to extract the commitments c_s and c_x. Therefore, the extractor can just search through all messages that were sent until it finds the input that matches the commitment values. Hiding follows from the hiding property of the commitments and the pseudorandomness of the PRG. The randomness extraction with the 2-universal hash function prevents the token from leaking any information that might allow a receiver to learn some parts of the randomness of the commitments.

We split the proof into two lemmata, showing the computational hiding property of $\Pi^{\mathrm{se}}_{\mathrm{COM}}$ in Lemma 1 and the straight-line extraction in Lemma 2.

Lemma 1. *The protocol $\Pi^{\mathrm{se}}_{\mathrm{COM}}$ in Fig. 3 is computationally hiding, given that* COM *is an extractable computationally hiding commitment scheme, f is a linear 2-universal hash function,* PRG *is a pseudorandom generator and* SIG *is an EUF-CMA-secure unique signature scheme.*

Proof. Let us consider a modified commit phase of the protocol $\Pi^{\mathrm{se}}_{\mathrm{COM}}$: instead of committing to the values s, x, N, σ_x, the sender S inputs random values in the

Protocol $\Pi^{\mathrm{se}}_{\mathrm{COM}}$

Let $\mathcal{T}$ be an instance of $\mathcal{F}^{\text{ru-strict}}_{\text{wrap}}$ and PRG be a pseudorandom generator. Further let COM be a computationally hiding and extractable commitment scheme. Let SIG be a unique signature scheme according to Definition 8.

Global setup phase:

– Receiver: Compute $(\mathsf{vk}, \mathsf{sgk}) \leftarrow \mathsf{SIG.KeyGen}(1^\kappa)$. Program a stateless token T with the following functionality.
  - Upon receiving a message $(\mathtt{vk})$, return vk.
  - Upon receiving a message $(\mathtt{sign}, m)$, compute $\sigma_m \leftarrow \mathsf{SIG.Sign}(\mathsf{sgk}, m)$ and output σ_m.

  Send $(\mathtt{create}, \mathsf{T})$ to $\mathcal{T}$.

– Sender: Query $\mathcal{T}$ with $(\mathtt{vk})$ to obtain the verification key vk and check if it is a valid verification key for SIG.

Commit phase:

1. Receiver: Choose a nonce $N \leftarrow \{0,1\}^\kappa$ uniformly at random and send it to the sender.
2. Sender: Let s be the sender's input.
   – Draw $x \leftarrow \{0,1\}^{3\kappa}$ uniformly at random and choose a linear 2-universal hash function f from the family of linear 2-universal hash functions $\{f_h : \{0,1\}^{4\kappa} \to \{0,1\}^\kappa\}_{h \leftarrow \mathcal{H}}$.
   – Send $(\mathtt{seize})$ to $\mathcal{T}$. Set $p_x = x||N$ and send $(\mathtt{sign}, p_x)$ to $\mathcal{T}$ to obtain σ_x. Abort if $\mathsf{SIG.Vfy}(\mathsf{vk}, p_x, \sigma_x) \neq 1$.
   – Derive $(\mathsf{otp}, r) \leftarrow \mathsf{PRG}(f(p_x))$ with $|\mathsf{otp}| = |s|$ and compute $c_s = s \oplus \mathsf{otp}$, $(c_x, r) \leftarrow \mathsf{COM.Commit}(p_x)$ and $(c_\sigma, d_\sigma) \leftarrow \mathsf{COM.Commit}(\sigma_x, x, N)$.
   – Send (c_s, c_x, c_σ, f) to the receiver. Release $\mathcal{T}$ by sending $(\mathtt{release})$.

Unveil phase:

3. Sender: Send $(s, x, \sigma_x, d_\sigma)$ to the receiver.
4. Receiver: Set $p_x = x||N$ and compute $(\mathsf{otp}, r) \leftarrow \mathsf{PRG}(f(p_x))$. Check if $\mathsf{SIG.Vfy}(\mathsf{vk}, p_x, \sigma_x) = 1$, $\mathsf{COM.Open}(c_x, r, x) = 1$, $\mathsf{COM.Open}(c_\sigma, d_\sigma, (\sigma_x, x, N)) = 1$ and $c_s = s \oplus \mathsf{otp}$. If not, abort; otherwise accept.

Fig. 3. Computationally secure straight-line extractable commitment scheme in the $\mathcal{F}^{\text{ru-strict}}_{\text{wrap}}$-hybrid model.

commitments and replaces the generated pseudorandom string by a completely random string. Thus no information about the actual input remains. In the following, we will show that from the receiver's point of view, the real protocol and the modified protocol as described above are computationally indistinguishable. This implies that the commit phase of the protocol $\Pi^{\mathrm{se}}_{\mathrm{COM}}$ is computationally hiding. Consider the following series of hybrid experiments.

Experiment 0: The real protocol $\Pi^{\mathrm{se}}_{\mathrm{COM}}$.

Experiment 1: Identical to Experiment 0, except that instead of computing $(\mathsf{otp}, r) \leftarrow \mathsf{PRG}(f(p_x))$, draw a uniformly at random and compute $(\mathsf{otp}, r) \leftarrow \mathsf{PRG}(a)$.

Experiment 2: Identical to Experiment 1, except that instead of using $\mathsf{PRG}(a)$ to obtain otp and r, S draws otp and r uniformly at random.

Experiment 3: Identical to Experiment 2, except that instead of using COM to commit to (σ_x, x, N), S commits to a random string of the same length.

Experiment 4: Identical to Experiment 3, except that instead of using COM to commit to p_x with randomness r, S commits to a random string of the same length. This is the ideal protocol.

Experiments 0 and 1 are statistically close, given that f is a linear 2-universal hash function and SIG is unique. A malicious receiver $\mathcal{A}_{\mathsf{R}}$ provides a maliciously programmed token $\mathcal{T}^*$ which might help distinguish the two experiments. In particular, the token might hold a state and it could try to communicate with $\mathcal{A}_{\mathsf{R}}$ via two communication channels:

1. $\mathcal{T}^*$ can try to hide messages in the signatures.
2. $\mathcal{T}^*$ can abort depending on the input of S.

The first case is prevented by using a unique signature scheme. The sender S asks $\mathcal{T}^*$ for a verification key vk^* and can verify that this key has the correct form for the assumed signature scheme. Then the uniqueness property of the signature scheme states that each message has a unique signature. Furthermore, there exist no other verification keys such that a message has two different signatures. It was shown in [3] that unique signatures imply subliminal-free signatures. Summarized, given an adversary $\mathcal{A}_{\mathsf{R}}$ that can hide messages in the signatures, we can use this adversary to construct another adversary that can break the uniqueness property of the signature scheme.

The second case is a bit more involved. The main idea is to show that applying a 2-universal hash function to p_x generates a uniformly distributed value, even if R has some information about p_x. Since x is drawn uniformly at random from $\{0,1\}^{3\kappa}$, $\mathcal{T}^*$ can only abort depending on a logarithmic part of the input. Otherwise, the probability for the event that $\mathcal{T}^*$ aborts becomes negligible in κ (because the leakage function is fixed once the token is sent). Let X be the random variable describing inputs into the signature token and let Y describe the random variable representing the leakage. In the protocol, we apply $f \in \{f_h : \{0,1\}^{4\kappa} \rightarrow \{0,1\}^{\kappa}\}_{h \leftarrow \mathcal{H}}$ to X, which has at least min-entropy 3κ, ignoring the nonce N. Y has at most 2 possible outcomes, abort or proceed. Thus, [16] gives a lower bound for the average min-entropy of X given Y, namely

$$\tilde{H}_\infty(X|Y) \geq H_\infty(X) - H_\infty(Y) = 3\kappa - 1.$$

Note that f is chosen *after* R^* sent the token. This means that we can apply the Generalized Leftover Hash Lemma (cf. [16]):

$$\Delta((f_{\mathcal{H}}(X), H, Y); (U_k, H, Y)) \leq \frac{1}{2}\sqrt{2^{\tilde{H}_\infty(X|Y)} 2^\kappa} \leq \frac{1}{2}\sqrt{2^{-(3\kappa-1)+\kappa}} \leq 2^{-\kappa}$$

We conclude that from $\mathcal{A}_\mathsf{R}$'s view, $f(x)$ is distributed uniformly over $\{0,1\}^\kappa$ and thus Experiment 0 and Experiment 1 are statistically indistinguishable. We will only sketch the rest of the proof.

Computational indistinguishability of Experiments 1 and 2 follows directly from the pseudorandomness of PRG, i.e. given a receiver R^* that distinguishes both experiments, we can use this receiver to construct an adversary that distinguishes random from pseudorandom values. Experiment 2 and Experiment 3 are computationally indistinguishable given that COM is computationally hiding. From a distinguishing receiver R^* we can directly construct an adversary that breaks the hiding property of the commitment scheme. And by the exact same argumentation, Experiments 3 and 4 are computationally indistinguishable. □

We now show the straight-line extractability of $\Pi^{\text{se}}_{\text{COM}}$.

Lemma 2. *The protocol $\Pi^{\text{se}}_{\text{COM}}$ in Fig. 3 is straight-line extractable, given that* COM *is an extractable computationally hiding commitment scheme and* SIG *is an EUF-CMA-secure unique signature scheme.*

Proof. Consider the extraction algorithm in Fig. 4. It searches the inputs of $\mathcal{A}_\mathsf{S}$ into the hybrid functionality $\mathcal{F}^{\text{ru-strict}}_{\text{wrap}}$ for the combination of input and randomness for the commitment that is to be extracted.

Extractor $\mathsf{Ext}_{\mathsf{SEC}}$

Upon input $c^* = \big((c^*_s, c^*_x, c^*_\sigma, f^*), Q\big)$, where Q is the set of all queries that $\mathcal{A}_\mathsf{S}$ sent to $\mathcal{F}^{\text{ru-strict}}_{\text{wrap}}$, start the following algorithm.

1. For all $\alpha \in Q$, compute $(\hat{\mathsf{otp}}, \hat{r}) \leftarrow \mathsf{PRG}(f^*(\alpha))$ and test if $\mathsf{COM.Open}(c^*_x, \hat{r}, \alpha) = 1$. Otherwise, abort.
2. Let $(\hat{\mathsf{otp}}, \hat{r})$ be the values obtained in the previous step. Output $\hat{s} = c^*_s \oplus \hat{\mathsf{otp}}$.

Fig. 4. The extraction algorithm for the straight-line extractable commitment protocol $\Pi^{\text{se}}_{\text{COM}}$.

Let Q denote the set of inputs that $\mathcal{A}_\mathsf{S}$ sent to $\mathcal{F}^{\text{ru-strict}}_{\text{wrap}}$. Extraction will fail only in the event that a value x^* is unveiled that has never been sent to $\mathcal{T}$, i.e. $p^*_x \notin Q$. We have to show that $\mathsf{Ext}_{\mathsf{SEC}}$ extracts c^*_s with overwhelming probability, i.e. if the receiver accepts the commitment, an abort in Step 1 happens only with negligible probability.

Assume for the sake of contradiction that $\mathcal{A}_{\mathsf{S}}$ causes this event with non-negligible probability $\varepsilon(\kappa)$. We will use $\mathcal{A}_{\mathsf{S}}$ to construct an adversary $\mathcal{B}$ that breaks the EUF-CMA security of the signature scheme SIG with non-negligible probability. Let vk be the verification key that $\mathcal{B}$ receives from the EUF-CMA experiment. $\mathcal{B}$ simulates $\mathcal{F}_{\text{wrap}}^{\text{ru-strict}}$ for $\mathcal{A}_{\mathsf{S}}$ by returning vk upon receiving a query $(\mathtt{vk})$; further let Q be the set of queries that $\mathcal{A}_{\mathsf{S}}$ sends to $\mathcal{F}_{\text{wrap}}^{\text{ru-strict}}$. For each query $(\mathtt{sign}, m)$, $\mathcal{B}$ forwards the message to the signature oracle of the EUF-CMA game and returns the resulting signature σ to $\mathcal{A}_{\mathsf{S}}$.

$\mathcal{B}$ now simulates the interaction between $\mathcal{A}_{\mathsf{S}}$ and R up to the point when $\mathcal{A}_{\mathsf{S}}$ sends the message c_σ^*. The next messages between $\mathcal{A}_{\mathsf{S}}$ and R represent the interaction between an honest receiver and a malicious commitment sender $\mathcal{A}'_{\mathsf{S}}$ for the extractable commitment scheme COM. Thus, $\mathcal{B}$ constructs a malicious $\mathcal{A}'_{\mathsf{S}}$ from the state of $\mathcal{A}_{\mathsf{S}}$, which interacts with an external commitment receiver.

Due to the extractability of COM, there exists an extractor Ext that on input $(c_\sigma^*, \mathcal{A}'_{\mathsf{S}})$ outputs a message $(\hat{\sigma}_x, \hat{x}, \hat{N})$ except with negligible probability $\nu(\kappa)$. $\mathcal{B}$ runs Ext, sets $\hat{p}_x = \hat{x}||\hat{N}$ and outputs $(\hat{\sigma}_x, \hat{p}_x)$ to the EUF-CMA experiment and terminates.

From $\mathcal{A}_{\mathsf{S}}$'s view, the above simulation is distributed identically to the real protocol conditioned on the event that the unveil of the commitment c_σ succeeds. By assumption, $\mathcal{A}_{\mathsf{S}}$ succeeds in committing to a signature with non-negligible probability $\varepsilon(\kappa)$ in this case. It follows that the extractor Ext of COM will output a message $(\hat{\sigma}_x, \hat{x}, \hat{N})$ with non-negligible probability $\varepsilon(\kappa) - \nu(\kappa)$. Thus $\mathcal{B}$ will output a valid signature $\hat{\sigma}_x$ for a value $\hat{p}_x$ with non-negligible probability. However, it did not query the signature oracle on this value, which implies breaking the EUF-CMA security of the signature scheme SIG.

Thus, the extractor $\mathsf{Ext}_{\mathsf{SEC}}$ will correctly output the value s with overwhelming probability. □

Obtaining UC-Secure Commitments

In order to achieve computationally secure two-party computation, we want to transform the straight-line extractable commitment from Sect. 3.2 into a UC-secure commitment. A UC-secure commitment can be used to create a UC-secure CRS via a coin-toss (e.g. [20]). General feasibility results, e.g. [9], then imply two-party computation from this CRS.

One possibility to obtain a UC-secure commitment from our straight-line extractable commitment is to use the compiler of Damgård and Scafuro [15], which transforms any straight-line extractable commitment into a UC-secure commitment. The compiler provides an information-theoretic transformation, but this comes at the cost of requiring $O(\kappa)$ straight-line extractable commitments to commit to one bit only. If we use a signature token, this translates to many calls to the signature token and makes the protocol rather inefficient.

Instead, we adapt the UC commitment protocol of [8] to our model. The key insight in their protocol is that trapdoor extraction is sufficient to realize a UC-secure commitment. They propose to use a trapdoor commitment in conjunction with straight-line extractable commitments via a global random oracle to realize a UC-secure commitment. If we wanted to replace their commitments with our construction, we would encounter a subtle problem that we want to discuss here. In their compiler, the commitment sender first commits to his input via the trapdoor commitment scheme. Then, he queries the random oracle with his input (which is more or less equivalent to a straight-line extractable commitment) and the unveil information for the trapdoor commitment. In the security proof against a corrupted sender, the simulator has to extract the trapdoor commitment. Thus, in their case, the simulator just searches all queries to the random oracle for the correct unveil information. In our very strict model, if we replace the oracle call with our straight-line extractable commitments, this approach fails. At first sight, it seems possible to just use the extractor for the straight-line extractable commitment to learn the value. However, it is crucial for the proof of security against a corrupted receiver that the commitment value is never published. Without this value, however, the extraction procedure will not work. Further, while we can still see all queries that are made to the hardware token, the simulator does not (necessarily) learn the complete input, but rather a precomputed value for the signature. Therefore, a little more work is necessary in order to realize a UC-secure commitment in our model.

In essence, we can use the techniques of the straight-line extractable commitment from the previous section, although we have to enhance it at several points. First, we need to query the signature token twice, for both x and r, instead of deriving r from x via a PRG. This is necessary because all protocol steps have to be invertible in order to equivocate the commitment, and finding a preimage for a PRG is not efficiently possible. Second, we have to replace the extractable commitments by *extractable trapdoor* commitments[1].

The protocol proceeds as follows: First, the receiver chooses a trapdoor for the trapdoor commitment $\mathsf{TCOM}_{\mathsf{ext}}$ and commits to it via a straight-line extractable commitment. This ensures that the simulator against a corrupted receiver can extract the trapdoor and then equivocate the commitments of $\mathsf{TCOM}_{\mathsf{ext}}$. The sender then commits with $\mathsf{TCOM}_{\mathsf{ext}}$ to his input (in a similar fashion as in the straight-line extractable commitment) and uses the token to sign the unveil information. Against a corrupted sender, the simulator can thus extract the unveil information and thereby extract the commitment. The commitment is sent to the receiver, which concludes the commit phase. To unveil, the sender first commits to the unveil information of $\mathsf{TCOM}_{\mathsf{ext}}$ such that he cannot change his commitment when the receiver unveils the trapdoor in the next step. From there, the commitments are checked for validity and if everything checks out, the commitment is accepted. The formal description of our protocol is given in Fig. 5.

Theorem 2. *The protocol Π_{COM} in Fig. 5 computationally UC-realizes $\mathcal{F}_{\mathrm{COM}}$ (cf. Sect. 2.1) in the $\mathcal{F}_{\mathrm{wrap}}^{\text{ru-strict}}$-hybrid model, using $\mathcal{F}_{\mathrm{wrap}}^{\text{ru-strict}}$ as a catalyst, given that $\mathsf{TCOM}_{\mathsf{ext}}$ is an extractable trapdoor commitment, SECOM is a straight-line extractable commitment and SIG is an EUF-CMA-secure unique signature scheme.*

[1] Note that any commitment scheme can be made extractable (with rewinding) via an interactive protocol, e.g. [23,41].

Protocol Π_{COM}

Let $\mathsf{TCOM}_{\mathsf{ext}}$ be an extractable trapdoor commitment scheme and let SECOM be the straight-line extractable commitment from Section 3.2.

Global Setup phase:

- Sender and receiver: Compute $(\mathsf{vk}, \mathsf{sgk}) \leftarrow \mathsf{SIG.KeyGen}(1^\kappa)$. Program a stateless token $\mathsf{T_S}$ and $\mathsf{T_R}$, respectively, with the following functionality.
  - Upon receiving a message $(\mathtt{vk})$, return vk.
  - Upon receiving a message $(\mathtt{sign}, m)$, compute $\sigma_m \leftarrow \mathsf{SIG.Sign}(\mathsf{sgk}, m)$ and output σ_m.

  Send $(\mathtt{create}, \mathsf{T_S})$ to $\mathcal{T}_\mathsf{S}$ and $(\mathtt{create}, \mathsf{T_R})$ to $\mathcal{T}_\mathsf{R}$, respectively.
- Sender and receiver: Query $\mathcal{T}_\mathsf{S}$ and $\mathcal{T}_\mathsf{R}$, respectively, with $(\mathtt{vk})$ to obtain the verification key vk and check if it is a valid verification key for SIG.

Commit phase:

1. Receiver: Compute $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{TCOM}_{\mathsf{ext}}.\mathsf{KeyGen}(1^\kappa)$ and draw a nonce $N \leftarrow \{0,1\}^\kappa$. Further compute $(c_{\mathsf{sk}}, d_{\mathsf{sk}}) \leftarrow \mathsf{SECOM.Commit}(\mathsf{sk})$ and send $(\mathsf{pk}, c_{\mathsf{sk}}, N)$ to the sender.
2. Sender: Let s be the sender's input.
   - Draw $x, r \leftarrow \{0,1\}^{3\kappa}$ uniformly at random and choose a linear 2-universal hash function f from the family of linear 2-universal hash functions $\{f_h : \{0,1\}^{4\kappa} \rightarrow \{0,1\}^\kappa\}_{h \leftarrow \mathcal{H}}$.
   - Send $(\mathtt{seize})$ to $\mathcal{T}_\mathsf{S}$. Compute $p_x = x||N$ and send $(\mathtt{sign}, p_x)$ to $\mathcal{T}_\mathsf{S}$ to obtain σ_x. Then, compute $p_r = r||N$ and send $(\mathtt{sign}, p_r)$ to $\mathcal{T}_\mathsf{S}$ to obtain σ_r. Abort if $\mathsf{SIG.Vfy}(\mathsf{vk}, p_x, \sigma_x) \neq 1$ or $\mathsf{SIG.Vfy}(\mathsf{vk}, p_r, \sigma_r) \neq 1$.
   - Compute $c_s = f(p_x) \oplus s$, $(c_x, f(p_r)) \leftarrow \mathsf{TCOM}_{\mathsf{ext}}.\mathsf{Commit}(p_x)$ and $(c_\sigma, d_\sigma) \leftarrow \mathsf{TCOM}_{\mathsf{ext}}.\mathsf{Commit}(\sigma_x, \sigma_r, p_x, p_r, N)$.
   - Send (c_s, c_x, c_σ, f) to the receiver. Release $\mathcal{T}_\mathsf{S}$ by sending $(\mathtt{release})$.

Unveil phase:

3. Sender: Compute $(c_d, d_d) \leftarrow \mathsf{SECOM.Commit}(f(p_r), d_\sigma)$ and send c_d to the receiver.
4. Receiver: Send $(\mathsf{sk}, d_{\mathsf{sk}})$ to the sender.
5. Sender: Check if $\mathsf{TCOM}_{\mathsf{ext}}.\mathsf{TVer}(\mathsf{pk}, \mathsf{sk}) = 1$ and $\mathsf{SECOM.Open}(c_{\mathsf{sk}}, d_{\mathsf{sk}}, \mathsf{sk}) = 1$. Send $(s, p_x, p_r, \sigma_x, \sigma_r, d_\sigma)$ to the receiver.
6. Receiver: Check if $\mathsf{SIG.Vfy}(\mathsf{vk}, p_s, \sigma_s) = \mathsf{SIG.Vfy}(\mathsf{vk}, p_r, \sigma_r) = 1$. Additionally, check if $\mathsf{TCOM}_{\mathsf{ext}}.\mathsf{Open}(c_x, f(p_r), p_x) = 1$, $\mathsf{TCOM}_{\mathsf{ext}}.\mathsf{Open}(c_\sigma, d_\sigma, (\sigma_s, \sigma_r, p_x, p_r, N)) = 1$ and $c_s \oplus f(p_x) = s$. If not, abort; otherwise accept.

Fig. 5. Computationally UC-secure protocol realizing $\mathcal{F}_{\text{COM}}$ in the $\mathcal{F}_{\text{wrap}}^{\text{ru-strict}}$-hybrid model.

Proof. **Corrupted sender.** Consider the simulator in Fig. 6. It is basically a modified version of the extraction algorithm for the straight-line extractable commitment. Against a corrupted sender, we only have to extract the input of the sender and input it into the ideal functionality.

Simulator $\mathcal{S}_\mathsf{S}$

- Upon receiving a message $(\mathtt{sign}, m)$ from $\mathcal{A}_\mathsf{S}$, relay this message to $\mathcal{T}_\mathsf{S}$ and store m in a list Q. Forward the reply from $\mathcal{T}_\mathsf{S}$ to $\mathcal{A}_\mathsf{S}$.
- Upon receiving a message $(\mathtt{vk})$, relay this message to $\mathcal{T}_\mathsf{S}$ and forward the reply to $\mathcal{A}_\mathsf{S}$.
- (Commit) Simulate Step 1 of Π_{COM} and let (c_s^*, c_σ^*, f^*) be the answer from $\mathcal{A}_\mathsf{S}$. Test for all $\alpha_i, \alpha_j \in Q$ if $\mathsf{TCOM}_{\mathsf{ext}}.\mathsf{Open}(c_x^*, f^*(\alpha_j), \alpha_i) = 1$, otherwise abort. Let $(\hat{p}_x, \hat{p}_r) = (\alpha_i, \alpha_j)$ be the values obtained in the previous step. Compute $\hat{s} = c_s^* \oplus f^*(\hat{p}_x)$ and send $(\mathtt{commit}, \hat{s})$ to $\mathcal{F}_{\mathrm{COM}}$.
- (Unveil) Simulate the behavior of an honest receiver and obtain s^*. If $s^* = \hat{s}$, send $(\mathtt{unveil})$ to $\mathcal{F}_{\mathrm{COM}}$, otherwise abort.

Fig. 6. Simulator against a corrupted sender in the protocol Π_{COM}

The only possibility for an environment $\mathcal{Z}$ to distinguish $\mathsf{Real}_{\mathcal{A}_\mathsf{S}}^{\Pi_{\mathrm{COM}}}$ and $\mathsf{Ideal}_{\mathcal{S}_\mathsf{S}}^{\mathcal{F}_{\mathrm{COM}}}$ is the case of an abort by the simulator. However, we can adapt Lemma 2 to this scenario.

It follows that the extraction is successful with overwhelming probability and the simulation is thus indistinguishable from a real protocol run.

Corrupted receiver. The case of a corrupted receiver is more complicated. The simulator proceeds as follows. In the commit phase, he just commits to the all zero string and sends the rest of the messages according to the protocol. To equivocate the commitment, the simulator first extracts the trapdoor $\hat{\mathsf{sk}}$ from the commitment that the receiver sent in the commit phase. He computes the image t under the 2-universal hash function f that equivocates c_s to the value $\hat{s}$ obtained from the ideal functionality. Then, he samples a preimage $\hat{p}_x$ of t, and uses the trapdoor $\hat{\mathsf{sk}}$ to equivocate the commitment c_x to $\hat{p}_x$. Let $\hat{p}_r$ be the new unveil information. The simulator sends both $\hat{p}_x$ and $\hat{p}_r$ to the token $\mathcal{T}_\mathsf{R}$ to obtain σ_x and σ_r. Now, the second commitment c_σ has to be equivocated to the new signatures and inputs. From there, the simulator just executes a normal protocol run with the newly generated values.

Let $\mathcal{A}_\mathsf{R}$ be the dummy adversary. The formal description of the simulator is given in Fig. 7.

Experiment 0: This is the real model.

Experiment 1: Identical to Experiment 0, except that $\mathcal{S}_1$ aborts if the extraction of $\hat{\mathsf{sk}}$ from c_{sk}^* fails, although $\mathsf{SECOM}.\mathsf{Open}(c_{\mathsf{sk}}^*, d_{\mathsf{sk}}^*, \mathsf{sk}^*) = 1$.

Experiment 2: Identical to Experiment 1, except that $\mathcal{S}_2$ uses a uniformly random value t_x instead of applying f to p_x, and computes a preimage $\hat{p}_x$ of t_x under the linear 2-universal hash function f.

Experiment 3: Identical to Experiment 2, except that $\mathcal{S}_3$ computes $(c_\sigma, d_\sigma) \leftarrow \mathsf{TCOM}_{\mathsf{ext}}.\mathsf{Commit}(0)$ in the commit phase. In the unveil phase, he sends $(\mathtt{sign}, \hat{p}_x), (\mathtt{sign}, \hat{p}_r)$ to $\mathcal{T}_\mathsf{R}$. As an unveil information, he computes $\hat{d}_\sigma \leftarrow \mathsf{TCOM}_{\mathsf{ext}}.\mathsf{Equiv}(\hat{\mathsf{sk}}, (\hat{\sigma}_x, \hat{\sigma}_r, \hat{p_x}, \hat{p}_r, N), c_\sigma, d_\sigma)$.

Experiment 4: Identical to Experiment 3, except that $\mathcal{S}_4$ computes $(c_x, d_x) \leftarrow \mathsf{TCOM}_{\mathsf{ext}}.\mathsf{Commit}(0)$ in the commit phase and then computes the unveil information $\hat{p}_r \leftarrow \mathsf{TCOM}_{\mathsf{ext}}.\mathsf{Equiv}(\hat{\mathsf{sk}}, \hat{p_x}, c_x, d_x)$. This is the ideal model.

Simulator $\mathcal{S}_{\mathsf{R}}$

- Upon receiving a message $(\mathtt{sign}, m)$ from $\mathcal{A}_{\mathsf{R}}$, relay this message to $\mathcal{T}_{\mathsf{R}}$ and store m in a list Q. Forward the reply from $\mathcal{T}_{\mathsf{R}}$ to $\mathcal{A}_{\mathsf{R}}$.
- Upon receiving a message $(\mathtt{vk})$, relay this message to $\mathcal{T}_{\mathsf{R}}$ and forward the reply to $\mathcal{A}_{\mathsf{R}}$.
- (Commit) Upon receiving a message $(\mathtt{committed})$ from $\mathcal{F}_{\mathrm{COM}}$ and a message $(\mathsf{pk}^*, c^*_{\mathsf{sk}}, N)$ from $\mathcal{A}_{\mathsf{R}}$, simulate Step 2 of Π_{COM} with input $s = 0$.
- (Unveil) Upon receiving a message $(\mathtt{opened}, \hat{s})$, proceed as follows:
  - Start the straight-line extractor $\mathsf{Ext}_{\mathsf{SEC}}$ from SECOM to extract the commitment c^*_{sk} to obtain $\hat{\mathsf{sk}}$ and check if $\mathsf{TCOM}_{\mathsf{ext}}.\mathsf{TVer}(\mathsf{pk}^*, \hat{\mathsf{sk}}) = 1$, if not abort.
  - Compute $t = \hat{c}_s \oplus \hat{s}$ and choose a preimage $\hat{p}_x \in \{x \mid f(x) = t\}$ of this value under f.
  - Compute $\hat{p}_r \leftarrow \mathsf{TCOM}_{\mathsf{ext}}.\mathsf{Equiv}(\hat{\mathsf{sk}}, \hat{p}_x, \hat{c}_x, \hat{d}_x)$, send $(\mathtt{sign}, \hat{p}_x)$ and $(\mathtt{sign}, \hat{p}_r)$ to $\mathcal{T}_{\mathsf{R}}$ and obtain $\hat{\sigma}_x$ and $\hat{\sigma}_r$, respectively.
  - Compute $\hat{d'}_\sigma \leftarrow \mathsf{TCOM}_{\mathsf{ext}}.\mathsf{Equiv}(\hat{\mathsf{sk}}, (\hat{\sigma}_x, \hat{\sigma}_r, \hat{p}_x, \hat{p}_r, N), \hat{c}_\sigma, \hat{d}_\sigma)$.
  - Execute the unveil phase according to Π_{COM}: Commit to $\hat{d'}_\sigma$ and $f(\hat{p}_r)$ in Step 3, and abort if $\mathsf{sk}^* \neq \hat{\mathsf{sk}}$ in Step 5. Otherwise, send $(\hat{s}, \hat{p}_x, \hat{p}_r, \hat{\sigma}_x, \hat{\sigma}_r, \hat{d'}_\sigma, N)$ to $\mathcal{A}_{\mathsf{R}}$.

Fig. 7. Simulator against a corrupted receiver in the protocol Π_{COM}

Experiment 0 and Experiment 1 are computationally indistinguishable given that SECOM is a straight-line extractable commitment. A distinguishing environment can directly be transformed into an adversary that breaks the straight-line extraction property. Experiments 1 and 2 are statistically indistinguishable, given that f is a 2-universal hash function (the same argumentation as in Lemma 1 applies). Additionally, it is obvious that a preimage is efficiently sampleable due to the linearity of f. Experiment 2 and Experiment 3 are computationally indistinguishable, given that $\mathsf{TCOM}_{\mathsf{ext}}$ is a trapdoor commitment scheme. A distinguishing environment $\mathcal{Z}$ can straightforwardly be used to break the equivocation property of the commitment scheme. The same argumentation holds for Experiment 3 and Experiment 4. □

4 Ideal Signature Tokens

The model considered in the previous section allows a broad class of signature algorithms that can be placed on the token. This comes with the drawback that some UC functionalities cannot be realized. In particular, non-interactive protocols are directly ruled out by the model. In this section, we want to explore what is theoretically feasible with reusable hardware tokens, at the cost of limiting the types of signature tokens that are suitable for our scenario. Therefore, we require that the complete message that is to be signed is given to the signature token. Nevertheless, there are currently available signature cards that can be used for the protocols that are presented in this section.

4.1 Model

In contrast to $\mathcal{F}_{\text{wrap}}^{\text{ru-strict}}$, we now adapt the simulation trapdoor of Canetti et al. [8] from a global random oracle to the scenario of reusable tamper-proof hardware. To overcome the problem that the simulator cannot read queries to the setup functionality outside of the current protocol, the authors require parties that query the setup to include the current session id SID of the protocol. If a malicious party queries the setup in another protocol, using the SID of the first protocol, the setup will store this query in a list and give the simulator access to this list (via the ideal functionality with which the simulator communicates). This mechanism ensures that the simulator only learns illegitimate queries, since honest parties will always use the correct SID.

We thus enhance the standard resettable wrapper functionality $\mathcal{F}_{\text{wrap}}^{\text{resettable}}$ by the query list, and parse inputs as a concatenation of actual input and the session id (cf. Fig. 8).

Compared to our previous reusable token specification $\mathcal{F}_{\text{wrap}}^{\text{ru-strict}}$, it is no longer necessary to use a nonce to bind the messages to one specific protocol instance. Thus, the inherent interaction of the $\mathcal{F}_{\text{wrap}}^{\text{ru-strict}}$-hybrid model is removed in the $\mathcal{F}_{\text{wrap}}^{\text{ru}}$-hybrid model. This will allow a much broader class of functionalities to be realized. For our purposes, however, we have to assume that the token learns the complete input, in contrast to the strict model. This is similar to the model assumed in [29], but in contrast to their work, we focus on untrusted tokens.

Let us briefly state why we believe that this model is still useful. On the one hand, there are signature tokens that support that the user inputs the complete message without any preprocessing. On the other hand, the messages that we input are typically rather short (linear in the security parameter), implying that the efficiency of the token is not reduced by much. Even to the contrary, this allows us to construct more round- and communication-efficient protocols, such that the overall efficiency increases.

Our security notion is as follows.

Definition 10. *Let $\mathcal{F}$ be an ideal functionality and let Π be a protocol. We say that Π UC-realizes $\mathcal{F}$ in the* global tamper-proof hardware model *if for any real PPT adversary $\mathcal{A}$, there exists an ideal PPT adversary $\mathcal{S}$ such that for every PPT enviroment $\mathcal{Z}$, it holds that*

$$\mathsf{Ideal}_{\mathcal{F},\mathcal{S}}^{\mathcal{F}_{\text{wrap}}^{\text{ru}}}(\mathcal{Z}) \approx \mathsf{Real}_{\Pi,\mathcal{A}}^{\mathcal{F}_{\text{wrap}}^{\text{ru}}}(\mathcal{Z})$$

Compared to the standard UC security, the setup is now available both in the real and the ideal settings.

Functionality $\mathcal{F}_{\text{wrap}}^{\text{ru}}$

Implicitly parametrized by a security parameter κ and a list $\bar{\mathcal{F}}$ of ideal functionality programs.

Creation:

1. Await an input $(\texttt{create}, \mathsf{M}, t)$ from the token issuer, where M is a deterministic Turing machine and $t \in \mathbb{N}$. Store (M, t) and send $(\texttt{created})$ to the adversary. Ignore all further `create`-messages.
2. Await a message $(\texttt{delivery})$ from the adversary. Then, send $(\texttt{ready})$ to the token receiver.

Execution:

3. Await an input $(\texttt{run}, w)$ from the receiver with party id PID and session id SID. Parse w as (w', sid). If no `create`-message has been sent, return a special symbol $\perp$. Otherwise, run M on w' from its most recent state and add $(sid, w', \mathsf{M}(w'))$ to the list of illegitimate queries Q_{sid} if $\mathsf{SID} \neq sid$. When M halts without generating output or t steps have passed, send $\perp$ to the receiver; otherwise store the current state of M and send the output of M to the receiver.

Reset (adversarial receiver only):

4. Upon receiving a message $(\texttt{reset})$ from a corrupted token receiver, reset M to its initial state.
5. Upon receiving a message $(\texttt{list})$ from an ideal functionality in the list $\bar{\mathcal{F}}$ with SID sid, return Q_{sid}.

Fig. 8. The wrapper functionality by which we model reusable resettable tamper-proof hardware. The runtime bound t is merely needed to prevent malicious token senders from providing a perpetually running program code M; it will be omitted throughout the rest of the chapter.

4.2 UC-Secure Non-Interactive Two-Party Computation

In this section, we show how to realize UC-secure non-interactive computation and the required tools. In the full version [36] we show a small modification to the straight-line extractable commitment from Sect. 3.2 such that it is non-interactive by simply removing the nonce. This is used for the construction in the next section.

Non-Interactive Straight-Line Witness-Extractable Arguments
Our protocol is based on the construction of Pass [39], who presented a protocol for a non-interactive straight-line witness-extractable proof (NIWIAoK) in the random oracle model. Let $\Pi = (\alpha, \beta, \gamma)$ be a Σ-protocol, i.e. a three message zero-knowledge proof system. We also assume that Π has special soundness, i.e. from answers γ_1, γ_2 to two distinct challenges β_1, β_2, it is possible to reconstruct the witness that the prover used.

The main idea of his construction is as follows. Instead of performing a Σ-protocol interactively, a Fiat-Shamir transformation [22] is used to make the protocol non-interactive. The prover computes the first message α of the Σ-protocol, selects two possible challenges β_1 and β_2, computes the resulting answers γ_1 and γ_2 based on the witness w according to the Σ-protocol for both challenges and computes commitments c_i to the challenge/response pairs. Instead of having the verifier choose one challenge, in [22], a hash function is applied to the commitment to determine which challenge is to be used. The prover then sends (α, c) and the unveil information of the c_i to the verifier. The verifier only has to check if the unveil is correct under the hash function and if the resulting Σ-protocol transcript $(\alpha, \beta_i, \gamma_i)$ is correct. The resulting protocol only has soundness $\frac{1}{2}$ and thus has to be executed several times in parallel. [39] replaces the hash function by a random oracle and thus obtains a proof system. Further, if the commitments to (β_i, γ_i) are straight-line extractable, the resulting argument system will be witness-extractable, i.e. an argument of knowledge.

The straight-line extractable commitment $\Pi^{\mathrm{se}}_{\mathrm{COM}}$ from Sect. 3.2 requires interaction, so we cannot directly plug this into the protocol without losing the non-interactive nature of the argument system. But note that the first message of $\Pi^{\mathrm{se}}_{\mathrm{COM}}$ is simply sending a nonce, which is no longer necessary in the $\mathcal{F}^{\mathrm{ru}}_{\mathrm{wrap}}$-hybrid model. Thus, by omitting this message, $\Pi^{\mathrm{se}}_{\mathrm{COM}}$ becomes a valid non-interactive straight-line extractable commitment.

A formal description of the protocol complete NIWIAoK is given in Fig. 9.

Theorem 3. *The protocol Π_{NIWI} in Fig. 9 is a straight-line witness-extractable argument as per Definition 6 in the $\mathcal{F}^{\mathrm{ru}}_{\mathrm{wrap}}$-hybrid model, given that* NICOM *is a straight-line extractable commitment scheme and* SIG *is an EUF-CMA-secure unique signature scheme.*

Proof. Let Π be a public-coin special-sound honest-verifier zero-knowledge (SHVZK) protocol.

Completeness: Completeness of Π_{NIWI} follows directly from the completeness of the Σ-protocol Π.

Witness-Indistinguishability: Cramer et al. [13,39] show that a SHVZK protocol directly implies a public-coin witness-indistinguishable protocol. Since witness-indistinguishable protocols are closed under parallel composition as shown be Feige and Shamir [21], Π_{NIWI} is witness-indistinguishable.

Extractablility: Let $\mathsf{Ext}_{\mathsf{NIC}}$ be the straight-line extractor of NICOM. We will construct a straight-line extractor for Π_{NIWI} (cf. Fig. 10).
It remains to show that if the verifier accepts, $\mathsf{Ext}_{\mathsf{NIWI}}$ outputs a correct witness with overwhelming probability. First, note that $\mathsf{Ext}_{\mathsf{NIC}}$ extracts the inputs of c^* with overwhelming probability, and by the special soundness of Π, we know that if both challenges in the commitment are extracted, $\mathsf{Ext}_{\mathsf{NIWI}}$ will obtain a witness. Thus, the only possibility for $\mathsf{Ext}_{\mathsf{NIWI}}$ to fail with the extraction is if a malicious PPT prover $\mathcal{A}_{\mathsf{P}}$ manages to convince the verifier with a witness w^* such that $(x, w^*) \notin \mathcal{R}_{\mathcal{L}}$.

Protocol Π_{NIWI}

Let (α, β, γ) denote the three messages of a Σ-protocol Π for a language $\mathcal{L}$. Further let NICOM be an instance of $\Pi^{\text{se}}_{\text{COM}}$ from Section 3.2 without the first message. Let SIG be a unique signature scheme according to Definition 8.

Global setup phase:

- Verifier: Compute $(\mathsf{vk}, \mathsf{sgk}) \leftarrow \mathsf{SIG.KeyGen}(1^\kappa)$. Program a stateless token T with the following functionality.
  - Upon receiving a message $(\texttt{vk})$, return vk.
  - Upon receiving a message $(\texttt{sign}, m)$, compute $\sigma_m \leftarrow \mathsf{SIG.Sign}(\mathsf{sgk}, m)$ and output σ_m.

  Send $(\texttt{create}, \mathsf{T})$ to $\mathcal{T}$.
- Sender: Query $\mathcal{T}$ with $(\texttt{vk})$ to obtain the verification key vk and check if it is a valid verification key for SIG.

Proof phase:

1. Prover: Let a statement x and a witness w be the prover's input, such that $(x, w) \in \mathcal{R}_\mathcal{L}$. Let $l = \mathsf{poly}(\kappa)$ be the length of the signature.
   - Compute l first messages $\alpha = (\alpha^{(1)}, \dots, \alpha^{(l)})$ of the Σ-protocol. Pick $2l$ random challenges $(\beta_0^{(1)}, \beta_1^{(1)}), \dots, (\beta_0^{(l)}, \beta_1^{(l)})$ for the Σ-protocol with $\beta_0^{(i)} \neq \beta_1^{(i)} \, \forall i \in \{1, \dots, l\}$. Compute the corresponding answers $(\gamma_0^{(1)}, \gamma_1^{(1)}), \dots, (\gamma_0^{(l)}, \gamma_1^{(l)})$ for the Σ-protocol from w.
   - Commit to the challenge/response pairs $(\beta_b^{(i)}, \gamma_b^{(i)})$ via $(c_b^{(i)}, d_b^{(i)}) \leftarrow \mathsf{NICOM.Commit}(\beta_b^{(i)}, \gamma_b^{(i)})$ for all $i \in \{1, \dots, l\}$ and $b \in \{0, 1\}$. Let $c = \big((c_0^{(1)}, c_1^{(1)}), \dots, (c_0^{(l)}, c_1^{(l)})\big)$.
   - Send $(\texttt{sign}, (\alpha, c))$ to $\mathcal{T}$ and let σ denote the result. Abort if $\mathsf{SIG.Verify}(\mathsf{vk}, (\alpha, c), \sigma) \neq 1$.

   Send $\pi = (\alpha, c, \sigma, (d_{\sigma_1}^{(1)}, \dots, d_{\sigma_l}^{(l)}), (\beta_{\sigma_1}^{(1)}, \gamma_{\sigma_1}^{(1)}), \dots, (\beta_{\sigma_l}^{(l)}, \gamma_{\sigma_l}^{(l)}))$ to the verifier where σ_i signifies the i-th bit of σ.
2. Verifier: First, check if $\mathsf{SIG.Verify}(\mathsf{vk}, (a, c), \sigma) = 1$. If that is not the case, abort; otherwise check for all i that $(\alpha^{(i)}, \beta_{\sigma_i}^{(i)}, \gamma_{\sigma_i}^{(i)})$ is an accepting transcript for $x \in \mathcal{L}$ and $\mathsf{NICOM.Open}(c_{\sigma_i}^{(i)}, d_{\sigma_i}^{(i)}, (\beta_{\sigma_i}^{(i)}, \gamma_{\sigma_i}^{(i)})) = 1$. If that check is passed, accept; otherwise abort.

Fig. 9. Computationally secure non-interactive straight-line witness-extractable argument in the $\mathcal{F}^{\text{ru}}_{\text{wrap}}$-hybrid model.

Each of the l instances of Π has soundness $\frac{1}{2}$, since a malicious $\mathcal{A}_\mathsf{P}$ can only answer at most one challenge correctly, and otherwise a witness is obtained. Thus, $\mathcal{A}_\mathsf{P}$ has to make sure that in all l instances, the correctly answered challenge is selected. Assume for the sake of contradiction that $\mathcal{A}_\mathsf{P}$ manages to convince the verifier with some non-negligible probability $\varepsilon(\kappa)$ of a witness w^* such that $(x, w^*) \notin \mathcal{R}_\mathcal{L}$. We will construct an adversary $\mathcal{B}$ from $\mathcal{A}_\mathsf{P}$ that breaks the EUF-CMA property of SIG with probability $\varepsilon(\kappa)$.

Let $\mathcal{B}$ be the adversary for the EUF-CMA game. Let vk be the verification key that $\mathcal{B}$ receives from the EUF-CMA game. $\mathcal{B}$ simulates $\mathcal{F}^{\text{ru}}_{\text{wrap}}$ to $\mathcal{A}_\mathsf{P}$ by

Extractor $\mathsf{Ext}_{\mathsf{NIWI}}$

Let $\mathsf{Ext}_{\mathsf{SEC}}$ be the extraction algorithm for SECOM. Upon input $\big(\pi^* = (\alpha^*, c^*, \sigma^*, (d^{*(1)}_{\sigma_1}, \ldots, d^{*(l)}_{\sigma_l})), Q\big)$, where Q is the set of queries to $\mathcal{F}^{\mathrm{ru}}_{\mathrm{wrap}}$, start the following algorithm.

1. Run the verifier algorithm on π^*, if it aborts, abort. Run $\mathsf{Ext}_{\mathsf{NIC}}$ with input $\big(c^*, Q\big)$ to extract all commitments and obtain $(\hat{\beta}^{(i)}_b, \hat{\gamma}^{(i)}_b)\, \forall i \in \{1, \ldots, l\}$.
2. Select the first correct witness $\hat{w}$ derived from $(\hat{\gamma}^{(i)}_0, \hat{\gamma}^{(i)}_1)$ and output $\hat{w}$.

Fig. 10. The extraction algorithm for the non-interactive straight-line witness-extractable argument $\mathit{\Pi}_{\mathrm{NIWI}}$.

returning vk upon receiving a query $(\mathtt{vk})$; further let Q be the set of queries that $\mathcal{A}_{\mathsf{P}}$ sends to $\mathcal{F}^{\mathrm{ru}}_{\mathrm{wrap}}$. For each query $(\mathtt{sign}, m)$, $\mathcal{B}$ forwards the message to the signature oracle of the EUF-CMA game and returns the resulting signature σ to $\mathcal{A}_{\mathsf{P}}$.
If $\mathcal{B}$ receives a signature query of the form $(\mathtt{sign}, m^*)$ with $m^* = (\alpha^*, c^*)$, start the extractor $\mathsf{Ext}_{\mathsf{NIC}}$ with input (c^*, Q) to extract the commitments c^* using Q. Create a signature σ^* by selecting σ^*_i as the index of the correctly evaluating challenge. The verifier will only accept if that is the case. If $\mathsf{SIG.Verify}(\mathsf{vk}, (\alpha^*, c^*), \sigma^*) = 1$, send (m^*, σ^*) to the EUF-CMA game, otherwise abort. We thus have that $\mathcal{A}_{\mathsf{P}}$ wins the EUF-CMA game with probability $\varepsilon(\kappa)$, which contradicts the EUF-CMA security of SIG. □

UC-secure NISC

Non-interactive secure computation (NISC) [30] is typically a two-party protocol. The main idea is to execute a constant round two-party computation, but reduce the number of rounds to two. In the OT-hybrid model, garbled circuits realize a non-interactive evaluation of any functionality (if the sender requires no output): the sender garbles the circuit and sends it to the receiver, who learns some labels via the OTs to evaluate the garbled circuit. It remains to realize the OT protocol with minimal interaction, and such a protocol was provided by Peikert et al. [43], taking 2 rounds of interaction given a CRS. Combining the two building blocks, a NISC protocol proceeds as follows: the receiver first encodes his input using the first message of the OT protocol and sends it to the sender. The sender in turn garbles the circuit and his inputs depending on the received message and sends the resulting garbled values to the receiver. Now the receiver can obtain some of the labels and evaluate the garbled circuit.

In order to obtain NISC, [8] build such a one-sided simulatable OT using a NIWIAoK as constructed in the previous section. The construction is black-box, i.e. we can directly replace their NIWIAoK with ours and obtain the same result. The actual NISC protocol of [8] is based on the protocol of Ashfar et al. [1]. Our modifications to the protocol are only marginal. In order for the simulation against the sender to work, the simulator must extract the seeds that the sender used to create the circuits. That is the main technical difference between [8] and our solution. [8] have the sender send a random value to their global random oracle and use the answer as the seed. Thus, the simulator learns the seed and can extract the sender's inputs. In our case, we let the sender choose a random value and have him send it to $\mathcal{F}_{\text{wrap}}^{\text{ru}}$ to obtain a signature, which allows us to extract this value. Due to possible leakage the sender has to apply a 2-universal hash function to the random value and use the result as the seed, but the technique (and the proof) is essentially the same as for our straight-line extractable commitment scheme. We provide a detailed protocol description in the full version [36].

5 Limitations

It is known that there exist limitations regarding the feasibility of UC-secure protocols based on resettable tamper-proof hardware, both with computational and with statistical security. Concerning statistical security, Goyal et al. [25] show that non-interactive commitments and OT cannot be realized from resettable tamper-proof hardware tokens, even with standalone security. In the computational setting, Döttling et al. [20] and Choi et al. [12] show that if (any number of) tokens are sent only in one direction, i.e. are not exchanged by both parties, it is impossible to realize UC-secure protocols without using non-black-box techniques. Intuitively, this follows from the fact that the simulator does not have any additional leverage over a malicious receiver of such a token. Thus, a successful simulator strategy could be applied by a malicious receiver as well. The above mentioned results apply to our scenario as well.

Jumping ahead, the impossibilities stated next hold for both specifications of reusable tamper-proof hardware that we present in the following. In particular, GUC and GUC-like frameworks usually impose the restriction that the simulator only has black-box access to the reusable setup. Thus, compared to the standard definition of resettable tamper-proof hardware, the model of resettable reusable tamper-proof hardware has some limitations concerning non-interactive two-party computation. The degree of non-interactivity that can be achieved with resettable hardware, i.e. just sending tokens (and possibly an additional message) to the receiver, is impossible to obtain in the model of resettable reusable hardware.

Corollary 1. *There exists no protocol Π_{PF} using any number of reusable and resettable hardware tokens $\mathcal{T}_1, \ldots, \mathcal{T}_n$ issued from the sender to the receiver that computationally UC-realizes the ideal point function $\mathcal{F}_{\text{PF}}$.*

Proof (Sketch). This follows directly from the observation that the simulator for protocols based on reusable hardware is only allowed to have black-box access to the token, i.e. the simulator does not have access to the code of the token(s). Applying [12,20] yields the claim.

The best we can hope for is a protocol for non-interactive two-party computation where the parties exchange two messages (including hardware tokens) to obtain a (somewhat) non-interactive protocol. Maybe even more interesting, even stateful reusable hardware tokens will not yield any advantage compared to resettable tokens, if the tokens are only sent in one direction.

Corollary 2. *There exists no protocol Π_{OT} using any number of reusable and stateful hardware tokens $\mathcal{T}_1, \ldots, \mathcal{T}_n$ issued from the sender to the receiver that statistically UC-realizes $\mathcal{F}_{\mathrm{OT}}$.*

Proof (Sketch). First note, as above, that the simulator of a protocol against a token sender will not get the token code because he only has black-box access to the token. Thus the simulator cannot use rewinding during the simulation, which is the one advantage that he has over the adversary. The simulator falls back to observing the input/output behavior of the token, exactly as in the case of standard resettable hardware. Due to the impossibility of statistically secure OT based on resettable hardware [25], the claim follows.

Acknowledgement. The authors would like to thank Dirk Achenbach and Björn Kaidel for helpful discussions on an earlier version of this paper, and the anonymous reviewers for their comments. We further thank Maciej Obremski for disussions on the entropy estimation of the signatures.

References

1. Afshar, A., Mohassel, P., Pinkas, B., Riva, B.: Non-interactive secure computation based on cut-and-choose. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 387–404. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_22
2. Agrawal, S., Ananth, P., Goyal, V., Prabhakaran, M., Rosen, A.: Lower bounds in the hardware token model. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 663–687. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54242-8_28
3. Bohli, J.-M., González Vasco, M.I., Steinwandt, R.: A subliminal-free variant of ECDSA. In: Camenisch, J.L., Collberg, C.S., Johnson, N.F., Sallee, P. (eds.) IH 2006. LNCS, vol. 4437, pp. 375–387. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74124-4_25
4. Boureanu, I., Ohkubo, M., Vaudenay, S.: The limits of composable crypto with transferable setup devices. In: Bao, F., Miller, S., Zhou, J., Ahn, G.J. (eds.) ASIACCS 15, pp. 381–392. ACM Press, April 2015
5. Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols. In: 42nd FOCS, pp. 136–145. IEEE Computer Society Press, October 2001
6. Canetti, R., Dodis, Y., Pass, R., Walfish, S.: Universally composable security with global setup. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 61–85. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-70936-7_4
7. Canetti, R., Fischlin, M.: Universally composable commitments. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 19–40. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_2

8. Canetti, R., Jain, A., Scafuro, A.: Practical UC security with a global random oracle. In: Ahn, G.J., Yung, M., Li, N. (eds.) ACM CCS 14, pp. 597–608. ACM Press, November 2014
9. Canetti, R., Lindell, Y., Ostrovsky, R., Sahai, A.: Universally composable two-party and multi-party secure computation. In: 34th ACM STOC, pp. 494–503. ACM Press, May 2002
10. Canetti, R., Shahaf, D., Vald, M.: Universally composable authentication and key-exchange with global PKI. In: Cheng, C.-M., Chung, K.-M., Persiano, G., Yang, B.-Y. (eds.) PKC 2016. LNCS, vol. 9615, pp. 265–296. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49387-8_11
11. Chandran, N., Goyal, V., Sahai, A.: New constructions for UC secure computation using tamper-proof hardware. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 545–562. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_31
12. Choi, S.G., Katz, J., Schröder, D., Yerukhimovich, A., Zhou, H.-S.: (Efficient) universally composable oblivious transfer using a minimal number of stateless tokens. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 638–662. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54242-8_27
13. Cramer, R., Damgård, I., Schoenmakers, B.: Proofs of partial knowledge and simplified design of witness hiding protocols. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 174–187. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48658-5_19
14. Damgård, I., Nielsen, J.B., Wichs, D.: Universally composable multiparty computation with partially isolated parties. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 315–331. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00457-5_19
15. Damgård, I., Scafuro, A.: Unconditionally secure and universally composable commitments from physical assumptions. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8270, pp. 100–119. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-42045-0_6
16. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM J. Comput. **38**(1), 97–139 (2008)
17. Döttling, N., Kraschewski, D., Müller-Quade, J.: Unconditional and composable security using a single stateful tamper-proof hardware token. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 164–181. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19571-6_11
18. Döttling, N., Kraschewski, D., Müller-Quade, J., Nilges, T.: From stateful hardware to resettable hardware using symmetric assumptions. In: Au, M.-H., Miyaji, A. (eds.) ProvSec 2015. LNCS, vol. 9451, pp. 23–42. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-26059-4_2
19. Döttling, N., Kraschewski, D., Müller-Quade, J., Nilges, T.: General statistically secure computation with bounded-resettable hardware tokens. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015. LNCS, vol. 9014, pp. 319–344. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46494-6_14
20. Döttling, N., Mie, T., Müller-Quade, J., Nilges, T.: Implementing resettable UC-functionalities with untrusted tamper-proof hardware-tokens. In: Sahai, A. (ed.) TCC 2013. LNCS, vol. 7785, pp. 642–661. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36594-2_36
21. Feige, U., Shamir, A.: Witness indistinguishable and witness hiding protocols. In: 22nd ACM STOC, pp. 416–426. ACM Press, May 1990

22. Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_12
23. Goldreich, O.: The Foundations of Cryptography: Basic Techniques, vol. 1. Cambridge University Press, Cambridge (2001)
24. Goldwasser, S., Kalai, Y.T., Rothblum, G.N.: One-time programs. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 39–56. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_3
25. Goyal, V., Ishai, Y., Mahmoody, M., Sahai, A.: Interactive locking, zero-knowledge PCPs, and unconditional cryptography. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 173–190. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_10
26. Goyal, V., Ishai, Y., Sahai, A., Venkatesan, R., Wadia, A.: Founding cryptography on tamper-proof hardware tokens. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 308–326. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11799-2_19
27. Hazay, C., Polychroniadou, A., Venkitasubramaniam, M.: Composable security in the tamper-proof hardware model under minimal complexity. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9985, pp. 367–399. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53641-4_15
28. Hazay, C., Polychroniadou, A., Venkitasubramaniam, M.: Constant round adaptively secure protocols in the tamper-proof hardware model. In: Fehr, S. (ed.) PKC 2017. LNCS, vol. 10175, pp. 428–460. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54388-7_15
29. Hofheinz, D., Müller-Quade, J., Unruh, D.: Universally composable zero-knowledge arguments and commitments from signature cards. In: Proceedings of the 5th Central European Conference on Cryptology MoraviaCrypt 2005 (2005)
30. Ishai, Y., Kushilevitz, E., Ostrovsky, R., Prabhakaran, M., Sahai, A.: Efficient non-interactive secure computation. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 406–425. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_23
31. Ishai, Y., Prabhakaran, M., Sahai, A.: Founding cryptography on oblivious transfer – efficiently. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 572–591. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_32
32. Jager, T.: Verifiable random functions from weaker assumptions. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015. LNCS, vol. 9015, pp. 121–143. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46497-7_5
33. Katz, J.: Universally composable multi-party computation using tamper-proof hardware. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 115–128. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72540-4_7
34. Kolesnikov, V.: Truly efficient string oblivious transfer using resettable tamper-proof tokens. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 327–342. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-11799-2_20
35. Lysyanskaya, A.: Unique signatures and verifiable random functions from the DH-DDH separation. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 597–612. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45708-9_38
36. Mechler, J., Müller-Quade, J., Nilges, T.: Universally composable (non-interactive) two-party computation from untrusted reusable hardware tokens. Cryptology ePrint Archive, Report 2016/615 (2016). http://eprint.iacr.org/2016/615
37. Micali, S., Rabin, M.O., Vadhan, S.P.: Verifiable random functions. In: 40th FOCS, pp. 120–130. IEEE Computer Society Press, October 1999

38. Moran, T., Segev, G.: David and Goliath commitments: UC computation for asymmetric parties using tamper-proof hardware. In: Smart, N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 527–544. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78967-3_30
39. Pass, R.: On deniability in the common reference string and random oracle model. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 316–337. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_19
40. Pass, R., Shi, E., Tramèr, F.: Formal abstractions for attested execution secure processors. In: Coron, J.-S., Nielsen, J.B. (eds.) EUROCRYPT 2017. LNCS, vol. 10210, pp. 260–289. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56620-7_10
41. Pass, R., Wee, H.: Black-box constructions of two-party protocols from one-way functions. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 403–418. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00457-5_24
42. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (1992). https://doi.org/10.1007/3-540-46766-1_9
43. Peikert, C., Vaikuntanathan, V., Waters, B.: A framework for efficient and composable oblivious transfer. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 554–571. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_31