Universally Composable Σ-protocols in the Global Random-Oracle Model

Anna Lysyanskaya and
Leah Namisa Rosenbloom

Brown University, Providence RI 02906, USA
{anna_lysyanskaya,leah_rosenbloom}@brown.edu

Abstract. Numerous cryptographic applications require efficient non-interactive zero-knowledge proofs of knowledge (NIZKPoK) as a building block. Typically they rely on the Fiat-Shamir heuristic to do so, as security in the random-oracle model is considered good enough in practice. However, there is a troubling disconnect between the stand-alone security of such a protocol and its security as part of a larger, more complex system where several protocols may be running at the same time. Provable security in the general universal composition model (GUC model) of Canetti et al. is the best guarantee that nothing will go wrong when a system is part of a larger whole, even when all parties share a common random oracle. In this paper, we prove the minimal necessary properties of generally universally composable (GUC) NIZKPoK in any global random-oracle model, and show how to achieve efficient and GUC NIZKPoK in both the restricted programmable and restricted observable (non-programmable) global random-oracle models.

1 Introduction

Non-interactive zero-knowledge proofs of knowledge (NIZKPoK) [5,28,42] form the basis of many cryptographic protocols that are on the cusp of widespread adoption in practice. For example, the Helios voting system [1] and other efficient systems employing cryptographic shuffles [46] use zero-knowledge proofs of knowledge to ensure that each participant in the system correctly followed the protocol and shuffled or decrypted its inputs correctly. Anonymous e-cash [12] and e-token [11] systems use them to compute proofs of validity of an e-coin or e-token. In group signatures [18,2] they are used to ensure that the signer is in possession of a group signing key. In anonymous credential constructions [13,14], they are used to ensure that the user identified by a given pseudonym is in possession of a credential issued by a particular organization.

The non-interactive aspect of NIZKPoK is especially important to most of these applications—it enables a prover to form a proof of some attribute for a *general* verifier rather than forcing the prover to talk to each verifier individually, which is inefficient in most cases and infeasible for some applications. It is also extremely important that the NIZKPoK be efficient. Thus, the constructions

cited above use efficient Σ-protocols [26] made non-interactive via the Fiat-Shamir heuristic [29] to instantiate the NIZKPoK in the random-oracle model (ROM) [3]. Recall that a Σ-protocol for a relation R is, in a nutshell, a $(1-\mathsf{negl})$-sound honest-verifier three-move proof system in which the single message from the verifier to the prover is a random ℓ-bit string. The Fiat-Shamir transform makes the proof system non-interactive by replacing the message from the verifier with the output of a random oracle (RO).

Recently, a better understanding of how badly such NIZKPoK fare in the *concurrent* setting emerged [44,27,4,39]. Allowing for secure concurrent executions is of vital importance for the real-world application of any of the cryptographic protocols mentioned above, and especially for distributed protocols. But Drijvers et al. [27] demonstrated subtleties in the proofs of security for concurrent protocol executions that often go undetected, leaving building-block cryptographic protocols vulnerable to attacks like Wagner [44] and Benhamouda et al.'s exploitation of the ROS problem [4].

One way to circumvent the unique subtleties of composing cryptographic primitives is to prove that each primitive is *universally composable* using Canetti's universal composition (UC) framework [19]. In the UC framework, the security of a particular session of a protocol is analyzed with respect to an environment, which represents an arbitrary set of concurrent protocols. The environment in the UC framework can talk to and collude with the traditional "adversary" in cryptographic protocols, directing it to interfere with the protocol. However, the original UC framework did not provide a mechanism for parties in different settings to use a shared global functionality, for instance a shared RO or common reference string (CRS). In real-world applications, it is virtually guaranteed that parties will share setup and state between sessions.

To address the issue of shared state and concurrency in the UC framework, Canetti, Dodis, Pass, and Walfish developed the *general* UC (GUC) framework, which considers "global" functionalities $\mathcal{G}$ that can be queried by any party in any session at any time, including the environment [20]. Canetti, Jain, and Scafuro later showed several practical applications of the GUC framework with a restricted observable global RO $\mathcal{G}_{\mathtt{roRO}}$ as the only trusted setup. They include commitment, oblivious transfer, and secure function evaluation protocols, all GUC in the $\mathcal{G}_{\mathtt{roRO}}$-hybrid model [22]. Building on Canetti et al.'s framework, Camenisch, Drijvers, Gagliardoni, Lehmann, and Neven developed a restricted *programmable* observable global RO, denoted $\mathcal{G}_{\mathtt{rpoRO}}$, that allows for more efficient GUC commitments in the $\mathcal{G}_{\mathtt{rpoRO}}$-hybrid model [10].

Thus, the $\mathcal{G}_{\mathtt{roRO}}$- and $\mathcal{G}_{\mathtt{rpoRO}}$-hybrid models are attractive ones for constructing and analyzing practical and composable non-interactive zero-knowledge proofs. Obtaining an efficient NIZKPoK (for a relation R) in either global ROM from an efficient Σ-protocol (for the same relation) is a natural goal. We begin by showing that any protocol that can be considered a GUC NIZKPoK in *any* global ROM must satisfy particular flavors of completeness, zero-knowledge, and soundness (formalized in Definitions 3, 4, and 5, respectively) — i.e., that these flavors are necessary to achieve security in the global RO model.

Theorem 1 (Informal). *If a protocol is a GUC NIZKPoK in any global ROM, then it satisfies Definitions 3, 4, and 5.*

Next, we obtain GUC NIZKPoK in the (programmable) $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model by using a straight-line compiler on *any* Σ-protocol. A straight-line compiler [30] transforms a Σ-protocol into a non-interactive zero-knowledge proof system in which the knowledge extractor uses the proof itself as well as the adversary's random-oracle query history in order to compute an adversarial prover's witness. (More formally, the resulting protocol satisfies our Definitions 3-5.)

Theorem 2 (Informal). *The non-interactive proof system obtained by running any Σ-protocol for relation R through any straight-line compiler is a GUC NIZKPoK for relation R in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model.*

While the programming property of $\mathcal{G}_{\texttt{rpoRO}}$ is helpful in proving security, it also localizes aspects of the global RO by providing a programming verification interface that concurrent protocols cannot access. It is unclear how localized interfaces that are vital to the security of component protocols might impact the security analysis of composed protocols.

Therefore, we also consider NIZKPoK in the less restrictive (non-programmable) $\mathcal{G}_{\texttt{roRO}}$-hybrid model, where $\mathcal{G}_{\texttt{roRO}}$'s interfaces are completely public. Unfortunately, Pass [40] and Canetti et al. [22] point out that it is not possible to construct NIZKPoK using *only* a global functionality, because there is no way for the simulator in the security experiment to exercise control over it. We introduce a new model called the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model, in which protocol participants have access to a trusted common reference string (CRS) functionality. Participants can compute this CRS for a one-time cost at the beginning of the session using only $\mathcal{G}_{\texttt{roRO}}$ and Canetti et al.'s GUC non-interactive secure computation (NISC) protocol [22]. We prove that any straight-line compiler in conjunction with our new construction, which uses a special type of Σ-protocol called an OR-protocol [26,24], is sufficient to transform any Σ-protocol into a GUC NIZKPoK in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model.

Theorem 3 (Informal). *The non-interactive proof system obtained by composing any Σ-protocol for relation R with a local CRS relation S and running the combined OR-protocol through any straight-line compiler is a GUC NIZKPoK for relation $R \vee S$ in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model.*

The straight-line compiler we use ensures that the protocols we obtain satisfy the flavors of completeness, zero-knowledge, and soundness from Definitions 3, 4, and 5. Combined with Theorem 1, this demonstrates that these flavors are both necessary and sufficient.

Finally, we realize our GUC transforms for Σ-protocols using Kondi and shelat's randomized version of the Fischlin transform [35,30], demonstrating that it is possible to construct *efficient* GUC NIZKPoK from a broad class of Σ-protocols in both the $\mathcal{G}_{\texttt{rpoRO}}$ and $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid models.

Along the way, we uncover theoretical observations that may be of independent interest. First, that straight-line compilers afford strong security guarantees: because they work exclusively using information the adversary already knows, we can compose them with other building blocks such as zero-knowledge simulators without compromising the security of the overall system. This "decoupling" property [30], and security properties of non-rewinding extractors in general, are of interest in the quantum random-oracle model (QROM), where rewinding is tricky because of the no-cloning theorem [45,34,43]. It is the subject of future work to explore whether other mechanisms of straight-line extraction (for example, ones that do not rely on the adversary's query history) [17,40,34,43] are sufficient to bootstrap Σ-protocols into GUC NIZKPoK in the $\mathcal{G}_{\texttt{rpoRO}}$- or $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid models, a different global ROM, or the QROM.

Organization. In the remainder of the introduction, we provide general background information on Σ-protocols, the GUC model, the global ROM(s), and straight-line extraction. In Section 2, we give formal definitions of Σ-protocols and straight-line compilers. Section 3 contains definitions of GUC-security in various global ROMs and a proof of Theorem 1 (that any GUC NIZKPoK must have the security properties afforded by straight-line compilers). In Section 4, we prove Theorem 2 (that any straight-line compiler is sufficient to transform any Σ-protocol into a GUC NIZKPoK in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model), and in Section 5 we prove Theorem 3 (that any straight-line compiler in conjunction with our OR-protocol construction is sufficient to complete the transform in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model). Finally in Section 6, we leverage the randomized Fischlin transform to efficiently realize our constructions in both global ROMs.

Σ-Protocols. A Σ-protocol for a binary $\mathcal{NP}$ relation R is a three-round, public-coin proof system. On input x and w such that $(x, w) \in R$, the prover generates its first message $\texttt{com}$ (in the literature on Σ protocols, this first message is often referred to as a "commitment"). In response, the honest verifier sends a unique ℓ-length *random* "challenge" $\texttt{chl}$ to the prover. Finally, the prover "responds" with a value $\texttt{res}$. The resulting transcript $(\texttt{com}, \texttt{chl}, \texttt{res})$ is then fed to a verification algorithm that determines whether the verifier accepts or rejects.

Σ-protocols must additionally satisfy three properties. First, they must satisfy *completeness*: if the prover has a valid witness and both parties engage in the protocol honestly, the verifier always accepts. Next, they must be *special honest-verifier zero-knowledge*: there must exist a simulator algorithm that on input x and $\texttt{chl} \in \{0,1\}^\ell$ outputs an accepting transcript $(\texttt{com}, \texttt{chl}, \texttt{res})$ for x such that, if $\texttt{chl}$ was chosen uniformly at random, $(\texttt{com}, \texttt{chl}, \texttt{res})$ is indistinguishable from that output by an honest prover on input x. Finally, they must have *special soundness*: if there are two accepting transcripts for any statement with the same commitment $\texttt{com}$ but different challenges $\texttt{chl} \neq \texttt{chl}'$, there exists an extractor algorithm that can produce a valid witness from the transcripts. The stronger version of soundness, special *simulation* soundness, says that special soundness must still hold even if an adversary has oracle access to the simulator.

The Σ-protocol format captures many practical zero-knowledge proof systems. For example, Wikström [46] shows Σ-protocols for proving a rich set of relations between ElGamal ciphertexts, which in turn allow proving that a set of ciphertexts was shuffled correctly; similar protocols exist for Paillier ciphertexts [23,17]. A robust body of literature exists giving Σ-protocols for proving that values committed using Pedersen [41] and Fujisaki-Okamoto [32] commitments satisfy general algebraic and Boolean circuits [8,15,16] and lie in certain integer ranges [6,36]. For all the Σ-protocols listed above, the size and complexity of the proof system is a $O(1)$ factor of the complexity of verifying the underlying relation $R(x, w)$, making Σ-protocols extremely desirable in practice.

Σ-protocols are also the most efficient technique to achieve zero-knowledge proofs of knowledge of a commitment opening in the lattice setting [38,25], where the complexity grows by a factor of $O(k)$ in order to achieve soundness $(1-2^{-k})$. Thus, for all the relations R cited above, our results immediately yield the most efficient known GUC NIZKPoK in the global ROM.

The General Universal Composability (GUC) Model. Our security experiment is that of the GUC model of Canetti et al. [20], which enables the UC-security analysis of protocols with global functionalities.

Briefly, the UC and GUC modeling of the world envisions an adversarial environment $\mathcal{Z}$, which provides inputs to honest participants, observes their outputs, and (at a high level) directs the order in which messages are passed between different system components. Additionally, the world includes honest participants (that receive inputs from $\mathcal{Z}$ and let $\mathcal{Z}$ observe their outputs) and adversarial participants controlled by the adversary $\mathscr{A}$ (whose behavior is also directed and observed by $\mathcal{Z}$).

The ideal world additionally contains an ideal functionality $\mathcal{F}$ and an ideal adversary $\mathcal{S}$, also called the simulator. In the ideal world, the honest participants pass their inputs directly to $\mathcal{F}$ and receive output from it. The real world does not contain such a functionality; instead, the honest participants run a cryptographic protocol. The corrupted participants in the ideal world always communicate through $\mathcal{S}$, who simulates their view and may pass their inputs to $\mathcal{F}$ through a private channel. There are also worlds in between these two: in a $\mathcal{G}$-hybrid world, the honest participants run a protocol that can make calls to an ideal functionality $\mathcal{G}$. In the GUC model, $\mathcal{G}$ is accessible not only to the honest participants, but also to $\mathcal{Z}$. A cryptographic protocol is said to be (G)UC with respect to a functionality $\mathcal{F}$ (in other words, the protocol (G)UC-realizes $\mathcal{F}$) if for any real-world adversary $\mathscr{A}$, there exists an "ideal" adversary (simulator) $\mathcal{S}$ which creates a view for the environment (in the ideal world) that is indistinguishable from its view of the cryptographic protocol.

In our case, the ideal functionality is the NIZKPoK ideal functionality, or $\mathcal{F}_{\texttt{NIZK}}$, which works as follows. An honest participant in a protocol session s can compute a proof π of knowledge of w such that $(x, w) \in R$ by querying $\mathcal{F}_{\texttt{NIZK}}$'s **Prove** interface and giving it (s, x, w). The string π itself is computed according to the algorithm `SimProve` provided by the ideal adversary $\mathcal{S}$. The functionality

guarantees the zero-knowledge property because `SimProve` is independent of w. An honest participant can also verify a supposed proof π for x by querying $\mathcal{F}_{\texttt{NIZK}}$'s **Verify** interface on input (x, π). $\mathcal{F}_{\texttt{NIZK}}$ ensures the soundness of the proof system as follows: if the proof π was *not* issued by $\mathcal{F}_{\texttt{NIZK}}$, then it runs an extractor algorithm `Extract` provided by $\mathcal{S}$ to try to compute a witness w from the proof π. The `Extract` algorithm may also require additional inputs from $\mathcal{S}$.

The Global Random-Oracle Models (Global ROMs). The traditional random oracle (RO) $H : \{0,1\}^* \to \{0,1\}^\ell$ is a function that takes any string as input and returns a uniformly random ℓ-bit string as output [3]. The global random-oracle model (global ROM) allows us to capture the realistic scenario in which the same RO is reused by many parties over many (potentially concurrent) executions of numerous distinct protocols. As envisioned by Canetti et al. [22] and formalized by Camenisch et al. [10], the "strict" global RO functionality $\mathcal{G}_{\texttt{sRO}}$ is a public, universally-accessible RO that can be queried by any party in any protocol execution, including by the arbitrary concurrent protocols modeled by the environment in the UC framework [20].

Pass [40], Canetti and Fischlin [21], Canetti et al. [20,22], and Camenisch et al. [10] have all discussed the limitations of $\mathcal{G}_{\texttt{sRO}}$. In particular, Canetti and Fischlin [21] demonstrated that it is impossible to achieve UC commitments with *only* a global setup, and Canetti et al. extended this argument to commitments and zero knowledge in the GUC framework [20] and the $\mathcal{G}_{\texttt{roRO}}$-hybrid model [22]. The limitation stems from the fact that in a "strict" setup, the simulator does not have any special advantage over a regular protocol participant. In our setting, $\mathcal{F}_{\texttt{NIZK}}$ needs to *observe* the adversary's RO queries in order to extract witnesses and ensure the special soundness property. Most zero-knowledge simulators also rely on the extra ability to *program* the RO at selected points in order to simulate proofs of statements without witnesses.

Canetti et al. first introduced a global RO $\mathcal{G}_{\texttt{roRO}}$ with a restricted "observability" property [22]. The ideal adversary (simulator) $\mathcal{S}$ in the security proof of a protocol Π emulating an ideal functionality $\mathcal{F}$ in the $\mathcal{G}_{\texttt{roRO}}$-hybrid model is able to observe all adversarial queries to $\mathcal{G}_{\texttt{roRO}}$ as follows. First, $\mathcal{S}$ can observe the corrupted parties' queries to $\mathcal{G}_{\texttt{roRO}}$ by directly monitoring their input and output wires (recall that in the ideal world, corrupted parties communicate through $\mathcal{S}$). The *environment's* queries to $\mathcal{G}_{\texttt{roRO}}$, on the other hand, are not directly monitored by $\mathcal{S}$. Since $\mathcal{G}_{\texttt{roRO}}$ is completely public, the environment is free to query it anytime; however, the environment is not free to query it with the same session identifier (SID) as the participants in Π or $\mathcal{F}$, because it is external to legitimate sessions of Π by definition. In order to ensure the environment's queries are still available to the simulator, $\mathcal{G}_{\texttt{roRO}}$ checks whether the SID for a query matches the SID of the querent. In the event that it does not, this query is labelled "illegitimate," creating the restriction. $\mathcal{G}_{\texttt{roRO}}$ makes a record of all illegitimate queries available to an ideal functionality $\mathcal{F}$ with the correct SID, if it exists. We will see that for our construction of GUC NIZKPoK in the $\mathcal{G}_{\texttt{rpoRO}}$- and $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-

hybrid models, $\mathcal{F}_{\texttt{NIZK}}$ can leverage these queries to extract witnesses from the environment's proofs.

Camenisch et al.'s restricted *programmable* observable global RO $\mathcal{G}_{\texttt{rpoRO}}$ [10] builds on the functionality of $\mathcal{G}_{\texttt{roRO}}$ as follows. In order to ensure that programming is restricted to the simulator, $\mathcal{G}_{\texttt{rpoRO}}$ has an `IsProgrammed` interface that allows participants with a particular SID to check whether the output of $\mathcal{G}_{\texttt{rpoRO}}$ was programmed on some input pertaining to the *same session*. Honest parties in the challenge session can therefore check whether the adversary has programmed $\mathcal{G}_{\texttt{rpoRO}}$, and can refuse to continue the protocol if so. In the real world, no programming occurs; in the ideal world, the simulator, who controls the corrupted parties' views of the experiment, can program $\mathcal{G}_{\texttt{rpoRO}}$ and then pretend it did not program anything by returning "false" to all of the corrupted parties' `IsProgrammed` queries. Since only parties running a legitimate protocol session s are allowed to use the `IsProgrammed` interface for s, the environment cannot make `IsProgrammed` queries for s—if it could, it would easily be able to distinguish between the real and ideal experiments by checking whether honest parties' responses were programmed.

We show how to construct efficient, GUC NIZKPoK in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model. However, we believe there may be downsides to programmable global ROs like $\mathcal{G}_{\texttt{rpoRO}}$: it is not clear how compromising the fully-public aspect of the global RO with a locally-restricted interface might impact the overall composability of protocols proven secure in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model.[1] In order to achieve efficient GUC NIZKPoK *without* this localized interface, we build a new hybrid model called the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model. The $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model shifts the localized interface from inside of the global RO to *inside of the protocol*. For a one-time cost at the beginning of the protocol execution, participants can compute this CRS securely and realize $\mathcal{F}_{\texttt{NIZK}}$ *using only the observable global RO* $\mathcal{G}_{\texttt{roRO}}$ by leveraging Canetti et al.'s GUC NISC protocol [22]. Similar mechanisms are used in practice to obtain practical NIZKPoK in other ROMs [7].

In the real world, our ideal CRS functionality $\mathcal{F}_{\texttt{CRS}}$ returns a random string `CRS` (the CRS our real-world participants might compute using the NISC protocol). In the ideal world, the simulator generates `CRS` itself, along with a trapdoor `trap` that only it knows. The proof-generation process in our construction of GUC NIZKPoK in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model is to show that the prover either knows a "real" witness w for a statement x such that $(x, w) \in R$, *or* it knows the trapdoor to the CRS. The `Prove` and `SimProve` algorithms differ only in the witness used: a real prover must use a real witness, while the simulator can use `trap` in a way that we will show is imperceptible to the environment. We formalize this intuition using an OR-protocol [24,26] over the original relation R and what we call a samplable-hard relation for the CRS.

Straight-Line Extraction and the Fischlin Transform. The original Fischlin transform [30] is a non-interactive transform for Σ-protocols in the stan-

[1] For a full discussion of the subtle differences between observation and programming privileges in the global ROM(s), see Appendix A.2 in the full version [37].

dard ROM that allows for *straight-line* (or *online*) extraction. Straight-line extraction is a process by which the extractor can produce a witness straight from a valid proof without any further interaction with the prover. (In order to do so, it will need additional, auxiliary information available to the extractor algorithm only.) This is in contrast to extraction in the "rewinding" model, in which the extractor resets the prover to a previous state and hopes for a certain pattern of interaction before it can obtain a witness. Straight-line extraction is necessary in the (G)UC model, which does not allow the simulator to rewind the environment [20]. Furthermore, straight-line extraction produces a tight reduction, which avoids security nuances surrounding the forking lemma [33].

In order to create a straight-line extractable proof system from a Σ-protocol, the Fischlin transform essentially forces the prover to rewind itself, requiring multiple proofs on repeated commitments until the probability that the prover has generated at least two responses to different challenges on the same commitment is overwhelming. Kondi and shelat recently showed that because the Fischlin prover is deterministic—that is, because it tests challenges by iterating from zero to some fixed constant—the original transform is open to a "replay" attack that breaks the the witness indistinguishability property of OR-protocols [35]. To avoid the attack, Fischlin's original construction requires the underlying Σ-protocols to have a property called *quasi-unique responses*, which Kondi and shelat demonstrate precludes the transformation of OR-protocols. Kondi and shelat show how this property can be omitted (and most OR-protocols transformed) by randomizing the challenge selection process and replacing the quasi-unique responses property with a (more general) property called *strong special soundness*. We review the details of the resulting "randomized" Fischlin transform [31,35] in Appendix A.12 of the full version of the paper [37].

2 Preliminaries

We use standard notation, available in Appendix A.1 of the full version [37].

2.1 Σ-protocols, Revisited

Let R be any efficiently computable binary relation. For pairs $(x, w) \in R$, or equivalently such that $R(x, w) = 1$, we call x a statement in the language of R, denoted L_R, and say w is a witness to $x \in L_R$. We consider Σ-protocols over a relation R between a prover P and a verifier V that have the general commit-challenge-respond format discussed in Section 1, which Damgård formalizes as a protocol template [26]. Since we will later introduce compilers for Σ-protocols—first to make them non-interactive and straight-line extractable and then to make them GUC—it will be helpful to define Σ-protocol interfaces with precise inputs and outputs. We begin by formalizing an algorithmic version of the protocol template τ as a tuple of algorithms $(\texttt{Setup}, \texttt{Commit}, \texttt{Challenge}, \texttt{Respond}, \texttt{Decision})$, the details of which are provided alongside Damgård's original version in Appendix A.3 [37].

Σ-protocols must also satisfy the properties of completeness, special honest-verifier zero-knowledge (SHVZK), and special soundness (SS). The SHVZK property requires the existence of a simulator algorithm `SimProve` for simulating proofs, and the SS property requires an extractor algorithm `Extract` for extracting witnesses. Therefore, our algorithmic specification of a Σ-protocol includes three additional algorithms: `SimSetup`, `SimProve`, and `Extract`.

In order to more easily translate our definition of Σ-protocols into the non-interactive setting, we combine the `Commit`, `Challenge`, and `Respond` algorithms of the protocol template into a `Prove` interface. For now we are still dealing with the interactive version, and the specification of `Prove` below is a two-party protocol where the first input to the algorithm is the prover's input, and the second input is the verifier's. After running `Prove`, both parties obtain the same copy of the proof transcript $\pi = (\texttt{com}, \texttt{chl}, \texttt{res})$. In the next section, we will introduce a straight-line compiler that makes the `Prove` interface a non-interactive algorithm in the random-oracle model (ROM). The non-interactive, straight-line extractable (NISLE) proof system resulting from the transformation will have different versions of the SHVZK and SS properties; because we will work almost exclusively with these versions, we defer formal definitions and discussions of the original formulations [26] to Appendix A.5 of the full version of the paper [37].

Definition 1 (Σ-protocol). *A* Σ-protocol for a relation R *based on a protocol template* τ *(Definition 15 in [37]) is a tuple of efficient procedures* $\Sigma_{R,\tau} = (\texttt{Setup}, \texttt{Prove}, \texttt{Verify}, \texttt{SimSetup}, \texttt{SimProve}, \texttt{Extract})$*, defined as follows.*

- $\texttt{ppm} \leftarrow \texttt{Setup}(1^\lambda)$*: Given a security parameter* 1^λ*, invoke* $\tau.\texttt{Setup}(1^\lambda)$ *to obtain the public parameters* `ppm`*.*
- $\pi \leftarrow \texttt{Prove}((\texttt{ppm}, x, w), (\texttt{ppm}, x))$*: Let the first (resp. second) argument to* `Prove` *be the input of the prover (resp. verifier), where both parties get* `ppm` *and the statement* x*, but only the prover gets* w*. P and V run* $\tau.\texttt{Commit}$*,* $\tau.\texttt{Challenge}$*, and* $\tau.\texttt{Respond}$*. Output* $\pi = (\texttt{com}, \texttt{chl}, \texttt{res})$*.*
- $\{0,1\} \leftarrow \texttt{Verify}(\texttt{ppm}, x, \pi)$*: Given a proof* π *for statemenet* x*, parse* π *as* $(\texttt{com}, \texttt{chl}, \texttt{res})$ *and output the result of running* $\tau.\texttt{Decision}$ *on input* $(x, \texttt{com}, \texttt{chl}, \texttt{res})$*.* `Verify` *must satisfy the* completeness property *from Definition 18 in Appendix A.5 of the full version of the paper [37].*
- $(\texttt{ppm}, z) \leftarrow \texttt{SimSetup}(1^\lambda)$*: Generate* `ppm` *and the simulation trapdoor* z*. Together,* `SimSetup` *and* `SimProve` *must satisfy the* special honest-verifier zero-knowledge property *from Definition 19 in Appendix A.5.*
- $\pi \leftarrow \texttt{SimProve}(\texttt{ppm}, z, x, \texttt{chl})$: *Given public parameters* `ppm`*, trapdoor* z*, statement* x*, and a challenge* `chl`*, produce a proof* $\pi = (\texttt{com}, \texttt{chl}, \texttt{res})$*.*
- $w \leftarrow \texttt{Extract}(\texttt{ppm}, x, \pi, \pi')$: *Given two proofs* $\pi = (\texttt{com}, \texttt{chl}, \texttt{res})$ *and* $\pi' = (\texttt{com}, \texttt{chl}', \texttt{res}')$ *for a statement* x *such that* $\tau.\texttt{Decision}(x, \pi) = \tau.\texttt{Decision}(x, \pi') = 1$ *and* $\texttt{chl} \neq \texttt{chl}'$*, output a witness* w*.* `Extract` *must satisfy the* special soundness property *from Definition 20 in Appendix A.5.*

For convenience and when the meaning is clear, we use Σ_R *to represent* $\Sigma_{R,\tau}$ *and omit* `ppm` *from the input of the algorithms.*

2.2 Straight-Line Compilers

Inspired by the straight-line transform due to Fischlin [31,30] described in Section 1, our formalization of a straight-line compiler (SLC) for Σ-protocols in the random-oracle model (ROM) takes any interactive Σ-protocol Σ_R for relation R and creates a non-interactive, straight-line extractable (NISLE) proof system $\Pi_R^{\mathtt{SLC}}$ for the same relation. Both the proof simulation and witness extraction procedures in a NISLE proof system are non-interactive *algorithms* in the ROM—the challenger in the security experiment may not rely on rewinding the prover, but is permitted to use the adversary's previous queries to the RO.

The non-interactive equivalent of the special honest-verifier zero-knowledge (SHVZK) game must reflect the fact that the zero-knowledge simulator might be programming the RO. The SHVZK property must continue to hold even as the RO is updated, meaning that if the simulator changes the RO at all, it must be done in a way that is imperceptible to to the adversary $\mathscr{A}$. Note that the definition does not imply that the simulator *has* to program the RO—just that if it does, it must do so imperceptibly. This nuance is important because we will later give a construction in Section 5.3 for GUC NIZKPoK in the (non-programmable) $\mathcal{G}_{\mathtt{roRO}}$-$\mathcal{F}_{\mathtt{CRS}}$-hybrid model—this construction should not (and does not) contradict our result from Theorem 1, which says that any GUC NIZKPoK must meet the requirements of non-interactive (multiple) SHVZK.

In the non-interactive version of the special soundness (SS) game in Fischlin's construction, the `Extract` algorithm works on input $(x, \pi, \mathcal{Q}_{\mathscr{A}})$, where $\mathcal{Q}_{\mathscr{A}}$ are $\mathscr{A}$'s queries to the RO. Fischlin's approach is not the only one for achieving straight-line extraction. Verifiable encryption [17,9] provides a different mechanism: the parameters `ppm` contain a public key, and the proof π contains an encryption of the witness under this key. The extractor's trapdoor is the decryption key. The latter approach requires additional machinery: it needs a proof system for proving that a plaintext of a particular ciphertext is a witness w, and thus cannot be constructed directly from Σ_R. It is the subject of future work to determine how such a "key-based" extractor would fare; for now, we assume the extractor works on the adversary's queries to the RO.

Finally, Fischlin proposes an optional (negligible) weakening of the completeness property, which we call overwhelming completeness, that allows protocol designers to optimize other parameters for efficiency reasons. Certainly any SLC that satisfies the regular notion of completeness will also satisfy the weaker notion, so we recall the weaker property below and demonstrate in Section 3.5 that it is sufficient for GUC NIZKPoK.

Definition 2 (Straight-Line Compiler). *An algorithm* `SLC` *is a* straight-line compiler (SLC) *in the random-oracle model if given any Σ-protocol Σ_R for relation R (Definition 1) as input, it outputs a tuple of* algorithms $\Pi_R^{\mathtt{SLC}} = (\mathtt{Setup}^H, \mathtt{Prove}^H, \mathtt{Verify}^H, \mathtt{SimSetup}, \mathtt{SimProve}, \mathtt{Extract})$ *with access to random oracle H that satisfy the following properties: overwhelming completeness (Definition 3), non-interactive multiple special honest-verifier zero-knowledge (Definition 4), and non-interactive special simulation-soundness (Definition 5).*

We refer to $\Pi_R^{\mathtt{SLC}} \leftarrow \mathtt{SLC}(\Sigma_R)$ *as a non-interactive, straight-line extractable (NISLE) proof system for* R*, and proofs generated by* $\Pi_R^{\mathtt{SLC}}$ *as non-interactive, straight-line extractable zero-knowledge proofs of knowledge (NISLE ZKPoK).*

Definition 3 (Overwhelming Completeness). *A NISLE proof system* $\Pi_R^{\mathtt{SLC}} = (\mathtt{Setup}^H, \mathtt{Prove}^H, \mathtt{Verify}^H, \mathtt{SimSetup}, \mathtt{SimProve}, \mathtt{Extract})$ *for relation* R *in the random-oracle model has the* overwhelming completeness *property if for any security parameter* λ*, any random oracle* H*, any* $(x, w) \in R$*, and any proof* $\pi \leftarrow \Pi_R^{\mathtt{SLC}}.\mathtt{Prove}^H(x, w)$*,*

$$\Pr[\Pi_R^{\mathtt{SLC}}.\mathtt{Verify}^H(x, \pi) = 1] \geq 1 - \mathsf{negl}(\lambda).$$

Recall from the introduction of this section that the simulator in the non-interactive version of the SHVZK experiment is allowed to program the RO. In order to precisely describe this programming, we differentiate in Figure 1 the traditional RO H_f, which is parameterized by a function $f \leftarrow_{\$} F$ selected from random function family F, from the programmable RO H_L, which is parameterized by a *list* L that can be added to (but not edited by) the simulator. We call this type of oracle a "Random List Oracle," and provide the simulator algorithms in the non-interactive SHVZK game oracle access to an interface $\mathtt{Prog}_L$, which allows the caller to map any (previously unmapped) input x to an output v of its choice. The adversary's inability to distinguish between the real-world oracle H_f that is simply a random function and the ideal-world oracle H_L that is a list managed by the simulator is an essential part of the non-interactive SHVZK experiment—it ensures that the introduction of the non-interactivity property (via queries to a programmable RO) does not compromise the SHVZK property.

RO $H_f(x)$	Random List Oracle $H_L(x)$	Interface $\mathtt{Prog}_L(x, v)$
1 : **return** $f(x)$	1 : **if** $\exists\ v$ **s.t.** $(x, v) \in L$:	1 : **if** $\nexists\ v'$ **s.t.** $(x, v') \in L$:
	2 : **return** v	2 : L.**append**(x, v)
	3 : **else** :	
	4 : $v \leftarrow \{0,1\}^{\ell}$	
	5 : L.**append**(x, v)	
	6 : **return** v	

Fig. 1. Random Oracle Functionalities for NIM-SHVZK and NI-SSS Games.

In the standard definition of SHVZK, $\mathscr{A}$ is only permitted to issue *one* `Prove` query. In the GUC security experiment (and in most natural applications of Σ-protocols), the environment is allowed to issue polynomially-many `Prove` queries, and we will still need the SHVZK property to hold. Therefore, we present a version of non-interactive *multiple* SHVZK (NIM-SHVZK) [30].

Definition 4 (Non-Interactive Multiple SHVZK). *A NISLE proof system* $\Pi_R^{\mathtt{SLC}} = (\mathtt{Setup}^H, \mathtt{Prove}^H, \mathtt{Verify}^H, \mathtt{SimSetup}, \mathtt{SimProve}, \mathtt{Extract})$ *for relation* R *in the random-oracle model has the* non-interactive multiple special honest-verifier zero-knowledge (NIM-SHVZK) *property if for any security parameter* λ*, any random oracle* H*, any* PPT *adversary* $\mathscr{A}$*, and a bit* $b \leftarrow_{\$} \{0,1\}$*, there exists some negligible function* negl *such that* $\Pr[b' = b] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$*, where* b' *is the result of running the game* $\mathsf{NIM\text{–}SHVZK}^{H_*,*}_{\mathscr{A},\Pi_R^{\mathtt{SLC}}}(1^\lambda, b)$ *from Figure 2. We say* $\mathscr{A}$ *wins the* NIM–SHVZK *game if* $\Pr[b' = b] > \frac{1}{2} + \mathsf{negl}(\lambda)$.

$\mathsf{NIM\text{–}SHVZK}^{H_*,F}_{\mathscr{A},\Pi_R^{\mathtt{SLC}}}(1^\lambda, 0)$: REAL

1 : $f \leftarrow_{\$} F$
2 : $\mathtt{ppm} \leftarrow \Pi_R^{\mathtt{SLC}}.\mathtt{Setup}^{H_f}(1^\lambda)$
3 : $\mathtt{st} \leftarrow \mathscr{A}^{H_f}(1^\lambda, \mathtt{ppm})$
4 : **while** $\mathtt{st} \notin \{0,1\}$:
5 : $\quad(\mathtt{Prove}, x, w, \mathtt{st}) \leftarrow \mathscr{A}^{H_f}(\mathtt{st})$
6 : $\quad$**if** $R(x,w) = 1$:
7 : $\quad\quad\pi \leftarrow \Pi_R^{\mathtt{SLC}}.\mathtt{Prove}^{H_f}(x,w)$
8 : $\quad$**else** :
9 : $\quad\quad\pi \leftarrow \perp$
10 : $\quad\mathtt{st} \leftarrow \mathscr{A}^{H_f}(\mathtt{st}, \pi)$
11 : **return** st

$\mathsf{NIM\text{–}SHVZK}^{H_*,\mathtt{Prog}}_{\mathscr{A},\Pi_R^{\mathtt{SLC}}}(1^\lambda, 1)$: IDEAL

1 : $L \leftarrow \perp$
2 : $\mathtt{ppm}, z \leftarrow \Pi_R^{\mathtt{SLC}}.\mathtt{SimSetup}^{\mathtt{Prog}_L}(1^\lambda)$
3 : $\mathtt{st} \leftarrow \mathscr{A}^{H_L}(1^\lambda, \mathtt{ppm})$
4 : **while** $\mathtt{st} \notin \{0,1\}$:
5 : $\quad(\mathtt{Prove}, x, w, \mathtt{st}) \leftarrow \mathscr{A}^{H_L}(\mathtt{st})$
6 : $\quad$**if** $R(x,w) = 1$:
7 : $\quad\quad\pi \leftarrow \Pi_R^{\mathtt{SLC}}.\mathtt{SimProve}^{\mathtt{Prog}_L}(z,x)$
8 : $\quad$**else** :
9 : $\quad\quad\pi \leftarrow \perp$
10 : $\quad\mathtt{st} \leftarrow \mathscr{A}^{H_L}(\mathtt{st}, \pi)$
11 : **return** st

Fig. 2. Non-Interactive Multiple SHVZK (NIM-SHVZK) Game.

Similarly, the environment in the ideal-world GUC experiment will have access to polynomially-many proofs generated by the SimProve algorithm, which $\mathcal{F}_{\mathtt{NIZK}}$ will use to simulate proofs. We therefore define our straight-line compilers to have the NI special *simulation* soundness property (NI-SSS), which says that special soundness must still hold even after an adversary has seen polynomially-many proofs from the simulator. Fischlin's original construction is both NIM-SHVZK and NI-SSS [30]. We will use his results in Section 6.1 to prove that the randomized Fischlin transform [35,30] is also NIM-SHVZK and NI-SSS.

Definition 5 (Non-Interactive Special Simulation-Soundness). *A NISLE proof system* $\Pi_R^{\mathtt{SLC}} = (\mathtt{Setup}^H, \mathtt{Prove}^H, \mathtt{Verify}^H, \mathtt{SimSetup}, \mathtt{SimProve}, \mathtt{Extract})$ *for relation* R *in the random-oracle model has the* non-interactive special simulation-soundness *property if for any security parameter* λ*, any random oracle* H*, and any* PPT *adversary* $\mathscr{A}$*, there exists some negligible function* negl *such that*

$$\Pr[\mathtt{Fail} \leftarrow \mathsf{NI\text{–}SSS}^{H_*,\mathtt{Prog}}_{\mathscr{A},\Pi_R^{\mathtt{SLC}}}(1^\lambda)] \leq \mathsf{negl}(\lambda),$$

where $\mathsf{NI\text{–}SSS}$ *is the game described in Figure 3. We say* $\mathscr{A}$ *wins if* $\Pr[\texttt{Fail} \leftarrow \mathsf{NI\text{–}SSS}^{H_*,\texttt{Prog}}_{\mathscr{A},\Pi_R^{\mathsf{SLC}}}(1^\lambda)] > \mathsf{negl}(\lambda)$.

$\mathsf{NI\text{–}SSS}^{H_*,\texttt{Prog}}_{\mathscr{A},\Pi_R^{\mathsf{SLC}}}(1^\lambda)$

$L \leftarrow \bot$
$\texttt{ppm}, z \leftarrow \Pi_R^{\mathsf{SLC}}.\texttt{SimSetup}^{\texttt{Prog}_L}(1^\lambda)$
$\texttt{st} \leftarrow \mathscr{A}^{H_L}(1^\lambda, \texttt{ppm})$
$\texttt{pflist}, \texttt{Response} \leftarrow \bot$
while $\texttt{st} \neq \bot$:
  $(\texttt{Query}, \mathcal{Q}_\mathscr{A}, \texttt{st}) \leftarrow \mathscr{A}^{H_L}(\texttt{st})$
  if $\texttt{Query} = (\texttt{Prove}, x, w)$:
    if $R(x, w) = 1$:
      $\pi \leftarrow \Pi_R^{\mathsf{SLC}}.\texttt{SimProve}^{\texttt{Prog}_L}(z, x)$
      $\texttt{pflist}.\textbf{append}(x, \pi)$
      $\texttt{Response} \leftarrow (x, \pi)$
  elseif $\texttt{Query} = (\texttt{Challenge}, x, \pi)$
    if $\Pi_R^{\mathsf{SLC}}.\texttt{Verify}^{H_L}(x, \pi) = 1 \wedge (x, \pi) \notin \texttt{pflist}$:
      $w \leftarrow \Pi_R^{\mathsf{SLC}}.\texttt{Extract}(x, \pi, \mathcal{Q}_\mathscr{A})$
      if $R(x, w) = 0$:
        return Fail
  $\texttt{st} \leftarrow \mathscr{A}^{H_L}(\texttt{st}, \texttt{Response})$
return Success

Fig. 3. Non-Interactive Special simulation-soundness (NI-SSS) Game.

Σ-protocols that maintain the SHVZK property under any non-interactive transform in the ROM must additionally have com messages with entropy that is superlogarithmic in the security parameter [31], such that the adversary cannot exhaustively query commitments to the RO and check whether the challenge supplied by the prover matches what it receives. We recall and discuss Fischlin's *superlogarithmic commitment entropy* property further in Appendix A.7 [37].

2.3 OR-protocols

Rather than producing a proof corresponding to a single statement x in a language L_R, the prover in an OR-protocol proves that it knows a witness for *either* a statement x_0 in L_{R_0} *or* another statement x_1 in L_{R_1}. At a high level, the prover does this by simulating the proof of the statement for which it does not have

a witness, while computing the proof of the statement for which it *does* have a witness honestly.

Our definition is adapted directly from Damgård's [26], with a few minor tweaks to make it more general. Since we will use the OR-protocol functionality as a black box in our construction, it suffices for the purpose of understanding our results to treat the OR-protocol as a Σ-protocol (according to Definition 1) with *compound inputs*. For example, we represent the compound statement $x_0 \vee x_1$ with the upper-case variable $X = (x_0, x_1)$. The witness $W = (w, b)$ includes a witness along with a bit b such that $(x_b, w) \in R_b$. We provide the detailed version of our definition alongside Damgård's, as well as a discussion of the minor differences between them, in Appendix A.8 of the full version [37].

3 Properties of GUC NIZKPoK

In this section we formalize the definitions of the programmable global RO $\mathcal{G}_{\texttt{rpoRO}}$ and the observable global RO $\mathcal{G}_{\texttt{roRO}}$, the ideal NIZKPoK functionality $\mathcal{F}_{\texttt{NIZK}}$, the CRS ideal functionality $\mathcal{F}_{\texttt{CRS}}$, and the security requirements for protocols that GUC-realize $\mathcal{F}_{\texttt{NIZK}}$ in the $\mathcal{G}_{\texttt{rpoRO}}$- and $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid models. We then show that the non-interactive multi-SHVZK and non-interactive special simulation-soundness properties are *strictly necessary* to obtain GUC NIZKPoK in any global ROM.

3.1 $\mathcal{G}_{\texttt{roRO}}$ and $\mathcal{G}_{\texttt{rpoRO}}$, Revisited

Building on the overview of the global ROM(s) given in Section 1, we now formalize Canetti et al.'s restricted observable global RO $\mathcal{G}_{\texttt{roRO}}$ [22] and Camenisch et al.'s restricted programmable observable global RO $\mathcal{G}_{\texttt{rpoRO}}$. As with traditional ROs, both oracles act as functions that respond to each input string $x_i \in \{0,1\}^*$ with a uniformly random ℓ-bit string $v_i \in \{0,1\}^\ell$. We call this original algorithm `Query`. Since $\mathcal{G}_{\texttt{rpoRO}}$ builds on the interfaces of $\mathcal{G}_{\texttt{roRO}}$, we will start with the specification of $\mathcal{G}_{\texttt{roRO}}$ and follow with the extra interfaces of $\mathcal{G}_{\texttt{rpoRO}}$.

The first thing $\mathcal{G}_{\texttt{roRO}}$ does when it receives a query is to check whether the querent's SID `sid` matches the session s for which it has requested randomness. If $\texttt{sid} \neq s$, $\mathcal{G}_{\texttt{roRO}}$ assumes this is an "illegitimate" query made by the environment, and records the query in its special list of illegitimate queries for s, denoted $\mathcal{Q}_s$. In the original version of the definition [22], only the ideal functionality $\mathcal{F}^s$ for session s can query $\mathcal{G}_{\texttt{roRO}}$ using the `Observe` interface to get the list of illegitimate queries for s. However, note that no honest provers' queries will ever be recorded in this list, as they will only ever be querying $\mathcal{G}_{\texttt{roRO}}$ for randomness sessions in which they are participating legitimately. Therefore, we follow Camenisch et al.'s version of the restricted observability property [10] and simply release the list $\mathcal{Q}_s$ to anyone who wants it.

Definition 6 (Observable Global RO $\mathcal{G}_{\texttt{roRO}}$). [22,10] *The* observable global RO $\mathcal{G}_{\texttt{roRO}}$ *is a tuple of algorithms* $(\texttt{Query}, \texttt{Observe})$ *defined over an output length* ℓ *and an initially empty list of queries* $\mathcal{Q}$*:*

- $v \leftarrow \texttt{Query}(x)$: *Parse* x *as* (s, x') *where* s *is an SID. If a list* $\mathcal{Q}_s$ *of illegitimiate queries for* s *does not yet exist, set* $\mathcal{Q}_s = \perp$. *If the caller's SID* $\neq s$, *add* (x, v) *to* $\mathcal{Q}_s$. *If there already exists a pair* (x, v) *in the query list* $\mathcal{Q}$, *return* v. *Otherwise, choose* v *uniformly at random from* $\{0,1\}^\ell$, *store the pair* (x, v) *in* $\mathcal{Q}$, *and return* v.
- $\mathcal{Q}_s \leftarrow \texttt{Observe}(s)$: *If a list* $\mathcal{Q}_s$ *of illegitimate queries for* s *does not yet exist, set* $\mathcal{Q}_s = \perp$. *Return* $\mathcal{Q}_s$.

In addition to the `Query` and `Observe` interfaces, Camenisch et al.'s restricted *programmable* observable global RO $\mathcal{G}_{\texttt{rpoRO}}$ has two extra interfaces, `Program` and `IsProgrammed`. $\mathcal{G}_{\texttt{rpoRO}}$ keeps track of which queries have been programmed using the set `prog`. Note that since privileged (simulator-only) programming is not allowed in the GUC model, anyone can program $\mathcal{G}_{\texttt{rpoRO}}$. In order to functionally restrict this privilege to the simulator, Camenisch et al. introduces the `IsProgrammed` interface, which reveals whether or not $\mathcal{G}_{\texttt{rpoRO}}$ was programmed on an index $x = (s, x')$, but only to a calling party with $\texttt{sid} = s$. Notably, this interface directly restricts the environment from ever seeing whether or not the oracle was programmed (since the environment is by definition not part of any legitimate protocol session), and indirectly restricts the adversary from ever seeing whether or not the oracle was programmed (since the simulator is in charge of its view in the ideal-world experiment in which programming is employed.)

Definition 7 (Restricted Programmable Observable Global RO $\mathcal{G}_{\texttt{rpoRO}}$). [10] *The* restricted programmable observable global random oracle $\mathcal{G}_{\texttt{rpoRO}}$ *is a tuple of algorithms* $(\texttt{Query}, \texttt{Observe}, \texttt{Program}, \texttt{IsProgrammed})$ *defined over an output length* ℓ *and initially empty lists* $\mathcal{Q}$ *(queries) and* `prog` *(programmed queries):*

- $v \leftarrow \texttt{Query}(x)$: *Same as Definition 6 above.*
- $\mathcal{Q}_s \leftarrow \texttt{Observe}(s)$: *Same as Definition 6 above.*
- $\{0,1\} \leftarrow \texttt{Program}(x, v)$: *If* $\exists v' \in \{0,1\}^\ell$ *such that* $(x, v') \in \mathcal{Q}$ *and* $v \neq v'$, *output* 0. *Otherwise, add* (x, v) *to* $\mathcal{Q}$ *and* `prog` *and output* 1.
- $\{0,1\} \leftarrow \texttt{IsProgrammed}(x)$: *Parse* x *as* (s, x'). *If the caller's SID* $\neq s$, *output* $\perp$. *Otherwise if* $x \in \texttt{prog}$, *output* 1. *Otherwise, output* 0.

3.2 The NIZKPoK Ideal Functionality

We now formalize the NIZKPoK ideal functionality $\mathcal{F}_{\texttt{NIZK}}$. Recall from Section 1 that in the "ideal" world, the honest parties who would execute protocol Π are actually dummy parties who do not perform any computations of their own. Instead, they pass all of their inputs to an ideal functionality $\mathcal{F}_{\texttt{NIZK}}$, who instructs them on how to respond. As is standard in the (G)UC framework [19,20,22], there is one ideal functionality for each SID s. A dummy party with SID s can only send input and receive output from the $\mathcal{F}_{\texttt{NIZK}}$ with the same SID, denoted $\mathcal{F}^s_{\texttt{NIZK}}$.

Each $\mathcal{F}^s_{\texttt{NIZK}}$ will need to run some kind of setup, then process proofs and verifications on behalf of the honest parties in its session. Recall that in order to be NIZKPoK, the proofs must be *non-interactive*, *zero-knowledge* (satisfying

the SHVZK property), and *proofs of knowledge* (satisfying the SS property). These properties imply the existence of SHVZK simulator algorithms $\texttt{SimSetup}$ and $\texttt{SimProve}$ that do not take the prover's witness as input, as well as of the SS algorithm $\texttt{Extract}$ that can compute witnesses from adversarially-created proofs. During $\mathcal{F}_{\texttt{NIZK}}$'s **Setup** procedure, $\mathcal{F}_{\texttt{NIZK}}$ requests the specifications of these algorithms from the ideal adversary (simulator) $\mathcal{S}$.

Note that there are two conditions in which $\mathcal{F}_{\texttt{NIZK}}$ can output $\texttt{Fail}$. The first is a completeness error, where $\mathcal{F}_{\texttt{NIZK}}$'s execution of the $\texttt{SimProve}$ algorithm on input $(x, w) \in R$ fails to produce a proof π such that $\texttt{Verify}(x, \pi) = 1$. The second is an extraction error, where $\mathcal{F}_{\texttt{NIZK}}$'s execution of the $\texttt{Extract}$ algorithm on input a valid, non-simulated proof tuple (x, π) fails to produce a witness w such that $R(x, w) = 1$. In the proof of Theorem 1 in Section 3.5, we will draw a direct correspondence between these failures and the functionality of a Σ-protocol.

Definition 8 (NIZKPoK Ideal Functionality). *The ideal functionality $\mathcal{F}_{\texttt{NIZK}}$ of a* non-interactive zero-knowledge proof of knowledge (NIZKPoK) *is defined as follows.*

Setup: *Upon receiving the request* $(\texttt{Setup}, s)$ *from a party* $P = (\texttt{pid}, \texttt{sid})$*, first check whether* $\texttt{sid} = s$*. If it doesn't, output* $\perp$*. Otherwise, if this is the first time that* $(\texttt{Setup}, s)$ *was received, pass* $(\texttt{Setup}, s)$ *to the ideal adversary* $\mathcal{S}$*, who returns the tuple* $(\texttt{Algorithms}, s, \texttt{Setup}, \texttt{Prove}, \texttt{Verify}, \texttt{SimSetup}, \texttt{SimProve}, \texttt{Extract})$ *with definitions for the algorithms* $\mathcal{F}_{\texttt{NIZK}}$ *will use.* $\mathcal{F}_{\texttt{NIZK}}$ *stores the tuple.*

Prove: *Upon receiving a request* $(\texttt{Prove}, s, x, w)$ *from a party* $P = (\texttt{pid}, \texttt{sid})$*, first check that* $\texttt{sid} = s$ *and* $R(x, w) = 1$*. If not, output* $\perp$*. Otherwise, compute* π *according to the* $\texttt{SimSetup}$ *and* $\texttt{SimProve}$ *algorithms and check that* $\texttt{Verify}(x, \pi) = 1$*. If it doesn't, output* $\texttt{Fail}$*. Otherwise, record then output the message* $(\texttt{Proof}, s, x, \pi)$*.*

Verify: *Upon receiving a request* $(\texttt{Verify}, s, x, \pi)$ *from a party* $P = (\texttt{pid}, \texttt{sid})$*, first check that* $\texttt{sid} = s$*. If it doesn't, output* $\perp$*. Otherwise if* $\texttt{Verify}(x, \pi) = 0$*, output* $(\texttt{Verification}, s, x, \pi, 0)$*. Otherwise if* $(\texttt{Proof}, s, x, \pi)$ *is already stored, output* $(\texttt{Verification}, s, x, \pi, 1)$*. Otherwise, compute* w *according to the* $\texttt{Extract}$ *algorithm. If* $R(x, w) = 1$*, output* $(\texttt{Verification}, s, x, \pi, 1)$ *for a successful extraction. Else if* $R(x, w) = 0$*, output* $\texttt{Fail}$*.*

3.3 The CRS Ideal Functionality

Below is the ideal common reference string (CRS) functionality, which relies on a generic "$\texttt{GenCRS}$" algorithm. In Section 5.1, we will articulate the properties that $\texttt{GenCRS}$ must have for the purposes of our construction.

Definition 9 (CRS Ideal Functionality). *The ideal functionality $\mathcal{F}_{\texttt{CRS}}$ of a* common reference string (CRS) *for a particular CRS generation mechanism* $\texttt{GenCRS}$ *is defined as follows.*

Query: *Upon receiving a request* $(\texttt{Query}, s)$ *from a party* $P = (\texttt{pid}, \texttt{sid})$*, first check whether* $\texttt{sid} = s$*. If it doesn't, output* $\perp$*. Otherwise, if this is the first time that* $(\texttt{Query}, s)$ *was received, compute* x *according to the algorithm* `GenCRS` *and store the tuple* $(\texttt{CRS}, s, x)$*. Return* $(\texttt{CRS}, s, x)$*.*

3.4 GUC Security Definitions

We are now ready to formalize what it means for a protocol Π to be a GUC NIZKPoK in the $\mathcal{G}_{\texttt{rpoRO}}$- and $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid models. We review the standard GUC model real- and ideal-world experiments given by Canetti et al. [20] in Appendix A.9 of the full version of the paper [37], noting that we are working in the *passive corruption model*—i.e. $\mathcal{Z}$ must decide at the time of a party's invocation whether or not they are corrupt.

Definition 10 (GUC NIZKPoK in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid Model). *A protocol* $\Pi = (\texttt{Setup}, \texttt{Prove}, \texttt{Verify}, \texttt{SimSetup}, \texttt{SimProve}, \texttt{Extract})$ *with security parameter* λ GUC-realizes the NIZKPoK ideal functionality $\mathcal{F}_{\texttt{NIZK}}$ in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model *if for all efficient* $\mathscr{A}$*, there exists an ideal adversary* $\mathcal{S}$ *efficient in expectation such that for all efficient environments* $\mathcal{Z}$*,*

$$\mathsf{IDEAL}^{\mathcal{G}_{\texttt{rpoRO}}}_{\mathcal{F}_{\texttt{NIZK}},\mathcal{S},\mathcal{Z}}(1^\lambda, \texttt{aux}) \approx_c \mathsf{REAL}^{\mathcal{G}_{\texttt{rpoRO}}}_{\Pi,\mathscr{A},\mathcal{Z}}(1^\lambda, \texttt{aux}),$$

where $\mathcal{G}_{\texttt{rpoRO}}$ *is the restricted programmable observable global RO (Definition 7) and* `aux` *is any auxiliary information provided to the environment.*

Definition 11 (GUC NIZKPoK in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid Model). *A protocol* $\Pi = (\texttt{Setup}, \texttt{Prove}, \texttt{Verify}, \texttt{SimSetup}, \texttt{SimProve}, \texttt{Extract})$ *with security parameter* λ GUC-realizes *the NIZKPoK ideal functionality* $\mathcal{F}_{\texttt{NIZK}}$ *in the* $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$ *hybrid model if for all efficient* $\mathscr{A}$*, there exists an ideal adversary* $\mathcal{S}$ *efficient in expectation such that for all efficient environments* $\mathcal{Z}$*,*

$$\mathsf{IDEAL}^{\mathcal{G}_{\texttt{roRO}}}_{\mathcal{F}_{\texttt{NIZK}},\mathcal{S},\mathcal{Z}}(1^\lambda, \texttt{aux}) \approx_c \mathsf{REAL}^{\mathcal{G}_{\texttt{roRO}},\mathcal{F}_{\texttt{CRS}}}_{\Pi,\mathscr{A},\mathcal{Z}}(1^\lambda, \texttt{aux}),$$

where $\mathcal{G}_{\texttt{roRO}}$ *is the restricted observable global RO (Definition 6),* $\mathcal{F}_{\texttt{CRS}}$ *is the ideal CRS functionality (Definition 9), and* `aux` *is any auxiliary information provided to the environment.*

3.5 GUC NIZKPoK Are Complete, NIM-SHVZK, and NI-SSS

We prove in this section that any protocol $\Pi = (\texttt{Setup}, \texttt{Prove}, \texttt{Verify}, \texttt{SimSetup}, \texttt{SimProve}, \texttt{Extract})$ that GUC-realizes $\mathcal{F}_{\texttt{NIZK}}$ in *any* global ROM must be overwhelmingly complete, non-interactive multiple special honest-verifier zero-knowledge (NIM-SHVZK) and non-interactive special simulation simulation-sound (NI-SSS) according to the definitions in Section 2.2. In other words, the NIM-SHVZK and NI-SSS properties guaranteed by a straight-line compiler (SLC) are *strictly necessary* to create GUC NIZKPoK in the global ROM.

As we show briefly in Appendix B.1 [37], any ordinary Σ-protocol that is regular SHVZK is also multi-SHVZK. The more interesting result is the necessity of special simulation-soundness, since that is not a property guaranteed by all Σ-protocols—it will be up to the SLC to create a special simulation-sound NISLE proof system even when the underlying Σ-protocol is only regular special-sound. In the proof of Theorem 3 in the full version of his paper [30], Fischlin shows that the NISLE proof systems resulting from his transform satisfy both NIM-SHVZK and NI-SSS. A key element in Fischlin's proof that will surface again in the proof of Theorem 1 below, as well as in the proofs of Theorems 3 and 4, is the observation that an `Extract` algorithm based on the adversary's query history functionally decouples the extraction process from the rest of the experiment—interacting with the extractor does not influence the adversary's view in any way. Intuitively, this is because `Extract` works solely using inputs that the adversary already knows.

Since the following result is independent of the choice of global RO, we recall the strict global RO $\mathcal{G}_{\texttt{sRO}}$ outlined by Canetti et al. [22] and formalized by Camenisch et al. [10] described in the introduction. $\mathcal{G}_{\texttt{sRO}}$ has the same parameters as $\mathcal{G}_{\texttt{rpoRO}}$ and $\mathcal{G}_{\texttt{roRO}}$ but only one interface, `Query`, which acts as globally accessible random function. The functionality of $\mathcal{G}_{\texttt{sRO}}$ is the minimal-most assumption of an RO in the GUC model, creating a direct correspondence to the standard RO H in the NIM-SHVZK and NI-SSS experiments. Because the point of using $\mathcal{G}_{\texttt{sRO}}$ here is to convey the *minimal* assumption needed (and not to prove the result *only* for $\mathcal{G}_{\texttt{sRO}}$), we use the generic notation $\mathcal{G}_{\texttt{RO}}$, which represents any global RO with a minimum of $\mathcal{G}_{\texttt{sRO}}$'s `Query` interface. The GUC security definition in the $\mathcal{G}_{\texttt{RO}}$-hybrid model is the same as in Definition 10, except that $\mathcal{G}_{\texttt{rpoRO}}$ is replaced with $\mathcal{G}_{\texttt{RO}}$ in the notation.

Theorem 1. *Let Π be a protocol that GUC-realizes $\mathcal{F}_{\texttt{NIZK}}$ in the $\mathcal{G}_{\texttt{RO}}$-hybrid model (Definition 10 where $\mathcal{G}_{\texttt{rpoRO}}$ is replaced with $\mathcal{G}_{\texttt{RO}}$). Then Π must be overwhelmingly complete (Definition 3), NIM-SHVZK (Definition 4) and NI-SSS (Definition 5).*

Proof Sketch. We proceed by cases and show that if Π is not overwhelmingly complete and NIM-SHVZK then it does not GUC-realize $\mathcal{F}_{\texttt{NIZK}}$, and similarly that if Π is not NI-SSS then it does not GUC-realize $\mathcal{F}_{\texttt{NIZK}}$. The full proof is available in Appendix B.2 of the full version of the paper [37].

In the first half of the proof, we construct a reduction that uses an adversary $\mathscr{A}$ that can win the NIM-SHVZK experiment from Figure 2 with non-negligible advantage to determine whether it is living in the real- or ideal-world GUC experiment. The reduction forwards $\mathscr{A}$'s oracle queries to and from $\mathcal{G}_{\texttt{RO}}$ and `Prove` queries to the GUC challenger, returning the proofs it receives back to $\mathscr{A}$. We note that since the reduction has no control over $\mathcal{G}_{\texttt{RO}}$, its view of $\mathcal{G}_{\texttt{RO}}$ is exactly the same as $\mathscr{A}$'s, so anything $\mathscr{A}$ can learn about the proofs from interacting with $\mathcal{G}_{\texttt{RO}}$, the reduction can also learn. Furthermore if the GUC challenger is running the ideal-world experiment and $\mathcal{F}_{\texttt{NIZK}}$ outputs `Fail` (indicating that `Simulate` failed to compute a valid proof for a statement-witness pair $(x, w) \in R$), the

reduction can immediately tell it is living in the ideal world. As long as $\mathcal{F}_{\texttt{NIZK}}$ does not produce `Fail`, the reduction simulates $\mathscr{A}$'s exact view of the challenger in the NIM-SHVZK game and succeeds in distinguishing the real- from ideal-world GUC experiments with the same probability as $\mathscr{A}$.

The second reduction uses an $\mathscr{A}$ that can win the NI-SSS game from Figure 3 with non-negligible advantage in order to distinguish between the GUC experiments. This reduction proceeds similarly to the last, forwarding all of $\mathscr{A}$'s queries to the relevant parties. The argument regarding the reduction's view of $\mathcal{G}_{\texttt{RO}}$ is identical to the argument above. In this case, however, there is a nuance to $\mathscr{A}$'s view: the regular NI–SSS challenger always produces *simulated* proofs, while the reduction will only produce simulated proofs if the GUC challenger is running the ideal-world experiment. We argue that in the case that the GUC challenger is running the real-world experiment, $\mathscr{A}$'s view from the reduction reduces to the regular non-interactive special soundness property given in Appendix A.6 [37], in which $\mathscr{A}$ can only run the regular `Prove` algorithm itself (and does not have oracle access to the simulator). The reduction therefore runs two copies of $\mathscr{A}$, returning proofs from the GUC challenger to the first copy $\mathscr{A}$ and generating proofs for the second copy $\mathscr{A}'$ itself using Π.`Prove`. If the GUC challenger is running the ideal-world experiment, the reduction is able to simulate $\mathscr{A}$'s exact view of the NI-SSS game, and the reduction will be able to determine that it is living in the ideal-world experiment with the same probability that $\mathscr{A}$ is able to output a proof that causes $\mathcal{F}_{\texttt{NIZK}}$'s `Extract` algorithm to output `Fail`. If the GUC challenger is running the real-world experiment and $\mathscr{A}'$ can output a valid proof such that Π.`Extract` fails but the GUC challenger does not fail, the reduction knows it is playing against the real-world GUC challenger, and can therefore distinguish the experiments with the same probability that $\mathscr{A}'$ succeeds in winning the NI-SS game.

Note that in order to check the result of Π.`Extract` against the GUC challenger's verification, the reduction must be able to be able to compute Π.`Extract` itself, which it can only do because it operates using $\mathcal{Q}_{\mathscr{A},\mathscr{A}'}$. It is the subject of future work to attempt the reduction in the case that the `Extract` algorithm requires a secret decryption key, as discussed in Section 2.2. Finally, note the reduction would not work if Π were *only* SS, since the adversary in the NI-SS game does not have well-defined behavior with respect to simulated proofs. □

4 GUC NIZKPoK in the Programmable Global ROM

We will now prove that any straight-line compiler (SLC) is sufficient to transform any Σ-protocol into a GUC NIZKPoK in the the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model.

Theorem 2. *Let Σ_R be any Σ-protocol for relation R (Definition 1), $\mathcal{G}_{\texttt{rpoRO}}$ be the restricted programmable observable global random oracle (Definition 6), and* `SLC` *be any straight-line compiler (Definition 2). Then the NISLE proof system $\Pi_R^{\texttt{SLC}} \leftarrow \texttt{SLC}(\Sigma_R)$ GUC-realizes $\mathcal{F}_{\texttt{NIZK}}$ in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model (Definition 10).*

Proof Sketch. In the ideal-world experiment, our simulator $\mathcal{S}$ hands the ideal functionality $\mathcal{F}_{\texttt{NIZK}}$ the tuple of algorithms $\Pi_R^{\texttt{SLC}}$, returns `false` to the corrupted

parties' `IsProgrammed` queries, and otherwise functions as a dummy adversary, forwarding communications between the environment and the protocol.

We proceed by creating a hybrid reduction starting in the real-world experiment that replaces each piece of the real-world protocol $\Pi_R^{\mathtt{SLC}}$ with the functionality of $\mathcal{F}_{\mathtt{NIZK}}$. First, we replace all of the environment's and adversary's connections to the real-world protocol participants with the "challenger" of our reduction, $\mathcal{C}$. This difference is syntactic, so the first two hybrids are identical.

In the next hybrid, we replace $\mathcal{C}$'s `Prove` functionality with the **Prove** interface of $\mathcal{F}_{\mathtt{NIZK}}$, and show the environment's views are indistinguishable between these experiments as long as $\Pi_R^{\mathtt{SLC}}$ has the non-interactive multiple special honest-verifier zero-knowledge (NIM-SHVZK) property. The reduction proceeds as follows. First, $\mathcal{C}$ always returns `false` to any of the adversary's `IsProgrammed` queries. As long as 1) $\Pi_R^{\mathtt{SLC}}.\mathtt{SimProve}$ produces valid proofs for statements $x \in L_R$ with overwhelming probability (which follows from overwhelming completeness), and 2) the environment's view of $\mathcal{G}_{\mathtt{rpoRO}}$ remains statistically indistinguishable between the hybrids (which follows from the NIM-SHVZK property and the restriction of the `IsProgrammed` interface), it remains to show that the outputs of $\Pi_R^{\mathtt{SLC}}.\mathtt{Prove}$ and $\Pi_R^{\mathtt{SLC}}.\mathtt{SimProve}$ are similarly indistinguishable. If the outputs are *statistically* indistinguishable—i.e. if Σ_R is statistical SHVZK and `SLC` preserves this property such that $\Pi_R^{\mathtt{SLC}}$ is statistical NIM-SHVZK—we are done. In the event that $\Pi_R^{\mathtt{SLC}}$ is only *computationally* NIM-SHVZK, we construct a (tight) reduction that uses an environment that can distinguish the two hybrids to win the NIM-SHVZK game from Figure 2. The reduction simply proceeds by forwarding all of the environment's RO queries to $\mathcal{G}_{\mathtt{rpoRO}}$, all `Prove` queries to the NIM-SHVZK challenger, and answering `Verify` queries itself by running $\Pi_R^{\mathtt{SLC}}.\mathtt{Verify}$. If the NIM-SHVZK challenger is playing with bit $b = 0$ and the proofs are according to $\Pi_R^{\mathtt{SLC}}.\mathtt{Prove}$, the reduction produces the environment's exact view of the first hybrid; otherwise if $b = 1$ and the proofs are according to $\Pi_R^{\mathtt{SLC}}.\mathtt{SimProve}$, it produces a view of the second hybrid. Therefore, our reduction succeeds with the same probability as the hybrid-distinguisher environment, contradicting the NIM-SHVZK property of $\Pi_R^{\mathtt{SLC}}$.

In the penultimate hybrid, we replace $\mathcal{C}$'s `Verify` functionality with the **Verify** interface of $\mathcal{F}_{\mathtt{NIZK}}$, and show the environment's views are computationally indistinguishable between these hybrids as long as $\Pi_R^{\mathtt{SLC}}$ has the non-interactive special simulation-soundness (NI-SSS) property. Recall that the **Verify** functionality of $\mathcal{F}_{\mathtt{NIZK}}$ uses the $\Pi_R^{\mathtt{SLC}}.\mathtt{Extract}$ algorithm, and fails whenever the witness extracted from a valid (non-simulated) proof is such that $R(x, w) = 0$. Our reduction uses an environment that can distinguish the simulate-only hybrid from the simulate-and-extract hybrid as a black-box to produce a proof that wins the NI-SSS game from Figure 3 as follows.

For `Prove` queries, the reduction simulates proofs according to either hybrid (both use $\Pi_R^{\mathtt{SLC}}.\mathtt{SimProve}$). Any time the environment wants to verify a proof that the reduction did not create itself, it gathers the environment's queries (which are freely available—recall that all of the environment's wires pass through $\mathcal{C}$) and sends the proof along with the environment's queries to the

NI-SSS challenger. Note that since the only difference between the hybrids is that the second hybrid can output `Fail` while the first never does, the only way for the environment to distinguish between them is to produce such a failure by outputting a valid (non-simulated) proof that causes $\Pi_R^{\mathtt{SLC}}.\mathtt{Extract}$ to fail. Since the challenger in the NI-SSS game also uses the $\Pi_R^{\mathtt{SLC}}.\mathtt{Extract}$ algorithm, the reduction succeeds with the same probability as the environment, contradicting the NI-SSS property and proving that the hybrids must be computationally indistinguishable.

The final step is to replace $\mathcal{C}$ with $\mathcal{F}_{\mathtt{NIZK}}$ and $\mathcal{S}$. Note that since $\mathcal{C}$ already runs the algorithms of $\mathcal{F}_{\mathtt{NIZK}}$ and returns `false` to corrupted parties' `IsProgrammed` queries, this is again only a syntactic difference, and the last two hybrids are identical. The full proof is available in Appendix B.3 of the full version of the paper [37]. □

5 GUC NIZKPoK in the Observable Global ROM

Recall from Section 1 that in order to avoid the session-localized `IsProgrammed` interface, we pursue GUC NIZKPoK in the $\mathcal{G}_{\mathtt{roRO}}$-$\mathcal{F}_{\mathtt{CRS}}$-hybrid model, where $\mathcal{F}_{\mathtt{CRS}}$ is the ideal CRS functionality from Section 3.3. We begin by discussing the specific properties of $\mathcal{F}_{\mathtt{CRS}}$'s CRS generation mechanism `GenCRS`, then introduce a compiler that creates GUC NIZKPoK from any Σ-protocol and any SLC in the $\mathcal{G}_{\mathtt{roRO}}$-$\mathcal{F}_{\mathtt{CRS}}$-hybrid model.

5.1 Generating a CRS that Plays Nice with Σ-protocols

In our construction, the prover convinces the verifier that either it knows a "real" witness, or else it knows the trapdoor to the CRS. In the real world, nobody knows the trapdoor (as long as the CRS is generated securely, for instance using Canetti et al.'s NISC protocol and only $\mathcal{G}_{\mathtt{roRO}}$ [22]). Therefore, all proofs executed by the regular `Prove` algorithm will be using real witnesses. In the ideal world, the simulator gets to generate the CRS for each session s with a trapdoor as part of the `SimProve` algorithm. `SimProve` is otherwise the same as `Prove`, except the witness is always the trapdoor for the CRS.

In order for this OR-proof to work, `Prove` and `SimProve` must be able to interpret the CRS as a statement $x = \mathtt{CRS}_s$ with a corresponding trapdoor witness $w = \mathtt{trap}_s$, such that the pair $(\mathtt{CRS}_s, \mathtt{trap}_s)$ satisfies some binary $\mathcal{NP}$ relation S. For efficiency purposes (since the simulator must run in polynomial-time) the CRS must be efficiently computable, and for security purposes, the trapdoor must be difficult to compute from the CRS. We call a relation that satisfies the efficiency property *samplable* and a relation that satisfies the security property *hard*. The intuition is similar to that of Fischlin's one-way instance generator [31].

Definition 12 (Samplable-Hard Relation). *A binary $\mathcal{NP}$ relation S is* samplable-hard *with respect to a security parameter λ if it has the following properties.*

1. **Sampling a statement-witness pair is easy.** *There exists a sampling algorithm* κ_S *that on input* 1^λ *outputs* (x, w) *such that* $S(x, w) = 1$ *and* $|x| = \mathsf{poly}(\lambda)$.
2. **Computing a witness from a statement is hard.** *For a randomly sampled statement-witness pair* $(x, w) \leftarrow \kappa_S(1^\lambda)$ *the probability that an efficient adversary* $\mathscr{A}$ *can find a valid witness given only the statement is negligible. Formally, for all PPT* $\mathscr{A}$*,*

$$\Pr[(x, w) \leftarrow \kappa_S(1^\lambda), w' \leftarrow \mathscr{A}(1^\lambda, x, \kappa_S) : (x, w') \in R] \leq \mathsf{negl}(\lambda).$$

Finally, we require that the relation S underlying the CRS has an efficient corresponding Σ-protocol Σ_S. Our construction will instantiate an OR-protocol $\Sigma_{\mathtt{R}\vee\mathtt{S}}$ based on Σ_R and Σ_S for the relation $R \vee S$.

Putting the pieces together, the CRS generation mechanism $\mathtt{GenCRS}$ for $\mathcal{F}_{\mathtt{CRS}}$ in our construction fixes S as a samplable-hard relation with corresponding efficient Σ-protocol Σ_S, and consists of running $(\mathtt{CRS}_s, \mathtt{trap}_s) \leftarrow \kappa_S(1^\lambda)$. We combine this $\mathcal{F}_{\mathtt{CRS}}$ with the restricted observable global RO $\mathcal{G}_{\mathtt{roRO}}$ to instantiate the $\mathcal{G}_{\mathtt{roRO}}$-$\mathcal{F}_{\mathtt{CRS}}$-hybrid model, and are now ready to introduce our GUC compiler.

5.2 GUC Compiler

We propose a compiler that uses any SLC in conjunction with the OR-protocol discussed in Sections 2.3 and 5.1 to transform any Σ-protocol into a GUC NIZKPoK in the $\mathcal{G}_{\mathtt{roRO}}$-$\mathcal{F}_{\mathtt{CRS}}$-hybrid model. The compiler works as follows.

First, $\mathcal{F}_{\mathtt{CRS}}$ is fixed as described in Section 5.1. The real-world $\mathtt{Setup}$ functionality runs the OR-protocol $\Sigma_{\mathtt{R}\vee\mathtt{S}}$ for relation $R \vee S$ through any SLC to obtain $\Pi^{\mathtt{SLC}}_{\mathtt{R}\vee\mathtt{S}}$, and returns the same setup parameters as $\Pi^{\mathtt{SLC}}_{\mathtt{R}\vee\mathtt{S}}$.

For each session s, provers in the real world query the CRS ideal functionality $\mathcal{F}^s_{\mathtt{CRS}}$ to obtain $\mathtt{CRS}_s$. Each time a real prover with SID s needs to create a proof of a statement x using witness w, it obtains $\mathtt{CRS}_s$ and sets the compound statement $X = (x, \mathtt{CRS}_s)$. It then generates a proof Π using $\Pi^{\mathtt{SLC}}_{\mathtt{R}\vee\mathtt{S}}.\mathtt{Prove}(X, W)$, where $W = (w, 0)$ to indicate it knows a witness for the first statement x. In order to verify the proof, a verifier first obtains $\mathtt{CRS}_s$ from $\mathcal{F}^s_{\mathtt{CRS}}$, then checks whether it is the correct CRS for session s. If it is, it the verifier outputs the result of running $\Pi^{\mathtt{SLC}}_{\mathtt{R}\vee\mathtt{S}}.\mathtt{Verify}(X, \Pi)$.

In the ideal world, the $\mathtt{SimSetup}$ algorithm begins by generating an empty list in which to store the simulated CRS for each session, denoted $\mathtt{simcrs}$. When it is time to prove a statement on behalf of an honest (dummy) party in session s, the compiler's $\mathtt{SimProve}$ algorithm generates $(\mathtt{CRS}_s, \mathtt{trap}_s) \leftarrow \kappa_S(1^\lambda)$ (if one has not been generated already), and computes the proof using $\Pi^{\mathtt{SLC}}_{\mathtt{R}\vee\mathtt{S}}.\mathtt{Prove}$, this time using $\mathtt{trap}_s$ as the witness.

Given a *non-simulated* proof and a list $\mathcal{Q}^s_{P^*}$ of adversarial provers' queries for session s, the compiler's $\mathtt{Extract}$ algorithm runs $\Pi^{\mathtt{SLC}}_{\mathtt{R}\vee\mathtt{S}}.\mathtt{Extract}$ using $\mathcal{Q}^s_{P^*}$ and tests the compound witness $W = (w_0, w_1)$. If $R_{\mathtt{R}\vee\mathtt{S}}(X, W) = 1$ but $R(x_0, w_0) = 0$, $\mathtt{Extract}$ outputs $\mathtt{Fail}$. Otherwise, it outputs W.

Note that this formulation diverges from the general intuition of an OR-protocol extractor (see Appendix A.8 of the full version of the paper [37]) in

that we require any valid witness W to imply that $R(x_0, w_0) = 1$, not that *either* $R(x_0, w_0) = 1$ *or* $S(x_1, w_1) = 1$. This is because we need to account for the fact that $\mathcal{F}_{\texttt{NIZK}}$ will never invoke the `Extract` algorithm on proofs it has generated using `SimProve`, and nobody else should ever have access to the CRS trapdoor. If $\mathcal{F}_{\texttt{NIZK}}$ gets a proof that verifies because $S(\texttt{CRS}_s, w_1) = 1$, it must be the case that an adversarial prover has acquired the trapdoor, and `Extract` forms its output in such a way that $\mathcal{F}_{\texttt{NIZK}}$ will output `Fail`. In our proof of security, we will bound the probability of this failure by constructing a reduction to the hardness property of S.

We give a formal construction of the candidate compiler below, and prove in Section 5.3 that it creates GUC NIZKPoK in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model.

Definition 13 (Candidate Compiler). *Let Σ_R be any Σ-protocol for relation R (Definition 1), $\mathcal{G}_{\texttt{roRO}}$ be the restricted observable global random oracle (Definition 6), Σ_S be an efficient Σ-protocol for samplable-hard relation S (Definition 12), $\mathcal{F}_{\texttt{CRS}}$ be the ideal CRS functionality (Definition 9) where* $\texttt{GenCRS} := \kappa_S$*, and* `SLC` *be any straight-line compiler (Definition 2). Then our* candidate compiler `guc` *is an algorithm that, on input Σ_R and* `SLC`*, produces a tuple of algorithms $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}} = (\texttt{Setup}^{\mathcal{G}_{\texttt{roRO}}}, \texttt{Prove}^{\mathcal{G}_{\texttt{roRO}},\mathcal{F}_{\texttt{CRS}}}, \texttt{Verify}^{\mathcal{G}_{\texttt{roRO}},\mathcal{F}_{\texttt{CRS}}}, \texttt{SimSetup}, \texttt{SimProve}, \texttt{Extract})$, defined in Figure 4.*

5.3 Realizing $\mathcal{F}_{\texttt{NIZK}}$ in the $\mathcal{G}_{\texttt{RO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid Model

We now prove that the algorithm `guc` from Definition 13 compiles any Σ-protocol into a GUC NIZKPoK in the $\mathcal{G}_{\texttt{RO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model.

Theorem 3. *Let Σ_R be any Σ-protocol for relation R (Definition 1), $\mathcal{G}_{\texttt{roRO}}$ be the restricted observable global random oracle (Definition 6), Σ_S be an efficient Σ-protocol for samplable-hard relation S (Definition 12), $\mathcal{F}_{\texttt{CRS}}$ be the ideal CRS functionality (Definition 9) where* $\texttt{GenCRS} := \kappa_S$*,* `SLC` *be any straight-line compiler (Definition 2), and* `guc` *be our candidate compiler (Definition 13). Then $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}} \leftarrow \texttt{guc}(\Sigma_R, \texttt{SLC})$ GUC-realizes $\mathcal{F}_{\texttt{NIZK}}$ in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model (Definition 11).*

Proof Sketch. The proof proceeds similarly to that of Theorem 2 in Section 4, where we construct a sequence of hybrids that transition between the real- and ideal-world GUC experiments. In the ideal-world experiment, our simulator $\mathcal{S}$ hands the ideal functionality $\mathcal{F}_{\texttt{NIZK}}$ the tuple of algorithms $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}}$ and otherwise functions as a dummy adversary, forwarding communications between the environment and the protocol. Throughout the proof when we say an argument is identical to an argument from the proof of Theorem 2, we mean identical up to the handling of the `IsProgrammed` interface, which does not exist in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model.

The first hybrid is identical to the first hybrid in the proof of Theorem 2: we replace all of the real-world protocol participants, $\mathcal{G}_{\texttt{roRO}}$, and now $\mathcal{F}_{\texttt{CRS}}$ with a challenger $\mathcal{C}$ who controls all of the wires in and out of the environment and the

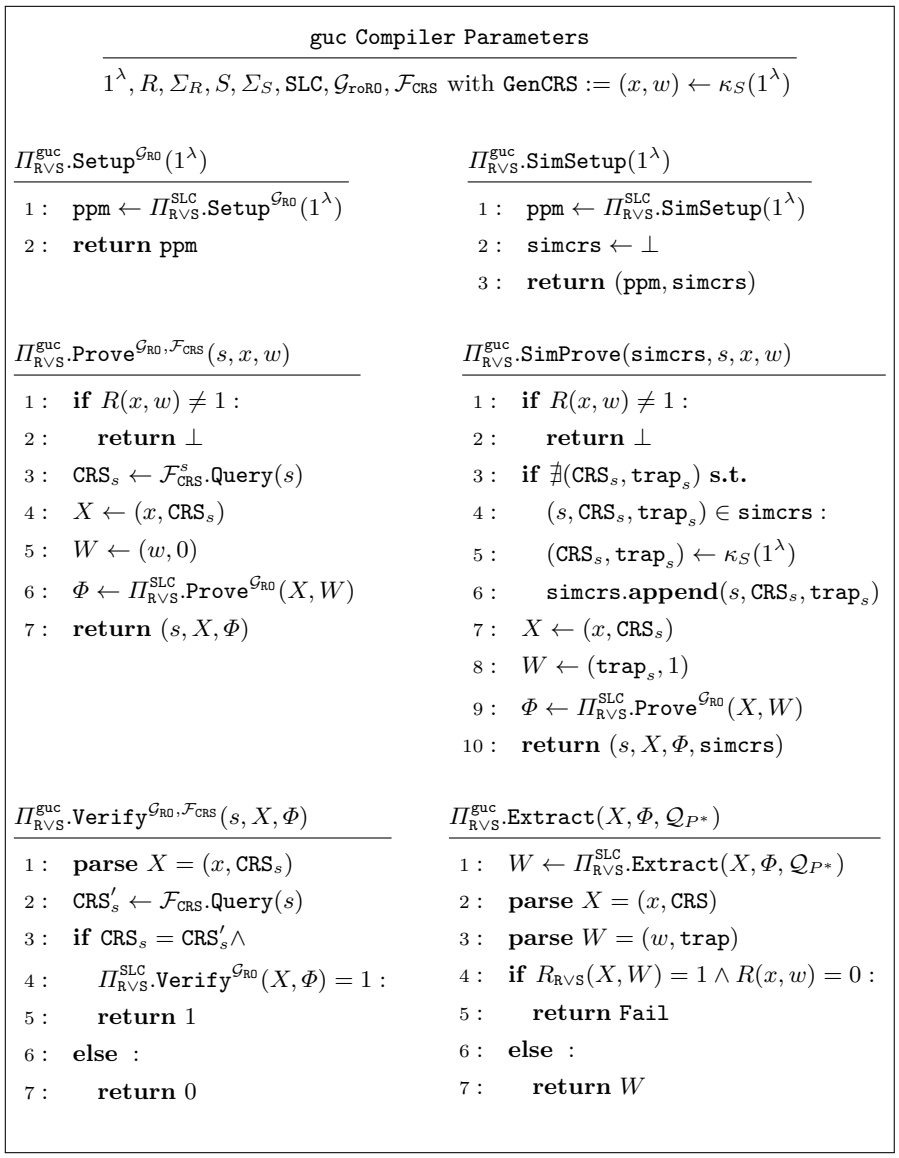

Fig. 4. Compiler $\Pi^{\mathtt{guc}}_{\mathtt{R}\vee\mathtt{S}} \leftarrow \mathtt{guc}(\Sigma_R, \mathtt{SLC})$ for Σ_R in the $\mathcal{G}_{\mathtt{roRO}}$-$\mathcal{F}_{\mathtt{CRS}}$-hybrid Model

adversary, noting this step permits $\mathcal{C}$ to program $\mathcal{G}_{\texttt{roRO}}$.[2] The second hybrid is also identical to the one in the proof of Theorem 2 above, except instead of jumping straight to replacing $\mathcal{C}$'s real-world `Prove` algorithm with the **Prove** interface of the ideal functionality, which will use $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}}.\texttt{SimSetup}$ and $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}}.\texttt{SimProve}$, we instead replace `Prove` with $\Pi^{\texttt{SLC}}_{\texttt{R}\vee\texttt{S}}.\texttt{SimSetup}$ and $\Pi^{\texttt{SLC}}_{\texttt{R}\vee\texttt{S}}.\texttt{SimProve}$. This step allows us to postpone giving the reduction access to the CRS trapdoors, since we will need to ensure that any adversarially-created proofs in the next hybrid will only avoid extraction if the adversary is somehow able to generate the trapdoor itself. By the arguments used in the proof of Theorem 2, we can reduce the indistinguishability of the first two hybrids to the NIM-SHVZK property of $\Pi^{\texttt{SLC}}_{\texttt{R}\vee\texttt{S}}$.

The third hybrid is identical to the third hybrid in the proof of Theorem 2 in that we replace $\mathcal{C}$'s `Verify` procedure with $\mathcal{F}_{\texttt{NIZK}}$'s **Verify** interface, which uses $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}}.\texttt{Extract}$. The proof of indistinguishability of the second and third hybrids will differ slightly due to the new failure condition in the $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}}.\texttt{Extract}$ algorithm: namely, the clause that says if the overall witness $W = (w, \texttt{trap}_s)$ is a valid witness for the statement $X = (x, \texttt{CRS}_s)$ but w is not a valid witness for x, output `Fail`. We can limit the probability of this failure by constructing a reduction to the hardness property of the samplable-hard relation: if the environment is able to produce a proof that meets the failure condition, the reduction can produce a tuple $(\texttt{CRS}_s, \texttt{trap}_s)$ given only $\texttt{CRS}_s \leftarrow \kappa_S(1^\lambda)$. Since the probability of generating such a tuple is negligible by the hardness property of S, the probability of such a failure is similarly negligible. The only other way for the environment to distinguish the hybrids is to produce a valid, non-extractable proof of a statement X—i.e. such that $R_{\texttt{R}\vee\texttt{S}}(X, W) = 0$ for $W \leftarrow \Pi^{\texttt{SLC}}_{\texttt{R}\vee\texttt{S}}.\texttt{Extract}(X, W)$. In this case, $\mathcal{C}$ can use this proof to contradict the NI-SSS (or NI-SS) property of $\Pi^{\texttt{SLC}}_{\texttt{R}\vee\texttt{S}}$ in the exact same way as the parallel reduction in the proof of Theorem 2.

Finally, the penultimate hybrid replaces $\Pi^{\texttt{SLC}}_{\texttt{R}\vee\texttt{S}}.\texttt{SimSetup}$ and $\Pi^{\texttt{SLC}}_{\texttt{R}\vee\texttt{S}}.\texttt{SimProve}$ with the candidate compiler's algorithms $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}}.\texttt{SimSetup}$ and $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}}.\texttt{SimProve}$. This step effectively reverts the proofs back to the real-world `Prove` mechanism, except $\mathcal{C}$ is using trapdoors rather than real witnesses. If $\Pi^{\texttt{SLC}}_{\texttt{R}\vee\texttt{S}}$ is statistical NIM-SHVZK, then there is automatically negligible difference in view between the third and penultimate hybrids. If, however, there is computational wiggle room between the proofs in the two experiments, *and* the distinguisher environment now has access to the extractor, we must ensure that the *only* way the environment can distinguish the hybrids is by the contents of the proofs (as opposed to somehow using its view of the new proofs, which use the CRS trapdoor, to cause the extractor to fail). We argue here that because the straight-line extractor works exclusively based on statements, proofs, and oracle queries that the environment made itself, anything the environment can learn from the extractor it could have learned on its own. Therefore, it cannot have possibly learned anything new about the hybrids from the extractor, and the reduction to computational NIM-SHVZK proceeds the same as before.

[2] As discussed by Camenish et al. [10], the challenger in such a hybrid experiment can make use of techniques like programming and rewinding that are otherwise "illegal" for the simulator to employ in the GUC model.

The last hybrid replaces $\mathcal{C}$ with $\mathcal{F}_{\texttt{NIZK}}$ and $\mathcal{S}$—this is again a syntactic rearrangement, and is functionally identical to the ideal-world experiment. The full version of this proof is available in Appendix B.4 of the full version [37]. □

6 Constructions via the Randomized Fischlin Transform

We demonstrated in the last two sections that any straight-line compiler (SLC) that satisfies Definition 2 is sufficient to transform any Σ-protocol Σ_R into a GUC NIZKPoK in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model, and sufficient in conjunction with our OR-protocol compiler to complete the transformation in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model. In this section, we will show that the randomized Fischlin transform [31,35] meets our definition of an SLC for a broad class of Σ-protocols, and therefore enables us to practically instantiate both sets of GUC NIZKPoK. The efficiency of the resulting proof systems reduce to the efficiency of the randomized Fischlin transform, which requires only a linear increase in the size of the proofs for small multiplicative and additive constants.

In this section, we review the randomized Fischlin transform `rFis` and show that it meets our definition of an SLC. We then apply `rFis` to efficiently realize GUC NIZKPoK in the $\mathcal{G}_{\texttt{rpoRO}}$- and $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid models, respectively.

6.1 The Randomized Fischlin Transform, Revisited

Recall from Section 1 that the randomized Fischlin transform due to Kondi and shelat [35] is a version of the Fischlin transform [31,30] in which the challenges are selected uniformly at random from the challenge space. In Fischlin's original construction, the Σ-protocols under transformation need a property called *quasi-unique responses*, which Kondi and shelat demonstrate precludes the transformation of OR-protocols. In order to use the randomized Fischlin transform on our OR-protocol construction in a way that preserves security, the OR-protocol must have the (more general) *strong* special soundness property. We consolidate the two properties below, and a brief discussion of the necessity of strong special soundness in Appendix A.10 of the full version of the paper [37].

Definition 14 (Required Properties for `rFis`). *A Σ-protocol Σ_R for relation R (Definition 1) has* required properties for the randomized Fischlin transform `rFis` *if it has the* quasi-unique responses property *(Definition 25 in Appendix A.10 [37]) or the* strong special soundness property *(Definition 26 in Appendix A.10 [37]).*

In the full version of his paper, Fischlin proves that his transform over Σ-protocols with quasi-unique responses creates a protocol that is both NIMSHVZK and NI-SSS in the standard ROM [30]. Kondi and shelat show that the randomized Fischlin transform over a Σ-protocol with the more general strong special soundness property creates a protocol that is standard (non-multi) NISHVZK and standard (non-simulation) strong NI-SS [35]. Therefore, it remains to show that the NI *multi*-SHVZK and strong special *simulation* soundness

properties are similarly preserved under the randomized transform for strong special-sound Σ-protocols. Our proof of the theorem below draws heavily on arguments from Fischlin [30] and Kondi and shelat [35]; the only novelty is in the (nearly verbatim) application of Fischlin's arguments for NIM-SHVZK and NI-SSS to the randomized transform. We therefore defer the technical details of the randomized Fischlin transform to Definition 29 in Appendix A.12, and the full proof to Appendix B.5 of the full version of the paper [37].

Theorem 4. *Let Σ_R be any Σ-protocol for relation R (Definition 1) with the required properties for* `rFis` *(Definition 14). Then the randomized Fischlin transform* `rFis` *(Definition 29 in Appendix A.12 [37]) is a straight-line compiler for Σ_R (Definition 2).*

Proof sketch. Recall that a straight-line compiler according to our definition must create protocols that are NIM-SHVZK and NIM-SSS. Kondi and shelat prove in Theorem 6.4 [35] that the tuple of algorithms $\Pi_R^{\texttt{rFis}}$ (denoted $\pi_{\texttt{NIZK}}^{\texttt{F}-\texttt{rand}}$ in their paper) produced by running the randomized Fischlin transform on any strong special sound Σ-protocol Σ_R for relation R is a NISLE ZKPoK for L_R in the standard random-oracle model. Since Kondi and shelat use the standard definitions of SHVZK and strong special soundness (Definitions 19 and 14 in the full version, respectively [37]), it remains to show that $\Pi_R^{\texttt{rFis}}$ satisfies NIM-SHVZK and NIM-SSS.

Fischlin shows in the proof of Theorem 3 [30] that his original transform satisfies the NIM-SHVZK and NI-SSS properties. Since the strong special soundness property replaces the quasi-unique responses property and the challenges in the randomized version are identically distributed to those in the original version, the proof of NIM-SHVZK and NI-SSS for the randomized Fischlin transform is almost identical to Fischlin's proof of Theorem 3. We discuss the minor differences in the full proof (Appendix B.5 [37]). □

6.2 Efficient, GUC NIZKPoK in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid Model

We demonstrated in Section 4 that any SLC is sufficient to compile any Σ-protocol into a GUC NIZKPoK in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model, and argued in Section 6.1 above that the transform `rFis` is an SLC. Therefore, given any Σ-protocol Σ_R that meets the requirements for `rFis`, $\Pi_R^{\texttt{rFis}} \leftarrow \texttt{rFis}(\Sigma_R)$ is sufficient to create GUC NIZKPoK in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model.

Corollary 1. *Let Σ_R be any Σ-protocol for a relation R (Definition 1) with the required properties for* `rFis` *(Definition 14) and* `rFis` *be the randomized Fischlin transform (Definition 29 in Appendix A.12 [37]). Then $\Pi_R^{\texttt{SLC}} \leftarrow \texttt{rFis}(\Sigma_R)$ GUC-realizes $\mathcal{F}_{\texttt{NIZK}}$ in the $\mathcal{G}_{\texttt{rpoRO}}$-hybrid model (Definition 10).*

Proof. The corollary follows directly from Theorems 2 and 4. □

6.3 Efficient, GUC NIZKPoK in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid Model

Our construction for the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model requires two layered compilers: any SLC, and our OR-protocol compiler `guc` from Definition 13. We proved in Theorem 3 that $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}} \leftarrow \texttt{guc}(\Sigma_R, \texttt{SLC})$ GUC-realizes $\mathcal{F}_{\texttt{NIZK}}$ for any Σ-protocol Σ_R, and again in Section 6.1 that `rFis` is an SLC. Therefore, $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}} \leftarrow \texttt{guc}(\Sigma_R, \texttt{rFis})$ creates GUC NIZKPoK in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model.

Corollary 2. *Let Σ_R be any Σ-protocol for a relation R (Definitions 1) with the required properties for* `rFis` *(Definition 14),* `rFis` *be the randomized Fischlin transform (Definition 29 in Appendix A.12 [37]), and* `guc` *be the candidate compiler from Definition 13. Then $\Pi^{\texttt{guc}}_{\texttt{R}\vee\texttt{S}} \leftarrow \texttt{guc}(\Sigma_R, \texttt{rFis})$ GUC-realizes $\mathcal{F}_{\texttt{NIZK}}$ in the $\mathcal{G}_{\texttt{roRO}}$-$\mathcal{F}_{\texttt{CRS}}$-hybrid model (Definition 11).*

Proof. The corollary follows directly from Theorems 3 and 4. □

Acknowledgements

Many thanks to Yashvanth Kondi and abhi shelat for crucial security analysis of our original OR-protocol construction, and to Jack Doerner for insightful discussions about $\mathcal{F}_{\texttt{NIZK}}$ that inspired our results in Section 3.5. This research was supported by NSF grant 2154170, and by grants from Meta.

References

1. Ben Adida. Helios: Web-based open-audit voting. In Paul C. van Oorschot, editor, *Proceedings of the 17th USENIX Security Symposium*, pages 335–348, 2008.
2. Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In Mihir Bellare, editor, *CRYPTO 2000*, volume 1880, pages 255–270, 2000.
3. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 62–73, 1993.
4. Fabrice Benhamouda, Tancrède Lepoint, Julian Loss, Michele Orrù, and Mariana Raykova. On the (in) security of ros. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 33–53. Springer, 2021.
5. Manuel Blum, Alfredo De Santis, Silvio Micali, and Guiseppe Persiano. Noninteractive zero-knowledge. *SIAM Journal of Computing*, 20(6):1084–1118, 1991.
6. Fabrice Boudot. Efficient proofs that a committed number lies in an interval. In *EUROCRYPT '00*, pages 431–444, 2000.
7. Sean Bowe, Ariel Gabizon, and Ian Miers. Scalable multi-party computation for zk-snark parameters in the random beacon model. *ePrint Archive*, 2017.
8. Stefan Brands. *Rethinking Public Key Infrastructure and Digital Certificates—Building in Privacy.* PhD thesis, Eindhoven Inst. of Tech., The Netherlands, 1999.
9. Jan Camenisch and Ivan Damgård. Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 331–345. Springer, 2000.

10. Jan Camenisch, Manu Drijvers, Tommaso Gagliardoni, Anja Lehmann, and Gregory Neven. The wonderful world of global random oracles. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 280–312. Springer, 2018.
11. Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, and Mira Meyerovich. How to win the clonewars: efficient periodic n-times anonymous authentication. pages 201–210. ACM, 2006.
12. Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Compact E-cash. In Ronald Cramer, editor, *Advances in Cryptology — Eurocrypt 2005*, volume 3494, pages 302–321. Springer, 2005.
13. Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045, pages 93–118. Springer Verlag, 2001.
14. Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In *SCN 2002*, volume 2576, pages 268–289, 2003.
15. Jan Camenisch and Markus Michels. Proving in zero-knowledge that a number n is the product of two safe primes. In *EUROCRYPT '99*, pages 107–122, 1999.
16. Jan Camenisch and Markus Michels. Separability and efficiency for generic group signature schemes. In *CRYPTO '99*, volume 1666, pages 413–430, 1999.
17. Jan Camenisch and Victor Shoup. Practical verifiable encryption and decryption of discrete logarithms. In *CRYPTO '03*, volume 2729, pages 126–144, 2003.
18. Jan Camenisch and Markus Stadler. Efficient group signature schemes for large groups. In *CRYPTO '97*, pages 410–424. Springer Verlag, 1997.
19. Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145. IEEE, 2001.
20. Ran Canetti, Yevgeniy Dodis, Rafael Pass, and Shabsi Walfish. Universally composable security with global setup. In *Theory of Cryptography Conference*, pages 61–85. Springer, 2007.
21. Ran Canetti and Marc Fischlin. Universally composable commitments. In *Annual International Cryptology Conference*, pages 19–40. Springer, 2001.
22. Ran Canetti, Abhishek Jain, and Alessandra Scafuro. Practical uc security with a global random oracle. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 597–608, 2014.
23. Ronald Cramer, Ivan Damgård, and Jesper Buus Nielsen. Multiparty computation from threshold homomorphic encryption. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045, pages 280–300. Springer Verlag, 2001.
24. Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Annual International Cryptology Conference*, pages 174–187. Springer, 1994.
25. Ronald Cramer, Ivan Damgård, Chaoping Xing, and Chen Yuan. Amortized complexity of zero-knowledge proofs revisited: Achieving linear soundness slack. In *Advances in Cryptology - EUROCRYPT 2017*, volume 10210 of *Lecture Notes in Computer Science*, pages 479–500, 2017.
26. Ivan Damgård. On σ-protocols. University of Aarhus, Department of Computer Science, 2002.
27. Manu Drijvers, Kasra Edalatnejad, Bryan Ford, Eike Kiltz, Julian Loss, Gregory Neven, and Igors Stepanovs. On the security of two-round multi-signatures. In *2019 IEEE Symposium on Security and Privacy*, pages 1084–1101. IEEE, 2019.
28. Uriel Feige, Dror Lapidot, and Adi Shamir. Multiple noninteractive zero knowledge proofs under general assumptions. 29(1):1–28, 1999.

29. Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the theory and application of cryptographic techniques*, pages 186–194. Springer, 1986.
30. Marc Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. 2005. Manuscript. Available from http://www.cryptoplexity.informatik.tu-darmstadt.de/media/crypt/publications_1/fischlinonline-extractor2005.pdf.
31. Marc Fischlin. Communication-efficient non-interactive proofs of knowledge with online extractors. In *Annual International Cryptology Conference*, pages 152–168. Springer, 2005.
32. Eiichiro Fujisaki and Tatsuaki Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In *CRYPTO '97*, pages 16–30, 1997.
33. Eu-Jin Goh and Stanisław Jarecki. A signature scheme as secure as the diffie-hellman problem. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 401–415. Springer, 2003.
34. Shuichi Katsumata. A new simple technique to bootstrap various lattice zero-knowledge proofs to qrom secure nizks. In *Annual International Cryptology Conference*, pages 580–610. Springer, 2021.
35. Yashvanth Kondi and abhi shelat. Improved straight-line extraction in the random oracle model with applications to signature aggregation. *Cryptology ePrint Archive*, 2022.
36. Helger Lipmaa. Statistical zero-knowledge proofs from diophantine equations. Manuscript. Available from http://eprint.iacr.org/2001/086, 2001.
37. Anna Lysyanskaya and Leah Namisa Rosenbloom. Universally composable sigma-protocols in the global random-oracle model. *Cryptology ePrint Archive*, 2022.
38. Vadim Lyubashevsky. Lattice signatures without trapdoors. In *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 738–755. Springer, 2012.
39. Jonas Nick, Tim Ruffing, and Yannick Seurin. Musig2: simple two-round schnorr multi-signatures. In *Annual International Cryptology Conference*, pages 189–221. Springer, 2021.
40. Rafael Pass. On deniability in the common reference string and random oracle model. In *Annual International Cryptology Conference*, pages 316–337, 2003.
41. Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *CRYPTO '92*, volume 576, pages 129–140, 1992.
42. Alfredo De Santis, Giovanni Di Crescenzo, Rafail Ostrovsky, Giuseppe Persiano, and Amit Sahai. Robust non-interactive zero knowledge. In *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 566–598. Springer, 2001.
43. Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 755–784. Springer, 2015.
44. David Wagner. A generalized birthday problem. In *Annual International Cryptology Conference*, pages 288–304. Springer, 2002.
45. John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.
46. Douglas Wikström. A commitment-consistent proof of a shuffle. In Colin Boyd and Juan Manuel González Nieto, editors, *ACISP*, pages 407–421. Springer, 2009.