Universal Ring Signatures in the Standard Model

Pedro Branco[1], Nico Döttling[2], and Stella Wohnig[2,3]

[1]Johns Hopkins University
[2]Helmholtz Center for Information Security (CISPA)
[3]Universität des Saarlandes

Abstract

Ring signatures allow a user to sign messages on behalf of an *ad hoc* set of users - a ring - while hiding her identity. The original motivation for ring signatures was whistleblowing [Rivest et al. ASIACRYPT'01]: a high government employee can anonymously leak sensitive information while certifying that it comes from a reliable source, namely by signing the leak. However, essentially all known ring signature schemes require the members of the ring to publish a structured verification key that is compatible with the scheme. This creates somewhat of a paradox since, if a user does not want to be framed for whistleblowing, they will stay clear of signature schemes that support ring signatures.

In this work, we formalize the concept of universal ring signatures (URS). A URS enables a user to issue a ring signature with respect to a ring of users, independently of the signature schemes they are using. In particular, none of the verification keys in the ring need to come from the same scheme. Thus, in principle, URS presents an effective solution for whistleblowing.

The main goal of this work is to study the feasibility of URS, especially in the standard model (i.e. no random oracles or common reference strings). We present several constructions of URS, offering different tradeoffs between assumptions required, the level of security achieved, and the size of signatures:

- Our first construction is based on superpolynomial hardness assumptions of standard primitives. It achieves compact signatures. That means the size of a signature depends only logarithmically on the size of the ring and on the number of signature schemes involved.
- We then proceed to study the feasibility of constructing URS from standard polynomially-hard assumptions only. We construct a non-compact URS from witness encryption and additional standard assumptions.
- Finally, we show how to modify the non-compact construction into a compact one by relying on indistinguishability obfuscation.

1 Introduction

Ring Signatures. Ring signatures, introduced in [RST01], allow for a user to create a signature σ for a message m with respect to an ad-hoc group of users R, called a ring. A ring signature should be: i) unforgeable, meaning that, given a valid signature σ for a ring R, it must have been created by one of the users in R; and ii) anonymous, meaning that it should be infeasible for someone, even if they have access to every signing key corresponding to the verification keys in the ring R, to identify which user created the signature.

Ring signatures have recently found wide-spread application in the context of cryptocurrencies. However in this work we revisit the original motivation of ring signatures: *whistleblowing* [RST01]. Using a ring signature scheme, a whistleblower in a high government office with access to some classified information can leak this information e.g. to the media, in a way that convinces them that this information comes from a reliable source, namely by signing the leak. At the same time, the identity of the whistleblower remains hidden in the ring of insiders. A critical aspect in this scenario is that *the whistleblower can issue such a signature without the consent of the other parties in the ring.*

Rivest, Shamir and Tauman-Kalai [RST01] showed that signature schemes with RSA verification keys can be used to issue ring signatures. If RSA signatures were the universally agreed-upon standard for digital signatures, this would be great for whistleblowers! Yet, currently there is a plethora of competing schemes and standards for digital signatures.

Support for ring signatures might however even deter users from adopting some signature scheme: Knowing that a certain signature scheme supports ring signatures, why should loyal government officials even use such a scheme and potentially be framed for being a whistleblower? Furthermore, wouldn't it even be in the interest of a government to mandate their officials to use signature schemes which do not allow to issue ring signatures? Can the kind of whistleblowing envisioned by [RST01] be prohibited by such measures? Are there effective countermeasures which protect users against being abused as a crowd in which a whistleblower seeks anonymity? Concretely, can we construct signature schemes which protect their users from being involuntarily forced into a ring?

Universal Ring Signatures. Formalizing the idea of a ring signature compatible with *all* digital signature schemes, we define the notion of *Universal Ring Signatures* (URS)[1]. URS allow users to create a ring signature for a ring composed of verification keys $R = (\mathsf{vk}_1, \ldots, \mathsf{vk}_\ell)$ *independently* of the structure of each vk_i and even the signature schemes which were used to create these keys. In other words, each vk_i can be a verification key from a *(possibly different) signature scheme.*[2] Most importantly, *none of the verification keys is required to*

[1] The term universal ring signatures was also used in [Tso13] to refer to a completely different property of ring signatures.

[2] For example, one of the verification keys can be from an SIS-based signature scheme and another from a group-based signature scheme.

be compatible with known ring signature schemes.

Thus, URS allow users to conceal their identity inside a ring in a *non-cooperative way*: The user can create a signature with respect to a ring of verification keys, even if they were specifically chosen to be incompatible with specific ring signature schemes. This is in stark contrast to standard ring signatures, where the parties *cooperate* by issuing verification keys that are compatible with a ring signature scheme, thus intentionally providing anonymity to one another (which is what happens in a cryptocurrency setting).

A URS provides a way out of the whistleblower problem described above. Equipped with a URS scheme, a whistleblower just needs to somehow specify (implicitly or explicitly) the verification keys of the users in the ring. However, unlike for all known ring signature schemes, these verification keys do not need to obey any particular structure.

Ring Signatures via Non-Interactive Zero-Knowledge Proofs. Non-interactive zero-knowledge (NIZK) proofs [BFM88] are a powerful and quite general tool to make protocols secure against malicious adversaries. In the context of ring signatures, the slightly stronger notion of non-interactive zero-knowledge proofs of knowledge (NIZKPoK) provide a stronger soundness guarantee, in the sense that any (efficient) prover providing a valid proof of some statement x must *know* corresponding witness w of x.

NIZKPoK proofs provide a direct approach to construct ring signatures: For a ring R, a message m and a commit c one provides a proof π which certifies that c commits to a signature σ such that the pair (σ, m) verifies under some verification key vk in the ring R.

This construction does not require that the verification keys in the ring R come from one and the same signature scheme. Thus, NIZKPoK proofs in fact imply universal ring signatures. Yet, NIZK (and thus also NIZKPoK) are known to be impossible in the standard model [GO94], that is without a common reference string and without making use of the random oracle heuristic [BR93]. We will later discuss the ramifications of relying on either the random oracle model or the random oracle heuristic in the construction of URS.

1.1 Our Results

The main problem we address in this work is the question of whether universal ring signatures exist in the standard model, and if so under which assumptions.

Before we tackle the problem of constructing universal ring signatures, we first provide definitions that formalize the requirements informally laid out above.

We present three standard model URS construction, offering different tradeoffs between compactness, security and primitives/assumptions needed to construct them. Our schemes are *fully* universal, in the sense that no assumptions on the structure of verification keys are made.

Our first construction is a URS scheme with compact signatures, i.e., the signature size depends only logarithmically on the number of users in the ring and

on the number of signature schemes. This scheme relies on superpolynomial hardness of standard assumptions. Specifically, we rely on a superpolynomially secure signature scheme, a (polynomially secure) perfectly binding commitment scheme, perfectly sound non-interactive witness-indistinguishability (NIWI) proof systems for NP and somewhere perfectly binding (SPB) hashing scheme [BDH$^+$19]. All of these primitives can be instantiated using standard hardness assumptions.

We get the following theorem.

Theorem 1 (Informal)**.** *Assuming the existence of perfectly binding commitment schemes, perfectly sound NIWI proof systems for* NP *and SPB hashing schemes (all three with polynomial security), there exists a universal ring signature scheme in the standard model with compact signatures under the condition that the underlying signature schemes are superpolynomially secure.*

While this construction provides the baseline for our investigation, it raises the question whether superpolynomial hardness is necessary to construct standard model universal ring signatures. Compared with 2-move blind signatures, we do know standard model constructions (again, no CRS or RO) from superpolynomial hardness assumptions [GRS$^+$11, GG14], yet we don't know of any such construction from polynomial hardness assumptions and in fact, it is known that no such construction is achievable via a black-box reduction [FS10]. Thus, it is conceivable that something similar might be the case for universal ring signatures.

Perhaps somewhat surprisingly, our second construction shows that this is not the case for URS: We provide a construction that enjoys a security reduction to polynomial and falsifiable hardness assumptions. Concretely, we rely on the existence of a witness encryption (WE) scheme for NP, a perfectly sound NIWI proof system for NP, an SPB hashing scheme, and a pseudorandom function (PRF). In terms of compactness, the size of the signatures of this scheme depends linearly on the number of users in the ring. Further, this scheme fulfills a slightly relaxed notion of anonymity, which we call t-anonymity, which requires that there need to be at least t honestly generated verification keys in the ring. The standard notion of anonymity corresponds to 2-anonymity.

Theorem 2 (Informal)**.** *Assuming the existence of a WE for* NP*, a perfectly sound NIWI proof system for* NP*, an SPB hashing scheme, and a PRF, there exists a (non-compact) universal ring signature scheme in the standard model with t-anonymity, where t is a parameter depending on the signature schemes involved.*

For all conceivable purposes, the parameter t here is a small constant. Concretely, t depends on the entropy κ of the honest verification keys involved. Asymptotically, any such key must have entropy at least $\kappa = \omega(\log(\lambda))$. Otherwise, it would be trivially insecure. Our only requirement on t will be that $t \cdot \kappa \geq \lambda$. In terms of concrete parameters, κ would have to be at least 50 bits (or else the underlying scheme would be trivially insecure). Setting $t = 3$ or $t = 4$ will be sufficient for this parameter choice.

This leaves open the question of compactness. Is perhaps any standard model URS necessarily non-compact?

We can also resolve this question negatively, yet under still a (potentially) stronger assumption: We provide a construction of a compact WE scheme from polynomial hardness assumptions for a special type of languages that we call (t, N) threshold conjunction languages, which together with Theorem 2 will imply a compact URS scheme from polynomial hardness assumptions.

A (t, N) threshold conjunction language is the set of statements $(x_1, \ldots, x_N)$ for which there are at least t valid statements x_i among them. The size of the ciphertexts we receive when encrypting under such a statement is compact in the sense that it only depends logarithmically on N. Our WE construction requires indistinguishability obfuscation ($i\mathcal{O}$), puncturable pseudorandom functions (PPRF) [BW13], somewhere statistically binding (SSB) hashing schemes [HW15, OPWW15] and (t, N)-linear secret sharing (LSS). We obtain the following theorem.

Theorem 3 (Informal)**.** *Assuming the existence of an $i\mathcal{O}$ for all circuits, a (non-compact) WE for NP, a PPRF, an SSB hashing scheme, and a (t, N)-LSS, there exists a compact WE scheme for (t, N) threshold conjunction languages, when $N - t \in \mathcal{O}(\log N)$.*

Combining the two previous theorems, we obtain our final URS construction. This URS construction achieves compact signatures.

Theorem 4 (Informal)**.** *Assuming the existence of a compact WE for $(N-1, N)$ threshold conjunction languages, a perfectly sound NIWI proof system for NP, an SPB hashing scheme and a PRF, there exists a compact universal ring signature scheme in the standard model with t-anonymity.*

1.2 Discussion and Interpretation of our Results

Returning to our main motivation, a URS enables whistleblowing since a whistleblower can *force* any honest users into a ring, regardless of which signature scheme they use. In this sense, one can view the process of signing a message using a URS as an *adversarial act*: even if a set of honest users do not want to hide the whistleblower, there are no effective measures on the level of signature schemes which could protect users from being included in an anonymity set.

Bearing this in mind, we interpret our results, which establish the feasibility of URS, as demonstrating the impossibility of designing signature schemes that resist coercion into rings. Needless to say, the rather heavy components involved in our constructions do not lead to practically useful protocols.

Above we briefly discussed that universal ring signatures can be constructed from NIZKPoK proofs and by now there is a plethora of constructions of NIZKPoK proofs from standard assumptions in the common reference string (CRS) model [BFM88, FLS90, GOS06b, PS19b, BKM20, JJ21], or alternatively in the random oracle model [BR93]. If the goal was to construct a practically useful URS

to provide support across different, seemingly incompatible but *common* signature schemes, then a protocol relying on succinct NIZKPoK arguments would be preferable. In such a setting, one would expect the users of these schemes to collaborate in the sense that they are willing to provide anonymity to one another, i.e. one could assume that all users trust a common reference string as well as all the signature schemes involved.

Yet, the scenario we are interested in is different, in the sense that the "users" have no reason to trust one another, as they were potentially forced into a ring against their will. In this sense, a universal ring signature scheme in the CRS could give users who have been forced into a ring against their will a means of plausible deniability, e.g. by claiming that they do not trust the CRS that was used to generate a universal ring signature, as the party who generated such a CRS may also forge such a signature.

On the other hand, if we consider URS in the random oracle model, then the unsoundness of the ROM could cause issues. When protocols in the ROM are instantiated, we replace the random oracle with a concrete hash function H. As shown by Goldwasser and Kalai [GK03], this heuristic can lead to unsound proof systems if the underlying language already depends on this (concrete) hash function H.

This issue also comes up in the context of universal ring signatures, as one of the signature schemes could be chosen *depending on the hash function* H. Somewhat more concretely, assume we wanted to build a signature scheme Σ^* which makes a URS relying on a random oracle unsound, in the sense that if any verification key of Σ^* is used in a ring R, then universal ring signatures can be forged, while Σ^* is still EUF-CMA secure. We could achieve this by taking any EUF-CMA secure signature scheme Σ and modifying it to Σ^* by additionally including into the verification keys vk^* of Σ^* an obfuscated program $\mathcal{O}$ which lets anyone publicly generate URS of rings involving vk^*. Note that this obfuscated program $\mathcal{O}$ needs to *know* a succinct description of the hash function H, but this is feasible as we assume H to be *instantiated*, rather than a random oracle. The same can in fact be argued for any fixed static common reference string CRS, i.e. CRS can be hardwired into $\mathcal{O}$. Note that while for such a scheme the size of the verification key would increase, both generation and verification would remain essentially unchanged.

Looking ahead, if such a transformation from Σ to Σ^* was done starting relative to one of our standard-model secure URS, then Σ^* would be necessarily insecure. But for a URS whose unforgeability rests on the CRS model or the random oracle model, we would generally expect such a Σ^* to be unforgeable (once the CRS or the RO has been instantiated).

The bottom line of this discussion is that it seems hard to argue that URS constructions in the CRS model or the ROM would be robust against signature schemes which undermine the unforgeability of the URS by depending on the concrete CRS which is used or the concrete hash function which instantiates the Fiat-Shamir paradigm.

1.3 Previous Works

Ring signatures have been extensively studied in the last two decades. Constructions in the random oracle model (ROM) include [RST01, AOS02, BGLS03, DKNS04, LPQ18]. Ring signatures in the CRS model were studied in [SW07, Boy07], where [Boy07] solves the interesting but orthogonal problem of how to include users in a ring whose public keys are not posted publicly by using a PKI structure. We can also find standard model constructions for ring signatures in e.g. [BKM06, BDH$^+$19, PS19a].

All works presented above assume some form of structure on the verification keys. For example, the work of [RST01] assumes that ring verification keys are RSA keys or the work of [BKM06] assumes that ring verification keys are composed by a standard verification key and a uniformly random string.

The only exceptions we are aware of are the works [AOS02, GGHAK21]. In these works, ring signatures that support different signature schemes are presented. However, these works are only *somewhat universal* in the sense that there are signature schemes that are not compatible with their schemes.[3] Moreover, these schemes are only secure in the ROM whereas we work in the standard model. In essence, the focus of these works is different from ours as they sacrifice universality for efficiency. In this work, we take the opposite direction.

A construction of a universal primitive from $i\mathcal{O}$ has previously been given for a notion called signature aggregators in [HKW15]. This allows to combine signatures from different users using arbitrary signature schemes into one signature to succinctly store and verify. The application and techniques used are however different and can not be transferred to ring signatures trivially.

2 Technical Overview

Before presenting our constructions of URS, we briefly recall the ring signature scheme of Backes *et al.* [BDH$^+$19]

In the scheme of [BDH$^+$19] (which is itself based on [BKM06]), verification keys are composed by $\mathsf{VK}_i = (\mathsf{vk}_i, \mathsf{pk}_i)$ where vk_i is a verification key of a standard signature scheme Sig and pk_i is a public key of a public-key encryption (PKE) scheme that has pseudorandom ciphertexts[4].

To sign a message m with respect to a ring $R = \{\mathsf{VK}_i\}_{i\in[\ell]}$, the signer i first generates a signature $\sigma \leftarrow \mathsf{Sig.Sign}(\mathsf{sk}_i, m)$ and then encrypts σ it using pk_i, that is, $\mathsf{ct}_0 \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}_i, \sigma)$. The signer then samples $\mathsf{ct}_1 \leftarrow\!\!\$\, \{0,1\}^\lambda$. One crucial point is that, if the underlying PKE has pseudorandom ciphertexts, then we cannot distinguish well-formed ciphertexts from uniformly random strings. In particular, this means that ct_0 contains (computationally) no information about the public key under which it was encrypted.

[3] More precisely, the scheme of [AOS02] is compatible with *trapdoor-one-way* and *three-move* signature schemes. The scheme of [GGHAK21] is compatible with certain sigma protocols. Any scheme outside of these classes is not compatible with their ring signature schemes.

[4] Examples of such PKE schemes exist from the LWE or DDH assumption.

The signer now proves that either ct_0 or ct_1 encrypts a valid signature under one of the verification keys in the ring using a non-interactive witness-indistinguishable (NIWI) proof system. If off-the-shelf NIWIs were used in this construction, the size of the proof would scale linearly with the size of the ring. This would lead to signatures of size $\mathcal{O}(|R| \cdot \mathsf{poly}(\lambda))$, where λ is the security parameter. To circumvent this problem, [BDH+19] employed a new strategy.

Compact NIWI proofs. The main ingredient to compress the size of the NIWI proof is a somewhere perfectly binding (SPB) hashing scheme. An SPB hashing scheme allows one to hash a database such that the hash perfectly binds to the database item an index i, while the hashing key hides the index i. [HW15, OPWW15, BDH+19].

Given $\mathsf{ct}_0, \mathsf{ct}_1$, the signer can now use a NIWI proof system together with a somewhere perfectly binding (SPB) hashing scheme to create a compact proof π that either ct_0 or ct_1 encrypts a valid signature under one of the keys in the ring. The basic idea here is that instead of proving a statement over all verification keys in the ring, it is sufficient to prove a statement about just two SPB hashes. More concretely, to compute the proof π, the signer first generates an SPB pair of hashing key/secret key $(\mathsf{hk}_j, \mathsf{shk}_j) \leftarrow \mathsf{SPB.KeyGen}(1^\lambda, i)$ that binds to position i, for $j \in \{0,1\}$. Then, it hashes R into a digest $h_j \leftarrow \mathsf{SPB.Hash}(\mathsf{hk}_j, R)$ for $j \in \{0,1\}$. Finally, the signer proves that there exists an index i such that one of the two statements is true:

1. ct_0 encrypts a valid signature under vk_i and hk_0 binds to i;
2. ct_1 encrypts a valid signature under vk_i and hk_1 binds to i.

The signature is composed by $(\mathsf{ct}_0, \mathsf{ct}_1, \mathsf{hk}_0, \mathsf{hk}_1, \pi)$. Thus, by the efficiency requirements of SPB, the signature has size $\mathcal{O}(\log |R| \cdot \mathsf{poly}(\lambda))$.

Finally, to verify that a signature is valid, one just needs to recompute h_j as the hash of R under hk_j, for $j \in \{0,1\}$, and check that π is a valid proof.

Security. Unforgeability and anonymity are roughly argued as follows in [BDH+19]. To argue unforgeability, the security of the scheme is reduced to the security of the underlying signature scheme. To do this, the reduction receives a verification key vk_{i^*} from the challenger, creates the remaining verification keys vk_i, for $i \neq i^*$, and also the public keys pk_i for all $i \in [\ell]$. Importantly, the public keys pk_i are created such that the reduction knows the corresponding secret keys.

Upon receiving a (ring signature) forge from the adversary, the reduction proceeds as follows:

1. Decrypt both ct_0 and ct_1, to obtain σ_0 and σ_1, respectively;
2. Check if any of σ_0, σ_1 is a valid signature under vk_{i^*}. If one of them is valid, the reduction outputs it as the forge.

By the perfect correctness of the SPB hashing and perfect soundness of the NIWI, the reduction outputs a valid forge with non-negligible probability.

To prove anonymity, one relies on the witness-indistinguishability of the NIWI and the fact that the underlying PKE has pseudorandom ciphertexts. Concretely, given two honestly generated verification keys vk_{i_0} and vk_{i_1}, build a sequence of hybrids to prove that a signature created under vk_{i_0} is indistinguishable from a signature created under vk_{i_1}. The sequence of hybrids starts by replacing ct_1 with an encryption of a valid signature under vk_{i_1}, and this change goes unnoticed since the PKE has pseudorandom ciphertexts. Next, change the index in the witness used to create the proof π from i_0 to i_1 using the witness-indistinguishability of the NIWI scheme.

2.1 Compact Universal Ring Signatures from Signatures with Superpolynomial Security

The construction of the Backes et al. scheme [BDH+19] serves as the starting point of our first construction. Observe that the ring signature verification keys of the Backes et al. scheme have a special format: each verification key VK_i is composed of a standard verification key vk_i and a public key pk_i.

The public key pk_i, which can be chosen by the unforgeability reduction, is what enables this reduction to extract a valid forge. In a URS, however, verification keys are not required to have any particular format. In particular, they are not required to include an independently chosen public key of a PKE. How can we facilitate the extraction of a forge by an unforgeability reduction in the setting of URS?

Commitments instead of Ciphertexts. Our first observation is that the ciphertexts in the scheme of Backes et al. [BDH+19] are never decrypted *in the actual scheme*. So, ciphertexts in this scheme actually serve as extractable commitments. Thus, a natural approach is to rely on commitments instead of ciphertexts in this construction. The main reason for using commitments instead of ciphertexts is that we can choose a *keyless* commitment scheme.

Using a commitment scheme, we can build a URS as follows: To sign a message m under a ring of users $R = \{\mathsf{vk}_1, \ldots, \mathsf{vk}_\ell\}$ (where each vk_i is from a possibly different signature scheme), a signer first creates a signature $\sigma \leftarrow \mathsf{Sig.Sign}_i(\mathsf{sk}_i, m)$ using its signature scheme Sig_i. Then, it commits to $(\mathsf{com}_0, \gamma_0) \leftarrow \mathsf{CS.Commit}(1^\lambda, \sigma)$ and to $(\mathsf{com}_1, \gamma_1) \leftarrow \mathsf{CS.Commit}(1^\lambda, 0)$ (where γ_b is the opening information). Using SPB and NIWI exactly as before, the signer can create a compact proof π that one of the commitments hides a valid signature under one of the keys in R.

Anonymity follows by essentially the same argument as before, where the hiding property of the underlying commitment is used instead of the ciphertext pseudorandomness of the PKE in [BDH+19].

Unforgeability from Superpolynomial Hardness. We now show how the unforgeability reduction can extract a valid forge from the adversary. Assume that the hiding property of the commitment scheme CS holds against

polynomial-time adversaries but that CS can be extracted in *superpolynomial-time*. We can then use *complexity leveraging* to prove the unforgeability of the scheme, given that the underlying signature schemes are unforgeable against superpolynomial-time adversaries.

Concretely, given a PPT adversary $\mathcal{A}$ that breaks the unforgeability of our URS, we can construct a superpolynomial-time reduction against the unforgeability of one of the Sig_i. The reduction, after receiving a forge $\Sigma^* = (\mathsf{com}_0^*, \mathsf{com}_1^*, \mathsf{hk}_0^*, \mathsf{hk}_1^*, \pi^*)$ by $\mathcal{A}$, opens both com_0 and com_1 by brute force to recover σ_0^* and σ_1^* respectively. Note that, since CS can be extracted in superpolynomial time, the reduction succeeds in recovering σ_0^* and σ_1^*. Now, as before, the reduction tests if there is a $b \in \{0,1\}$ such that $1 \leftarrow \mathsf{Sig.Verify}_i(\mathsf{vk}_i, m, \sigma_b^*)$ and outputs σ_b^* if it is the case.

2.2 Non-Compact Universal Ring Signatures from Witness Encryption

Considering both the construction of Backes et al. [BDH+19] and our construction in the last paragraph, the question emerges of how one could possibly *efficiently* extract a signature, even if we cannot shoehorn an extraction trapdoor into the protocol utilizing a CRS or augmenting the verification keys. Somewhat more abstractly:

Is it possible to extract a secret from a protocol when the protocol constraints don't allow us to embed an extraction gadget into the protocol?

Extracting via Witness Encryption. Our way out of this dilemma starts with the observation that by relying on a sufficiently strong tool, namely standard witness encryption (WE) [GGSW13], we can repurpose any *sufficiently cryptographic* object as a public key. In our case, these objects will be the verification keys of the honest parties.

Recall that a WE for an NP language $\mathcal{L}$ (with relation $\mathcal{R}$) allows an encrypter to encrypt a message m with respect to a statement x. If $x \in \mathcal{L}$, then a party in possession of a witness w such that $\mathcal{R}(x,w) = 1$ can recover the encrypted m. But, if $x \notin \mathcal{L}$, then indistinguishability of encryptions holds. Currently, we have constructions of WE from indistinguishability obfuscation ($i\mathcal{O}$) [GGH+13] or multilinear maps [GGSW13], but WE is potentially a weaker assumption than either of these.

To use the security of WE, we need to craft a language $\mathcal{L}$ with distinct true and false statements, such that witnesses of true statements allow for decryption, whereas ciphertexts under false statements hide the encrypted message. Ideally, true and false statements should be indistinguishable. Our design-choice of true and false statements will be informed by the following consideration: Consider two distributions of (honest) verification keys, one where each honest vk is generated using truly random coins, and another one where each honest $\tilde{\mathsf{vk}}$ is generated using (possibly correlated) pseudorandom coins. While these distributions are clearly computationally indistinguishable, under the right circumstances we

can also make them *statistically far*, meaning that one of them can serve as a distribution of true statements, while the other one will be the distribution of false statements.

More concretely, let PRG be a pseudorandom generator (PRG). We say that a verification key vk is *malformed* if it is created using random coins coming from a PRG, instead of using truly random coins. That is, for some seed s

$$(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda; \mathsf{PRG}(s)).$$

Similarly, a *well-formed* key vk is created using truly random coins.

Now, consider the language $\mathcal{L}$ parameterized by ℓ different verification keys $\{\mathsf{vk}_i\}_{i\in[\ell]}$. The *yes* instances of $\mathcal{L}$ are the instances $\{\mathsf{vk}_i\}_{i\in[\ell]}$ where *all but one of the verification keys are malformed*. In other words, there exist $\{s_i\}_{i\in[\ell]\setminus\{i^*\}}$ with $i^* \in [\ell]$ such that for all $i \in [\ell] \setminus \{i^*\}$

$$(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Sig.KeyGen}_i(1^\lambda; \mathsf{PRG}(s_i)).$$

Looking ahead, the dichotomy between *all but one key are malformed* vs *at least two keys are well-formed* is what will allow us to prove unforgeability and anonymity respectively. In the former case, the statement under which the WE ciphertext is created is true and, thus, we will be able to decrypt it. In the latter case, the statement is false. Therefore, we can use the security of the WE scheme.

At first glance, this approach seems to work. However, there is a caveat: when the reduction wants verification keys to be well-formed, it might accidentally end up creating them malformed. As an example, consider a signature scheme Sig whose verification keys have less min-entropy than the underlying PRG. Say the key generation algorithm $\mathsf{Sig.Gen}(1^\lambda, r)$ only uses the first $\lambda/3$ bits of r whereas the PRG seed has $\lambda/2$ bits of entropy. In other words, the distributions of well-formed keys and malformed keys might not be sufficiently statistically far. Then, there is a non-negligible probability that a key chosen from the well-formed distribution is actually malformed. We could assume that the underlying signature schemes have exponential security (e.g., verification keys have λ bits of min-entropy) but this would to some degree defeat the purpose of URS.

Replacing the PRG by a PRF. The solution for this problem is to use a pseudorandom function (PRF) instead of a PRG to sample malformed keys. Instead of generating malformed keys individually, we now generate them in a correlated fashion: A set of keys $\{\mathsf{vk}_i\}$ is malformed iff a PRF key K exists such that

$$(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Sig.KeyGen}_i(1^\lambda; \mathsf{PRF}(K, i)).$$

Note that now, all malformed keys are correlated via the PRF key. This implies that the distribution of t malformed keys has λ bits of min-entropy because as soon as we choose the PRF key, all malformed keys are fixed. On the other hand, when sampling t well-formed keys independently, the resulting distribution will

have $t\kappa$ bits of min-entropy where κ is the min-entropy of each verification key. Setting $t\kappa > \lambda$ we conclude that the distributions of well-formed and malformed keys are statistically far apart.

This fact will allow us to prove t-anonymity by *making the number of honest keys in the ring just large enough.*

Given this, we redefine the language $\mathcal{L}$ in the following way: *yes* instances of $\mathcal{L}$ are the instances $\{\mathsf{vk}_i\}_{i\in[\ell]}$ where *all but one of the verification keys are malformed.* In other words, there exists $K \in \{0,1\}^\lambda$ such that for all $i \in [\ell]\setminus\{i^*\}$

$$(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Sig.KeyGen}_i(1^\lambda; \mathsf{PRF}(K, i)).$$

The Scheme. Armed with a WE scheme WE for the language $\mathcal{L}$ described above, we now outline how we can construct a URS scheme.

The scheme is essentially the same as above except that we use the WE scheme for language $\mathcal{L}$ as a drop-in replacement for the commitment scheme.

To sign a message m with respect to the ring R, the signer encrypts a valid signature σ created using its own signing key. Then, it encrypts σ using WE under the statement $x = R$, that is, $\mathsf{ct}_0 \leftarrow \mathsf{WE.Enc}(1^\lambda, x, \sigma)$. Additionally, it creates the ciphertext $\mathsf{ct}_1 \leftarrow \mathsf{WE.Enc}(1^\lambda, x, 0)$. Finally, the signer can again use NIWI and SPB to prove compactly that one of the ciphertexts encrypts a valid signature.

We first analyze the size of the signature. Note that, for all known WE schemes, the ciphertext size is proportional to the size of the verification circuit for the language $\mathcal{L}$. Since the statement is of size $\mathcal{O}(|R| \cdot \mathsf{poly}(\lambda))$, then the ciphertexts output by WE are of size $\mathcal{O}(|R| \cdot \mathsf{poly}(\lambda))$. This implies that the signature is of size $\mathcal{O}(|R| \cdot \mathsf{poly}(\lambda))$.

Security. We now sketch how we prove the security of the scheme. As mentioned before, we will set all but one key to be malformed in order to prove unforgeability. Whereas in the t-anonymity proof, we set none of the keys to be malformed (recall that t-anonymity requires that the challenge ring as at least t honestly generated verification keys).

To prove unforgeability, we design a reduction that sets all verification keys, but the challenge key vk_{i^*} to be malformed. That is, $\{\mathsf{vk}_i\}_{i\in[\ell]\setminus\{i^*\}}$ are malformedly created using a PRF key K. By the security of the PRF, the adversary is not able to distinguish the case where the verification keys $\{\mathsf{vk}_i\}_{i\in[\ell]\setminus\{i^*\}}$ are well-formed from the case when they are malformed.

The crucial observation now is that the reduction has a valid witness $w = K$ for the statement $x = R$ under which WE ciphertexts are encrypted. This means that, upon receiving a URS forge

$$\Sigma^* = (\mathsf{ct}_0^*, \mathsf{ct}_1^*, \mathsf{hk}_0^*, \mathsf{hk}_1^*, \pi^*)$$

by the adversary, the reduction can use w to decrypt both ct_0^* and ct_1^*. An analysis identical as for the previous scheme shows us that, if Σ^* is a valid

URS signature, then there is a non-negligible probability that one of ct_0^* and ct_1^* decrypts to a valid signature σ^* under vk_{i^*}.

In the t-anonymity proof, we set *none* of the verification keys to be malformed, from which the adversary chooses t of them, say, $\mathsf{vk}_{i_0}, \ldots, \mathsf{vk}_{i_{t-1}}$. If the parameters of the PRF are chosen properly, then there is a negligible probability that $x \in \mathcal{L}$. As explained above, since all t verification keys are sampled independently, it is unlikely that $t-1$ share correlations via a PRF key K. This is because the distribution of $t-1$ honestly generated keys has much more min-entropy than $t-1$ malformed keys. Thus, there will be *at least two well formed* verification keys in the challenge ring R^* with overwhelming probability. We conclude that WE encryptions of σ are indistinguishable from WE encryptions of 0 by the security of the WE.

Given this, we can easily build a sequence of hybrids in a similar fashion as for the previous schemes. That is, given two honestly generated verification keys $\mathsf{vk}_{i_0}, \mathsf{vk}_{i_1}$ and a signature $\Sigma^* = (\mathsf{ct}_0^*, \mathsf{ct}_1^*, \mathsf{hk}_0^*, \mathsf{hk}_1^*, \pi^*)$ for a message m^* with respect to the ring R^* where $\mathsf{vk}_{i_0}, \mathsf{vk}_{i_1} \in R^*$:

1. We first replace ct_1^* by an encryption of a valid signature σ' under vk_{i_1}. By the security of the underlying WE, this change is undetected by the adversary.

2. We switch witnesses from i_0 to i_1, using the witness-indistinguishability of the NIWI scheme.

2.3 Compact Universal Ring Signatures from Indistinguishability Obfuscation

At first glance, the techniques that we employed in the previous construction seem hopeless in our ultimate goal of building a compact URS from falsifiable hardness assumptions. On the one hand, for all known WE schemes that we know of, the size of the ciphertexts grows with the size of the statement. On the other hand, if we try to reduce the size of the statement of the language $\mathcal{L}$, we immediately run into trouble.

The reason for this is that to be able to extract a valid forge, the reduction needs to set up all verification keys but the challenge one in a *special mode*.[5] If the reduction sets just a few of them in this special mode, anonymity does not hold anymore: An adversary breaking anonymity could just use the same strategy as the unforgeability reduction to extract a signature from the challenge URS signature since, in the anonymity game, all but two verification keys may be adversarially chosen.

Given this state of affairs, it seems implausible (or even impossible!) that we can achieve a compact URS scheme just from WE.

Our final contribution is to build a WE scheme for a special type of NP languages that we call *threshold conjunction languages*. A threshold conjunction

[5] In our case, the special mode is when keys are malformed.

language $\mathcal{L}'$ is a language of the form

$$\mathcal{L}' = \{(x_1, \ldots, x_N) : \exists (x_{i_1}, \ldots, x_{i_{N-1}}) \text{ s.t. } x_{i_1} \in \mathcal{L} \wedge \cdots \wedge x_{i_{N-1}} \in \mathcal{L}\}.$$

In other words, given an instance $x = (x_1, \ldots, x_N)$, x is a yes instance of $\mathcal{L}'$ if *all but one* of the x_i are instances of $\mathcal{L}$.

Compact URS from compact WE. Assume for now that we have a *compact* WE scheme for threshold conjunction languages. That is ciphertexts of such a scheme scale only logarithmically with N. Then, plugging this WE scheme into our construction from the previous section immediately yields a compact URS.

Compact witness encryption for threshold conjunction languages. It remains to show how we can obtain such a scheme. For simplicity, we focus on the case where we have N instances $x = (x_1, \ldots, x_N)$ and $x \in \mathcal{L}'$ iff $x_i \in \mathcal{L}$ for all $i \in [N]$. The case where all but one of the statements x_i must be true can be easily obtained by additionally using a secret sharing scheme.

The high-level idea of the construction is as follows: We build an obfuscated circuit $\bar{\mathcal{C}}$ that receives an index $i \in [N]$ and outputs non-compact WE ciphertexts $\mathsf{WE.Enc}(1^\lambda, x_i, r_i)$ for uniform $r_i \leftarrow\!\!\$\, \{0,1\}$.[6] The ciphertext of our new WE scheme for a message $m \in \{0,1\}$ is composed by $\bar{\mathcal{C}}$ and $c = m + \sum r_i$.

If one is in possession of witnesses for all statements x_i, then by the correctness of the underlying non-compact WE scheme, one can recover all r_i. On the other hand, if one of the statements x_{i^*} is false, then we can build a sequence of hybrids where we replace $\mathsf{WE.Enc}(1^\lambda, x_i, r_i)$ by an encryption of 0 and then replace c by a uniform value.

Although the idea seems to work at first glance, there is a critical issue: The scheme is not compact. The reason for this is that we have to hardwire all the statements in $\bar{\mathcal{C}}$, otherwise how does the circuit know under which statements it must encrypt each r_i? To circumvent this problem we use (again!) a somewhere statistically binding (SSB) hashing scheme in a similar way as [HW15].[7] That is, the circuit only has a hash value $h \leftarrow \mathsf{SSB.Hash}(\mathsf{hk}, \{x_1, \ldots, x_N\})$ hardwired. Now, when it receives (i, x_i, γ_i), it first checks if γ_i is a valid opening with respect to x_i, h. Since $\{x_1, \ldots, x_N\}$ is public, anyone can compute a valid opening

$$\gamma_i \leftarrow \mathsf{SSB.Open}(\mathsf{hk}, \{x_1, \ldots, x_N\}, i)$$

for every $i \in [N]$.

Recall that the verification algorithm of an SSB hashing scheme can be implemented in size $\mathcal{O}(\log N \cdot \mathsf{poly}(\lambda))$. Hence, the efficiency requirements are met and the circuit is now of size $\mathcal{O}(\log N \cdot \mathsf{poly}(\lambda))$.

We thus obtain a WE scheme that outputs ciphertexts that depend only logarithmically on N.

[6] To make the circuit size independent of N, we use a pseudorandom function (PRF) to succinctly describe all the r_i. This PRF has to be puncturable in order to use the *puncturing technique* of [SW14].

[7] This time we use SSB in its *statistically binding* form.

How to avoid the exponential security loss of current $i\mathcal{O}$ schemes. We stress that, although the scheme presented above enjoys a polynomial reduction to the underlying cryptographic primitives, current $i\mathcal{O}$ schemes incur a security loss - compared to the underlying hardness assumptions - which is proportional to the size of the domain of the circuit being obfuscated (e.g., [AJ15, BV15, BGL$^+$15]). This implies that the construction presented above suffers from an exponential security loss when we instantiate the $i\mathcal{O}$ scheme by any known construction since the circuit being obfuscated has an exponentially-sized domain.[8]

Intending to avoid this exponential security loss, we present an alternative construction of compact WE for threshold languages where we just obfuscate a program with a polynomial-size domain. Note that, if the domain of the obfuscated program has only polynomial size, then the security reduction from $i\mathcal{O}$ to the underlying hardness assumptions loses only a polynomial factor.

As explained above, the statements cannot be hardwired in the circuit, otherwise, the size of the obfuscated circuit is not compact. To avoid this conundrum, we utilize the $i\mathcal{O}$ for Turing machines (TM) scheme of [GS18].

We note that, in the scheme of [GS18], a TM is modeled as a sequence of circuits. The input is written on a tape and the obfuscated TM accesses the input via a laconic oblivious transfer (LOT) [CDG$^+$17]. We can consider a second tape which includes the statements $(x_1, \ldots, x_N)$ and from which the TM reads from using a LOT in a similar way as in [GS18]. Note that since $(x_1, \ldots, x_N)$ is public knowledge, this tape can be created by any party and does not have to be part of the description of the obfuscated TM. Instead, only the LOT hash needs to be hardwired in the TM. The size of the resulting obfuscated TM depends only logarithmically on the size of this tape.

Given this, to encrypt a message m, one obfuscates a TM $\mathcal{M}$ that receives an index $i \in [N]$ as input, retrieves x_i from the public tape and outputs $\mathsf{WE.Enc}(1^\lambda, x_i, r_i)$.[9] A ciphertext is composed by $\bar{\mathcal{M}}$ (which is the result of obfuscating $\mathcal{M}$) and $c = m + \sum r_i$. Decryption works exactly as before.

As mentioned before, the size of $\bar{\mathcal{M}}$ depends only logarithmically on N and, hence, the size of the ciphertext is $\mathcal{O}(\log N \cdot \mathsf{poly}(\lambda))$.

Furthermore, since the obfuscated TM $\bar{\mathcal{M}}$ has a polynomial-size domain, its security proof incurs only a polynomial security loss compared to the underlying hardness assumption.

3 Preliminaries

Throughout this work, λ denotes the security parameter and PPT stands for "probabilistic polynomial-time". A negligible function $\mathsf{negl}(n)$ in n is a function that vanishes faster than the inverse of any polynomial in n.

[8] Observe that the obfuscated circuit receives as input an index i, a statement x_i and an SSB proof γ_i.

[9] We remark that the underlying WE also has a domain of polynomial size hence it only looses a polynomial factor in security if it is based on $i\mathcal{O}$ [GGH$^+$13, GS18].

For $n \in \mathbb{N}$, $[n]$ denotes the set $\{1, \ldots, n\}$.

If S is a (finite) set, we denote by $x \leftarrow\!\!\$\, S$ an element $x \in S$ sampled according to a uniform distribution. If D is a distribution over S, $x \leftarrow\!\!\$\, D$ denotes an element $x \in S$ sampled according to D. If $\mathcal{A}$ is an algorithm, $y \leftarrow \mathcal{A}(x)$ denotes the output y after running $\mathcal{A}$ on input x. If $\mathcal{A}$ and $\mathcal{O}$ are algorithms, $\mathcal{A}^{\mathcal{O}}$ means that $\mathcal{A}$ has oracle access to $\mathcal{O}$.

We now present the cryptographic primitives used as building blocks for our main construction.

3.1 Signature Schemes

Definition 1 (Signature Scheme)**.** *A signature scheme* Sig *is composed of the following algorithms:*

- $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda; r)$ *takes as input the security parameter* λ *and random coins* $r \in \{0,1\}^\lambda$ *(whenever* r *is omitted, it means it is chosen uniformly at random). It outputs a pair of verification and signing keys* $(\mathsf{vk}, \mathsf{sk})$*.*
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$ *takes as input a signing key* sk *and a message* m*. It outputs a signature* σ*.*
- $b \leftarrow \mathsf{Verify}(\mathsf{vk}, \sigma, m)$ *takes as input a verification key* vk*, a signature* σ *and a message* m*. It outputs a bit* $b \in \{0,1\}$*.*

A signature scheme needs to have the following properties.

Definition 2 (Correctness)**.** *We say that a signature scheme is correct if for all* $\lambda \in \mathbb{N}$ *and every message* m *we have that*

$$\Pr\left[1 \leftarrow \mathsf{Verify}(\mathsf{vk}, \sigma, m) : \begin{array}{c}(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ \sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)\end{array}\right] = 1.$$

Definition 3 (Existential Unforgeability against Chosen Message Attacks)**.** *We say that a signature scheme is existentially unforgeable against chosen message attacks (EUF-CMA) if for all* $\lambda \in \mathbb{N}$ *and all adversaries* $\mathcal{A}$ *we have that*

$$\Pr\left[1 \leftarrow \mathsf{Verify}(\mathsf{vk}, \sigma^*, m^*) : \begin{array}{c}(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ (m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathsf{sk}, \cdot)}(\mathsf{vk})\end{array}\right] \leq \mathsf{negl}(\lambda)$$

where m^* *was never queried to the oracle* $\mathsf{Sign}(\mathsf{sk}, \cdot)$*.*

3.2 Non-Interactive Witness-Indistinguishable Proof Systems

Let $\mathcal{X}$ be a set and $\mathcal{L} \subseteq \mathcal{X}$ an NP language with witness space $\mathcal{W}$ and witness relation $\mathcal{R}$, i.e., $\mathcal{L} = \{x \in \mathcal{X} : \exists w \in \mathcal{W} \text{ s.t. } \mathcal{R}(x, w) = 1\}$.

Definition 4 (NIWI)**.** *Let $\mathcal{L}$ be an* NP *language. A non-interactive witness-indistinguishable (NIWI) proof system* NIWI *for language $\mathcal{L}$ is composed of the following algorithms:*

- $\pi \leftarrow \mathsf{Prove}(1^\lambda, x, w)$ *takes as input a security parameter λ, a statement $x \in \mathcal{X}$ and a witness $w \in \mathcal{W}$. It outputs a proof π.*
- $b \leftarrow \mathsf{Verify}(x, \pi)$ *takes as input a statement $x \in \mathcal{X}$ and a proof π. It outputs a bit $b \in \{0,1\}$.*

Definition 5 (Perfect Completeness)**.** *We say that a NIWI proof system is perfectly correct if for all $\lambda \in \mathbb{N}$, all statements $x \in \mathcal{X}$ and all witnesses $w \in \mathcal{W}$, if $\mathcal{R}(x,w) = 1$, then*

$$\Pr\left[1 \leftarrow \mathsf{Verify}(x,\pi) : \pi \leftarrow \mathsf{Prove}(1^\lambda, x, w)\right] = 1.$$

Definition 6 (Perfect Soundness)**.** *We say that a NIWI proof system has perfect soundness if for all $\lambda \in \mathbb{N}$, all statements $x \notin \mathcal{L}$ and all proofs π we have that*

$$\Pr\left[0 \leftarrow \mathsf{Verify}(x,\pi)\right] = 1.$$

Definition 7 (Witness-Indistinguishability)**.** *We say that a NIWI proof system is witness-indistinguishable if for all $\lambda \in \mathbb{N}$ and all adversaries $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ we have that*

$$\left|\Pr\left[b = b' : \begin{array}{l}(x, w_0, w_1, \mathsf{aux}) \leftarrow \mathcal{A}_1(1^\lambda);\ b \leftarrow\!\$\ \{0,1\} \\ \pi \leftarrow \mathsf{Prove}(1^\lambda, x, w_b);\ b' \leftarrow \mathcal{A}_2(\pi, \mathsf{aux})\end{array}\right] - \frac{1}{2}\right| \leq \mathsf{negl}(\lambda).$$

NIWI schemes can be constructed from pairing assumptions [GOS06a], i$\mathcal{O}$ [BP15] or derandomization assumptions [BOV03].

Proof size. Let $\mathcal{C}_x$ be the verification circuit for statement x and a certain relation $\mathcal{R}$, that is, $1 \leftarrow \mathcal{C}_x(w)$ if and only if $\mathcal{R}(x,w) = 1$. All known NIWI schemes for a relation $\mathcal{R}$ achieve a proof size $|\pi| \in \mathcal{O}\left(|\mathcal{C}_x| \cdot \mathsf{poly}(\lambda)\right)$ where $\pi \leftarrow \mathsf{NIWI.Prove}(x, w)$.

3.3 Commitment Schemes

Definition 8 (Commitment Scheme)**.** *A (non-interactive) commitment scheme (CS)* CS *is composed of the following algorithms:*

- $(\mathsf{com}, \gamma) \leftarrow \mathsf{Commit}(1^\lambda, m)$ *takes as input the security parameter λ and a message m. It outputs a commitment* com *and an opening information γ.*
- $b \leftarrow \mathsf{Verify}(\mathsf{com}, m, \gamma)$ *takes as input a commitment* com*, a message m and opening information γ. It outputs a bit $b \in \{0,1\}$.*

Definition 9 (Correctness)**.** *We say that a commitment scheme is correct if for all $\lambda \in \mathbb{N}$ and every message m we have that*

$$\Pr\left[1 \leftarrow \mathsf{Verify}(\mathsf{com}, m, \gamma) : (\mathsf{com}, \gamma) \leftarrow \mathsf{Commit}(1^\lambda, m)\right] = 1.$$

Definition 10 (Computational Hiding)**.** *We say that a commitment scheme is computationally hiding if for all $\lambda \in \mathbb{N}$ and all PPT adversaries $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ we have that*

$$\left| \Pr \left[b \leftarrow \mathcal{A}_2(\mathsf{com}, \mathsf{aux}) : \begin{array}{c} (m_0, m_1, \mathsf{aux}) \leftarrow \mathcal{A}_1(1^\lambda) \\ b \leftarrow\!\!\$ \{0,1\} \\ (\mathsf{com}, \gamma) \leftarrow \mathsf{Commit}(1^\lambda, m_b) \end{array} \right] - \frac{1}{2} \right| \leq \mathsf{negl}(\lambda).$$

Definition 11 (Perfect Binding)**.** *We say that a commitment scheme is perfectly binding if for all $\lambda \in \mathbb{N}$ and all adversaries $\mathcal{A}$ we have that*

$$\Pr \left[m_0 \neq m_1 \wedge b = b' = 1 : \begin{array}{c} (\mathsf{com}, m_0, \gamma_0, m_1, \gamma_1) \leftarrow \mathcal{A} \\ b \leftarrow \mathsf{Verify}(\mathsf{com}, m_0, \gamma_0) \\ b' \leftarrow \mathsf{Verify}(\mathsf{com}, m_1, \gamma_1) \end{array} \right] = 0.$$

3.4 Somewhere Statistically/Perfectly Binding Hashing

Somewhere statistically binding (SSB) hashing was first presented in [HW15] and several constructions for it were presented in [OPWW15]. In this work we will also use somewhere perfectly binding hashing [BDH+19] which is a stronger notion. However, most realizations of SSB hashing are also SPB hashing [BDH+19]. SPB hashing can then be instantiated from the hardness of assumptions such as DDH, QR or LWE [OPWW15].

Definition 12 (Somewhere Perfectly Binding Hashing)**.** *A somewhere perfectly binding (SPB) hashing scheme* SPB *is composed of the following algorithms:*

- $(\mathsf{hk}, \mathsf{shk}) \leftarrow \mathsf{Gen}(1^\lambda, n, i)$ *takes as input the security parameter λ, $n \in \mathbb{N}$ and an index $i \in [n]$. It outputs a pair of hashing and secret keys* $(\mathsf{hk}, \mathsf{shk})$.
- $h \leftarrow \mathsf{Hash}(\mathsf{hk}, D)$ *takes as input a hashing key* hk *and a database D of size n. It outputs a hash value h.*
- $\tau \leftarrow \mathsf{Open}(\mathsf{hk}, \mathsf{shk}, D, i)$ *takes as input a hashing key* hk*, a secret key* shk*, a database D and an index i. It outputs a proof τ.*
- $b \leftarrow \mathsf{Verify}(\mathsf{hk}, h, i, x, \tau)$ *takes as input a hashing key* hk*, a hash value h, an index i, a value x and a proof τ. It outputs a bit $b \in \{0,1\}$.*

We require that a SPB hashing scheme fulfills the following efficiency guarantees:

1. The hashing key hk and the proof τ are both of size $\mathcal{O}(\mathsf{poly}(\lambda) \cdot \log n)$;
2. The Verify algorithm can be represented by a circuit of size $\mathcal{O}(\mathsf{poly}(\lambda) \cdot \log n)$.

Additionally, an SPB hashing scheme fulfills the following properties.

Definition 13 (Correctness)**.** *We say that a SPB hashing scheme is correct if for all $\lambda \in \mathbb{N}$, all $n = \mathsf{poly}(\lambda)$, all databases D of size n, all indices $j, i \in [n]$ we have that*

$$\Pr\left[1 \leftarrow \mathsf{Verify}(\mathsf{hk}, h, i, x, \tau) : \begin{array}{c}(\mathsf{hk}, \mathsf{shk}) \leftarrow \mathsf{Gen}(1^\lambda, n, j) \\ h \leftarrow \mathsf{Hash}(\mathsf{hk}, D) \\ \tau \leftarrow \mathsf{Open}(\mathsf{hk}, \mathsf{shk}, D, i)\end{array}\right] = 1.$$

Definition 14 (Somewhere Perfectly Binding)**.** *We say that a SPB hashing scheme is somewhere perfectly binding if for all $\lambda \in \mathbb{N}$, all $n = \mathsf{poly}(\lambda)$, all keys hk, all databases D of size n, all indices $i \in [n]$, all database values x and all proofs τ we have that*

$$\Pr\left[D_i = x : \begin{array}{c}h \leftarrow \mathsf{Hash}(\mathsf{hk}, D) \\ 1 \leftarrow \mathsf{Verify}(\mathsf{hk}, h, i, x, \tau)\end{array}\right] = 1.$$

Definition 15 (Index Hiding)**.** *We say that a SPB hashing scheme is index hiding if for all $\lambda \in \mathbb{N}$ and all PPT adversaries $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ we have that*

$$\left|\Pr\left[b \leftarrow \mathcal{A}_2(\mathsf{hk}, \mathsf{aux}) : \begin{array}{c}(n, i_0, i_1, \mathsf{aux}) \leftarrow \mathcal{A}_1(1^\lambda) \\ b \leftarrow\!\!\$\, \{0,1\} \\ (\mathsf{hk}, \mathsf{shk}) \leftarrow \mathsf{Gen}(1^\lambda, n, i_b)\end{array}\right] - \frac{1}{2}\right| \leq \mathsf{negl}(\lambda).$$

An alternative with a weaker binding guarantee is SSB. We now present the syntax of SSB which is almost identical to the one of SPB.

Definition 16. *A somewhere statistically binding (SSB) scheme* SSB *is composed of the following algorithms*

- $\mathsf{hk} \leftarrow \mathsf{Gen}(1^\lambda, n, i)$ *takes as input the security parameter λ, $n \in \mathbb{N}$ and an index $i \in [n]$. It outputs a hashing key* hk*.*
- $h \leftarrow \mathsf{Hash}(\mathsf{hk}, D)$ *which is the same as above.*
- $\tau \leftarrow \mathsf{Open}(\mathsf{hk}, D, i)$ *takes as input a hashing key* hk*, a database D and an index i. It outputs a proof τ.*
- $b \leftarrow \mathsf{Verify}(\mathsf{hk}, h, i, x, \tau)$ *which is the same as above.*

An SSB also satisfies correctness, index hiding and the same efficiency requirements as above. These definitions can be straightforwardly adapted to SSB. Additionally, SSB must be somewhere statistically binding as defined below.

Definition 17 (Somewhere statistically binding)**.** *We say that a SSB hashing scheme is somewhere statistically binding if for all $\lambda \in \mathbb{N}$, all $n = \mathsf{poly}(\lambda)$, all databases D of size n, all indices $i \in [n]$, all database values x and all proofs τ we have that*

$$\Pr\left[D_i = x : \begin{array}{c}\mathsf{hk} \leftarrow \mathsf{Gen}(1^\lambda, n, i) \\ h \leftarrow \mathsf{Hash}(\mathsf{hk}, D) \\ 1 \leftarrow \mathsf{Verify}(\mathsf{hk}, h, i, x, \tau)\end{array}\right] = 1.$$

3.5 Pseudorandom Generators

We recall the definition of pseudorandom generators.

Definition 18 (Pseudorandom Generators)**.** *Let $\alpha = \alpha(\lambda)$ and $\beta = \beta(\lambda)$ be two polynomials. A pseudorandom generator $\mathsf{PRG} : \{0,1\}^\alpha \to \{0,1\}^\beta$ is a function such that for all PPT adversaries $\mathcal{A}$ we have that*

$$\left|\Pr\left[1 \leftarrow \mathcal{A}(\nu) : \begin{array}{c} s \leftarrow\$ \{0,1\}^\alpha \\ \nu \leftarrow \mathsf{PRG}(s) \end{array}\right] - \Pr\left[1 \leftarrow \mathcal{A}(\nu) : \nu \leftarrow\$ \{0,1\}^\beta\right]\right| \leq \mathsf{negl}(\lambda).$$

3.6 Witness Encryption

Witness encryption [GGSW13] is a special type of encryption where a message is encrypted with respect to an NP statement. Decryption is only possible for someone holding a corresponding witness.

Definition 19 (Witness Encryption)**.** *Let $\mathcal{L}$ be an NP language with relation $\mathcal{R}$. A witness encryption WE scheme for $\mathcal{L}$ is composed of the following algorithms:*

- $\mathsf{ct} \leftarrow \mathsf{Enc}(1^\lambda, x, m)$ *takes as input the security parameter λ, a statement $x \in \mathcal{X}$ and a message m. It outputs a ciphertext ct.*
- $m \leftarrow \mathsf{Dec}(w, \mathsf{ct})$ *takes as input a witness $w \in \mathcal{W}$ and a ciphertext ct. It outputs a message m.*

Definition 20 (Correctness)**.** *We say that a WE is correct if for all $\lambda \in \mathbb{N}$, all $x \in \mathcal{L}$ and all messages m we have that*

$$\Pr\left[m \leftarrow \mathsf{Dec}(w, \mathsf{ct}) : \mathsf{ct} \leftarrow \mathsf{Enc}(1^\lambda, x, m)\right] = 1$$

where $w \in \mathcal{W}$ is such that $\mathcal{R}(x, w) = 1$.

The standard security definition for witness encryption is soundness security.

Definition 21 (Soundness Security)**.** *We say that a WE is soundness secure if for all $\lambda \in \mathbb{N}$, for all adversaries $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ and for all $x \notin \mathcal{L}$ we have that*

$$\left|\Pr\left[b \leftarrow \mathcal{A}_2(\mathsf{ct}, \mathsf{aux}) : \begin{array}{c} (m_0, m_1, \mathsf{aux}) \leftarrow \mathcal{A}_1(1^\lambda) \\ b \leftarrow\$ \{0,1\} \\ \mathsf{ct} \leftarrow \mathsf{Enc}(1^\lambda, x, m_b) \end{array}\right] - \frac{1}{2}\right| \leq \mathsf{negl}(\lambda).$$

WE can be constructed from i$\mathcal{O}$ [GGH+13] or multilinear maps [GGSW13].

Ciphertext Size. Let $\mathcal{C}_x$ be the verification circuit for a statement x and a relation $\mathcal{R}$, that is, $1 \leftarrow \mathcal{C}_x(w)$ if and only if $\mathcal{R}(x, w) = 1$. All known WE schemes for a relation $\mathcal{R}$ achieve a ciphertext size $|\mathsf{ct}| \in \mathcal{O}\left(|\mathcal{C}_x| \cdot \mathsf{poly}(\lambda)\right)$ where $\mathsf{ct} \leftarrow \mathsf{WE.Enc}(1^\lambda, x, m)$.

3.7 Indistinguishability Obfuscation

Indistinguishability obfuscation [BGI+12] roughly states, that it is hard to distinguish obfuscations of functionally equivalent circuits.

Let $\mathsf{iO}(1^\lambda, \mathcal{C})$ be a uniform PPT algorithm that takes as input a security parameter λ and a circuit $\mathcal{C}$ and outputs a circuit $\bar{\mathcal{C}}$. iO is called an $i\mathcal{O}$ obfuscator for a circuit family $\mathfrak{C}$ if the following properties hold.

Definition 22 (Correctness)**.** *We say that an $i\mathcal{O}$ obfuscator iO is correct if for all $\lambda \in \mathbb{N}$, all $\mathcal{C} \in \mathfrak{C}$, all inputs x we have that*

$$\Pr\left[\bar{\mathcal{C}}(x) = \mathcal{C}(x) : \bar{\mathcal{C}} \leftarrow \mathsf{iO}(1^\lambda, \mathcal{C})\right] = 1$$

Definition 23 (Security)**.** *We say that an $i\mathcal{O}$ obfuscator iO is secure if for all $\lambda \in \mathbb{N}$, all pairs $(\mathcal{C}_0, \mathcal{C}_1)$ such that $|\mathcal{C}_0| = |\mathcal{C}_1|$ and $\mathcal{C}_0(x) = \mathcal{C}_1(x)$ for all inputs x, and all PPT adversaries $\mathcal{A}$ we have that*

$$\left|\Pr\left[1 \leftarrow \mathcal{A}(\bar{\mathcal{C}}) : \bar{\mathcal{C}} \leftarrow \mathsf{iO}(1^\lambda, \mathcal{C}_0)\right] - \Pr\left[1 \leftarrow \mathcal{A}(\bar{\mathcal{C}}) : \bar{\mathcal{C}} \leftarrow \mathsf{iO}(1^\lambda, \mathcal{C}_1)\right]\right| \leq \mathsf{negl}(\lambda).$$

3.8 Puncturable Pseudorandom Functions

Pseudorandom functions (PRF) were first introduced in [GGM84]. In this work, we use the concept of puncturable PRFs [BW13, KPTZ13, BGI14].

Definition 24 (Puncturable PRF)**.** *Let $\alpha = \alpha(\lambda)$ and $\beta = \beta(\lambda)$ be two polynomials. A puncturable PRF (PPRF) scheme $\mathsf{PPRF}_{\alpha,\beta} = \mathsf{PPRF}$ is composed of the following algorithms:*

- $k \leftarrow \mathsf{KeyGen}(1^\lambda)$ *takes as input a security parameter λ. It outputs a key k.*
- $y \leftarrow \mathsf{Eval}(k, x)$ *takes as input a key k and $x \in \{0,1\}^\alpha$. It outputs $y \in \{0,1\}^\beta$.*
- $k_S \leftarrow \mathsf{Punct}(k, S)$ *takes as input a key k and a subset $S \subseteq \{0,1\}^\alpha$. It outputs a punctured key k_S.*
- $y \leftarrow \mathsf{EvalPunct}(k_S, x)$ *takes as input a punctured key k_S and $x \in \{0,1\}^\alpha$. It outputs $y \in \{0,1\}^\beta$.*

Definition 25 (Correctness)**.** *A PPRF scheme PPRF is said to be correct if for all $\lambda \in \mathbb{N}$, for all $S \subseteq \{0,1\}^\alpha$, all $x \notin S$ we have that*

$$\Pr\left[\mathsf{Eval}(k, x) = \mathsf{EvalPunct}(k_S, x) : \begin{array}{c} k \leftarrow \mathsf{KeyGen}(1^\lambda) \\ k_S \leftarrow \mathsf{Punct}(k, S) \end{array}\right] = 1.$$

Definition 26 (Pseudorandomness)**.** *A PPRF scheme PPRF is said to be pseudorandom at punctured points if for all $\lambda \in \mathbb{N}$, all PPT adversaries $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ we have that*

$$\left|\begin{array}{l} \Pr\left[1 \leftarrow \mathcal{A}_2(k_S, S, T, \mathsf{aux}) : \begin{array}{c} (S, \mathsf{aux}) \leftarrow \mathcal{A}_1(1^\lambda);\ k \leftarrow \mathsf{KeyGen}(1^\lambda) \\ k_S \leftarrow \mathsf{Punct}(k, S);\ T \leftarrow \mathsf{Eval}(k, S) \end{array}\right] - \\ \Pr\left[1 \leftarrow \mathcal{A}_2(k_S, S, T, \mathsf{aux}) : \begin{array}{c} (S, \mathsf{aux}) \leftarrow \mathcal{A}_1(1^\lambda);\ k \leftarrow \mathsf{KeyGen}(1^\lambda) \\ k_S \leftarrow \mathsf{Punct}(k, S);\ T \leftarrow_\$ \{0,1\}^{\beta|S|} \end{array}\right] \end{array}\right| \leq \mathsf{negl}(\lambda).$$

Puncturable PRFs that can be punctured at $|S| = \mathsf{poly}(\lambda)$ points and they can be constructed from one-way functions. The size of the punctured key is $\mathcal{O}(|S| \cdot \mathsf{poly}(\lambda))$.

3.9 Linear Secret Sharing

Linear secret sharing (LSS) is used to divide a secret into shares such that if one is in possession of an authorized set of shares, then one can reconstruct the secret. In this work, we use threshold LSS (which, for simplicity, we simply refer to as LSS).

Definition 27 (Linear Secret Sharing)**.** *Let $t \leq N$. A (t, N)-linear secret sharing (LSS)* LSS *scheme is composed of the following algorithms:*

- $(s_1, \ldots, s_N) \leftarrow \mathsf{Share}(m)$ *takes as input a message m. It outputs N shares $(s_1, \ldots, s_N)$.*
- $m \leftarrow \mathsf{Reconstruct}(s_{i_1}, \ldots, s_{i_t})$ *takes as input t shares $(s_{i_1}, \ldots, s_{i_t})$. It outputs a message m.*

A (t, N)-LSS scheme, which is generated by a generating matrix in the systematic form, has the following additional algorithm:

- $(s_{i_{z+1}}, \ldots, s_{i_N}) \leftarrow \mathsf{RemainShare}(m, s_{i_1}, \ldots, s_{i_z})$ *that takes as input a message m and uniformly chosen shares $s_{i_j} \leftarrow\!\!\$\, \{0,1\}^\lambda$ for $j \in [z]$ with $z < t$, and outputs the remaining shares $(s_{i_{z+1}}, \ldots, s_{i_N})$.*

Definition 28 (Correctness)**.** *A LSS scheme* LSS *is said to be correct if for all messages m and all subsets $\{i_1, \ldots, i_t\} \subseteq [N]$*

$$\Pr\left[m = \mathsf{Reconstruct}(s_{i_1}, \ldots, s_{i_t}) : (s_1, \ldots, s_N) \leftarrow \mathsf{Share}(m)\right] = 1.$$

Moreover,

$$\Pr\left[m = \mathsf{Reconstruct}(s_{i_1}, \ldots, s_{i_t}) : \begin{array}{c} s_{i_j} \leftarrow\!\!\$\, \{0,1\}^\lambda \text{ for } j \in [z] \\ (s_{i_{z+1}}, \ldots, s_{i_N}) \leftarrow \mathsf{RemainShare}(m, s_{i_1}, \ldots, s_{i_z}) \end{array}\right] = 1$$

where $z < t$.

Definition 29 (Privacy)**.** *We say that a (t, N)-LSS scheme* LSS *is private if for all subsets $\{i_1, \ldots, i_z\} \subset [N]$ where $z < t$, all pairs of messages (m_0, m_1) and all PPT adversaries $\mathcal{A}$ we have that*

$$\left| \begin{array}{c} \Pr\left[1 \leftarrow \mathcal{A}(s_{0,i_1}, \ldots, s_{0,i_z}) : (s_{0,1}, \ldots, s_{0,N}) \leftarrow \mathsf{Share}(m_0)\right] - \\ \Pr\left[1 \leftarrow \mathcal{A}(s_{1,i_1}, \ldots, s_{1,i_z}) : (s_{1,1}, \ldots, s_{1,N}) \leftarrow \mathsf{Share}(m_1)\right] \end{array} \right| \leq \mathsf{negl}(\lambda).$$

4 Universal Ring Signatures

In this section we present the definition of URS. A URS is composed of a signing and a verification algorithm.

Definition 30 (Universal Ring Signature)**.** *A universal ring signature (URS) scheme* URS *is composed of the following algorithms:*

- $\Sigma \leftarrow \mathsf{Sign}(1^\lambda, \mathsf{sk}_i, m, R, i, S)$ *takes as input a security parameter* 1^λ*, a signing key* sk_i*, a message* m*, a ring of keys* $R = (\mathsf{vk}_1, \ldots, \mathsf{vk}_\ell)$ *an index* $i \in [\ell]$ *and a list of signature schemes* $S = \{\mathsf{Sig}_i = (\mathsf{Sig.KeyGen}_i, \mathsf{Sig.Sign}_i, \mathsf{Sig.Verify}_i)\}_{i\in[M]}$*, where each* vk_j *is a public verification key under exactly one*[10] *of the schemes* Sig_i*. It outputs a signature* Σ*.*
- $b \leftarrow \mathsf{Verify}(\Sigma, m, R, S)$ *takes as input a signature* σ*, a message* m*, a ring of keys* R *and a list of signature schemes* S*. It outputs a bit* $b \in \{0, 1\}$*.*

We want a URS to fulfill correctness, unforgeability and anonymity.

Definition 31 (Correctness)**.** *We say that a URS* $\mathsf{URS} = (\mathsf{Sign}, \mathsf{Verify})$ *is* correct *if for all* $\lambda \in \mathbb{N}$*, all* $\ell, M = \mathsf{poly}(\lambda)$*, all correct signature schemes* Sig'*, all* $j \in [\ell]$*, all messages* m *and all* $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{Sig}'.\mathsf{KeyGen}(1^\lambda)$*, we have that*

$$\Pr\left[1 \leftarrow \mathsf{Verify}\left(\mathsf{Sign}(1^\lambda, \mathsf{sk}, m, R, j, S), m, R, S\right)\right] = 1$$

for any $R = (\mathsf{vk}_1, \ldots, \mathsf{vk}_\ell)$ *such that* $\mathsf{vk}_j = \mathsf{vk}$ *and any* $S = \{\mathsf{Sig}_i\}_{i\in[M]}$ *such that* $\mathsf{Sig}' \in S$*. That is, the remaining elements in* R, S *may be arbitrarily chosen.*

We now define the unforgeability of a URS. A URS scheme should be compatible with any signature scheme. Hence, we would like to let the adversary choose signature schemes for the URS scheme. However, the adversary could choose an insecure signature scheme and, in this case, we cannot guarantee unforgeability. Hence, the experiment should provide a list of secure signature schemes and verification keys at the beginning of the experiment. The forge given by the adversary must be with respect to these verification keys.[11] Our definition is similar to the one of *unforgeability with respect to insider corruption* for standard ring signatures [BKM06], which is the strongest unforgeability definition.

Definition 32 (Unforgeability)**.** *Let* $\mathcal{A}$ *be an adversary. We denote by* Ls *a list of challenge signature schemes*

$$\mathsf{Ls} = \{\mathsf{Sig}_i = (\mathsf{Sig.KeyGen}_i, \mathsf{Sig.Sign}_i, \mathsf{Sig.Verify}_i)\}_{i\in[M]}.$$

Consider the following experiment, denoted by $\mathsf{Exp}^{\mathsf{URS}}_{\mathsf{Unf}}(\mathsf{Ls}, \mathcal{A}, 1^\lambda)$*:*

1. *The experiment provides* Ls *to* $\mathcal{A}$*.*
2. *The adversary outputs a list of indices* $\{\mathsf{ind}_i\}_{i\in[\ell]}$*.*

[10] In practice, keys/certificates are usually annoted with their respective schemes and we assume such a labelling here.

[11] Note that, in the unforgeability definition for standard ring signatures in [BKM06] a similar situation happens: The forge of the adversary must be with respect to verification keys created honestly and not with respect to maliciously chosen verification keys.

3. *For all* $i \in [\ell]$*, the experiment computes* $(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Sig.KeyGen}_{\mathsf{ind}_i}(1^\lambda)$ *and outputs* $R = (\mathsf{vk}_1, \ldots, \mathsf{vk}_\ell)$ *to the adversary. Also it initialises a set* $\mathcal{K} = \emptyset$ *and remembers the indices* ind_i*.*

4. *The adversary may now make three types of requests*[12]*:*

   - $\texttt{Corrupt}(i)$*, which the experiment answers with the secret key* sk_i*. Also it adds* vk_i *to* $\mathcal{K}$*.*
   - $\texttt{URSSign}(m, \bar{R}, i, \bar{S})$ *takes as input an index* $i \in [\ell]$*, a message* m*, a ring of keys* $\bar{R}$ *(not necessarily contained in* R*) and a list of signature schemes* $\bar{S}$*. If* $\mathsf{vk}_i \in \bar{R}$*, we denote its position as* i^**. If additionally* $\mathsf{Sig}_{\mathsf{ind}_i} \in \bar{S}$*, the experiment answers with* $\Sigma \leftarrow \mathsf{URS.Sign}(1^\lambda, \mathsf{sk}_i, m, \bar{R}, i^*, \bar{S})$*.*
   - $\texttt{Sign}(m, i)$ *takes as input an index* $i \in [\ell]$ *and a message* m*. The experiment answers with* $\Sigma \leftarrow \mathsf{Sig.Sign}_{\mathsf{ind}_i}(1^\lambda, \mathsf{sk}_i, m)$*.*

5. $\mathcal{A}$ *outputs* $(\Sigma^*, m^*, R^*, S^*)$*.*

6. *If* $1 \leftarrow \mathsf{Verify}(\Sigma^*, m^*, R^*, S^*)$*,* $R^* \subseteq R \setminus \mathcal{K}$*,* $S^* \subseteq \mathsf{Ls}$ *and the message* m^* *was never queried in a* `URSSign` *or* `Sign` *request, the experiment outputs* 1.[13] *Else, it outputs* 0*.*

We say that a URS $\mathsf{URS} = (\mathsf{Sign}, \mathsf{Verify})$ *is* unforgeable*, if for all* $\lambda \in \mathbb{N}$*,* $M = \mathsf{poly}(\lambda)$*, all lists of EUF-CMA secure signature schemes* $\mathsf{Ls} = \{\mathsf{Sig}_i\}_{i \in [M]}$ *and all PPT adversaries* $\mathcal{A}$ *we have that*

$$\Pr\left[1 \leftarrow \mathsf{Exp}^{\mathsf{URS}}_{\mathsf{Unf}}(\mathsf{Ls}, \mathcal{A}, 1^\lambda)\right] = \mathsf{negl}(\lambda).$$

In the anonymity experiment, the goal of the adversary is to guess which user created a given signature. We give a general definition called t-anonymity, which mandates that at least t honest keys in the anonymity set must be honestly chosen for anonymity to hold. The adversary may include at least t honest and additional maliciously chosen verification keys (potentially from insecure signature schemes) in a challenge ring. It should still be unable to determine which of the honest parties signed a given URS under that ring.

The case of 2-anonymity coincides with the definition of *anonymity against full key exposure* of [BKM06]. This is the strongest anonymity definition for ring signatures and is even known to imply unrepudiability, meaning that a member in the ring cannot prove that they did not sign the message [PS19a]. As it is the standard case, we will refer to 2-anonymity as *anonymity* throughout this work.

[12] Note that as the key generation algorithms are publicly available, the adversary may honestly generate key pairs itself. The corruption oracle simply serves to corrupt the initial honest keys. Arbitrary additional adversarially chosen keys can be included in ring signature queries, as we do not require $\bar{R} \subseteq R$.

[13] We can consider the stronger notion, where a forge is valid, if no query of the form $\texttt{URSSign}(m^*, R^*, \cdot, \cdot)$ or $\texttt{Sign}(m^* || R^*, i)$ for $\mathsf{vk}_i \in R^*$ was made. This can be achieved by the standard trick of signing the message $(m^* || R^*)$ instead of m^* or a hash $H(m^* || R^*)$ thereof for compactness.

Definition 33 (t-Anonymity)**.** *Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ be an adversary. We denote a list of challenge signature schemes by $\mathsf{Ls} = \{\mathsf{Sig}_i = (\mathsf{Sig.KeyGen}_i, \mathsf{Sig.Sign}_i, \mathsf{Sig.Verify}_i)\}_{i\in[M]}$. We define the t-anonymity experiment $\mathsf{Exp}^{\mathsf{URS}}_{\mathsf{Anon}_t}(\mathsf{Ls}, \mathcal{A}, 1^\lambda)$ as follows:*

1. $(\{\mathsf{ind}_i\}_{i\in[\ell]}, \mathsf{aux}_1) \leftarrow \mathcal{A}_1(1^\lambda, \mathsf{Ls})$.
2. *For all $i \in [\ell]$, the experiment computes $(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Sig.KeyGen}_{\mathsf{ind}_i}(1^\lambda; \mathsf{r}_i)$ with random coins r_i and sets $K = (\mathsf{vk}_1, \ldots, \mathsf{vk}_\ell)$.*
3. *$(m^*, R^* = (\mathsf{vk}'_1, \ldots, \mathsf{vk}'_p), S^* = (\mathsf{Sig}'_1, \ldots, \mathsf{Sig}'_q), (j_k)_{k\in[t]}, \mathsf{aux}_2) \leftarrow \mathcal{A}_2(K, (\mathsf{r}_1, \ldots, \mathsf{r}_\ell), \mathsf{aux}_1)$ where $\mathsf{vk}'_{j_k} \in K$ for $k \in [t]$ with indices l_k in K (i.e. $\mathsf{vk}'_{j_k} = \mathsf{vk}_{l_k}$). Additionally, the signature schemes corresponding to these public keys, $\mathsf{Sig}_{\mathsf{ind}_{l_k}}$, must be in the set S^*. If these conditions are violated, the experiment aborts.*
4. *$\Sigma^* \leftarrow \mathsf{URS.Sign}(1^\lambda, \mathsf{sk}_{l_k}, m^*, R^*, j_k, S^*)$ where $k \leftarrow\!\!\$\, [t]$.*
5. *$k' \leftarrow \mathcal{A}_3(\Sigma^*, \mathsf{aux}_2)$.*
6. *If $k = k'$, then output 1. Else, output 0.*

We say that a URS $\mathsf{URS} = (\mathsf{Sign}, \mathsf{Verify})$ is t-anonymous*, if for all $\lambda \in \mathbb{N}$, all sizes $M = \mathsf{poly}(\lambda)$, all lists of signature schemes $\mathsf{Ls} = \{\mathsf{Sig}_i\}_{i\in[M]}$ and all PPT adversaries $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ we have that*

$$\left|\Pr\left[1 \leftarrow \mathsf{Exp}^{\mathsf{URS}}_{\mathsf{Anon}_t}(\mathsf{Ls}, \mathcal{A}, 1^\lambda)\right] - \frac{1}{t}\right| = \mathsf{negl}(\lambda).$$

Efficiency of URS. We remark that URS inherits the efficiency of the most inefficient signature scheme in the ring. For this reason, it is unlikely that we can construct a URS with good and practical parameters and efficiency.

5 Universal Ring Signature from Signature Schemes with Superpolynomial Security

In this section, we present a construction of URS that is based on signature schemes that are superpolynomially hard to forge. From this hardness, we can prove security of the URS scheme using complexity leveraging.

5.1 Construction

We start by presenting the construction of this URS scheme.

For simplicity, we assume, that there is an upper bound on the size of all descriptions of signature verification circuits. Also, for public keys $\mathsf{vk} \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$, we assume that they are labeled with their respective schemes. That is, there is a function $\mathsf{tag}(.,.)$ which takes vk and a signature scheme Sig

and outputs 1, iff the key vk was made under Sig, but 0 for any other signature verification scheme as input. $\mathsf{Sig.Verify}$ should only accept keys vk with the corresponding tag to Sig, that is $\mathsf{tag}(\mathsf{vk}, \mathsf{Sig}) = 1$.

In the scheme below, we use a commitment scheme whose hiding property holds against PPT adversaries, but can be broken in superpolynomial time $T'(\lambda) \in \omega(\mathsf{poly}(\lambda))$ Additionally, we assume that all used signature schemes are unforgeable against adversaries running in $\mathcal{O}(T'(\lambda) \cdot \mathsf{poly}(\lambda))$. A signature of our URS for a message m includes a commitment to a signature of m in one of the underlying signature schemes. This will give our reduction, that runs in superpolynomial time, an advantage in the unforgeability experiment, where it may extract the commitments and provide a forge against the underlying signature scheme. However, this opening strategy cannot be used by an adversary against anonymity, as they are running in polynomial time.

Construction 1. *Let:*

- CS *be a commitment scheme such that the hiding property holds against polynomial-time adversaries but can be broken in superpolynomial-time* $T'(\lambda) \in \omega(\mathsf{poly}(\lambda))$.
- SPB *be a SPB hashing scheme;*
- $\mathcal{L}$ *be a language such that*

$$\mathcal{L} = \left\{ \begin{array}{c} (m, \mathsf{com}, \mathsf{hk}, h, \mathsf{rhk}, rh) : \exists (\mathsf{vk}, i, \mathsf{Sig.Verify}, \mathsf{ind}, \tau, \rho, \sigma, \gamma) \ s.t. \\ 1 \leftarrow \mathsf{SPB.Verify}(\mathsf{hk}, h, i, \mathsf{vk}, \tau) \\ 1 \leftarrow \mathsf{SPB.Verify}(\mathsf{rhk}, rh, \mathsf{ind}, \mathsf{Sig.Verify}, \rho) \\ 1 \leftarrow \mathsf{CS.Verify}(\mathsf{com}, \sigma, \gamma) \\ 1 \leftarrow \mathsf{Sig.Verify}(\mathsf{vk}, m, \sigma) \end{array} \right\};$$

  where $\mathsf{Sig.Verify}$ *is a description of the verification algorithm of a signature scheme* Sig.[14]

- NIWI *be a NIWI scheme for the language*

$$\mathcal{L}_{\mathsf{OR}} = \left\{ \begin{array}{c} (m, \mathsf{com}_0, \mathsf{com}_1, \mathsf{hk}_0, \mathsf{hk}_1, h_0, h_1, \mathsf{rhk}_0, \mathsf{rhk}_1, rh_0, rh_1) : \\ \exists b \in \{0,1\} \ s.t. \ (m, \mathsf{com}_b, \mathsf{hk}_b, h_b, \mathsf{rhk}_b, rh_b) \in \mathcal{L} \end{array} \right\}.$$

We now describe our scheme in full detail.

$\mathsf{Sign}(1^\lambda, \mathsf{sk}_i, m, R = (\mathsf{vk}_1, \ldots, \mathsf{vk}_\ell), i, S = \{\mathsf{Sig}_i\}_{i \in [M]})$

- *Determine an index* ind *such that* $\mathsf{tag}(\mathsf{vk_i}, \mathsf{Sig_{ind}})$. *Parse* $\mathsf{Sig_{ind}} = (\mathsf{Sig.KeyGen}, \mathsf{Sig.Sign}, \mathsf{Sig.Verify})$. *Set* $S' = \{\mathsf{Sig.Verify}_i\}_{i \in [M]}$ *to be the list of verification algorithms in* S.
- *Compute* $\sigma \leftarrow \mathsf{Sig.Sign}(\mathsf{sk}_i, m)$.

[14] We assume that for all schemes, $|\mathsf{Sig.Verify}|$ is bounded by a polynomial $\beta(\lambda)$.

- *Compute* $(\mathsf{hk}_j, \mathsf{shk}_j) \leftarrow \mathsf{SPB.Gen}(1^\lambda, \ell, i)$ *and* $h_j \leftarrow \mathsf{SPB.Hash}(\mathsf{hk}_j, R)$ *for* $j \in \{0,1\}$. *Also, compute the proof* $\tau \leftarrow \mathsf{SPB.Open}(\mathsf{hk}_0, \mathsf{shk}_0, R, i)$.
- *Compute* $(\mathsf{rhk}_j, \mathsf{rshk}_j) \leftarrow \mathsf{SPB.Gen}(1^\lambda, M, \mathsf{ind})$ *and* $rh_j \leftarrow \mathsf{SPB.Hash}(\mathsf{rhk}_j, S')$ *for* $j \in \{0,1\}$. *Also, compute the proof* $\rho \leftarrow \mathsf{SPB.Open}(\mathsf{rhk}_0, \mathsf{rshk}_0, S', \mathsf{ind})$.
- *Compute* $(\mathsf{com}_0, \gamma_0) \leftarrow \mathsf{CS.Commit}(1^\lambda, \sigma)$ *and* $(\mathsf{com}_1, \gamma_1) \leftarrow \mathsf{CS.Commit}(1^\lambda, 0)$.
- *Set* $x = (m, \mathsf{com}_0, \mathsf{com}_1, \mathsf{hk}_0, \mathsf{hk}_1, h_0, h_1, \mathsf{rhk}_0, \mathsf{rhk}_1, rh_0, rh_1)$.
- *Set* $w = (\mathsf{vk}, i, \mathsf{Sig.Verify}_{\mathsf{ind}}, \mathsf{ind}, \tau, \rho, \sigma, \gamma_0)$.
- *Compute the proof* $\pi \leftarrow \mathsf{NIWI.Prove}(x, w)$.
- *Output* $\Sigma = (\mathsf{com}_0, \mathsf{com}_1, \mathsf{hk}_0, \mathsf{hk}_1, \mathsf{rhk}_0, \mathsf{rhk}_1, \pi)$.

$\mathsf{Verify}(\Sigma, m, R, S = \{\mathsf{Sig}_i\}_{i\in[M]})$:

- *Parse* Σ *as* $(\mathsf{com}_0, \mathsf{com}_1, \mathsf{hk}_0, \mathsf{hk}_1, \mathsf{rhk}_0, \mathsf{rhk}_1, \pi)$. *Set* $S' = \{\mathsf{Sig.Verify}_i\}_{i\in[M]}$ *to be the list of verification algorithms in* S.
- *Compute* $h_j \leftarrow \mathsf{SPB.Hash}(\mathsf{hk}_j, R)$ *for* $j \in \{0,1\}$.
- *Compute* $rh_j \leftarrow \mathsf{SPB.Hash}(\mathsf{rhk}_j, S')$ *for* $j \in \{0,1\}$.
- *Set* $x = (m, \mathsf{com}_0, \mathsf{com}_1, \mathsf{hk}_0, \mathsf{hk}_1, h_0, h_1, \mathsf{rhk}_0, \mathsf{rhk}_1, rh_0, rh_1)$.
- *If* $1 \leftarrow \mathsf{NIWI.Verify}(x, \pi)$, *output* 1. *Else, output* 0.

We remark, that we only require the verification algorithms of the underlying signature schemes to verify a URS signature. Therefore, we only include these algorithms in S', which is hashed down by SPB and provided to NIWI. This is to reduce size. Essentially, our verification algorithm URS.Verify could only take the list of signature verification algorithms S' as an input, but we state the full list of signature schemes to fit our more general definition.

Signature size. A signature for a message m with respect to a ring R (of size ℓ) and a list of schemes S (of size M) is composed of $\Sigma = (\mathsf{com}_0, \mathsf{com}_1, \mathsf{hk}_0, \mathsf{hk}_1, \mathsf{rhk}_0, \mathsf{rhk}_1, \pi)$. Both $\mathsf{com}_0, \mathsf{com}_1$ are of size $\mathcal{O}(\mathsf{poly}(\lambda))$ and independent of ℓ and M. The size of the hashing keys $\mathsf{hk}_0, \mathsf{hk}_1$, the proof τ and the circuit $\mathsf{SPB.Verify}(\mathsf{hk}, h, i, \mathsf{vk}, \tau)$ can be bounded by $\mathcal{O}(\log(\ell) \cdot \mathsf{poly}(\lambda))$. Analogously, $\mathsf{rhk}_0, \mathsf{rhk}_1$, ρ and the runtime of $\mathsf{SPB.Verify}(\mathsf{rhk}, rh, \mathsf{ind}, \mathsf{Sig.Verify}, \rho)$ are bounded by $\mathcal{O}(\log(M) \cdot \mathsf{poly}(\lambda))$.[15]

Given that, we conclude that the circuit that verifies the relation of language $\mathcal{L}$ has size at most $\mathcal{O}((\log(M) + \log(\ell)) \cdot \mathsf{poly}(\lambda))$. Hence, the proof π has size $\mathcal{O}((\log(M) + \log(\ell)) \cdot \mathsf{poly}(\lambda))$. We conclude that the total size of the signature is $\mathcal{O}((\log(M) + \log(\ell)) \cdot \mathsf{poly}(\lambda))$. Thus, it grows only logarithmic in the number of users in the ring and logarithmic in the number of signature schemes.

[15]This holds, as we assumed, that we can bound $|\mathsf{Sig.Verify}|$ by a polynomial $\beta(\lambda)$ for all signature schemes Sig.

5.2 Proofs

We now show that the construction presented above fulfills the required properties for a URS. We start by showing correctness. Then we proceed to prove unforgeability and anonymity. Our proof of unforgeability uses a superpolynomial-time reduction.

Theorem 5 (Correctness)**.** *The scheme presented in Construction 1 is correct, given that* NIWI *is perfectly complete and* SPB *and* CS *are correct.*

Proof. Let $\lambda \in \mathbb{N}$, $\ell, M = \mathsf{poly}(\lambda)$, $j \in [\ell]$, message m and a correct signature scheme Sig' be given. Let keys be constructed by $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{Sig}'.\mathsf{KeyGen}(1^\lambda)$. Let a ring $R = (\mathsf{vk}_1, \ldots, \mathsf{vk}_\ell)$ be chosen with $\mathsf{vk}_j = \mathsf{vk}$ and $S = (\mathsf{Sig}_1, \ldots, \mathsf{Sig}_M)$ such that $\mathsf{Sig}' \in S$. Now we need to show, that

$$\Pr\left[1 \leftarrow \mathsf{Verify}\left(\mathsf{Sign}(1^\lambda, \mathsf{sk}, m, R, j, S), m, R, S\right)\right] = 1$$

As SPB is deterministic and all other values are explicitly given, the input statement $(m, \mathsf{com}_0, \mathsf{com}_1, \mathsf{hk}_0, \mathsf{hk}_1, h_0, h_1, \mathsf{rhk}_0, \mathsf{rhk}_1, rh_0, rh_1)$ to NIWI.Verify is the same as what was originally input to NIWI.Prove. So by the perfect completeness of NIWI, we only need to show that $w \leftarrow (\mathsf{vk}, i, \mathsf{Sig.Verify}_{\mathsf{ind}}, \mathsf{ind}, \tau, \rho, \sigma, \gamma_0)$ was in fact a valid witness. The statement $1 \leftarrow \mathsf{CS.Verify}(\mathsf{com}_0, \sigma, \gamma_0)$ holds by construction and the correctness of CS. Also note, that by assumption there exists an index ind such that $\mathsf{Sig}_{\mathsf{ind}}$ is the scheme corresponding to vk, so such an index can be chosen in URS.Sign. The conditions in $\mathcal{L}_{\mathsf{OR}}$ are then fulfilled for the first disjunct by construction and using the correctness of SPB and $\mathsf{Sig}_{\mathsf{ind}}$. □

Theorem 6 (Unforgeability)**.** *We assume, that our commitment scheme allows extraction in superpolynomial time $T'(\lambda) \in \omega(\mathsf{poly}(\lambda))$, but is secure against PPT adversaries. Assume that the challenge signature schemes $\mathsf{LS} = \{\mathsf{Sig}_i\}_{i \in [M]}$ are unforgeable against adversaries running in time $T'(\lambda) \cdot \mathsf{poly}(\lambda)$. Then the scheme presented in Construction 1 is unforgeable against PPT adversaries, given that* NIWI *is perfectly sound and* SPB *is somewhere perfectly binding.*

At a high-level, we will build a superpolynomial-time reduction that breaks unforgeability for the underlying signature scheme. The reduction, upon receiving the challenge URS signature $\Sigma^* = (\mathsf{com}_0^*, \mathsf{com}_1^*, \mathsf{hk}_0^*, \mathsf{hk}_1^*, \mathsf{rhk}_0^*, \mathsf{rhk}_1^*, \pi^*)$ from the adversary, opens the commitments com_0^* and com_1^* using brute force. Note that, since we allow the reduction to run in superpolynomial time, it will succeed in breaking the hiding property of the commiment scheme. Then, by the perfect soundess of the NIWI scheme, the reduction can extract a valid signature from either com_0 or com_1 with non-negligible probability and, thus, break the unforgeability of the signature scheme.

Proof. To prove the theorem, we show that if there exists a PPT adversary, that is able to win the unforgeability experiment of Definition 32, then we can build an algorithm that is able to forge a signature for one of the underlying Sig_i schemes in time $T'(\lambda) \cdot \mathsf{poly}(\lambda)$. More precisely, if $\mathcal{A}$ is able to break the

unforgeability, then there exists an algorithm $\mathcal{B}$ that breaks the EUF-CMA security of one of the Sig_i. In the following, let $\mathcal{C}$ be the challenger of Definition 3. We now describe $\mathcal{B}(\mathsf{Ls})$ in full detail:

1. $\mathcal{B}$ provides $\mathsf{Ls} = \{\mathsf{Sig}_i\}_{i\in[M]}$ to $\mathcal{A}$.

2. Upon receiving the indices $\{\mathsf{ind}_i\}_{i\in[\ell]}$ from $\mathcal{A}$, $\mathcal{B}$ guesses an index $i^* \leftarrow [\ell]$ uniformly at random. It creates $(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Sig.KeyGen}_{\mathsf{ind}_i}(1^\lambda)$ for all $i \neq i^*$ and sets vk_{i^*} to be a verification key under $\mathsf{Sig}_{\mathsf{ind}_{i^*}}$ given by the challenger for EUF-CMA security of that scheme $\mathcal{C}$. It sends $R = \{\mathsf{vk}_i\}_{i\in[\ell]}$ to $\mathcal{A}$.

3. $\mathcal{B}$ simulates the oracles $\mathtt{OCorrupt}$, $\mathtt{URSign}$ and $\mathtt{OSign}$ in the following way:

   - $\mathtt{OCorrupt}(i)$: Whenever $\mathcal{A}$ sends a query i, $\mathcal{B}$ reveals sk_i if $i \neq i^*$. Otherwise, it aborts the protocol;
   - $\mathtt{URSign}(m, \bar{R}, i, \bar{S})$: Whenever $\mathcal{A}$ sends a query $(m, \bar{R}, i, \bar{S})$, $\mathcal{B}$ proceeds as in the experiment, if $i \neq i^*$. If $i = i^*$, $\mathcal{B}$ checks whether $\mathsf{vk}_{i^*} \in \bar{R}$ and denotes its position as j^*. If additionally $\mathsf{Sig}_{\mathsf{ind}_{i^*}} \in \bar{S}$, $\mathcal{B}$ sends a query to $\mathcal{C}$ for message m. Upon receiving the signature σ for m, they compute a signature Σ as they would in $\mathsf{URS.Sign}(1^\lambda, \mathsf{sk}_{i^*}, m, \bar{R}, j^*, \bar{S})$, except that they use the σ they received instead of computing it by $\mathsf{Sig.Sign}_{\mathsf{ind}_{i^*}}(\mathsf{sk}_{i^*}, m)$. This can be done without the knowledge of sk_{i^*}.
     $\mathcal{B}$ returns Σ to $\mathcal{A}$.
   - $\mathtt{OSign}(i, m)$: Whenever $\mathcal{A}$ sends a query (i, m) with $i \neq i^*$, $\mathcal{B}$ sends $\sigma \leftarrow \mathsf{Sig.Sign}(\mathsf{sk}_i, m)$. Otherwise, it sends a query m to $\mathcal{C}$ and, upon receiving a signature σ, it outputs σ to $\mathcal{A}$.

4. Upon receiving $\Sigma^* = (\mathsf{com}_0^*, \mathsf{com}_1^*, \mathsf{hk}_0^*, \mathsf{hk}_1^*, \mathsf{rhk}_0^*, \mathsf{rhk}_1^*, \pi^*)$, plus m^*, R^* and S^* from $\mathcal{A}$, $\mathcal{B}$ opens both commitments com_0 and com_1 to recover σ_0^* and σ_1^*, respectively. By assumption, this can be done in time $2T'(\lambda)$. If $1 \leftarrow \mathsf{Sig.Verify}(\mathsf{vk}_{i^*}, m^*, \sigma_0^*)$, it outputs σ_0^*. Else if $1 \leftarrow \mathsf{Sig.Verify}(\mathsf{vk}_{i^*}, m^*, \sigma_1^*)$, it outputs σ_1^*. Else, it aborts.

We now analyze the success probability of $\mathcal{B}$ in breaking the EUF-CMA property of Definition 3.

Before $\mathcal{A}$ outputs a potential forge, unless they query to corrupt vk_{i^*}, $\mathcal{B}$ only differs from the experiment, in that it queries a signing oracle for vk_{i^*} instead of computing signatures itself. Therefore until such a query would be made, the index i^* is uniform in the view of $\mathcal{A}$. The probability that $\mathcal{A}$ does not query $\mathsf{OCorrupt}$ on i^* is thus at least $1/\ell$. We now condition on this query not happening: Assume that Σ^* output by $\mathcal{A}$ is such that $1 \leftarrow \mathsf{Verify}(\Sigma^*, m^*, R^*, S^*)$, where $R^* = (\mathsf{vk}_{i_1}, \ldots, \mathsf{vk}_{i_{\ell'}})$.

Since NIWI is perfectly sound, then w.l.o.g, $(m^*, \mathsf{com}_0, \mathsf{hk}_0, h_0, \mathsf{rhk}_0, rh_0) \in \mathcal{L}$. This means there exists a tuple $(\mathsf{vk}', i', \mathsf{Sig.Verify}', \mathsf{ind}', \tau', \rho', \sigma', \gamma')$ such that $1 \leftarrow \mathsf{SPB.Verify}(\mathsf{hk}_0, h_0, i', \mathsf{vk}', \tau')$, $1 \leftarrow \mathsf{SPB.Verify}(\mathsf{rhk}_0, rh_0, \mathsf{ind}', \mathsf{Sig.Verify}', \rho')$,

$1 \leftarrow \mathsf{CS.Verify}(\mathsf{com}_0, \sigma', \gamma')$ and $1 \leftarrow \mathsf{Sig.Verify}'(\mathsf{vk}', m^*, \sigma')$. Thus, by the somewhere perfectly binding property of SPB we have that $\mathsf{vk}' = \mathsf{vk}_{i_{i'}}$ with probability 1. Moreover, since i^* is chosen uniformly at random from the point-of-view of $\mathcal{A}$, then $i^* = i_{i'}$ with probability at least $1/\ell$. Since we assumed that the vk are tagged with what scheme they correspond to, we can assume here that this is then a valid forge under Sig'.

If this happens, then σ' is a valid signature for message m^* under vk_{i^*} and $\mathcal{B}$ is able to break the EUF-CMA of Sig_{i^*} with probability at least $\frac{1}{\ell^2} \Pr\left[1 \leftarrow \mathsf{Exp}^{\mathsf{URS}}_{\mathsf{Unf}}\right]$.

Now, we need to analyse the time which $\mathcal{B}$ requires. Since $\mathcal{A}$ is PPT, and the answering of requests is possible in polynomial time as well, as all algorithms invoked run in $\mathsf{poly}(\lambda)$, the time spent until $\mathcal{A}$ outputs a forge is in $\mathsf{poly}(\lambda)$. Then, $\mathcal{B}$ runs in a total time of $2T'(\lambda)+\mathsf{poly}(\lambda)$. This contradicts the assumption that Sig_{i^*} is EUF-CMA against adversaries running in time $\mathcal{O}(\mathsf{poly}(\lambda) \cdot T'(\lambda))$. □

Theorem 7 (Anonymity)**.** *Assume that* SPB *is index hiding,* NIWI *is witness-indistinguishable and* CS *is hiding. Then the scheme presented in Construction 1 is anonymous.*

To prove the theorem above, we build a sequence of hybrids starting from the anonymity game where $b = 0$ and ending at a hybrid describing the game for $b = 1$. Let vk_{i_0} and vk_{i_1} be the challenge verification keys in the anonymity game and let $\Sigma = (m^*, \mathsf{com}_0, \mathsf{com}_1, \mathsf{hk}_0, \mathsf{hk}_1, \mathsf{rhk}_0, \mathsf{rhk}_1, \pi)$ be the challenge signature build using vk_{i_0}. In the first hybrid, we change hk_1 and rhk_1 to be SPB hashing keys binding to index i_1. Next, we replace com_1 by a commitment of a valid signature under vk_{i_1}. In the next hybrid, we can replace the proof π by a new one computed using the new signature under vk_{i_1} (this change goes unnoticed by the witness indistinguishability of the NIWI). We can now replace com_0 by a commitment of a valid signature under vk_{i_1}. In the next step, we replace hk_0 and rhk_0 to be SPB hashing keys binding to index i_1 and, finally, compute π as the proof that com_0 is a commitment to a valid signature under vk_{i_1} for which hk_0 and rhk_0 bind to.

Proof. Let $\mathsf{Ls} = \{\mathsf{Sig}_i\}_{i\in[M]}$ be a list of signature schemes. In the following we will only modify our response to $\mathcal{A}$ after they made their challenge query. That means, we have already received indices $\{\mathsf{ind}_i\}_{i\in\ell}$ from $\mathcal{A}$ and provided them with a ring R of verification keys as well as random coins. Let now $(i_0, i_1, m^*, R^*, S^*)$ be the challenge query of $\mathcal{A}$ in the game of Definition 33. We denote by j_0, j_1 the indices of $\mathsf{vk}_{i_0}, \mathsf{vk}_{i_1}$ in R^* and by $\mathsf{ind}'_0, \mathsf{ind}'_1$ the indices of their corresponding signature schemes in S^*. Let S' be the list of signature verification algorithms in S^*. The proof of the theorem follows from the following sequence of hybrids.

Hybrid $\mathcal{H}_0$. This is the real anonymity experiment defined in Definition 33 where $b = 0$. That is, the challenger outputs $\Sigma = (m^*, \mathsf{com}_0, \mathsf{com}_1, \mathsf{hk}_0, \mathsf{hk}_1,$

$\mathsf{rhk}_0, \mathsf{rhk}_1, \pi)$ where

$$\begin{aligned}
\sigma_{i_0} &\leftarrow \mathsf{Sig.Sign}_{\mathsf{ind}_{i_0}}(\mathsf{sk}_{i_0}, m^*) \\
(\mathsf{hk}_a, \mathsf{shk}_a) &\leftarrow \mathsf{SPB.Gen}(1^\lambda, |R^*|, j_0) \text{ for } a \in \{0,1\} \\
\tau &\leftarrow \mathsf{SPB.Open}(\mathsf{hk}_0, \mathsf{shk}_0, R^*, j_0) \\
(\mathsf{rhk}_a, \mathsf{rshk}_a) &\leftarrow \mathsf{SPB.Gen}(1^\lambda, |S'|, \mathsf{ind}'_0) \text{ for } a \in \{0,1\} \\
\rho &\leftarrow \mathsf{SPB.Open}(\mathsf{rhk}_0, \mathsf{rshk}_0, S', \mathsf{ind}'_0) \\
(\mathsf{com}_0, \gamma_0) &\leftarrow \mathsf{CS.Commit}(1^\lambda, \sigma_{i_0}) \\
(\mathsf{com}_1, \gamma_1) &\leftarrow \mathsf{CS.Commit}(1^\lambda, 0) \\
\pi &\leftarrow \mathsf{NIWI.Prove}(x, w)
\end{aligned}$$

where $x = (m, \mathsf{com}_0, \mathsf{com}_1, \mathsf{hk}_0, \mathsf{hk}_1, h_0, h_1, \mathsf{rhk}_0, \mathsf{rhk}_1, rh_0, rh_1)$ and $w = (\mathsf{vk}, j_0, \mathsf{Sig.Verify}_{\mathsf{ind}_{i_0}}, \mathsf{ind}'_0, \tau, \rho, \sigma_{i_0}, \gamma_0)$.

Hybrid $\mathcal{H}_1$. This hybrid is identical to the previous one except that it switches the index in key creation to $(\mathsf{hk}_1, \mathsf{shk}_1) \leftarrow \mathsf{SPB.Gen}(1^\lambda, |R^*|, j_1)$. Additionally, it computes a new opening $\tau' \leftarrow \mathsf{SPB.Open}(\mathsf{hk}_1, \mathsf{shk}_1, R^*, j_1)$.

Claim 1. *Assume that* SPB *is index hiding. Then hybrids $\mathcal{H}_0$ and $\mathcal{H}_1$ are indistinguishable.*

Proof. Assume an adversary $\mathcal{A}$ has a non-negligible advantage in distinguishing $\mathcal{H}_0$ from $\mathcal{H}_1$. We build a reduction $\mathcal{R}$ against the index-hiding game as follows: $\mathcal{R}$ chooses $(|R^*|, j_0, j_1)$ as challenge and receives hk_1 from the challenger. $\mathcal{R}$ uses this key instead of computing $(\mathsf{hk}_1, \mathsf{shk}_1) \leftarrow \mathsf{SPB.Gen}(1^\lambda, |R^*|, j_0)$ in an otherwise perfect simulation of $\mathcal{H}_0$. As τ' is not output in $\mathcal{H}_1$, from the view of $\mathcal{A}$, the output of $\mathcal{R}$ is identical to $\mathcal{H}_0$, if the challenge bit in the index hiding game was 0 and identical to $\mathcal{H}_1$ otherwise. Therefore, we can output whatever $\mathcal{A}$ outputs and receive the same advantage. □

Hybrid $\mathcal{H}_{1b}$. This hybrid is identical to the previous one except that it uses $(\mathsf{rhk}_1, \mathsf{rshk}_1) \leftarrow \mathsf{SPB.Gen}(1^\lambda, |S'|, \mathsf{ind}'_1)$. Additionally, it computes an opening $\rho' \leftarrow \mathsf{SPB.Open}(\mathsf{rhk}_1, \mathsf{rshk}_1, S', \mathsf{ind}'_1)$.

Claim 2. *Assume that* SPB *is index hiding. Then hybrids $\mathcal{H}_1$ and $\mathcal{H}_{1b}$ are indistinguishable.*

The proof is identical to the one for Claim 1.

Hybrid $\mathcal{H}_2$. This hybrid is identical to the previous one except that it uses $\sigma' \leftarrow \mathsf{Sig.Sign}_{\mathsf{ind}_{i_1}}(\mathsf{sk}_{i_1}, m^*)$ and $(\mathsf{com}_1, \gamma_1) \leftarrow \mathsf{CS.Commit}(1^\lambda, \sigma')$.

Claim 3. *Assume that* CS *is hiding. Then hybrids $\mathcal{H}_{1b}$ and $\mathcal{H}_2$ are indistinguishable.*

Proof. Assume an adversary $\mathcal{A}$ has a non-negligible advantage in distinguishing $\mathcal{H}_{1b}$ from $\mathcal{H}_2$. We build a reduction $\mathcal{R}$ against the hiding property of CS as follows: $\mathcal{R}$ chooses $m_0 = 0$ and $m_1 = \sigma'$ as challenge in the hiding game. Then it receives com from the challenger and uses this commitment as com_1 instead of computing com_1 itself in an otherwise perfect simulation of $\mathcal{H}_{1b}$. As γ_1 is not needed in $\mathcal{H}_{1b}$ or $\mathcal{H}_2$, all further computations are possible and the output of $\mathcal{R}$ is identically distributed to $\mathcal{H}_{1b}$, if the commitment hides 0, and it is identically distributed to $\mathcal{H}_2$ otherwise. Therefore, we can output whatever $\mathcal{A}$ outputs and receive the same advantage. □

Hybrid $\mathcal{H}_3$. This hybrid is identical to the previous one except that $\pi \leftarrow \mathsf{NIWI.Prove}(x, w')$ where $w' = (\mathsf{vk}_{i_1}, j_1, \mathsf{Sig.Verify}_{\mathsf{ind}_{i_1}}, \mathsf{ind}'_1, \tau', \rho', \sigma', \gamma_1)$.

Claim 4. *Assume that* NIWI *is witness-indistinguishable. Then hybrids* $\mathcal{H}_2$ *and* $\mathcal{H}_3$ *are indistinguishable.*

Proof. Assume an adversary $\mathcal{A}$' has a non-negligible advantage in distinguishing $\mathcal{H}_2$ from $\mathcal{H}_3$. We build a reduction $\mathcal{R}$ against the witness indistinguishability game as follows: $\mathcal{R}$ chooses (x, w, w') where $w = (\mathsf{vk}_{i_0}, j_0, \mathsf{Sig.Verify}_{\mathsf{ind}_{i_0}}, \mathsf{ind}'_0, \tau, \rho, \sigma_{i_0}, \gamma_0)$ and $w' = (\mathsf{vk}_{i_1}, j_1, \mathsf{Sig.Verify}_{\mathsf{ind}_{i_1}}, \mathsf{ind}'_1, \tau', \rho', \sigma', \gamma_1)$ as their challenge. Then it receives a proof π from the challenger that it uses instead of computing $\pi \leftarrow \mathsf{NIWI.Prove}(x, w)$ in an otherwise perfect simulation of $\mathcal{H}_2$. We remark that by our previous changes, the conditions for the second disjunct in $\mathcal{L}_{\mathsf{OR}}$ are now fulfilled by correctness of $\mathsf{SPB}, \mathsf{CS}$ and Sig if the witness is w'. For the witness w, the first disjunct still holds, as no changes were made to its inputs. This means the statement-witness pairs were valid in all hybrids so far.

Now, clearly the output of $\mathcal{R}$ is identically distributed to $\mathcal{H}_2$, if the challenge bit in the witness indistuingishability game was 0 and to $\mathcal{H}_3$ otherwise. Therefore, we can output whatever $\mathcal{A}$ outputs and receive the same advantage. □

Hybrid $\mathcal{H}_4$. This hybrid is identical to the previous one except that it randomly chooses $\mathsf{com}_0 \leftarrow \mathsf{CS.Commit}(1^\lambda, 0)$.

Claim 5. *Assume that* CS *is hiding. Then hybrids* $\mathcal{H}_3$ *and* $\mathcal{H}_4$ *are indistinguishable.*

The proof of the claim is identical to the proof of Claim 3.

Hybrid $\mathcal{H}_5$. This hybrid is identical to the previous one except that it computes $(\mathsf{hk}_0, \mathsf{shk}_0) \leftarrow \mathsf{SPB.Gen}(1^\lambda, |R^*|, j_1)$, $\tau \leftarrow \mathsf{SPB.Open}(\mathsf{hk}_0, \mathsf{shk}_0, R^*, j_1)$, $(\mathsf{rhk}_0, \mathsf{rshk}_0) \leftarrow \mathsf{SPB.Gen}(1^\lambda, |S'|, \mathsf{ind}'_1)$ and $\rho \leftarrow \mathsf{SPB.Open}(\mathsf{rhk}_0, \mathsf{rshk}_0, S', \mathsf{ind}'_1)$.

Claim 6. *Assume that* SPB *is index hiding. Then hybrids* $\mathcal{H}_4$ *and* $\mathcal{H}_5$ *are indistinguishable.*

The proof of the claim is identical to the proof of Claim 1.

Hybrid $\mathcal{H}_6$. This hybrid is identical to the previous one except that it uses $\sigma'' \leftarrow \mathsf{Sig.Sign}_{\mathsf{ind}_{i_1}}(\mathsf{sk}_{i_1}, m^*)$ and $(\mathsf{com}_0, \gamma_0) \leftarrow \mathsf{CS.Commit}(1^\lambda, \sigma'')$.

Claim 7. *Assume that* CS *is hiding. Then hybrids $\mathcal{H}_5$ and $\mathcal{H}_6$ are indistinguishable.*

The proof of the claim is identical to the proof of Claim 3.

Hybrid $\mathcal{H}_7$. This hybrid is identical to the previous one except that $\pi \leftarrow \mathsf{NIWI.Prove}(x, w'')$ where $w'' = (\mathsf{vk}_{i_1}, j_1, \mathsf{Sig.Verify}_{\mathsf{ind}_{i_1}}, \mathsf{ind}'_1, \tau, \rho, \sigma'', \gamma_0)$.

Claim 8. *Assume that* NIWI *is witness-indistinguishable. Then hybrids $\mathcal{H}_6$ and $\mathcal{H}_7$ are indistinguishable.*

The proof of the claim is identical to the proof of Claim 4. We note, that now again, the first disjunct in $\mathcal{L}_{\mathsf{OR}}$ is fulfilled by the previous modifications.

Hybrid $\mathcal{H}_8$. This hybrid is identical to the previous one except that it randomly chooses $\mathsf{com}_1 \leftarrow \mathsf{CS.Commit}(1^\lambda, 0)$.

Claim 9. *Assume that* CS *is hiding. Then hybrids $\mathcal{H}_7$ and $\mathcal{H}_8$ are indistinguishable.*

The proof of the claim is identical to the proof of Claim 3. Since $\mathcal{H}_8$ is identical to the experiment with challenge bit $b = 1$ and indistinguishable from $\mathcal{H}_0$, we have therefore shown, that $\mathcal{A}$ can not have more than non-negligible advantage. □

6 Non-compact Universal Ring Signature from Witness Encryption

In this section we present a URS scheme from falsifiable assumptions. The resulting URS has a signature size that scales with the size of the ring. We first present the construction. Then, we proceed to the analysis of the scheme.

6.1 Construction

We now present our construction for URS from WE.

Construction 2. *Let*

- $\mathsf{PRF} : \mathcal{K} \times [\ell] \to \{0,1\}^\lambda$ *be a PRF.*
- $\mathcal{L}'$ *be a language such that*

$$\mathcal{L}' = \left\{ \begin{array}{c} (\{\mathsf{vk}_i\}_{i\in[\ell]} : \exists \left(\{\mathsf{Sig}_{i_j}\}_{j\in[\ell-1]}, K\right) \ \ s.t. \\ r_{i_j} \leftarrow \mathsf{PRF}(K, i_j) \\ (\mathsf{vk}_{i_j}, \mathsf{sk}_{i_j}) \leftarrow \mathsf{Sig.KeyGen}_{i_j}(1^\lambda; r_{i_j}) \end{array} \right\}.$$

- WE *be a witness encryption scheme for language* $\mathcal{L}'$.
- SPB *be a SPB hashing scheme;*
- $\mathcal{L}$ *be a language such that*

$$\mathcal{L} = \left\{ \begin{array}{c} (m, \mathsf{ct}, \mathsf{hk}, h, \mathsf{rhk}, rh, x) : \exists (\mathsf{vk}, i, \mathsf{Sig.Verify}, \mathsf{ind}, \tau, \rho, \sigma, r_{\mathsf{ct}}) \ s.t. \\ 1 \leftarrow \mathsf{SPB.Verify}(\mathsf{hk}, h, i, \mathsf{vk}, \tau) \\ 1 \leftarrow \mathsf{SPB.Verify}(\mathsf{rhk}, rh, \mathsf{ind}, \mathsf{Sig.Verify}, \rho) \\ \mathsf{ct} \leftarrow \mathsf{WE.Enc}(1^\lambda, x, \sigma; r_{\mathsf{ct}}) \\ 1 \leftarrow \mathsf{Sig.Verify}(\mathsf{vk}, m, \sigma) \end{array} \right\};$$

  where $\mathsf{Sig.Verify}$ *is a description of the verification algorithm of a signature scheme* Sig.[16]

- NIWI *be a NIWI scheme for the language*

$$\mathcal{L}_{\mathsf{OR}} = \left\{ \begin{array}{c} (m, \mathsf{ct}_0, \mathsf{ct}_1, \mathsf{hk}_0, \mathsf{hk}_1, h_0, h_1, \mathsf{rhk}_0, \mathsf{rhk}_1, rh_0, rh_1, x) : \\ \exists b \in \{0,1\} \ s.t. \ (m, \mathsf{ct}_b, \mathsf{hk}_b, h_b, \mathsf{rhk}_b, rh_b, x) \in \mathcal{L} \end{array} \right\}.$$

We now describe the scheme in full detail.

$\mathsf{Sign}(1^\lambda, \mathsf{sk}_i, m, R = (\mathsf{vk}_1, \ldots, \mathsf{vk}_\ell), i, S = \{\mathsf{Sig}_i\}_{i \in [M]})$**:**

- *Determine an index* ind *with* $\mathsf{tag}(\mathsf{vk_i}, \mathsf{Sig}_{\mathsf{ind}})$. *Parse* $\mathsf{Sig}_{\mathsf{ind}} = (\mathsf{Sig.KeyGen}, \mathsf{Sig.Sign}, \mathsf{Sig.Verify})$. *Set* $S' = \{\mathsf{Sig.Verify}_i\}_{i \in [M]}$ *to be the list of verification algorithms in* S.
- *Compute* $\sigma \leftarrow \mathsf{Sig.Sign}(\mathsf{sk}_i, m)$.
- *Compute* $(\mathsf{hk}_j, \mathsf{shk}_j) \leftarrow \mathsf{SPB.Gen}(1^\lambda, \ell, i)$ *and* $h_j \leftarrow \mathsf{SPB.Hash}(\mathsf{hk}_j, R)$ *for* $j \in \{0,1\}$. *Also, compute the proof* $\tau \leftarrow \mathsf{SPB.Open}(\mathsf{hk}_0, \mathsf{shk}_0, R, i)$.
- *Compute* $(\mathsf{rhk}_j, \mathsf{rshk}_j) \leftarrow \mathsf{SPB.Gen}(1^\lambda, M, \mathsf{ind})$ *and* $rh_j \leftarrow \mathsf{SPB.Hash}(\mathsf{rhk}_j, S')$ *for* $j \in \{0,1\}$. *Also, compute the proof* $\rho \leftarrow \mathsf{SPB.Open}(\mathsf{rhk}_0, \mathsf{rshk}_0, S', \mathsf{ind})$.
- *Encrypt* $\mathsf{ct}_0 \leftarrow \mathsf{WE.Enc}(1^\lambda, x', \sigma; r_{\mathsf{ct}})$ *and* $\mathsf{ct}_1 \leftarrow \mathsf{WE.Enc}(1^\lambda, x', 0)$, *where* $x' = R$.
- *Set* $x = (m, \mathsf{ct}_0, \mathsf{ct}_1, \mathsf{hk}_0, \mathsf{hk}_1, h_0, h_1, \mathsf{rhk}_0, \mathsf{rhk}_1, rh_0, rh_1, x')$.
- *Set* $w = (\mathsf{vk}, i, \mathsf{Sig.Verify}_{\mathsf{ind}}, \mathsf{ind}, \tau, \rho, \sigma, r_{\mathsf{ct}})$.
- *Compute the proof* $\pi \leftarrow \mathsf{NIWI.Prove}(x, w)$.
- *Output* $\Sigma \leftarrow (\mathsf{ct}_0, \mathsf{ct}_1, \mathsf{hk}_0, \mathsf{hk}_1, \mathsf{rhk}_0, \mathsf{rhk}_1, \pi)$.

[16] We assume again, that for all schemes, $|\mathsf{Sig.Verify}|$ is bounded by a polynomial $b(\lambda)$.

$\mathsf{Verify}(\Sigma, m, R, S)$**:**

- *Parse* $\Sigma = (\mathsf{ct}_0, \mathsf{ct}_1, \mathsf{hk}_0, \mathsf{hk}_1, \mathsf{rhk}_0, \mathsf{rhk}_1, \pi)$. *Set* $S' = \{\mathsf{Sig.Verify}_i\}_{i\in[M]}$ *to be the list of verification algorithms in* S.
- *Compute* $h_j \leftarrow \mathsf{SPB.Hash}(\mathsf{hk}_j, R)$ *for* $j \in \{0,1\}$.
- *Compute* $rh_j \leftarrow \mathsf{SPB.Hash}(\mathsf{rhk}_j, S')$ *for* $j \in \{0,1\}$.
- *Set* $x = (m, \mathsf{ct}_0, \mathsf{ct}_1, \mathsf{hk}_0, \mathsf{hk}_1, h_0, h_1, \mathsf{rhk}_0, \mathsf{rhk}_1, rh_0, rh_1, R)$.
- *If* $1 \leftarrow \mathsf{NIWI.Verify}(x, \pi)$*, output* 1*. Else, output* 0.

Signature size. A signature for a message m under a ring R (of size ℓ) and a list of schemes S (of size M) is of the form $\Sigma = (\mathsf{ct}_0, \mathsf{ct}_1, \mathsf{hk}_0, \mathsf{hk}_1, \mathsf{rhk}_0, \mathsf{rhk}_1, \pi)$. We first analyze the size of the ciphertexts $\mathsf{ct}_0, \mathsf{ct}_1$. The circuit that verifies the relation $\mathcal{R}'$ of language $\mathcal{L}'$ needs to have size at least $\mathcal{O}(\ell \cdot \mathsf{poly}(\lambda))$ since witnesses for this language are of that size. It is clear that the conditions can be checked in a circuit of this size.

Moreover, a similar analysis as the one made for Construction 1 shows that the total size of $(\mathsf{hk}_0, \mathsf{hk}_1, \mathsf{rhk}_0, \mathsf{rhk}_1, \pi)$ is $\mathcal{O}((\log \ell + \log M) \cdot \mathsf{poly}(\lambda))$. We may assume, that $M \leq \ell$ because signature schemes that no corresponding key exists for in R may be omitted without altering functionality.

We conclude that the signatures in this scheme have size $\mathcal{O}(\ell \cdot \mathsf{poly}(\lambda))$.

6.2 Proofs

We now give the proofs of the security of the proposed scheme.

Theorem 8 (Correctness)**.** *The scheme presented in Construction 2 is correct, given that* NIWI *is perfectly complete.*

Proof. Let $\lambda \in \mathbb{N}$, $\ell, M = \mathsf{poly}(\lambda)$, and Sig' be a correct signature scheme. Let further $j \in [\ell]$, a messages m and a key pair honestly constructed by $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{Sig}'.\mathsf{Gen}(1^\lambda)$ be given. Now, for $R = (\mathsf{vk}_1, \ldots, \mathsf{vk}_\ell)$ such that $\mathsf{vk}_j = \mathsf{vk}$ and $S = \{\mathsf{Sig}_i\}_{i\in[M]}$ such that $\mathsf{Sig}' \in S$, we have to show

$$\Pr\left[1 \leftarrow \mathsf{Verify}\left(\mathsf{Sign}(1^\lambda, \mathsf{sk}, m, R, j, S), m, R, S\right)\right] = 1$$

.

Clearly, the statement x in $\mathsf{Verify}\left(\mathsf{Sign}(1^\lambda, \mathsf{sk}_j, m, R, j, S), m, R, S\right)$ is identical to the statement in $\mathsf{Sign}(1^\lambda, \mathsf{sk}_j, m, R, j, S)$. Therefore by the perfect completeness of NIWI, it remains to show that $w = (\mathsf{vk}, i, \mathsf{Sig.Verify}_{\mathsf{ind}}, \mathsf{ind}, \tau, \rho, \sigma, r_{\mathsf{ct}})$ was a valid witness. The case $b = 0$ in $\mathcal{L}_{\mathsf{OR}}$ is fulfilled by construction and correctness of Sig' and SPB. Therefore, Verify outputs 1. □

Theorem 9 (Unforgeability)**.** *Assume that* Sig_i *is EUF-CMA,* PRF *is a pseudorandom function,* NIWI *is perfectly sound and* WE *is correct. Then, the scheme presented in Construction 2 is unforgeable.*

To prove unforgeability, we first build a hybrid where the experiment computes all verification keys, except for vk_{i^*}, using randomness from a PRF (instead of using truly random coins). Note that this change goes unnoticed given that PRF is a PRF. Next, we build a reduction to the unforgeability of the underlying signature scheme. The idea is similar to the proof of Theorem 6. Namely, the goal of the reduction is to extract a valid signature from either ct_0 or ct_1. To do this, note that the reduction is in possession of the key K such that vk_i is created using random coins $\mathsf{PRF}(K, i)$, for all $i \neq i^*$ where vk_{i^*} is the challenge verification key. Then, by the correctness of the WE and the perfect soundness of the NIWI, the reduction can use K to decrypt both ct_0 and ct_1. In the end, there is a non-negligible probability that the reduction can extract a valid signature under vk_{i^*}, thus breaking the unforgeability of the signature scheme.

Proof. Let $\mathcal{A}$ be a PPT adversary against the unforgeability of URS. Consider the following sequence of hybrids.

Hybrid $\mathcal{H}_0$. This is the real unforgeability experiment defined in Definition 32. In particular, all verification keys vk_i computed by the challenger are computed honestly using $\mathsf{Sig.KeyGen}_i$. That is, $(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Sig.KeyGen}(1^\lambda)$.

Hybrid $\mathcal{H}_1$. This hybrid is identical to the previous one except that the experiment samples $i^* \leftarrow\!\!\$\, [\ell]$. Let $\{i_1, \ldots, i_{\ell-1}\} = [\ell] \setminus \{i^*\}$.

Note that this hybrid is identically distributed from the view of the adversary.

Hybrid $\mathcal{H}_{2,j}$. This hybrid is identical to the previous one, except that the challenger sets the verification keys vk_{i_j} to be computed using randomness coming from a PRF. That is, the experiment samples $K \leftarrow\!\!\$\, \{0,1\}^\lambda$ and computes $(\mathsf{vk}_{i_j}, \mathsf{sk}_{i_j}) \leftarrow \mathsf{Sig.KeyGen}_{\mathsf{ind}_{i_j}}(1^\lambda, r_{i_j})$ where $r_{i_j} \leftarrow \mathsf{PRF}(K, i_j)$. This hybrid is defined for $j = \{1, \ldots, \ell - 1\}$.

Claim 10. *Assume that* PRF *is a PRF. Then, hybrids* $\mathcal{H}_1$ *and* $\mathcal{H}_{2,\ell-1}$ *are indistinguishable.*

Proof. We prove that hybrids $\mathcal{H}_{2,j-1}$ and $\mathcal{H}_{2,j}$ are indistinguishable, for all $j \in \{1, \ldots, \ell - 1\}$ and where $\mathcal{H}_{2,0} = \mathcal{H}_1$.

Suppose that there is an adversary $\mathcal{A}$ that is able to distinguish hybrids $\mathcal{H}_{2,j-1}$ and $\mathcal{H}_{2,j}$. Then, there is a reduction $\mathcal{R}$ that breaks the security of the underlying PRF.

The reduction receives ν from the challenger and computes the key vk_j by $(\mathsf{vk}_j, \mathsf{sk}_j) \leftarrow \mathsf{Sig.KeyGen}_{\mathsf{ind}_{i_j}}(1^\lambda; \nu)$. For all $i \neq j$, the remaining vk_i are computed as in hybrid $\mathcal{H}_{2,j-1}$. From now on, the reduction behaves exactly as in $\mathcal{H}_{2,j-1}$.

Note that, if $\nu \leftarrow\!\!\$\, \{0,1\}^\beta$ is a uniform string then the simulation is identical to $\mathcal{H}_{2,j-1}$. On the other hand, if $\nu \leftarrow \mathsf{PRF}(K, i_j)$ for some $K \leftarrow\!\!\$\, \{0,1\}^\lambda$ then the simulation is identical to $\mathcal{H}_{2,j}$. Therefore, $\mathcal{R}$ outputs whatever $\mathcal{A}$ outputs and gets the same advantage. □

We now prove that we can reduce the hardness of unforgeability for the scheme in Hybrid $\mathcal{H}_{2,\ell-1}$ to the EUF-CMA of the underlying signature scheme.

Let $\mathcal{A}$ be an adversary that wins in $\mathcal{H}_{2,\ell-1}$. We provide the description of an adversary $\mathcal{B}$ that breaks the EUF-CMA of one of the underlying signature schemes $\mathsf{Sig}_{\mathsf{ind}_{i^*}}$. Let $\mathcal{C}$ be the challenger of Definition 3.

1. $\mathcal{B}$ provides $\mathsf{Ls} = \{\mathsf{Sig}_i\}_{i\in[M]}$ to $\mathcal{A}$.
2. Upon receiving the indices $\{\mathsf{ind}_i\}_{i\in[\ell]}$ from $\mathcal{A}$, $\mathcal{B}$ guesses an index $i^* \leftarrow [\ell]$ uniformly at random. It samples $K \leftarrow\$ \{0,1\}^\lambda$. It creates $(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Sig.KeyGen}_{\mathsf{ind}_i}(1^\lambda; r_i)$ for all $i \neq i^*$ where $r_i \leftarrow \mathsf{PRF}(K, i)$ and sets vk_{i^*} to be a verification key under $\mathsf{Sig}_{\mathsf{ind}_{i^*}}$ given by the challenger $\mathcal{C}$ for EUF-CMA security of that scheme. $\mathcal{B}$ sends $R = \{\mathsf{vk}_i\}_{i\in[\ell]}$ to $\mathcal{A}$.
3. $\mathcal{B}$ simulates the oracles $\mathtt{OCorrupt}$, $\mathtt{URSign}$ and $\mathtt{OSign}$ in the following way:
   - $\mathtt{OCorrupt}(i)$: Whenever $\mathcal{A}$ sends a query i, $\mathcal{B}$ reveals sk_i if $i \neq i^*$. Otherwise, it aborts the protocol;
   - $\mathtt{URSign}(m, \bar{R}, i, \bar{S})$: Whenever $\mathcal{A}$ sends a query $(m, \bar{R}, i, \bar{S})$, $\mathcal{B}$ proceeds as in the experiment, for $i \neq i^*$. If $i = i^*$, $\mathcal{B}$ checks whether $\mathsf{vk}_{i^*} \in \bar{R}$ and denotes its position as j^*. If additionally $\mathsf{Sig}_{\mathsf{ind}_{i^*}} \in \bar{S}$, $\mathcal{B}$ sends a query to $\mathcal{C}$ for message m and, upon receiving the signature σ for m, it proceeds to compute a signature Σ as in the hybrid, using σ instead of computing it itself.
   - $\mathtt{OSign}(i, m)$: Whenever $\mathcal{A}$ sends a query (i, m) with $i \neq i^*$, $\mathcal{B}$ sends $\sigma \leftarrow \mathsf{Sig.Sign}(\mathsf{sk}_i, m)$. Otherwise, it sends a query m to $\mathcal{C}$ and, upon receiving a signature σ, it outputs σ to $\mathcal{A}$.
4. Upon receiving $\Sigma^* = (\mathsf{ct}_0^*, \mathsf{ct}_1^*, \mathsf{hk}_0^*, \mathsf{hk}_1^*, \mathsf{rhk}_0^*, \mathsf{rhk}_1^*, \pi^*)$, plus m^*, R^* and S^* from $\mathcal{A}$, $\mathcal{B}$ decrypts $\sigma_0^* \leftarrow \mathsf{WE.Dec}(w', \mathsf{ct}_0^*)$ and $\sigma_1^* \leftarrow \mathsf{WE.Dec}(w', \mathsf{ct}_1^*)$, using the witness $w' = (\{\mathsf{Sig}_{\mathsf{ind}_i}\}_{i\in[\ell]\setminus\{i^*\}}, K)$. Per our construction of the keys, this is a valid witness. If $1 \leftarrow \mathsf{Sig.Verify}(\mathsf{vk}_{i^*}, m^*, \sigma_0^*)$, it outputs σ_0^*. Else if $1 \leftarrow \mathsf{Sig.Verify}(\mathsf{vk}_{i^*}, m^*, \sigma_1^*)$, it outputs σ_1^*.

Note that the statement x' is in $\mathcal{L}'$, because $\mathcal{B}$ creates all verification keys vk_i as $(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Sig.KeyGen}_{\mathsf{ind}_i}(1^\lambda, r_i)$, where $r_i \leftarrow \mathsf{PRF}(K, i)$ for all $i \neq i^*$. A witness for x' is thus exactly $w' = (\{\mathsf{Sig}_{\mathsf{ind}_i}\}_{i\in[\ell]\setminus\{i^*\}}, K)$.

Following a similar analysis as the one of Theorem 6, we conclude that $\mathcal{B}$ succeeds in extracting a valid forge with probability at least $\frac{1}{\ell^2} \Pr\left[1 \leftarrow \mathsf{Exp}^{\mathsf{URS}}_{\mathsf{Unf}}\right]$.

Remark also that $\mathcal{B}$ only takes polynomial time to output a valid forge, given that $\mathcal{A}$ runs in polynomial time. This concludes the proof of the theorem. □

Theorem 10 (t-Anonymity)**.** *Assume that* NIWI *is witness-indistinguishable,* SPB *is index hiding and* WE *is soundness secure. Then the scheme presented in Construction 2 is t-anonymous where $t = (\lambda - \omega(\log\lambda))/q$ and q is a lower bound of the min-entropy of verification keys in the ring.*

The proof of the theorem is similar to the proof of Theorem 7. However, now we would like to use the security of the WE to replace ct_1 by an encryption of a valid signature under one key (and then replace back by an encryption of 0). To do this, we note that (unlike the unforgeability security proof described above) all verification keys in K are computed using truly random coins. The challenge ring given by the adversary must include at least t of these keys. A simple information-theoretical argument states that there is only a negligible probability that there is a PRF key K such that $t-1$ of these honestly generated verification keys are malformed. This is because they are sampled independently and thus it is unlikely that they are correlated via a PRF key. Hence, we can conclude that $\ell-1$ verification keys in the adversary's ring are not created using random coins $\mathsf{PRF}(K, i)$, except with negligible probability. In other words, there is a negligible probability that $x' \in \mathcal{L}'$. We can thus use the security of the WE to safely replace encryptions of signatures and encryptions of 0. That is, we switch out the encrypted signature in ct_0 from one under one challenge key to a signature under another one.

Proof. Let $\mathsf{Ls} = \{\mathsf{Sig}_i\}_{i\in[M]}$ be a list of unforgeable signature schemes. In the following we will only modify our response to $\mathcal{A}$ after they made their challenge query. That means, we have already received indices $\{\mathsf{ind}_i\}_{i\in\ell}$ from $\mathcal{A}$ and provided them with a ring R of verification keys and respective random coins. Let now $(m^*, R^* = (\mathsf{vk}'_1, \ldots, \mathsf{vk}'_p), S^* = (\mathsf{Sig}'_1, \ldots, \mathsf{Sig}'_q), (j_k)_{k\in[t]})$ be the challenge query of $\mathcal{A}$ in the game of definition 33. Let $j_0 = j_k$ for any $k \in \{2, 3, \ldots, t\}$. We show that the encryptions using vk'_{j_0} and vk'_{j_1} are not distinguishable. Let i_0, i_1 be the indices for these challenge keys in K, that is $\mathsf{vk}_{i_0} = \mathsf{vk}'_{j_0}, \mathsf{vk}_{i_1} = \mathsf{vk}'_{j_1}$ in R^* and by $\mathsf{ind}'_0, \mathsf{ind}'_1$ the indices of their corresponding signature verification schemes in S^*. The proof of the theorem follows from the following sequence of hybrids.

Hybrid $\mathcal{H}_0$. This is the real anonymity experiment defined in Definition 33 where the key at index j_0 is used in encryption. That is, the challenger outputs $\Sigma^* = (\mathsf{ct}_0, \mathsf{ct}_1, \mathsf{hk}_0, \mathsf{hk}_1, \mathsf{rhk}_0, \mathsf{rhk}_1, \pi)$ where

$$\begin{aligned}
\sigma_0 &\leftarrow \mathsf{Sig.Sign}_{\mathsf{ind}_{i_0}}(\mathsf{sk}_{i_0}, m^*)\\
\mathsf{ct}_0 &\leftarrow \mathsf{WE.Enc}(1^\lambda, x', \sigma_0; r_{\mathsf{ct}})\\
\mathsf{ct}_1 &\leftarrow \mathsf{WE.Enc}(1^\lambda, x', 0)\\
\pi &\leftarrow \mathsf{NIWI.Prove}(x, w_0)
\end{aligned}$$

where $x = (m, \mathsf{ct}_0, \mathsf{ct}_1, \mathsf{hk}_0, \mathsf{hk}_1, h_0, h_1, \mathsf{rhk}_0, \mathsf{rhk}_1, rh_0, rh_1, R^*)$, $x' = R^*$ and $w_0 = (\mathsf{vk}, j_0, \mathsf{Sig.Verify}_{\mathsf{ind}_{i_0}}, \mathsf{ind}'_0, \tau, \rho, \sigma_0, r_{\mathsf{ct}})$.

Hybrid $\mathcal{H}_1$. This hybrid is identical to the previous one, except that the challenger sets $(\mathsf{hk}_1, \mathsf{shk}_1) \leftarrow \mathsf{SPB.Gen}(1^\lambda, |R^*|, j_1)$. Additionally, it computes $\tau' \leftarrow \mathsf{SPB.Open}(\mathsf{hk}_1, \mathsf{shk}_1, R^*, j_1)$. Also, it sets $(\mathsf{rhk}_1, \mathsf{rshk}_1) \leftarrow \mathsf{SPB.Gen}(1^\lambda, |S'|, \mathsf{ind}'_1)$. Additionally, it computes $\rho' \leftarrow \mathsf{SPB.Open}(\mathsf{rhk}_1, \mathsf{rshk}_1, S', \mathsf{ind}'_1)$.

Claim 11. *Assume that* SPB *is index hiding. Then hybrids* $\mathcal{H}_0$ *and* $\mathcal{H}_1$ *are indistinguishable.*

The proof of the claim is identical to the proof of Claim 1.

Hybrid $\mathcal{H}_2$. This hybrid is identical to the previous, except that the challenger computes $\sigma_1 \leftarrow \mathsf{Sig.Sign}_{\mathsf{ind}_{i_1}}(\mathsf{sk}_{i_1}, m^*)$ and sets $\mathsf{ct}_1 \leftarrow \mathsf{WE.Enc}(1^\lambda, x', \sigma_1; r'_{\mathsf{ct}})$.

Claim 12. *Assume that* WE *is soundness secure. Then hybrids* $\mathcal{H}_1$ *and* $\mathcal{H}_2$ *are indistinguishable.*

Proof. First, note that all verification keys vk_i given to the adversary $\mathcal{A}$ are generated as $(\mathsf{vk}_i, \mathsf{sk}_i) \leftarrow \mathsf{Sig.KeyGen}_{\mathsf{ind}_i}(1^\lambda; r_i)$ where $r_i \leftarrow\$ \{0,1\}^\lambda$ (here we explicitly input random coins r_i into the key generation algorithm).

We claim that, if each $r_i \leftarrow\$ \{0,1\}^\lambda$, then $x' \notin \mathcal{L}'$ except with negligible probability. To prove this, we show that if $\mathsf{vk}_i \leftarrow \mathsf{Sig.Gen}(1^\lambda, r_i)$ for $r_i \leftarrow\$ \{0,1\}^\lambda$ then there is a negligible probability that there exists a PRF key K such that $\mathsf{vk}'_i \leftarrow \mathsf{Sig.Gen}(1^\lambda, \mathsf{PRF}(K, i))$ and $\mathsf{vk}_i = \mathsf{vk}'_i$ for at least $t-1$ keys.

Assume that the min-entropy of each verification key is at least q bits, that is, $\mathbb{H}_\infty(\mathsf{vk}_i) \geq q$. Since each vk_i is independently sampled then $\mathbb{H}_\infty(\mathsf{vk}_1, \ldots, \mathsf{vk}_{t-1}) \geq (t-1)q$. On the other hand, the number of $t-1$ tuples $(\mathsf{vk}'_1, \ldots, \mathsf{vk}'_{t-1})$ such that each vk'_i is created using $\mathsf{vk}'_i \leftarrow \mathsf{Sig.Gen}(1^\lambda, \mathsf{PRF}(K, i))$ is 2^λ. This is because of two reasons: i) once we choose the PRF key $K \in \{0,1\}^\lambda$, the verification keys vk'_i are fixed; and ii) the number of different PRF keys is 2^λ.

We now compute the probability that $(\mathsf{vk}_1, \ldots, \mathsf{vk}_{t-1}) = (\mathsf{vk}'_1, \ldots, \mathsf{vk}'_{t-1})$ where $\mathsf{vk}'_i \leftarrow \mathsf{Sig.Gen}(1^\lambda, \mathsf{PRF}(K, i))$ for some $K \in \{0,1\}^\lambda$.
Since $\mathbb{H}_\infty(\mathsf{vk}_1, \ldots, \mathsf{vk}_{t-1}) \geq (t-1)q$, then $\Pr[(\mathsf{vk}_1, \ldots, \mathsf{vk}_{t-1}) = (\alpha_1, \ldots, \alpha_{t-1})] \leq 2^{-(t-1)q}$, for any tuple $(\alpha_1, \ldots, \alpha_{t-1})$ in the range of $\mathsf{Sig.Gen}$, by the definition of min-entropy. Hence,

$$\Pr\left[\begin{array}{c}(\mathsf{vk}_1, \ldots, \mathsf{vk}_{t-1}) = \\ (\mathsf{vk}'_1, \ldots, \mathsf{vk}'_{t-1})\end{array} : \begin{array}{c}\mathsf{vk}'_i \leftarrow \mathsf{Sig.Gen}(1^\lambda, \mathsf{PRF}(K, i)) \\ \text{for some } K \in \{0,1\}^\lambda\end{array}\right] \leq 2^\lambda \frac{1}{2^{(t-1)q}} = 2^{\lambda-(t-1)q}$$

where the first inequality is obtained by applying a union bound over the number of possible different PRF keys. Setting $t \geq (\lambda + \omega(\log \lambda))/q + 1$, we get that the probability above is negligible in λ. Hence $x' \notin \mathcal{L}$ except with negligible probability.

Now, since $x' \notin \mathcal{L}'$ and given an adversary that distinguishes both games, we can easily build a reduction $\mathcal{R}$ that breaks the soundness security of the underlying WE. The reduction simply sets $m_0 = 0$ and $m_1 = \sigma_1$ as the messages to be sent to the challenger of the soundness security of WE. Upon receiving a ciphertext ct from the challenger, it sets $\mathsf{ct}_1 = \mathsf{ct}$ in an otherwise perfect simulation of $\mathcal{H}_0$. If $b = 0$ (in the soundness security game), then the game played by $\mathcal{A}$ is identical to $\mathcal{H}_0$, otherwise it is identical to $\mathcal{H}_1$. Therefore, $\mathcal{R}$ outputs whatever $\mathcal{A}$ outputs and gets the same advantage. □

Hybrid $\mathcal{H}_3$. This hybrid is identical to the previous one, except that the challenger computes $\pi \leftarrow \mathsf{NIWI.Prove}(x, w_1)$ where $w_1 = (\mathsf{vk}_{i_1}, j_1, \mathsf{Sig.Verify}_{\mathsf{ind}_{i_1}}, \mathsf{ind}'_1, \tau', \rho', \sigma_1, r'_{\mathsf{ct}})$.

Claim 13. *Assume that* NIWI *is witness indistinguishable. Then hybrids $\mathcal{H}_2$ and $\mathcal{H}_3$ are indistinguishable.*

The proof of the claim is identical to the proof of Claim 4.

Hybrid $\mathcal{H}_4$. This hybrid is identical to the previous, except that the challenger computes $\sigma'_1 \leftarrow \mathsf{Sig.Sign}_{\mathsf{ind}_{i_1}}(\mathsf{sk}_{i_1}, m^*)$ and sets $\mathsf{ct}_0 \leftarrow \mathsf{WE.Enc}(1^\lambda, x', \sigma'_1; r''_{\mathsf{ct}})$.

Claim 14. *Assume that* WE *is soundness secure. Then hybrids $\mathcal{H}_3$ and $\mathcal{H}_4$ are indistinguishable.*

The proof of the claim is identical to the proof of Claim 12.

Hybrid $\mathcal{H}_5$. This hybrid is identical to the previous one, except that the challenger sets $(\mathsf{hk}_0, \mathsf{shk}_0) \leftarrow \mathsf{SPB.Gen}(1^\lambda, |R^*|, j_1)$. It computes $\tau \leftarrow \mathsf{SPB.Open}(\mathsf{hk}_0, \mathsf{shk}_0, R^*, j_1)$. Also, it computes $(\mathsf{rhk}_0, \mathsf{rshk}_0) \leftarrow \mathsf{SPB.Gen}(1^\lambda, |S'|, \mathsf{ind}'_1)$ and $\rho \leftarrow \mathsf{SPB.Open}(\mathsf{rhk}_0, \mathsf{rshk}_0, S', \mathsf{ind}'_1)$.

Claim 15. *Assume that* SPB *is index hiding. Then hybrids $\mathcal{H}_4$ and $\mathcal{H}_5$ are indistinguishable.*

The proof of the claim is identical to the proof of Claim 1.

Hybrid $\mathcal{H}_6$. This hybrid is identical to the previous one except that the challenger sets $\pi \leftarrow \mathsf{NIWI.Prove}(x, w_2)$ for $w_2 = (\mathsf{vk}_{i_1}, j_1, \mathsf{Sig.Verify}_{\mathsf{ind}_{i_1}}, \mathsf{ind}'_1, \tau, \rho, \sigma'_1, r''_{\mathsf{ct}})$.

Claim 16. *Assume that* NIWI *is witness indistinguishable. Then hybrids $\mathcal{H}_5$ and $\mathcal{H}_6$ are indistinguishable.*

The proof of the claim is identical to the proof of Claim 4.

Hybrid $\mathcal{H}_7$. This hybrid is identical to the previous one except that the challenger sets $\mathsf{ct}_1 \leftarrow \mathsf{WE.Enc}(1^\lambda, x', 0)$.

Claim 17. *Assume that* WE *is soundness secure. Then hybrids $\mathcal{H}_6$ and $\mathcal{H}_7$ are indistinguishable.*

The proof of the claim is identical to the proof of Claim 12.

This hybrid is identical to the real anonymity experiment of Definition 33 where the key at index j_1 is used in encryption. This concludes the proof of the theorem. □

7 Compact Witness Encryption for Threshold Conjunction Languages

In this section we present a WE scheme that is compact for threshold conjunction languages. We first define the notion of threshold conjunction languages.

Definition 34 (Threshold Conjunction Languages)**.** *Let $\mathcal{L}$ be an* NP *language, with relation $\mathcal{R}$. We define a (t, N)-threshold conjunction language $\mathcal{L}'$ as follows*

$$\mathcal{L}' = \left\{(x_1, \ldots, x_N) : \exists \{i_j\}_{j\in[t]} \in [N] \text{ s.t. } x_{i_j} \in \mathcal{L}\right\}.$$

In other words, an accepting instance $(x_1, \ldots, x_N)$ of $\mathcal{L}'$ is one such that there are at least t accepting instances x_{i_j}.

7.1 Construction from Indistinguishability Obfuscation

We now describe our WE scheme for any (t, N)-threshold conjunction language $\mathcal{L}'$. The protocol achieves compact ciphertexts, i.e., of size $\mathcal{O}(\log N)$, when $N - t \in \mathcal{O}(\log N)$.

Construction 3. *Let $N \in \mathsf{poly}(\lambda)$ and t be such that $N - t \in \mathcal{O}(\log N)$ and $\mathcal{L}$ be an* NP *language. Let*

- LSS *be a (t, N)-LSS scheme. In the following, we assume that shares can be written as strings in $\{0, 1\}^\lambda$.*
- WE *be a (non-compact) WE scheme for language $\mathcal{L}$.*
- iO *be an obfuscator for all circuits.*
- PPRF *be a puncturable PRF.*
- SSB *be an SSB hashing scheme.*

Additionally, consider the following circuit $\mathcal{C}[\lambda, \mathsf{hk}, h, k_0, k_1, t, N]$ which has the values λ, hk, h, k_0, k_1, t and N hardwired.

$\mathcal{C}[\lambda, \mathsf{hk}, h, k_0, k_1, t, N](i, \tau_i, x_i)$:

- *If* $0 \leftarrow \mathsf{SSB.Verify}(\mathsf{hk}, h, i, x_i, \tau_i)$ *or* $i \geq t$*, return* $\perp$*.*
- *Compute* $s_i \leftarrow \mathsf{PPRF.Eval}(k_0, i)$ *and random coins* $r_i \leftarrow \mathsf{PPRF.Eval}(k_1, i)$*.*
- *Compute* $\mathsf{ct}_i \leftarrow \mathsf{WE.Enc}(1^\lambda, x_i, s_i; r_i)$*. Output* ct_i*.*

We now define the WE scheme for the (t, N)-conjunction language $\mathcal{L}'$.

$\mathsf{Enc}(1^\lambda, x, m)$:

- *Parse* $x = (x_1, \ldots, x_N)$.
- *Create PPRF keys* $k_0 \leftarrow \mathsf{PPRF.KeyGen}(1^\lambda)$ *and* $k_1 \leftarrow \mathsf{PPRF.KeyGen}(1^\lambda)$.
- *For* $i \in [t-1]$, *compute pseudorandom shares* $s_i \leftarrow \mathsf{PPRF}(k_0, i)$. *Compute the remaining shares* $(s_t, \ldots, s_N) \leftarrow \mathsf{LSS.RemainShare}(m, s_1, \ldots, s_{t-1})$.
- *Compute* $\mathsf{hk} \leftarrow \mathsf{SSB.Gen}(1^\lambda, t-1, j)$ *for* $j \leftarrow\!\!\$\, [t-1]$. *Moreover, compute* $h \leftarrow \mathsf{SSB.Hash}(\mathsf{hk}, \{x_1, \ldots, x_{t-1}\})$.
- *Consider the circuit* $\mathcal{C} = \mathcal{C}[\lambda, \mathsf{hk}, h, k_0, k_1, t, N]$. *Compute* $\bar{\mathcal{C}} \leftarrow \mathsf{iO}(1^\lambda, \mathcal{C})$.
- *For* $i \in \{t, \ldots, N\}$, *compute encryptions* $\mathsf{ct}_i \leftarrow \mathsf{WE.Enc}(1^\lambda, x_i, s_i)$.
- *Output* $\mathsf{ct} = (\{\mathsf{ct}_i\}_{i \in \{t,\ldots,N\}}, \bar{\mathcal{C}}, \mathsf{hk})$.

$\mathsf{Dec}(w, \mathsf{ct})$:

- *Parse* $w = (w_{i_1}, \ldots, w_{i_t})$ *and* ct *as* $(\{\mathsf{ct}_i\}_{i \in \{t,\ldots,N\}}, \bar{\mathcal{C}}, \mathsf{hk})$
- *For* $i \in [t-1]$, *compute* $\tau_i \leftarrow \mathsf{SSB.Open}(\mathsf{hk}, \{x_1, \ldots, x_{t-1}\}, i)$ *and run* $\mathsf{ct}_i \leftarrow \bar{\mathcal{C}}(i, \tau_i, x_i)$.
- *For* $j \in [t]$, *decrypt* $s_{i_j} \leftarrow \mathsf{WE.Dec}(w_{i_j}, \mathsf{ct}_{i_j})$.
- *Reconstruct* $m \leftarrow \mathsf{LSS.Reconstruct}(s_{i_1}, \ldots, s_{i_t})$. *Output* m.

Ciphertext size. The ciphertext is of the form $(\{\mathsf{ct}_i\}_{i \in \{t,\ldots,N\}}, \bar{\mathcal{C}}, \mathsf{hk})$. Assume that the language $\mathcal{L}$ has a verification circuit $\mathcal{C}_\mathcal{L}$.

The ciphertexts ct_i for $i \in \{t, \ldots, N\}$ have size $\mathcal{O}(|\mathcal{C}_\mathcal{L}| \cdot \mathsf{poly}(\lambda))$. Since $N - t \in \mathcal{O}(\log(N))$, then the size of $\{\mathsf{ct}_i\}_{i \in \{t,\ldots,N\}}$ is $\mathcal{O}(\log(N) \cdot |\mathcal{C}_\mathcal{L}| \cdot \mathsf{poly}(\lambda))$.

The obfuscated circuit $\mathcal{C}$ implements the $\mathsf{SSB.Verify}$ algorithm which is of size $\mathcal{O}(\log(N))$. Moreover, all other operations in $\mathcal{C}$ are independent of N and depend only on $|\mathcal{C}_\mathcal{L}|$. Hence, $|\mathcal{C}| \in \mathcal{O}(\log(N) \cdot |\mathcal{C}_\mathcal{L}| \cdot \mathsf{poly}(\lambda))$.

Finally, the hashing key hk is of size $\mathcal{O}(\log(N))$ by the efficiency requirements of SSB.

We conclude that the scheme presented above outputs ciphertexts of size $\mathcal{O}(\log(N) \cdot |\mathcal{C}_\mathcal{L}| \cdot \mathsf{poly}(\lambda))$.

7.2 Proofs

We now prove that the scheme is correct and soundness secure.

Theorem 11 (Correctness)**.** *The scheme presented in Construction 3 is correct, given that* LSS, SSB *and* WE *are correct.*

Proof. Assume that $x = (x_1, \ldots, x_N) \in \mathcal{L}$. That is, there exists indices $i_1, \ldots, i_t$ such that $x_{i_j} \in \mathcal{L}_{i_j}$. Let $w_{i_1}, \ldots, w_{i_t}$ be the corresponding witnesses.

First, note that for all $i \in [t]$ and by the correctness of the SSB hashing scheme, the circuit $\mathcal{C}[\lambda, \mathsf{hk}, h, k_0, k_1, t, N](i, \tau_i, x_i)$ always outputs $\mathsf{ct}_i \leftarrow \mathsf{WE.Enc}(1^\lambda, x_i, s_i)$ since $1 \leftarrow \mathsf{SSB.Verify}(\mathsf{hk}, h, i, x_i, \tau_i)$ for $\mathsf{hk} \leftarrow \mathsf{SSB.Gen}(1^\lambda, t-1, j)$ (for $j \leftarrow\!\!\$\, [t-1]$), $h \leftarrow \mathsf{SSB.Hash}(\mathsf{hk}, \{x_1, \ldots, x_{t-1}\}$ and $\tau_i \leftarrow \mathsf{SSB.Open}(\mathsf{hk}, \{x_1, \ldots, x_{t-1}\}, i)$.

Moreover, $s_{i_j} \leftarrow \mathsf{WE.Dec}(w_{i_j}, \mathsf{ct}_{i_j})$ holds by the correctness of the WE scheme, giving us access to t of N shares. Finally, the correctness of the LSS scheme implies that we succesfully extract $m \leftarrow \mathsf{LSS.Reconstruct}(s_{i_1}, \ldots s_{i_t})$. □

Theorem 12 (Soundness security)**.** *The scheme presented in Construction 3 is soundness secure given that* SSB *is index hiding and somewhere statistically binding,* iO *is a secure $i\mathcal{O}$ obfuscator,* PPRF *is pseudorandom at punctured points,* WE *is soundness secure and* LSS *is private.*

Before presenting the formal proof, we give a brief outline of it. The proof follows a sequence of hybrids, where the last one can be reduced to the privacy of the LSS. First, note that if $x \notin \mathcal{L}'$, then there do not exist t instances $x_i \in \mathcal{L}$. Assume, for simplicity that $t = N$, then there exists an index i^* such that $x_{i^*} \notin \mathcal{L}$. We start with a hybrid that is identical to the real soundness security game.

Then, we use the index hiding of the SSB hashing scheme to replace hk by a hashing key that is binding to index i^*. We then use the *puncturing* technique of [SW14]. That is, we create punctured PRF keys k_0' and k_1' (by puncturing the PPRF keys k_0 and k_1 respectively) at the point i^*. At the same time, we embed into the obfuscated circuit the ciphertext $\mathsf{ct}_{i^*} \leftarrow \mathsf{WE.Enc}(1^\lambda, x_{i^*}, s_{i^*}; r_{i^*})$ where $s_{i^*} \leftarrow \mathsf{PPRF.Eval}(k_0, i^*)$ and $r_{i^*} \leftarrow \mathsf{PPRF.Eval}(k_1, i^*)$. Given that the SSB is somewhere statistically binding at the point i^*, the circuits are functionally equivalent and we can use the security of the $i\mathcal{O}$ obfuscator to argue indistinguishability. We can now replace the values s_{i^*}, r_{i^*} by uniform ones since the PPRF is pseudorandom at punctured points. Finally, we replace ct_{i^*} by an encryption of 0. To conclude the proof, we can easily build a reduction to the security of the LSS.

In the more general case, some WE encryptions with respect to false statements are computed using the obfuscated program and some of them are given in the plain. For the former ones, we simply repeat the process above. For the latter ones, we use the security of the WE to replace these encryptions by encryptions of 0.

Proof. Assume that $x \notin \mathcal{L}'$. That is, there exists $x_{i_j} \notin \mathcal{L}$ for $j \in [N - t + 1]$ (where $N - t + 1 \in \log(N)$). Let $\delta \in [N]$ be such that $i_1, \ldots, i_\delta \leq t - 1 < i_{\delta+1}, \ldots, i_{N-t+1}$. The proof of the theorem follows from the following sequence

of hybrids:

$$\begin{aligned}\mathcal{H}_0 &\approx \mathcal{H}_{1,1} \approx \cdots \approx \mathcal{H}_{1,5}\\ &\approx \mathcal{H}_{2,1} \approx \cdots \approx \mathcal{H}_{2,5}\\ &\vdots\\ &\approx \mathcal{H}_{\delta,1} \approx \cdots \approx \mathcal{H}_{\delta,5}\\ &\approx \mathcal{H}_{\delta+1,1} \approx \cdots \approx \mathcal{H}_{\delta+1,N-t+1-\delta}\end{aligned}$$

where $\approx$ denotes that the games are computationally indistinguishable. The first hybrid $\mathcal{H}_0$ denotes the real soundness security experiment of Definition 21. The last hybrid can be reduced to the privacy of the underlying LSS.

Hybrid $\mathcal{H}_0$. This is the real soundness security game as defined in Definition 21.

Hybrid $\mathcal{H}_{j,1}$. This hybrid is identical to the previous one, if j=1, and identical to $\mathcal{H}_{j-1,5}$ otherwise, except that the challenger sets $\mathsf{hk} \leftarrow \mathsf{SSB.Gen}(1^\lambda, t-1, i_j)$ if $i_j \leq t-1$. This hybrid is defined for $j = 1, \ldots, \delta$.

Claim 18. *Assume that* SSB *is index hiding. Then hybrids $\mathcal{H}_{j-1,0}$ and $\mathcal{H}_{j,1}$ are indistinguishable, for $j \in \{1, \ldots, \delta\}$ where $\mathcal{H}_{0,0} = \mathcal{H}_0$ and $\mathcal{H}_{j-1,0} = \mathcal{H}_{j-1,5}$ (defined below).*

The proof of the claim is similar to the proof of Claim 1.

Hybrid $\mathcal{H}_{j,2}$. This hybrid is identical to the previous one except that, if $i_j \leq t-1$, the challenger computes the keys $k'_0 \leftarrow \mathsf{PPRF.KeyGen}(1^\lambda)$ and $k'_1 \leftarrow \mathsf{PPRF.KeyGen}(1^\lambda)$, the punctured keys $k_{i_j} \leftarrow \mathsf{PPRF.Puncture}(k'_0, S)$ and $k'_{i_j} \leftarrow \mathsf{PPRF.Puncture}(k'_1, S)$ where $S = \{i_1, \ldots, i_j\}$, and sets $k_0 = k_{i_j}$ and $k_1 = k'_{i_j}$. Moreover, it computes $\mathsf{ct}_{i_j} \leftarrow \mathsf{WE.Enc}(1^\lambda, x_{i_j}, s_{i_j}; r_{i_j})$ where $s_{i_j} \leftarrow \mathsf{PPRF.Eval}(k'_0, i_j)$ and $r_{i_j} \leftarrow \mathsf{PPRF.Eval}(k'_1, i_j)$.

Additionally, the challenger modifies

$$\mathcal{C} = \mathcal{C}[\lambda, \mathsf{hk}, h, k_0, k_1, t, N, \mathsf{ct}_{i_1}, \ldots, \mathsf{ct}_{i_{j-1}}]$$

to a circuit

$$\mathcal{D} = \mathcal{D}[\lambda, \mathsf{hk}, h, k_0, k_1, t, N, \mathsf{ct}_{i_1}, \ldots, \mathsf{ct}_{i_{j-1}}, \mathsf{ct}_{i_j}]$$

that behaves exactly as $\mathcal{C}$ except on input (i, τ_i, x_i) with $i = i_j$. In this case, the circuit $\mathcal{D}$ first checks if $1 \leftarrow \mathsf{SSB.Verify}(\mathsf{hk}, h, i, x_i, \tau_i)$ and, if so, it outputs ct_{i_j} that is hardwired.

This hybrid is defined for $j = 1, \ldots, \delta$.

Claim 19. *Assume that* iO *is a secure $i\mathcal{O}$ obfuscator for all circuits and* SSB *is somewhere statistically binding. Then hybrids $\mathcal{H}_{j,1}$ and $\mathcal{H}_{j,2}$ are indistinguishable for $j = \{1, \ldots, \delta\}$.*

Proof. Given an adversary $\mathcal{A}'$ that is able to distinguish both hybrids, we can build a reduction $\mathcal{R}$ that breaks the security of the underlying iO scheme.

To see this, first observe that the circuits $\mathcal{C}$ and $\mathcal{D}$ are functionally equivalent. That is, for every input (i, τ_i, x_i), we claim that

$$\mathcal{C}(i, \tau_i, x_i) = \mathcal{D}(i, \tau_i, x_i).$$

This fact can be established by noting that the only possible inputs where $\mathcal{C}$ and $\mathcal{D}$ could differ are of the form $(i_j, \cdot, \cdot)$. However, by the statistically binding property of SSB (which is binding at position i_j) we have that there exists only one possible form of inputs $(i_j, \cdot, \cdot)$ that output something different then $\bot$, which - for both circuits - is $(i_j, \tau_{i_j}, x_{i_j})$ for a verifying proof τ_{i_j}.

For this type of input $\mathcal{D}$ outputs the hardwired ciphertext $\mathsf{ct}_{i_j} \leftarrow \mathsf{WE.Enc}(1^\lambda, x_{i_j}, s_{i_j}; r_{i_j})$, where $s_{i_j} \leftarrow \mathsf{PPRF.Eval}(k'_0, i_j)$ and $r_{i_j} \leftarrow \mathsf{PPRF.Eval}(k'_1, i_j)$. This coincides with the output of $\mathcal{C}$ by definition.

We now describe the reduction $\mathcal{R}$ against security of iO. The reduction $\mathcal{R}$ chooses

$$\mathcal{C} = \mathcal{C}[\lambda, \mathsf{hk}, h, k_0, k_1, t, N, \mathsf{ct}_{i_1}, \ldots, \mathsf{ct}_{i_{j-1}}]$$

and

$$\mathcal{D} = \mathcal{D}[\lambda, \mathsf{hk}, h, k_0, k_1, t, N, \mathsf{ct}_{i_1}, \ldots, \mathsf{ct}_{i_{j-1}}, \mathsf{ct}_{i_j}]$$

as challenge circuits. Upon receiving the obfuscated circuit $\bar{\mathcal{C}}$ from the challenger, $\mathcal{R}$ simply outputs the ciphertext $\mathsf{ct} = (\{\mathsf{ct}_i\}_{i \in \{t, \ldots, N\}}, \bar{\mathcal{C}}, \mathsf{hk})$ (where all other values are computed as in hybrid $\mathcal{H}_{j,1}$).

Remark that, if $\bar{\mathcal{C}} \leftarrow \mathsf{iO}(1^\lambda, \mathcal{C})$, then the game is identical to $\mathcal{H}_{j,1}$. Else if $\bar{\mathcal{C}} \leftarrow \mathsf{iO}(1^\lambda, \mathcal{D})$ the game is identical to $\mathcal{H}_{j,2}$. The reduction outputs the same as $\mathcal{A}$ and has the same advantage. □

Hybrid $\mathcal{H}_{j,3}$. This hybrid is identical to the previous one except that, if $i_j \leq t - 1$, the challenger samples $r_{i_j} \leftarrow\!\!\$\, \{0,1\}^\lambda$.[17] This hybrid is defined for $j = 1, \ldots, \delta$.

Claim 20. *Assume that* PPRF *is pseudorandom at punctured points. Then hybrids* $\mathcal{H}_{j,2}$ *and* $\mathcal{H}_{j,3}$ *are indistinguishable.*

Proof. Let $\mathcal{A}'$ be an adversary that distinguishes both hybrids. We build a reduction $\mathcal{R}$ that breaks the pseudorandomness at punctured points of the underlying PPRF.

The reduction works as follows: It sends $S = \{i_1, \ldots, i_j\}$ to the PPRF challenger. Upon receiving k_S and the challenge $T = \{y_1, \ldots, y_j\}$, the reduction behaves exactly as in hybrid $\mathcal{H}_{j,2}$ except that it sets $k_1 = k_S$ and $r_{i_j} = y_j$. Observe that, if $y_j \leftarrow \mathsf{PPRF.Eval}(k, i_j)$ then the simulated game is identical to $\mathcal{H}_{j,2}$. Else if y is uniformly chosen, then the simulated game is identical to

[17] Note that we are puncturing the PPRF on at most $N - t + 1 \in \mathcal{O}(\log N)$ points. So the size of the punctured key is $\mathcal{O}(\log N \cdot \mathsf{poly}(\lambda))$. This means that the size of the ciphertext of our WE scheme does not exceed $\mathcal{O}(\log N \cdot \mathsf{poly}(\lambda))$.

$\mathcal{H}_{j,3}$. We output whatever $\mathcal{A}$ outputs and conclude that $\mathcal{R}$ breaks the pseudorandomness at punctured points with exactly the same advantage that $\mathcal{A}$ has in distinguishing the hybrids. □

Hybrid $\mathcal{H}_{j,4}$. This hybrid is identical to the previous one except that, if $i_j \leq t-1$, the challenger samples $s_{i_j} \leftarrow\!\$\, \{0,1\}^\lambda$. This hybrid is defined for $j = 1, \ldots, \delta$.

Claim 21. *Assume that* PPRF *is pseudorandom at punctured points. Then hybrids $\mathcal{H}_{j,3}$ and $\mathcal{H}_{j,4}$ are indistinguishable.*

The claim follows by a similar argument as the one of Claim 20

Hybrid $\mathcal{H}_{j,5}$. This hybrid is identical to the previous one except that, if $i_j \leq t-1$, the challenger computes ct_{i_j} as $\mathsf{ct}_{i_j} \leftarrow \mathsf{WE.Enc}(1^\lambda, x_{i_j}, 0)$. This hybrid is defined for $j = 1, \ldots, \delta$.

Claim 22. *Assume that* WE *is soundness secure and $x_{i_j} \notin \mathcal{L}$. Then hybrids $\mathcal{H}_{j,4}$ and $\mathcal{H}_{j,5}$ are indistinguishable.*

Proof. Let $\mathcal{A}$ be an adversary that is able to distinguish both hybrids. We build a reduction $\mathcal{R}$ that breaks the soundness security of the underlying WE scheme.

The reduction simply sends the challenge messages $m_0 = s_{i_j}$ and $m_1 = 0$. Upon receiving ct from the challenge, $\mathcal{R}$ behaves exactly as in hybrid $\mathcal{H}_{j,4}$ except that it sets $\mathsf{ct}_{i_j} = \mathsf{ct}$. Note that if $\mathsf{ct} \leftarrow \mathsf{WE.Enc}(1^\lambda, x_{i_j}, s_{i_j})$ then the game is identical to $\mathcal{H}_{j,4}$, whereas if $\mathsf{ct} \leftarrow \mathsf{WE.Enc}(1^\lambda, x_{i_j}, 0)$ then the game is identical to $\mathcal{H}_{j,5}$. We output whatever $\mathcal{A}$ outputs and conclude that $\mathcal{R}$ breaks the soundness security with exactly the same advantage that $\mathcal{A}$ has in distinguishing the hybrids. □

Hybrid $\mathcal{H}_{\delta+1,j}$. This hybrid is identical to $\mathcal{H}_{\delta,5}$ for $j = 1$ and identical to $\mathcal{H}_{\delta+1,j-1}$ otherwise, except that, if $t-1 < i_{\delta+j} \leq N$, the challenger computes $\mathsf{ct}_{i_{j+\delta}}$ as $\mathsf{ct}_{i_{j+\delta}} \leftarrow \mathsf{WE.Enc}(1^\lambda, x_{i_{j+\delta}}, 0)$. This hybrid is defined for $j = 1, \ldots, N - t + 1 - \delta$.

Claim 23. *Assume that* WE *is soundness secure. Then hybrids $\mathcal{H}_{\delta+1,j-1}$ and $\mathcal{H}_{\delta+1,j}$ are indistinguishable, for $j = 1, \ldots, N - t + 1 - \delta$ where $\mathcal{H}_{\delta+1,0} = \mathcal{H}_{\delta,5}$.*

The claim follows by a similar argument as the one of Claim 22.

We finally show that the advantage of the adversary is negligible given that the LSS is private.

Claim 24. *Assume that* LSS *is private. Then the advantage of $\mathcal{A}$ in hybrid $\mathcal{H}_{\delta+1,N-t+1-\delta}$ is negligible.*

Proof. Let $\mathcal{A}$ be an adversary that breaks the soundness security of our scheme in hybrid $\mathcal{H}_{\delta+1,N-t+1-\delta}$. We show that there is a reduction $\mathcal{R}$ that uses $\mathcal{A}$ and breaks the privacy of LSS. $\mathcal{A}$ starts by sending (m_0, m_1), which $\mathcal{R}$ redirects to the LSS challenger. $\mathcal{R}$ receives $(\bar{s}_{i_1^*}, \ldots, \bar{s}_{i_{t-1}^*})$. It sets $s_{i_j^*} = \bar{s}_{i_j^*}$ for all

$i_j^* \in [N] \setminus \{i_1, \ldots, i_{N-t+1}\}$. Then, it behaves exactly as in hybrid $\mathcal{H}_{\delta+1,N-t+1-\delta}$. Upon receiving a bit b'' from $\mathcal{A}$, $\mathcal{R}$ outputs b''.

Note that the game is identical to the game in $\mathcal{H}_{\delta+1,N-t+1-\delta}$ with challenge bit $b' = b$ where b is the bit of the LSS game. Hence, $\mathcal{R}$ has the same advantage as $\mathcal{A}$. □

This concludes the proof of the theorem. □

7.3 Construction from Indistinguishability Obfuscation with Polynomial Security Loss

Let $\mathcal{C} : \{0,1\}^\zeta \to \{0,1\}^\nu$ be a circuit. It is well-known that current constructions of $i\mathcal{O}$ incur a security loss of 2^ζ. Hence, when we obfuscate circuits with a domain of exponential size (in the security parameter) then the resulting obfuscation incurs an exponential security loss (e.g., [AJ15, BV15, BGL+15]). We note that this fact may be an artifact of known $i\mathcal{O}$ constructions and that our construction from the previous section enjoys a polynomial security reduction to an $i\mathcal{O}$ scheme.

Nevertheless, with the goal of avoiding the exponential security loss caused by known $i\mathcal{O}$ constructions, we build a scheme using $i\mathcal{O}$ for a TM with only a polynomially-size domain. We therefore incur only a polynomial security loss.

Let $\mathfrak{M}$ be a family of TMs and $\mathsf{siO}(1^\lambda, \mathcal{M})$ be a PPT algorithm that takes as input a security parameter and a TM $\mathcal{M}$, and outputs an obfuscated TM $\bar{\mathcal{M}}$. The algorithm siO is called a *succinct $i\mathcal{O}$ obfuscator* for a family of TMs $\mathfrak{M}$ if it is correct, secure and succinct. Correctness and security are defined in a similar fashion as in definitions 22 and 23.

Definition 35 (Succinctness)**.** *Let $\mathcal{M}$ be a TM that runs in time t. We say that a succinct $i\mathcal{O}$ obfuscator siO is succinct if the running time of $\mathsf{siO}(1^\lambda, \mathcal{M})$ (and the size of its output, that is, the size of the obfuscated TM) is bounded by $\mathsf{poly}(\lambda, |\mathcal{M}|, \log t)$.*

We additionally require that both TM $\mathcal{M}$ and $\bar{\mathcal{M}}$ have access to a public read-only tape tp_p. That is, tp_p is not part of the description of $\mathcal{M}$ nor of $\bar{\mathcal{M}}$ but both TMs can make read operations of the tape. We write $\mathcal{M}^{\mathsf{tp}_p}$ to denote a TM with access to tp_p and we write $x_i \leftarrow \mathsf{Retrieve}(\mathsf{tp}_p, i)$ to denote the operation that $\mathcal{M}$ performs to retrieve the i-th block of tp_p. Note that the scheme of [GS18] allows for such TMs, which access the public tape tp_p via a laconic oblivious transfer (LOT) [CDG+17]. The hash value for the LOT scheme is hardwired on $\mathcal{M}$. Moreover, the resulting obfuscated TM has size logarithmic in the size of the public tape tp_p.

For TMs of polynomially-sized domains, the transformation of [BGL+15] incurs only a polynomial security loss starting from the scheme of [GS18].

Lemma 1 ([BGL+15, GS18])**.** *The scheme of [GS18], when applied to a TM with domain of polynomial size incurs only a polynomial security loss in the security reduction.*

Remark 1. *We remark that WE can be built from $i\mathcal{O}$ in a straightforward way [GGH+13]. Hence, if $i\mathcal{O}$ for TM with polynomially-size domains can be built while incurring only in a polynomial security loss in the security reduction, then the same holds for WE if the input size on the encryption algorithm is only of polynomial size. We will use this fact in the construction below.*

Construction 4. *Let $N \in \mathsf{poly}(\lambda)$ and t be such that $N - t \in \mathcal{O}(\log N)$ and $\mathcal{L}$ be a* NP *language. Let*

- $\mathsf{LSS} =$ *be a (t, N)-LSS scheme. In the following, we assume that shares can be written as strings in $\{0,1\}^\lambda$.*
- WE *be a (non-compact) WE scheme for language $\mathcal{L}$.*
- siO *be a succinct obfuscator for all TMs that can read from a public tape tp_p via a* Retrieve *algorithm (this can be done via a LOT scheme as described above).*
- PPRF *be a puncturable PRF.*

Additionally, consider the following TM $\mathcal{M}^{\mathsf{tp}_p}[\lambda, k_0, k_1, t, N]$ which has the values λ, k_0, k_1, t and N hardwired and accesses a public tape tp_p.

$\mathcal{M}^{\mathsf{tp}_p}[\lambda, k_0, k_1, t, N](i \in [N])$:

- *If $i \geq t$, abort the computation.*
- *Retrieve $x_i \leftarrow \mathsf{Retrieve}(\mathsf{tp}_p, i)$.*
- *Compute $s_i \leftarrow \mathsf{PPRF.Eval}(k_0, i)$ and random coins $r_i \leftarrow \mathsf{PPRF.Eval}(k_1, i)$.*
- *Compute $\mathsf{ct}_i \leftarrow \mathsf{WE.Enc}(1^\lambda, x_i, s_i; r_i)$. Output ct_i.*

We now define the WE scheme for the (t, N)-conjunction language $\mathcal{L}'$.

$\mathsf{Enc}(1^\lambda, x, m)$:

- *Parse $x = (x_1, \ldots, x_N)$.*
- *Create PPRF keys $k_0 \leftarrow \mathsf{PPRF.KeyGen}(1^\lambda)$ and $k_1 \leftarrow \mathsf{PPRF.KeyGen}(1^\lambda)$.*
- *For $i \in [t-1]$, compute pseudorandom shares $s_i \leftarrow \mathsf{PPRF}(k, i)$. Compute the remaining shares $(s_t, \ldots, s_N) \leftarrow \mathsf{LSS.RemainShare}(m, s_1, \ldots, s_{t-1})$.*
- *Consider the TM $\mathcal{M}^{\mathsf{tp}_p} = \mathcal{M}^{\mathsf{tp}_p}[\lambda, k_0, k_1, t, N]$ with the tape tp_p initialized to $(x_1, \ldots, x_{t-1})$. Compute $\bar{\mathcal{M}}^{\mathsf{tp}_p} \leftarrow \mathsf{siO}(1^\lambda, \mathcal{M}^{\mathsf{tp}_p})$.*
- *For $i \in \{t, \ldots, N\}$, compute encryptions $\mathsf{ct}_i \leftarrow \mathsf{WE.Enc}(1^\lambda, x_i, s_i)$.*
- *Output $\mathsf{ct} = (\{\mathsf{ct}_i\}_{i \in \{t, \ldots, N\}}, \bar{\mathcal{M}}^{\mathsf{tp}_p})$.*

$\mathsf{Dec}(w, \mathsf{ct})$:

- *Parse* $w = (w_{i_1}, \ldots, w_{i_t})$ *and* ct *as* $(\{\mathsf{ct}_i\}_{i\in\{t,\ldots,N\}}, \bar{\mathcal{M}}^{\mathsf{tp}_p})$. *Initialize the tape* $\mathsf{tp}_p = (x_1, \ldots, x_{t-1})$.
- *For* $i \in [t-1]$, *run* $\mathsf{ct}_i \leftarrow \bar{\mathcal{M}}^{\mathsf{tp}_p}(i)$.
- *For* $j \in [t]$, *decrypt* $s_{i_j} \leftarrow \mathsf{WE.Dec}(w_{i_j}, \mathsf{ct}_{i_j})$.
- *Reconstruct* $m \leftarrow \mathsf{LSS.Reconstruct}(s_{i_1}, \ldots, s_{i_t})$. *Output* m.

Ciphertext size. The ciphertext is of the form $\mathsf{ct} = (\{\mathsf{ct}_i\}_{i\in\{t,\ldots,N\}}, \bar{\mathcal{M}}^{\mathsf{tp}_p})$. Assume that the language $\mathcal{L}$ has a verification circuit $\mathcal{C}_{\mathcal{L}}$.

The ciphertexts ct_i for $i \in \{t, \ldots, N\}$ have size $\mathcal{O}(|\mathcal{C}_{\mathcal{L}}| \cdot \mathsf{poly}(\lambda))$. Since $N - t \in \mathcal{O}(\log N)$, the size of $\{\mathsf{ct}_i\}_{i\in\{t,\ldots,N\}}$ is $\mathcal{O}(\log(N) \cdot |\mathcal{C}_{\mathcal{L}}| \cdot \mathsf{poly}(\lambda))$.

Moreover, the obfuscated TM $\bar{\mathcal{M}}^{\mathsf{tp}_p}$ is of size $\mathcal{O}(\log(N) \cdot |\mathcal{C}_{\mathcal{L}}| \cdot \mathsf{poly}(\lambda))$ since the tape tp_p is of size $\mathcal{O}(N)$.

Therefore, the total size of the ciphertext is $\mathcal{O}(\log(N) \cdot |\mathcal{C}_{\mathcal{L}}| \cdot \mathsf{poly}(\lambda))$.

7.4 Proofs

We now prove that the scheme is correct and soundness secure.

Theorem 13 (Correctness)**.** *The scheme presented in Construction 4 is correct, given that* LSS *and* WE *are correct.*

The proof is similar to the proof of Theorem 11.

Theorem 14 (Soundness security)**.** *The scheme presented in Construction 4 is soundness secure given that* siO *is a secure succinct iO obfuscator,* PPRF *is pseudorandom at punctured points,* WE *is soundness secure and* LSS *is private.*

The proof of the Theorem follows the same outline as the proof of Theorem 12.

Proof. As in the proof of Theorem 12, assume that $x \notin \mathcal{L}'$. That is, there exists $x_{i_j} \notin \mathcal{L}$ for $j \in [N-t+1]$ (where $N-t+1 \in \log(N)$). Let $\delta \in [N]$ be such that $i_1, \ldots, i_\delta \leq t-1$. The proof of the theorem follows from the following sequence of hybrids:

$$\begin{aligned}
\mathcal{H}_0 &\approx \mathcal{H}_{1,1} \approx \cdots \approx \mathcal{H}_{1,4} \\
&\approx \mathcal{H}_{2,1} \approx \cdots \approx \mathcal{H}_{2,4} \\
&\vdots \\
&\approx \mathcal{H}_{\delta,1} \approx \cdots \approx \mathcal{H}_{\delta,4} \\
&\approx \mathcal{H}_{\delta+1,1} \approx \cdots \approx \mathcal{H}_{\delta+1,N-t+1-\delta}
\end{aligned}$$

where $\approx$ denotes that the games are computationally indistinguishable. The first hybrid $\mathcal{H}_0$ denotes the real soundness security experiment of Definition 21. The last hybrid can be reduced to the privacy of the underlying LSS.

Hybrid $\mathcal{H}_0$. This is the real soundness security game as defined in Definition 21.

Hybrid $\mathcal{H}_{j,1}$. This hybrid is identical to the previous one[18] except that, if $i_j \leq t-1$, the challenger computes the keys $k'_0 \leftarrow \mathsf{PPRF.KeyGen}(1^\lambda)$ and $k'_1 \leftarrow \mathsf{PPRF.KeyGen}(1^\lambda)$, the punctured keys $k_{i_j} \leftarrow \mathsf{PPRF.Puncture}(k'_0, S)$ and $k'_{i_j} \leftarrow \mathsf{PPRF.Puncture}(k'_1, S)$ where $S = \{i_1, \ldots, i_j\}$, and sets $k_0 = k_{i_j}$ and $k_1 = k'_{i_j}$. Moreover, it computes $\mathsf{ct}_{i_j} \leftarrow \mathsf{WE.Enc}(1^\lambda, x_{i_j}, s_{i_j}; r_{i_j})$ where $s_{i_j} \leftarrow \mathsf{PPRF.Eval}(k'_0, i_j)$ and $r_{i_j} \leftarrow \mathsf{PPRF.Eval}(k'_1, i_j)$.

Additionally, the challenger modifies $\mathcal{M}^{\mathsf{tp}_p} = \mathcal{M}^{\mathsf{tp}_p}[\lambda, k_0, k_1, t, N, \mathsf{ct}_{i_1}, \ldots, \mathsf{ct}_{i_{j-1}}](i)$ to a TM $\mathcal{D}^{\mathsf{tp}_p} = \mathcal{D}^{\mathsf{tp}_p}[\lambda, k_0, k_1, t, N, \mathsf{ct}_{i_1}, \ldots, \mathsf{ct}_{i_{j-1}}, \mathsf{ct}_{i_j}]$ that behaves exactly as $\mathcal{M}^{\mathsf{tp}_p}$ except when $i = i_j$. In this case, the TM $\mathcal{D}$ outputs ct_{i_j} that is hardwired.

This hybrid is defined for $j = 1, \ldots, \delta$.

Claim 25. *Assume that* siO *is a secure succinct iO obfuscator for all TM (with access to a public tape* tp_p*). Then hybrids* $\mathcal{H}_{j,0}$ *and* $\mathcal{H}_{j,1}$ *are indistinguishable for* $j = \{1, \ldots, \delta\}$ *where* $\mathcal{H}_{0,0} = \mathcal{H}_0$ *and* $\mathcal{H}_{j-1,0} = \mathcal{H}_{j-1,4}$ *(defined below).*

The proof of the claim is identical to the proof of Claim 19.

Hybrid $\mathcal{H}_{j,2}$. This hybrid is identical to the previous one except that, if $i_j \leq t-1$, the challenger samples $r_{i_j} \leftarrow\!\!\$\, \{0,1\}^\lambda$.[19] This hybrid is defined for $j = \{1, \ldots, \delta\}$.

Claim 26. *Assume that* PPRF *is pseudorandom at punctured points. Then hybrids* $\mathcal{H}_{j,1}$ *and* $\mathcal{H}_{j,2}$ *are indistinguishable.*

The proof of the claim is identical to the proof of Claim 20.

Hybrid $\mathcal{H}_{j,3}$. This hybrid is identical to the previous one except that, if $i_j \leq t-1$, the challenger samples $s_{i_j} \leftarrow\!\!\$\, \{0,1\}^\lambda$. This hybrid is defined for $j = \{1, \ldots, \delta\}$.

Claim 27. *Assume that* PPRF *is pseudorandom at punctured points. Then hybrids* $\mathcal{H}_{j,2}$ *and* $\mathcal{H}_{j,3}$ *are indistinguishable.*

The claim follows by a similar argument as in the proof of Claim 20

Hybrid $\mathcal{H}_{j,4}$. This hybrid is identical to the previous one except that, if $i_j \leq t-1$, the challenger computes ct_{i_j} as $\mathsf{ct}_{i_j} \leftarrow \mathsf{WE.Enc}(1^\lambda, x_{i_j}, 0)$. This hybrid is defined for $j = \{1, \ldots, \delta\}$.

Claim 28. *Assume that* WE *is soundness secure and* $x_{i_j} \notin \mathcal{L}$*. Then hybrids* $\mathcal{H}_{j,3}$ *and* $\mathcal{H}_{j,4}$ *are indistinguishable.*

[18] The previous hybrid is $\mathcal{H}_0$ for $\mathcal{H}_{1,1}$ and $\mathcal{H}_{j-1,4}$ otherwise.

[19] Note that we are puncturing the PPRF on at most $N - t + 1 \in \mathcal{O}(\log N)$ points. So the size of the punctured key is $\mathcal{O}(\log N \mathsf{poly}(\lambda))$. This means that the size of the ciphertext of our WE scheme does not exceed $\mathcal{O}(\log N \mathsf{poly}(\lambda))$.

The claim follows by a similar argument as the one of Claim 22.

Hybrid $\mathcal{H}_{\delta+1,j}$. This hybrid is identical to $\mathcal{H}_{\delta,4}$ for $j = 0$ and identical to $\mathcal{H}_{\delta+1,j-1}$ otherwise, except that, if $t - 1 < i_{\delta+j} \leq N$, the challenger computes $\mathsf{ct}_{i_{j+\delta}}$ as $\mathsf{ct}_{i_{j+\delta}} \leftarrow \mathsf{WE.Enc}(1^\lambda, x_{i_{j+\delta}}, 0)$. This hybrid is defined for $j = \{1, \ldots, N - t + 1 - \delta\}$.

Claim 29. *Assume that* WE *is soundness secure. Then hybrids* $\mathcal{H}_{\delta+1,j-1}$ *and* $\mathcal{H}_{\delta+1,j}$ *are indistinguishable, for* $j = \{1, \ldots, N-t+1-\delta\}$ *where* $\mathcal{H}_{\delta+1,0} = \mathcal{H}_{\delta,4}$.

The claim follows by a similar argument as the one of Claim 22.

We finally show that the advantage of the adversary is negligible given that the LSS is private.

Claim 30. *Assume that* LSS *is private. Then the advantage of* $\mathcal{A}$ *in hybrid* $\mathcal{H}_{\delta+1,N-t+1-\delta}$ *is negligible.*

The proof of the claim follows a similar argument to the proof of Claim 24.

This concludes the proof of the theorem. □

7.5 Compact Universal Ring Signature from Compact WE for Threshold Conjunction Languages

Consider again the URS construction of Section 6. One of the requirements of this URS scheme is a (non-compact) WE for a language $\mathcal{L}'$ which is itself a $(N-1, N)$ -threshold conjunction language. When we plug the WE scheme for (t, N)-threshold conjunction languages as a drop in replacement for non-compact WE, we obtain a compact URS scheme.

Specifically, the following theorem is a direct consequence of plugging the compact WE scheme for (t, N)-threshold conjunction languages described above with the URS signature from Section 6.

Theorem 15. *Let*

- $\mathsf{PRG} : \{0,1\}^{\lambda/2} \to \{0,1\}^\lambda$ *be a PRG.*
- $\mathcal{L}'$ *be the* $(\ell-1, \ell)$ *threshold conjunction language defined in Construction 2.*
- WE *be a compact witness encryption scheme for the* $(\ell-1, \ell)$ *threshold conjunction language* $\mathcal{L}'$*. As we have just established, this primitive can be built from secure* $i\mathcal{O}$*,* $(\ell-1, \ell)$*-LSS, (non-compact) WE for* NP*, PPRF and SSB.*
- SPB *be a SPB hashing scheme;*
- $\mathcal{L}$ *and* $\mathcal{L}_{\mathsf{OR}}$ *be the languages defined in Construction 2.*
- NIWI *be a NIWI scheme for* $\mathcal{L}_{\mathsf{OR}}$.

Then there exists a URS scheme that satisfies correctness, anonymity and unforgeability. Moreover, a signature Σ with respect to a ring of users R and a ring of signature schemes S has size $|\Sigma| \in \mathcal{O}((\log \ell + \log M)\mathsf{poly}(\lambda))$ where $\ell = |R|$ and $M = |S|$.

Proof. The construction is the same as the one of Construction 2 where the standard WE scheme is replaced by our new compact WE scheme for $(\ell - 1, \ell)$ threshold conjunction languages of Construction 3.

The size of the signature in the Construction 2 is dominated by the size of the non-compact WE ciphertexts. By replacing it by the compact WE for threshold conjunction languages, it is easy to see that the resulting signature has size $\mathcal{O}((\log \ell + \log M)\mathsf{poly}(\lambda))$.

The properties of correctness, unforgeability and anonymity can be established using the same arguments as the ones of theorems 8, 9 and 10. □

Acknowledgments

Pedro Branco: Part of this work was done while at IST University of Lisbon.

Nico Döttling: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them. (ERC-2021-STG 101041207 LACONIC)

References

[AJ15] Prabhanjan Ananth and Abhishek Jain. Indistinguishability obfuscation from compact functional encryption. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 308–326, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[AOS02] Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. 1-out-of-n signatures from a variety of keys. In Yuliang Zheng, editor, *Advances in Cryptology – ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 415–432, Queenstown, New Zealand, December 1–5, 2002. Springer, Heidelberg, Germany.

[BDH+19] Michael Backes, Nico Döttling, Lucjan Hanzlik, Kamil Kluczniak, and Jonas Schneider. Ring signatures: Logarithmic-size, no setup - from standard assumptions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 281–311, Darmstadt, Germany, May 19–23, 2019. Springer, Heidelberg, Germany.

[BFM88] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications (extended abstract). In *20th Annual ACM Symposium on Theory of Computing*, pages 103–112, Chicago, IL, USA, May 2–4, 1988. ACM Press.

[BGI+12] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. *J. ACM*, 59(2), May 2012.

[BGI14] Elette Boyle, Shafi Goldwasser, and Ioana Ivan. Functional signatures and pseudorandom functions. In Hugo Krawczyk, editor, *PKC 2014: 17th International Conference on Theory and Practice of Public Key Cryptography*, volume 8383 of *Lecture Notes in Computer Science*, pages 501–519, Buenos Aires, Argentina, March 26–28, 2014. Springer, Heidelberg, Germany.

[BGL+15] Nir Bitansky, Sanjam Garg, Huijia Lin, Rafael Pass, and Sidharth Telang. Succinct randomized encodings and their applications. In Rocco A. Servedio and Ronitt Rubinfeld, editors, *47th Annual ACM Symposium on Theory of Computing*, pages 439–448, Portland, OR, USA, June 14–17, 2015. ACM Press.

[BGLS03] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432, Warsaw, Poland, May 4–8, 2003. Springer, Heidelberg, Germany.

[BKM06] Adam Bender, Jonathan Katz, and Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In Shai Halevi and Tal Rabin, editors, *TCC 2006: 3rd Theory of Cryptography Conference*, volume 3876 of *Lecture Notes in Computer Science*, pages 60–79, New York, NY, USA, March 4–7, 2006. Springer, Heidelberg, Germany.

[BKM20] Zvika Brakerski, Venkata Koppula, and Tamer Mour. NIZK from LPN and trapdoor hash via correlation intractability for approximable relations. In *CRYPTO (3)*, volume 12172 of *Lecture Notes in Computer Science*, pages 738–767. Springer, 2020.

[BOV03] Boaz Barak, Shien Jin Ong, and Salil P. Vadhan. Derandomization in cryptography. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 299–315, Santa Barbara, CA, USA, August 17–21, 2003. Springer, Heidelberg, Germany.

[Boy07] Xavier Boyen. Mesh signatures. In Moni Naor, editor, *Advances in Cryptology – EUROCRYPT 2007*, volume 4515 of *Lecture Notes in*

Computer Science, pages 210–227, Barcelona, Spain, May 20–24, 2007. Springer, Heidelberg, Germany.

[BP15] Nir Bitansky and Omer Paneth. ZAPs and non-interactive witness indistinguishability from indistinguishability obfuscation. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015: 12th Theory of Cryptography Conference, Part II*, volume 9015 of *Lecture Notes in Computer Science*, pages 401–427, Warsaw, Poland, March 23–25, 2015. Springer, Heidelberg, Germany.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93: 1st Conference on Computer and Communications Security*, pages 62–73, Fairfax, Virginia, USA, November 3–5, 1993. ACM Press.

[BV15] Nir Bitansky and Vinod Vaikuntanathan. Indistinguishability obfuscation from functional encryption. In Venkatesan Guruswami, editor, *56th Annual Symposium on Foundations of Computer Science*, pages 171–190, Berkeley, CA, USA, October 17–20, 2015. IEEE Computer Society Press.

[BW13] Dan Boneh and Brent Waters. Constrained pseudorandom functions and their applications. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology – ASIACRYPT 2013, Part II*, volume 8270 of *Lecture Notes in Computer Science*, pages 280–300, Bengalore, India, December 1–5, 2013. Springer, Heidelberg, Germany.

[CDG+17] Chongwon Cho, Nico Döttling, Sanjam Garg, Divya Gupta, Peihan Miao, and Antigoni Polychroniadou. Laconic oblivious transfer and its applications. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 33–65, Santa Barbara, CA, USA, August 20–24, 2017. Springer, Heidelberg, Germany.

[DKNS04] Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup. Anonymous identification in ad hoc groups. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 609–626, Interlaken, Switzerland, May 2–6, 2004. Springer, Heidelberg, Germany.

[FLS90] Uriel Feige, Dror Lapidot, and Adi Shamir. Multiple non-interactive zero knowledge proofs based on a single random string (extended abstract). In *31st Annual Symposium on Foundations*

of Computer Science, pages 308–317, St. Louis, MO, USA, October 22–24, 1990. IEEE Computer Society Press.

[FS10] Marc Fischlin and Dominique Schröder. On the impossibility of three-move blind signature schemes. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 197–215, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany.

[GG14] Sanjam Garg and Divya Gupta. Efficient round optimal blind signatures. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 477–495, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany.

[GGH+13] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th Annual Symposium on Foundations of Computer Science*, pages 40–49, Berkeley, CA, USA, October 26–29, 2013. IEEE Computer Society Press.

[GGHAK21] Aarushi Goel, Matthew Green, Mathias Hall-Andersen, and Gabriel Kaptchuk. Stacking sigmas: A framework to compose σ-protocols for disjunctions. Cryptology ePrint Archive, Report 2021/422, 2021. `https://ia.cr/2021/422`.

[GGM84] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions (extended abstract). In *25th Annual Symposium on Foundations of Computer Science*, pages 464–479, Singer Island, Florida, October 24–26, 1984. IEEE Computer Society Press.

[GGSW13] Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness encryption and its applications. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *45th Annual ACM Symposium on Theory of Computing*, pages 467–476, Palo Alto, CA, USA, June 1–4, 2013. ACM Press.

[GK03] Shafi Goldwasser and Yael Tauman Kalai. On the (in)security of the Fiat-Shamir paradigm. In *44th Annual Symposium on Foundations of Computer Science*, pages 102–115, Cambridge, MA, USA, October 11–14, 2003. IEEE Computer Society Press.

[GO94] Oded Goldreich and Yair Oren. Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1):1–32, December 1994.

[GOS06a] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for NIZK. In Cynthia Dwork, editor, *Advances in Cryptology – CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 97–111, Santa Barbara, CA, USA, August 20–24, 2006. Springer, Heidelberg, Germany.

[GOS06b] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero knowledge for NP. In Serge Vaudenay, editor, *Advances in Cryptology – EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 339–358, St. Petersburg, Russia, May 28 – June 1, 2006. Springer, Heidelberg, Germany.

[GRS+11] Sanjam Garg, Vanishree Rao, Amit Sahai, Dominique Schröder, and Dominique Unruh. Round optimal blind signatures. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 630–648, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Heidelberg, Germany.

[GS18] Sanjam Garg and Akshayaram Srinivasan. A simple construction of iO for turing machines. In Amos Beimel and Stefan Dziembowski, editors, *TCC 2018: 16th Theory of Cryptography Conference, Part II*, volume 11240 of *Lecture Notes in Computer Science*, pages 425–454, Panaji, India, November 11–14, 2018. Springer, Heidelberg, Germany.

[HKW15] Susan Hohenberger, Venkata Koppula, and Brent Waters. Universal signature aggregators. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part II*, volume 9057 of *Lecture Notes in Computer Science*, pages 3–34, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany.

[HW15] Pavel Hubacek and Daniel Wichs. On the communication complexity of secure function evaluation with long output. In Tim Roughgarden, editor, *ITCS 2015: 6th Conference on Innovations in Theoretical Computer Science*, pages 163–172, Rehovot, Israel, January 11–13, 2015. Association for Computing Machinery.

[JJ21] Abhishek Jain and Zhengzhong Jin. Non-interactive zero knowledge from sub-exponential DDH. In *EUROCRYPT (1)*, volume 12696 of *Lecture Notes in Computer Science*, pages 3–32. Springer, 2021.

[KPTZ13] Aggelos Kiayias, Stavros Papadopoulos, Nikos Triandopoulos, and Thomas Zacharias. Delegatable pseudorandom functions and applications. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *ACM CCS 2013: 20th Conference on Computer and Communications Security*, pages 669–684, Berlin, Germany, November 4–8, 2013. ACM Press.

[LPQ18] Benoît Libert, Thomas Peters, and Chen Qian. Logarithmic-size ring signatures with tight security from the DDH assumption. In Javier López, Jianying Zhou, and Miguel Soriano, editors, *ESORICS 2018: 23rd European Symposium on Research in Computer Security, Part II*, volume 11099 of *Lecture Notes in Computer Science*, pages 288–308, Barcelona, Spain, September 3–7, 2018. Springer, Heidelberg, Germany.

[OPWW15] Tatsuaki Okamoto, Krzysztof Pietrzak, Brent Waters, and Daniel Wichs. New realizations of somewhere statistically binding hashing and positional accumulators. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 121–145, Auckland, New Zealand, November 30 – December 3, 2015. Springer, Heidelberg, Germany.

[PS19a] Sunoo Park and Adam Sealfon. It wasn't me! - Repudiability and claimability of ring signatures. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part III*, volume 11694 of *Lecture Notes in Computer Science*, pages 159–190, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Heidelberg, Germany.

[PS19b] Chris Peikert and Sina Shiehian. Noninteractive zero knowledge for NP from (plain) learning with errors. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019, Part I*, volume 11692 of *Lecture Notes in Computer Science*, pages 89–114, Santa Barbara, CA, USA, August 18–22, 2019. Springer, Heidelberg, Germany.

[RST01] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565, Gold Coast, Australia, December 9–13, 2001. Springer, Heidelberg, Germany.

[SW07] Hovav Shacham and Brent Waters. Efficient ring signatures without random oracles. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *PKC 2007: 10th International Conference on Theory and Practice of Public Key Cryptography*, volume 4450 of *Lecture Notes in Computer Science*, pages 166–180, Beijing, China, April 16–20, 2007. Springer, Heidelberg, Germany.

[SW14] Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In David B. Shmoys, editor, *46th Annual ACM Symposium on Theory of Computing*, pages 475–484, New York, NY, USA, May 31 – June 3, 2014. ACM Press.

[Tso13] Raylin Tso. A new way to generate a ring: Universal ring signature. *Computers & Mathematics with Applications*, 65(9):1350–1359, 2013. Advanced Information Security.