Shorter Ring Signatures from Standard Assumptions

Alonso González[1]*

ENS de Lyon, Laboratoire LIP (U. Lyon, CNRS, ENSL, INRIA, UCBL), France.
alonso.gonzalez@ens-lyon.fr

Abstract. Ring signatures, introduced by Rivest, Shamir and Tauman (ASIACRYPT 2001), allow to sign a message on behalf of a set of users while guaranteeing authenticity and anonymity. Groth and Kohlweiss (EUROCRYPT 2015) and Libert et al. (EUROCRYPT 2016) constructed schemes with signatures of size logarithmic in the number of users. An even shorter ring signature, of size independent from the number of users, was recently proposed by Malavolta and Schröder (ASIACRYPT 2017). However, all these short signatures are obtained relying on strong and controversial assumptions. Namely, the former schemes are both proven secure in the random oracle model while the later requires non-falsifiable assumptions.

The most efficient construction under mild assumptions remains the construction of Chandran et al. (ICALP 2007) with a signature of size $\Theta(\sqrt{n})$, where n is the number of users, and security is based on the Diffie-Hellman assumption in bilinear groups (the SXDH assumption in asymmetric bilinear groups).

In this work we construct an asymptotically shorter ring signature from the hardness of the Diffie-Hellman assumption in bilinear groups. Each signature comprises $\Theta(\sqrt[3]{n})$ group elements, signing a message requires computing $\Theta(\sqrt[3]{n})$ exponentiations, and verifying a signature requires $\Theta(n^{2/3})$ pairing operations. To the best of our knowledge, this is the first ring signature based on bilinear groups with $o(\sqrt{n})$ signatures and sublinear verification complexity.

1 Introduction

Ring signatures, introduced by Rivest, Shamir and Tauman, [28], allow to anonymously sign a message on behalf of a ring of users $R = \{P_1, \ldots, P_n\}$, only if the signer belongs to that ring. That is, no one outside R can forge a valid signature and an honestly computed signature reveals no information about the actual signer. Unlike other similar primitives such as group signatures [7], ring signatures are not coordinated: each user generates secret/public keys on his own — i.e. no central authorities — and might sign on behalf of a ring without the approval or assistance of the other members.

*This work was funded in part by the French ANR ALAMBIC project (ANR-16-CE39-0006).

The original motivation for ring signatures was anonymous leakage of secrets. Suppose a high rank officer wants to leak some sensitive document to a journalist without revealing its identity. To do so, it signs this document using a ring signature where the ring contains all other high rank officers. The journalist is convinced that some high rank officer signed the document, but it has no clue who, while this leakage might go unnoticed for the rest of officers.

More recently, ring signatures have also found applications in the construction of confidential transactions for cryptocurrencies. In a usual (non-anonymous) transaction the user computes a signature that assesses if is allowed to spend coins. In cryptocurrencies like Monero, a user form a ring from public keys in the blockchain to issue a ring signature on the transaction. Thereby, the anonymity properties of the ring signature guarantee untraceability of the transaction and fungibility, i.e. two coins can be mutually substituted. Given the practical usefulness of ring signatures, it becomes crucial to study and improve its efficiency and security.

1.1 Related Work

The efficiency of a ring signature might be splitted into three parameters: the signature size, the time required for computing a signature, and the time required for verifying a signature. Among these metrics, the signature size has received the most attention and improvements in the size usually imply improvement in the other metrics. In terms of signature size, two of the most efficient constructions have signature size logarithmic in the size of the ring [18, 23]. Both constructions rely on the random oracle model, which is an idealization of hash functions with known theoretical inconsistencies [13]. Malavolta et al. constructed a constant size ring signature without random oracles [24] using SNARKS [11, 8, 17] as a subroutine, which are known to require controversial non-falsifiable assumptions such as the knowledge of exponent assumption [12, 26]. Unlike traditional falsifiable assumptions (e.g. DDH), is not possible to efficiently check whether the adversary effectively breaks the assumption yielding non-explicit security reductions [26]. In practice, random oracles and non-falsifiable assumptions offer great efficiency at the price of less understood security guarantees. Therefore, we believe that it is important and challenging to explore practical constructions from milder assumptions.

Using only standard assumptions like RSA, Chase and Lysyanskaya proposed a ring signature scheme whose size is independent from the number of users [6]. Their ring signature is built on top of signatures of knowledge and accumulators, following Dodis et al. [9]. The scheme description is only sketched and no proof of security is given but, for fairness (as also noted in [24]), their work is previous to the (now standard) formal definition of ring signatures of Bender et al. [2]. Anyway, signatures of knowledge are built on top of simulation sound NIZK which in turn is built from standard NIZK. The underlying statements involve multiplications modulo $\phi(N)$ and exponentiations modulo N, where N an RSA modulus. To the best of our knowledge, no efficient NIZK schemes under standard assumptions are known for statements of this kind. Thus, the only alternative under standard assumptions seems the NIZK for circuit satisfiability of Groth, Ostrovsky and Sahai [20]. A naive implementation of this protocol would require, at least, perfectly binding bit-by-bit commitments of integers in $\mathbb{Z}_N$. Typically, N requires 1024 bits so this solution requires at least 1024 elements of a bilinear group. On contrast, our construction is far more efficient than that for any $n < 10^4$. Although it might be possible to avoid committing bit-by-bit, there would be still many challenges. For example, it would require a NIZK proof that $a = b^y \mod N$, for $a, b \in \mathbb{Z}_N, y \in \mathbb{Z}_{\phi(N)}$, for which the only solution seems to be committing to y bit-by-bit (in order to use binary exponentiation) leading again to proofs of $\sim$ 1024 group elements. Our conclusion is that is not clear how to implement Chase and Lysyanskaya's ring signature in a practical way.

Despite Chase and Lysyanskaya's construction, without random oracles or non-falsifiable assumptions all constructions have signatures of size linear in the size of the ring, being the sole exception the $\Theta(\sqrt{n})$ ring signature of Chandran et al. [5]. They construct a simple and elegant ring signature which at its core implements a *set-membership proof*, i.e. a proof that some committed public key belongs to the set of public keys of the ring users. Their set-membership proof is quite strong, in the sense that the verification keys may be even chosen by the adversary. Going a step forward, we will build a more efficient but weaker set-membership proof which is still useful for building ring signatures.

We note that no improvements in the signature size have been made within a decade. In fact, although two previous works claim to construct signatures of constant [4] or logarithmic [16] size, in the full version (see [15]) of this work we show that one construction fails to give a correct proof of security and the other is in fact of size $\Theta(n)$. The only (non-asymptotic) improvements we are aware of are [27, 14].

1.2 Our contribution

In this work we present the first ring signature based on bilinear groups whose signature size is asymptotically smaller than Chandran et al.'s, and whose security is proven under falsifiable assumptions and without random oracles. The signature consists of $\Theta(\sqrt[3]{n})$ group elements, computing a signature requires $\Theta(\sqrt[3]{n})$ exponentiations, and verifying a signature requires $\Theta(n^{2/3})$ pairings. Our ring signature is perfectly anonymous, i.e. it completely hides the identity of the actual signer, and is computationally infeasible to forge signatures for non-members of the ring.

As a first step, we construct a $\Theta(\sqrt[3]{n})$ ring signature whose security relies on a security assumption — the permutation pairing assumption — introduced by Groth and Lu [19] in an unrelated setting: proofs of correctness of a shuffle. While the assumption is "non-standard", in the sense that is not a "DDH like" assumption, it is a falsifiable assumption and it was proven hard in generic symmetric bilinear groups by Groth and Lu. We work on asymmetric groups (Type III groups [10]) and thus we give a natural translation of the permutation pairing assumption which we also prove secure in generic asymmetric bilinear groups.

We give a second construction which is solely based on the security of the DDH assumption in both base groups (the so called SXDH assumption). The construction is highly inspired in the first construction, but we manage to get rid of the permutation pairing assumption and further shorten the size of the signature. A comparison of our ring signatures and Chandran et al.'s is given in Table 1.

	Chandran et al. [5]	Sect. 3.2	Sect. 4.2
CRS size $\mathbb{G}_1/\mathbb{G}_2$	4/4	4/4	4/8
Verification key size $\mathbb{G}_1/\mathbb{G}_2$	1/0	2/5	10/9
Signature size $\mathbb{G}_1/\mathbb{G}_2$	$12\sqrt{n}+10/15\sqrt{n}+8$	$24\sqrt[3]{n}+36/34\sqrt[3]{n}+24$	$18\sqrt[3]{n}+30/34\sqrt[3]{n}+18$
Signature generation #exps.	$37\sqrt{n}+23$	$80\sqrt[3]{n}+71$	$72\sqrt[3]{n}+61$
Verification #pairings	$2n+60\sqrt{n}+38$	$8n^{2/3}+162\sqrt[3]{n}+118$	$8n^{2/3}+122\sqrt[3]{n}+94$
Assumption	SXDH	PPA	SXDH
Erasures	No	Yes	No

Table 1: Comparison of Chandran et al.'s ring signature and ours for a ring of size n. 'Signature generation' is given in number of exponentiations, 'Verification' is given in number of pairings, and all other rows are given in number of group elements. The security of the three schemes is proved under the unforgeability of the Boneh-Boyen signature scheme plus the corresponding assumption indicated in the row 'Assumption'. The last row states if the key generation algorithm erases its random coins after generating the verification and secret keys.

1.3 Technical Overview

Most ring signature constructions have followed the next approach. Given a ring of users, defined by the set of their verification keys, and a message: a) sign the message, b) prove in zero-knowledge knowledge of a signature which can be verified using some committed/randomized verification key, and then c) prove in zero-knowledge that this verification key belongs to the set of public keys in the ring. The most expensive part is c) and is sometimes called a *set-membership proof.*

We observe that, when proving unforgeability, *all the verification keys forming the ring are honestly generated.* Indeed, it only makes sense to guarantee unforgeability when all the members of the ring are honest (otherwise the adversary knows at least one secret key) and thus the set-membership proof might assume that all verification keys were honestly generated. It turns out that all the schemes we are aware of, in particular Chandran et al.'s, obviate this property, meaning that their set-membership proofs work even for adversarially chosen verification keys. We ask the following natural question.

> *Can we construct more efficient set membership proofs (without random oracles or non-falsifiable assumptions) when verification keys are sampled from a known distribution?*

We answer this question in the affirmative constructing a $\Theta(\sqrt[3]{n})$ set membership proof specially tailored to the case when the verification keys are honestly sampled. In contrast, Chandran et al.'s proof is of size $\Theta(\sqrt{n})$ but it makes no assumption on the verification keys distribution.

Our Construction from the Permutation Pairing Assumption. Our main technical tools are two hash functions compatible with Groth-Sahai proofs.

The first function, h, is *second-preimage resistant* under a slightly different notion of collision. Given $\mathbf{A} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$ randomly sampled from the domain of h, it is hard to find $\mathbf{A}'$ such that $h(\mathbf{A}') = h(\mathbf{A})$ whenever $\mathbf{A}'$ is not a permutation of $\mathbf{A}$. We give a simple instantiation of h based on the permutation pairing assumption (PPA). For simplicity, consider a symmetric bilinear group $\mathbb{G}$ of order q and generated by $\mathcal{P}$ (it can be extended to asymmetric bilinear groups as we show in section 2.1). This assumption states that, given $\boldsymbol{a}_1 = (x_1\mathcal{P}, x_1^2\mathcal{P}), \ldots, \boldsymbol{a}_m = (x_m\mathcal{P}, x_m^2\mathcal{P})$, for $x_1, \ldots, x_m \leftarrow \mathbb{Z}_q$, the only way to compute $\boldsymbol{a}'_1 = (y_1\mathcal{P}, y_1^2\mathcal{P}), \ldots, \boldsymbol{a}'_m = (y_m\mathcal{P}, y_m^2\mathcal{P})$ such that $\sum_{i=1}^m \boldsymbol{a}'_i = \sum_{i=1}^m \boldsymbol{a}_i$ is to take $\mathbf{A}'$ as a permutation of the columns of $\mathbf{A}$. It is straightforward to note that $h(\mathbf{A}) := \sum_{i=1}^m \boldsymbol{a}_i$ is second-preimage resistant "modulo permutations", given the hardness of PPA.

Our second function, g, is collision-resistant in the traditional sense. It uses $\mathbf{A}$ as key and returns $g_{\mathbf{A}}(vk_1, \ldots, vk_m) = \sum_{i=1}^m e(\boldsymbol{a}_i, vk_i)$ for $vk_1, \ldots, vk_m \in \mathbb{G}$. Groth and Lu conjectured that it is hard to find non-trivial $vk_1, \ldots, vk_m \in \mathbb{G}$ such that $\sum_{i=1}^m e(\boldsymbol{a}_i, vk_i) = 0$ when each $\boldsymbol{a}_i$ is of the form $(x_i\mathcal{P}, x_i^2\mathcal{P})$ and $x_i \leftarrow \mathbb{Z}_q$ [19]. They give some evidence that this assumption might be true proving its hardness in the generic bilinear group model. It follows that g is collision resistant given the hardness of the aforementioned assumption. In order to be more compatible with Groth-Sahai proofs (say, structure-preserving) we compute g's outputs in the base group, instead of the target group $\mathbb{G}_T$. To render $g_{\mathbf{A}}(\boldsymbol{vk}) \in \mathbb{G}$ efficiently computable we make $sk_i\boldsymbol{a}_i$ publicly available, where $vk_i = sk_i\mathcal{P}$, and redefine g as $g_{\mathbf{A}}(\boldsymbol{vk}) = \sum_i sk_i\boldsymbol{a}_i$. Note that the discrete logarithm in base $\mathcal{P}_T = e(\mathcal{P}, \mathcal{P})$ of g defined over $\mathbb{G}_T$ and the discrete logarithm in base $\mathcal{P}$ of g defined over $\mathbb{G}$ remain the same.

Each $\boldsymbol{a}_i$ will be taken from the ring member's verification key and hence, since all these verification keys are honestly sampled, when proving unforgeability we may assume that $\mathbf{A}$ is honestly sampled from the PPA distribution.

The Basic Construction. In our ring signature, each user possesses an "extended verification key" which contains the verification key of a Boneh-Boyen signature scheme $vk = sk\mathcal{P}$ plus $\boldsymbol{a}$ and $sk\boldsymbol{a}$, where sk is the corresponding secret key.[1] We want to show that some commitment c opens to vk and $vk \in$

[1] Although any signature scheme compatible with Groth-Sahai proofs suffices (e.g. structure preserving signatures), we would rather keep it simple and stick to Boneh-Boyen signature which, since the verification key is just one group element, simplifies the notation and reduces the size of the final signature.

$\{vk_1, \ldots, vk_n\}$. To do so, we arrange the n elements of the ring into $n^{2/3}$ blocks of size $m = \sqrt[3]{n}$. We use the following notation: for $\{s_1, \ldots, s_n\}$ define $s_{i,j} := s_{(i-1)m+j}$, where $1 \leq i \leq n^{2/3}, 1 \leq j \leq m$. Assume that $vk = vk_{\mu,\nu}$.

Split $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ into $\mathbf{A}_i := (\boldsymbol{a}_{i,1}, \ldots, \boldsymbol{a}_{i,m})$ and $(vk_1, \ldots, vk_n)$ into $\boldsymbol{vk}_i = (vk_{i,1}, \ldots, vk_{i,m})$, for $1 \leq i \leq n^{2/3}$, and define $H := \{h(\mathbf{A}_1), \ldots, h(\mathbf{A}_{n^{2/3}})\}$ and $G := \{g_{\mathbf{A}_1}(\boldsymbol{vk}_1), \ldots, g_{\mathbf{A}_{n^{2/3}}}(\boldsymbol{vk}_{n^{2/3}})\}$. We use Chandran et al.'s set-membership proof of size $\Theta(\sqrt{n})$ to prove knowledge of some $h(\mathbf{A}_\mu) \in H$. Since $|H| = n^{2/3}$, this proof is of size $\Theta(\sqrt[3]{n})$. Then we prove knowledge of $\mathbf{A}'$, a preimage of $h(\mathbf{A}_\mu)$ such that $\boldsymbol{a}'_1 = \boldsymbol{a}_{\mu,\nu}$. Using Groth-Sahai proofs it requires commitments to the $\sqrt[3]{n}$ columns of $\mathbf{A}'$ plus a $\Theta(1)$ proof that $h(\mathbf{A}') = h(\mathbf{A}_\mu)$. Hence, this part of the proof adds up to $\Theta(\sqrt[3]{n})$ group elements.

We give a second set-membership proof of knowledge of some $g_{\mathbf{A}_{\mu'}}(\boldsymbol{vk}_{\mu'}) \in G$ such that $\mu' = \mu$ (this is straightforward to do with Chandran et al.'s set-membership proof). We commit to $\boldsymbol{vk}'$, a permutation of $\boldsymbol{vk}_\mu$ such that $vk'_1 = vk_{\mu,\nu}$ (and consistent with $\mathbf{A}'$), and we prove using Groth-Sahai proofs that $g_{\mathbf{A}_{\mu'}}(\boldsymbol{vk}_{\mu'}) = g_{\mathbf{A}'}(\boldsymbol{vk}')$. Again, this part of the proof adds $\Theta(\sqrt[3]{n})$ group elements.

The proof that $h(\mathbf{A}') = h(\mathbf{A}_\mu)$ implies that $\mathbf{A}'$ is a permutation of $\mathbf{A}_\mu$, which can be equivalently written as $\mathbf{A}' = \mathbf{A}_\mu\mathbf{P}$, where $\mathbf{P}$ is some permutation matrix. Given that $e(g_{\mathbf{A}'}(\boldsymbol{vk}'), \mathcal{P}) = e(\mathbf{A}_\mu\mathbf{P}, \boldsymbol{vk}') = e(g_{\mathbf{A}_\mu}(\mathbf{P}\boldsymbol{vk}'), \mathcal{P}) = e(g_{\mathbf{A}_\mu}(\boldsymbol{vk}_\mu), \mathcal{P})$, the collision resistance of g implies that $vk'_1, \ldots, vk'_m$ is a permutation of $vk_{\mu,1}, \ldots, vk_{\mu,m}$. We conclude that $vk_{\mu,\nu} = vk'_1$ is in the ring.

Getting rid of the permutation pairing assumption. The PPA-based ring signature has the disadvantage that the PPA is not a constant-size assumption and belongs to the class of the so called q-assumptions (such as the Strong Diffie-Hellman assumption among others). It is then desirable to have a similar construction under more standard constant-size assumptions such as the SXDH assumption.

Consider the set of binary vectors of size m and the function h defined as the hamming weight of a binary vector $h(\boldsymbol{\beta}) = \sum_{i=1}^m \beta_i$. Analogously as with the PPA, $h(\boldsymbol{\beta}) = h(\boldsymbol{\beta}')$ and $\boldsymbol{\beta}, \boldsymbol{\beta}' \in \{0,1\}^m$ implies that $\boldsymbol{\beta}'$ is a permutation of $\boldsymbol{\beta}$. (Note that in this case $\boldsymbol{\beta}'$ is a permutation of $\boldsymbol{\beta}$ unconditionally.) We use this property of binary vectors as a replacement of the PPA. Define also $g_{\boldsymbol{\beta}}(\boldsymbol{vk}) := \sum_i \beta_i vk_i$. Although g is longer collision resistant, it turns out that proofs that $h(\boldsymbol{\beta}') = h(\boldsymbol{\beta})$ and $g_{\boldsymbol{\beta}'}(\boldsymbol{vk}') = g_{\boldsymbol{\beta}}(\boldsymbol{vk})$ will still allow us to prove unforgeability.[2]

Each possible ring member generates a single $\beta \in \{0,1\}$ and her extended verification key contains commitments $\boldsymbol{a} = \mathsf{Com}(\beta)$, $\boldsymbol{d} = \mathsf{Com}(\beta vk)$, and vk. Additionally it contains π, a Groth-Sahai proof that $\beta \in \{0,1\}$, and θ, a Groth-Sahai proof that $y = \beta vk$ where y is $\boldsymbol{d}$'s opening. Although g and h are not efficiently

[2] Even when the adversary only knows a commitment to $\boldsymbol{\beta}$, as it will be in our case, g is not collision resistant. For small rings, the adversary may guess $\boldsymbol{\beta}$ with non-negligible probability and solve $\sum_i \beta_i(vk_i - vk'_i) = 0$ for some non trivial $\boldsymbol{vk}'$. However, this adversary is not even not aware that it has found a collision.

computable from the extended verification keys, it is possible to compute commitments to $h(\boldsymbol{\beta})$ and $g_{\boldsymbol{\beta}}(\boldsymbol{vk})$ using the homomorphic properties of Groth-Sahai commitments. Indeed $\mathsf{Com}(h(\boldsymbol{\beta})) = \sum_i \boldsymbol{a}_i$ and $\mathsf{Com}(g_{\boldsymbol{\beta}}(\boldsymbol{vk})) = \sum_i \boldsymbol{d}_i$. Using this fact together with the re-randomizability of Groth-Sahai proofs (see [1]) we will emulate the ring signature in the PPA setting.

Assume the signer wish to sign on behalf of the ring $R = \{vk_{1,1}, \ldots, vk_{n^{2/3},m}\}$ knowing the secret key corresponding to $vk_{\mu,\nu}$. Define $\mathbf{A}_1, \ldots, \mathbf{A}_{n^{2/3}}$ as in the PPA construction and let $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{n^{2/3}}$ the respective openings. In the first part of the signature, the signer proves knowledge of some $\mathsf{Com}(h(\boldsymbol{\beta}_\mu))$ from $H = \{\mathsf{Com}(h(\boldsymbol{\beta}_1)), \ldots, \mathsf{Com}(h(\boldsymbol{\beta}_{n^{2/3}}))\}$ and then commits to $\mathbf{A}'$, a permutation of a re-randomization of $\mathbf{A}_\mu$ such that $\boldsymbol{a}'_1$ is a re-randomization of $\boldsymbol{a}_{\mu,\nu}$. Then it shows with a Groth-Sahai proof that a) $\sum_i \boldsymbol{a}'_i - \mathsf{Com}(h(\boldsymbol{\beta}_\mu)) = \mathsf{Com}(0)$, and b) $\beta'_1 \ldots, \beta'_m \in \{0,1\}$ re-randomizing proofs $\pi_{\mu,1}, \ldots, \pi_{\mu,m}$. It follows that $\boldsymbol{\beta}'$, the vector of openings of $\mathbf{A}'$, is a permutation of $\boldsymbol{\beta}_\mu$, the vector of openings of $\mathbf{A}_\mu$.

In the second part the signer proves knowledge of some $\mathsf{Com}(g_{\boldsymbol{\beta}_\mu}(\boldsymbol{vk}_\mu))$ from $G = \{\mathsf{Com}(g_{\boldsymbol{\beta}_1}(\boldsymbol{vk}_1)), \ldots, \mathsf{Com}(g_{\boldsymbol{\beta}_{n^{2/3}}}(\boldsymbol{vk}_{n^{2/3}}))\}$ and computes commitments $\boldsymbol{c}'_1, \ldots, \boldsymbol{c}'_m$ to $vk'_1 = vk_{\mu,1}, \ldots, vk'_m = vk_{\mu,m}$, respectively. In section 4.1 we show that, from $\boldsymbol{d}_{\mu,1}, \ldots, \boldsymbol{d}_{\mu,m}$ and $\theta_{\mu,1}, \ldots, \theta_{\mu,m}$ one can derive a proof that $\sum_i \beta'_i vk'_i = \sum_i \beta_{\mu,i} vk_{\mu,i}$, or equivalently a proof that $g_{\boldsymbol{\beta}'}(\boldsymbol{vk}') = g_{\boldsymbol{\beta}_\mu}(\boldsymbol{vk}_\mu)$.

Zero-knowledge of the set-membership proof implies perfect anonymity of the ring signature, and follows from the fact that all proofs are statistically independent of vk when the Groth-Sahai CRS is perfectly hiding. Soundness implies unforgeability, and follows from the following argument.

Without loss of generality, we may assume that $\boldsymbol{vk}_\mu$ has not repeated entries since the verifier might drop all repeated entries in R without changing the statement. Suppose an adversary wish to convince the verifier that $vk = vk'_1$ is in R while in fact $vk \notin R$. In particular, this implies that vk'_1 is different from each of $vk_{\mu,1}, \ldots, vk_{\mu,m}$. By the pigeonhole principle, there must be also some $vk_{\mu,i}$ that is different from each of $vk'_1, \ldots, vk'_m$.

Since we can guess such μ, i pair beforehand with non negligible probability $1/Q$, where Q is the maximum number of verification keys. We can jump to a game where we program $\mathbf{A} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_Q)$ such that its opening $\boldsymbol{\beta} \in \{0,1\}^Q$ is of hamming weight 1 and $\beta_{\mu,i} = 1$. By the hiding property of the commitment scheme, which is based on the SXDH assumption, the adversary notices such change in $\mathbf{A}$ only with negligible probability. Given that $\boldsymbol{\beta}'$ is a permutation of $\boldsymbol{\beta}$, in this game the equation $\sum_i \beta'_i vk'_i = \sum_i \beta_{\mu,i} vk_{\mu,i}$ is in fact $vk'_j = vk_{\mu,i}$, for some $1 \le j \le m$, and hence the adversary has 0 probability of winning.

The erasures assumption. A ring signature must tolerate the adaptive corruption of the verification keys. That is, an adversary may adaptively ask for the random coins used for generating the verification keys. In the PPA-based ring signature, this amounts to reveal x_i and x_i^2 which is is incompatible with the PPA (unless one considers a much stronger interactive assumption). The only alternative seems to be assume that the key generation algorithm can erase its random coins.[3]

But this is not the case for the SXDH-based construction. To avoid erasures, each possible ring member samples the extended verification key with $\beta = 0$. Thereby, Every answer to a corruption query is of the form $0, sk$ plus all the random coins used to generate the extended verification key.

We can argue as before that an adversary may produce some $vk \notin R$ with roughly the same probability even if $\mathbf{A}$ is computed from a random binary vector $\boldsymbol{\beta}$ of hamming weight 1 with the unique 1 in the right place. In this case we can answer all corruption queries with the exception of the unique verification key for which $\beta = 1$. But anyway, the probability that the adversary corrupts this verification key is no greater than $1/Q$ so we can safely abort if this is the case. The rest of the argument is exactly as before.

Relation to [14]. Our construction is similar to the set membership proof of González et al. [14, Appendix D.2] also of size $\Theta(\sqrt[3]{n})$. There, the CRS contains a matrix $\mathbf{A}$ of size $2 \times m$ that is used to compute $\sqrt[3]{n}$ hashes of $n^{2/3}$ of subsets of verification keys of size $\sqrt[3]{n}$. Then some hidden hash is shown to belong to the set for $n^{2/3}$ hashes. These hashes are computed as a linear combination of the columns of $\mathbf{A}$ with the verification keys.

One could turn this construction into a ring signature including $vk\mathbf{A}$ in each verification key. However, the fact that $\mathbf{A}$ is fixed implies that signatures of size $\Theta(\sqrt[3]{n})$ can be obtained only when $n \leq m^3$. So, asymptotically, this is not a $\Theta(\sqrt[3]{n})$ signature. Furthermore, the verification key will be of size $\Theta(m)$. In contrast, our ring signature verification keys are of size $\Theta(1)$ and the size of the ring is unbounded.

2 Preliminaries

We write PPT as a shortcut for probabilistic polynomial time Turing machine.

Let Gen_a be some PPT which on input 1^λ, where λ is the security parameter, returns the *group key* which is the description of an asymmetric bilinear group $gk := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_T = e(\mathcal{P}_1, \mathcal{P}_2), q)$, where $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ are groups of prime order q, the element $\mathcal{P}_s$ is a generator of $\mathbb{G}_s$, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is an efficiently computable and non-degenerated bilinear map. We will use additive notation for the group operation of all groups.

Elements in $\mathbb{G}_s$ are denoted implicitly as $[a]_s := a\mathcal{P}_s$, where $a \in \mathbb{Z}_q$, $s \in \{1, 2, T\}$. The pairing operation is written as a product $\cdot$, that is $[a]_1 \cdot [b]_2 = [a]_1[b]_2 = [b]_2[a]_1 = e([a]_1, [b]_2) = [ab]_T$. Vectors and matrices are denoted in boldface. Given a matrix $\mathbf{T} = (t_{i,j})$, $[\mathbf{T}]_s$ is the natural embedding of $\mathbf{T}$ in $\mathbb{G}_s$, that is, the matrix whose (i, j)th entry is $t_{i,j}\mathcal{P}_s$. Given a matrix $\mathbf{S}$ with the same number of rows as $\mathbf{T}$, we define $\mathbf{S}|\mathbf{T}$ as the concatenation of $\mathbf{S}$ and $\mathbf{T}$.

[3] We elaborate more on the erasures assumption for ring signatures in the full version of this work [15].

2.1 Hardness Assumptions

We use a natural translation to asymmetric groups of the permutation pairing assumption introduced by Groth and Lu.

Definition 1 (Permutation Pairing Assumption [19]). *Let* $\mathcal{Q}_m = \overbrace{\mathcal{Q}|\dots|\mathcal{Q}}^{m\ times}$*, where concatenation of distributions is defined in the natural way and* $\mathcal{Q} : \boldsymbol{a} = \binom{x}{x^2}$*,* $x \leftarrow \mathbb{Z}_q$*. We say that the m-permutation pairing assumption holds relative to* Gen_a *if for any adversary* A

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}_a(1^\lambda); \mathbf{A} \leftarrow \mathcal{Q}_m; \\ ([\mathbf{Z}]_1, [\underline{\boldsymbol{z}}]_2) \leftarrow \mathsf{A}(gk, [\mathbf{A}]_1, [\mathbf{A}]_2): \\ \text{(i) } \sum_{i=1}^m [\boldsymbol{z}_i]_1 = \sum_{i=1}^m [\boldsymbol{a}_i]_1, \\ \text{(ii) } \forall i \in [m]\ [z_{1,i}]_1[1]_2 = [1]_1[\underline{z}_i]_2 \textit{ and } [z_{2,i}]_1[1]_2 = [z_{1,i}]_1[\underline{z}_i]_2, \\ \textit{ and } \mathbf{Z} \textit{ is not a permutation of the columns of } \mathbf{A} \end{array}\right],$$

where $[\mathbf{Z}] = [\boldsymbol{z}_1|\cdots|\boldsymbol{z}_m]_1 \in \mathbb{G}_1^{2\times m}, [\mathbf{A}]_1 = [\boldsymbol{a}_1|\cdots|\boldsymbol{a}_m]_1 \in \mathbb{G}_1^{2\times m}$*,* $[\underline{\boldsymbol{z}}]_2 = [(\underline{z}_1, \dots, \underline{z}_m)]_2 \in \mathbb{G}_2^{1\times m}$*, is negligible in* λ*.*

Groth and Lu proved the hardness of the PPA in generic symmetric bilinear groups [19]. In the full version of this work we show that the m-PPA in generic asymmetric groups is as hard as the PPA in generic symmetric groups [15].

For constructing the function g in the PPA instantiation we require the assumption that is hard to find $[\boldsymbol{x}]_2 \in \mathbb{G}_2^m \setminus \{0\}$ such that $[\boldsymbol{x}^\top]_2[\mathbf{A}^\top]_1 = 0$, where $\mathbf{A} \leftarrow \mathcal{Q}_m$. Groth and Lu proved the generic hardness of the natural translation of this assumption to symmetric groups [19]. We observe that this assumption corresponds to a kernel assumption [25], the $\mathcal{Q}_m^\top$-KerMDH assumption in symmetric groups.

Definition 2 (Kernel Diffie-Hellman Assumption in $\mathbb{G}$ [25]). *Let* $gk \leftarrow \mathsf{Gen}_a(1^\lambda)$ *and* $\mathcal{D}_{\ell,k}$ *a distribution over* $\mathbb{Z}_q^{\ell\times k}$*. The Kernel Diffie-Hellman assumption in* $\mathbb{G}$ *(*$\mathcal{D}_{\ell,k}$-$\mathsf{KerMDH}_{\mathbb{G}_s}$*) says that every PPT Algorithm has negligible advantage in the following game: given* $[\mathbf{A}]$*, where* $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$*, find* $[\boldsymbol{x}] \in \mathbb{G}^\ell$*,* $\boldsymbol{x} \neq \mathbf{0}$*, such that* $[\boldsymbol{x}]^\top[\mathbf{A}] = [\mathbf{0}]_T$*.*

Our assumption is the natural translation of the $Q_m^\top$-KerMDH assumption to asymmetric groups, where $[\mathbf{A}]_s$ is also given in $\mathbb{G}_{3-s}$. Such assumption is a weaker variant of a *split* KerMDH assumption, introduced in [14], where the adversary might find an element in $\mathrm{Ker}(\mathbf{A})$ which is splitted between $\mathbb{G}_1$ and $\mathbb{G}_2$.

Definition 3 (Split Kernel Diffie-Hellman Assumption [14]). *Let* $gk \leftarrow \mathsf{Gen}_a(1^\lambda)$ *and* $\mathcal{D}_{\ell,k}$ *a distribution over* $\mathbb{Z}_q^{\ell\times k}$*. The Split Kernel Diffie-Hellman assumption (*$\mathcal{D}_{\ell,k}$-$\mathsf{SKerMDH}$*) says that every PPT Algorithm has negligible advantage in the following game: given* $[\mathbf{A}]_1, [\mathbf{A}]_2$*, where* $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$*, find* $[\boldsymbol{x}]_1 \in \mathbb{G}_1^\ell, [\boldsymbol{y}]_2 \in \mathbb{G}_2^\ell$*,* $\boldsymbol{x} \neq \boldsymbol{y}$*, such that* $[\boldsymbol{x}]_1^\top[\mathbf{A}]_1 = [\boldsymbol{y}]_2^\top[\mathbf{A}]_2$*.*

Our weaker variant restricts the adversary to give solutions only in $\mathbb{G}_1$ (i.e. $[\boldsymbol{y}]_2 = 0$), while we simply refer to it as the $Q_m^\top$-$\mathsf{SKerMDH}$. González et al. proved that, in generic asymmetric groups, the $\mathcal{D}_{\ell,k}$-$\mathsf{SKerMDH}$ is as hard as the $\mathcal{D}_{\ell,k}$-KerMDH assumption in symmetric groups, for any distribution $\mathcal{D}_{\ell,k}$ [14]. We conclude that the $Q_m^\top$-$\mathsf{SKerMDH}$ is hard in generic asymmetric groups (and of course, the weaker variant that we will be using).

Finally, we recall also the definition of the Decisional Diffie-Hellman assumption (in matrix notation).

Definition 4 (Decisional Diffie-Hellman (DDH) in $\mathbb{G}_s$). *Let $gk \leftarrow \mathsf{Gen}_a(1^\lambda)$ and let $\mathbf{A} := (a, 1)^\top$, $a \leftarrow \mathbb{Z}_q$. We say that the DDH assumption holds relative to Gen_a if for all PPT adversaries D*

$$\mathbf{Adv}_{\mathrm{DDH},\mathsf{Gen}_s}(\mathsf{D}) := |\Pr[\mathsf{D}(gk, [\mathbf{A}]_s, [\mathbf{A}w]_s) = 1] - \Pr[\mathsf{D}(gk, [\mathbf{A}]_s, [\boldsymbol{z}]_s) = 1]|$$

is negligible in λ, where the probability is taken over $gk \leftarrow \mathsf{Gen}_a(1^\lambda)$, $a \leftarrow \mathbb{Z}_q$, $w \leftarrow \mathbb{Z}_q$, $[\boldsymbol{z}]_2 \leftarrow \mathbb{G}_s^2$, and the coin tosses of the adversary. We say that the Symmetric eXternal Diffie-Hellman (SXDH) assumption holds if the DDH assumption holds in both $\mathbb{G}_1$ and $\mathbb{G}_2$.

2.2 Ring Signature Definition

We follow Chandran et al.'s definitions [5], which extends the original definition of Bender et al. [2] by including a CRS and perfect anonymity. We allow erasures in the key generation algorithm.

Definition 5 (Ring Signature). *A ring signature scheme consists of a quadruple of PPT algorithms $(\mathsf{CRSGen}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ that respectively, generate the common reference string, generate keys for a user, sign a message, and verify the signature of a message. More formally:*

- $\mathsf{CRSGen}(gk)$, *where gk is the group key, outputs the common reference string ρ.*
- $\mathsf{KeyGen}(\rho)$ *is run by the user. It outputs a public verification key vk and a private signing key sk.*
- $\mathsf{Sign}_{\rho,sk}(m, R)$ *outputs a signature σ on the message m with respect to the ring $R = \{vk_1, \ldots, vk_n\}$. We require that (vk, sk) is a valid key-pair output by KeyGen and that $vk \in R$.*
- $\mathsf{Verify}_{\rho,R}(m, \sigma)$ *verifies a purported signature σ on a message m with respect to the ring of public keys R and reference string ρ. It outputs 1 if σ is a valid signature for m with respect to R and ρ, and 0 otherwise.*

The quadruple $(\mathsf{CRSGen}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ is a ring signature with perfect anonymity if it has perfect correctness, computational unforgeability and perfect anonymity as defined below.

Definition 6 (Perfect Correctness). *We require that a user can sign any message on behalf of a ring where she is a member. A ring signature* (CRSGen, $\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify}$) *has perfect correctness if for any unbounded adversary* A *we have:*

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}(1^\lambda); \rho \leftarrow \mathsf{CRSGen}(gk); (vk, sk) \leftarrow \mathsf{KeyGen}(\rho); \\ (m, R) \leftarrow \mathsf{A}(\rho, vk, sk); \sigma \leftarrow \mathsf{Sign}_{\rho,sk}(m; R) : \\ \mathsf{Verify}_{\rho,R}(m, \sigma) = 1 \ \textit{or}\ vk \notin R \end{array}\right] = 1$$

Definition 7 (Computational Unforgeability). *A ring signature scheme* ($\mathsf{CRSGen}, \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify}$) *is unforgeable if it is infeasible to forge a ring signature on a message without controlling one of the members in the ring. Formally, it is unforgeable when for all PPT adversaries* A *we have that*

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}(1^\lambda); \rho \leftarrow \mathsf{CRSGen}(gk); (m, R, \sigma) \leftarrow \mathsf{A}^{\mathsf{VKGen},\mathsf{Sign},\mathsf{Corrupt}}(\rho) : \\ \mathsf{Verify}_{\rho,R}(m, \sigma) = 1 \end{array}\right]$$

is negligible in λ*, where*

- VKGen *on query number* i *selects randomness* w_i*, computes* $(vk_i, sk_i) := \mathsf{KeyGen}(\rho; w_i)$ *and returns* vk_i*.*
- $\mathsf{Sign}(i, m, R)$ *returns* $\sigma \leftarrow \mathsf{Sign}_{\rho,sk_i}(m, R)$*, provided* (vk_i, sk_i) *has been generated by* VKGen *and* $vk_i \in R$*.*
- $\mathsf{Corrupt}(i)$ *returns* sk_i *provided* (vk_i, sk_i) *has been generated by* VKGen*. (The fact that* w_i *is not revealed allows the erasure of the random coins used in the generation of* (vk_i, sk_i)*).*
- A *outputs* (m, R, σ) *such that* Sign *has not been queried with* $(*, m, R)$ *and* R *only contains keys* vk_i *generated by* VKGen *where* i *has not been corrupted.*

Definition 8 (Perfect Anonymity). *A ring signature scheme* ($\mathsf{CRSGen}, \mathsf{KeyGen}$, $\mathsf{Sign}, \mathsf{Verify}$) *has perfect anonymity, if a signature on a message* m *under a ring* R *and key* vk_{i_0} *looks exactly the same as a signature on the message* m *under the ring* R *and key* vk_{i_1}*, where* $vk_{i_0}, vk_{i_1} \in R$*. This means that the signer's key is hidden among all the honestly generated keys in the ring. Formally, we require that for any unbounded adversary* A*:*

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}(1^\lambda); \rho \leftarrow \mathsf{CRSGen}(gk); \\ (m, i_0, i_1, R) \leftarrow \mathsf{A}^{\mathsf{KeyGen}(\rho)}(\rho); \sigma \leftarrow \mathsf{Sign}_{\rho,sk_{i_0}}(m, R) : \\ \mathsf{A}(\sigma) = 1 \end{array}\right] =$$
$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}(1^\lambda); \rho \leftarrow \mathsf{CRSGen}(gk); \\ (m, i_0, i_1, R) \leftarrow \mathsf{A}^{\mathsf{KeyGen}(\rho)}(\rho); \sigma \leftarrow \mathsf{Sign}_{\rho,sk_{i_1}}(m, R) : \\ \mathsf{A}(\sigma) = 1 \end{array}\right]$$

where A *chooses* i_0, i_1 *such that* $(vk_{i_0}, sk_{i_0}), (vk_{i_1}, sk_{i_1})$ *have been generated by the oracle* $\mathsf{KeyGen}(\rho)$*.*

2.3 Groth-Sahai Proofs in the SXDH Instantiation

The Groth Sahai (GS) proof system is a non-interactive witness indistinguishable proof system (and in some cases also zero-knowledge) for the language of quadratic equations over a bilinear group. The admissible equation types must be in the following form:

$$\sum_{j=1}^{m_y} f(\alpha_j, \mathsf{y}_j) + \sum_{i=1}^{m_x} f(\mathsf{x}_i, \beta_i) + \sum_{i=1}^{m_x}\sum_{j=1}^{m_y} f(\mathsf{x}_i, \gamma_{i,j}\mathsf{y}_j) = t, \tag{1}$$

where $\boldsymbol{\alpha} \in A_1^{m_y}$, $\boldsymbol{\beta} \in A_2^{m_x}$, $\boldsymbol{\Gamma} = (\gamma_{i,j}) \in \mathbb{Z}_q^{m_x \times m_y}$, $t \in A_T$, and $A_1, A_2, A_T \in \{\mathbb{Z}_q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T\}$ are equipped with some bilinear map $f : A_1 \times A_2 \to A_T$.

The GS proof system is a *commit-and-prove* proof system, that is, the prover first commits to solutions of equation (1) using the GS commitments, and then computes a proof that the committed values satisfies equation (1).

GS proofs are perfectly sound when the CRS is sampled from the perfectly binding distribution, and perfectly witness-indistinguishable when sampled from the perfectly hiding distribution. Computational indistinguishability of both distributions implies either perfect soundness and computational witness indistinguishability or computational soundness and perfect witness-indistinguishability.

Further, Belenky et al. noted that Groth-Sahai proofs can be *re-randomized* [1]. This means that, given commitments and proofs showing the satisfiability of some equation, on can compute new proofs which looks exactly as fresh proofs (i.e. computed with fresh randomness) for the same equation, even without knowing the commitment openings nor the randomness. In this work compute such proofs for integer equations $\beta(\beta - 1) = 0$ and $\beta x = y$.

2.4 Groth-Sahai Commitments.

Following Groth and Sahai's work [21], in asymmetric groups and using the SXDH assumption, GS commitments are vectors in $\mathbb{G}_\gamma^2$, $\gamma \in \{1, 2\}$, the form

$$\mathsf{GS.Com}_{ck_\gamma}([x]_\gamma; \boldsymbol{r}) := \begin{pmatrix} [0]_\gamma \\ [x]_\gamma \end{pmatrix} + r_\gamma \left[\boldsymbol{u}_1 - \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right]_\gamma + r_2[\boldsymbol{u}_2]_\gamma$$
$$\mathsf{GS.Com}_{ck_\gamma}(x; \boldsymbol{r}) := x[\boldsymbol{u}_1]_\gamma + r[\boldsymbol{u}_2]_\gamma$$

where $ck_\gamma := [\boldsymbol{u}_1|\boldsymbol{u}_2]_\gamma$, and $\boldsymbol{u}_2$ are sampled from the same distribution as $\mathbf{A}$, the matrix from definition 4. The GS reference string is formed by the commitment keys ck_1, ck_2 and $\boldsymbol{u}_1 := w\boldsymbol{u}_2 + \boldsymbol{e}_2$ in the perfectly binding setting, and $\boldsymbol{u}_1 := w\boldsymbol{u}_2$ in the perfectly hiding setting, for $w \leftarrow \mathbb{Z}_q$.

We define commitments to row vectors as the horizontal concatenation of commitments to each of the coordinates. That is, for $\boldsymbol{x} \in \mathbb{Z}_q^m$ and $\boldsymbol{r} \in \mathbb{Z}_q^m$

$$\mathsf{GS.Com}_{ck_\gamma}(\boldsymbol{x}^\top; \boldsymbol{r}^\top) := [\boldsymbol{u}_1]_\gamma \boldsymbol{x}^\top + [\boldsymbol{u}_2]_\gamma \boldsymbol{r}^\top \in \mathbb{G}_\gamma^{2\times m}.$$

Given a Groth-Sahai commitment $[\boldsymbol{c}]_\gamma$, we will say that $[\boldsymbol{c}']_\gamma$ is a re-randomization of $[\boldsymbol{c}]_\gamma$ if $[\boldsymbol{c}']_\gamma = [\boldsymbol{c}]_\gamma + \mathsf{GS.Com}_{ck_s}(0; \delta)$, for $\delta \leftarrow \mathbb{Z}_q$.

2.5 Boneh-Boyen Signatures

Boneh and Boyen introduced a short signature — each signature consists of only one group element — which is secure against existential forgery under weak chosen message attacks without random oracles [3]. The verification of the validity of any signature-message pair can be written as a set of pairing product equations. Thereby, using Groth-Sahai proofs one can show the possession of a valid signature without revealing the actual signature.

We construct our ring signature using Boneh-Boyen signatures, but we could replace the Boneh-Boyen signature scheme with any structure preserving signature scheme secure under milder assumptions (e.g. [22]). We rather keep it simple and stick to Boneh-Boyen signature which, since the verification key is just one group element, simplifies the notation and reduces the size of the final signature.

Definition 9 (weak Existential Unforgeability (wUF-CMA)). *We say that a signature scheme* $\Sigma = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Ver})$ *is wUF-CMA if for any PPT adversary* A

$$\Pr\left[\begin{array}{l} gk \leftarrow \mathsf{Gen}_a(1^\lambda), (m_1, \ldots, m_{q_{\mathsf{sig}}}) \leftarrow \mathsf{A}(gk), (sk, vk) \leftarrow \mathsf{KGen}(1^\lambda), \\ (m, \sigma) \leftarrow \mathsf{A}(\mathsf{Sign}_{sk}(m_1), \ldots, \mathsf{Sign}_{sk}(m_{q_{\mathsf{sig}}})) : \\ \mathsf{Ver}_{vk}(m, \sigma) = 1 \textit{ and } m \notin \{m_1, \ldots, m_{q_{\mathsf{sig}}}\} \end{array}\right]$$

is negligible in λ.

The Boneh-Boyen signature described bellow is wUF-CMA under the *m-strong Diffie-Hellman* assumption.

$\mathsf{BB.KeyGen}$**:** Given a group key gk, pick $x \leftarrow \mathbb{Z}_q$. The secret/public key pair is defined as $(sk, vk) := (x, [x]_{3-s})$.

$\mathsf{BB.Sign}$**:** Given a secret key $sk \in \mathbb{Z}_q$ and a message $m \in \mathbb{Z}_q$, output the signature $[\sigma]_s := \left[\frac{1}{x+m}\right]_s$. In the unlikely case that $x + m = 0$ we let $[\sigma]_s := [0]_s$.

$\mathsf{BB.Ver}$**:** On input the verification key $[vk]_{3-s}$, a message $m \in \mathbb{Z}_q$, and a signature $[\sigma]_s$, verify that $[m + x]_{3-s}[\sigma]_s = [1]_T$.

It is direct to prove knowledge of a Boneh-Boyen signature for some message m under some committed verification key with a Groth-Sahai proof for the verification equation. In our SXDH based ring signature we need to prove a slightly different statement. Since we have a commitment to the secret key $[\boldsymbol{c}]_2 = \mathsf{Com}_{ck_2}(x; s) = x[\boldsymbol{w}_1]_2 + s[\boldsymbol{w}_2]_2$ we need to show that

$$e([\sigma]_1, m[\boldsymbol{w}_1]_2 + [\boldsymbol{c}]_2) - [\boldsymbol{w}_1]_T = e([\tilde{s}]_1, [w_2]_2), \qquad (2)$$

for some $[\tilde{s}]_1 \in \mathbb{G}_1$.

2.6 Chandran et al.'s Set-Membership Proof

The core of Chandran et al.'s ring signature is a set-membership proof of size $\Theta(\sqrt{n})$ for a set $S \subset \mathbb{G}_\gamma$, $\gamma \in \{1,2\}$, of size n. Assume that $S = \{[s_1]_\gamma, \ldots, [s_n]_\gamma\}$. The proof arranges elements of the set in a matrix of size $m \times m$, where $m := \sqrt{n}$, $[\mathbf{S}]_\gamma := \begin{pmatrix} [s_{1,1}]_\gamma & \cdots & [s_{1,m}]_\gamma \\ \vdots & \ddots & \vdots \\ [s_{m,1}]_\gamma & \cdots & [s_{m,m}]_\gamma, \end{pmatrix}$ where $s_{i,j} := s_{(i-1)m+j}$ for $1 \leq i,j \leq m$.

Let $[s_\alpha]_\gamma$ the element for which the prover wants to show that $[s_\alpha]_\gamma \in S$ and let i_α, j_α such that $s_\alpha = s_{i_\alpha, j_\alpha}$. The prover selects the j_α th column of $[\mathbf{S}]_\gamma$ and then the i_α th element of that column. To do so, the prover commits to

1. $b_1, \ldots, b_m \in \{0,1\}$ such that $b_j = 1$ iff $j = j_\alpha$,
2. $b'_1, \ldots, b'_m \in \{0,1\}$ such that $b'_i = 1$ iff $i = i_\alpha$,
3. $[\kappa_1]_\gamma := [s_{1,j_\alpha}]_\gamma, \ldots, [\kappa_m]_\gamma := [s_{m,j_\alpha}]_\gamma$.

Using Groth-Sahai proofs, the prover proves that

i. $b_1(b_1-1) = 0, \ldots, b_m(b_m-1) = 0, b'_1(b'_m-1) = 0, \ldots, b'_m(b'_m-1) = 0$,
ii. $\sum_{i=1}^m b_i = 1$ and $\sum_{i=1}^m b'_i = 1$,
iii. $[\kappa_1]_\gamma = \sum_{j=1}^m b_j [s_{1,j}]_\gamma, \ldots, [\kappa_m]_\gamma = \sum_{j=1}^m b_j [s_{m,j}]_\gamma$,
iv. $[s_\alpha]_\gamma = \sum_{i=1}^m b'_i [\kappa_i]_\gamma$.

Equations i and ii prove that $(b_1, \ldots, b_m)$ and $(b'_1, \ldots, b'_m)$ are unitary vectors, equation iii proves that $([\kappa_1]_\gamma, \ldots, [\kappa_m]_\gamma)^\top$ is a column of $[\mathbf{S}]_\gamma$, and equation iv proves that $[s_\alpha]_\gamma$ is an element of $([\kappa_1]_\gamma, \ldots, [\kappa_m]_\gamma)$.

In our SXDH based ring signature we need this set-membership to show that some vector $[\boldsymbol{s}]_\gamma$ is the re-randomization of one of the elements of the set of commitments $S = \{[\boldsymbol{s}]_\gamma, \ldots, [\boldsymbol{s}_n]_\gamma\} \subseteq \mathbb{G}_\gamma^2$. That is, there exists some $\delta \in \mathbb{Z}_q$ such that $[\boldsymbol{s}]_\gamma - \mathsf{GS.Com}_{ck_\gamma}(0;\delta) \in S$. The proof remains the same but now the prover computes re-randomizations

3'. $[\boldsymbol{\kappa}_1]_\gamma := [\boldsymbol{s}_{1,j_\alpha}]_\gamma + \mathsf{GS.Com}_{ck_\gamma}(0;\delta_1), \ldots, [\boldsymbol{\kappa}_m]_\gamma := [\boldsymbol{s}_{m,j_\alpha}]_\gamma + \mathsf{GS.Com}_{ck_\gamma}(0;\delta_m)$,

and Groth-Sahai proofs that

iii'. $[\boldsymbol{\kappa}_1]_\gamma - \sum_{j=1}^m b_j [\boldsymbol{s}_{1,j}]_\gamma = \mathsf{GS.Com}_{ck_\gamma}(0;\delta_1), \ldots, [\boldsymbol{\kappa}_m]_\gamma - \sum_{j=1}^m b_j [\boldsymbol{s}_{m,j}]_\gamma = \mathsf{GS.Com}_{ck_\gamma}(0;\delta_m)$,
iv'. $[\boldsymbol{s}]_\gamma - \sum_{i=1}^m b'_i [\boldsymbol{\kappa}_i]_\gamma = \mathsf{GS.Com}_{ck_\gamma}(0;\delta - \delta_{i_\alpha})$.

2.7 Hash Functions

We recall the definition of a hash function plus a weaker notion where the adversary needs to find a second preimage (see [29]). We consider a function $h : \mathcal{K} \times \mathcal{M} \to \mathcal{Y}$ and an algorithm KGen which on input a group key randomly samples an element from $\mathcal{K}$.

Definition 10 (Collision Resistance). *We say that h is a hash-function family with collision resistance if for all PPT adversary* A

$$\mathbf{Adv}_h^{\mathsf{Col}}(\mathsf{A}) := \Pr[k \leftarrow \mathsf{KGen}(1^\lambda), (x, x') \leftarrow \mathsf{A}(k) : x \neq x' \text{ and } h_k(x) = h_k(x')]$$

is negligible in λ.

We use a weaker variant of collision resistance for our hash function based on the PPA assumption.

Definition 11 (Second-Preimage Resistance). *We say that h is a hash-function family with always second-preimage resistance if for all PPT adversary* A

$$\mathbf{Adv}_h^{\mathsf{Sec}}(\mathsf{A}) := \Pr\left[\begin{array}{c} k \leftarrow \mathsf{KGen}(gk), x \leftarrow \mathcal{M}, x' \leftarrow A(k, x) : \\ x \neq x' \text{ and } h_k(x) = h_k(x') \end{array}\right]$$

is negligible in λ.

3 Our Construction in the PPA setting

The high level description of our PPA based ring signature was already given in sect. 1.3. Next we proceed to formally define the hash functions h and g a then we give the formal description and security proof of the protocol.

3.1 The hash functions h and g

We instantiate definition 10 with the function g and 11 with h defined as follows. For h, $\mathcal{M} = Q_m$, $\mathcal{Y} = \mathbb{G}_1^2$, $\mathsf{KGen} = \mathsf{Gen}_a$, and

$$h(A) := \sum_{([\boldsymbol{a}]_1, [\boldsymbol{a}]_2) \in A} [\boldsymbol{a}]_1, \text{ where}$$

$$\mathcal{Q}_m := \{\mathbf{A} \in \mathbb{Z}_q^{2\times m} : A = (\boldsymbol{a}_1 | \cdots | \boldsymbol{a}_m) \text{ and } \boldsymbol{a}_i = (a_{i,1}, a_{i,2})^\top \text{ s.t. } a_{i,2} = a_{i,1}^2\} \text{ and}$$

$$Q_m = \{A : \exists \mathbf{A} \in \mathcal{Q}_m \text{ s.t. } A' = \cup_{i=1}^m ([\boldsymbol{a}_i]_1, [\boldsymbol{a}_i]_2)\}.$$

It might seem odd to define Q_m as sets of vectors in both groups while h only require elements in one group. However, this will be crucial in the security proof of our ring signature, where we need to compute $[vk\boldsymbol{a}]_2$, for some $vk \in \mathbb{Z}_q$, without knowledge of $\boldsymbol{a}$. For simplicity, we may just write $h(A)$ for $A \subseteq \mathbb{G}_1^2$ (which is still well defined).

Given a second preimage h, it is trivial to construct an adversary breaking the m-PPA assumption. Indeed, Let $[\mathbf{A}]_1, [\mathbf{A}]_2$ the challenge of the m-PPA assumption and let A the set of columns of $[\mathbf{A}]_1$ and $[\mathbf{A}]_2$, which is clearly uniformly distributed in Q_m. Then given any $A' \in Q_m$ such that $A' \neq A$ and $h(A) = h(A')$, it holds that $[\mathbf{A}']_1$, the matrix whose columns are the first components of the elements of A', is not a permutation of $[\mathbf{A}]_1$ and hence breaks m-PPA assumption. Then for any adversary A there is an adversary B such that $\mathbf{Adv}^{\mathsf{aPre}_g}(\mathsf{A}) = \mathbf{Adv}_{m\text{-}\mathsf{PPA}}(\mathsf{B})$.

In the case of g, $\mathcal{M} = \mathbb{G}_2^m$, $\mathcal{Y} = \mathbb{G}_2^2$, and $\mathsf{KGen}_{\mathsf{global}}$ picks a group description $gk \leftarrow \mathsf{Gen}_a(1^\lambda)$, while $\mathsf{KGen}_{\mathsf{local}}$ picks $[\boldsymbol{a}]_1 \in \mathbb{G}_1^{2\times m}$, where $\boldsymbol{a} \leftarrow \mathcal{Q}_1$, and the function is defined as

$$g_{[\mathbf{A}]_1}([\boldsymbol{x}]_2) := [\mathbf{A}\boldsymbol{x}]_2.$$

Although not efficiently computable, one can efficiently check if $g_{[\mathbf{A}]_1}([\boldsymbol{x}]_2) = g_{[\mathbf{A}]_1}([\boldsymbol{x}']_2)$ using the pairing operation. Further, in our scheme we will publish values of the form $[\boldsymbol{a}_i x_i]_2$ which will render g efficiently computable.

Given a collision $[\boldsymbol{x}]_2, [\boldsymbol{x}']_2$ for g, then $([\boldsymbol{x}]_2 - [\boldsymbol{x}]_2') \neq [\mathbf{0}]$ is in the kernel of $[\mathbf{A}]_1$. Therefore, is trivial to prove that for any adversary A against static collision resistance there is an adversary B such that $\mathbf{Adv}^{\mathsf{Col}_g}(\mathsf{A}) = \mathbf{Adv}_{\mathcal{Q}_m^\top\text{-}\mathsf{SKerMDH}}(\mathsf{B})$, whenever $\mathbf{A} \leftarrow \mathcal{Q}_m$.

We note that given $A \in Q_m, [\mathbf{A}]_1 \in \mathbb{G}_1^{2\times m}, [\boldsymbol{x}]_2 \in \mathbb{G}_2^m$, $[\boldsymbol{y}]_1 \in \mathbb{G}_2^2$ and $[\boldsymbol{y}']_1 \in \mathbb{G}_2^1$ one can express the statements $A \in Q_m$, $g_{[\mathbf{A}]_1}([\boldsymbol{x}]_2) = [\boldsymbol{y}]_2$, and $h(A) = [\boldsymbol{y}']_1$ as (3),(4), and (5), respectively.

$$\begin{aligned} &e([a_1]_1,[1]_2) = e([1]_1,[b_1]_2) \text{ and} \\ &e([a_2]_1,[1]_2) = e([a_1]_1,[b_1]_2) \text{ for each } ([\boldsymbol{a}]_1,[\boldsymbol{b}]_2) \in A \end{aligned} \tag{3}$$

$$\sum_{j=1}^{m} e([a_{i,j}]_1,[x_i]_1) = e([1]_1,[y_i]_2) \text{ for each } i \in \{1,2\} \tag{4}$$

$$\sum_{([\boldsymbol{a}]_1,[\boldsymbol{a}]_2)\in A} [a_i]_1 = [y_i']_1 \text{ for each } i \in \{1,2\}. \tag{5}$$

Hence, one can compute Groth-Sahai proofs of size $\Theta(m), \Theta(1)$, and $\Theta(1)$, respectively, for the satisfiability of each statement.

Finally, we prove a simple lemma that relates both functions

Lemma 1. *Let $A \leftarrow Q_m, A' \in Q_m, [\boldsymbol{x}]_2, [\boldsymbol{x}']_2 \in \mathbb{G}_2^m$, and $[\mathbf{A}]_1, [\mathbf{A}']_1$ the matrices whose columns are the first component of the elements of A and A', respectively. Then $h(A) = h(A')$ and $g_{[\mathbf{A}]_1}([\boldsymbol{x}]_2) = g_{[\mathbf{A}']_1}([\boldsymbol{x}']_2)$ implies that A' is a second preimage of $h(A)$ or there exists a permutation matrix $\mathbf{P}$ such that $g_{[\mathbf{A}]_1}([\boldsymbol{x}]_2) = g_{[\mathbf{A}]_1}([\mathbf{P}\boldsymbol{x}']_2)$.*

Proof. If $A \neq A'$, then A' is a second preimage of $h(A)$. Else, there is a permutation matrix $\mathbf{P}$ such that $[\mathbf{A}']_1 = [\mathbf{AP}]_1$. Then

$$g_{[\mathbf{A}]_1}([\boldsymbol{x}]_2) = g_{[\mathbf{A}']_1}([\boldsymbol{x}']_2) \Longleftrightarrow g_{[\mathbf{A}]_1}([\boldsymbol{x}]_2) = g_{[\mathbf{AP}]_1}([\boldsymbol{x}']_2) = g_{[\mathbf{A}]_1}([\mathbf{P}\boldsymbol{x}']_2).$$

3.2 Our Ring Signature

In the following let $n := |R|, m := \sqrt[3]{n}$, and for $1 \leq \alpha \leq n$ define $1 \leq \mu \leq n^{2/3}$ and $1 \leq \nu \leq m$ such that $\alpha = (\mu - 1)m + \nu$. For a sequence $\{s\}_{1\leq i\leq n}$ we define $s_{\mu,\nu} := s_{(\mu-1)m+\nu}$. Consider $\mathsf{OT} = (\mathsf{OT.KeyGen}, \mathsf{OT.Sign}, \mathsf{OT.Ver})$ a one-time signature scheme.

$\mathsf{CRSGen}(gk)$**:** Pick a perfectly hiding CRS for the Groth-Sahai proof system $\mathsf{crs}_{\mathsf{GS}}$ and define $(ck_1, ck_2) := \mathsf{crs}_{\mathsf{GS}}$. Note that $\mathsf{crs}_{\mathsf{GS}}$ can be also used for the $\Theta(\sqrt{n})$ set-membership of Chandran et al. The CRS is $\rho := (gk, \mathsf{crs}_{\mathsf{GS}})$.

$\mathsf{KeyGen}(\rho)$**:** Pick $\boldsymbol{a} \leftarrow \mathcal{Q}$ and $(sk, [vk]_2) \leftarrow \mathsf{BB.KeyGen}(gk)$, compute $[\boldsymbol{a}]_1$, $[\boldsymbol{a}]_2$ and then erase $\boldsymbol{a}$ (but if not erased we prove security under the $(\tilde{\ell}, m)$-PPA). The secret key is sk and the extended verification key is $\tilde{vk} := ([vk]_2, [\boldsymbol{a}]_1, [\boldsymbol{a}]_2, \boldsymbol{a}[vk]_2)$.

$\mathsf{Sign}_{\rho,sk}(m, R)$**:** Let α the index of the signer with respect to R.

1. Compute $(sk_{\mathsf{ot}}, vk_{\mathsf{ot}}) \leftarrow \mathsf{OT.KeyGen}(gk)$ and $\sigma_{\mathsf{ot}} \leftarrow \mathsf{OT.Sign}_{sk_{\mathsf{ot}}}(m, R)$.
2. Compute $[\boldsymbol{c}]_2 := \mathsf{GS.Com}_{ck_2}([vk_\alpha]_2; \boldsymbol{r})$, $\boldsymbol{r} \leftarrow \mathbb{Z}_q^2$, $[\sigma]_1 \leftarrow \mathsf{BB.Sign}_{sk_\alpha}(vk_{\mathsf{ot}})$, $[\boldsymbol{d}]_1 := \mathsf{GS.Com}_{ck_1}([\sigma]_1; \boldsymbol{s})$, $\boldsymbol{s} \leftarrow \mathbb{Z}_q^2$, and a GS proof π_{BB} that $\mathsf{BB.Ver}_{[vk]_2}([\sigma]_1, vk_{\mathsf{ot}}) = 1$.
3. For $1 \le i \le n^{2/3}$, let $[\boldsymbol{\kappa}_i]_2 = ([vk_{i,1}]_2, \ldots, [vk_{i,m}]_2)^\top$, $A_i = \{([\boldsymbol{a}_{i,1}]_1, [\boldsymbol{a}_{i,1}]_2), \ldots, ([\boldsymbol{a}_{i,m}]_1, [\boldsymbol{a}_{i,m}]_2)\}$, and $[\mathbf{A}_i]_1 := [\boldsymbol{a}_{i,1}| \cdots |\boldsymbol{a}_{i,m}]_1$. Define the sets $H = \{h(A_1), \ldots, h(A_{n^{2/3}})\}$ and $G = \{g_{[\mathbf{A}_1]_1}([\boldsymbol{\kappa}_1]_2) \ldots, g_{[\mathbf{A}_{n^{2/3}}]_1}([\boldsymbol{\kappa}_{n^{2/3}}]_2)\}$.
4. Let $[\boldsymbol{x}]_1 := h(A_\mu)$ and $[\boldsymbol{y}]_2 = g_{[\mathbf{A}_\mu]_1}([\boldsymbol{\kappa}_\mu]_2)$. Compute GS commitments to $[\boldsymbol{x}]_1$ and $[\boldsymbol{y}]_2$ and compute proofs π_G and π_H that they belong to G and H, respectively. It is also proven that they appear in the same positions reusing the commitments to $b_1, \ldots, b_m$ and $b'_1, \ldots, b'_m$, used in the set-membership proof of Chandran et al., which define $[\boldsymbol{x}]_1$'s and $[\boldsymbol{y}]_2$'s position in H and G respectively.
5. Let $[\boldsymbol{\kappa}']_2 := ([vk_\alpha]_2, [vk_{\mu,1}]_2, \ldots, [vk_{\alpha-1}]_2, [vk_{\alpha+1}]_2, \ldots, [vk_{\mu,m}]_2)^\top \in \mathbb{G}_2^m$, $[\mathbf{A}']_1 := [\boldsymbol{a}_\alpha|\boldsymbol{a}_{\mu,1}| \cdots |\boldsymbol{a}_{\alpha-1}|\boldsymbol{a}_{\alpha+1}| \cdots |\boldsymbol{a}_{\mu,m}]_1 \in \mathbb{G}_1^{2\times m}$ and $A' = \{([\boldsymbol{a}_{\mu,1}]_1, [\boldsymbol{a}_{\mu,1}]_2), \ldots, ([\boldsymbol{a}_{\mu,1}]_1, [\boldsymbol{a}_{\mu,1}]_2)\}$. Compute GS commitments to all but the first element of $[\boldsymbol{\kappa}']_2$ (note that $[\boldsymbol{c}]_2$ is a commitment to the first element of $[\boldsymbol{\kappa}']_2$). Compute also a GS proof π_g that $g_{[\mathbf{A}']_1}([\boldsymbol{\kappa}']_2) = [\boldsymbol{y}]_2$, a GS proof π_h that $h(A') = [\boldsymbol{x}]_1$, and a GS proof π_{Q_m} that $A' \in Q_m$.
6. Return the signature $\boldsymbol{\sigma} := (vk_{\mathsf{ot}}, \sigma_{\mathsf{ot}}, [\boldsymbol{c}]_2, [\boldsymbol{d}]_1, \pi_{\mathsf{BB}}, \pi_G, \pi_H, \pi_g, \pi_h, \pi_{Q_m})$. (GS proofs include commitments to variables).

$\mathsf{Verify}_{\rho,R}(m, \boldsymbol{\sigma})$**:** Verify the validity of the one-time signature and of all the proofs. Return 0 if any of these checks fails and 1 otherwise.

We prove the following theorem which states the security of our construction.

Theorem 1. *The scheme presented in this section is a ring signature scheme with perfect correctness, perfect anonymity and computational unforgeability under the Q_{gen}-permutation pairing assumption, the $\mathcal{Q}^\top_{Q_{\mathsf{gen}}}$-$\mathsf{SKerMDH}$ assumption, the* SXDH *assumption, and the assumption that the one-time signature and the Boneh-Boyen signature are unforgeable. Concretely, for any PPT adversary* A *against the unforgeability of the scheme, there exist adversaries* $\mathsf{B}_1, \mathsf{B}_2, \mathsf{B}_3, \mathsf{B}_4, \mathsf{B}_5$ *such that*

$$\begin{aligned}\mathbf{Adv}(\mathsf{A}) \le & \mathbf{Adv}_{\mathrm{SXDH}}(\mathsf{B}_1) + \mathbf{Adv}_{Q_{\mathsf{gen}}\text{-PPA}}(\mathsf{B}_2) + \mathbf{Adv}_{\mathcal{Q}^\top_{Q_{\mathsf{gen}}}\text{-}\mathsf{SKerMDH}}(\mathsf{B}_3) + \\ & Q_{\mathsf{gen}}(Q_{\mathsf{sign}}\mathbf{Adv}_{\mathsf{OT}}(\mathsf{B}_4) + \mathbf{Adv}_{\mathsf{BB}}(\mathsf{B}_5)),\end{aligned}$$

where Q_{gen} and Q_{sign} are, respectively, upper bounds for the number of queries that A *makes to its* VKGen *and* Sign *oracles.*

Proof. Perfect correctness follows directly from the definitions. Perfect anonymity follows from the fact that the perfectly hiding Groth-Sahai CRS defines perfectly hiding commitments and perfect witness-indistinguishable proofs, information theoretically hiding any information about $\tilde{vk}$.

We say that an unforgeability adversary is "eager" if makes all its queries to the VKGen oracle at the beginning. Note that any non-eager adversary A' can be perfectly simulated by an eager adversary that makes Q_{gen} queries to VKGen and answers A' queries to VKGen "on demand". This is justified by the fact that the output of VKGen is independent of all previous outputs.

W.l.o.g. we assume that A is an eager adversary. Computational unforgeability follows from the indistinguishability of the following games

Game_0: This is the real unforgeability experiment. Game_0 returns 1 if the adversary A produces a valid forgery and 0 if not.

Game_1: This is game exactly as Game_0 with the following differences:
- The Groth-Sahai CRS is sampled together with its discrete logarithms from the perfectly binding distribution. Note that the discrete logarithms of the CRS allow to open the Groth-Sahai commitments.
- At the beginning, variables err_2 and err_3 are initialized to 0 and a random index i^* is chosen from $\{1, \ldots, Q_{\mathsf{gen}}\}$.
- On a query to $\mathsf{Corrupt}$ with argument i, if $i = i^*$ set $\mathsf{err}_3 \leftarrow 1$ and proceed as in Game_0.
- Let (m, R, σ) the purported forgery output by A. If $[vk]_2$, the opening of commitment $[\boldsymbol{c}_{\mu,\nu}]_2$ from σ, is not equal to $[vk_{i^*}]_2$, set $\mathsf{err}_3 \leftarrow 1$. If $[vk]_2 \notin R$, then set $\mathsf{err}_2 = 1$.

Game_2: This is game exactly as Game_1 except that, if err_2 is set to 1, Game_2 aborts.

Game_3: This is game exactly as Game_2 except that, if err_3 is set to 1, Game_3 aborts.

Since in Game_1 variables err_2 and err_3 are just dummy variables, the only difference with Game_0 comes from the Groth-Sahai CRS distribution. It follows that there is an adversary B_1 against SXDH such that $|\Pr[\mathsf{Game}_0 = 1] - \Pr[\mathsf{Game}_1 = 1]| \leq \mathbf{Adv}_{\mathrm{SXDH}}(\mathsf{B}_1)$.

Lemma 2. *There exist adversaries B_2 and B_3 against the Q_{gen}-permutation pairing assumption and against the $\mathcal{Q}_{Q_{\mathsf{gen}}}^{\top}$-$\mathsf{KerMDH}$ assumption, respectively, such that*

$$|\Pr[\mathsf{Game}_2 = 1] - \Pr[\mathsf{Game}_1 = 1]| \leq \mathbf{Adv}_{Q_{\mathsf{gen}}\text{-PPA}}(\mathsf{B}_2) + \mathbf{Adv}_{\mathcal{Q}_{Q_{\mathsf{gen}}}^{\top}\text{-}\mathsf{SKerMDH}}(\mathsf{B}_3).$$

Proof. Note that

$$\begin{aligned}\Pr[\mathsf{Game}_1 = 1] = & \Pr[\mathsf{Game}_1 = 1 | \mathsf{err}_2 = 0] \Pr[\mathsf{err}_2 = 0] + \\ & \Pr[\mathsf{Game}_1 = 1 | \mathsf{err}_2 = 1] \Pr[\mathsf{err}_2 = 1] \\ \leq & \Pr[\mathsf{Game}_2 = 1] + \Pr[\mathsf{Game}_1 = 1 | \mathsf{err}_2 = 0] \\ \Longrightarrow & |\Pr[\mathsf{Game}_2 = 1] - \Pr[\mathsf{Game}_1 = 1]| \leq \Pr[\mathsf{Game}_1 = 1 | \mathsf{err}_2 = 1].\end{aligned}$$

We proceed to bound this last probability constructing two adversaries against collision resistance of g and preimage resistance of h. Let $1 \leq \mu \leq n^{2/3}$ the index defined in π_G and π_S.

Consider an adversary A_h that finds a second preimage of h when $\mathcal{M} = Q_{Q_{\mathsf{gen}}}$. A_h receives as challenge $B \in Q_{Q_{\mathsf{gen}}}$ and honestly simulates Game_1 with the following exception. On the i th query of A to VKGen picks $(sk, [vk]) \leftarrow \mathsf{BB.KeyGen}(1^\lambda)$ and sets $(sk_i, \tilde{vk_i}) := (sk, ([vk]_2, [\boldsymbol{b}_i]_1, [\boldsymbol{b}_i]_2, sk[\boldsymbol{b}_i]_2))$, where $([\boldsymbol{b}_i]_1, [\boldsymbol{b}_i]_2)$ is the i th element of B. When A corrupts the i th party, it returns sk_i but it might also request $\boldsymbol{a}_i$ to its oracle if we are proving security under the (ℓ, m)-PPA assumption. When A outputs and π_{Q_m}, A_h extracts $A' = \{([\boldsymbol{a}'_1]_1, [\boldsymbol{a}'_1]_2), \ldots, ([\boldsymbol{a}'_m]_1, [\boldsymbol{a}'_m]_2\}$ and returns $A' \cup \bar{A}_\mu$, where $\bar{A}_\mu := B \setminus A_\mu$.

Consider another adversary A_g against the collision resistance of g when $\mathcal{M} = \mathbb{G}^{Q_{\mathsf{gen}}}$. B receives as challenge $[\mathbf{B}]_1 \in \mathbb{G}_1^{2\times Q_{\mathsf{gen}}}$ and $[\mathbf{B}]_2 \in \mathbb{G}_2^{2\times Q_{\mathsf{gen}}}$ and honestly simulates Game_1 embedding $[\mathbf{B}]_1, [\mathbf{B}]_2$ in the user keys in the same way as A_h. When A outputs $[\boldsymbol{c}]_2, \mathsf{GS.Com}_{ck_2}([\kappa'_2]_2), \ldots, \mathsf{GS.Com}_{ck_2}([\kappa'_m]_2)$, A_g extracts $[vk], [\kappa'_2], \ldots, [\kappa'_m]$. W.l.o.g. assume that $\mathbf{B} = \mathbf{A}_\mu | \bar{\mathbf{A}}_\mu$, where $\bar{\mathbf{A}}_\mu$ is some matrix whose rows are the discrete logs of the elements of $\bar{A}_\mu$. A_g attempts to extract a permutation matrix $\mathbf{P}$ such that $[\mathbf{A}']_1 = [\mathbf{A}_\mu]_1\mathbf{P}$. If there is no such permutation matrix, then A_g aborts. Else, A_g returns $\begin{pmatrix}[\boldsymbol{\kappa}_\mu]_2\\ [\mathbf{0}]_2\end{pmatrix}, \begin{pmatrix}\mathbf{P}[\boldsymbol{\kappa}']_2\\ [\mathbf{0}]_2\end{pmatrix} \in \mathbb{G}_2^{Q_{\mathsf{gen}}}$, where $[\kappa'_1]$ is the opening of $[\boldsymbol{c}]$.

Perfect soundness of proof π_g (recall that the Groth-Sahai CRS is perfectly binding) implies that

$$g_{[\mathbf{A}']_1}([\boldsymbol{\kappa}']_2) = [\boldsymbol{y}]_2.$$

Perfect soundness of proof π_g and π_{Q_m} implies that

$$h(A') = [\boldsymbol{x}]_1 \text{ and } A' \in Q_m.$$

Given perfect soundness of proofs π_G, π_H, it holds that that

$$\begin{aligned} &g_{[\mathbf{A}']_1}([\boldsymbol{\kappa}']_2) = g_{[\mathbf{A}_\mu]_1}([\boldsymbol{\kappa}_\mu]_2)\\ &h(A') = h(A_\mu). \end{aligned}$$

By Lemma 1 we get that either $A' \neq A_\mu$ is a second preimage for $h(A_\mu)$, thus $A' \cup \bar{A}_\mu \neq B$ and A_h is successful, or there exists a permutation matrix $\mathbf{P}$, which is the one that A_g searches, such that $g_{[\mathbf{A}_\mu]_1}(\mathbf{P}[\boldsymbol{\kappa}']_2) = g_{[\mathbf{A}_\mu]_1}([\boldsymbol{\kappa}_\mu]_2)$. $\mathsf{err}_2 = 1$ implies that $[vk]_2 = [\kappa'_1]_2 \neq [\kappa_{\mu,i}]_2$, for all $1 \leq i \leq m$, and thus $\mathbf{P}[\boldsymbol{\kappa}']_2 \neq [\boldsymbol{\kappa}_\mu]_2$ and, since $[\mathbf{B}]_1 = [\mathbf{A}_\mu|\bar{\mathbf{A}}_\mu]_1$,

$$g_{[\mathbf{A}_\mu]_1}(\mathbf{P}[\boldsymbol{\kappa}']_2) = g_{[\mathbf{B}]_1}\begin{pmatrix}\mathbf{P}[\boldsymbol{\kappa}']_2\\ [\mathbf{0}]_2\end{pmatrix} = g_{[\mathbf{A}_\mu]_1}([\boldsymbol{\kappa}_\mu]_2) = g_{[\mathbf{B}]_1}\begin{pmatrix}[\boldsymbol{\kappa}_\mu]_2\\ [\mathbf{0}]_2\end{pmatrix}$$

and A_g is successful.

As stated in Section 2.7, from A_h we can construct an adversary B_2 that breaks the Q_{gen}-PPA assumption and from A_g we can construct an adversary B_3 that breaks the $\mathcal{Q}_m^\top$-$\mathsf{SKerMDH}$ assumption, with the same advantages. We conclude that

$$\Pr[\mathsf{Game}_1 = 1|\mathsf{err}_2 = 1] \leq \mathbf{Adv}_{Q_{\mathsf{gen}}\text{-PPA}}(\mathsf{B}_2) + \mathbf{Adv}_{\mathcal{Q}_{Q_{\mathsf{gen}}}^\top\text{-}\mathsf{SKerMDH}}(\mathsf{B}_3)$$

Lemma 3.
$$\Pr[\mathsf{Game}_3 = 1] \geq \frac{1}{Q_{\mathsf{gen}}} \Pr[\mathsf{Game}_2 = 1].$$

Proof. It holds that

$$\begin{aligned}\Pr[\mathsf{Game}_3 = 1] &= \Pr[\mathsf{Game}_3 = 1 | \mathsf{err}_3 = 0] \Pr[\mathsf{err}_3 = 0] \\ &= \Pr[\mathsf{Game}_2 = 1 | \mathsf{err}_3 = 0] \Pr[\mathsf{err}_3 = 0] \\ &= \Pr[\mathsf{err}_3 = 0 | \mathsf{Game}_2 = 1] \Pr[\mathsf{Game}_2 = 1].\end{aligned}$$

The probability that $\mathsf{err}_3 = 0$ given $\mathsf{Game}_2 = 1$ is the probability that the Q_{cor} calls to $\mathsf{Corrupt}$ do not abort and that $[vk]_2 = [vk_{i^*}]_2$. Since A is an eager adversary, at the i th call to $\mathsf{Corrupt}$ the index i^* is uniformly distributed over the $Q_{\mathsf{gen}} - i + 1$ indices of uncorrupted users. Similarly, when A outputs its purported forgery, the probability that $[vk]_2 = [vk_{i^*}]_2$ is $1/(Q_{\mathsf{gen}} - Q_{\mathsf{cor}})$, since $[vk]_2 \in R$ (or otherwise Game_2 would have aborted). Therefore

$$\Pr[\mathsf{err}_2 = 1 | \mathsf{Game}_2 = 1] = \frac{Q_{\mathsf{gen}} - 1}{Q_{\mathsf{gen}}} \frac{Q_{\mathsf{gen}} - 2}{Q_{\mathsf{gen}} - 1} \cdots \frac{Q_{\mathsf{gen}} - Q_{\mathsf{cor}}}{Q_{\mathsf{gen}} - Q_{\mathsf{cor}} + 1} \frac{1}{Q_{\mathsf{gen}} - Q_{\mathsf{cor}}} = \frac{1}{Q_{\mathsf{gen}}}.$$

Lemma 4. *There exist adversaries B_4 and B_5 against the unforgeability of the one-time signature scheme and the weak unforgeability of the Boneh-Boyen signature scheme such that*

$$\Pr[\mathsf{Game}_3 = 1] \leq Q_{\mathsf{sig}} \mathbf{Adv}_{\mathsf{OT}}(\mathsf{B}_4) + \mathbf{Adv}_{\mathsf{BB}}(\mathsf{B}_5)$$

Proof. We construct adversaries B_4 and B_5 as follows.

B_4 receives $vk_{\mathsf{ot}}^{\dagger}$ and simulates Game_3 honestly but with the following differences. It chooses a random $j^* \in \{1, \ldots, Q_{\mathsf{sig}}\}$ and answer the j^* th query to $\mathsf{Sign}(i, m^{\dagger}, R^{\dagger})$ honestly but computing $\sigma_{\mathsf{ot}}^{\dagger}$ querying on $(m^{\dagger}, R^{\dagger})$ its oracle and setting $vk_{\mathsf{ot}}^{\dagger}$ as the corresponding one-time verification key. Finally, when A outputs its purported forgery $(m, R, (\sigma_{\mathsf{ot}}, vk_{\mathsf{ot}}, \ldots))$, B_4 outputs the corresponding one-time signature.

B_5 receives $[vk]_2$ and simulates Game_3 honestly but with the following differences. Let $i := 0$. B_5 computes $(sk_{\mathsf{ot}}^i, vk_{\mathsf{ot}}^i) \leftarrow \mathsf{OT.KeyGen}(gk)$, for each $1 \leq i \leq Q_{\mathsf{sig}}$ and queries its signing oracle on $(vk_{\mathsf{ot}}^1, \ldots, vk_{\mathsf{ot}}^{Q_{\mathsf{sig}}})$ obtaining $[\sigma_1]_1, \ldots, [\sigma_{Q_{\mathsf{sig}}}]_1$. On the i^* th query of A to the key generation algorithm, B_5 picks $\boldsymbol{a} \leftarrow \mathcal{Q}$ and outputs $\tilde{vk} := ([vk]_2, [\boldsymbol{a}]_1, [\boldsymbol{a}]_2, \boldsymbol{a}[vk]_2)$. When A queries the signing oracle on input (i^*, m, R), B_5 computes an honest signature but replaces vk_{ot} with vk_{ot}^i and $[\sigma]_1$ with $[\sigma_i]_2$, and then adds 1 to i. Finally, when A outputs its purported forgery $(m, R, (\sigma_{\mathsf{ot}}, vk_{\mathsf{ot}}, [\boldsymbol{c}]_2, [\boldsymbol{d}]_1, \ldots))$, it extracts $[\sigma]_1$ from $[\boldsymbol{d}]_1$ as its forgery for vk_{ot}.

Let E be the event where vk_{ot}, from the purported forgery of A, has been previously output by Sign. We have that

$$\Pr[\mathsf{Game}_3 = 1] \leq \Pr[\mathsf{Game}_3 = 1 | E] + \Pr[\mathsf{Game}_3 = 1 | \neg E].$$

Since (m, R) has never been signed by a one-time signature and that, conditioned on E, the probability of $vk_{\mathsf{ot}} = vk_{\mathsf{ot}}^{\dagger}$ is $1/Q_{\mathsf{sig}}$, then

$$Q_{\mathsf{sig}} \mathbf{Adv}_{\mathsf{OT}}(\mathsf{B}_4) \geq \Pr[\mathsf{Game}_3 = 1 | E]$$

Finally, if $\neg E$ holds, then $[\sigma]$ is a forgery for vk_{ot} and thus

$$\mathbf{Adv}_{\mathsf{BB}}(\mathsf{B}_5) \geq \Pr[\mathsf{Game}_3 = 1 | \neg E]$$

4 Our Construction in the SXDH setting

Our construction follow the high-level description depicted in section 1.3 with the only difference that we do not use the verification key of the Boneh-Boyen signature vk, but a commitment to the secret key x. The only reason is efficiency since in this way we use Groth-Sahai proofs for integer equations instead of equations involving group elements.

For $\boldsymbol{\beta} \in \{0,1\}^m$ we define $h(\boldsymbol{\beta}) := \sum_{i=1}^m \beta_i$ and $g_{\boldsymbol{\beta}}(\boldsymbol{x}) := \sum_{i=1}^m \beta_i x_i$. Unlike the PPA-based construction, we do not prove collision resistance of h or g (g is not collision resistant). Instead, these functions are only used as shorthand and to keep an intuitive link with the PPA-based construction.

In the high level description of our ring signature in the SXDH setting from section 1.3 it was left to show how to derive a proof that $g_{\boldsymbol{\beta}'}(\boldsymbol{x}') = g_{\boldsymbol{\beta}_\mu}(\boldsymbol{x}_\mu)$, which is described in following section.

4.1 NIZK proof that $g_{\boldsymbol{\beta}'}(\boldsymbol{x}') = g_{\boldsymbol{\beta}}(\boldsymbol{x})$

Let $[\mathbf{U}]_1$ and $[\mathbf{W}]_2$ Groth-Sahai commitment keys. Consider $[\boldsymbol{a}_i]_1 = \mathsf{Com}(\beta_i; r_i)$, $[\boldsymbol{c}_i]_2 = \mathsf{Com}_{[\mathbf{W}]_2}(x_i; s)$, and $[\boldsymbol{d}_i] = \mathsf{Com}_{[\mathbf{U}]_1}(y_i; t)$, where $y_i = \beta_i x_i$, $\beta \in \{0,1\}$, $r, s, t \in \mathbb{Z}_q$, and $1 \leq i \leq m$. Consider also $[\boldsymbol{g}]_1$, a re-randomization of $\sum_{i=1}^m [\boldsymbol{d}_i]_1 = \mathsf{Com}(g_{\boldsymbol{\beta}}(\boldsymbol{x}))$, and $[\mathbf{A}']_1$ and $[\mathbf{C}']_2$ permutations of re-randomizations of $[\mathbf{A}]_1 := ([\boldsymbol{a}_1] | \cdots | [\boldsymbol{a}_m])$ and $[\mathbf{C}]_2 := ([\boldsymbol{c}_1]_2 | \cdots | [\boldsymbol{c}_m]_2)$, respectively. We want to construct a proof that $g_{\boldsymbol{\beta}'}(\boldsymbol{x}') = g_{\boldsymbol{\beta}}(\boldsymbol{x})$, or equivalently $\sum_{i=1}^m \beta_i' x_i' = \sum_{i=1}^m \beta_i x_i$, only from the extended verification keys and the random coins used in the re-randomizations.

Apart from $[\boldsymbol{a}_i]_1, [\boldsymbol{c}_i]_2, [\boldsymbol{d}_i]_1$, the extended verification key contains Groth-Sahai proofs $[\boldsymbol{\psi}_i]_2, [\boldsymbol{\omega}_i]_1$ for the equation $\beta_i x_i = y_i$. Each of these proofs satisfy the verification equation

$$[\boldsymbol{a}_i]_1 [\boldsymbol{c}_i^\top]_2 - [\boldsymbol{d}_i]_1 [\boldsymbol{w}_1^\top]_2 = [\boldsymbol{u}_2]_1 [\boldsymbol{\psi}_i^\top]_2 + [\boldsymbol{\omega}_i]_1 [\boldsymbol{w}_2^\top]_2.$$

$[\mathbf{A}']_1$, $[\mathbf{C}']_2$ and $[\boldsymbol{g}]_1$ are computed as $[\mathbf{A}']_1 = [\mathbf{A}]_1 \mathbf{P} + [\boldsymbol{u}_2]_1 \boldsymbol{\delta}_a^\top$, $[\mathbf{C}']_2 = [\mathbf{C}]_2 \mathbf{P} + [\boldsymbol{w}_2]_2 \boldsymbol{\delta}_c^\top$, and $[\boldsymbol{g}]_1 = \sum_{i=1}^m [\boldsymbol{d}_i]_1 + [\boldsymbol{u}_2]_1 \delta_g$, where $\mathbf{P}$ is a permutation matrix and $\boldsymbol{\delta}_a, \boldsymbol{\delta}_c \in \mathbb{Z}_q^m$ and $\delta_g \in \mathbb{Z}_q$. The right side of the verification equation for equation $\sum_{i=1}^m \beta_i' x_i' - y = 0$, where $y = \sum_{i=1}^n \beta_i x_i$ is the opening of $[\boldsymbol{d}']_1$ and

$\boldsymbol{\beta}', \boldsymbol{x}'$ are the openings of $[\mathbf{A}']_1$ and $[\mathbf{C}']_2$ respectively, is equal to

$$\begin{aligned}
&[\mathbf{A}']_1[\mathbf{C}'^{\top}]_2 - [\boldsymbol{d}']_1[\boldsymbol{w}_1^{\top}]_2 \\
&= [\mathbf{A}]_1\mathbf{P}\mathbf{P}^{\top}[\mathbf{C}^{\top}]_2 + [\mathbf{A}]_1\mathbf{P}\boldsymbol{\delta}_c[\boldsymbol{w}_2^{\top}]_2 + [\boldsymbol{u}_2]_1\boldsymbol{\delta}_a^{\top}[\mathbf{C}'^{\top}]_2 - [\boldsymbol{d}']_1[\boldsymbol{w}_2^{\top}]_2 \\
&= \sum_{i=1}^{m}([\boldsymbol{a}_i]_1[\boldsymbol{c}_i^{\top}]_2 - [\boldsymbol{d}_i]_1[\boldsymbol{w}_1^{\top}]) + [\mathbf{A}]_1\mathbf{P}\boldsymbol{\delta}_c[\boldsymbol{w}_2^{\top}]_2 + [\boldsymbol{u}_2]_1(\boldsymbol{\delta}_a^{\top}[\mathbf{C}'^{\top}]_2 - \delta_g[\boldsymbol{w}_1^{\top}]_2) \\
&= [\boldsymbol{u}_2]_1\left(\sum_{i=1}^{m}[\boldsymbol{\psi}_i]_1 + [\mathbf{C}']_2\boldsymbol{\delta}_a - \delta_g[\boldsymbol{w}_1]_2\right)^{\top} + \left(\sum_{i=1}^{m}[\boldsymbol{\omega}_i]_1 + [\mathbf{A}]_1\mathbf{P}\boldsymbol{\delta}_c\right)[\boldsymbol{w}_2^{\top}]_2.
\end{aligned}$$

The last equation indicates that the proof must be the terms multiplying $[\boldsymbol{u}_2]_1$ and $[\boldsymbol{w}_2^{\top}]_2$ plus randomization terms. That is, for $\xi \leftarrow \mathbb{Z}_q$

$$\begin{aligned}
[\boldsymbol{\psi}']_2 &= \sum_{i=1}^{m}[\boldsymbol{\psi}_i]_1 + [\mathbf{C}']_2\boldsymbol{\delta}_a - \delta_g[\boldsymbol{w}_1]_2 + \xi[\boldsymbol{w}_2]_2 \\
[\boldsymbol{\omega}']_1 &= \sum_{i=1}^{m}[\boldsymbol{\omega}_i]_1 + [\mathbf{A}]_1\mathbf{P}\boldsymbol{\delta}_c - \xi[\boldsymbol{u}_2]_1. \qquad (6)
\end{aligned}$$

Assuming $[\boldsymbol{d}']_1$ is correctly computed, the proof is sound because it satisfy the Groth-Sahai verification equation for $\sum_{i=1}^{m}\beta_i'x_i' - \sum_{i=1}^{m}\beta_i x_i = 0$. Furthermore, the proof is uniformly distributed conditioned on satisfying the verification equation and thus follows exactly the same distribution as a fresh Groth-Sahai proof.

4.2 Our Ring Signature

In the following let $n := |R|, m := \sqrt[3]{n}$, and for $1 \leq \alpha \leq n$ define $1 \leq \mu \leq n^{2/3}$ and $1 \leq \nu \leq m$ such that $\alpha = (\mu - 1)m + \nu$. For a sequence $\{s\}_{1\leq i\leq n}$ we define $s_{\mu,\nu} := s_{(\mu-1)m+\nu}$. Consider $\mathsf{OT} = (\mathsf{OT.KeyGen}, \mathsf{OT.Sign}, \mathsf{OT.Ver})$ a one-time signature scheme. We assume that ring descriptions don't contain repeated elements.

$\mathsf{CRSGen}(gk)$**:** Pick three perfectly hiding CRS for the Groth-Sahai proof system ck_1, ck_2, ck_2', where $ck_1 := [\mathbf{U}]_1, ck_2 := [\mathbf{V}]_2, ck_2' := [\mathbf{W}]_2$. We use ck_1, ck_2 for the $\Theta(\sqrt{n})$ set-membership of Chandran et al. The CRS is $\rho := (gk, ck_1, ck_2, ck_2')$.

$\mathsf{KeyGen}(\rho)$**:** Pick $(x, [x]_2) \leftarrow \mathsf{BB.KeyGen}(gk)$, compute $[\boldsymbol{a}]_1 := \mathsf{Com}_{[\mathbf{U}]_1}(\beta = 0; r)$, where $r \leftarrow \mathbb{Z}_q$, plus a Groth-Sahai proof π that $\beta(\beta - 1) = 0$. Compute also $[\boldsymbol{c}]_2 = \mathsf{GS.Com}_{ck_2'}(x; s), [\boldsymbol{d}]_1 := \mathsf{GS.Com}_{ck_1}(y; t)$, where $s, t \leftarrow \mathbb{Z}_q$, and a proof $[\boldsymbol{\psi}]_2, [\boldsymbol{\omega}]_1$ that $\beta x = y$. The secret key is x and the extended verification key is $\widetilde{vk} := ([x]_2, [\boldsymbol{a}]_1, [\boldsymbol{c}]_2, [\boldsymbol{d}]_1, \pi, [\boldsymbol{\psi}]_2, [\boldsymbol{\omega}]_1)$.

$\mathsf{Sign}_{\rho,x}(m, R)$**:** Let $\alpha = (\mu - 1)m + \nu$ the index of the signer with respect to R.

1. Compute $(sk_{\mathsf{ot}}, vk_{\mathsf{ot}}) \leftarrow \mathsf{OT.KeyGen}(gk)$ and $\sigma_{\mathsf{ot}} \leftarrow \mathsf{OT.Sign}_{sk_{\mathsf{ot}}}(m, R)$.

2. For $1 \le i \le n^{2/3}$, let $[\mathbf{A}_i]_1 := [\boldsymbol{a}_{i,1}|\dots|\boldsymbol{a}_{i,m}]_1$, $[\boldsymbol{h}_i]_1 := \sum_{j=1}^m [\boldsymbol{a}_{i,j}]_1$ and $[\boldsymbol{g}_i]_1 := \sum_{j=1}^m [\boldsymbol{d}_{i,j}]_1$. Define the sets $H = \{[\boldsymbol{h}_1]_2, \dots, [\boldsymbol{h}_{n^{2/3}}]_2\}$ and $G = \{[\boldsymbol{g}_1]_2 \dots, [\boldsymbol{g}_{n^{2/3}}]_2\}$.
3. Let $[\boldsymbol{h}]_1 := [\boldsymbol{h}_\mu] + \delta_h[\boldsymbol{u}_1]_1$ and $[\boldsymbol{g}]_1 = [\boldsymbol{g}_\mu]_1 + \delta_g[\boldsymbol{u}_2]_1$, $\delta_g, \delta_h \leftarrow \mathbb{Z}_q$. Compute proofs π_G and π_H that they belong to G and H, respectively. It is also proven that they appear in the same positions reusing the commitments to $b_1, \dots, b_m$ and $b'_1, \dots, b'_m$, used in the set-membership proof of Chandran et al., which define $[\boldsymbol{h}]_1$'s and $[\boldsymbol{g}]_2$'s positions in H and G respectively.
4. Let $[\mathbf{C}']_2 := [\boldsymbol{c}_{\mu,\nu}|\boldsymbol{c}_{\mu,1}|\cdots|\boldsymbol{c}_{\mu,m}]_2 + [\boldsymbol{w}_2]_2\boldsymbol{\delta}_c^\top$ and $[\mathbf{A}']_1 := [\boldsymbol{a}_{\mu,\nu}|\boldsymbol{a}_{\mu,1}|\cdots|\boldsymbol{a}_{\mu,m}]_1 + [\boldsymbol{u}_2]_1\boldsymbol{\delta}_a^\top \in \mathbb{G}_1^{2\times m}$, where $\boldsymbol{\delta}_a, \boldsymbol{\delta}_c \leftarrow \mathbb{Z}_q^m$ (the ν-th row is moved to the front of each matrix). Use $[\mathbf{A}_\mu]_1, [\mathbf{C}']_2$, $\mathbf{P}$ the permutation matrix that swaps the first element with the ν-th element, and $[\boldsymbol{\psi}_{\mu,i}]_2, [\boldsymbol{\omega}_{\mu,i}]_1$ plus $\boldsymbol{\delta}_a, \boldsymbol{\delta}_c, \delta_g$ to derive $\pi_g = ([\boldsymbol{\psi}']_2, [\boldsymbol{\omega}']_1)$, a proof that $g_{\boldsymbol{\beta}'}(\boldsymbol{x}') = g_{\boldsymbol{\beta}}(\boldsymbol{x})$, as in equation (6).
5. Compute a proof π_h that $h(\boldsymbol{\beta}') = h(\boldsymbol{\beta}_\mu)$ as the GS proof that $\sum_{i=1}^m [\boldsymbol{a}'_i]_1 - [\boldsymbol{h}]_1 = \tilde{\delta}_h[\boldsymbol{u}_2]$, where $\tilde{\delta}_h = \sum_{i=1}^m \delta_{a,i} - \delta_h$.
6. Compute a GS proof π_{bits} that $\boldsymbol{\beta}'$, the vector of openings of $\mathbf{A}'$, belongs to $\{0,1\}^m$ re-randomizing proofs $\pi_{\mu,\nu}, \pi_{\mu,1}, \dots, \pi_{\mu,m}$.
7. Compute $[\sigma]_1 \leftarrow \mathsf{BB.Sign}_{x_{\mu,\nu}}(vk_{\mathsf{ot}})$, $[\boldsymbol{f}]_1 \leftarrow \mathsf{GS.Com}_{ck_1}([\sigma]_1)$, and a GS proof π_{BB} of satisfiability of equation (2) with $[\boldsymbol{c}_{\mu,\nu}]_2$ the commitment to the secret key.
8. Return the signature $\boldsymbol{\sigma} := (vk_{\mathsf{ot}}, \sigma_{\mathsf{ot}}, [\boldsymbol{f}]_1, [\mathbf{A}']_2, [\mathbf{C}']_2, [\boldsymbol{g}]_1, [\boldsymbol{h}]_1, \pi_G, \pi_H, \pi_g, \pi_h, \pi_{\mathsf{bits}}, \pi_{\mathsf{BB}})$. (GS proofs include commitments to variables).

$\mathsf{Verify}_{\rho,R}(m, \boldsymbol{\sigma})$: Verify the validity of the one-time signature and of all the proofs. Return 0 if any of these checks fails and 1 otherwise.

We prove the following theorem which states the security of our construction.

Theorem 2. *The scheme presented in this section is a ring signature scheme with perfect correctness, perfect anonymity and computational unforgeability under the* SXDH *assumption, and the assumption that the one-time signature and the Boneh-Boyen signature are unforgeable. Concretely, for any PPT adversary* A *against the unforgeability of the scheme, there exist adversaries* $\mathsf{B}_1, \mathsf{B}_2, \mathsf{B}_3$ *such that*

$$\mathbf{Adv}(\mathsf{A}) \le (Q_{\mathsf{gen}}^2 + 1)\mathbf{Adv}_{\mathrm{SXDH}}(\mathsf{B}_1) + Q_{\mathsf{gen}}Q_{\mathsf{sig}}\mathbf{Adv}_{\mathsf{OT}}(\mathsf{B}_2) + Q_{\mathsf{gen}}\mathbf{Adv}_{\mathsf{BB}}(\mathsf{B}_3),$$

where Q_{gen} *and* Q_{sign} *are, respectively, upper bounds for the number of queries that* A *makes to its* VKGen *and* Sign *oracles.*

Proof. Perfect correctness follows directly from the definitions. Perfect anonymity follows from the fact that the perfectly hiding Groth-Sahai commitment keys defines perfectly hiding commitments and perfect witness-indistinguishable proofs, information theoretically hiding any information about $\widetilde{vk}$ and x. Further, the re-randomized commitments are random elements $\mathbb{G}_2^1$ or $\mathbb{G}_2^2$, and hence independent of the original commitments, and the re-randomized proofs follows the same distribution of the honest proofs and hence, they don't reveal any information about $\widetilde{vk}$ and x.

We say that an unforgeability adversary is "eager" if makes all its queries to the VKGen oracle at the beginning. Note that any non-eager adversary A' can be perfectly simulated by an eager adversary that makes Q_{gen} queries to VKGen and answers A' queries to VKGen "on demand". This is justified by the fact that the output of VKGen is independent of all previous outputs.

W.l.o.g. we assume that A is an eager adversary. Computational unforgeability follows from the indistinguishability of the following games

Game_0: This is the real unforgeability experiment. Game_0 returns 1 if the adversary A produces a valid forgery and 0 if not.

Game_1: This is game exactly as Game_0 with the following differences:

- The commitment key ck_2' is sampled together with its discrete logarithms from the perfectly binding distribution. Note that the discrete logarithms of ck_2' allow to open commitments $[\boldsymbol{c}_i]_2$ and $[\boldsymbol{c}_j]_2$ for $i \in [Q_{\mathsf{gen}}]$ and $j \in [m]$.
- At the beginning, variables $\mathsf{err}_1, \mathsf{err}_2$, err_3 and err_4 are initialized to 0 and random index i^* from $\{1, \ldots, Q_{\mathsf{gen}}\}$ is chosen.
- On a query to $\mathsf{Corrupt}$ with argument i, if $i = i^*$ set $\mathsf{err}_3 \leftarrow 1$.
- Let (m, R, σ) the purported forgery output by A.
  * If $[x]_2 \notin R$, then set $\mathsf{err}_1 = 1$.
  * If $i^* \neq (m-1)\mu + i$ for all $i \in [m]$, where μ is the index defined in π_G and π_H, or there is some $j \in [m]$ such that $[x_{i^*}]_2 = [x_j']_2$, then set $\mathsf{err}_2 \leftarrow 1$.
  * If $[x_1']_2$, the opening of commitment $[\boldsymbol{c}_1']_2$ from σ, is not equal to $[x_{i^*}]_2$, set $\mathsf{err}_4 \leftarrow 1$.

Game_2: This is game exactly as Game_1 except that, if err_1 is set to 1, Game_2 aborts.

$\mathsf{Game}_{2,1}$: This game is exactly as Game_1 except that, if at the onset $\mathsf{err}_1 = 0$ or $\mathsf{err}_2 = 1$, $\mathsf{Game}_{2,1}$ aborts.

$\mathsf{Game}_{2,2}$: This game is exactly as $\mathsf{Game}_{2,1}$ except that in the i^*th query to VKGen commitment $[\boldsymbol{a}_{i^*}]_1$ is set to $\mathsf{Com}_{[\mathbf{U}]_1}(\beta_{i^*} = 1; r_{i^*})$, $r_{i^*} \leftarrow \mathbb{Z}_q$. Additionally, if err_3 is set to 1 abort.

$\mathsf{Game}_{2,3}$: This game is exactly as $\mathsf{Game}_{2,2}$ except that ck_1 and ck_2 are sampled from the perfectly binding distribution.

Game_3: This is game exactly as Game_2 except that, if err_3 or err_4 are set to 1, Game_3 aborts.

Game_4: This is game exactly as Game_3 except that, if err_3 is set to 1, Game_4 aborts.

Since in Game_1 variables $\mathsf{err}_1, \mathsf{err}_2$ and err_3 are just dummy variables, the only difference with Game_0 comes from ck_2' distribution. Similarly, the only difference between $\mathsf{Game}_{2,2}$ and $\mathsf{Game}_{2,3}$ comes from ck_1 and ck_2 distribution. It follows that there an adversaries $\mathsf{B}_1, \mathsf{B}_2$ against SXDH such that $|\Pr[\mathsf{Game}_0 = 1] - \Pr[\mathsf{Game}_1 = 1]| \leq \mathbf{Adv}_{\mathrm{SXDH}}(\mathsf{B}_1)$ and $|\Pr[\mathsf{Game}_{2,2} = 1] - \Pr[\mathsf{Game}_{2,3} = 1]| \leq \mathbf{Adv}_{\mathrm{SXDH}}(\mathsf{B}_2)$.

Lemma 5.

$$\Pr[\mathsf{Game}_1 = 1] \leq \Pr[\mathsf{Game}_2 = 1] + Q_{\mathsf{gen}} \Pr[\mathsf{Game}_{2,1} = 1]$$

Proof.

$$\begin{aligned}\Pr[\mathsf{Game}_1 = 1] =& \Pr[\mathsf{Game}_1 = 1 | \mathsf{err}_1 = 0] \Pr[\mathsf{err}_1 = 0] + \\ & \Pr[\mathsf{Game}_1 = 1 | \mathsf{err}_1 = 1] \Pr[\mathsf{err}_1 = 1] \\ \leq & \Pr[\mathsf{Game}_2 = 1] + \Pr[\mathsf{Game}_1 = 1 | \mathsf{err}_1 = 1] \Pr[\mathsf{err}_1 = 1]\end{aligned}$$

Now we proceed to bound $\Pr[\mathsf{Game}_1 = 1 | \mathsf{err}_1 = 1] \Pr[\mathsf{err}_1 = 1]$. It holds that

$$\begin{aligned}\Pr[\mathsf{Game}_{2,1} = 1] &= \Pr[\mathsf{Game}_1 = 1, \mathsf{err}_1 = 1, \mathsf{err}_2 = 0] \\ &= \Pr[\mathsf{err}_2 = 0 | \mathsf{Game}_1 = 1, \mathsf{err}_1 = 1] \Pr[\mathsf{Game}_1 = 1, \mathsf{err}_1 = 1] \\ &\geq \frac{1}{Q_{\mathsf{gen}}} \Pr[\mathsf{Game}_1 = 1 | \mathsf{err}_1 = 1] \Pr[\mathsf{err}_1 = 1].\end{aligned}$$

where the last inequality follows from the fact that $\mathsf{err}_1 = 1$ implies that $[x'_1]_2 \notin R$ and then $x'_i \neq x_{\mu,k}$ for all $k \in [m]$. Given that all entries of $\boldsymbol{x}_\mu$ must be different, there is least one $j \in [m]$ such that $x_{\mu,j} \neq x'_k$ for all $k \in [m]$. Since j^* is completely hidden to the adversary, it follows that $\Pr[\mathsf{err}_2 = 0 | \mathsf{Game}_1 = 1, \mathsf{err}_1 = 1] \geq \Pr[j^* = (m-1)\mu + j] = 1/Q_{\mathsf{gen}}$.

Lemma 6. $\Pr[\mathsf{Game}_{2,1} = 1] \leq Q_{\mathsf{gen}} \Pr[\mathsf{Game}_{2,2} = 1]$

Proof. Since ck_1 and ck_2 are perfectly hiding there is no information revealed about $\boldsymbol{\beta}$ through the extended verification keys or the signatures. Then, it holds that $\Pr[\mathsf{Game}_{2,2} = 1] = \Pr[\mathsf{err}_3 = 0 | \mathsf{Game}_{2,1} = 1] \Pr[\mathsf{Game}_{2,1} = 1]$ and $\Pr[\mathsf{err}_3 = 0 | \mathsf{Game}_{2,1} = 1]$ is the probability that the Q_{corr} calls to $\mathsf{Corrupt}$ do not abort. Since A is an eager adversary, the probability that i^* doesn't hit any of the Q_{corr} corrupted users is $(Q_{\mathsf{gen}} - Q_{\mathsf{corr}})/Q_{\mathsf{gen}} \geq 1/Q_{\mathsf{gen}}$ and then $\Pr[\mathsf{Game}_{2,2} = 1] \geq 1/Q_{\mathsf{gen}} \Pr[\mathsf{Game}_{2,1} = 1]$.

Lemma 7. $\Pr[\mathsf{Game}_{2,3} = 1] = 0$

Proof. Since ck_1, ck_2 and ck'_2 are perfectly binding, all Groth-Sahai proofs are perfectly sound. If π_{bits} and π_h are valid proofs, then $\boldsymbol{\beta}'$, the opening of $[\mathbf{A}']$, is a permutation of $\boldsymbol{\beta}_\mu$. Since $\mathsf{err}_1 = 1$ and $\mathsf{err}_2 = 0$, it holds that $x_{i^*} = x_{\mu,i^*_\mu}$, for some $i^*_\mu \in [m]$, and $x_{\mu,i^*} \neq x'_j$ for all j. Furthermore, since $\beta_{i^*} = \beta_{\mu,i^*_\mu} = 1$, then $\beta_{j^*} = 1$ for some unique $j^* \in [m]$.

Finally, equation $\sum_{i=1}^m \beta'_i x'_i = \sum_{i=1}^m \beta_{\mu,i} x_{\mu,i}$ becomes $x'_{j^*} = x_{\mu,i^*_\mu}$, and therefore can't be satisfied. We conclude that $\pi_{\mathsf{bits}}, \pi_h$, and π_g can't be valid proofs simultaneously and thus $\Pr[\mathsf{Game}_{2,3} = 1] = 0$.

Lemma 8.

$$\Pr[\mathsf{Game}_2 = 1] \leq Q_{\mathsf{gen}} \Pr[\mathsf{Game}_3 = 1].$$

Proof. It holds that

$$\begin{aligned}\Pr[\mathsf{Game}_3 = 1] &= \Pr[\mathsf{Game}_3 = 1 | \mathsf{err}_3 = 0, \mathsf{err}_4 = 0] \Pr[\mathsf{err}_3 = 0, \mathsf{err}_4 = 0] \\ &= \Pr[\mathsf{Game}_2 = 1 | \mathsf{err}_3 = 0, \mathsf{err}_4 = 0] \Pr[\mathsf{err}_3 = 0, \mathsf{err}_4 = 1] \\ &= \Pr[\mathsf{err}_3 = 0, \mathsf{err}_4 = 0 | \mathsf{Game}_2 = 1] \Pr[\mathsf{Game}_2 = 1].\end{aligned}$$

The probability that $\mathsf{err}_3 = 0$ and $\mathsf{err}_4 = 0$ given $\mathsf{Game}_3 = 1$ is the probability that the Q_{corr} calls to $\mathsf{Corrupt}$ do not abort and that $[x'_1]_2 = [x_{i^*}]_2$. Since A is an eager adversary, the probability that i^* doesn't hit any of the Q_{corr} corrupted users is $Q_{\mathsf{gen}} - Q_{\mathsf{corr}}/Q_{\mathsf{gen}}$. Similarly, when A outputs its purported forgery, the probability that $[x'_1]_2 = [x_{i^*}]_2$ is $1/(Q_{\mathsf{gen}} - Q_{\mathsf{corr}})$, since $[x'_1]_2 \in R$ (or otherwise Game_3 would have aborted). Therefore

$$\Pr[\mathsf{err}_3 = 0, \mathsf{err}_4 = 0 | \mathsf{Game}_2 = 1] = \frac{Q_{\mathsf{gen}} - Q_{\mathsf{corr}}}{Q_{\mathsf{gen}}} \frac{1}{Q_{\mathsf{gen}} - Q_{\mathsf{corr}}} = \frac{1}{Q_{\mathsf{gen}}}.$$

Lemma 9. *There exist adversaries* B_3 *and* B_4 *against the unforgeability of the one-time signature scheme and the weak unforgeability of the Boneh-Boyen signature scheme such that*

$$\Pr[\mathsf{Game}_3 = 1] \leq Q_{\mathsf{sig}} \mathbf{Adv}_{\mathsf{OT}}(\mathsf{B}_3) + \mathbf{Adv}_{\mathsf{BB}}(\mathsf{B}_4)$$

Proof. We construct adversaries B_3 and B_4 as follows.

B_3 receives $vk^{\dagger}_{\mathsf{ot}}$ and simulates Game_3 honestly but with the following differences. It chooses a random $j^* \in \{1, \ldots, Q_{\mathsf{sig}}\}$ and answer the j^* th query to $\mathsf{Sign}(i, m^{\dagger}, R^{\dagger})$ honestly but computing $\sigma^{\dagger}_{\mathsf{ot}}$ querying on $(m^{\dagger}, R^{\dagger})$ its oracle and setting $vk^{\dagger}_{\mathsf{ot}}$ as the corresponding one-time verification key. Finally, when A outputs its purported forgery $(m, R, (\sigma_{\mathsf{ot}}, vk_{\mathsf{ot}}, \ldots))$, B_3 outputs the corresponding one-time signature.

B_4 receives $[x]_2$ and simulates Game_3 honestly but with the following differences. Let $i := 0$. B_4 computes $(sk^i_{\mathsf{ot}}, vk^i_{\mathsf{ot}}) \leftarrow \mathsf{OT.KeyGen}(gk)$, for each $1 \leq i \leq Q_{\mathsf{sig}}$ and queries its signing oracle on $(vk^1_{\mathsf{ot}}, \ldots, vk^{q_{\mathsf{sig}}}_{\mathsf{ot}})$ obtaining $[\sigma_1]_1, \ldots, [\sigma_{Q_{\mathsf{sig}}}]_1$. On the i^* th query of A to the key generation algorithm, B_4 it computes $[\boldsymbol{a}]_1 := \beta[\boldsymbol{u}_1]_1 + r[\boldsymbol{u}_2]$, for $\beta = 0$, $[\boldsymbol{c}]_2 = [x]_2 \boldsymbol{w}_1 + s[\boldsymbol{w}_2]_2$ and $[\boldsymbol{d}]_1 = y[\boldsymbol{u}_1]_1 + t[\boldsymbol{u}_2]_1$ and $[\boldsymbol{\psi}]_2, [\boldsymbol{\omega}]_1$ as a Groth-Sahai proof for equation $\beta x = y$, for $\beta = y = 0$. The proof π_{bits} that $\boldsymbol{\beta} \in \{0, 1\}$ is honestly computed and A outputs $\boldsymbol{vk} := ([x]_2, [\boldsymbol{a}]_1, [\boldsymbol{c}]_2, [\boldsymbol{d}]_1, [\boldsymbol{\psi}]_2, [\boldsymbol{\omega}]_1, \pi)$. When A queries the signing oracle on input (i^*, m, R), B_4 computes an honest signature but replaces vk_{ot} with vk^i_{ot} and $[\sigma]_1$ with $[\sigma_i]_2$, and then adds 1 to i. Finally, when A outputs its purported forgery $(m, R, (\sigma_{\mathsf{ot}}, vk_{\mathsf{ot}}, [\boldsymbol{f}]_2, [\mathbf{A}']_1, \ldots))$, it extracts $[\sigma]_1$ from $[\boldsymbol{f}]_1$ as its forgery for vk_{ot}.

Let E be the event where vk_{ot}, from the purported forgery of A, has been previously output by Sign. We have that

$$\Pr[\mathsf{Game}_4 = 1] \leq \Pr[\mathsf{Game}_4 = 1 | E] + \Pr[\mathsf{Game}_4 = 1 | \neg E].$$

Since (m, R) has never been signed by a one-time signature and that, conditioned on E, the probability of $vk_{\mathsf{ot}} = vk^{\dagger}_{\mathsf{ot}}$ is $1/Q_{\mathsf{sig}}$, then

$$Q_{\mathsf{sig}} \mathbf{Adv}_{\mathsf{OT}}(\mathsf{B}_4) \geq \Pr[\mathsf{Game}_4 = 1 | E]$$

Finally, if $\neg E$ holds, then $[\sigma]_1$ is a forgery for vk_{ot} and thus

$$\mathbf{Adv}_{\mathsf{BB}}(\mathsf{B}_4) \geq \Pr[\mathsf{Game}_4 = 1 | \neg E].$$

5 Acknowledgments

We thank to the anonymous reviewers for the constructive feedback. It was very useful for simplifying the SXDH-based construction. We also thanks Carla Ràfols and Mojtaba Khalili for their comments on earlier versions of this work. This work was funded in part by the French ANR ALAMBIC project (ANR-16-CE39-0006).

References

1. M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham. Randomizable proofs and delegatable anonymous credentials. In S. Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 108–125, Santa Barbara, CA, USA, Aug. 16–20, 2009. Springer, Heidelberg, Germany.
2. A. Bender, J. Katz, and R. Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In S. Halevi and T. Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 60–79, New York, NY, USA, Mar. 4–7, 2006. Springer, Heidelberg, Germany.
3. D. Boneh and X. Boyen. Short signatures without random oracles. In C. Cachin and J. Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 56–73, Interlaken, Switzerland, May 2–6, 2004. Springer, Heidelberg, Germany.
4. P. Bose, D. Das, and C. P. Rangan. Constant size ring signature without random oracle. In E. Foo and D. Stebila, editors, *ACISP 15*, volume 9144 of *LNCS*, pages 230–247, Brisbane, QLD, Australia, June 29 – July 1, 2015. Springer, Heidelberg, Germany.
5. N. Chandran, J. Groth, and A. Sahai. Ring signatures of sub-linear size without random oracles. In L. Arge, C. Cachin, T. Jurdzinski, and A. Tarlecki, editors, *ICALP 2007*, volume 4596 of *LNCS*, pages 423–434, Wroclaw, Poland, July 9–13, 2007. Springer, Heidelberg, Germany.
6. M. Chase and A. Lysyanskaya. On signatures of knowledge. In C. Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 78–96, Santa Barbara, CA, USA, Aug. 20–24, 2006. Springer, Heidelberg, Germany.
7. D. Chaum and E. van Heyst. Group signatures. In D. W. Davies, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 257–265, Brighton, UK, Apr. 8–11, 1991. Springer, Heidelberg, Germany.
8. G. Danezis, C. Fournet, J. Groth, and M. Kohlweiss. Square span programs with applications to succinct NIZK arguments. In P. Sarkar and T. Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 532–550, Kaoshiung, Taiwan, R.O.C., Dec. 7–11, 2014. Springer, Heidelberg, Germany.
9. Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup. Anonymous identification in ad hoc groups. In C. Cachin and J. Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 609–626, Interlaken, Switzerland, May 2–6, 2004. Springer, Heidelberg, Germany.

10. S. Galbraith, K. Paterson, and N. Smart. Pairings for cryptographers. Cryptology ePrint Archive, Report 2006/165, 2006. `http://eprint.iacr.org/2006/165`.
11. R. Gennaro, C. Gentry, B. Parno, and M. Raykova. Quadratic span programs and succinct NIZKs without PCPs. In T. Johansson and P. Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 626–645, Athens, Greece, May 26–30, 2013. Springer, Heidelberg, Germany.
12. C. Gentry and D. Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. In L. Fortnow and S. P. Vadhan, editors, *43rd ACM STOC*, pages 99–108, San Jose, CA, USA, June 6–8, 2011. ACM Press.
13. S. Goldwasser and Y. T. Kalai. On the (in)security of the Fiat-Shamir paradigm. In *44th FOCS*, pages 102–115, Cambridge, MA, USA, Oct. 11–14, 2003. IEEE Computer Society Press.
14. A. González, A. Hevia, and C. Ràfols. QA-NIZK arguments in asymmetric groups: New tools and new constructions. In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 605–629, Auckland, New Zealand, Nov. 30 – Dec. 3, 2015. Springer, Heidelberg, Germany.
15. A. Gonzlez. Shorter ring signatures from standard assumptions. Cryptology ePrint Archive, Report 2017/905, 2017. `https://eprint.iacr.org/2017/905`.
16. C. Gritti, W. Susilo, and T. Plantard. Logarithmic size ring signatures without random oracles. *IET Information Security*, 10(1):1–7, 2016.
17. J. Groth. On the size of pairing-based non-interactive arguments. In M. Fischlin and J.-S. Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 305–326, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany.
18. J. Groth and M. Kohlweiss. One-out-of-many proofs: Or how to leak a secret and spend a coin. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 253–280, Sofia, Bulgaria, Apr. 26–30, 2015. Springer, Heidelberg, Germany.
19. J. Groth and S. Lu. A non-interactive shuffle with pairing based verifiability. In K. Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 51–67, Kuching, Malaysia, Dec. 2–6, 2007. Springer, Heidelberg, Germany.
20. J. Groth, R. Ostrovsky, and A. Sahai. Perfect non-interactive zero knowledge for NP. In S. Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 339–358, St. Petersburg, Russia, May 28 – June 1, 2006. Springer, Heidelberg, Germany.
21. J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432, Istanbul, Turkey, Apr. 13–17, 2008. Springer, Heidelberg, Germany.
22. C. S. Jutla and A. Roy. Improved structure preserving signatures under standard bilinear assumptions. Cryptology ePrint Archive, Report 2017/025, 2017. `http://eprint.iacr.org/2017/025`.
23. B. Libert, S. Ling, K. Nguyen, and H. Wang. Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors. In M. Fischlin and J.-S. Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 1–31, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany.
24. G. Malavolta and D. Schröder. Efficient ring signatures in the standard model. In T. Takagi and T. Peyrin, editors, *ASIACRYPT 2017, Part II*, volume 10625 of *LNCS*, pages 128–157, Hong Kong, China, Dec. 3–7, 2017. Springer, Heidelberg, Germany.

25. P. Morillo, C. Ràfols, and J. L. Villar. The kernel matrix Diffie-Hellman assumption. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 729–758, Hanoi, Vietnam, Dec. 4–8, 2016. Springer, Heidelberg, Germany.
26. M. Naor. On cryptographic assumptions and challenges (invited talk). In D. Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 96–109, Santa Barbara, CA, USA, Aug. 17–21, 2003. Springer, Heidelberg, Germany.
27. C. Ràfols. Stretching groth-sahai: NIZK proofs of partial satisfiability. In Y. Dodis and J. B. Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, pages 247–276, Warsaw, Poland, Mar. 23–25, 2015. Springer, Heidelberg, Germany.
28. R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In C. Boyd, editor, *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 552–565, Gold Coast, Australia, Dec. 9–13, 2001. Springer, Heidelberg, Germany.
29. P. Rogaway and T. Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In B. K. Roy and W. Meier, editors, *FSE 2004*, volume 3017 of *LNCS*, pages 371–388, New Delhi, India, Feb. 5–7, 2004. Springer, Heidelberg, Germany.