

A Ring Signature of size $\Theta(\sqrt[3]{n})$ without Random Oracles

Alonso González

Ecole Normale Supérieure de Lyon, Laboratoire LIP (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 (called a ring) while guaranteeing authenticity, i.e. only members of the ring can produce valid signatures, and anonymity, i.e. signatures hide the actual signer. In terms of efficiency, the shortest ring signatures are of size $\Theta(\log n)$, where n is the size of the ring, and are due to Groth and Kohlweiss (EUROCRYPT 2015) and Libert et al. (EUROCRYPT 2016). But both schemes are proven secure in the random oracle model. Without random oracles the most efficient construction remains the one of Chandran et al. (ICALP 2007) with a signature of size $\Theta(\sqrt{n})$. In this work we construct a ring signature of size $\Theta(\sqrt[3]{n})$ without random oracles. Our construction uses bilinear groups and we prove its security under the permutation pairing assumption, introduced by Groth and Lu (ASIACRYPT 2007).

1 Introduction

Ring signatures, introduced by Rivest, Shamir and Tauman, [23], allow to anonymously sign a message on behalf of a ring of users P_1, \dots, P_n , only if the signer belongs to that ring. Although there are other cryptographic schemes that provide similar guarantees (e.g. group signatures [9]), 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.

While the more efficient constructions have signature size logarithmic in the size of the ring [13,18], all of them rely on the random oracle model. Without random oracles 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. [8]. We remark that no asymptotic improvements to Chandran et al.’s construction have been made since their introduction (only improvements in the constants by Ràfols [22] and by González et al. [10]). Although some previous works claim to construct signatures of constant [7] or logarithmic [12] size, they are either in a weaker security model or we can identify a flaw in the construction (see Section 1.4).

In this work we present the first ring signature (without random oracles) whose signature size is asymptotically smaller than Chandran et al.’s. Our ring

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.

The security of our construction relies on a security assumption – the permutation pairing assumption – introduced by Groth and Lu [14] in an unrelated setting: proofs of correctness of a shuffle. While the assumption is “non-standard”, in the sense that it is not a “DDH like” assumption, it is a falsifiable assumption and it was proven hard in generic symmetric groups by Groth and Lu. For simplicity, we work on symmetric groups ($\mathbb{G}_1 = \mathbb{G}_2$) but our techniques can be easily extended to asymmetric as we show in Appendix A.2.

Our ring signature outperforms Chandran et al.’s in terms signature size for any $n > 246$, in terms of signature generation time for any $n > 205$, and in terms of verifier efficiency for any $n > 170$. However, this analysis should be taken with care, since Chandran et al.’s signature is proven secure under the decisional linear (DLin) assumption while ours is proven secure under the permutation pairing assumption. Therefore, it could be the case that our scheme would be as secure as Chandran et al.’s at higher values of the security parameter. In Table 1 we provide a comparison between our scheme and Chandran et al.’s.

	Chandran et al. [8]	This work
CRS size	9	9
Verification key size	1	5
Signature size	$24\sqrt{n} + 24$	$39\sqrt[3]{n} + 30\sqrt[6]{n} + 81$
Signature generation time	$42\sqrt{n} + 49$	$69\sqrt[3]{n} + 42\sqrt[6]{n} + 142$
Verification time	$3n + 120\sqrt{n} + 121$	$6n^{2/3} + 210\sqrt[3]{n} + 186\sqrt[6]{n} + 411$

Table 1: Comparison of Chandran et al.’s ring signature and ours for a ring of size n . ‘Signature generation time’ is measured in number of exponentiations, ‘Verification time’ is measured in number of pairings, and all other rows are measured in number of group elements.

1.1 Chandran et al.’s Construction

Our scheme follows the ring signature of Chandran et al. Consider a symmetric bilinear group $gk := (\mathbb{G}, \mathbb{G}_T, e, \mathcal{P}, q)$ of prime order q , where \mathcal{P} is a generator. Define $[x] = x\mathcal{P}$ for any $x \in \mathbb{Z}_q$. Consider also a Boneh-Boyen signature scheme [4] which secret/verification keys are of the form $(sk, [vk])$, where sk is equal to vk . The validity of a Boneh-Boyen signature $[\sigma] \in \mathbb{G}$ for a message $m \in \mathbb{Z}_q$ under the verification $[vk]$ corresponds to the satisfiability of an equation $\text{eq}([\sigma], [vk], m)$ over the bilinear group. Thereby, one can prove possession of a

valid signature, without revealing the signature, using Groth-Sahai proofs.[15]¹² Given also a one-time signature scheme, the signature of the message m for a ring $R = \{[vk_1], \dots, [vk_n]\}$ is computed as follows:

- a) Pick a one-time signature key $(sk_{\text{ot}}, vk_{\text{ot}})$, sign m with sk_{ot} , and sign vk_{ot} with sk .
- b) Show possession of valid signature of vk_{ot} under $[vk]$ using Groth-Sahai proofs.
- c) Show that $[vk] \in R$.

The most costly part is c) and the core of Chandran et al.'s construction is a proof of size $\Theta(\sqrt{n})$ of c). We call this kind of proof a set-membership proof and we describe Chandran et al.'s below.

The proof arranges the set of verification keys on a matrix of size $m \times m$, where $m := \sqrt{n}$, as depicted below

$$[\mathbf{V}] := \begin{pmatrix} [vk_{1,1}] & \cdots & [vk_{1,m}] \\ \vdots & \ddots & \vdots \\ [vk_{m,1}] & \cdots & [vk_{m,m}] \end{pmatrix}$$

where $vk_{i,j} := vk_{(i-1)m+j}$ for $1 \leq i, j \leq m$.

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

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

Using Groth-Sahai proofs, the prover proves that

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

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

¹ We assume here some familiarity with the Groth-Sahai proof system. We provide a description of Groth-Sahai proofs on Section 2.1

² We could replace the Boneh-Boyen signature scheme with any structure preserving signature scheme secure under milder assumptions (e.g. [16]). 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.

1.2 High Level Description of our Construction

In our scheme the secret/verification keys of party P is (sk, \mathbf{vk}) , where $\mathbf{vk} = ([vk], [\mathbf{a}], \mathbf{a}[vk])$, $(sk, [vk])$ are secret/verification keys of the Boneh-Boyen signature scheme, and $\mathbf{a} \in \mathbb{Z}_q^2$ is chosen independently for each key from some distribution \mathcal{Q} to be specified later. Suppose that \mathbf{vk} is the α th element in the ring $R = \{\mathbf{vk}_1, \dots, \mathbf{vk}_n\}$ and let $1 \leq i_\alpha, j_\alpha, k_\alpha \leq m$ such that $\mathbf{vk}_\alpha = \mathbf{vk}_{i_\alpha, j_\alpha, k_\alpha}$, where $\mathbf{vk}_{i,j,k} = \mathbf{vk}^{(i-1)m^2+(j-1)m+k}$ for $1 \leq i, j, k \leq m$ and $m := \sqrt[3]{n}$. Below we describe a $\Theta(\sqrt[3]{n})$ set-membership-proof in R .

Consider the sets

$$S := \{[s_1], \dots, [s_{n^{2/3}}]\} := \left\{ \sum_{i=1}^m [\mathbf{a}_{i,1,1}], \dots, \sum_{i=1}^m [\mathbf{a}_{i,m,m}] \right\} \text{ and}$$

$$S' := \{[s'_1], \dots, [s'_{n^{2/3}}]\} := \left\{ \sum_{i=1}^m \mathbf{a}_{i,1,1}[vk_{i,1,1}], \dots, \sum_{i=1}^m \mathbf{a}_{i,m,m}[vk_{i,m,m}] \right\}.$$

The prover commits to $[\mathbf{x}] = [s_\mu]$ and $[\mathbf{y}] = [s'_{\mu'}]$, for $\mu = \mu' = (j_\alpha - 1)m + k_\alpha$, and shows, using (twice) the set-membership proof of Chandran et al., that $[\mathbf{x}] \in S$ and that $[\mathbf{y}] \in S'$. The prover also needs to assure that $\mu = \mu'$, which can be done reutilizing the commitment to μ (in fact to its representation as two unitary vectors of size m) used in the proof that $[\mathbf{x}] \in S$ and in the proof that $[\mathbf{y}] \in S'$. Since both sets are of size $n^{2/3}$, the two set membership proofs are of size $\Theta(\sqrt[3]{n})$.

Now that the prover has committed to elements $[\mathbf{x}] = \sum_{i=1}^m [\mathbf{a}_{i,j_\alpha,k_\alpha}]$ and $[\mathbf{y}] = \sum_{i=1}^m \mathbf{a}_{i,j_\alpha,k_\alpha}[vk_{i,j_\alpha,k_\alpha}]$, it additionally commits to $[\kappa_1] := [vk_{1,j_\alpha,k_\alpha}], \dots, [\kappa_m] := [vk_{m,j_\alpha,k_\alpha}]$ and $[\mathbf{z}_1] := [\mathbf{a}_{1,j_\alpha,k_\alpha}], \dots, [\mathbf{z}_m] := [\mathbf{a}_{m,j_\alpha,k_\alpha}]$. The prover now gives a proof that

$$\sum_{i=1}^m [\mathbf{z}_i][\kappa_i] = [\mathbf{y}][1]. \quad (1)$$

Assume for a while that $\mathbf{z}_1, \dots, \mathbf{z}_m$ is a permutation of $\mathbf{a}_{1,j_\alpha,k_\alpha}, \dots, \mathbf{a}_{m,j_\alpha,k_\alpha}$, that is $\mathbf{z}_i = \mathbf{a}_{\pi(i),j_\alpha,k_\alpha}$, $1 \leq i \leq m$, for some permutation $\pi \in S_m$. Therefore, equation (1) implies that

$$\begin{aligned} \sum_{i=1}^m [\mathbf{z}_i][\kappa_i] &= \sum_{i=1}^m [\mathbf{a}_{\pi(i),j_\alpha,k_\alpha}][\kappa_i] = \sum_{i=1}^m [\mathbf{a}_{i,j_\alpha,k_\alpha}][\kappa_{\pi^{-1}(i)}] \\ &= \sum_{i=1}^m [\mathbf{a}_{i,j_\alpha,k_\alpha}][vk_{i,j_\alpha,k_\alpha}]. \end{aligned}$$

Then $\kappa_1, \dots, \kappa_m$ is a permutation of $vk_{1,j_\alpha,k_\alpha}, \dots, vk_{m,j_\alpha,k_\alpha}$ (the same defined by $\mathbf{z}_1, \dots, \mathbf{z}_m$), unless $(\kappa_{\pi^{-1}(1)} - vk_{1,j_\alpha,k_\alpha}), \dots, \kappa_{\pi^{-1}(m)} - vk_{m,j_\alpha,k_\alpha})^\top$ is in the kernel of \mathbf{A} . However, this is in general a hard problem and in fact corresponds a to kernel matrix Diffie-Hellman assumption, in the terminology of Morillo et al. [21]. For the distribution \mathcal{Q} (defined later), Groth and Lu showed the hardness of this problem in the generic group model [14].

Finally, the prover shows, using Chandran et al.'s set-membership proof, that $[vk_\alpha] \in \{[\kappa_1], \dots, [\kappa_m]\}$ which implies that $[vk_\alpha] = [vk_{i_\alpha, j_\alpha, k_\alpha}]$.

It is only left to show that $\mathbf{z}_1, \dots, \mathbf{z}_m$ is a permutation of $\mathbf{a}_{1, j_\alpha, k_\alpha}, \dots, \mathbf{a}_{m, j_\alpha, k_\alpha}$. To do so we will use the following assumption introduced by Groth and Lu [14].

Definition 1 (Permutation Pairing Assumption). Let $\mathcal{Q}_m = \underbrace{\mathcal{Q} \dots \mathcal{Q}}_{m \text{ times}}$, where concatenation of distributions is defined in the natural way and

$$\mathcal{Q} : \mathbf{a} = \begin{pmatrix} x \\ x^2 \end{pmatrix}, \quad x \leftarrow \mathbb{Z}_q.$$

We say that the m -permutation pairing assumption holds relative to Gen_s if for any adversary \mathbf{A}

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

where $[\mathbf{Z}] = [(z_1, \dots, z_m)]$, $[\mathbf{A}] = [(\mathbf{a}_1, \dots, \mathbf{a}_m)] \in \mathbb{G}^{2 \times m}$, is negligible in λ .

If the prover additionally proves that equations (i) and (ii) from definition 1 are satisfied for $\mathbf{A} := (\mathbf{a}_{1, j_\alpha, k_\alpha}, \dots, \mathbf{a}_{m, j_\alpha, k_\alpha})$, which can be done with $\Theta(m)$ group elements using Groth-Sahai proofs, the assumption is guaranteeing that the columns of \mathbf{Z} are a permutation of the columns of \mathbf{A} .

1.3 Discussion

Extending our technique. A natural question is if this technique can be applied once again. That is, to compute a $\Theta(\sqrt[4]{n})$ proof, compute commitments to an element from $S = \{\sum_{i=1}^m \mathbf{a}_{i,1,1,1}[vk_{i,1,1,1}], \dots, \sum_{i=1}^m \mathbf{a}_{i,m,m,m}[vk_{i,m,m,m}]\}$ and $S' = \{\sum_{i=1}^m [\mathbf{a}_{i,1,1,1}], \dots, \sum_{i=1}^m [\mathbf{a}_{i,m,m,m}]\}$, and then prove that they belong to the respective sets with our set-membership proof of size $\Theta(\sqrt[3]{n})$. Since $|S| = |S'| = n^{3/4}$, proof will be of size $\Theta(\sqrt[3]{n^{3/4}}) = \Theta(\sqrt[4]{n})$. However, this is not possible since the $\Theta(\sqrt[3]{n})$ proof is not a set-membership proof for arbitrary sets but only for sets where each element is of the form $([vk], \mathbf{a}[vk], [\mathbf{a}])$. Clearly, elements from S and S' do not have this form.

Erasures. In the security proof we need to embed an instance of the permutation pairing assumption on the verification keys. On the other hand, the adversary may adaptively corrupt parties obtaining all the random coins used to generate the verification key, which amounts to reveal \mathbf{a} (the discrete logs of $[\mathbf{a}]$) and is incompatible with the permutation pairing assumption. Since is not clear how to obliviously sample $[x]$ and $[x^2]$ and we can only guess the set of corrupted parties with negligible probability, we are forced to use erasures. That is, after sampling $\mathbf{a} \leftarrow \mathcal{Q}$ and computing $[\mathbf{a}]$, the key generation algorithm erases \mathbf{a} .

Getting rid of the non-standard assumptions. Gonzalez et al. [11] modify Groth and Lu’s proof of correctness of a shuffle [14] to get rid of the permutation pairing assumption. They showed that the statement “[$\mathbf{z}_1, \dots, \mathbf{z}_m$] is a permutation of [$\mathbf{a}_1, \dots, \mathbf{a}_m$]” can be showed with a proof that [$\mathbf{z}_1, \dots, \mathbf{z}_m$] \in {[$\mathbf{a}_1, \dots, \mathbf{a}_m$]} and a proof that $\sum_{i=1}^m [\mathbf{z}_i] = \sum_{i=1}^m [\mathbf{a}_i]$. Gonzalez et al. construct a $\Theta(m)$ proof that [$\mathbf{z}_1, \dots, \mathbf{z}_m$] \in {[$\mathbf{a}_1, \dots, \mathbf{a}_m$]} under standard assumptions (DLin in symmetric groups) and also noted that finding an element on the kernel of \mathbf{A} is harder than DLin if $\mathbf{a}_1, \dots, \mathbf{a}_m \leftarrow \mathbb{Z}_q^2$.

If we use Gonzalez et al.’s techniques we would have to show that [$\mathbf{z}_1, \dots, \mathbf{z}_m$] \in {[$\mathbf{a}_{1,j_\alpha,k_\alpha}, \dots, \mathbf{a}_{m,j_\alpha,k_\alpha}$]}. However, since we can’t reveal j_α, k_α , we need to commit to {[$\mathbf{a}_{1,j_\alpha,k_\alpha}, \dots, \mathbf{a}_{m,j_\alpha,k_\alpha}$]} and show that they are appropriately computed, which requires at least $\Omega(m^2)$ group elements.

We note that we are using features of the permutation pairing assumption that were ignored by Gonzalez et al. and by Groth and Lu. Intuitively, we are using the fact that $\sum_{i=1}^m [\mathbf{a}_{i,j_\alpha,k_\alpha}]$ “defines” the set $S_{j_\alpha,k_\alpha} := \{[\mathbf{a}_{1,j_\alpha,k_\alpha}], \dots, [\mathbf{a}_{m,j_\alpha,k_\alpha}]\}$ in the sense that is all what we need to show membership in S_{j_α,k_α} . This feature allows us to select S_{j_α,k_α} from S using only $\Theta(\sqrt[3]{n})$ group elements.

Relation to [10]. Our construction is similar to the set membership proof of Gonzalez et al. [10, Appendix D.2]. However, the proof system from [10] does not suffice for constructing a ring signature because there the CRS is fixed to a specific set and thus, the resulting ring signature will be fixed to a specific ring.

1.4 Flawed or Weaker Ring Signatures

Bose et al. claim to construct a constant-size ring signature in the standard model [7]. However, they construct a weak ring signature where: a) the public keys are generated all at once in a correlated way; b) the set of parties which are able to participate in a ring is fixed as well as the maximum ring size; and c) the key size is linear in the maximum ring size. In the work of Chandran et al. and also in our setting: a) the key generation is independently run by the user using only the CRS as input; b) any party can be member of the ring as long as she has a verification key, and the maximum ring size is unbounded; and c) the key size is constant. These stronger requirements are in line with the original spirit of non-coordination of Rivest et al. [23].

Gritti et al. claim to construct a logarithmic ring signature in the standard model [12]. However, their construction is flawed as explained below.³ In page 12, Gritti et al. define $v_{b_i} := v_{b_1 \dots b_i *}$, where $b_1 \dots b_i *$ is the set of all bit-strings of size $d := \log n$ whose prefix is $b_1 \dots b_i$. From this, one has to conclude that v_{b_i} is a set (or vector) of group elements of size 2^{d-i} . In the same page they define the commitment $D_{b_i} := v_{b_i} h^{s_{b_i}}$, for random $s_{b_i} \in \mathbb{Z}_q$, which, according to the previous observation, is the multiplication of a set (or vector) of group elements with a group element. Given that length reducing group to group commitments are

³ We use multiplicative notation for the group operations to keep the expressions as they appear in the original work.

known to not exist [1], its representation requires at least 2^{d-i} group elements.⁴ Since commitments D_{b_0}, \dots, D_{b_d} are part of the signature, the actual signature size is $\Theta(2^d) = \Theta(n)$, rather than $\Theta(d) = \Theta(\log n)$ as claimed by Gritti et al.

2 Preliminaries

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

Let Gen_s be some probabilistic polynomial time algorithm which on input 1^λ , where λ is the security parameter, returns the *group key* which is the description of a symmetric bilinear group $gk := (q, \mathbb{G}, \mathbb{G}_T, e, \mathcal{P})$, where \mathbb{G} and \mathbb{G}_T are groups of prime order q , the element \mathcal{P} is a generator of \mathbb{G} , and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is an efficiently computable and non-degenerated bilinear map.

Elements in \mathbb{G} are denoted implicitly as $[a] := a\mathcal{P}$, where $a \in \mathbb{Z}_q$, and elements in \mathbb{G}_T are denoted as $[a]_T := a\mathcal{P}$, where $\mathcal{P}_T := e(\mathcal{P}, \mathcal{P})$. The pairing operation is written as a product \cdot , that is $[a] \cdot [b] = [a][b] = e([a], [b]) = [ab]_T$. Vectors and matrices are denoted in boldface. Given a matrix $\mathbf{T} = (t_{i,j})$, $[\mathbf{T}]$ is the natural embedding of \mathbf{T} in \mathbb{G} , that is, the matrix whose (i, j) th entry is $t_{i,j}\mathcal{P}$. 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} .

We recall the definition of the decisional linear assumption (in matricial notation) and the kernel matrix Diffie-Hellman assumption.

Definition 2 (Decisional Diffie-Hellman Assumption (DLin)). Let $gk \leftarrow \text{Gen}_s(1^\lambda)$ and let

$$\mathbf{A} := \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix}, \quad a_1, a_2 \leftarrow \mathbb{Z}_q.$$

We say that the DLin assumption holds relative to Gen_s if for all PPT adversaries \mathcal{D}

$$\text{Adv}_{\text{DLin}, \text{Gen}_s}(\mathcal{D}) := |\Pr[\mathcal{D}(gk, [\mathbf{A}], [\mathbf{A}\mathbf{w}]) = 1] - \Pr[\mathcal{D}(gk, [\mathbf{A}], [\mathbf{z}]) = 1]|$$

is negligible in λ , where the probability is taken over $gk \leftarrow \text{Gen}_s(1^\lambda)$, $a_1, a_2 \leftarrow \mathbb{Z}_q$, $\mathbf{w} \leftarrow \mathbb{Z}_q^2$, $[\mathbf{z}] \leftarrow \mathbb{G}^3$, and the coin tosses of the adversary.

Definition 3 (Kernel Diffie-Hellman Assumption in \mathbb{G} [20]). Let $gk \leftarrow \text{Gen}_s(1^\lambda)$ and $\mathcal{D}_{\ell,k}$ a distribution over $\mathbb{Z}_q^{\ell \times k}$. The Kernel Diffie-Hellman assumption in \mathbb{G} ($\mathcal{D}_{\ell,k}$ -KerMDH $_{\mathbb{G}_T}$) says that every PPT Algorithm has negligible advantage in the following game: given $[\mathbf{A}]$, where $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, find $[\mathbf{x}] \in \mathbb{G}^\ell$, $\mathbf{x} \neq \mathbf{0}$, such that $[\mathbf{x}]^\top [\mathbf{A}] = [\mathbf{0}]_T$.

We will be using the Q_m^\top -KerMDH assumption, which was proven secure in the generic bilinear group model by Groth and Lu [14].

⁴ In fact, there exists length reducing *weak* group to group commitments [2] but is far from clear how to use them with Groth-Sahai proofs as required by Gritti et al.

2.1 Groth-Sahai Proofs in the DLin 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:

$$\sum_{j=1}^{m_y} f(\alpha_j, \gamma_j) + \sum_{i=1}^{m_x} f(x_i, \beta_i) + \sum_{i=1}^{m_x} \sum_{j=1}^{m_y} f(x_i, \gamma_{i,j} \gamma_j) = t, \quad (2)$$

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

The GS proof system is a *commit-and-prove* proof system, that is, the prover first commits to solutions of equation (2) using the GS commitments, and then computes a proof that the committed values satisfies equation (2).

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 distribution implies either perfect soundness and computational witness indistinguishability or computational soundness and perfect witness-indistinguishability.

Groth-Sahai Commitments. Following Groth and Sahai's work [15], in symmetric groups and using the DLin assumption, GS commitments are vectors in \mathbb{G}^3 of the form

$$\begin{aligned} \text{GS.Com}_{ck}([x]; \mathbf{r}) &:= \begin{pmatrix} [0] \\ [0] \\ [x] \end{pmatrix} + r_1[\mathbf{u}_1] + r_2[\mathbf{u}_2] + r_3[\mathbf{u}_3] \\ \text{GS.Com}_{ck}(x; \mathbf{r}) &:= x \begin{pmatrix} [0] \\ [\mathbf{u}_1] + \begin{pmatrix} [0] \\ [0] \\ [1] \end{pmatrix} \end{pmatrix} + r_1[\mathbf{u}_2] + r_2[\mathbf{u}_3] \end{aligned}$$

where $ck := ([\mathbf{u}_1][\mathbf{u}_2][\mathbf{u}_3])$, $(\mathbf{u}_2|\mathbf{u}_3) = \mathbf{A}$, and \mathbf{A} is the matrix from definition 2. The GS reference string is the commitment key ck and $\mathbf{u}_1 := w_1\mathbf{u}_2 + w_2\mathbf{u}_3$ in the perfectly binding setting, and $\mathbf{u}_1 := w_1\mathbf{u}_2 + w_2\mathbf{u}_3 - \mathbf{e}_3$ in the perfectly hiding setting, for $w_1, w_2 \leftarrow \mathbb{Z}_q$.

2.2 Ring Signature Definition

We follow Chandran et al.'s definitions [8], which extends the original definition of Bender et al. [3] by including a CRS and perfect anonymity. We allow erasures in the key generation algorithm.

Definition 4 (Ring Signature). A ring signature scheme consists of a quadruple of PPT algorithms (CRSGen, KeyGen, Sign, 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:

- $\text{CRSGen}(gk)$, where gk is the group key, outputs the common reference string ρ .
- $\text{KeyGen}(\rho)$ is run by the user. It outputs a public verification key vk and a private signing key sk .
- $\text{Sign}_{\rho,sk}(m, R)$ outputs a signature σ on the message m with respect to the ring $R = \{vk_1, \dots, vk_n\}$. We require that (vk, sk) is a valid key-pair output by KeyGen and that $vk \in R$.
- $\text{Verify}_{\rho,R}(m, \sigma)$ 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 $(\text{CRSGen}, \text{KeyGen}, \text{Sign}, \text{Verify})$ is a ring signature with perfect anonymity if it has perfect correctness, computational unforgeability and perfect anonymity as defined below.

Definition 5 (Perfect Correctness). We require that a user can sign any message on behalf of a ring where she is a member. A ring signature $(\text{CRSGen}, \text{KeyGen}, \text{Sign}, \text{Verify})$ has perfect correctness if for any unbounded adversary A we have:

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

Definition 6 (Computational Unforgeability). A ring signature scheme $(\text{CRSGen}, \text{KeyGen}, \text{Sign}, \text{Verify})$ 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 any non-uniform polynomial time adversaries A we have that

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

is negligible in the security parameter, where

- VKGen on query number i selects randomness w_i , computes $(vk_i, sk_i) := \text{KeyGen}(\rho; w_i)$ and returns vk_i .
- $\text{Sign}(i, m, R)$ returns $\sigma \leftarrow \text{Sign}_{\rho,sk_i}(m, R)$, provided (vk_i, sk_i) has been generated by VKGen and $vk_i \in R$.
- $\text{Corrupt}(i)$ 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 7 (Perfect Anonymity). A ring signature scheme $(\text{CRSGen}, \text{KeyGen}, \text{Sign}, \text{Verify})$ 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 :

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

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 $\text{KeyGen}(\rho)$.

2.3 Boneh-Boyen Signatures

Boneh and Boyen introduce 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 [4]. 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.

Definition 8 (weak Existential Unforgeability (wUF-CMA)). We say that a signature scheme $\Sigma = (\text{KGen}, \text{Sign}, \text{Ver})$ is wUF-CMA if for any adversary A

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

is negligible in λ .

The Boneh-Boyen signature is proven wUF-CMA secure under the m -strong Diffie-Hellman assumption, which is described below.

Definition 9 (m -SDH assumption). For any adversary A

$$\Pr \left[gk \leftarrow \text{Gen}_s(1^\lambda), x \leftarrow \mathbb{Z}_q : A(gk, [x], [x^2], \dots, [x^m]) = (c, \left[\frac{1}{x+c} \right]) \right]$$

is negligible in λ .

The Boneh-Boyen signature scheme is described below.

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

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

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

3 Our Construction

In the following consider $\text{OT} = (\text{OT.KeyGen}, \text{OT.Sign}, \text{OT.Ver})$ a one-time signature scheme.

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

KeyGen(ρ): Pick $\mathbf{a} \leftarrow \mathcal{Q}$ and $(sk, [vk]) \leftarrow \text{BB.KeyGen}(gk)$, compute $[\mathbf{a}]$ and then erase \mathbf{a} . The secret key is sk and the verification key is $\mathbf{vk} := ([vk], [\mathbf{a}], \mathbf{a}[vk])$.

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

2. Compute $[\mathbf{c}] := \text{GS.Com}_{ck}([vk]; \mathbf{r})$, $\mathbf{r} \leftarrow \mathbb{Z}_q^3$, $[\sigma] \leftarrow \text{BB.Sign}_{sk}(vk_{\text{ot}})$, $[\mathbf{d}] := \text{GS.Com}_{ck}([\sigma]; \mathbf{s})$, $\mathbf{s} \leftarrow \mathbb{Z}_q^3$, and a GS proof π_{GS} that $\text{BB.Ver}_{[vk]}([\sigma], vk_{\text{ot}}) = 1$ (which can be expressed as a set of pairing product equations).

3. Parse R as $\{\mathbf{vk}_{1,1,1}, \dots, \mathbf{vk}_{m,m,m}\}$, where $m := \sqrt[3]{n}$, $n := |R|$, and let $\alpha = (i_\alpha - 1)m^2 + (j_\alpha - 1)m + k_\alpha$ the index of \mathbf{vk} in R . Define the sets $S = \{\sum_{i=1}^m [\mathbf{a}_{i,1,1}], \dots, \sum_{i=1}^m [\mathbf{a}_{i,m,m}]\}$ and $S' = \{\sum_{i=1}^m \mathbf{a}_{i,1,1}[vk_{i,1,1}], \dots, \sum_{i=1}^m \mathbf{a}_{i,m,m}[vk_{i,m,m}]\}$.

4. Let $[\mathbf{x}] := \sum_{i=1}^m [\mathbf{a}_{i,j_\alpha,k_\alpha}]$ and $[\mathbf{y}] = \sum_{i=1}^m \mathbf{a}_{i,j_\alpha,k_\alpha}[vk_{i,j_\alpha,k_\alpha}]$. Compute GS commitments to $[\mathbf{x}]$ and $[\mathbf{y}]$, and compute proofs π_1 and π_2 that they belong to S and S' , 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 $[\mathbf{x}]$'s and $[\mathbf{y}]$'s position in S and S' respectively.

5. Let $[\kappa_1] := [vk_{1,j_\alpha,k_\alpha}], \dots, [\kappa_m] := [vk_{m,j_\alpha,k_\alpha}]$ and $[\mathbf{z}_1] := [\mathbf{a}_{1,j_\alpha,k_\alpha}], \dots, [\mathbf{z}_m] := [\mathbf{a}_{m,j_\alpha,k_\alpha}]$. Compute GS commitments to $[\kappa_1], \dots, [\kappa_m]$ and $[\mathbf{z}_1], \dots, [\mathbf{z}_m]$, and GS proof π_κ that $\sum_{i=1}^m [\kappa_i][\mathbf{z}_i] = [\mathbf{y}][1]$ and a GS proof π_z that $\sum_{i=1}^m [\mathbf{z}_i] = [\mathbf{x}]$ and $[z_{2,i}][1] = [z_{1,i}][z_{1,i}]$ for each $1 \leq i \leq m$.

6. Compute a proof π_3 that $[vk]$ belongs to $S_3 = \{[\kappa_1], \dots, [\kappa_m]\}$.

7. Return the signature $\sigma := (vk_{\text{ot}}, \sigma_{\text{ot}}, [\mathbf{c}], [\mathbf{d}], \pi_1, \pi_2, \pi_3, \pi_\kappa, \pi_z)$. (GS proofs include commitments to variables).

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

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 $\mathcal{Q}_{q_{\text{gen}}}^\top$ -KerMDH assumption, the DLin assumption, and the assumption that the one-time signature and the Boneh-Boyen signature are unforgeable. Concretely, for any PPT adversary \mathbf{A} against the unforgeability of the scheme, there exist adversaries $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{B}_4, \mathbf{B}_5$ such that*

$$\begin{aligned} \text{Adv}(\mathbf{A}) \leq & \text{Adv}_{\text{DLin}}(\mathbf{B}_1) + \text{Adv}_{q_{\text{gen}}\text{-PPA}}(\mathbf{B}_2) + \text{Adv}_{\mathcal{Q}_{q_{\text{gen}}}^\top\text{-KerMDH}}(\mathbf{B}_3) + \\ & q_{\text{gen}}(q_{\text{sig}} \text{Adv}_{\text{OT}}(\mathbf{B}_4) + \text{Adv}_{\text{BB}}(\mathbf{B}_5)), \end{aligned}$$

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 \mathbf{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”.

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

Game₀: This is the real unforgeability experiment. **Game₀** returns 1 if the adversary A produces a valid forgery and 0 if not.

Game₁: This is game exactly as **Game₀** with the following differences:

- The Groth-Sahai CRS is sampled together with its discrete logarithms from the perfectly binding distribution.
- At the beginning, variables err_2 and err_3 are initialized to 0, and a random index i^* is chosen from $\{1, \dots, q_{\text{gen}}\}$.
- On a query to **Corrupt** with argument i , if $i = i^*$ set $\text{err}_3 \leftarrow 1$ and proceed as in **Game₀**.
- Let (m, R, σ) the purported forgery output by A . If $[vk]$, the opening of commitment $[c]$ from σ , is not equal to $[vk_{i^*}]$, set $\text{err}_3 \leftarrow 1$. If $[vk] \notin R$, then set $\text{err}_2 = 1$.

Game₂: This is game exactly as **Game₁** except that, if err_2 is set to 1, **Game₂** aborts.

Game₃: This is game exactly as **Game₂** except that, if err_3 is set to 1, **Game₃** aborts.

Since in **Game₁** variables err_2 and err_3 are just dummy variables, the only difference with **Game₀** comes from the Groth-Sahai CRS distribution. It follows that there is an adversary B_1 against DLin such that $|\Pr[\text{Game}_0 = 1] - \Pr[\text{Game}_1 = 1]| \leq \mathbf{Adv}_{\text{DLin}}(B_1)$.

Lemma 1. *There exist adversaries B_2 and B_3 against the q_{gen} -permutation pairing assumption and against the $\mathcal{Q}_{q_{\text{gen}}}^\top$ -KerMDH assumption, respectively, such that*

$$|\Pr[\text{Game}_2 = 1] - \Pr[\text{Game}_1 = 1]| \leq \mathbf{Adv}_{q_{\text{gen}}\text{-PPA}}(B_2) + \mathbf{Adv}_{\mathcal{Q}_{q_{\text{gen}}}^\top\text{-KerMDH}}(B_3).$$

Proof. Note that

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

We proceed to bound this last probability.

Consider an adversary B_2 against the q_{gen} -permutation pairing assumption defined as follows. B_2 receives as challenge $[\mathbf{A}'] \in \mathbb{G}^{2 \times q_{\text{gen}}}$ and honestly simulates Game_1 with the following exception. On the i th query of A to VKGen picks $(sk, [vk]) \leftarrow \text{BB.KeyGen}(1^\lambda)$ and sets $(sk_i, \mathbf{vk}_i) := (sk, ([vk], [\mathbf{a}'_i], sk[\mathbf{a}'_i]))$, where $[\mathbf{a}'_i]$ is the i th column of $[\mathbf{A}']$. When A outputs $\text{GS.Com}_{ck_{\text{GS}}}([\mathbf{z}_1]), \dots, \text{GS.Com}_{ck_{\text{GS}}}([\mathbf{z}_m])$, as part of π_z , B_2 extract $[z_1], \dots, [z_m]$. Let $1 \leq j_\alpha, k_\alpha \leq m$ the indices defined by π_1 and π_2 , B returns $([z_1], \dots, [z_m], [\tilde{\mathbf{a}}_1], \dots, [\tilde{\mathbf{a}}_{q_{\text{gen}}-m}])$, where $[\tilde{\mathbf{a}}_1], \dots, [\tilde{\mathbf{a}}_{q_{\text{gen}}-m}]$ are the columns of $[\mathbf{A}']$ which are different from $[\mathbf{a}'_{1,j_\alpha,k_\alpha}], \dots, [\mathbf{a}'_{m,j_\alpha,k_\alpha}]$.

Consider another adversary B_3 against the $\mathcal{Q}_{q_{\text{gen}}}^\top$ -KerMDH assumption defined as follows. B receives as challenge $[\mathbf{A}'] \in \mathbb{G}^{2 \times q_{\text{gen}}}$ and honestly simulates Game_1 embedding $[\mathbf{A}']$ in the user keys in the same way as B_2 . When A outputs $\text{GS.Com}_{ck_{\text{GS}}}([\kappa_1]), \dots, \text{GS.Com}_{ck_{\text{GS}}}([\kappa_m])$, as part of π_κ , B_3 extract $[\kappa_1], \dots, [\kappa_m]$. B_3 attempts to extract a permutation π such that $[z_i] = [\mathbf{a}'_{\pi(i),j_\alpha,k_\alpha}]$ for each $1 \leq i \leq m$. If there is no such permutation, B_3 aborts. Finally, B_3 returns $([0], \dots, [0], [\kappa_{\pi^{-1}(1)}] - [vk_{1,j_\alpha,k_\alpha}], \dots, [\kappa_{\pi^{-1}(m)}] - [vk_{m,j_\alpha,k_\alpha}], [0], \dots, [0])^\top \in \mathbb{G}^{q_{\text{gen}}}$.

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

$$\sum_{i=1}^m [\kappa_i][z_i] = [\mathbf{y}].$$

Perfect soundness of proof π_z implies that

$$\begin{aligned} \sum_{i=1}^m [z_i] &= [\mathbf{x}] \text{ and} \\ [z_{i,2}][1] &= [z_{i,1}][z_{i,1}] \text{ for all } 1 \leq i \leq m. \end{aligned} \quad (3)$$

Perfect soundness of proofs π_1, π_2, π_3 implies, respectively, that

$$\sum_{i=1}^m [\kappa_i][z_i] = \sum_{i=1}^m \mathbf{a}'_{i,j_\alpha,k_\alpha} [vk_{i,j_\alpha,k_\alpha}], \quad (4)$$

$$\sum_{i=1}^m [z_i] = \sum_{i=1}^m [\mathbf{a}'_{i,j_\alpha,k_\alpha}], \quad (5)$$

where $1 \leq j_\alpha, k_\alpha \leq m$ are the indices defined in π_1, π_2 , and that $[vk] = [\kappa_{i_\alpha}]$, for some $1 \leq i_\alpha \leq m$.

Let E the event where $[z_1], \dots, [z_m]$ is a permutation of $[\mathbf{a}'_{1,j_\alpha,k_\alpha}], \dots, [\mathbf{a}'_{m,j_\alpha,k_\alpha}]$, and assume that we are in the case $\neg E$. Equation (5) and imply that

$$\sum_{i=1}^{q_{\text{gen}}-m} [\tilde{\mathbf{a}}_i] + \sum_{i=1}^m [z_i] = \sum_{i=1}^{q_{\text{gen}}} [\mathbf{a}'_i]$$

and, together with equation (3), the fact that $[\tilde{\mathbf{a}}_{i,2}][1] = [\tilde{\mathbf{a}}_{i,1}][\tilde{\mathbf{a}}_{i,1}]$, and that we assume $\neg E$, implies that B_2 breaks the q_{gen} -permutation pairing assumption.

Therefore

$$\Pr[\text{Game}_2 = 1 | \text{err}_2 = 1 \wedge \neg E] \leq \mathbf{Adv}_{q_{\text{gen}}\text{-PPA}}(\mathbf{B}_2).$$

Assume now that we are in the case E . Equation (4) implies that

$$\sum_{i=1}^m (\kappa_i - vk_{\pi(i), j_\alpha, k_\alpha}) \mathbf{a}_{\pi(i), j_\alpha, k_\alpha} = 0.$$

Since $[vk] = [\kappa_{i_\alpha}] \notin R$, then $[\kappa_{i_\alpha}] \neq vk_{i, j_\alpha, k_\alpha}$ for all $1 \leq i \leq m$. Therefore $([0], \dots, [0], [\kappa_{\pi^{-1}(1)}] - [vk_{1, j_\alpha, k_\alpha}], \dots, [\kappa_{\pi^{-1}(m)}] - [vk_{m, j_\alpha, k_\alpha}], [0], \dots, [0]) \neq \mathbf{0}$ and \mathbf{B}_3 breaks the $\mathcal{Q}_{q_{\text{gen}}}^\top$ -KerMDH assumption. We conclude that

$$\Pr[\text{Game}_2 = 1 | \text{err}_2 = 1 \wedge E] \leq \mathbf{Adv}_{\mathcal{Q}_{q_{\text{gen}}}^\top\text{-KerMDH}}(\mathbf{B}_3)$$

The lemma follows from the fact that

$$\begin{aligned} \Pr[\text{Game}_1 = 1 | \text{err}_2 = 1] &= \Pr[\text{Game}_1 = 1 | \text{err}_2 = 1 \wedge \neg E] \Pr[\neg E] + \\ &\quad \Pr[\text{Game}_1 = 1 | \text{err}_2 = 1 \wedge E_1] \Pr[E_1] \\ &\leq \Pr[\text{Game}_1 = 1 | \text{err}_2 = 1 \wedge \neg E] + \\ &\quad \Pr[\text{Game}_1 = 1 | \text{err}_2 = 1 \wedge E_1] \\ &\leq \mathbf{Adv}_{q_{\text{gen}}\text{-PPA}}(\mathbf{B}_2) + \mathbf{Adv}_{\mathcal{Q}_{q_{\text{gen}}}^\top\text{-KerMDH}}(\mathbf{B}_3) \end{aligned}$$

Lemma 2.

$$\Pr[\text{Game}_3 = 1] \geq \frac{1}{q_{\text{gen}}} \Pr[\text{Game}_2 = 1].$$

Proof. It holds that

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

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

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

Lemma 3. *There exist adversaries \mathbf{B}_4 and \mathbf{B}_5 against the unforgeability of the one-time signature scheme and the weak unforgeability of the Boneh-Boyen signature scheme such that*

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

Proof. We construct adversaries B_4 and B_5 as follows.

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

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

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

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

$$q_{\text{sig}} \text{Adv}_{\text{OT}}(B_4) \geq \Pr[\text{Game}_3 = 1|E]$$

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

$$\text{Adv}_{\text{BB}}(B_5) \geq \Pr[\text{Game}_3 = 1|\neg E]$$

References

1. M. Abe, K. Haralambiev, and M. Ohkubo. Group to group commitments do not shrink. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 301–317, Cambridge, UK, Apr. 15–19, 2012. Springer, Heidelberg, Germany. 7
2. M. Abe, M. Kohlweiss, M. Ohkubo, and M. Tibouchi. Fully structure-preserving signatures and shrinking commitments. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 35–65, Sofia, Bulgaria, Apr. 26–30, 2015. Springer, Heidelberg, Germany. 7
3. 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. 8
4. 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. 2,

5. D. Boneh and X. Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. *Journal of Cryptology*, 21(2):149–177, Apr. 2008. 20
6. D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany. 18
7. 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, Wollongong, NSW, Australia, June 29 – July 1, 2015. Springer, Heidelberg, Germany. 1, 6
8. 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. 1, 2, 8
9. 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. 1
10. 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. 1, 6
11. A. González and C. Ràfols. New techniques for non-interactive shuffle and range arguments. In M. Manulis, A.-R. Sadeghi, and S. Schneider, editors, *ACNS 16*, volume 9696 of *LNCS*, pages 427–444, Guildford, UK, June 19–22, 2016. Springer, Heidelberg, Germany. 6
12. C. Gritti, W. Susilo, and T. Plantard. Logarithmic size ring signatures without random oracles. *IET Information Security*, 10(1):1–7, 2016. 1, 6
13. 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. 1
14. 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. 2, 4, 5, 6, 7
15. 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. 3, 8
16. 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>. 3
17. E. Kiltz and H. Wee. Quasi-adaptive NIZK for linear subspaces revisited. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128, Sofia, Bulgaria, Apr. 26–30, 2015. Springer, Heidelberg, Germany.
18. 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. 1

19. B. Libert, T. Peters, M. Joye, and M. Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 514–532, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany.
20. P. Morillo, C. Ràfols, and J. L. Villar. Matrix computational assumptions in multilinear groups. Cryptology ePrint Archive, Report 2015/353, 2015. <http://eprint.iacr.org/2015/353>. 7
21. 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. 4
22. 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. 1
23. 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. 1, 6
24. 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.
25. V. Shoup. Lower bounds for discrete logarithms and related problems. In W. Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266, Konstanz, Germany, May 11–15, 1997. Springer, Heidelberg, Germany. 18

A Our construction in Asymmetric Groups

In this section we construct a natural translation of our protocol to asymmetric groups and prove its security under a natural translation of the PPA assumption to asymmetric groups.

A.1 Asymmetric Bilinear Groups

Let Gen_a be some probabilistic polynomial time algorithm which on input 1^λ , where λ is the security parameter, returns the *group key* which is the description of an asymmetric bilinear group $gk := (q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \mathcal{P}_1, \mathcal{P}_2)$, where $\mathbb{G}_1, \mathbb{G}_2$ and \mathbb{G}_T are groups of prime order q , the elements $\mathcal{P}_1, \mathcal{P}_2$ are generators of $\mathbb{G}_1, \mathbb{G}_2$ respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is an efficiently computable, non-degenerate bilinear map.

Elements in \mathbb{G}_s , are denoted implicitly as $[a]_s := a\mathcal{P}_s$, where $s \in \{1, 2, T\}$ and $\mathcal{P}_T := e(\mathcal{P}_1, \mathcal{P}_2)$. The pairing operation will be written as a product \cdot , that is $[a]_1 \cdot [b]_2 = [a]_1[b]_2 = e([a]_1, [b]_2) = [ab]_T$. 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 $t_{i,j}\mathcal{P}_s$.

A.2 The Permutation Pairing Assumption in Asymmetric Groups

We define a natural variant of the PPA assumption in asymmetric groups, which we call aPPA, and show its hardness in the generic group model

Definition 10 (PPA Assumption in Asymmetric Groups). Let $\mathcal{Q}_m = \underbrace{\mathcal{Q} | \dots | \mathcal{Q}}_{m \text{ times}}$, where concatenation of matrix distributions is defined in the natural way and

$$\mathcal{Q} : \mathbf{a} = \begin{pmatrix} x \\ x^2 \end{pmatrix}, x \leftarrow \mathbb{Z}_q.$$

We say that the m -permutation pairing assumption (m -aPPA) holds relative to Gen_a if for any adversary \mathbf{A}

$$\Pr \left[\begin{array}{l} gk \leftarrow \text{Gen}_a(1^\lambda); \mathbf{A} \leftarrow \mathcal{Q}_m; ([\mathbf{Y}]_1, [\mathbf{Z}]_2) \leftarrow \mathbf{A}(gk, [\mathbf{A}]_1, [(a_{1,1}, \dots, a_{1,m})]_2) : \\ \text{(i) } \sum_{i=1}^m [\mathbf{y}_i]_1 = \sum_{i=1}^m [\mathbf{a}_i]_1, \\ \text{(ii) } \forall 1 \leq i \leq m \ [y_{1,i}]_1 [1]_2 = [1]_1 [z_{1,i}]_2 \text{ and } [y_{2,i}]_1 [1]_2 = [y_{1,i}]_1 [z_i]_2, \\ \text{and } \mathbf{Y} \text{ is not a permutation of the columns of } \mathbf{A} \end{array} \right],$$

where $[\mathbf{Y}] = [(\mathbf{y}_1, \dots, \mathbf{y}_m)]_1$, $[\mathbf{A}]_1 = [(\mathbf{a}_1, \dots, \mathbf{a}_m)]_1 \in \mathbb{G}_1^{2 \times m}$ and $[\mathbf{Z}]_2 = [(z_1, \dots, z_m)]_2 \in \mathbb{G}_2^{1 \times m}$, is negligible in λ .

A.3 Security of the aPPA Assumption in the Generic Group Model

The generic group model is an idealized model for analysing the security of cryptographic assumptions or cryptographic schemes. A proof of security in the generic group model guarantees that no attacker that only uses the algebraic structure of the (bilinear) group, is successful in breaking the assumption/scheme. Conversely, for a generically secure assumption/scheme, a successful attack must exploit the structure of the (bilinear) group that is actually used in the protocol (e.g. a Barreto-Naehring curve in the case of bilinear groups).

We use the natural generalization of Shoup's generic group model [25] to the asymmetric bilinear setting, as it was used for instance by Boneh et al. [6]. In such a model an adversary can only access elements of $\mathbb{G}_1, \mathbb{G}_2$ or \mathbb{G}_T via a query to a group oracle, which gives him a randomized encoding of the queried element. The group oracle must be consistent with the group operations (allowing to query for the encoding of constants in either group, for the encoding of the sum of previously queried elements in the same group and for the encoding of the product of pairs in $\mathbb{G}_1 \times \mathbb{G}_2$).

We prove the following theorem which states generic security of the m -aPPA assumption.

Theorem 2. *If the m -PPA assumption holds in generic symmetric bilinear groups, then the m -aPPA holds in generic asymmetric bilinear groups.*

Proof. Suppose there is an adversary A in the asymmetric generic bilinear group model against the m -PPA assumption. We show how to construct an adversary B against the m -aPPA assumption in the symmetric generic group model.

Adversary B has oracle access to the randomized encodings $\sigma : \mathbb{Z}_q \rightarrow \{0, 1\}^n$, and $\sigma_T : \mathbb{Z}_q \rightarrow \{0, 1\}^n$. It receives as a challenge $\{\sigma(a_{i,j}) : 1 \leq i \leq m, j \in \{1, 2\}\}$.

Adversary B simulates the generic hardness game for A as follows. It defines encodings

$$\xi_1 : \mathbb{Z}_q \rightarrow \{0, 1\}^n, \quad \xi_2 : \mathbb{Z}_q \rightarrow \{0, 1\}^n \text{ and } \xi_T : \mathbb{Z}_q \rightarrow \{0, 1\}^n$$

as $\xi_1 = \sigma, \xi_T = \sigma_T$ and ξ_2 a random encoding function. B keeps a list L_A with the values that have been queried by A to the group oracle. The list is initialized as

$$L_A = \{(A_{i,j}, \xi_1(a_{i,j}), 1), (A_{i,j}, \xi_2(a_{i,j}), 2) : 1 \leq i \leq m, j \in \{1, 2\}\},$$

where $\xi_2(a_{i,j}) \in \{0, 1\}^n$ are chosen uniformly at random conditioned on being pairwise distinct. Adversary B keeps another list L_B with the queries it makes to its own group oracle. The list L_B is initialized as

$$L_B = \{(A_{i,j}, \sigma(a_{i,j}), 1) : 1 \leq i \leq m, j \in \{1, 2\}\}.$$

B keeps also partial function $\psi : \{0, 1\}^n \rightarrow \{0, 1\}^n$ initialized as $\psi(\xi_1(a_{i,j})) = \xi_2(a_{i,j})$, for $1 \leq i \leq m, j \in \{1, 2\}$, and $\psi(s) = \perp$ for any other s .

Each element in the list L_A is a tuple (P, s, μ) , where $P \in \mathbb{Z}_q[A_{1,1}, \dots, A_{\ell,k}]$, $\mu \in \{1, 2, T\}$ and $s = \xi_\mu(P_i(a_{1,1}, \dots, a_{\ell,k}))$. The polynomial P is one of the following:

- a) $P = A_{i,j}$, i.e. it is one of the initial values in the query list L_A or
- b) a constant polynomial or
- c) $P = Q + R$ for some $(Q, t, \mu), (R, u, \mu) \in L_A$ or
- d) $P = QR$ for some $(P, t, 1), (R, u, 2) \in L_A, \mu = T$.

For L_B the same holds except that $\mu \in \{1, T\}$ and except that d) is changed to: d) $P = QR$ for some $(Q, t, 1), (R, u, 1) \in L_B$ and $\mu = T$.

Without loss of generality we can identify the queries of A with pairs (P, μ) meeting the restrictions described above. If $(P, s, \mu) \in L_A$, for some s , it replies with the same answer s .

Else, when B receives a (valid) query (P, μ) , it forwards the query (P, ν) to its own group oracle who replies with s , where $\nu = \mu$, if $\mu \in \{1, T\}$, or $\nu = 1$, if $\mu = 2$. Then (P, s, ν) is appended to L_B and to L_A . In the case $\mu \in \{1, 2\}$, if $\psi(s) = \perp$ it chooses t at random conditioned on being distinct from all other values in the image of ψ and defines $\psi(s) := t$. Then B appends $(P, \psi(s), 2)$ to L_B . Finally B answers A's query with s , if $\mu \in \{1, T\}$, or $\psi(s)$, if $\mu = 2$.

At the onset of the simulation, A will output as a solution to the challenge a pair

$$\mathbf{Y} = \begin{pmatrix} y_{1,1} & \cdots & y_{1,m} \\ y_{2,1} & \cdots & y_{2,m} \end{pmatrix}, \mathbf{Z} = (z_1, \dots, z_m)$$

such that $(P_{i,j}, y_{i,j}, 1), (Q_i, z_i, 2) \in L_A$ for all $1 \leq i \leq n, j \in \{1, 2\}$. If the challenge is successful it must also hold that

$$\xi_T(P_{1,i} \cdot 1) = \xi_T(1 \cdot Q_i) \iff P_{1,i}(a_{1,1}, \dots, a_{2,m}) = Q_i(a_{1,1}, \dots, a_{2,m}) \quad (6)$$

and

$$\begin{aligned} \xi_T(P_{2,1} \cdot 1) &= \xi_T(P_{1,i} Q_i) \\ &\iff P_{2,i}(a_{1,1}, \dots, a_{2,m}) = P_{1,i}(a_{1,1}, \dots, a_{2,m}) \cdot Q_i(a_{1,1}, \dots, a_{2,m}) \end{aligned} \quad (7)$$

Since $a_{1,1}, \dots, a_{2,m}$ remains statistically hidden to the adversary, it must choose $P_{i,1} \equiv Q_i$ and $P_{2,i} \equiv P_{1,i} \cdot Q_i$ since otherwise, by the Schwartz-Zippel lemma, equations (6) and (7) only hold with negligible probability. We conclude that $P_{2,i} = P_{1,i}^2$ and thus **B** might output **Y** which is a solution of the m -PPA assumption.

A.4 Ring Signature in Asymmetric groups

Boneh-Boyen Signatures in Asymmetric Groups The asymmetric Boneh-Boyen signature can be proven wUF-CMA secure under the asymmetric m -strong *Diffie-Hellman* assumption [5], which is described below.

Definition 11 (*m -SDH assumption*). *For any adversary A*

$$\Pr \left[gk \leftarrow \text{Gen}_a(1^\lambda), x \leftarrow \mathbb{Z}_q : A(gk, [x]_1, [x^2]_1, \dots, [x^m]_1, [x]_2) = (c, \left[\frac{1}{x+c} \right]_1) \right]$$

is negligible in λ .

The Boneh-Boyen signature scheme is described below.

BB.KeyGen: Given a group key gk , pick $vk \leftarrow \mathbb{Z}_q$. The secret/public key pair is defined as $(sk, [vk]_2) := (vk, [vk]_2)$.

BB.Sign: Given a secret key $sk \in \mathbb{Z}_q$ and a message $m \in \mathbb{Z}_q$, output the signature $[\sigma]_1 := \left[\frac{1}{sk+m} \right]_1$. In the unlikely case that $sk + m = 0$ we let $[\sigma]_1 := [0]_1$.

BB.Ver: On input the verification key $[vk]_2$, a message $m \in \mathbb{Z}_q$, and a signature $[\sigma]_1$, verify that $[\sigma]_1 [m + vk]_2 = [1]_T$.

Our construction

CRSGen(gk): Pick a perfectly hiding CRS for the Groth-Sahai proof system crs_{GS} , and a CRS for the proof of the $\Theta(\sqrt{n})$ proof of membership in a set crs_{set} of Chandran et al., and output $\rho := (gk, \text{crs}_{\text{GS}}, \text{crs}_{\text{set}})$.

KeyGen(ρ): Pick $\mathbf{a} \leftarrow \mathcal{Q}$ and $(sk, [vk]_2) \leftarrow \text{BB.KeyGen}(gk)$, compute $[\mathbf{a}]_1$ and $[b]_2 := [a_{1,1}]_2$ and then erase \mathbf{a} . The secret key is sk and the verification key is $\mathbf{vk} := ([vk]_2, [\mathbf{a}]_1, [b]_2, \mathbf{a}[vk]_2)$.

- $\text{Sign}_{\rho, sk}(m, R)$: 1. Compute $(sk_{\text{ot}}, vk_{\text{ot}}) \leftarrow \text{OT.KeyGen}(gk)$ and $\sigma_{\text{ot}} \leftarrow \text{OT}.$
 $\text{Sign}_{sk_{\text{ot}}}(m, R).$
2. Compute $[c]_2 := \text{GS.Com}_{ck}([vk]_2; \mathbf{r}), \mathbf{r} \leftarrow \mathbb{Z}_q^2, [\sigma]_1 \leftarrow \text{BB.Sign}_{sk}(vk_{\text{ot}}),$
 $[\mathbf{d}]_1 := \text{GS.Com}_{ck}([\sigma]_1; \mathbf{s}), \mathbf{s} \leftarrow \mathbb{Z}_q^3,$ and a GS proof π_{GS} that $\text{BB.Ver}_{[vk]_2}([\sigma]_1, vk_{\text{ot}}) = 1$ (which can be expressed as a set of pairing product equations).
 3. Parse R as $\{\mathbf{vk}_{1,1,1}, \dots, \mathbf{vk}_{m,m,m}\},$ where $m := \sqrt[3]{n}, n := |R|,$ and let $\alpha = (i_\alpha - 1)m^2 + (j_\alpha - 1)m + k_\alpha$ the index of \mathbf{vk} in $R.$ Define the sets $S = \{\sum_{i=1}^m [\mathbf{a}_{i,1,1}]_1, \dots, \sum_{i=1}^m [\mathbf{a}_{i,m,m}]_1\}$ and $S' = \{\sum_{i=1}^m \mathbf{a}_{i,1,1}[vk_{i,1,1}]_2, \dots, \sum_{i=1}^m \mathbf{a}_{i,m,m}[vk_{i,m,m}]_2\}.$
 4. Let $[\mathbf{x}]_1 := \sum_{i=1}^m [\mathbf{a}_{i,j_\alpha,k_\alpha}]_1$ and $[\mathbf{y}]_2 = \sum_{i=1}^m \mathbf{a}_{i,j_\alpha,k_\alpha}[vk_{i,j_\alpha,k_\alpha}]_2.$ Compute GS commitments to $[\mathbf{x}]_1$ and $[\mathbf{y}]_2,$ and compute proofs π_1 and π_2 that they belong to S and $S',$ 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 $[\mathbf{x}]_1$'s and $[\mathbf{y}]_2$'s position in S and S' respectively.
 5. Let $[\kappa_1]_2 := [vk_{1,j_\alpha,k_\alpha}]_2, \dots, [\kappa_m]_2 := [vk_{m,j_\alpha,k_\alpha}]_2, [\mathbf{z}_1]_1 := [\mathbf{a}_{1,j_\alpha,k_\alpha}]_1,$
 $\dots, [\mathbf{z}_m]_1 := [\mathbf{a}_{m,j_\alpha,k_\alpha}]_1,$ and $[z'_1]_2 := [b_{1,j_\alpha,k_\alpha}]_2, \dots, [z'_m]_2 := [b_{m,j_\alpha,k_\alpha}]_2.$ Compute GS commitments to all these values and compute a GS proof π_κ that $\sum_{i=1}^m [\mathbf{z}_i]_1 [\kappa_i]_2 = [1]_1 [\mathbf{y}]_2$ and a GS proof π_z that $\sum_{i=1}^m [\mathbf{z}_i]_1 = [\mathbf{x}]_1,$
 $[z_{1,i}]_1 [1]_2 = [1]_1 [z'_i]_2,$ and $[z_{2,i}]_1 [1]_2 = [z_{1,i}]_1 [z'_i]_2$ for each $1 \leq i \leq m.$
 6. Compute a proof π_3 that $[vk]_2$ belongs to $S_3 = \{[\kappa_1]_2, \dots, [\kappa_m]_2\}.$
 7. Return the signature $\sigma := (vk_{\text{ot}}, \sigma_{\text{ot}}, [c]_2, [\mathbf{d}]_1, \pi_1, \pi_2, \pi_3, \pi_\kappa, \pi_z).$ (GS proofs include commitments to variables).
- $\text{Verify}_{\rho,R}(m, \sigma)$: Verify the validity of the one-time signature and of all the proofs. Return 0 if any of these checks fails and 1 otherwise.

The following theorem states the security of our scheme. Its proof is just a syntactic translation of the proof on the symmetric case and we omit it.

Theorem 3. *The scheme presented in this section is a ring signature scheme with perfect correctness, perfect anonymity and computational unforgeability under the m -permutation pairing assumption, the \mathcal{Q}_m^\top -KerMDH assumption, the SXDH assumption, and the assumption that the one-time signature and the Boneh-Boyen signature are unforgeable. Concretely, for any adversary \mathbf{A} against the unforgeability of the scheme, there exist adversaries $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{B}_4, \mathbf{B}_5$ such that*

$$\begin{aligned} \mathbf{Adv}(\mathbf{A}) \leq & \mathbf{Adv}_{\mathcal{L}_1\text{-MDDH}}(\mathbf{B}_1) + \mathbf{Adv}_{q_{\text{gen}}\text{-PPA}}(\mathbf{B}_2) + \mathbf{Adv}_{\mathcal{Q}_m^\top\text{-KerMDH}}(\mathbf{B}_3) + \\ & q_{\text{gen}}(q_{\text{sig}} \mathbf{Adv}_{\text{OT}}(\mathbf{B}_4) + \mathbf{Adv}_{\text{BB}}(\mathbf{B}_5)), \end{aligned}$$

where q_{gen} and q_{sig} are, respectively, upper bounds for the number of queries that \mathbf{A} makes to its VKGen and Sign oracles.