A Ring Signature of size $O(\sqrt[3]{n})$ 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), allows 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 anomimity, i.e. the signatures hides the actual signer. In terms of efficiency, in all constructions the size of the signature depends on the number of members of the ring. Indeed, the most efficient constructions require signatures of size $O(\log n)$, where n is the size of the ring (Groth and Kohlweiss EUROCYPT 2015, Libert et al. EUROCRYPT 2016). However, both constructions 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 signatgure of size $O(\sqrt{n})$.
In this work we construct a ring signature of size $O(\sqrt[3]{n})$ 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), which is a non-falsifiable assumption in bilinear groups.

1 Introduction

Ring signatures, introduced by Rivest, Shamir and Tauman, [18], allow to anonymously sign a message on behalf of a ring of users $P_1, \ldots, P_n$, only if the signer belongs to the ring. Although there are other cryptographic schemes that provides similar guarantees (e.g. 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.

While the more efficient constructions have signature size logarithmic in the size of the ring [11,15], all of them rely on the random oracle model. Without random oracles all the constructions have signatures of size linear in the size of the ring, being the the sole exception the $\Theta(\sqrt{n})$ ring signature of Chandran et al. [6]. 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 [17] and by González et al. [8]). Although some previous works claim to construct signatures of constant [5] or logarithmic [10] 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 whose signature size is asymptotically smaller than Chandran et al.'s. Specifically, our ring signature is of size $\Theta(\sqrt[3]{n})$. The security of our construction relies on a security assumption – the permutation pairing assumption – introduced by Groth and Lu [12] 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 to be generically hard 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 groups provided the natural translation to asymmetric groups of the Groth and Lu's assumption given in Appendix A.

1.1 Chandran et al.'s Costruction

Our scheme follows the ring signature of Chandran et al. Given a Boneh-Boyen signature scheme [3], where the secret/verification keys are of the form $(sk, [vk])$, $[vk]$ is an element of a symmetric bilinear group $\mathbb{G}$ (of order q) whose discrete logarithm is vk, and sk is equal to vk. The validity of a Boneh-Boyen signature $[\sigma] \in \mathbb{G}$ of a message $m \in \mathbb{Z}_q$ under th verficiation $[vk]$ corresponds to the satisfiability of an equation $\mathsf{eq}([\sigma], [vk], m)$. Therefore, one can prove possession of a valid signature without revealing the signature using Groth-Sahai proofs.[13][1][2] Given also a one-time signature scheme, the signature of the message m for a ring $R = \{[vk_1], \ldots, [vk_n]\}$ is computed as follows:

a) Pick a one-time signature key $(sk_{\mathsf{ot}}, vk_{\mathsf{ot}})$, sign m with sk_{ot}, and sign vk_{ot} with sk.
b) Show possesion 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 $\Theta(\sqrt[3]{n})$ of c) which we describe 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 $i, j \in [m]$.

[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. [14]). 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.

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 is selected. 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. $[\kappa_1] := [vk_{1,j_\alpha}], \ldots, [\kappa_m] := [vk_{m,j_\alpha}]$.

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 $\sum_{i=1}^m = 1$,
iii. $[\kappa_1] = \sum_{j=1}^m b_j[vk_{1,j}], \ldots, [\kappa_m] = \sum_{j=1}^m b_j[vk_{m,j}]$,
iv. $[vk_\alpha] = \sum_{i=1}^m b'_i[\kappa_i]$.

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

1.2 Our Construction

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

$$S := \{[\boldsymbol{s}_1], \ldots, [\boldsymbol{s}_{n^{2/3}}]\} := \left\{ \sum_{i\in[m]} [\boldsymbol{a}_{i,1,1}], \ldots, \sum_{i\in[m]} [\boldsymbol{a}_{i,m,m}] \right\} \text{ and}$$

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

The prover commits to $[\boldsymbol{x}] = [\boldsymbol{s}_\mu]$ and $[\boldsymbol{y}] = [\boldsymbol{s}'_{\mu'}]$, for $\mu = \mu' = (j_\alpha - 1)m + k_\alpha$, and shows, using (twice) the set-membership proof of Chandran et al., that $[\boldsymbol{x}] \in S$ and that $[\boldsymbol{y}] \in S'$, The prover also needs to assure that $\mu = \mu'$, which can be done reutilizing the commitment to μ (in fact to its binary representation) used in the proof that $[\boldsymbol{x}] \in S$ in the proof that $[\boldsymbol{y}] \in S'$. 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 commited to elements $[\boldsymbol{x}] = \sum_{i\in[m]}[\boldsymbol{a}_{i,j_\alpha,k_\alpha}]$ and $[\boldsymbol{y}] = \sum_{i\in[m]} \boldsymbol{a}_{i,j_\alpha,k_\alpha}[vk_{i,j_\alpha,k_\alpha}]$, it additionally commits to $[\kappa_1] := [vk_{1,j_\alpha,k_\alpha}], \ldots,$ $[\kappa_m] := [vk_{m,j_\alpha,k_\alpha}]$ and $[\boldsymbol{z}_1] := [\boldsymbol{a}_{1,j_\alpha,k_\alpha}], \ldots, [\boldsymbol{z}_m] := [\boldsymbol{a}_{m,j_\alpha,k_\alpha}]$. The prover now gives a proof that

$$\sum_{i\in[m]} [\boldsymbol{z}_i][\kappa_i] = [\boldsymbol{y}][1]. \tag{1}$$

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

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

Then $\kappa_1, \ldots, \kappa_m$ is a permutation of $vk_{1,j_\alpha,k_\alpha}, \ldots, vk_{m,j_\alpha,k_\alpha}$ (the same defined by $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_m$), unless $(\kappa_{\pi^{-1}(1)} - vk_{1,j_\alpha,k_\alpha}), \ldots, \kappa_{\pi^{-1}(m)} - vk_{m,j_\alpha,k_\alpha}))^\top$ is in the kernel of $\mathbf{A}$. However, this is in general a hard problem and corresponds to the $\mathcal{Q}_m^\top$-KerMDH assumption in the terminology of Morillo et al. [16]. For the distribution $\mathcal{Q}$ (defined later), Groth and Lu showed the hardness of this problem in the generic group model [12].

Finally, the prover commits also to $b_1, \ldots, b_m \in \{0, 1\}$ such that $b_i = 1$ iff $i = i_\alpha$ and shows that $[vk_\alpha] = \sum_{i=1}^m b_i[\kappa_i]$. This implies that $[vk_\alpha] = [vk_{i_\alpha,j_\alpha,k_\alpha}]$.

It is only left the to show that $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_m$ is a permutation of $\boldsymbol{a}_{1,j_\alpha,k_\alpha}, \ldots, \boldsymbol{a}_{m,j_\alpha,k_\alpha}$. To do so we will use the following assumption introduced by Groth and Lu [12].

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

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

We say that the m-permutation pairing assumption holds relative to Gen_s *if for any adversary* A

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

where $[\mathbf{Z}] = [(\boldsymbol{z}_1, \ldots, \boldsymbol{z}_m)], [\mathbf{A}] = [(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)] \in \mathbb{G}^{2\times m}$, *is negligible in k.*

If the prover additionally proves that equations (i) and (ii) from definition 1 are satisfied for $\mathbf{A} := (\boldsymbol{a}_{1,j_\alpha,k_\alpha}, \ldots, \boldsymbol{a}_{m,j_\alpha,k_\alpha})$, 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 $\mathbf{A}$, for some permutation $\pi \in S_m$.

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 $S = \{\sum_{i\in[m]} \boldsymbol{a}_{i,1,1,1}[vk_{i,1,1,1}], \ldots, \sum_{i\in[m]} \boldsymbol{a}_{i,m,m,m}[vk_{i,m,m,m}]\}$ and $S' = \{\sum_{i\in[m]}[\boldsymbol{a}_{i,1,1,1}], \ldots, \sum_{i\in[m]}[\boldsymbol{a}_{i,m,m,m}]\}$, and then prove that they belong to the respective sets with the 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 $([vk], \boldsymbol{a}[vk], [\boldsymbol{a}])$.

Erasures. In the security proof we need to embed an instance of the m-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 $\boldsymbol{a}$ and is incompatible with the m-permutation pairing assumption. Since is not clear how to obliviously sample $[x]$ and $[x^2]$ and we can guess the set of corrupted parties only with negligible probability, we are forced to use erasures. That is, after sampling $\boldsymbol{a} \leftarrow \mathcal{Q}$ and computing $[\boldsymbol{a}]$, the key generation algorithm erases $\boldsymbol{a}$.

Getting rid of the non-standard assumptions. Gonzalez et al. [9] modify the Groth and Lu's proof of correctness of a shuffle [12] to get rid of the permutation pairing assumption and the pairing product equation. They showed that the statement "$[\boldsymbol{z}_1], \ldots, [\boldsymbol{z}_m]$ is a permutation of $[\boldsymbol{a}_1], \ldots, [\boldsymbol{a}_m]$" can be showed with a proof that $[\boldsymbol{z}_1], \ldots, [\boldsymbol{z}_m] \in \{[\boldsymbol{a}_1], \ldots, [\boldsymbol{a}_m]]\}$ and that $\sum_{i=1}^m [\boldsymbol{z}_i] = \sum_{i=1}^m [\boldsymbol{a}_i]$. Gonzalez et al. construct a $O(m)$ proof that $[\boldsymbol{z}_1], \ldots, [\boldsymbol{z}_m] \in \{[\boldsymbol{a}_1, \ldots, [\boldsymbol{a}_m]]\}$ 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 $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m \leftarrow \mathbb{Z}_q^2$.

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

We note that we are using features of the permutation pairing assumption that where ignored by Gonzalez et al. and by Groth and Lu. Indeed, we used the fact that $\sum_{i=1}^m [\boldsymbol{a}_{i,j_\alpha,k_\alpha}]$ "defines" the set $S_{j_\alpha,k_\alpha} := \{[\boldsymbol{a}_{1,j_\alpha,k_\alpha}], \ldots, [\boldsymbol{a}_{m,j_\alpha,k_\alpha}]\}$ 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 $O(\sqrt[3]{n})$ group elements.

Relation to [8]. Our construction is similar to the set membership proof from [8, Appendix D.2]. However, the proof system from [8] 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 [5]. 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. [18].

Gritti et al. claim to construct a logarithmic ring signature in the standard model [10]. However, their construction is completely flawed as explained below. In page 12, Gritti et al. define $v_{b_i} := v_{b_1 \cdots b_i *}$, where $b_1 \cdots b_i *$ is the set of all bit-strings of size $d := \log n$ whose prefix is $b_1 \cdots b_i$. 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 known to not exist [1], its representation requires at least 2^{d-i} group elements . Since commitments $D_{b_0}, \ldots, D_{b_d}$ 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.[3]

2 Preliminaries

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 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ 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 $t_{i,j}\mathcal{P}_s$. We denote by $|\mathbb{G}_s|$ the bit-size of the elements of $\mathbb{G}_s$.

$\mathbf{I}_{n\times n}$ refers to the identity matrix in $\mathbb{Z}_q^{n\times n}$, $\mathbf{0}_{m\times n}$ and $\mathbf{1}_{m\times n}$ the all-zero and all-one matrices in $\mathbb{Z}_q^{m\times n}$, respectively, and $\boldsymbol{e}_i^n$ the ith element of the canonical basis of $\mathbb{Z}_q^n$ (simply $\mathbf{I}$, $\mathbf{0}$, $\mathbf{1}$, and $\boldsymbol{e}_i$, respectively, if m and n are clear from the context). Given some matrices $\mathbf{A} \in \mathbb{Z}_q^{m\times t}, \mathbf{A}_1 \in \mathbb{Z}_q^{m_1\times t}, \ldots, \mathbf{A}_n \in \mathbb{Z}_q^{m_n\times n}$, we define the operations

$$\boldsymbol{A}_1 \oplus \ldots \oplus \boldsymbol{A}_n := \begin{pmatrix} \boldsymbol{A}_1 \\ \vdots \\ \boldsymbol{A}_n \end{pmatrix} \qquad \mathbf{A}^n := \begin{pmatrix} \mathbf{A} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & \mathbf{A} \end{pmatrix}.$$

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

2.1 Groth-Sahai Proofs in the 2-Lin Instantiation

The Groth Sahai (GS) proof system allows to prove satisfiability of a set of quadratic equations in a bilinear group. The admissible equation types must be in the following form:

$$\sum_{j=1}^{m_y} f(\alpha_j, \mathsf{y}_j) + \sum_{i=1}^{m_x} f(\mathsf{x}_i, \beta_i) + \sum_{i=1}^{m_x}\sum_{j=1}^{m_y} f(\mathsf{x}_i, \gamma_{i,j}\mathsf{y}_j) = t, \tag{2}$$

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, one first commits to solutions of equation (2) using the GS commitments, and the computes a proof that the commited values satisfies (2).

Following Groth and Sahai's work [13], in symmetric groups and using the 2-Lin assumption, GS commitments are vectors in $\mathbb{G}^3$ of the form

$$\mathsf{GS.Com}_{ck}([x]; \boldsymbol{r}) = \begin{pmatrix} [0] \\ [0] \\ [x] \end{pmatrix} + r_1[\boldsymbol{u}_1] + r_2[\boldsymbol{u}_2] + r_3[\boldsymbol{u}_3]$$

where $ck := ([\boldsymbol{u}_1]||[\boldsymbol{u}_2]||[\boldsymbol{u}_3])$, $(\boldsymbol{u}_2|\boldsymbol{u}_3) \leftarrow \mathcal{L}_2$ and $\boldsymbol{u}_1 := w_1\boldsymbol{u}_2 + w_2\boldsymbol{u}_3$ in the perfectly binding setting, and $\boldsymbol{u}_1 := w_1\boldsymbol{u}_2 + w_2\boldsymbol{u}_3 - \boldsymbol{e}_3$ in the perfectly hiding setting, for $w_1, w_2 \leftarrow \mathbb{Z}_q$. Security of GS commitments follows from the hardness of the 2-Lin assumption in symmetric groups.

2.2 Ring Signature Definition

We follow Chandran et al.'s definitions [6], 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 2 (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.*

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

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

Definition 4 (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 any non-uniform polynomial time 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 th security parameter, 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 reveled 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 5 (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 Boneh-Boyen Signatures

Boneh and Boyen described a short signature – each signature consists of only one group element – which is UF-CMA without random oracles [3]. Interestingly, 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 (as done in Chandran et al.'s ring signature and our ring signature).

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

Definition 6 (m-SDH assumption). *For any adversary* A

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

is negligible in λ.

The Boneh-Boyen signature scheme is described below.

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

$\mathsf{BB.Sign}$**:** 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 $[\sigma] := [0]$.

$\mathsf{BB.Ver}$**:** 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

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

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

$\mathsf{Sign}_{\rho,sk}(m, R)$**:**

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 $[\boldsymbol{c}] := \mathsf{GS.Com}_{ck}([vk]; r)$, $r \leftarrow \mathbb{Z}_q$, $[\sigma] \leftarrow \mathsf{BB.Sign}_{sk}(vk_{\mathsf{ot}})$, $[\boldsymbol{d}] := \mathsf{GS.Com}_{ck}([\sigma]; s)$, $s \leftarrow \mathbb{Z}_q$, and a GS proof π_{GS} that $\mathsf{BB.Ver}_{[vk]}([\sigma], [vk_{\mathsf{ot}}]) = 1$ (which can be expressed as a set of pairing product equations).
3. Parse R as $\{\boldsymbol{vk}_{(1,1,1)}, \ldots, \boldsymbol{vk}_{(m,m,m)}\}$, where $m := \sqrt[3]{n}$, $n := |R|$, and let $\alpha = (i_\alpha, j_\alpha, k_\alpha)$ the index of $\boldsymbol{vk}$ in R. Define the sets $S = \{\sum_{i\in[m]}[\boldsymbol{a}_{(i,1,1)}], \ldots, \sum_{i\in[m]}[\boldsymbol{a}_{(i,m,m)}]\}$ and $S' = \{\sum_{i\in[m]} \boldsymbol{a}_{(i,1,1)}[vk_{(i,1,1)}], \ldots, \sum_{i\in[m]} \boldsymbol{a}_{(i,m,m)}[vk_{(i,m,m)}]\}$.

4. Let $[\boldsymbol{x}] := \sum_{i\in[m]}[\boldsymbol{a}_{(i,j_\alpha,k_\alpha)}]$ and $[\boldsymbol{y}] = \sum_{i\in[m]}\boldsymbol{a}_{(i,j_\alpha,k_\alpha)}[vk_{(i,j_\alpha,k_\alpha)}]$. Compute GS commitments to $[\boldsymbol{x}]$ and $[\boldsymbol{y}]$, 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 $b_1,\ldots,b_m$ and $b'_1,\ldots,b'_m$, used in the set-membership proof of Chandran et al., which define $[\boldsymbol{x}]$'s and $[\boldsymbol{y}]$'s position in S and S' respectively.
5. Let $[\kappa_1] := [vk_{(1,j_\alpha,k_\alpha)}],\ldots,[\kappa_m] := [vk_{(m,j_\alpha,k_\alpha)}]$ and $[\boldsymbol{z}_1] := [\boldsymbol{a}_{(1,j_\alpha,k_\alpha)}]$, $\ldots,[\boldsymbol{z}_m] := [\boldsymbol{a}_{(m,j_\alpha,k_\alpha)}]$. Compute GS commitments to $[\kappa_1],\ldots,[\kappa_m]$ and $[\boldsymbol{z}_1],\ldots,[\boldsymbol{z}_m]$, and GS proof π_κ that $\sum_{i\in[m]}[\kappa_i][\boldsymbol{z}_i] = [\boldsymbol{y}][1]$ and a GS proof π_z that $\sum_{i\in[m]}[\boldsymbol{z}_i] = [\boldsymbol{x}]$ and $[z_{2,i}][1] = [z_{1,i}][z_{1,i}]$ for each $i\in[m]$.
6. Compute a proof π_3 that $[vk]$ belongs to $S_3 = \{[\kappa_1],\ldots,[\kappa_m]\}$.
7. Return the signature $\boldsymbol{\sigma} := (vk_{\mathsf{ot}},\sigma_{\mathsf{ot}},[\boldsymbol{c}],[\boldsymbol{d}],\pi_1,\pi_2,\pi_3,\pi_\kappa,\pi_z)$. (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.

Theorem 1. *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* 2-Lin *assumption, and the assumption that the one-time signature and the Boneh-Boyen signature are unforgeable. Concretely, for any 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*

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

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 and perfect zero-knowledge proofs, information theoretically hiding any information about $\boldsymbol{vk}$.

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

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.
- At the beginning, variables err_2 and err_3 are initialized to 0, and a random index i^* is chosen from $[q_{\mathsf{gen}}]$.

- On a query to $\mathsf{Corrupt}$ with argument i, if $i = i^*$ set $\mathsf{err}_3 \leftarrow 1$ and proceed as in Game_2.
- Let (m, R, σ) the purported forgery output by A. If $[vk]$, the opening of commitment $[\boldsymbol{c}]$ from σ, is not equal to $[vk_{i^*}]$, set $\mathsf{err}_3 \leftarrow 1$. If $[vk] \notin R$, 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 variables err_2 and err_3 are just dummy variables, the only difference between Game_0 and Game_1 comes from the Groth-Sahai CRS distribution. It follows that there is an adversary B_1 against DLin such that $|\Pr[\mathsf{Game}_0 = 1] - \Pr[\mathsf{Game}_1 = 1]| \leq \mathbf{Adv}_{\mathcal{L}_2\text{-}\mathsf{MDDH}}(\mathsf{B}_1)$.

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

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

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.

We construct an adversary B_2 against the q_{gen}-permutation pairing assumption as follows. B_2 receives as challenge $[\mathbf{A}'] \in \mathbb{G}^{2 \times q_{\mathsf{gen}}}$ and honestly simulates Game_2 with the following exception. On the i th query of A to VKGen sets $[\boldsymbol{a}_i]$ as the i th column of $[\mathbf{A}']$. When A outputs $\mathsf{GS.Com}_{ck_{\mathsf{GS}}}([\boldsymbol{z}_1]), \ldots, \mathsf{GS.Com}_{ck_{\mathsf{GS}}}([\boldsymbol{z}_m])$, as part of π_z, B_2 extract $[\boldsymbol{z}_1], \ldots, [\boldsymbol{z}_m]$. Let $j_\alpha, k_\alpha \in [m]$ the indices defined by π_1 and π_2, B returns $([\boldsymbol{z}_1], \ldots, [\boldsymbol{z}_m], [\tilde{\boldsymbol{a}}_1], \ldots, [\tilde{\boldsymbol{a}}_{q_{\mathsf{gen}}-m}])$, where $[\tilde{\boldsymbol{a}}_1], \ldots, [\tilde{\boldsymbol{a}}_{q_{\mathsf{gen}}-m}]$ are the columns of $[\mathbf{A}']$ which are different from $[\boldsymbol{a}'_{(1,j_\alpha,k_\alpha)}], \ldots, [\boldsymbol{a}'_{(m,j_\alpha,k_\alpha)}]$.

We construct an adversary B_3 against the $\mathcal{Q}^{\top}_{q_{\mathsf{gen}}}$-KerMDH assumption as follows. B receives as challenge $[\mathbf{A}'] \in \mathbb{G}^{2 \times q_{\mathsf{gen}}}$ and honestly simulates Game_2 embedding $[\mathbf{A}']$ in the user keys (in the same way as B_2). When A outputs $\mathsf{GS.Com}_{ck_{\mathsf{GS}}}([\kappa_1]), \ldots, \mathsf{GS.Com}_{ck_{\mathsf{GS}}}([\kappa_m])$, as part of π_κ, B_3 extract $[\kappa_1], \ldots, [\kappa_m]$. B_3 attempts to extract a permutation π such that $[\boldsymbol{z}_i] = [\boldsymbol{a}'_{(\pi(i),j_\alpha,k_\alpha)}]$ for each $i \in [m]$. If there is no such permutation, B_3 aborts. Finally, B_3 returns $([0], \ldots, [0], [\kappa_{\pi^{-1}(1)}] - [vk_{(1,j_\alpha,k_\alpha)}], \ldots, [\kappa_{\pi^{-1}(m)}] - [vk_{(m,j_\alpha,k_\alpha)}], [0], \ldots)^{\top} \in \mathbb{G}^{q_{\mathsf{gen}}}$.

Let E the event where $[\boldsymbol{z}_1], \ldots, [\boldsymbol{z}_m]$ is a permutation of $[\boldsymbol{a}'_{(1,j_\alpha,k_\alpha)}], \ldots, [\boldsymbol{a}'_{(m,j_\alpha,k_\alpha)}]$, and assume that we are in the case $\neg E$. Soundness of proof π_κ implies that

$$\sum_{i \in [m]} [\kappa_i][\boldsymbol{z}_i] = [\boldsymbol{y}].$$

Soundness of proof π_z implies that

$$\sum_{i\in[m]} [\boldsymbol{z}_i] = [\boldsymbol{x}] \text{ and}$$
$$[z_{i,2}][1] = [z_{i,1}][z_{i,1}] \text{ for all } i \in [m]. \tag{3}$$

Soundness of proofs π_1, π_2, π_3 implies, respectively, that there exist $j_\alpha, k_\alpha \in [m]$ such that

$$\sum_{i\in[m]} [\kappa_i][\boldsymbol{z}_i] = \sum_{i\in[m]} \boldsymbol{a}'_{(i,j_\alpha,k_\alpha)}[vk_{(i,j_\alpha,k_\alpha)}], \tag{4}$$
$$\sum_{i\in[m]} [\boldsymbol{z}_i] = \sum_{i\in[m]} [\boldsymbol{a}'_{(i,j_\alpha,k_\alpha)}],, \tag{5}$$

and that $[vk] = [\kappa_{i^*}]$, for some $i^* \in [m]$.

Equation (5) and imply that

$$\sum_{i\in[q_{\mathsf{gen}}-m]} [\tilde{\boldsymbol{a}}_i] + \sum_{i\in[m]} [\boldsymbol{z}_i] = \sum_{i\in[q_{\mathsf{gen}}]} [\boldsymbol{a}'_i]$$

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

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

Assume now that we are in the case E. Therefore, equation (4) implies that

$$\sum_{i\in[m]} (\kappa_i - vk_{(\pi(i),j_\alpha,k_\alpha)})\boldsymbol{a}_{(\pi(i),j_\alpha,k_\alpha)} = 0.$$

Since $[vk] = [\kappa_{i^*}] \notin R$, then $[\kappa_{i^*}] \neq vk_{(i,j_\alpha,k_\alpha)}$ for all $i \in [m]$. Therefore $([0],\ldots,[0],[\kappa_{\pi^{-1}(1)}] - [vk_{(1,j_\alpha,k_\alpha)}],\ldots,[\kappa_{\pi^{-1}(m)}] - [vk_{(m,j_\alpha,k_\alpha)}]) \neq [\mathbf{0}]$ and B_3 breaks the $\mathcal{Q}^{\top}_{q_{\mathsf{gen}}}$-$\mathsf{KerMDH}$ assumption. We conclude that

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

The lemma follows from the fact that

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

Lemma 2.

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

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 $\mathsf{err}_2 = 0$ given $\mathsf{Game}_2 = 1$ is the probability that the q_{cor} calls to $\mathsf{Corrupt}$ do not abort and that $[vk] = [vk_{i^*}]$. 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 $[vk] = [vk_{i^*}]$ is $1/(q_{\mathsf{gen}} - q_{\mathsf{cor}})$, since $[vk] \in R$ (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 3. *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 $vk^{\dagger}_{\mathsf{ot}}$ and simulates Game_3 honestly but with the following differences. It chooses a random $j^* \in [q_{\mathsf{sig}}]$ 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 signature. Finally, when A outputs its purported forgery $(m, R, (\sigma_{\mathsf{ot}}, vk_{\mathsf{ot}}, \ldots))$, B_4 it 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 $(sk^i_{\mathsf{ot}}, vk^i_{\mathsf{ot}}) \leftarrow \mathsf{OT.KeyGen}(gk)$, for each $i \in [q_{\mathsf{sig}}]$ and queries its signing oracle on $(vk^1_{\mathsf{ot}}, \ldots, vk^{q_{\mathsf{sig}}}_{\mathsf{ot}})$ obtaining $[\sigma_1], \ldots, [\sigma_{q_{\mathsf{sig}}}]$. When A queries the signing oracle on input (i^*, m, R), B_5 computes an honest signature but replaces vk_{ot} with vk^i_{ot} and $[\sigma]$ with $[\sigma_i]$, and then adds 1 to i. Finally, when A outputs its purported forgery $(m, R, (\sigma_{\mathsf{ot}}, vk_{\mathsf{ot}}, [\boldsymbol{c}], [\boldsymbol{d}], \ldots))$, it extracts $[\sigma]$ from $[\boldsymbol{d}]$ 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

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

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

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

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

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

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. 6
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. 7
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. 2, 9
4. 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. 16
5. 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, 5
6. 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, 7
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. 1
8. 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, 5
9. 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. 5
10. C. Gritti, W. Susilo, and T. Plantard. Logarithmic size ring signatures without random oracles. *IET Information Security*, 10(1):1–7, 2016. 1, 6
11. 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
12. 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
13. 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. 2, 7

14. 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`. 2
15. 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
16. 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
17. 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
18. 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
19. 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. 16

A The Permutation Pairing Assumption in Asymmetric Groups

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

Definition 7 (PPA Assumption in Asymmetric Groups). *Let* $\mathcal{Q}_m = \underbrace{\mathcal{Q}|\ldots|\mathcal{Q}}_{m \text{ times}}$*, where concatenation of matrix distributions is defined in the natural way and*

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

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

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

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

A.1 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 [19] to the asymmetric bilinear setting, as it was used for instance by Boneh et al. [4]. 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 $\sigma : \mathbb{Z}_q \to \{0,1\}^n$, and $\sigma_T : \mathbb{Z}_q \to \{0,1\}^n$. 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

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

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

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

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

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

B keeps also partial function $\psi : \{0,1\}^n \to \{0,1\}^n$ 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 $P \in \mathbb{Z}_q[A_{1,1}, \ldots, A_{\ell,k}]$, $\mu \in \{1, 2, T\}$ and $s = \xi_\mu(P_i(a_{1,1}, \ldots, a_{\ell,k}))$. 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 $(Q, t, \mu), (R, u, \mu) \in L_{\mathsf{A}}$ or
d) $P = QR$ for some $(P, t, 1), (R, u, 2) \in L_{\mathsf{A}}$, $\mu = T$.

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

Without loss of generality we can identify the queries of A with pairs (P, μ) meeting the restrictions described above. If $(P, s, \mu) \in L_{\mathsf{A}}$, 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

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

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

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

and

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

Since $a_{1,1}, \ldots, a_{2,m}$ 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 $\mathbf{Y}$ which is a solution of the m-PPA assumption.