Further Lower Bounds for Structure-Preserving Signatures in Asymmetric Bilinear Groups

Essam Ghadafi

University of the West of England, Bristol, UK
essam.ghadafi@uwe.ac.uk

Abstract. Structure-Preserving Signatures (SPSs) are a useful tool for the design of modular cryptographic protocols. Recent series of works have shown that by limiting the message space of those schemes to the set of Diffie-Hellman (DH) pairs, it is possible to circumvent the known lower bounds in the Type-3 bilinear group setting thus obtaining the shortest signatures consisting of only 2 elements from the shorter source group. It has been shown that such a variant yields efficiency gains for some cryptographic constructions, including attribute-based signatures and direct anonymous attestation. Only the cases of signing a single DH pair or a DH pair and a vector from $\mathbb{Z}_p$ have been considered. Signing a vector of group elements is required for various applications of SPSs, especially if the aim is to forgo relying on heuristic assumptions.

An open question is whether such an improved lower bound also applies to signing a vector of $\ell > 1$ messages. We answer this question negatively for schemes existentially unforgeable under an adaptive chosen-message attack (EUF-CMA) whereas we answer it positively for schemes existentially unforgeable under a random-message attack (EUF-RMA) and those which are existentially unforgeable under a combined chosen-random-message attack (EUF-CMA-RMA). The latter notion is a leeway between the two former notions where it allows the adversary to adaptively choose part of the message to be signed whereas the remaining part of the message is chosen uniformly at random by the signer.

Another open question is whether strongly existentially unforgeable under an adaptive chosen-message attack (sEUF-CMA) schemes with 2-element signatures exist. We answer this question negatively, proving it is impossible to construct sEUF-CMA schemes with 2-element signatures even if the signature consists of elements from both source groups. On the other hand, we prove that sEUF-RMA and sEUF-CMA-RMA schemes with 2-element (unilateral) signatures are possible by giving constructions for those notions.

Among other things, our findings show a gap between random-message/combined chosen-random-message security and chosen-message security in this setting.

Keywords. Digital Signatures, Bilinear Groups, Structure-Preserving.

1 Introduction

Structure-Preserving Signatures (SPSs) [4] are signature schemes over bilinear groups where the messages, the verification key and the signatures consist of only group elements from either/both source groups. Verification of signatures in those schemes only involves evaluating Pairing-Product Equations (PPEs) and checking group memberships. Such properties make them compatible with widely used constructs such as ElGamal encryption [22] and Groth-Sahai proofs [37]. Hence, they are an ideal building block for designing cryptographic protocols not relying on heuristic assumptions such as random oracles [25]. They have numerous applications which include group signatures, e.g [4, 41], blind signatures, e.g. [4, 27], attribute-based signatures, e.g. [24], tightly secure encryption, e.g. [38, 3], malleable signatures, e.g. [12], anonymous credentials, e.g. [26, 18], network coding, e.g. [12], oblivious transfer, e.g. [34], direct anonymous attestation, e.g. [15, 31], and e-cash, e.g. [13].

Related Work. The notion was coined by Abe et al. [4] but earlier constructions conforming to the definition were given by [35, 34]. The notion has been extensively studied. Constructions in the Type-3 setting (cf. Section 2.1) include [4, 5, 30, 7, 20, 36, 32, 33]. Abe et al. [5] proved that signatures of schemes over Type-3 bilinear groups must contain at least 3 elements, which must include elements from both source groups, and require at least 2 PPEs for verification. This ruled out the existence of schemes with unilateral signatures, i.e. where all signature's components are from one of the source groups. Constructions relying on non-interactive assumptions were given by [19, 2, 17, 3, 40, 41, 39, 9, 29]. Abe et al. [6] proved that it is impossible to base the security of an optimal Type-3 scheme (i.e. with 3-element signatures) on non-interactive intractability assumptions. This in essence means that schemes based on non-interactive assumptions cannot be as efficient as their counterparts relying on interactive assumptions or those proven secure directly in the generic group model [45, 44]. More recently, Abe et al. [1] proved lower bounds for schemes signing bilateral messages and based on non-interactive intractability assumptions.

Ghadafi [31] gave a randomizable scheme which can only sign a single Diffie-Hellman pair (cf. Section 2.1) yielding 3-element unilateral signatures and requiring the evaluation of 2 PPEs, excluding the cost for checking the well-formedness of the message, to verify signatures. More recently, Ghadafi [32] gave constructions for a single Diffie-Hellman pair yielding signatures consisting of only 2 elements from the shorter source group and requiring besides checking the well-formedness of the message, the evaluation of a single PPE for verification. He argued that restricting the message space to the set of Diffie-Hellman pairs does not restrict applicability of the schemes and used direct anonymous attestation [16], which is a protocol deployed in practice, and attribute-based signatures [42] as an example. Even though [32] gave a partially structure-preserving scheme which can sign a vector of field elements along the single Diffie-Hellman pair, it was left as an open problem to investigate the case of structure-preserving signatures for a vector of group elements. More recently, Ghadafi [33] gave EUF-CMA constructions for a vector of DH pairs with 2-element bilateral signatures.

Constructions in the Type-2 setting (where an efficiently computable unidirectional homomorphism between the source groups exists) were given in [8, 20, 14, 1].

Fully structure-preserving schemes where even the secret key consists of only group elements from the source groups were recently given by [10, 36, 47].

Motivation & Contribution. Many applications of SPSs require signing a vector of group elements. For instance, consider the case when certifying the public keys of encryption or signature schemes. This is, for instance, required for constructing various variants of anonymous signatures, including group signatures [21], attribute-based signatures [42], proxy signatures [43], k-times anonymous authentication [46], and direct anonymous attestation [16]. This is particularly important when the aim is to dispense with relying on random oracles as in such cases one cannot use standard signature schemes which hinder the structure of the message, e.g. by hashing or requiring knowledge of their discrete logarithm. Therefore, the design of efficient SPS schemes for a vector of messages would have implications for various applications.

SPS schemes on Diffie-Hellman pairs have rendered themselves as a tool to get around the known lower bounds for SPS schemes thus improving efficiency without being too restrictive as they suffice for many applications of SPS schemes. Examples of where SPS schemes on Diffie-Hellman pairs provide better efficency than optimal SPS schemes on unilateral messages include [32, 23]. Also, as argued by [32], optimal SPS schemes on Diffie-Hellman pairs outperform some widely used non-structure-preserving schemes in terms of efficiency.

Note that the size of the elements of one of the source groups is twice as large as that of those from the other source group and hence having schemes with 2-element unilateral signatures from the shorter source group is desirable. A first intriguing open question is whether EUF-CMA SPS schemes for a vector of group elements with 2-element unilateral signatures are possible. We answer this question negatively by proving the impossibility of the existence of such schemes. However, we show that EUF-RMA and EUF-CMA-RMA (cf. Section 2.2) schemes are possible. The latter is a leeway between EUF-RMA and EUF-CMA where it allows the adversary to adaptively choose some part of the message whereas the remaining part of the message is chosen uniformly at random by the signer. While EUF-RMA and EUF-CMA-RMA are both weaker notions than EUF-CMA since unlike the latter, they restrict part of the message to being chosen uniformly at random, we envisage that EUF-CMA-RMA may suffice to replace EUF-CMA for some applications. Consider, for instance, κ-times anonymous authentication schemes [43], where an authority provides users with κ credentials which allow them to anonymously authenticate themselves κ times. The underlying idea for some of the existing constructions is that the credential is a signature by the authority on the user's public key/ID along with a random element chosen by the authority. EUF-CMA-RMA signature schemes may suffice to replace EUF-CMA schemes for such applications.

Another open question is whether strongly existentially unforgeable schemes under an adaptive chosen-message attack (sEUF-CMA) with 2-element (whether unilateral or bilateral) signatures exist. Strong unforgeability is essential for various applications, e.g. [11]. Optimal Type-3 sEUF-CMA schemes for unilateral messages, e.g. [20, 7, 36], have a lower bound of 3-element bilateral signatures, thus, investigating whether the improved lower bound that exploits a special structure of the message also applies to strong unforgeability would have implications for various applications of SPS schemes. We prove that sEUF-CMA schemes with 2-element signatures are not possible. This holds even if the signature is bilateral. On the other hand, we show that sEUF-RMA and sEUF-CMA-RMA schemes with 2-element (unilateral) signatures exist by giving constructions.

Our results highlight a gap between random-message/combined chosen-random-message security and chosen-message security in this setting.

Paper Organization. We provide some preliminary definitions in Section 2. In Section 3 we prove the impossibility of the existence of EUF-CMA schemes for a vector of $\ell > 1$ messages with 2-element unilateral signatures. In Section 4 we prove the impossibility of the existence of sEUF-CMA schemes with 2-element signatures regardless of whether the signatures are unilateral or bilateral. Finally, in Section 5 we construct a sEUF-CMA-RMA scheme for a vector of messages with 2-element unilateral signatures.

Notation. We write $y = A(x; r)$ when algorithm A on input x and randomness r outputs y. We write $y \leftarrow A(x)$ for the process of setting $y = A(x; r)$ where r is sampled at random. We also write $y \leftarrow S$ for sampling y uniformly at random from a set S. A function $\nu(.) : \mathbb{N} \rightarrow \mathbb{R}^+$ is negligible (in n) if for every polynomial $p(.)$ and all sufficiently large values of n, it holds that $\nu(n) < \frac{1}{p(n)}$. By PPT we mean running in probabilistic polynomial time in the relevant security parameter. We use $[k]$ to denote the set $\{1, \ldots, k\}$.

2 Preliminaries

In this section we provide some preliminary definitions.

2.1 Bilinear Groups

A bilinear group is a tuple $\mathcal{P} := (\mathbb{G}, \mathbb{H}, \mathbb{T}, p, G, \tilde{H}, e)$ where $\mathbb{G}$, $\mathbb{H}$ and $\mathbb{T}$ are groups of a prime order p, and G and $\tilde{H}$ generate $\mathbb{G}$ and $\mathbb{H}$, respectively. The function e is a non-degenerate bilinear map $e : \mathbb{G} \times \mathbb{H} \longrightarrow \mathbb{T}$. We refer to $\mathbb{G}$ and $\mathbb{H}$ as the source groups whereas we refer to $\mathbb{T}$ as the target group. We use multiplicative notation for all the groups. For clarity we will accent elements of $\mathbb{H}$ with $\tilde{}$. We let $\mathbb{G}^\times := \mathbb{G} \setminus \{1_\mathbb{G}\}$ and $\mathbb{H}^\times := \mathbb{H} \setminus \{1_\mathbb{H}\}$. We limit our attention to the efficient Type-3 setting [28], where $\mathbb{G} \neq \mathbb{H}$ and there is no efficiently computable homomorphism between the source groups in either direction. We assume there is an algorithm $\mathcal{BG}$ that on input a security parameter κ, outputs a description of bilinear groups.

The message space of the schemes we consider is the set of elements of the subgroup $\widehat{\mathbb{G}\mathbb{H}}$ of $\mathbb{G} \times \mathbb{H}$ defined as the image of the map $\psi : x \longmapsto (G^x, \tilde{H}^x)$ for

$x \in \mathbb{Z}_p$. One can efficiently test whether $(M, \tilde{N}) \in \widehat{\mathbb{GH}}$ by checking

$$e(M, \tilde{H}) = e(G, \tilde{N}) \cdot$$

Such pairs were called Diffie-Hellman (DH) pairs in [4]. We stress that we do not require that the signer knows the discrete logarithm of the message pair. In fact, in all of our proofs/constructions we assume a signer which does not know/does not exploit knowledge of such an exponent.

2.2 Digital Signatures

A digital signature scheme $\mathcal{DS}$ over a bilinear group $\mathcal{P}$ generated by $\mathcal{BG}$ for a message space $\mathcal{M}$ consists of the following algorithms:

$\mathsf{KeyGen}(\mathcal{P})$**:** On input $\mathcal{P}$, this outputs a pair of signing/verification keys $(\mathsf{sk}, \mathsf{vk})$.
$\mathsf{Sign}(\mathsf{sk}, m)$**:** On input the secret signing key sk and a message $m \in \mathcal{M}$, this outputs a signature σ on m.
$\mathsf{Verify}(\mathsf{vk}, m, \sigma)$**:** On input the verification key vk, a message $m \in \mathcal{M}$ and a signature σ, this outputs 0/1 indicating the invalidity/validity of σ on m.

Definition 1 (Correctness). *A signature scheme $\mathcal{DS}$ over a bilinear group generator $\mathcal{BG}$ is* (perfectly) correct *if for all $\kappa \in \mathbb{N}$:*

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

A signature scheme is said to be existentially unforgeable if it is hard to forge a signature on a new message that has not been signed before where the adversary may see signatures on other messages before outputting her forgery. We distinguish between adaptive chosen-message (EUF-CMA), random-message (EUF-RMA) and combined chosen-random-message (EUF-CMA-RMA) variants of existential unforgeability as defined below.

Definition 2 (EUF-CMA). *A signature scheme $\mathcal{DS}$ over a bilinear group generator $\mathcal{BG}$ is* Existentially Unforgeable under an adaptive Chosen-Message Attack *if for all $\kappa \in \mathbb{N}$ for all PPT adversaries $\mathcal{A}$, the following is negligible (in κ):*

$$\Pr\left[\begin{array}{c}\mathcal{P} \leftarrow \mathcal{BG}(1^\kappa); (\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(\mathcal{P}); (\sigma^*, m^*) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathsf{sk}, \cdot)}(\mathcal{P}, \mathsf{vk}) \\ : \mathsf{Verify}(\mathsf{vk}, m^*, \sigma^*) = 1 \wedge m^* \notin Q_{\mathsf{Sign}}\end{array}\right],$$

where Q_{Sign} is the set $\{m_i\}_{i=1}^q$ of messages queried to Sign*.*

Strong Existential Unforgeability under an adaptive Chosen-Message Attack (sEUF-CMA) is defined similarly and requires that the adversary cannot even output a new signature on a message that was queried to the sign oracle.

Definition 3 (EUF-RMA). *A signature scheme $\mathcal{DS}$ over a bilinear group generator $\mathcal{BG}$ is* Existentially Unforgeable under a Random-Message Attack *if for all $\kappa \in \mathbb{N}$ for all PPT adversaries $\mathcal{A}$, the following is negligible (in κ):*

$$\Pr\left[\begin{array}{r}\mathcal{P} \leftarrow \mathcal{BG}(1^\kappa); (\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(\mathcal{P}); (\sigma^*, m^*) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathsf{sk})}(\mathcal{P}, \mathsf{vk}) \\ : \mathsf{Verify}(\mathsf{vk}, m^*, \sigma^*) = 1 \,\wedge\, m^* \notin Q_{\mathsf{Sign}}\end{array}\right],$$

where Sign *uniformly samples a message m from $\mathcal{M}$ and returns m and a signature σ on it, and Q_{Sign} is the set $\{m_i\}_{i=1}^q$ of messages returned by* Sign.

Strong Existential Unforgeability under a Random-Message Attack (sEUF-RMA) is defined similarly and requires that the adversary cannot even output a new signature on a message that was chosen by Sign.

The following variant lies in between the two previous notions where it allows the adversary to adaptively choose some part of the message whereas the remaining part of the message is chosen uniformly at random by the sign oracle.

Definition 4 (EUF-CMA-RMA). *A signature scheme $\mathcal{DS}$ over a bilinear group generator $\mathcal{BG}$ for a message space $\mathcal{M} = \mathcal{M}_C \times \mathcal{M}_R$ is* Existentially Unforgeable under a combined Chosen-Random-Message Attack *if for all $\kappa \in \mathbb{N}$ for all PPT adversaries $\mathcal{A}$, the following is negligible (in κ):*

$$\Pr\left[\begin{array}{r}\mathcal{P} \leftarrow \mathcal{BG}(1^\kappa); (\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(\mathcal{P}); (\sigma^*, m^*, m'^*) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathsf{sk},\cdot)}(\mathcal{P}, \mathsf{vk}) \\ : \mathsf{Verify}(\mathsf{vk}, (m^*, m'^*), \sigma^*) = 1 \,\wedge\, (m^*, m'^*) \notin Q_{\mathsf{Sign}}\end{array}\right],$$

where when queried on a message $m_i \in \mathcal{M}_C$, Sign *uniformly samples a message m'_i from $\mathcal{M}_R$ and returns m'_i and a signature σ on (m_i, m'_i), and Q_{Sign} is the set $\{(m_i, m'_i)\}_{i=1}^q$ containing pairs on which signatures have been generated by* Sign.

Strong Existential Unforgeability under a combined Chosen-Random-Message Attack (sEUF-CMA-RMA) requires that the adversary cannot even output a new signature on a message pair on which she has obtained a signature from Sign.

2.3 Structure-Preserving Signatures

Structure-preserving signatures [4] are signature schemes defined over bilinear groups where the messages, the verification key and signatures are all group elements from either or both source groups, and verifying signatures only involves deciding group membership and evaluating PPEs of the form of Equation (1).

$$\prod_i \prod_j e(A_i, \tilde{B}_j)^{c_{i,j}} = 1_{\mathbb{T}}, \tag{1}$$

where $A_i \in \mathbb{G}$ and $\tilde{B}_j \in \mathbb{H}$ are group elements appearing in $\mathcal{P}, m, \mathsf{vk}, \sigma$, whereas $c_{i,j} \in \mathbb{Z}_p$ are public constants.

Generic Signer. We refer to a signer that can only decide group membership, evaluate the bilinear map e, compute the group operations in groups $\mathbb{G}, \mathbb{H}$ and $\mathbb{T}$, and compare group elements as a *generic signer*.

3 Impossibility of generic-signer EUF-CMA SPS Schemes for a vector of $\ell > 1$ Messages with 2-element Unilateral Signatures

In this section we prove that generic-signer EUF-CMA SPS schemes for a vector of $\ell > 1$ messages with 2-element unilateral signatures cannot exist. We start by proving the following theorem which is a generalization of Lemma 1 from [8] for SPS schemes for unilateral messages.

Theorem 1. *A generic-signer EUF-RMA SPS scheme for a vector of $\ell \geq 1$ DH pairs must have for any message vector superpolynomially many potential signatures.*

Proof. Since the signer is generic, the signature $\sigma = (\boldsymbol{R}, \tilde{\boldsymbol{S}}) \in \mathbb{G}^n \times \mathbb{H}^{\tilde{n}}$ on the message vector $\Big((M_i, \tilde{M}_i)\Big)_{i=1}^{\ell}$ is computed via entry-wise exponentiation as $\sigma = (\boldsymbol{R}, \tilde{\boldsymbol{S}}) := (G^{\boldsymbol{\alpha}} \prod_{i=1}^{\ell} M_i^{\boldsymbol{\alpha}'_i}, \tilde{H}^{\boldsymbol{\beta}} \prod_{i=1}^{\ell} \tilde{M}_i^{\boldsymbol{\beta}'_i)}$ for some vectors $(\boldsymbol{\alpha}, \boldsymbol{\alpha}'_1, \ldots, \boldsymbol{\alpha}'_\ell, \boldsymbol{\beta}, \boldsymbol{\beta}'_1, \ldots, \boldsymbol{\beta}'_\ell) \in \mathbb{Z}_p^{(\ell+1)n} \times \mathbb{Z}_p^{(\ell+1)\tilde{n}}$. Let's assume for contradiction that there is a scheme which has a polynomial number of potential signatures. This means there is a polynomial set $\{(\boldsymbol{\alpha}_i, \boldsymbol{\alpha}'_{i,1}, \ldots, \boldsymbol{\alpha}'_{i,\ell}, \boldsymbol{\beta}_i, \boldsymbol{\beta}'_{i,1}, \ldots, \boldsymbol{\beta}'_{i,\ell})\}_{i=1}^{\mathrm{poly}(\kappa)}$ for some polynomial ploy corresponding to the list of potential signatures. Now given signatures $\sigma_1 = (\boldsymbol{R}_1, \tilde{\boldsymbol{S}}_{\boldsymbol{1}})$ and $\sigma_2 = (\boldsymbol{R}_2, \tilde{\boldsymbol{S}}_{\boldsymbol{2}})$ on random DH message vectors $(\boldsymbol{M}_1, \tilde{\boldsymbol{M}}_1)$ and $(\boldsymbol{M}_2, \tilde{\boldsymbol{M}}_2)$, respectively, we have with probability $\frac{1}{\mathrm{poly}(\kappa)^2}$ that those signatures were constructed using the same vector $\big(\boldsymbol{\alpha}_i, \boldsymbol{\alpha}'_{i,1}, \ldots, \boldsymbol{\alpha}'_{i,\ell}, \boldsymbol{\beta}_i, \boldsymbol{\beta}'_{i,1}, \ldots, \boldsymbol{\beta}'_{i,\ell}\big)$ for some $i \in [\mathrm{ploy}(\kappa)]$. Thus, we have $\sigma^* = (\boldsymbol{R}^*, \tilde{\boldsymbol{S}}^*) = (\boldsymbol{R}_1^{1-\gamma} \boldsymbol{R}_2^{\gamma}, \tilde{\boldsymbol{S}}_1^{1-\gamma} \tilde{\boldsymbol{S}}_2^{\gamma})$ is a valid forgery on the message vector $\big(\boldsymbol{M}_1^{1-\gamma} \boldsymbol{M}_2^{\gamma}, \tilde{\boldsymbol{M}}_1^{1-\gamma} \tilde{\boldsymbol{M}}_2^{\gamma}\big)$ for any $\gamma \leftarrow \mathbb{Z}_p^{\times}$. This means such a scheme is not EUF-RMA secure against an adversary which makes 2 (non-adaptive) signing queries. □

We now proceed to proving the impossibility of the existence of generic-signer EUF-CMA (against $q > 1$ sign queries) SPS schemes for a vector of $\ell > 1$ messages with 2-element unilateral signatures. We prove that such schemes even for the simpler case where $\ell = 2$ cannot exist.

Theorem 2. *There is no generic-signer EUF-CMA (against $q > 1$ sign queries) SPS schemes for a vector of 2 DH pairs with 2-element unilateral signatures.*

Proof. We start by proving the following lemma regarding the number of verification equations required for schemes with 2-element signatures.

Lemma 1. *One verification equation (excluding the cost for verifying the well-formedness of the messages) is sufficient for a generic-signer SPS scheme with 2-element signatures.*

Proof. Assume a scheme has 2 verification equations. Both equations must pose non-trivial constraint on the signature components as otherwise we can reduce them to a single equation. Since each verification equation must involve at least 1 signature component, we have 3 cases:

- Both equations involve both signature components: This means we have 2 quadratic/linear equations in the discrete logarithm of the signature components. Such an equation system have at most 4 distinct solutions implying that there are at most 4 potential signatures for the message vector which contradicts the proof of Theorem 1.
- One equation involves both signature components whereas the other equation involves only one signature component: This means one equation is quadratic/linear involving both signature components, whereas the remaining equation is linear in one of the signature components. By substituting the value of the signature component in the linear equation into the other equation we end up with one verification equation that is sufficient for verifying the signature.
- Each verification equation involves a single signature component: Since the other constants (the verification key, the public parameters (if any) and the messages) are fixed, we have that each verification equation is a linear equation in one of the signature components, i.e. each equation is a linear equation in one unknown. Thus, there is exactly 1 potential signature for the message vector which contradicts the proof of Theorem 1.

□

Now let's assume WLOG that the signature is of the form $\sigma = (S_1, S_2) \in \mathbb{G}^2$, whereas the verification key is of the form $(\boldsymbol{X}, \tilde{\boldsymbol{Y}}) \in \mathbb{G}^n \times \mathbb{H}^{n'}$. The proof for the case where $\sigma = (\tilde{S}_1, \tilde{S}_2) \in \mathbb{H}^2$ is similar.

A generic signer computes the signature as $S_i := G^{\frac{\alpha_i(\boldsymbol{x},\boldsymbol{y})}{\alpha'_i(\boldsymbol{x},\boldsymbol{y})}} M_1^{\frac{\beta_{i,1}(\boldsymbol{x},\boldsymbol{y})}{\beta'_{i,1}(\boldsymbol{x},\boldsymbol{y})}} M_2^{\frac{\beta_{i,2}(\boldsymbol{x},\boldsymbol{y})}{\beta'_{i,2}(\boldsymbol{x},\boldsymbol{y})}}$ for some multivariate polynomials $\alpha_{i,}, \alpha'_i, \beta_{i,1}, \beta'_{i,1}, \beta_{i,2}, \beta'_{i,2} \in \mathbb{Z}_p[\boldsymbol{x}, \boldsymbol{y}]$ for $i \in \{1, 2\}$. Note that none of those polynomials has a term in m_1 or m_2, i.e. they are independent of the messages. Thus, it is infeasible for a generic signer to compute a non-trivial signature component where its discrete logarithm s_i contains a message m_i (for any $i \in \{1, 2\}$) in a term in the denominator. This means that we must have that the verification equation does not contain the pairings $e(S_i, \tilde{M}_j)$ for all $j \in [2]$ and some $i \in [2]$, i.e. either S_1 or S_2 is independent of the messages as otherwise this would mean that m_i appears in the denominator of one of the signature components. Let's assume WLOG that S_1 is independent of the messages, i.e. the verification equation does not contain the pairings $e(S_1, \tilde{M}_i)$ for $i = 1, 2$. This means the scheme has a verification equation of the following form:

$$e(S_1, \prod_{i=1}^{n'} \tilde{Y}_i^{a_i}) \prod_{i=1}^{2} e(\prod_{j=1}^{n} X_j^{c_{i,j}}, \tilde{M}_i) \prod_{i=1}^{2} e(M_i, \prod_{j=1}^{n'} \tilde{Y}_j^{e_{i,j}} \prod_{j=1}^{2} \tilde{M}_j^{u_{i,j}}) \\ e(S_2, \prod_{i=1}^{n'} \tilde{Y}_i^{b_i} \prod_{i=1}^{2} \tilde{M}_i^{d_i}) = \prod_{i=1}^{n} \prod_{j=1}^{n'} e(X_i, \tilde{Y}_j)^{t_{i,j}} \quad (2)$$

A generic signer cannot produce a signature component whose discrete logarithm has a term with any of the monomials: m_1^2, $m_1 m_2$, or m_2^2. Thus, WLOG we can also assume that the verification equation does not contain a pairing of the form $e(M_i, \tilde{M}_j)$ for all $i, j \in [2]$, i.e. $u_{i,j} = 0$ for all $i, j \in [2]$. This means the verification equation is of the following form:

$$e(S_1, \prod_{i=1}^{n'} \tilde{Y}_i^{a_i}) \prod_{i=1}^{2} e(\prod_{j=1}^{n} X_j^{c_{i,j}}, \tilde{M}_i) \prod_{i=1}^{2} e(M_i, \prod_{j=1}^{n'} \tilde{Y}_j^{e_{i,j}}) \\ e(S_2, \prod_{i=1}^{n'} \tilde{Y}_i^{b_i} \prod_{i=1}^{2} \tilde{M}_i^{d_i}) = \prod_{i=1}^{n} \prod_{j=1}^{n'} e(X_i, \tilde{Y}_j)^{t_{i,j}} \quad (3)$$

Lemma 2 below proves that a scheme with a verification equation of the form of Equation (3) is not secure against an adversary which makes 2 chosen-message sign queries, whereas Lemma 3 proves that even if we consider schemes with a verification equation of the form of Equation (2) such schemes are not EUF-CMA secure against an adversary that makes 3 chosen-message sign queries, which concludes the proof of the theorem.

Lemma 2. *A SPS scheme for a vector of 2 DH pairs with a verification equation of the form of Equation (3) is not EUF-CMA against* 2 *(non-adaptive) chosen-message sign queries.*

Proof. We have 2 cases as follows:

- Case $d_2 \neq 0$: Choose any 2 distinct messages $(M_{1,1}, \tilde{M}_{1,1}), (M_1^*, \tilde{M}_1^*)$ and set $(M_{1,2}, \tilde{M}_{1,2}) := (M_{1,1}, \tilde{M}_{1,1})^{\frac{-d_1}{d_2}}$, $(M_{2,1}, \tilde{M}_{2,1}) := (M_1^{*\frac{1}{\gamma}} M_{1,1}^{\frac{\gamma-1}{\gamma}}, \tilde{M}_1^{*\frac{1}{\gamma}} \tilde{M}_{1,1}^{\frac{\gamma-1}{\gamma}})$ and $(M_{2,2}, \tilde{M}_{2,2}) := (M_1^{*\frac{-d_1}{d_2\gamma}} M_{1,1}^{\frac{d_1(1-\gamma)}{d_2\gamma}}, \tilde{M}_1^{*\frac{-d_1}{d_2\gamma}} \tilde{M}_{1,1}^{\frac{d_1(1-\gamma)}{d_2\gamma}})$.
  After getting signatures $\sigma_1 = (S_{1,1}, S_{1,2})$ and $\sigma_2 = (S_{2,1}, S_{2,2})$ on the messages $((M_{1,1}, \tilde{M}_{1,1}), (M_{1,2}, \tilde{M}_{1,2}))$ and $((M_{2,1}, \tilde{M}_{2,1}), (M_{2,2}, \tilde{M}_{2,2}))$, respectively, we can compute a forgery $\sigma^* = (S_1^*, S_2^*) := (S_{1,1}^{1-\gamma} S_{2,1}^{\gamma}, S_{1,2}^{1-\gamma} S_{2,2}^{\gamma})$ on the message $((M_1^*, \tilde{M}_1^*), (M_2^*, \tilde{M}_2^*) := (M_1^*, \tilde{M}_1^*)^{\frac{-d_1}{d_2}})$. This is a valid signature and we have that $((M_1^*, \tilde{M}_1^*), (M_2^*, \tilde{M}_2^*)) \neq ((M_{1,1}, \tilde{M}_{1,1}), (M_{1,2}, \tilde{M}_{1,2}))$ and $((M_1^*, \tilde{M}_1^*), (M_2^*, \tilde{M}_2^*)) \neq ((M_{2,1}, \tilde{M}_{2,1}), (M_{2,2}, \tilde{M}_{2,2}))$ for any $\gamma \in \mathbb{Z}_p^{\times} \setminus \{1\}$.
- Case $d_2 = 0$: Choose random distinct messages $(M_{1,2}, \tilde{M}_{1,2}), (M_{2,2}, \tilde{M}_{2,2})$ and $(M_1^*, \tilde{M}_1^*)$ and set $(M_2^*, \tilde{M}_2^*) := (M_{1,2}^{1-\gamma} M_{2,2}^{\gamma}, \tilde{M}_{1,2}^{1-\gamma} \tilde{M}_{2,2}^{\gamma})$. Query the sign oracle on $((M_1^*, \tilde{M}_1^*), (M_{1,2}, \tilde{M}_{1,2}))$ and $((M_1^*, \tilde{M}_1^*), (M_{2,2}, \tilde{M}_{2,2}))$ to get signatures $\sigma_1 = (S_{1,1}, S_{1,2})$ and $\sigma_2 = (S_{2,1}, S_{2,2})$, respectively. We have that $\sigma^* = (S_1^*, S_2^*) := (S_{1,1}^{1-\gamma} S_{2,1}^{\gamma}, S_{1,2}^{1-\gamma} S_{2,2}^{\gamma})$ is a valid forgery on $((M_1^*, \tilde{M}_1^*), (M_2^*, \tilde{M}_2^*))$ for any $\gamma \leftarrow \mathbb{Z}_p^{\times}$. We have that $((M_1^*, \tilde{M}_1^*), (M_2^*, \tilde{M}_2^*)) \notin \{((M_1^*, \tilde{M}_1^*), (M_{1,2}, \tilde{M}_{1,2})), ((M_1^*, \tilde{M}_1^*), (M_{2,2}, \tilde{M}_{2,2}))\}$.

This concludes the proof. □

Lemma 3. *A SPS scheme for a vector of 2 DH pairs with a verification equation of the form of Equation (2) is not EUF-CMA against* 3 *(non-adaptive) chosen-message sign queries.*

Proof. We have 2 cases as follows:

- Case $d_2 \neq 0$: Choose any distinct messages: $(M_1^*, \tilde{M}_1^*)$, $(M_2^*, \tilde{M}_2^*)$ and $(M_{3,1}, \tilde{M}_{3,1})$. Set:

  $$\begin{aligned}
  (M_{1,1}, \tilde{M}_{1,1}) &:= (M_1^{*\frac{\gamma-1}{2\gamma}} M_{3,1}^{\frac{\gamma+1}{2\gamma}}, \tilde{M}_1^{*\frac{\gamma-1}{2\gamma}} \tilde{M}_{3,1}^{\frac{\gamma+1}{2\gamma}})\\
  (M_{1,2}, \tilde{M}_{1,2}) &:= (M_1^{*\frac{d_1(\gamma+1)}{2d_2\gamma}} M_{3,1}^{\frac{-d_1(\gamma+1)}{2d_2\gamma}} M_2^*, \tilde{M}_1^{*\frac{d_1(\gamma+1)}{2d_2\gamma}} \tilde{M}_{3,1}^{\frac{-d_1(\gamma+1)}{2d_2\gamma}} \tilde{M}_2^*)\\
  (M_{2,1}, \tilde{M}_{2,1}) &:= (M_1^{*\frac{\gamma+1}{2\gamma}} M_{3,1}^{\frac{\gamma-1}{2\gamma}}, \tilde{M}_1^{*\frac{\gamma+1}{2\gamma}} \tilde{M}_{3,1}^{\frac{\gamma-1}{2\gamma}})\\
  (M_{2,2}, \tilde{M}_{2,2}) &:= (M_1^{*\frac{d_1(\gamma-1)}{2d_2\gamma}} M_{3,1}^{\frac{d_1(1-\gamma)}{2d_2\gamma}} M_2^*, \tilde{M}_1^{*\frac{d_1(\gamma-1)}{2d_2\gamma}} \tilde{M}_{3,1}^{\frac{d_1(1-\gamma)}{2d_2\gamma}} \tilde{M}_2^*)\\
  (M_{3,2}, \tilde{M}_{3,2}) &:= (M_1^{*\frac{d_1}{d_2}} M_{3,1}^{\frac{-d_1}{d_2}} M_2^*, \tilde{M}_1^{*\frac{d_1}{d_2}} \tilde{M}_{3,1}^{\frac{-d_1}{d_2}} \tilde{M}_2^*)
  \end{aligned}$$

  Now query the sign oracle on the messages $((M_{1,1}, \tilde{M}_{1,1}), (M_{1,2}, \tilde{M}_{1,2}))$, $((M_{2,1}, \tilde{M}_{2,1}), (M_{2,2}, \tilde{M}_{2,2}))$ and $((M_{3,1}, \tilde{M}_{3,1}), (M_{3,2}, \tilde{M}_{3,2}))$, to get the signatures $\sigma_1 = (S_{1,1}, S_{1,2})$, $\sigma_2 = (S_{2,1}, S_{2,2})$ and $\sigma_3 = (S_{3,1}, S_{3,2})$, respectively. We can now compute a forgery $\sigma^* = (S_1^*, S_2^*) := (S_{1,1}^{-\gamma} S_{2,1}^{\gamma} S_{3,1}, S_{1,2}^{-\gamma} S_{2,2}^{\gamma} S_{3,2})$ on the message $((M_1^*, \tilde{M}_1^*), (M_2^*, \tilde{M}_2^*))$. This is a valid signature and we have that $((M_1^*, \tilde{M}_1^*), (M_2^*, \tilde{M}_2^*)) \notin \big\{((M_{1,1}, \tilde{M}_{1,1}), (M_{1,2}, \tilde{M}_{1,2})), ((M_{2,1}, \tilde{M}_{2,1}), (M_{2,2}, \tilde{M}_{2,2})), ((M_{3,1}, \tilde{M}_{3,1}), (M_{3,2}, \tilde{M}_{3,2}))\big\}$ for any $\gamma \in \mathbb{Z}_p^{\times} \setminus \{-1, 1\}$.
- Case $d_2 = 0$: Choose any distinct messages: $(M_1^*, \tilde{M}_1^*)$, $(M_{2,2}, \tilde{M}_{2,2})$ and $(M_{3,2}, \tilde{M}_{3,2})$. Set

  $$\begin{aligned}
  (M_{1,1}, \tilde{M}_{1,1}) = (M_{2,1}, \tilde{M}_{2,1}) = (M_{3,1}, \tilde{M}_{3,1}) &:= (M_1^*, \tilde{M}_1^*)\\
  (M_2^*, \tilde{M}_2^*) &:= (M_{2,2}^{\frac{\gamma+1}{2}} M_{3,2}^{\frac{1-\gamma}{2}}, \tilde{M}_{2,2}^{\frac{\gamma+1}{2}} \tilde{M}_{3,2}^{\frac{1-\gamma}{2}})\\
  (M_{1,2}, \tilde{M}_{1,2}) &:= (M_{2,2}^{\frac{1-\gamma}{2}} M_{3,2}^{\frac{\gamma+1}{2}}, \tilde{M}_{2,2}^{\frac{1-\gamma}{2}} \tilde{M}_{3,2}^{\frac{\gamma+1}{2}})
  \end{aligned}$$

  Now query the sign oracle on the messages $((M_{1,1}, \tilde{M}_{1,1}), (M_{1,2}, \tilde{M}_{1,2}))$, $((M_{2,1}, \tilde{M}_{2,1}), (M_{2,2}, \tilde{M}_{2,2}))$ and $((M_{3,1}, \tilde{M}_{3,1}), (M_{3,2}, \tilde{M}_{3,2}))$, to get the signatures $\sigma_1 = (S_{1,1}, S_{1,2})$, $\sigma_2 = (S_{2,1}, S_{2,2})$ and $\sigma_3 = (S_{3,1}, S_{3,2})$, respectively. We can now compute a forgery $\sigma^* = (S_1^*, S_2^*) := (S_{1,1} S_{2,1}^{\gamma} S_{3,1}^{-\gamma}, S_{1,2} S_{2,2}^{\gamma} S_{3,2}^{-\gamma})$ on the message $((M_1^*, \tilde{M}_1^*), (M_2^*, \tilde{M}_2^*))$. This is a valid signature and we have that $((M_1^*, \tilde{M}_1^*), (M_2^*, \tilde{M}_2^*)) \notin \big\{((M_{1,1}, \tilde{M}_{1,1}), (M_{1,2}, \tilde{M}_{1,2})), ((M_{2,1}, \tilde{M}_{2,1}), (M_{2,2}, \tilde{M}_{2,2})), ((M_{3,1}, \tilde{M}_{3,1}), (M_{3,2}, \tilde{M}_{3,2}))\big\}$ for any $\gamma \in \mathbb{Z}_p^{\times} \setminus \{-1, 1\}$.

This concludes the proof. □

The following corollary follows from Theorem 2.

Corollary 1. *There is no generic-signer EUF-CMA SPS scheme for a vector of $\ell > 1$ DH pairs with 2-element unilateral signatures.*

4 Impossibility of sEUF-CMA (against $q > 1$ sign queries) SPS Schemes with 2-element Signatures

In this section we prove the impossibility of the existence of sEUF-CMA SPS schemes with 2-element (unilateral/bilateral) signatures. However, in Section 5 we show that sEUF-RMA and sEUF-CMA-RMA with 2-element (unilateral) signatures are possible by giving concrete constructions.

Theorem 3. *There is no generic-signer sEUF-CMA (against $q > 1$ sign queries) SPS scheme with 2-element signatures.*

Proof. Lemma 1 proved that 1 PPE is sufficient for verifying 2-element signatures. The following 2 lemmata complete the proof, where the first deals with the case of bilateral signatures whereas the second deals with unilateral signatures.

Lemma 4. *There is no generic-signer sEUF-CMA (against $q > 1$ sign queries) SPS scheme with 2-element bilateral signatures.*

Proof. Let's WLOG assume that the signature is of the form $\sigma = (S_1, \tilde{S}_2) \in \mathbb{G} \times \mathbb{H}$, whereas the verification key (including any public parameters) is of the form $(\boldsymbol{X}, \tilde{\boldsymbol{Y}}) \in \mathbb{G}^n \times \mathbb{H}^{n'}$. The case where the signature is transposed is similar.

A generic signer computes the signature as $S_1 := M^{\frac{\alpha_1(\boldsymbol{x},\boldsymbol{y})}{\alpha'_1(\boldsymbol{x},\boldsymbol{y})}} G^{\frac{\beta_1(\boldsymbol{x},\boldsymbol{y})}{\beta'_1(\boldsymbol{x},\boldsymbol{y})}}$ and $\tilde{S}_2 := \tilde{M}^{\frac{\alpha_2(\boldsymbol{x},\boldsymbol{y})}{\alpha'_2(\boldsymbol{x},\boldsymbol{y})}} \tilde{H}^{\frac{\beta_2(\boldsymbol{x},\boldsymbol{y})}{\beta'_2(\boldsymbol{x},\boldsymbol{y})}}$ for some polynomials $\alpha_1, \alpha'_1, \beta_1, \beta'_1, \alpha_2, \alpha'_2, \beta_2, \beta'_2 \in \mathbb{Z}_p[\boldsymbol{x}, \boldsymbol{y}]$. Note that none of those polynomials has a term in m. Without knowledge of the discrete logarithm of the message m, it is infeasible for a generic signer to compute a non-trivial signature component where its discrete logarithm s_i contains the message m in a term in the denominator. Thus, we must have that either $e(S_1, \tilde{M})$ or $e(M, \tilde{S}_2)$ does not feature in the verification equation. WLOG let's assume that $e(S_1, \tilde{M})$ does not appear in the verification equation. The proof for the other case where $e(M, \tilde{S}_2)$ does not appear in the verification equation is similar.

Such a scheme would have a verification equation of the following form:

$$e(S_1, \prod_{i=1}^{n'} \tilde{Y}_i^{c_i} \tilde{S}_2^d) e(\prod_{i=1}^{n} X_i^{b_i}, \tilde{M}) e(M, \prod_{i=1}^{n'} \tilde{Y}_i^{e_i} \tilde{S}_2^f \tilde{M}^k)$$
$$e(\prod_{i=1}^{n} X_i^{a_i}, \tilde{S}_2) = \prod_{i=1}^{n} \prod_{j=1}^{n'} e(X_i, \tilde{Y}_j)^{t_{i,j}} \tag{4}$$

We have 3 cases as follows:

- Case for some $i \in [n']$, $c_i \neq 0$: After getting a signature $\sigma = (S_1, \tilde{S}_2)$ on a (random) message $(M, \tilde{M})$, fix any $i \in [n']$ where $c_i \neq 0$, we can compute a new signature $\sigma^* = (S_1^*, \tilde{S}_2^*)$ on the random message $(M, \tilde{M})$ as follows:

$$S_1^* := M^{\frac{-\gamma f}{c_i + \gamma d}} S_1^{\frac{c_i}{c_i + \gamma d}} \prod_{j=1}^{n} X_j^{\frac{-a_j \gamma}{c_i + \gamma d}} \qquad \tilde{S}_2^* := \tilde{S}_2^{\frac{c_i + \gamma d}{c_i}} Y_i^{\gamma} \prod_{j \neq i} Y_j \frac{c_j \gamma}{c_i}$$

The new signature is a valid forgery and we have $\sigma^* \neq \sigma$ for any $\gamma \in \mathbb{Z}_p^{\times}$.

- Case $c_i = 0$ for all $i \in [n']$ but $d \neq 0$: After getting a signature $\sigma = (S_1, \tilde{S}_2)$ on a (random) message $(M, \tilde{M})$, we can compute a new signature $\sigma^* = (S_1^*, \tilde{S}_2^*)$ on the random message $(M, \tilde{M})$ as follows:

$$S_1^* := M^{\frac{f-\gamma f}{\gamma d}} S_1^{\frac{1}{\gamma}} \prod_{i=1}^{n} X_i^{\frac{a_i - a_i \gamma}{\gamma d}} \qquad\qquad \tilde{S}_2^* := \tilde{S}_2^{\gamma}$$

  The new signature is a valid forgery and $\sigma^* \neq \sigma$ for any $\gamma \in \mathbb{Z}_p^{\times} \setminus \{1\}$.
- Case $c_i = 0$ for all $i \in [n']$ and $d = 0$: This means the verification equation does not involve the component S_1 and hence the signature consists of only 1 element and the equation is linear in s_2 (the discrete logarithm of $\tilde{S}_2$). This means for any message there is exactly 1 potential signature which contradicts Theorem 1.

This concludes the proof. □

Lemma 5. *There is no generic-signer sEUF-CMA (against $q > 1$ sign queries) SPS scheme with 2-element unilateral signatures.*[1]

Proof. WLOG let's count any public parameters (if any) as part of the verification key vk. Such a scheme would have signatures of the form $\sigma = (S_1, S_2) \in \mathbb{G}^2$, a verification key of the form $(\boldsymbol{X}, \boldsymbol{Y}) \in \mathbb{G}^n \times \mathbb{H}^{n'}$, and a verification equation of the following form:

$$\prod_{i=1}^{2} e(S_i, \prod_{j=1}^{n'} \tilde{Y}_j^{c_{i,j}} \tilde{M}^{d_i}) e(\prod_{i=1}^{n} X_i^{a_i}, \tilde{M}) e(M, \prod_{i=1}^{n'} \tilde{Y}_i^{b_i} \tilde{M}^{f}) = \prod_{i=1}^{n} \prod_{j=1}^{n'} e(X_i, \tilde{Y}_j)^{t_{i,j}} \quad (5)$$

Theorem 1 proved that for a scheme to be EUF-RMA secure (against $q > 1$ sign queries), it must have superpolynomially many potential signatures. After obtaining any 2 distinct signatures $\sigma = (S_1, S_2)$ and $\sigma' = (S_1', S_2')$ on any message $(M, \tilde{M})$, we have that $\sigma^* = (S_1^*, S_2^*) := (S_1^{\gamma} S_1'^{1-\gamma}, S_2^{\gamma} S_2'^{1-\gamma})$ is with overwhelming probability a new valid signature on $(M, \tilde{M})$ for any $\gamma \in \mathbb{Z}_p^{\times} \setminus \{1\}$. □

This concludes the proof. □

5 sEUF-CMA-RMA Scheme for Diffie-Hellman Vectors

Here we construct a sEUF-CMA-RMA scheme with 2-element unilateral signatures for the message space $\mathcal{M} = \mathcal{M}_{\mathrm{C}} \times \mathcal{M}_{\mathrm{R}}$ where $\mathcal{M}_{\mathrm{C}} = \widehat{\mathbb{GH}}$ and $\mathcal{M}_{\mathrm{R}} = \widehat{\mathbb{GH}}^{\eta}$ for any $\eta \geq 1$. This also implies the existence of sEUF-RMA schemes with 2-element unilateral signatures.

Given the description of Type-3 bilinear groups $\mathcal{P}$ output by $\mathcal{BG}(1^{\kappa})$, the scheme is as follows:

[1] Our result is stronger than that of [32] since we consider a bilateral verification key.

- $\mathsf{KeyGen}(\mathcal{P})$: Select $u, w_1, w_2, x, y_1, \ldots, y_\eta \leftarrow \mathbb{Z}_p$. Set $X := G^x$, $Y_i := G^{y_i}$ for all $i \in [\eta]$, $U := G^u$, $\tilde{W}_1 := \tilde{H}^{w_1}$ and $\tilde{W}_2 := \tilde{H}^{w_2}$. Set $\mathsf{sk} := (w_1, w_2, u, x, y_1, \ldots, y_\eta)$ and $\mathsf{vk} := (\tilde{W}_1, \tilde{W}_2, U, X, Y_1, \ldots, Y_\eta) \in \mathbb{H}^2 \times \mathbb{G}^{2+\eta}$.
- $\mathsf{Sign}\left(\mathsf{sk}, \left(M, \tilde{M}\right), \left((M'_1, \tilde{M}'_1), \ldots, (M'_\eta, \tilde{M}'_\eta)\right)\right)$: To sign $\left((M, \tilde{M}), \left((M'_1, \tilde{M}'_1), \ldots, (M'_\eta, \tilde{M}'_\eta)\right)\right) \in \widehat{\mathbb{GH}}^{1+\eta}$, select $r \leftarrow \mathbb{Z}_p$ and set $R := G^r$, and $S := (M^{r+x} \prod_{i=1}^{\eta} M_i'^{r+y_i} R^{w_1} U)^{\frac{1}{w_2}}$. Return $\sigma := (R, S) \in \mathbb{G}^2$.
- $\mathsf{Verify}\left(\mathsf{vk}, \left((M, \tilde{M}), \left((M'_1, \tilde{M}'_1), \ldots, (M'_\eta, \tilde{M}'_\eta)\right)\right), \sigma = (R, S)\right)$: Return 1 only if $R, S \in \mathbb{G}$, $(M, \tilde{M}) \in \widehat{\mathbb{GH}}$, for all $i \in [\eta] : (M'_i, \tilde{M}'_i) \in \widehat{\mathbb{GH}}$, and

$$e(S, \tilde{W}_2) = e(R, \tilde{M} \prod_{i=1}^{\eta} \tilde{M}'_i \tilde{W}_1) e(X, \tilde{M}) \prod_{i=1}^{\eta} e(Y_i, \tilde{M}'_i) e(U, \tilde{H}),$$

otherwise, return 0.

Remark 1. We can set $Y_1 = G$ which reduces the size of the verification key by one group element.

Security of the Scheme. Correctness of the scheme follows by inspection and is straightforward to verify. We now prove the following theorem.

Theorem 4. *The scheme is sEUF-CMA-RMA secure in the generic group model.*

Proof. We show that no linear combinations representing Laurent polynomials (of degrees ranging from -1 to 2 after q sign queries) in the discrete logarithms of the group elements the adversary sees correspond to a forgery on a new message.

At the start of the game, the only elements in $\mathbb{H}$ the adversary sees are $\tilde{H}$, $\tilde{W}_1$, $\tilde{W}_2$ which correspond to the discrete logarithms $1, w_1, w_2$, respectively, whereas the only elements in $\mathbb{G}$ the adversary sees are G, $X, Y_1, \ldots, Y_\eta, U$ which correspond to the discrete logarithms 1, x, $y_1, \ldots, y_\eta, u$, respectively.

Note that the only elements of $\mathbb{H}$ the q sign queries return are the uniformly random parts of the message $\{\boldsymbol{\tilde{M}'_{i,j}}\}$ for $i \in [q]$ and $j \in [\eta]$. Thus, at the i-th sign query on the message $(M_i, \tilde{N}_i) \in \widehat{\mathbb{GH}}$, m_i and n_i the discrete logarithms of M_i and $\tilde{N}_i$, respectively, can only be linear combinations of the discrete logarithms of the elements in $\mathbb{G}$ and $\mathbb{H}$, respectively, the adversary sees up to that point of time. Thus, we have

$$m_i = a_{m_i} + b_{m_i} u + c_{m_i} x + \sum_{k=1}^{\eta} d_{m_{i,k}} y_k + \sum_{\ell=1}^{i-1} \sum_{k=1}^{\eta} e_{m_{i,\ell,k}} m'_{\ell,k} + \sum_{j=1}^{i-1} f_{m_{i,j}} r_j$$

$$+ \sum_{j=1}^{i-1} g_{m_{i,j}} \left(\frac{m_j (r_j + x) + \sum_{k=1}^{\eta} m'_{j,k} (r_j + y_k) + r_j w_1 + u}{w_2} \right)$$

$$n_i = a_{n_i} + b_{n_i} w_1 + c_{n_i} w_2 + \sum_{\ell=1}^{i-1} \sum_{k=1}^{\eta} d_{n_{i,\ell,k}} m'_{\ell,k}$$

Since for all $i \in [q]$, we must have that $(M_i, \tilde{N}_i) \in \widehat{\mathbb{GH}}$, i.e. $m_i = n_i$, we must have that $a_{m_i} = a_{n_i}$, $b_{m_i} = b_{n_i} = c_{m_i} = c_{n_i} = 0$, $d_{m_{i,k}} = 0$ for all $k \in [\eta]$, $f_{m_{i,j}} = g_{m_{i,j}} = 0$ for all $j \in [i-1]$, and $d_{n_{i,\ell,k}} = e_{m_{i,\ell,k}}$ for all $\ell \in [i-1]$ and $k \in [\eta]$. Thus, we have

$$m_i = n_i = a_{m_i} + \sum_{\ell=1}^{i-1} \sum_{k=1}^{\eta} e_{m_{i,\ell,k}} m'_{\ell,k}$$

If the message is well-formed, then at the i-th sign query, the adversary will receive a signature of the form $\sigma_i = (r_i, s_i)$, where s_i is of the following form:

$$s_i = \frac{m_i(r_i + x) + \sum_{j=1}^{\eta} m'_{i,j}(r_i + y_j) + r_i w_1 + u}{w_2}$$

At the end of the game (after at most q sign queries), we must have

$$m^* = n^* = a_m + \sum_{\ell=1}^{q} \sum_{k=1}^{\eta} e_{m_{\ell,k}} m'_{\ell,k}$$
$$m'^*_j = n'^*_j = a_{m'_j} + \sum_{\ell=1}^{q} \sum_{k=1}^{\eta} e_{m'_{j,\ell,k}} m'_{\ell,k} \text{ for all } j \in [\eta]$$

Similarly, since the adversary can only construct her forgery as linear combinations of the Laurent polynomials she sees in the game, we have at the end of the game that r^* and s^* must be linear combinations of the Laurent polynomials in $\mathbb{G}$. Thus, we have:

$$r^* = a_r + b_r u + c_r x + \sum_{i=1}^{\eta} d_{r_i} y_i + \sum_{i=1}^{q} \sum_{j=1}^{\eta} e_{r_{i,j}} m'_{i,j} + \sum_{i=1}^{q} f_{r_i} r_i$$
$$+ \sum_{i=1}^{q} g_{r_i} \Big(\frac{m_i(r_i + x) + \sum_{j=1}^{\eta} m'_{i,j}(r_i + y_j) + r_i w_1 + u}{w_2} \Big)$$
$$s^* = a_s + b_s u + c_s x + \sum_{i=1}^{\eta} d_{s_i} y_i + \sum_{i=1}^{q} \sum_{j=1}^{\eta} e_{s_{i,j}} m'_{i,j} + \sum_{i=1}^{q} f_{s_i} r_i$$
$$+ \sum_{i=1}^{q} g_{s_i} \Big(\frac{m_i(r_i + x) + \sum_{j=1}^{\eta} m'_{i,j}(r_i + y_j) + r_i w_1 + u}{w_2} \Big)$$

Since by the verification equation we must have that:

$$s^* w_2 = r^*(m^* + \sum_{j=1}^{\eta} m'^*_j + w_1) + m^* x + \sum_{j=1}^{\eta} m'^*_j y_j + u$$

Thus, we must have that:

$$
\begin{aligned}
&a_s w_2 + b_s u w_2 + c_s x w_2 + \sum_{i=1}^{\eta} d_{s_i} y_i w_2 + \sum_{i=1}^{q}\sum_{j=1}^{\eta} e_{s_{i,j}} m'_{i,j} w_2 + \sum_{i=1}^{q} f_{s_i} r_i w_2 \\
&\qquad + \sum_{i=1}^{q} g_{s_i}\Big(m_i(r_i + x) + \sum_{j=1}^{\eta} m'_{i,j}(r_i + y_j) + r_i w_1 + u\Big) \\
&\quad =\Big(a_r + b_r u + c_r x + \sum_{i=1}^{\eta} d_{r_i} y_i + \sum_{i=1}^{q}\sum_{j=1}^{\eta} e_{r_{i,j}} m'_{i,j} + \sum_{i=1}^{q} f_{r_i} r_i \\
&\qquad + \sum_{i=1}^{q} g_{r_i}\Big(\frac{m_i(r_i + x) + \sum_{j=1}^{\eta} m'_{i,j}(r_i + y_j) + r_i w_1 + u}{w_2}\Big)\Big)\Big(m^* + \sum_{i=1}^{\eta} m_i'^* + w_1\Big) \\
&\qquad + m^* x + \sum_{i=1}^{\eta} m_i'^* y_i + u
\end{aligned}
$$

There is no term of the form $\frac{uw_1}{w_2}$ on the LHS, so we must have that for all $i \in [q]$ that $g_{r_i} = 0$. Also, for all $i \in [\eta]$, there are no terms of the form xw_1, $y_i w_1$, uw_1 or w_1 on the LHS so we must have that $c_r = 0$, $d_{r_i} = 0$ for all $i \in [\eta]$, $b_r = 0$ and $a_r = 0$. Thus, we have:

$$
\begin{aligned}
&a_s w_2 + b_s u w_2 + c_s x w_2 + \sum_{i=1}^{\eta} d_{s_i} y_i w_2 + \sum_{i=1}^{q}\sum_{j=1}^{\eta} e_{s_{i,j}} m'_{i,j} w_2 + \sum_{i=1}^{q} f_{s_i} r_i w_2 \\
&\qquad + \sum_{i=1}^{q} g_{s_i}\Big(m_i(r_i + x) + \sum_{j=1}^{\eta} m'_{i,j}(r_i + y_j) + r_i w_1 + u\Big) \\
&= \Big(\sum_{i=1}^{q}\sum_{j=1}^{\eta} e_{r_{i,j}} m'_{i,j} + \sum_{i=1}^{q} f_{r_i} r_i\Big)\Big(m^* + \sum_{i=1}^{\eta} m_i'^* + w_1\Big) + m^* x + \sum_{i=1}^{\eta} m_i'^* y_i + u
\end{aligned}
$$

There are no terms on the RHS with any of the monomials w_2, uw_2, xw_2, $y_i w_2$ for any $i \in [\eta]$, $r_i w_2$ for any $i \in [q]$, or $m'_{i,j} w_2$ for any $i \in [q]$ and $j \in [\eta]$. Thus, we must have that $a_s = 0$, $b_s = 0$, $c_s = 0$, $d_{s_i} = 0$ for all $i \in [\eta]$, $f_{s_i} = 0$ for all $i \in [q]$, and for all $i \in [q]$ and all $j \in [\eta]$ that $e_{s_{i,j}} = 0$. Thus, we have:

$$
\begin{aligned}
&\sum_{i=1}^{q} g_{s_i}\Big(m_i(r_i + x) + \sum_{j=1}^{n} m'_{i,j}(r_i + y_j) + r_i w_1 + u\Big) \\
&=\Big(\sum_{i=1}^{q}\sum_{j=1}^{\eta} e_{r_{i,j}} m'_{i,j} + \sum_{i=1}^{q} f_{r_i} r_i\Big)\Big(m^* + \sum_{i=1}^{\eta} m_i'^* + w_1\Big) + m^* x + \sum_{i=1}^{\eta} m_i'^* y_i + u
\end{aligned}
$$

There are no terms of the form $m'_{i,j} w_1$ for any $i \in [q]$ and any $j \in [\eta]$ on the LHS. Thus, we must have that $e_{r_{i,j}} = 0$ for all $i \in [q]$ and all $j \in [\eta]$ and hence we must have that:

$$\begin{aligned}&\sum_{i=1}^{q} g_{s_i}\Big(m_i(r_i+x)+\sum_{j=1}^{\eta} m'_{i,j}(r_i+y_j)+r_iw_1+u\Big)\\ =&\sum_{i=1}^{q} f_{r_i}r_im^* + \sum_{i=1}^{q} f_{r_i}r_i\sum_{i=1}^{\eta} m_i'^* + \sum_{i=1}^{q} f_{r_i}r_iw_1 + m^*x + \sum_{i=1}^{\eta} m_i'^* y_i + u\end{aligned}$$

By the term u we have that $\sum\limits_{i=1}^{q} g_{s_i} = 1$ and we must have that there is at least one value of $g_{s_i} \neq 0$. Also, by the term r_iw_1 we have that $g_{s_i} = f_{r_i}$ for all $i \in [q]$. Note that $m'_{i,j}$ for all $i \in [q]$ and all $j \in [\eta]$ on the LHS are all chosen uniformly at random by the sign oracle. Also, there is no term on the LHS containing the monomial $m_{i,j}r_k$ for any $k \neq i$. Thus, we cannot have for any $i, j \in [q]$ where $i \neq j$ that $f_{r_i} \neq 0$ and $f_{r_j} \neq 0$. This means we must have for some $i \in [q]$ that:

$$\begin{aligned}&g_{s_i}m_i(r_i+x)+g_{s_i}\sum_{j=1}^{\eta} m'_{i,j}(r_i+y_j)+g_{s_i}r_iw_1+g_{s_i}u\\ &= f_{r_i}r_im^* + f_{r_i}r_i\sum_{i=1}^{\eta} m_i'^* + f_{r_i}r_iw_1 + m^*x + \sum_{i=1}^{\eta} m_i'^* y_i + u\end{aligned}$$

Since we must have that $\sum\limits_{i=1}^{q} g_{s_i} = 1$ and for all $i \in [q]$ that $g_{s_i} = f_{r_i}$, we must have:

$$\begin{aligned}&m_i(r_i+x)+\sum_{j=1}^{\eta} m'_{i,j}(r_i+y_j)+r_iw_1+u\\ &= r_im^* + r_i\sum_{i=1}^{\eta} m_i'^* + r_iw_1 + m^*x + \sum_{i=1}^{\eta} m_i'^* y_i + u\end{aligned}$$

By the monomial x, we must have that $m^* = m_i$, whereas by the monomial y_j we must have that $m'_{i,j} = m_j'^*$ for all $j \in [\eta]$. The above also means we have $r^* = r_i$ and $s^* = s_i$. This means (r^*, s^*) is not a valid forgery.

Remark 2. The proof holds even if we have that $y_1 = 1$ which means we can reduce the size of the verification key by eliminating 1 group element.

This concludes the proof. □

References

1. M. Abe, M. Ambrona, M. Ohkubo, and M. Tibouchi. Lower Bounds on Structure-Preserving Signatures for Bilateral Messages. In *SCN 2018*, Springer LNCS 11035, 3–22, 2018.

2. M. Abe, M. Chase, B. David, M. Kohlweiss, R. Nishimaki and M. Ohkubo. Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions. In *ASIACRYPT 2012*, Springer LNCS 7658, 4–24, 2012.
3. M. Abe, B. David, M. Kohlweiss, R. Nishimaki and M. Ohkubo. Tagged One-Time Signatures: Tight Security and Optimal Tag Size. In *PKC 2013*, Springer LNCS 7778, 312–331, 2013.
4. M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev and M. Ohkubo. Structure-preserving signatures and commitments to group elements. In *CRYPTO 2010*, Springer LNCS 6223, 209–236, 2010.
5. M. Abe, J. Groth, K. Haralambiev and M. Ohkubo. Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups. In *CRYPTO 2011*, Springer LNCS 6841, 649–666, 2011.
6. M. Abe, J. Groth and M. Ohkubo. Separating Short Structure-Preserving Signatures from Non-interactive Assumptions. In *ASIACRYPT 2011*, Springer LNCS 7073, 628–646, 2011.
7. M. Abe, J. Groth, M. Ohkubo and M. Tibouchi. Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures. In TCC 2014, Springer LNCS 8349, 688–712, 2014.
8. M. Abe, J. Groth, M. Ohkubo and M. Tibouchi. Structure-Preserving Signatures from Type II Pairings. In CRYPTO 2014, Springer LNCS 8616, 390–407, 2014.
9. M. Abe, D. Hofheinz, R. Nishimaki, M. Ohkubo and J. Pan. Compact Structure-Preserving Signatures with Almost Tight Security. In CRYPTO 2017, Springer LNCS 10402, 548–580, 2017.
10. M. Abe, M. Kohlweiss, M. Ohkubo and M. Tibouchi. Fully Structure-Preserving Signatures and Shrinking Commitments. In *EUROCRYPT 2015*, Springer LNCS 9057, 35–65, 2015.
11. J.H. An, Y. Dodis and T. Rabin. On the Security of Joint Signature and Encryption. In *EUROCRYPT 2002*, Springer LNCS 2332, 83–107, 2002.
12. N. Attrapadung, B. Libert and T. Peters. Computing on authenticated data: new privacy definitions and constructions. In *ASIACRYPT 2012*, Springer LNCS 7658, 367–385, 2012.
13. F. Baldimtsi, M. Chase, G. Fuchsbauer, and M. Kohlweiss. Anonymous Transferable E-Cash. In *PKC 2015*, Springer LNCS 9020, 101–124, 2015.
14. G. Barthe, E. Fagerholm, D. Fiore, A. Scedrov, B. Schmidt and M. Tibouchi. Strongly-Optimal Structure Preserving Signatures from Type II Pairings: Synthesis and Lower Bounds. In *PKC 2015*, Springer LNCS 9020, 355–376, 2015.
15. D. Bernhard, G. Fuchsbauer and E. Ghadafi. Efficient Signatures of Knowledge and DAA in the Standard Model. In *ACNS 2013*, Springer LNCS 7954, 518–533, 2013.
16. E. Brickell, J. Camenisch and L. Chen. Direct anonymous attestation. *ACM CCS 2004*, ACM, 132–145, 2004.
17. J. Camenisch, M. Dubovitskaya and K. Haralambiev. Efficient Structure-Preserving Signature Scheme from Standard Assumptions. In *SCN 2012*, Springer LNCS 7485, 76–94, 2012.
18. J. Camenisch, M. Dubovitskaya, K. Haralambiev, and M. Kohlweiss. Composable and Modular Anonymous Credentials: Definitions and Practical Constructions. In *ASIACRYPT 2015*, Springer LNCS 9453, 262–288, 2015.
19. M. Chase and M. Kohlweiss. A New Hash-and-Sign Approach and Structure-Preserving Signatures from DLIN. In *SCN 2012*, Springer LNCS 7485, 131–148, 2012.

20. S. Chatterjee and A. Menezes. Type 2 Structure-Preserving Signature Schemes Revisited. In *ASIACRYPT 2015*, Springer LNCS 9452, 286–310, 2015.
21. D. Chaum and E. van Heyst. Group signatures. In *EUROCRYPT 1991*, Springer LNCS 547, 257–265, 1991.
22. T. ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In IEEE Transactions on Information Theory, volume 31(4), 1985, 469–472, 1985.
23. A. El Kaafarani and E. Ghadafi. Attribute-Based Signatures with User-Controlled Linkability Without Random Oracles. In *Cryptography and Coding (IMACC)*, Springer LNCS 10655, 161–184, 2017.
24. A. El Kaafarani, E. Ghadafi and D. Khader. Decentralized Traceable Attribute-Based Signatures. In *CT-RSA 2014*, Springer LNCS 8366, 327–348, 2014.
25. A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *CRYPTO 1986*, Springer LNCS 263, 186–194, 1986.
26. G. Fuchsbauer. Commuting signatures and verifiable encryption. In *EUROCRYPT 2011*, Springer LNCS 6632, 224–245, 2011.
27. G. Fuchsbauer, C. Hanser and D. Slamanig. Practical Round-Optimal Blind Signatures in the Standard Model. In *CRYPTO 2015*, Springer LNCS 9216, 233–253, 2015.
28. S. Galbraith, K. Paterson and N.P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, **156**, 2008, 3113–3121, 2008.
29. R. Gay, D. Hofheinz, L. Kohl, and J. Pan. More Efficient (Almost) Tightly Secure Structure-Preserving Signatures. In *EUROCRYPT 2018*, Springer LNCS 10821, 230–258, 2018.
30. E. Ghadafi. Formalizing Group Blind Signatures and Practical Constructions without Random Oracles. In *ACISP 2013*, Springer LNCS 7959, 330–346, 2013.
31. E. Ghadafi. Short Structure-Preserving Signatures. In *CT-RSA 2016*, Springer LNCS 9610, 305–321, 2016.
32. E. Ghadafi. More Efficient Structure-Preserving Signatures - Or: Bypassing the Type-III Lower Bounds. In *ESORICS 2017*, Springer LNCS 10493, 43–61, 2017.
33. E. Ghadafi. How Low Can You Go? Short Structure-Preserving Signatures for Diffie-Hellman Vectors. In *Cryptography and Coding (IMACC)*, Springer LNCS 10655, 185–204, 2017.
34. M. Green and S. Hohenberger. Universally Composable Adaptive Oblivious Transfer. In *ASIACRYPT 2008*, Springer LNCS 5350, 179–197, 2008.
35. J. Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In *ASIACRYPT 2006*, Springer LNCS 4284, 444–459, 2006.
36. J. Groth. Efficient Fully Structure-Preserving Signatures for Large Messages. In *ASIACRYPT 2015*, Springer LNCS 9452, 239-259, 2015.
37. J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In SIAM Journal on Computing, volume 41(5), 1193–1232, 2012.
38. D. Hofheinz and T. Jager. Tightly Secure Signatures and Public-Key Encryption. In *CRYPTO 2012*, Springer LNCS 7417, 590–607, 2012.
39. C.S. Jutla and A. Roy. Improved Structure Preserving Signatures Under Standard Bilinear Assumptions. In *PKC 2017*, Springer LNCS 10175, 183–209, 2017.
40. E. Kiltz, J. Pan and H. Wee. Structure-Preserving Signatures from Standard Assumptions, Revisited. In *CRYPTO 2015*, Springer LNCS 9216, 275–295, 2015.
41. B. Libert, T. Peters and M. Yung. Short Group Signatures via Structure-Preserving Signatures: Standard Model Security from Simple Assumptions. In *CRYPTO 2015*, Springer LNCS 9216, 296–316, 2015.

42. H.K. Maji, M. Prabhakaran and M. Rosulek. Attribute-Based Signatures. In *CT-RSA 2011*, Springer LNCS 6558, 376–392, 2011.
43. M. Mambo, K. Usuda and E. Okamoto. Proxy Signatures for Delegating Signing Operation. In *ACM CCS 1996*, ACM, 48–57, 1996.
44. U. Maurer. Abstract models of computation in cryptography. In *Cryptography and Coding (IMACC)*, Springer LNCS 3796, 1–12, 2005.
45. V. Shoup. Lower Bounds for Discrete Logarithms and Related Problems. In *EUROCRYPT 1997*, Springer LNCS 3152, 41–55, 1997.
46. I. Teranisi, J. Furukawa and K. Sako. k-Times Anonymous Authentication. In *ASIACRYPT 2004*, Springer LNCS 3329, 308–322, 2004.
47. Y. Wang, Z. Zhang, T. Matsuda, G. Hanaoka and K. Tanaka. How to Obtain Fully Structure-Preserving (Automorphic) Signatures from Structure-Preserving Ones. In *ASIACRYPT 2016*, Springer LNS 10032, 465–495, 2016.