How Low Can You Go? Short Structure-Preserving Signatures for Diffie-Hellman Vectors

Essam Ghadafi(✉)

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

Abstract. Structure-Preserving Signatures (SPSs) are an important tool for the design of modular cryptographic protocols. It has been proven that such schemes in the most efficient Type-3 bilinear group setting have a lower bound of 3-element signatures, which must include elements from both base groups, and a verification overhead of at least 2 Pairing-Product Equations (PPEs). Very recently, Ghadafi (ESORICS 2017) showed that by restricting the message space to the set of Diffie-Hellman pairs (which does not hinder applicability of the schemes), some of the existing lower bounds for the single message case can be circumvented. However, the case of signing multiple messages, which is required for many applications, was left as an open problem since the techniques used for signing single messages do not seem to lend themselves to the multi-message setting. In this work we investigate this setting and answer the question in the affirmative. We construct schemes that sign vectors of messages and which yield shorter signatures than optimal schemes for vectors of unilateral messages. More precisely, we construct 2 fully randomiazble schemes that sign vectors of Diffie-Hellman pairs yielding signatures consisting of only 2 elements regardless of the size of the vector signed. We also construct a unilateral scheme that signs a pair of messages yielding signatures consisting of 3 elements from the shorter base group. All of our schemes require a single PPE for verification (not counting the cost of verifying the well-formedness of the messages). Thus, all of our schemes compare favourably to all existing schemes with respect to signature size and verification overhead. Even when considering single messages, our first 2 schemes compare favourably to the best existing schemes in many aspects including the verification overhead and the key size.

Keywords: Digital signatures · Structure-preserving signatures · Type-3 groups

1 Introduction

Structure-Preserving Signatures (SPSs) [3] are pairing-based signature schemes where the message, the verification key and the signature consist of only group

M. O'Neill (Ed.): IMACC 2017, LNCS 10655, pp. 185–204, 2017.
https://doi.org/10.1007/978-3-319-71045-7_10

elements from one or both base groups, and signature verification requires evaluating Pairing-Product Equations (PPEs). Due to their elegant structure and the fact that they compose nicely with existing widely used tools such as ElGamal encryption [20] and Groth-Sahai proofs [34], SPS schemes are an ideal building block for designing cryptographic protocols not relying on random oracles [22].

The notion has numerous applications which include group signatures, e.g [3,38], blind signatures, e.g. [3,25], attribute-based signatures, e.g. [21], tightly secure encryption, e.g. [2,35], malleable signatures, e.g. [9], anonymous credentials, e.g. [16,24], network coding, e.g. [9], oblivious transfer, e.g. [31], direct anonymous attestation, e.g. [13,28], and e-cash, e.g. [10].

Related Work. The term "structure-preserving signature" was first formally introduced by Abe et al. [3] but earlier schemes conforming to the definition were given in [31,32]. The notion has received a significant amount of attention and many studies on the notion have been published. Constructions of such schemes in the Type-3 setting (cf. Section 2.1) include [3,4,6,19,27,33]. The vast majority of those constructions rely on security proofs in the generic group model [40,41]. Abe et al. [4] proved that signatures of any scheme in the Type-3 bilinear group setting must contain at least 3 elements, which must include elements from both base groups, and require at least 2 PPEs for verification. This rules out the existence of schemes with unilateral signatures, i.e. where all components of the signature are from the same group.

Constructions relying on standard assumptions, e.g. DLIN and DDH, were given by [1,2,15,18,36–38]. Abe et al. [5] proved that it is impossible to base the security of an optimal Type-3 scheme on non-interactive intractability assumptions. Their result guarantees that schemes based on non-interactive intractability assumptions can never be as efficient as their counterparts relying on interactive assumptions or those proven secure directly in the generic group model. In fact all existing constructions based on standard (static) assumptions are far less efficient than existing optimal schemes.

Recently, Ghadafi [28] gave a randomizable scheme yielding signatures consisting of 3 elements from the shorter base group which signs a single Diffie-Hellman (cf. Section 2.1) pair. Signatures of his scheme are shorter than those of optimal schemes for unilateral messages since the bit size of the elements of the second base group are at least twice that of those from the first base group. Verification in his scheme requires, besides checking the well-formedness of the message, the evaluation of 2 PPEs. However, his scheme is only capable of signing a single message and it is unclear whether it can be extended (or even if that is at all possible) to signing multiple messages while preserving the signature size. More recently, Ghadafi [29] defined the notion of unilateral structure-preserving signatures on Diffie-Hellman pairs and gave constructions for a single Diffie-Hellman pair yielding signatures consisting of only 2 elements from the shorter base group. Ghadafi 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 [14], which is a protocol deployed in practice, and attribute-based signatures [39] as an example. Even though Ghadafi [29] 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.

Constructions in the Type-2 setting (where there is an efficiently computable homomorphism between the base groups in one direction) were given in [7,11,19]. Fully structure-preserving schemes where even the secret key consists of only group elements from the base groups were recently given by [8,33,42].

Numerous applications require signing a vector of group elements, e.g. when certifying the public key of an encryption/signature scheme, without hindering the structure of the messages, i.e. without hashing. This is particularly important when the aim is to avoid relying on random oracles. Therefore, the design of efficient signature schemes conforming to those requirements would have implications for various applications. Note that SPS schemes for Diffie-Hellman tuples proved useful for many applications see e.g. [3,13,24,27,29].

Our Contribution. We construct 3 new fully randomizable structure-preserving schemes for vectors of messages which yield shorter signatures than all existing schemes for vectors of unilateral messages. Our first 2 schemes yield signatures consisting of 2 elements and requiring 1 PPE for verification. Our third scheme which signs a vector of size 2 yield (unilateral) signatures consisting of 3 elements from the shorter base group and require 1 PPE for verification. The verification overhead of our schemes also compares favourably to exiting schemes, in particular, when verifying multiple signatures on the same message vector, which is what a number of applications require.

Even when signing single messages, our first 2 schemes compare favourably in many measures, e.g. the key size and verification overhead, to the best existing scheme [29].

Paper Organization. We provide some preliminary definitions in Sect. 2. In Sect. 3 we give two new fully randomizable schemes for signing arbitrary vectors of messages. In Sect. 4 we give a scheme for signing a pair of messages. In Sect. 5 we compare the efficiency of our constructions with that of existing ones.

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 $\{1, \ldots, k\}$. We use capital letters for group elements and small letters for field elements.

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 $e : \mathbb{G} \times \mathbb{H} \longrightarrow \mathbb{T}$. For clarity, elements of $\mathbb{H}$ will be accented with $\tilde{}$. We use multiplicative notation for all the groups. We let $\mathbb{G}^\times := \mathbb{G} \setminus \{1_\mathbb{G}\}$ and $\mathbb{H}^\times := \mathbb{H} \setminus \{1_\mathbb{H}\}$. In this paper, we work in the efficient Type-3 setting [26], where $\mathbb{G} \neq \mathbb{H}$ and there is no efficiently computable homomorphism between the 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 $\widehat{\mathbb{GH}}$ 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 pairs in [3,23]. An important observation here is that techniques used for batch verification, e.g. [12,17], can be applied when verifying the well-formedness of a vector of Diffie-Hellman pairs. This reduces the cost for verifying a vector of ℓ pairs from 2ℓ pairings to 2 pairings.

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 $\mathcal{P}$, it outputs a pair of secret/verification keys $(\mathsf{sk}, \mathsf{vk})$.
$\mathsf{Sign}(\mathsf{sk}, m)$ on input sk and a message $m \in \mathcal{M}$, it outputs a signature σ.
$\mathsf{Verify}(\mathsf{vk}, m, \sigma)$ outputs 1 if σ is a valid signature on m w.r.t. vk and 0 otherwise.

Besides the usual correctness requirement, we require existential unforgeability.

Definition 1 (Existential Unforgeability). *A signature scheme $\mathcal{DS}$ over a bilinear group generator $\mathcal{BG}$ is* Existentially-Unforgeable against adaptive Chosen-Message Attack (EUF-CMA) *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 of messages queried to Sign.

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

A weaker variant of EUF-CMA is *Existential Unforgeability against a Random-Message Attack (EUF-RMA)* in which the sign oracle samples a message uniformly from the message space and returns the message and a signature on it. In one-time signatures, the adversary is restricted to a single signing query.

We consider schemes which are publicly re-randomizable where there is an algorithm $\mathsf{Randomize}$ that on input (vk, m, σ) outputs a new signature σ' on m. A desirable property for such class of schemes is that randomized signatures are indistinguishable from fresh signatures.

Definition 2 (Randomizability). *A signature scheme $\mathcal{DS}$ over a bilinear group generator $\mathcal{BG}$ is* randomizable *if for all $\kappa \in \mathbb{N}$ for all stateful adversaries $\mathcal{A}$ the following probability is negligibly close to $\frac{1}{2}$.*

$$\Pr\left[\begin{array}{l}\mathcal{P} \leftarrow \mathcal{BG}(1^\kappa); (\mathsf{sk}, \mathsf{vk}) \leftarrow \mathsf{KeyGen}(\mathcal{P}); (\sigma^*, m^*) \leftarrow \mathcal{A}(\mathcal{P}, \mathsf{sk}, \mathsf{vk}); \sigma_0 \leftarrow \mathsf{Sign}(\mathsf{sk}, m^*);\\ \sigma_1 \leftarrow \mathsf{Randomize}(\mathsf{vk}, m^*, \sigma^*); b \leftarrow \{0,1\} : \mathsf{Verify}(\mathsf{vk}, m^*, \sigma^*) = 1 \wedge \mathcal{A}(\sigma_b) = b\end{array}\right]$$

When the above is exactly $\frac{1}{2}$, we say the scheme has *Perfect Randomizability.*

2.3 Structure-Preserving Signatures

Structure-preserving signatures [3] are signature schemes defined over bilinear groups where the messages, the verification key and signatures are all group elements from either or both base groups, and verifying signatures only involves deciding group membership of the signature components 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 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 Constant-Size Schemes for Diffie-Hellman Vectors

In this section, we give 2 new schemes for signing a vector of Diffie-Hellman pairs.

3.1 Scheme I

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

- $\mathsf{KeyGen}(\mathcal{P})$: Select $x_1, \ldots, x_\ell, y \leftarrow \mathbb{Z}_p$. Set $X_i := G^{x_i}$ for all $i \in [\ell]$, $\tilde{Y} := \tilde{H}^y$, $\mathsf{sk} := (x_1, \ldots, x_\ell, y)$ and $\mathsf{vk} := (X_1, \ldots, X_\ell, \tilde{Y}) \in \mathbb{G}^\ell \times \mathbb{H}$.
- $\mathsf{Sign}\left(\mathsf{sk}, \left((M_1, \tilde{N}_1), \ldots, (M_\ell, \tilde{N}_\ell)\right)\right)$: To sign $\left((M_1, \tilde{N}_1), \ldots, (M_\ell, \tilde{N}_\ell)\right) \in \widehat{\mathbb{GH}}^{\ell}$, select $r \leftarrow \mathbb{Z}_p$ and set $R := G^r$, and $\tilde{S} := (\prod_{i=1}^{\ell} \tilde{N}_i^{x_i} \cdot \tilde{Y}^{x_1} \cdot \tilde{H})^{\frac{1}{r}}$. Return $\sigma := (R, \tilde{S}) \in \mathbb{G} \times \mathbb{H}$.
- $\mathsf{Verify}\left(\mathsf{vk}, \left((M_1, \tilde{N}_1), \ldots, (M_\ell, \tilde{N}_\ell)\right), \sigma = (R, \tilde{S})\right)$: Return 1 iff $R \in \mathbb{G}$, $\tilde{S} \in \mathbb{H}$, for all $i \in [\ell] : (M_i, \tilde{N}_i) \in \widehat{\mathbb{GH}}$, and

$$e(R, \tilde{S}) = \prod_{i=1}^{\ell} e(X_i, \tilde{N}_i) e(X_1, \tilde{Y}) e(G, \tilde{H}) \cdot$$

- $\mathsf{Randomize}\left(\mathsf{vk}, \left((M_1, \tilde{N}_1), \ldots, (M_\ell, \tilde{N}_\ell)\right), \sigma = (R, \tilde{S})\right)$: Select $r' \leftarrow \mathbb{Z}_p$, and return $\sigma' := (R^{r'}, \tilde{S}^{\frac{1}{r'}})$.

Efficiency of the Scheme. The public key for signing a vector of size ℓ has size $\ell|\mathbb{G}| + |\mathbb{H}|$ whereas the signature is of size $|\mathbb{G}| + |\mathbb{H}|$ regardless of the size of the message vector. Thus, our signatures are shorter than all existing schemes since the best existing optimal schemes for unilateral messages, e.g. [4], have signatures of size $2|\mathbb{G}|+|\mathbb{H}|$. Assuming that the messages are already well-formed, verification requires only a single PPE with $\ell+2$ pairings where 1 pairing, i.e. the pairing $e(G, \tilde{H})$ can be pre-computed. Hence, we only require $\ell + 1$ pairings for each signature after the first signature. If the messages are already assumed to be well-formed, this compares favourably to existing schemes since the most efficient existing scheme requires 2 PPE for verification. The scheme yields very short proofs of knowledge when combined with Groth-Sahai proofs [34] as one requires a proof for a linear (rather than quadratic) equation. As a result, our scheme outperforms the best existing scheme [29] in this respect. Refer to Sect. 5 for concrete efficiency comparison with existing schemes.

Security of the Scheme. The scheme is perfectly randomizable as the distribution of re-randomized signatures is identical to that of fresh signatures on the same vector. We now prove the following theorem.

Theorem 1. *The scheme is EUF-CMA secure.*

Proof. Correctness of the scheme follows by inspection and is straightforward to verify. The following two lemmata prove unforgeability of the scheme against adaptive chosen-message attacks. Lemma 1 proves that the case when $\ell = 1$ is secure in the generic group model whereas Lemma 2 reduces any attack on the scheme when $\ell > 1$ to the case when $\ell = 1$ which is proved by Lemma 1.

Lemma 1. *The scheme for $\ell = 1$ is EUF-CMA secure in the generic group model.*

Proof. We proceed by proving that no linear combinations (which represent Laurent polynomials in the discrete logarithms) of the group elements the adversary sees in the game correspond to a forgery on a new message.

At the start of the game, the only elements in $\mathbb{H}$ the adversary sees are $\tilde{H}$, $\tilde{Y}$ which correspond to the discrete logarithms 1 and y, respectively. Also, at the start of the game the only elements in $\mathbb{G}$ the adversary sees are G, X which correspond to the discrete logarithms 1 and x, respectively.

At the j-th sign query on the message $(M_j, \tilde{N}_j)$, m_j and n_j (the discrete logarithms of M_j and $\tilde{N}_j$, respectively, can only be a linear combination 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

$$m_j = a_{m_j} + b_{m_j} x + \sum_{i=1}^{j-1} c_{m_j,i} r_i$$

$$n_j = a_{n_j} + b_{n_j} y + \sum_{i=1}^{j-1} c_{n_j,i} \frac{n_i x + xy + 1}{r_i}$$

For the message to satisfy $(M_j, \tilde{N}_j) \in \widehat{\mathbb{GH}}$, we must have that $m_j = n_j$ and hence we must have that $a_{m_j} = a_{n_j}$, $b_{m_j} = b_{n_j} = 0$ and for all i that $c_{m_j,i} = c_{n_j,i} = 0$. This ensures that the message queried is nothing but a constant polynomial. If the message is well-formed [1], the sign oracle responds with a signature of the form

$$\left(r_j, s_j = \frac{n_j x + xy + 1}{r_j}\right)$$

Since the adversary is generic, she can only construct $\Big((M^*, \tilde{N}^*), \sigma^* = (R^*, \tilde{S}^*)\Big)$ as a linear combination of the group elements she sees in the game. Thus, we have

$$m^* = a_m + b_m x + \sum_{i=1}^{q} c_{m,i} r_i \qquad r^* = a_r + b_r x + \sum_{i=1}^{q} c_{r,i} r_i$$

$$n^* = a_n + b_n y + \sum_{i=1}^{q} c_{n,i} \frac{n_i x + xy + 1}{r_i} \qquad s^* = a_s + b_s y + \sum_{i=1}^{q} c_{s,i} \frac{n_i x + xy + 1}{r_i}$$

Since the forged message $(M^*, \tilde{N}^*)$ must correspond to a Diffie-Hellman pair, we must have $m^* = n^*$ and thus $a_m = a_n$, $b_m = b_n = 0$ and $c_{m,i} = c_{n,i} = 0$ for all $i \in [q]$ and hence $m^* = n^* = a_m$. For the forgery to be accepted, r^* and s^* must satisfy $r^* s^* = n^* x + xy + 1$. Therefore, we must have

$$\left(a_r + b_r x + \sum_{i=1}^{q} c_{r,i} r_i\right)\left(a_s + b_s y + \sum_{i=1}^{q} c_{s,i} \frac{n_i x + xy + 1}{r_i}\right) = n^* x + xy + 1$$

[1] We remark that the scheme remains secure even if the sign oracle only gets $\tilde{N}_j$ as long as the final forgery is on a well-formed message $(M^*, \tilde{N}^*) \in \widehat{\mathbb{GH}}$.

Thus, we must have

$$\begin{aligned} & a_r a_s + a_r b_s y + \sum_{i=1}^{q} a_r c_{s,i} \frac{n_i x + xy + 1}{r_i} \\ & + a_s b_r x + b_s b_r xy + \sum_{i=1}^{q} b_r c_{s,i} \frac{n_i x^2 + x^2 y + x}{r_i} \\ & + a_s \sum_{i=1}^{q} c_{r,i} r_i + b_s y \sum_{i=1}^{q} c_{r,i} r_i + \sum_{i=1}^{q} c_{r,i} r_i \sum_{i=1}^{q} c_{s,i} \frac{n_i x + xy + 1}{r_i} \\ & \quad = n^* x + xy + 1 \end{aligned}$$

There is no term in $\frac{xy}{r_i}$ or $\frac{x^2 y}{r_i}$ on the RHS so we must have for all $i \in [q]$ that $a_r c_{s,i} = 0$ and $b_r c_{s,i} = 0$. This means that we either have that $c_{s,i} = 0$ for all $i \in [q]$ or we have $a_r = b_r = 0$.

- Case $a_r = b_r = 0$: In this case we must have

$$a_s \sum_{i=1}^{q} c_{r,i} r_i + b_s y \sum_{i=1}^{q} c_{r,i} r_i + \sum_{i=1}^{q} c_{r,i} r_i \sum_{i=1}^{q} c_{s,i} \frac{n_i x + xy + 1}{r_i} = n^* x + xy + 1$$

There are no terms in r_i or $r_i y$ on the RHS so we must have for all $i \in [q]$ that $a_s c_{r,i} = 0$ and $b_s c_{r,i} = 0$. This means that we either have that $c_{r,i} = 0$ for all $i \in [q]$ or we have $a_s = b_s = 0$. The former case cannot occur as otherwise the LHS will not have a term in xy and hence the equality will not hold. So we must have $a_s = b_s = 0$ and hence we must have

$$\sum_{i=1}^{q} c_{r,i} r_i \sum_{i=1}^{q} c_{s,i} \frac{n_i x + xy + 1}{r_i} = n^* x + xy + 1$$

There is no term on the RHS of the form $\frac{r_j xy}{r_i}$ for any $i, j \in [q]$ where $i \neq j$. Thus, we must have $c_{r,i} c_{s,j} = 0$ for all $i \neq j$. This means we must have for some $i \in [q]$

$$c_{r,i} c_{s,i} n_i x + c_{r,i} c_{s,i} xy + c_{r,i} c_{s,i} = n^* x + xy + 1$$

By the monomial xy, we must have $c_{r,i} c_{s,i} = 1$ from which it is clear that the only way the equality will hold is if $n^* = n_i$ from some $i \in [q]$ which means the forgery is not valid as the signature is on a message that was queried to the sign oracle.
- Case $c_{s,i} = 0$ for all $i \in [q]$: In this case we must have

$$a_r a_s + a_r b_s y + a_s b_r x + b_s b_r xy + a_s \sum_{i=1}^{q} c_{r,i} r_i + b_s y \sum_{i=1}^{q} c_{r,i} r_i = n^* x + xy + 1$$

The only term on the LHS with the monomial xy is the term $b_s b_r xy$ thus for the equality to hold we must have that $b_s \neq 0$ and $b_r \neq 0$. There is no term on the RHS with the monomial $r_i y$ and since we cannot have $b_s = 0$, we must have that $c_{r,i} = 0$ for all $i \in [q]$, which means we have:

$$a_r a_s + a_r b_s y + a_s b_r x + b_s b_r xy = n^* x + xy + 1$$

There is no term on the RHS wih the monomial y and since we cannot have $b_s = 0$, we must have that $a_r = 0$ which means we have:

$$a_s b_r x + b_s b_r xy = n^* x + xy + 1$$

which cannot hold.

□

Lemma 2. *The scheme for $\ell > 1$ is EUF-CMA secure.*

Proof. We proceed by showing that any valid forgery in the case $\ell > 1$ can be reduced to a forgery for the case $\ell = 1$.

Let $\mathcal{A}$ be a successful adversary in the $\ell > 1$ case we show how to construct an adversary $\mathcal{B}$ who uses adversary $\mathcal{A}$ to break the scheme for the case $\ell = 1$ which would contradict Lemma 1.

Adversary $\mathcal{B}$ gets $\mathsf{vk}' = (X', \tilde{Y}')$ from her game where she has access to a sign oracle for a single Diffie-Hellman pair. She chooses $x_1, \ldots, x_{\ell-1} \leftarrow \mathbb{Z}_p$ and sets $\tilde{Y} := \tilde{Y}'$, $X_1 := X'$ and $X_i := X'^{x_{i-1}}$ for $i = 2, \ldots, \ell$. She starts $\mathcal{A}$ on the verification key $\mathsf{vk} := (X_1, \ldots, X_\ell, \tilde{Y})$. Note that since $x_1, \ldots, x_{\ell-1}$ are chosen uniformly at random, the verification key vk $\mathcal{A}$ sees is indistinguishable from one she gets from the real signer. When receiving a query on $\boldsymbol{m}_i = \Big((M, \tilde{N})_{i,1}, \ldots, (M, \tilde{N})_{i,\ell}\Big)$ from $\mathcal{A}$, $\mathcal{B}$ returns $\perp$ if $(M, \tilde{N})_{i,j} \notin \widehat{\mathbb{GH}}$ for any $j \in [\ell]$. Otherwise, she forwards $(M'_i, \tilde{N}'_i) := \Big(M_{i,1} \cdot \prod_{j=2}^{\ell} M_{i,j}^{x_{j-1}}, \tilde{N}_{i,1} \cdot \prod_{j=2}^{\ell} \tilde{N}_{i,j}^{x_{j-1}}\Big) \in \widehat{\mathbb{GH}}$ to her sign oracle and returns the signature she gets to $\mathcal{A}$. Such a signature is a valid signature on the message $\boldsymbol{m}_i = \Big((M, \tilde{N})_{i,1}, \ldots, (M, \tilde{N})_{i,\ell}\Big)$ w.r.t. the verification key $\mathsf{vk} = (X_1, \ldots, X_\ell, \tilde{Y})$.

When $\mathcal{A}$ outputs her forgery σ^* on $\boldsymbol{m}^* = \Big((M^*, \tilde{N}^*)_1, \ldots, (M^*, \tilde{N}^*)_\ell\Big)$, $\mathcal{B}$ returns $(M', \tilde{N}') := \Big(M_1^* \cdot \prod_{j=2}^{\ell} M_j^{*\,x_{j-1}}, \tilde{N}_1^* \cdot \prod_{j=2}^{\ell} \tilde{N}_j^{*\,x_{j-1}}\Big) \in \widehat{\mathbb{GH}}$ and σ^* as the answer in her game. Thus, $\mathcal{B}$ wins her game with the same advantage as that of $\mathcal{A}$ in her game. □

3.2 Scheme II

We show here that by transposing the signature components of Scheme I, we obtain a scheme with signatures $(S, \tilde{R}) \in \mathbb{G} \times \mathbb{H}$ where $\tilde{R}$ is information-theoretically independent of the message vector. The verification key matches that of Scheme I, i.e. the verification key size is $\ell|\mathbb{G}| + |\mathbb{H}|$. Note that the scheme has the property that signing requires only the $\mathbb{G}$ components of the messages whereas verification requires, besides verifying well-formedness of the messages, only the $\mathbb{H}$ components of the messages. We remark that existing schemes with similar properties have found various applications, see e.g. [13,28].

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

- $\mathsf{KeyGen}(\mathcal{P})$: Select $x_1, \ldots, x_\ell, y \leftarrow \mathbb{Z}_p$. Set $X_i := G^{x_i}$ for all $i \in [\ell]$, $\tilde{Y} := \tilde{H}^y$, $\mathsf{sk} := (x_1, \ldots, x_\ell, y)$, and $\mathsf{vk} := (X_1, \ldots, X_\ell, \tilde{Y}) \in \mathbb{G}^\ell \times \mathbb{H}$.
- $\mathsf{Sign}\left(\mathsf{sk}, \left((M_1, \tilde{N}_1), \ldots, (M_\ell, \tilde{N}_\ell)\right)\right)$: To sign $\left((M_1, \tilde{N}_1), \ldots, (M_\ell, \tilde{N}_\ell)\right) \in \widehat{\mathbb{GH}}^{\ell}$, select $r \leftarrow \mathbb{Z}_p$ and set $\tilde{R} := \tilde{H}^r$, and $S := (\prod_{i=1}^{\ell} M_i^{x_i} \cdot X_1^y \cdot G)^{\frac{1}{r}}$. Return $\sigma := (\tilde{R}, S) \in \mathbb{H} \times \mathbb{G}$.
- $\mathsf{Verify}\left(\mathsf{vk}, \left((M_1, \tilde{N}_1), \ldots, (M_\ell, \tilde{N}_\ell)\right), \sigma = (\tilde{R}, S)\right)$: Return 1 iff $\tilde{R} \in \mathbb{H}$, $S \in \mathbb{G}$, for all $i \in [\ell] : (M_i, \tilde{N}_i) \in \widehat{\mathbb{GH}}$, and
$$e(S, \tilde{R}) = \prod_{i=1}^{\ell} e(X_i, \tilde{N}_i) e(X_1, \tilde{Y}) e(G, \tilde{H}) \cdot$$
- $\mathsf{Randomize}\left(\mathsf{vk}, \left((M_1, \tilde{N}_1), \ldots, (M_\ell, \tilde{N}_\ell)\right), \sigma = (\tilde{R}, S)\right)$: Select $r' \leftarrow \mathbb{Z}_p$, and return $\sigma' := (\tilde{R}^{r'}, S^{\frac{1}{r'}})$.

The scheme has identical efficiency as that of Scheme I.

Security of the Scheme. The scheme is perfectly randomizable as the distribution of re-randomized signatures is identical to that of fresh signatures on the same vector.

Theorem 2. *The scheme is EUF-CMA secure.*

Proof. Correctness of the scheme follows by inspection and is straightforward to verify. The following two lemmata prove unforgeability of the scheme against adaptive chosen-message attacks. Lemma 3 proves that the case when $\ell = 1$ is secure in the generic group model whereas Lemma 4 reduces any attack on the scheme when $\ell > 1$ to the case when $\ell = 1$ which is proved by Lemma 3.

Lemma 3. *The scheme for $\ell = 1$ is EUF-CMA secure in the generic group model.*

Proof. We proceed by proving that no linear combinations (which represent Laurent polynomials in the discrete logarithms) of the group elements the adversary sees in the game correspond to a forgery on a new message.

At the start of the game, the only elements in $\mathbb{H}$ the adversary sees are $\tilde{H}$, $\tilde{Y}$ which correspond to the discrete logarithms 1 and y, respectively. Also, at the start of the game the only elements in $\mathbb{G}$ the adversary sees are G, X which correspond to the discrete logarithms 1 and x, respectively.

At the j-th query on message $(M_j, \tilde{N}_j)$, m_j and n_j which are the discrete logarithm of the message can only be a linear combination of the elements in the respective groups so far. Thus, we have

$$m_j = a_{m_j} + b_{m_j} x + \sum_{i=1}^{j-1} c_{m_j,i} \frac{m_i x + xy + 1}{r_i}$$
$$n_j = a_{n_j} + b_{n_j} y + \sum_{i=1}^{j-1} c_{n_j,i} r_i$$

For the message to satisfy $(M_j, \tilde{N}_j) \in \widehat{\mathbb{GH}}$, we must have that $m_j = n_j$ and hence we must have that $a_{m_j} = a_{n_j}$, $b_{m_j} = b_{n_j} = 0$ and for all i that $c_{m_j,i} = c_{n_j,i} = 0$. This ensures that the message queried is nothing but a constant polynomial.

If the message is well-formed, the sign oracle responds with a signature of the form

$$\left(r_j, s_j = \frac{m_j x + xy + 1}{r_j} \right)$$

Since the adversary is generic, she can only construct $(M^*, \tilde{N}^*)$ and $\sigma^* = (\tilde{R}^*, S^*)$ as a linear combination of the group elements she sees in the game. Thus, we must have

$$m^* = a_m + b_m x + \sum_{i=1}^{q} c_{m,i} \frac{m_i x + xy + 1}{r_i} \qquad r^* = a_r + b_r y + \sum_{i=1}^{q} c_{r,i} r_i$$
$$n^* = a_n + b_n y + \sum_{i=1}^{q} c_{n,i} r_i \qquad s^* = a_s + b_s x + \sum_{i=1}^{q} c_{s,i} \frac{m_i x + xy + 1}{r_i}$$

Since the forged message $(M^*, \tilde{N}^*)$ must correspond to a Diffie-Hellman pair, we must have $m^* = n^*$ and thus $a_m = a_n$, $b_m = b_n = 0$ and $c_{m,i} = c_{n,i} = 0$ for all $i \in [q]$ and hence $m^* = n^* = a_m$. For the forgery to be accepted, r^* and s^* must satisfy $s^* r^* = m^* x + xy + 1$. Therefore, we must have

$$\left(a_r + b_r y + \sum_{i=1}^{q} c_{r,i} r_i \right) \left(a_s + b_s x + \sum_{i=1}^{q} c_{s,i} \frac{m_i x + xy + 1}{r_i} \right) = m^* x + xy + 1$$

Thus, we must have

$$\begin{aligned} & a_r a_s + a_r b_s x + \sum_{i=1}^{q} a_r c_{s,i} \frac{m_i x + xy + 1}{r_i} \\ & + a_s b_r y + b_s b_r xy + \sum_{i=1}^{q} b_r c_{s,i} \frac{m_i xy + xy^2 + y}{r_i} \\ & + a_s \sum_{i=1}^{q} c_{r,i} r_i + b_s x \sum_{i=1}^{q} c_{r,i} r_i + \sum_{i=1}^{q} c_{r,i} r_i \sum_{i=1}^{q} c_{s,i} \frac{m_i x + xy + 1}{r_i} \\ & = m^* x + xy + 1 \end{aligned}$$

There is no term in $\frac{xy}{r_i}$ or $\frac{xy^2}{r_i}$ on the RHS so we must have for all $i \in [q]$ that $a_r c_{s,i} = 0$ and $b_r c_{s,i} = 0$. This means that we either have that $c_{s,i} = 0$ for all $i \in [q]$ or we have $a_r = b_r = 0$.

- Case $a_r = b_r = 0$: Here we must have

$$a_s \sum_{i=1}^{q} c_{r,i} r_i + b_s x \sum_{i=1}^{q} c_{r,i} r_i + \sum_{i=1}^{q} c_{r,i} r_i \sum_{i=1}^{q} c_{s,i} \frac{m_i x + xy + 1}{r_i} = m^* x + xy + 1$$

There is no terms in r_i or $r_i x$ on the RHS so we must have for all $i \in [q]$ that $a_s c_{r,i} = 0$ and $b_s c_{r,i} = 0$. This means that we either have that $c_{r,i} = 0$ for all $i \in [q]$ or we have $a_s = b_s = 0$. The former case cannot occur as otherwise the LHS will not have a term in xy and hence the equality will not hold. So we must have $a_s = b_s = 0$ and hence we have

$$\sum_{i=1}^{q} c_{r,i} r_i \sum_{i=1}^{q} c_{s,i} \frac{m_i x + xy + 1}{r_i} = m^* x + xy + 1$$

There is no term on the RHS of the form $\frac{r_j xy}{r_i}$ for any $i, j \in [q]$ where $i \neq j$. Thus, we must have $c_{r,i} c_{s,i} = 0$ if $i \neq j$. This means we have

$$c_{r,i} c_{s,i} m_i x + c_{r,i} c_{s,i} xy + c_{r,i} c_{s,i} = m^* x + xy + 1$$

By the monomial xy, we must have $c_{r,i} c_{s,i} = 1$ from which it is clear that the only way the equality will hold is if $m^* = m_i$ from some $i \in [q]$ which means the forgery is not valid as the signature is on a message that was queried to the sign oracle.

- Case $c_{s,i} = 0$ for all $i \in [q]$:

Thus, we must have

$$a_r a_s + a_r b_s x + a_s b_r y + b_s b_r xy + a_s \sum_{i=1}^{q} c_{r,i} r_i + b_s x \sum_{i=1}^{q} c_{r,i} r_i = m^* x + xy + 1$$

The only term on the LHS with the monomial xy is the term $b_s b_r xy$ thus for the equality to hold we must have that $b_s \neq 0$ and $b_r \neq 0$. There is no term on the RHS with the monomial $r_i x$ and since we cannot have $b_s = 0$, we must have that $c_{r,i} = 0$ for all $i \in [q]$, which means we have:

$$a_r a_s + a_r b_s x + a_s b_r y + b_s b_r xy = m^* x + xy + 1$$

There is no term on the RHS wih the monomial y and since we cannot have $b_r = 0$, we must have that $a_s = 0$ which means we have:

$$a_r b_s x + b_s b_r xy = m^* x + xy + 1$$

which cannot hold.

□

Lemma 4. *The scheme for $\ell > 1$ is EUF-CMA secure.*

Proof. We proceed by showing that any valid forgery in the case $\ell > 1$ can be reduced to a forgery for the case $\ell = 1$.

Let $\mathcal{A}$ be a successful adversary in the $\ell > 1$ case we show how to construct an adversary $\mathcal{B}$ who uses adversary $\mathcal{A}$ to break the scheme for the case $\ell = 1$ which would contradict Lemma .

Adversary $\mathcal{B}$ gets $\mathsf{vk}' = (X', \tilde{Y}')$ from her game where she has access to a sign oracle for a single Diffie-Hellman pair. She chooses $x_1, \ldots, x_{\ell-1} \leftarrow \mathbb{Z}_p$ and sets $\tilde{Y} := \tilde{Y}'$, $X_1 := X'$ and $X_i := X'^{x_{i-1}}$ for $i = 2, \ldots, \ell$. She starts $\mathcal{A}$ on the verification key $\mathsf{vk} := (X_1, \ldots, X_\ell, \tilde{Y})$. Note that since $x_1, \ldots, x_{\ell-1}$ are chosen uniformly at random, the verification key vk $\mathcal{A}$ sees is indistinguishable from one she gets from the real signer. When receiving a query on $\boldsymbol{m}_i = \Big((M, \tilde{N})_{i,1}, \ldots, (M, \tilde{N})_{i,\ell}\Big)$ from $\mathcal{A}$, $\mathcal{B}$ returns $\perp$ if $(M, \tilde{N})_{i,j} \notin \widehat{\mathbb{GH}}$ for any $j \in [\ell]$. Otherwise, she forwards $(M'_i, \tilde{N}'_i) := \Big(M_{i,1} \cdot \prod_{j=2}^{\ell} M_{i,j}^{x_{j-1}}, \tilde{N}_{i,1} \cdot \prod_{j=2}^{\ell} \tilde{N}_{i,j}^{x_{j-1}}\Big) \in \widehat{\mathbb{GH}}$ to her sign oracle and returns the signature she gets to $\mathcal{A}$. Such a signature is a valid signature on the message $\boldsymbol{m}_i = \Big((M, \tilde{N})_{i,1}, \ldots, (M, \tilde{N})_{i,\ell}\Big)$ w.r.t. the verification key $\mathsf{vk} = (X_1, \ldots, X_\ell, \tilde{Y})$.

When $\mathcal{A}$ outputs her forgery σ^* on $\boldsymbol{m}^* = \Big((M^*, \tilde{N}^*)_1, \ldots, (M^*, \tilde{N}^*)_\ell\Big)$, $\mathcal{B}$ returns $(M', \tilde{N}') := \Big(M_1^* \cdot \prod_{j=2}^{\ell} M_j^{*\,x_{j-1}}, \tilde{N}_1^* \cdot \prod_{j=2}^{\ell} \tilde{N}_j^{*\,x_{j-1}}\Big) \in \widehat{\mathbb{GH}}$ and σ^* as the answer in her game. Thus, $\mathcal{B}$ wins her game with the same advantage as that of $\mathcal{A}$ in her game. □

4 Unilateral Scheme for 2 Diffie-Hellman Pairs

We give here a scheme for 2 pairs of Diffie-Hellman messages yielding unilateral signatures of size $3|\mathbb{G}|$. The scheme is an extension of the recent single-message scheme from [29] where we use different randomness for each message. Signatures of this scheme are still shorter than those of all existing optimal Type-3 schemes since the latter require that at least one of the components of σ is from the second base group. The scheme is also more efficient than the single-message scheme from [28]. The verification key of the scheme is of size $3|\mathbb{H}|$, whereas verification of signatures require 1 PPE and 3 pairings, excluding the cost for verifying well-formedness of the messages. Given the description of Type-3 bilinear groups $\mathcal{P}$ output by $\mathcal{BG}(1^\kappa)$, the scheme is as follows:

- $\mathsf{KeyGen}(\mathcal{P})$: Select $x_1, x_2, y \leftarrow \mathbb{Z}_p$. Set $\mathsf{sk} := (x_1, x_2, y)$ and $\mathsf{vk} := (\tilde{X}_1, \tilde{X}_2, \tilde{Y}) := (\tilde{H}^{x_1}, \tilde{H}^{x_2}, \tilde{H}^{y}) \in \mathbb{H}^3$.
- $\mathsf{Sign}\Big(\mathsf{sk}, \Big((M_1, \tilde{N}_1), (M_2, \tilde{N}_2)\Big)\Big)$: To sign $\Big((M_1, \tilde{N}_1), (M_2, \tilde{N}_2)\Big) \in \widehat{\mathbb{GH}}^2$, select $r_1, r_2 \leftarrow \mathbb{Z}_p$, set $R_1 := G^{r_1}$, $R_2 := G^{r_2}$, $S := \left((G^{x_1} \cdot M_1)^{r_1} \cdot (G^{x_2} \cdot M_2)^{r_2}\right)^{\frac{1}{y}}$. Return $\sigma := (R_1, R_2, S) \in \mathbb{G}^3$.

- $\mathsf{Verify}\left(\mathsf{vk}, \left((M_1, \tilde{N}_1), (M_2, \tilde{N}_2)\right), \sigma = (R_1, R_2, S)\right)$: Return 1 iff $R_1 \in \mathbb{G}^\times$, $R_2, S \in \mathbb{G}$, $\left((M_1, \tilde{N}_1), (M_2, \tilde{N}_2)\right) \in \widehat{\mathbb{GH}}^2$ and
$$e(S, \tilde{Y}) = e(R_1, \tilde{X}_1 \cdot \tilde{N}_1) e(R_2, \tilde{X}_2 \cdot \tilde{N}_2) \cdot$$
- $\mathsf{Randomize}\left(\mathsf{vk}, \left((M_1, \tilde{N}_1), (M_2, \tilde{N}_2)\right), \sigma = (R_1, R_2, S)\right)$: Select $r' \leftarrow \mathbb{Z}_p^\times$, and set $R_1' := R_1^{r'}$, $R_2' := R_2^{r'}$, $S' := S^{r'}$. Return $\sigma' := (R_1', R_2', S')$.

Correctness of the scheme follows by inspection and is straightforward to verify. We remark here that the signer will always be able to link a randomized signature to the original signature from which it was obtained even if we additionally require that $R_2 \neq 1_\mathbb{G}$. For instance, the malicious signer can choose $r_2 = -r_1$ which will make all randomized versions of the signature in question satisfy $R_1' \cdot R_2' = 1_\mathbb{G}$. Another way the signer can link a randomized signature to its original signature is by using knowledge of the exponents r_1 and r_2 since we will always have that $R_1'^{\frac{1}{r_1}} = R_2'^{\frac{1}{r_2}}$.

We now prove the following theorem.

Theorem 3. *The scheme is EUF-CMA secure in the generic group model.*

Proof. Public elements in $\mathbb{H}$ are $\tilde{H}$, $\tilde{X}_1$,$\tilde{X}_2$, and $\tilde{Y}$ which correspond to the discrete logarithms 1, x_1, x_2, and y, respectively. At the i-th signing query, we have that $((m_{i,1}, n_{i,1}), (m_{i,2}, n_{i,2}))$, which are the discrete logarithms of the queried message $\left((M_{i,1}, \tilde{N}_{i,1}), (M_{i,2}, \tilde{N}_{i,2})\right)$, must be of the form

$$n_{i,k} = a_{n_{i,k}} + b_{n_{i,k}} x_1 + c_{n_{i,k}} x_2 + d_{n_{i,k}} y$$
$$m_{i,k} = a_{m_{i,k}} + \sum_{j=1}^{i-1} b_{m_{i,k,j}} r_{1_j} + \sum_{j=1}^{i-1} c_{m_{i,k,j}} r_{2_j} + \sum_{j=1}^{i-1} d_{m_{i,k,j}} \frac{r_{1_j} m_{1_j} + r_{1_j} x_1 + r_{2_j} m_{2_j} + r_{2_j} x_2}{y},$$

for $k = 1, 2$. Since we must have $m_{i,1} = n_{i,1}$ and $m_{i,1} = n_{i,2}$ for the messages to be valid, we have $m_{i,1} = n_{i,1} = a_{m_{i,1}} = a_{n_{i,1}}$ and $m_{i,2} = n_{i,2} = a_{m_{i,2}} = a_{n_{i,2}}$, i.e. the messages queried to the signing oracle correspond to constant polynomials. Note that the sign oracle does not produce any elements in $\mathbb{H}$.

After q signing queries, $((m_1^*, n_1^*), (m_2^*, n_2^*))$, which are the discrete logarithms of the forged Diffie-Hellman pairs $\left((M_1^*, \tilde{N}_1^*), (M_2^*, \tilde{N}_2^*)\right)$, must be of the form

$$n_k^* = a_{n_k} + b_{n_k} x_1 + c_{n_k} x_2 + d_{n_k} y$$
$$m_k^* = a_{m_k} + \sum_{i=1}^{q} b_{m_{k,i}} r_{1_i} + \sum_{i=1}^{q} c_{m_{k,i}} r_{2_i} + \sum_{i=1}^{q} d_{m_{k,i}} \frac{r_{1_i} m_{1_i} + r_{1_i} x_1 + r_{2_i} m_{2_i} + r_{2_i} x_2}{y},$$

for $k = 1, 2$. Since we must have $m_1^* = n_1^*$ and $m_2^* = n_2^*$ for the forgery to be a valid element of $\widehat{\mathbb{GH}}^2$, we have $m_1^* = n_1^* = a_{m_1} = a_{n_1}$ and $m_2^* = n_2^* = a_{m_2} = a_{n_2}$.

Similarly, the signature (R_1^*, R_2^*, S^*) has the form

$$r_1^* = a_{r_1} + \sum_{i=1}^{q} b_{r_{1,i}} r_{1_i} + \sum_{i=1}^{q} c_{r_{1,i}} r_{2_i} + \sum_{i=1}^{q} d_{r_{1,i}} \frac{r_{1_i} m_{1_i} + r_{1_i} x_1 + r_{2_i} m_{2_i} + r_{2_i} x_2}{y}$$

$$r_2^* = a_{r_2} + \sum_{i=1}^{q} b_{r_{2,i}} r_{1_i} + \sum_{i=1}^{q} c_{r_{2,i}} r_{2_i} + \sum_{i=1}^{q} d_{r_{2,i}} \frac{r_{1_i} m_{1_i} + r_{1_i} x_1 + r_{2_i} m_{2_i} + r_{2_i} x_2}{y}$$

$$s^* = a_s + \sum_{i=1}^{q} b_{s,i} r_{1_i} + \sum_{i=1}^{q} c_{s,i} r_{2_i} + \sum_{i=1}^{q} d_{s,i} \frac{r_{1_i} m_{1_i} + r_{1_i} x_1 + r_{2_i} m_{2_i} + r_{2_i} x_2}{y}$$

For the forgery to be a valid signature, (r_1^*, r_2^*, s^*) must satisfy $s^* y = r_1^* m_1^* + r_1^* x_1 + r_2^* m_2^* + r_2^* x_2$. So we must have

$$\begin{aligned}
&\Big(a_s + \sum_{i=1}^{q} b_{s,i} r_{1_i} + \sum_{i=1}^{q} c_{s,i} r_{2_i} + \sum_{i=1}^{q} d_{s,i} \frac{r_{1_i} m_{1_i} + r_{1_i} x_1 + r_{2_i} m_{2_i} + r_{2_i} x_2}{y}\Big) y \\
&= \left(a_{r_1} + \sum_{i=1}^{q} b_{r_{1,i}} r_{1_i} + \sum_{i=1}^{q} c_{r_{1,i}} r_{2_i} + \sum_{i=1}^{q} d_{r_{1,i}} \frac{r_{1_i} m_{1_i} + r_{1_i} x_1 + r_{2_i} m_{2_i} + r_{2_i} x_2}{y}\right) (x_1 + m_1^*) \\
&\quad + \left(a_{r_2} + \sum_{i=1}^{q} b_{r_{2,i}} r_{1_i} + \sum_{i=1}^{q} c_{r_{2,i}} r_{2_i} + \sum_{i=1}^{q} d_{r_{2,i}} \frac{r_{1_i} m_{1_i} + r_{1_i} x_1 + r_{2_i} m_{2_i} + r_{2_i} x_2}{y}\right) (x_2 + m_2^*)
\end{aligned}$$

There is no term in y, $r_{1_i} y$ or $r_{2_i} y$ on the RHS so we must have $a_s = 0$ and $b_{s,i} = c_{s,i} = 0$ for all i.

Also, there are no terms in x_1, x_2, $r_{1_i} x_2$, $r_{2_i} x_1$, $\frac{r_{1_i} x_1^2}{y}$, or $\frac{r_{2_i} x_2^2}{y}$ on the LHS so we must have $a_{r_1} = a_{r_2} = 0$ and $c_{r_{1,i}} = b_{r_{2,i}} = d_{r_{1,i}} = d_{r_{2,i}}$ for all i. Thus, we have

$$\begin{aligned}
&\sum_{i=1}^{q} d_{s,i} (r_{1_i} m_{1_i} + r_{1_i} x_1 + r_{2_i} m_{2_i} + r_{2_i} x_2) \\
&\qquad = \sum_{i=1}^{q} b_{r_{1,i}} r_{1_i} m_1^* + \sum_{i=1}^{q} b_{r_{1,i}} r_{1_i} x_1 + \sum_{i=1}^{q} c_{r_{2,i}} r_{2_i} m_2^* + \sum_{i=1}^{q} c_{r_{2,i}} r_{1_i} x_2
\end{aligned}$$

Since we must have $r_1^* \neq 0$, it follows that we must have at least for one value of i that $b_{r_{1,i}} \neq 0$. By the monomial $r_{1_i} x_1$, we have $b_{r_{1,i}} = d_{s,i}$. Since $d_{s,i} \neq 0$, we also have that $c_{r_{2,i}} = d_{s,i}$. Now by the monomial r_{1_i}, we have that $b_{r_{1,i}} m_1^* = d_{s,i} m_{1_i}$ from which it follows that $m_1^* = m_{1_i}$. Similarly, by the monomial r_{2_i}, we have that $c_{r_{2,i}} m_2^* = d_{s,i} m_{2_i}$ from which it follows that $m_2^* = m_{2_i}$. Thus, the forgery is on a message pair that was queried to the oracle. □

5 Efficiency Comparison

We compare in Table 1 the efficiency of our schemes with that of existing ones.

Table 1. Efficiency comparison between our schemes and existing Type-3 schemes

Scheme	σ		vk		PP		$\mathcal{M}$	Randomizable	Verification Cost			
									1 Signature		n Signatures	
	$\mathbb{G}$	$\mathbb{H}$	$\mathbb{G}$	$\mathbb{H}$	$\mathbb{G}$	$\mathbb{H}$			PPE	Pairing	PPE	Pairing
[3] I	5	2	$8 + 2\ell$	4	-	-	$\mathbb{G}^\ell$	Partially	2	$6 + 2\ell + 4^\dagger$	$2n$	$6n + 2\ell + 4^\dagger$
[3] II	2	5	$8 + 2\ell$	4	-	-	$\mathbb{H}^\ell$	Partially	2	$6 + 2\ell + 4^\dagger$	$2n$	$6n + 2\ell + 4^\dagger$
[4]	2	1	ℓ	1	-	-	$\mathbb{H}^\ell$	Yes	2	$3 + \ell + 1^\dagger$	$2n$	$3n + \ell + 1^\dagger$
[33] 1	1	2	ℓ	-	-	1	$\mathbb{H}^\ell$	Yes	2	$2 + \ell + 3^\dagger$	$2n$	$2n + \ell + 3^\dagger$
[33] 2	1	2	ℓ	-	-	1	$\mathbb{H}^\ell$	No	2	$3 + \ell + 3^\dagger$	$2n$	$3n + \ell + 3^\dagger$
Ours I	1	1	ℓ	1	-	-	$\widehat{\mathbb{GH}}^\ell$	Yes	$1 + \ell^*$ Or $1 + 1^*$	$1 + \ell + 1^\dagger + 2\ell^*$ Or $1 + \ell + 1^\dagger + 2^*$	$n + \ell^*$ Or $n + 1^*$	$n + \ell + 1^\dagger + 2\ell^*$ Or $n + \ell + 1^\dagger + 2^*$
Ours II	1	1	ℓ	1	-	-	$\widehat{\mathbb{GH}}^\ell$	Yes	$1 + \ell^*$ Or $1 + 1^*$	$1 + \ell + 1^\dagger + 2\ell^*$ Or $1 + \ell + 1^\dagger + 2^*$	$n + \ell^*$ Or $n + 1^*$	$n + \ell + 1^\dagger + 2\ell^*$ Or $n + \ell + 1^\dagger + 2^*$

In the table numbers superscripted with † are the number of pairings that can be precomputed, whereas numbers superscripted with $*$ are the cost needed to verify well-formedness of the Diffie-Hellman message. The latter cost is constant when verifying multiple signatures on the same message. Also, as mentioned earlier, one can use techniques from batch verification, e.g. [12,17], to reduce the cost required for verifying the well-formedness of a vector of ℓ Diffie-Hellman pairs to a single PPE and 2 pairings. For our schemes, we give 2 estimations for the efficiency overhead where the first is for the case where no batch verification is applied to verifying the well-formedness of the messages, whereas the second cost is when batch verification is applied in that respect. For all schemes listed, public parameters PP do not include the default group generators. Note that the security of all schemes in the table except for [3] which rely on non-interactive q-type assumptions is proven in the generic group model. For the cost of verification, we give two estimations which are for verifying 1 and n different signatures on the same message vector.

As can be seen from the table, our schemes outperform existing schemes w.r.t signature size. The size of the verification key of our schemes matches the best existing scheme. Also, the verification cost compares favourably especially when verifying various signatures on the same message vector which is the case for many applications, e.g. when the user is required to prove possession of various credentials/attributes from an authority or possibly different authorities.

5.1 Efficiency in the Single Message Setting

The best existing scheme in terms of signature size and verification overhead is the one recently given in [29] which has signatures of size $2|\mathbb{G}|$ and verification key of size $2|\mathbb{H}|$. When used on their own, the scheme in [29] has slightly shorter signatures than ours, whereas schemes I and II of ours have shorter verification key. In fact, the combined size of signatures and verification key in the 3 schemes are identical. Note that the scheme in [29] has the slight non-standard requirement that one needs to check that a signature component (which is information-theoretically independent of the message) is not the trivial element and hence in the case that one needs to commit to that signature component, one needs more expensive alternatives to prove that it conforms to the requirement, which is not the case in our schemes. Let's now compare the verification overhead when verifying n signatures on the same message. Ignoring the cost of checking that $(M, \tilde{N}) \in \widehat{\mathbb{G}\mathbb{H}}$, the scheme in [29] would require $2n$ pairings, whereas schemes I and II of ours require only $n + 2$ pairings where one of the pairings, i.e. $e(G, \tilde{H})$ can be pre-computed and used for signatures on other messages, i.e. the cost drops to only $n + 1$ pairings after verifying signatures on the first message. Thus, it is obvious that ours have less computational overhead when verifying multiple signatures on the same message.

Let's now compare the performance of Scheme I of ours and the one in [29] when combined with Groth-Sahai [34] to prove knowledge of a signature on a committed message. We consider the most efficient instantiation of the proofs which relies on the SXDH assumption as noted by [30]. The scheme from [29] has signatures of the form $(R, S) \in \mathbb{G}^2$ and a verification key of the form $(\tilde{X}, \tilde{Y}) \in \mathbb{H}^2$, and verification requires checking that $(M, \tilde{N}) \in \widehat{\mathbb{G}\mathbb{H}}$, $R \neq 1_{\mathbb{G}}$, and evaluating the following PPE:

$$e(S, \tilde{Y}) = e(R, \tilde{X} \cdot \tilde{N}) \tag{2}$$

In the terminology of [34], Equation (2) is a quadratic PPE. When proving knowledge of a signature, one has to commit to M, $\tilde{N}$ and S and thus we need to produce a proof for the satisfiability of (2) as well as the quadratic PPE $e(G, \tilde{N}) = e(M, \tilde{H})$ to prove that $(M, \tilde{N}) \in \widehat{\mathbb{G}\mathbb{H}}$. The total size of the Groth-Sahai commitments is $4|\mathbb{G}| + 2|\mathbb{H}|$, whereas the size of the proof for each of the above equations is $4|\mathbb{G}|+4|\mathbb{H}|$. Thus, the total size of the witness indistinguishable Groth-Sahai proof of knowledge is $12|\mathbb{G}| + 10|\mathbb{H}|$.

Scheme I of ours has signatures of the form $(R, \tilde{S}) \in \mathbb{G} \times \mathbb{H}$ and a verification key of the form $(X, \tilde{Y}) \in \mathbb{G} \times \mathbb{H}$, and verification requires checking that $(M, \tilde{N}) \in \widehat{\mathbb{G}\mathbb{H}}$ and evaluating the following PPE:

$$e(R, \tilde{S}) = e(X, \tilde{N} \cdot \tilde{Y}) e(G, H) \tag{3}$$

When proving knowledge, we need to commit to M, $\tilde{N}$ and $\tilde{S}$ and thus we need to produce a proof for the satisfiability of (3), which is a linear PPE since components of the witness are all from the same group, as well as the quadratic PPE to prove that $(M, \tilde{N}) \in \widehat{\mathbb{G}\mathbb{H}}$. The total size of the Groth-Sahai commitments is $2|\mathbb{G}| + 4|\mathbb{H}|$. The size of the proof for (3) is $2|\mathbb{G}|$ whereas proving $(M, \tilde{N}) \in \widehat{\mathbb{G}\mathbb{H}}$ requires a proof of size $4|\mathbb{G}| + 4|\mathbb{H}|$. Thus, the total size of the witness indistinguishable Groth-Sahai proof of knowledge is $8|\mathbb{G}| + 8|\mathbb{H}|$. From the above, it is obvious when proving knowledge of signatures using Groth-Sahai proofs, which was the main motivation behind introducing the structure-preserving signatures notion, and which is required for the vast majority of applications of the notion, e.g. group, blind, attribute-based signatures, e-cash, etc., our scheme outperforms the best existing scheme. The efficiency gain has implication for various applications.

Acknowledgements. We thank anonymous IMA International Conference on Cryptography and Coding reviewers for valuable comments.

References

1. Abe, M., Chase, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Constant-size structure-preserving signatures: generic constructions and simple assumptions. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 4–24. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_3
2. Abe, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Tagged one-time signatures: tight security and optimal tag size. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 312–331. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36362-7_20
3. Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., Ohkubo, M.: Structure-preserving signatures and commitments to group elements. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 209–236. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_12
4. Abe, M., Groth, J., Haralambiev, K., Ohkubo, M.: Optimal structure-preserving signatures in asymmetric bilinear groups. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 649–666. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22792-9_37
5. Abe, M., Groth, J., Ohkubo, M.: Separating short structure-preserving signatures from non-interactive assumptions. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 628–646. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_34
6. Abe, M., Groth, J., Ohkubo, M., Tibouchi, M.: Unified, minimal and selectively randomizable structure-preserving signatures. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 688–712. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54242-8_29
7. Abe, M., Groth, J., Ohkubo, M., Tibouchi, M.: Structure-preserving signatures from type II pairings. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 390–407. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44371-2_22
8. Abe, M., Kohlweiss, M., Ohkubo, M., Tibouchi, M.: Fully structure-preserving signatures and shrinking commitments. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 35–65. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_2
9. Attrapadung, N., Libert, B., Peters, T.: Computing on authenticated data: new privacy definitions and constructions. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 367–385. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_23
10. Baldimtsi, F., Chase, M., Fuchsbauer, G., Kohlweiss, M.: Anonymous transferable E-Cash. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 101–124. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_5
11. Barthe, G., Fagerholm, E., Fiore, D., Scedrov, A., Schmidt, B., Tibouchi, M.: Strongly-Optimal structure preserving signatures from Type II pairings: synthesis and lower bounds. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 355–376. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_16

12. Bellare, M., Garay, J.A., Rabin, T.: Fast batch verification for modular exponentiation and digital signatures. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 236–250. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0054130
13. Bernhard, D., Fuchsbauer, G., Ghadafi, E.: Efficient signatures of knowledge and DAA in the standard model. In: Jacobson, M., Locasto, M., Mohassel, P., Safavi-Naini, R. (eds.) ACNS 2013. LNCS, vol. 7954, pp. 518–533. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38980-1_33
14. Brickell, E., Camenisch, J., Chen, L.: Direct anonymous attestation. In: CCS 2004, ACM, pp. 132–145 (2004)
15. Camenisch, J., Dubovitskaya, M., Haralambiev, K.: Efficient structure-preserving signature scheme from standard assumptions. In: Visconti, I., De Prisco, R. (eds.) SCN 2012. LNCS, vol. 7485, pp. 76–94. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32928-9_5
16. Camenisch, J., Dubovitskaya, M., Haralambiev, K., Kohlweiss, M.: Composable and modular anonymous credentials: definitions and practical constructions. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9453, pp. 262–288. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48800-3_11
17. Camenisch, J., Hohenberger, S., Pedersen, M.Ø.: Batch verification of short signatures. J. Cryptology **25**(4), 723–747 (2012)
18. Chase, M., Kohlweiss, M.: A New hash-and-sign approach and structure-preserving signatures from DLIN. In: Visconti, I., De Prisco, R. (eds.) SCN 2012. LNCS, vol. 7485, pp. 131–148. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32928-9_8
19. Chatterjee, S., Menezes, A.: Type 2 structure-preserving signature schemes revisited. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 286–310. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48797-6_13
20. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theor. **31**(4), 469–472 (1985)
21. El Kaafarani, A., Ghadafi, E., Khader, D.: Decentralized traceable attribute-based signatures. In: Benaloh, J. (ed.) CT-RSA 2014. LNCS, vol. 8366, pp. 327–348. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-04852-9_17
22. Fiat, A., Shamir, A.: How To prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_12
23. Fuchsbauer, G.: Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. In: Cryptology ePrint Archive, Report 2009/320
24. Fuchsbauer, G.: Commuting Signatures and verifiable encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 224–245. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_14
25. Fuchsbauer, G., Hanser, C., Slamanig, D.: Practical round-optimal blind signatures in the standard model. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 233–253. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_12
26. Galbraith, S., Paterson, K., Smart, N.P.: Pairings for cryptographers. Discrete Appl. Math. **156**, 3113–3121 (2008)
27. Ghadafi, E.: Formalizing group blind signatures and practical constructions without random oracles. In: Boyd, C., Simpson, L. (eds.) ACISP 2013. LNCS, vol. 7959, pp. 330–346. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39059-3_23

28. Ghadafi, E.: Short structure-preserving signatures. In: Sako, K. (ed.) CT-RSA 2016. LNCS, vol. 9610, pp. 305–321. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-29485-8_18
29. Ghadafi, E.: More efficient structure-preserving signatures - or: bypassing the Type-III lower bounds. In: Foley, S.N., Gollmann, D., Snekkenes, E. (eds.) ESORICS 2017. LNCS, vol. 10493, pp. 43–61. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66399-9_3
30. Ghadafi, E., Smart, N.P., Warinschi, B.: Groth–Sahai proofs revisited. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 177–192. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13013-7_11
31. Green, M., Hohenberger, S.: Universally composable adaptive oblivious transfer. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 179–197. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-89255-7_12
32. Groth, J.: Simulation-Sound NIZK proofs for a practical language and constant size group signatures. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 444–459. Springer, Heidelberg (2006). https://doi.org/10.1007/11935230_29
33. Groth, J.: Efficient fully structure-preserving signatures for large messages. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 239–259. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48797-6_11
34. Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. SIAM J. Comput. **41**(5), 1193–1232 (2012)
35. Hofheinz, D., Jager, T.: Tightly secure signatures and public-key encryption. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 590–607. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_35
36. Jutla, C.S., Roy, A.: Improved structure preserving signatures under standard bilinear assumptions. In: Fehr, S. (ed.) PKC 2017. LNCS, vol. 10175, pp. 183–209. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54388-7_7
37. Kiltz, E., Pan, J., Wee, H.: Structure-preserving signatures from standard assumptions, revisited. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 275–295. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_14
38. Libert, B., Peters, T., Yung, M.: Short group signatures via structure-preserving signatures: standard model security from simple assumptions. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 296–316. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_15
39. Maji, H.K., Prabhakaran, M., Rosulek, M.: Attribute-based signatures. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 376–392. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19074-2_24
40. Maurer, U.: Abstract models of computation in cryptography. In: Smart, N.P. (ed.) Cryptography and Coding 2005. LNCS, vol. 3796, pp. 1–12. Springer, Heidelberg (2005). https://doi.org/10.1007/11586821_1
41. Shoup, V.: Lower bounds for discrete logarithms and related problems. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 256–266. Springer, Heidelberg (1997). https://doi.org/10.1007/3-540-69053-0_18
42. Wang, Y., Zhang, Z., Matsuda, T., Hanaoka, G., Tanaka, K.: How to obtain fully structure-preserving (automorphic) signatures from structure-preserving ones. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 465–495. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_16