More Efficient Structure-Preserving Signatures - Or: Bypassing the Type-III Lower Bounds

Essam Ghadafi(✉)

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

Abstract. Structure-Preserving Signatures (SPSs) are an important cryptographic primitive that is useful for the design of modular cryptographic protocols. It has be shown that in the most efficient Type-III bilinear group setting such schemes 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). In this work we show how to circumvent these lower bounds by constructing more efficient schemes than existing optimal schemes. Towards this end, we first formally define the notion of Unilateral Structure-Preserving Signatures on Diffie-Hellman pairs (USPSDH) as Type-III SPS schemes with messages being Diffie-Hellman pairs and signatures being elements of one of the base groups, i.e. unilateral. We construct a number of new fully randomizable SPS schemes that are existentially unforgeable against adaptive chosen-message attacks, and which yield signatures consisting of only 2 elements from the shorter base group, and which require only a single PPE for verification (not counting the cost of verifying the well-formedness of the message). Thus, our signatures are at least half the size of the best existing scheme for unilateral messages. Our first scheme has a feature that permits controlled randomizability which might be of independent interest. We also give various optimal strongly unforgeable one-time schemes with 1-element signatures, including a new scheme for unilateral messages that matches the best existing scheme in every respect. We prove optimality of our constructions by proving different lower bounds and giving some impossibility results. We also show how to extend our schemes to sign a vector of messages. Finally, we highlight how our schemes yield more efficient instantiations of various cryptographic protocols, including variants of attribute-based signatures and direct anonymous attestation, which is a protocol deployed in practice. Our results offer value along two fronts: On the theoretical side, our results serve as a workaround to bypass existing lower bounds. On the practical side, our constructions could lead to more efficient instantiations of various cryptographic protocols.

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013)/ERC Grant Agreement no. 307937 and EPSRC grant EP/J009520/1. The work was also sponsored by the Computer Science and Creative Technologies Department at the University of the West of England. Part of the work was done while the author was at University College London.

S.N. Foley et al. (Eds.): ESORICS 2017, Part II, LNCS 10493, pp. 43–61, 2017.
DOI: 10.1007/978-3-319-66399-9_3

1 Introduction

Structure-Preserving Signatures (SPSs) [3] are pairing-based digital signature schemes whose messages, verification key and signatures are all group elements from one or both base groups, and signature verification involves evaluating Pairing-Product Equations (PPEs). Such schemes compose nicely with existing popular tools such as Groth-Sahai proofs [37] and ElGamal encryption [23] and hence they are a useful tool for the design of cryptographic protocols not relying on random oracles [25]. They have numerous applications which include group signatures, e.g. [3,41], blind signatures, e.g. [3,28], attribute-based signatures, e.g. [24,31], tightly secure encryption, e.g. [2,38], malleable signatures, e.g. [10], anonymous credentials, e.g. [17,27], network coding, e.g. [10], oblivious transfer, e.g. [34], direct anonymous attestation, e.g. [13,32], and e-cash, e.g. [11].

Related Work. The term "structure-preserving signature" was coined by Abe et al. [3] but earlier schemes conforming to the definition were given in [34,35]. The notion received a significant amount of attention and many studies regarding lower bounds for the design of such schemes as well as new schemes matching those bounds have been published. Abe et al. [3] constructed schemes based on non-interactive intractability assumptions which work in the different bilinear group settings. Abe et al. [4] showed that signature of such schemes in the Type-III bilinear group setting (cf. Sect. 2.1) must have at least 3 elements, which must come from both base groups, and require at least 2 PPEs for verification which rules out the existence of schemes with unilateral signatures. They gave optimal constructions and proved their security in the generic group model [43,45]. Abe et al. [5] proved that it is impossible to base the security of an optimal Type-III scheme on non-interactive intractability assumptions. Other Type-III constructions were given in [6,21,30,36]. Recently, Ghadafi [32] gave a randomizable scheme with signatures consisting of 3 elements from the shorther base group which can also be regarded as a USPSDH scheme. Verification in his scheme requires, besides checking the well-formedness of the message, the evaluation of 2 PPEs.

Constructions relying on standard assumptions, e.g. DLIN or DDH, were given by [1,2,16,19,39–41]. It is well known that schemes based on standard assumptions are less efficient than their counterparts relying on non-standard assumptions or those proven directly in the generic group model.

Constructions in the Type-II setting (where there is an efficiently computable isomorphism between the base groups in one direction) were given in [7,12,21].

Recently, fully structure-preserving schemes where even the secret key consists of only group elements from the base groups were given in [8,36,46].

Our Techniques. All existing Type-III constructions for unilateral messages have the common feature that one of the signature components involves an exponent that is either the inverse or the square of some random field element chosen as part of the signing. Hence, verification in these schemes relies on a pairing involving two signature components and this is the reason that none of these schemes has unilateral signatures. In fact, as proven by Abe et al. [4], it is impossible to have a Type-III scheme for unilateral messages with unilateral signatures. We adopt a different approach to obtain schemes with short unilateral signatures. First, we require that messages are Diffie-Hellman pairs [3,26] of the form $(G^m, \tilde{H}^m)$ for some $m \in \mathbb{Z}_p$ where $\hat{e} : \mathbb{G} \times \mathbb{H} \longrightarrow \mathbb{T}$ is a bilinear map (cf. Sect. 2.1) and $\mathbb{G} := \langle G \rangle$ and $\mathbb{H} := \langle \tilde{H} \rangle$. Also, unlike existing schemes, none of the signature components in our schemes involves inverses or squares of the randomness used in the signing. Instead, one of the signature components involves the inverse of a field element from the secret key which can be cancelled out in the verification by pairing the concerned signature component with the corresponding public key which belongs to the opposite base group. This way we obtain schemes with optimal unilateral signatures and which require optimal number of verification equations. We remark that there exist Type-III schemes for the same message space as ours yielding unilateral signatures, e.g. [30,32], however, those schemes are not optimal.

Our Contribution. After defining USPSDH schemes in Sect. 2.4, we provide the following contributions:-

- (Sect. 3) Two new fully randomizable SPS schemes that are existentially unforgeable against a chosen-message attack. Our schemes yield unilateral signatures consisting of only 2 elements and hence they are at least half the size of the shortest existing Type-III SPS scheme. Verification in our schemes requires, besides checking the well-formedness of the message, the evaluation of a single PPE. Our first construction has a feature that permits controlled randomizability (combined unforgeability) which might be of independent interest.
- (Sect. 4) New optimal strongly EUF-CMA secure one-time schemes for a vector of messages with 1 element signatures, including a scheme for unilateral messages matching the best existing scheme [6] in every measure.
- (Sect. 5) An optimal CMA-secure partially structure-preserving scheme that simultaneously signs a Diffie-Hellman pair and a vector in $\mathbb{Z}_p^k$.
- We highlight (in Sect. 6) some applications of our schemes which include efficient instantiations of Direct Anonymous Attestation (DAA) [15] and variants of attribute-based signatures [24,31,42] which outperform existing constructions not relying on random oracles.
- We prove (in Sect. 7) the following lower bound/impossibility results:
  (i) A lower bound of 2 elements for signatures of schemes secure against a random-message attack for more than 1 signing query.
  (ii) A lower bound of 2 elements for the verification key of optimal schemes. This holds even when the adversary is restricted to 1 random-message signing query.
  (iii) The impossibility of strongly existentially-unforgeable schemes secure against more than 1 chosen-message signing query.

Why are USPSDH Schemes Interesting? From our results, it is clear that USPSDH signature schemes yield the shortest SPS signatures since they allow one to circumvent the lower bounds in the Type-III setting. It is particularly interesting when the signatures are from the first base group as the bit size of the elements of that group is at least half the size of those of the second group.

While traditional Type-III SPS schemes have shorter messages since message components of those schemes lie in one of the base groups and not both, this is a small price to pay to get smaller signatures and more efficient verification. Even though the restriction that messages are Diffie-Hellman pairs imposed by USPSDH schemes might give the false impression that these variants are less general than traditional SPS schemes, we stress that such a restriction is not a too strong one and USPSDH schemes suffice for many practical applications of traditional SPS schemes. So besides serving as a workaround to circumvent the lower bounds, such variants are useful in practice.

Being in the Type-III setting, (optimal) USPSDH schemes enjoy much better efficiency (including shorter message sizes) than existing Type-II schemes since the Type-III setting yields shorter group representations and better efficiency. Note that verifying the well-formedness of the message only needs to be performed once when verifying multiple signatures on the same message. Consider, for example, attribute-based signatures [42] where the signer needs to prove she has multiple attributes from (possibly different) attribute authorities. The same applies to applications requiring a user to prove that she has multiple tokens/credentials/certificates from an authority or possibly different authorities. Even when considering a single signature on the message, ours still compare favorably to existing ones in many aspects as shown in Table 1, where 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. For all schemes listed, public parameters do not include the default group generators. Note that the security of all schemes in the table except for [3,26] which rely on non-interactive q-type assumptions and [30] which relies on an interactive assumption is proven in the generic group model.

Our schemes compare favorably even to some widely-used non-structure-preserving schemes. For instance, ours are more efficient than the Camenisch-Lysyanskaya scheme [18] and Waters' scheme [20,47]. Also, the size of our signatures and the verification key are the same as those of the recent scheme by Pointcheval and Sanders [44]. Moreover, the (interactive) intractability assumptions underlying our schemes are comparable to those underlying [18,44].

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. By $[k]$, we denote the set $\{1, \ldots, k\}$. We will use capital letters for group elements and small letters for field elements.

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

Work	σ		vk		PP		$\mathcal{M}$	Randomizable	#PPE	#Pairings
	$\mathbb{G}$	$\mathbb{H}$	$\mathbb{G}$	$\mathbb{H}$	$\mathbb{G}$	$\mathbb{H}$				
[26]	3	2	1	1	3	1	$\widehat{\mathbb{GH}}$	No	$3+1^*$	$7+2^*$
[3] 1	5	2	10	4	-	-	$\mathbb{G}$	Partially	2	$8+4^\dagger$
[3] 2	2	5	10	4	-	-	$\mathbb{H}$	Partially	2	$8+4^\dagger$
[4] 1	2	1	1	3	-	-	$\mathbb{G}\times\mathbb{H}$	No	2	$5+2^\dagger$
[4] 2	2	1	1	1	-	-	$\mathbb{H}$	Yes	2	$4+1^\dagger$
[30]	4	-	-	2	-	-	$\widehat{\mathbb{GH}}$	Yes	$3+1^*$	$6+2^*$
[21] 1	1	2	2	-	-	-	$\mathbb{H}$	No	2	$4+1^\dagger$
[21] 2	1	2	2	-	-	-	$\mathbb{H}$	Yes	2	$5+1^\dagger$
[21] 3	2	1	-	2	-	-	$\mathbb{G}$	Yes	2	$5+1^\dagger$
[6] 1	3	1	-	1	1	-	$\mathbb{G}$	Yes	2	$4+2^\dagger$
[6] 2	2	1	-	1	1	-	$\mathbb{G}$	No	2	$4+2^\dagger$
[12]	1	2	2	-	-	-	$\mathbb{H}$	Yes	2	$3+2^\dagger$
[36] 1	1	2	1	-	-	1	$\mathbb{H}$	Yes	2	$3+3^\dagger$
[36] 2	1	2	1	-	-	1	$\mathbb{H}$	No	2	$4+3^\dagger$
[32]	3	-	-	2	-	-	$\widehat{\mathbb{GH}}$	Yes	$2+1^*$	$5+2^*$
Ours I	2	-	-	2	-	-	$\widehat{\mathbb{GH}}$	Yes[1]	$1+1^*$	$2+1^\dagger+2^*$
Ours II	2	-	-	2	-	-	$\widehat{\mathbb{GH}}$	Yes	$1+1^*$	$2+2^*$

[1] Randomization requires possession of at least 2 distinct signatures on the message.

2 Preliminaries

In this section we provide some preliminary definitions.

2.1 Bilinear Groups

A bilinear group is a tuple $\mathcal{P} := (\mathbb{G}, \mathbb{H}, \mathbb{T}, p, G, \tilde{H}, \hat{e})$ 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 $\hat{e}$ is a non-degenerate bilinear map $\hat{e} : \mathbb{G} \times \mathbb{H} \longrightarrow \mathbb{T}$. For clarity, elements of $\mathbb{H}$ will be accented with $\tilde{}$. We use multiplicative notation for all the groups. We let $\mathbb{G}^\times := \mathbb{G} \backslash \{1_\mathbb{G}\}$ and $\mathbb{H}^\times := \mathbb{H} \backslash \{1_\mathbb{H}\}$. In this paper, we work in the efficient Type-III setting [29], where $\mathbb{G} \neq \mathbb{H}$ and there is no efficiently computable isomorphism 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 $\hat{e}(M, \tilde{H}) = \hat{e}(G, \tilde{N})$. Such pairs were called Diffie-Hellman pairs in [3,26].

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 Eq. (1).

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

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 $\hat{e}$, compute the group operations in groups $\mathbb{G}, \mathbb{H}$ and $\mathbb{T}$, and compare group elements as a *generic signer*.

2.4 Unilateral Structure-Preserving Signatures on Diffie-Hellman Pairs

We define Unilateral Structure-Preserving Signatures on Diffie-Hellman Pairs (USPSDH) as Type-III SPS schemes with the following additional requirements:

(i) Messages are of the form $(M, \tilde{N}) \in \widehat{\mathbb{GH}} \subset \mathbb{G} \times \mathbb{H}$.
(ii) Either signatures are of the form $\sigma = (S_1, \ldots, S_k) \in \mathbb{G}^k$ and the verification key is $\mathsf{vk} = (\tilde{Y}_1, \ldots, \tilde{Y}_n) \in \mathbb{H}^n$ or signatures are of the form $\sigma = (\tilde{S}_1, \ldots, \tilde{S}_k) \in \mathbb{H}^k$ and the verification key is $\mathsf{vk} = (Y_1, \ldots, Y_n) \in \mathbb{G}^n$.

We remark that there exist schemes, e.g. [30,32], which conform to the above requirements. Also, there are schemes, e.g. [3,26], which satisfy the first requirement but not the second.

3 Optimal EUF-CMA Secure Constructions

In this section, we give two new optimal constructions of USPSDH schemes.

3.1 Construction I

Here we give our first EUF-CMA secure construction. Given the description of Type-III bilinear groups $\mathcal{P}$ output by $\mathcal{BG}(1^\kappa)$, the scheme is as follows:

- $\mathsf{KeyGen}(\mathcal{P})$: Select $x, y \leftarrow \mathbb{Z}_p^\times$. Set $\mathsf{sk} := (x, y)$, $\mathsf{vk} := (\tilde{X}, \tilde{Y}) = (\tilde{H}^x, \tilde{H}^y) \in \mathbb{H}^2$.
- $\mathsf{Sign}(\mathsf{sk}, (M, \tilde{N}))$: To sign $(M, \tilde{N}) \in \widehat{\mathbb{GH}}$, select $r \leftarrow \mathbb{Z}_p$, and set $R := G^r$, $S := \left((G^x \cdot M)^r \cdot G\right)^{\frac{1}{y}}$. Return $\sigma := (R, S) \in \mathbb{G}^2$.
- $\mathsf{Verify}(\mathsf{vk}, (M, \tilde{N}), \sigma = (R, S))$: Return 1 iff $R, S \in \mathbb{G}$, $(M, \tilde{N}) \in \widehat{\mathbb{GH}}$, and $\hat{e}(S, \tilde{Y}) = \hat{e}(R, \tilde{X} \cdot \tilde{N})\hat{e}(G, \tilde{H})$.

Correctness of the scheme follows by inspection and is straightforward to verify. The scheme is not strongly unforgeable since for instance given two distinct signatures $\sigma_1 = (R_1, S_1)$ and $\sigma_2 = (R_2, S_2)$ on a message $(M, \tilde{N})$, one can without knowledge of the signing key compute a new signature $\sigma' = (R', S')$ on the same message by computing e.g. $(R' := R_1^2 \cdot R_2^{-1}, S' := S_1^2 \cdot S_2^{-1})$.

Theorem 1. *The scheme is EUF-CMA secure in the generic group model.*[1]

Proof. We prove 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 $\tilde{H}$, $\tilde{X}$, $\tilde{Y}$ which correspond to the discrete logarithms 1, x and y, respectively. Note the signing oracle produces no new elements in $\mathbb{H}$. Thus, at the i-th sign query on $(M_i, \tilde{N}_i)$, $\tilde{N}_i$ can only be a linear combination of $\tilde{H}$, $\tilde{X}$, and $\tilde{Y}$. Similarly, M_i can only be a linear combination of G, $\{R_j\}_{j=1}^{i-1}$, $\{S_j\}_{j=1}^{i-1}$. Thus, we have

$$n_i = a_{n_i} + b_{n_i}x + c_{n_i}y \qquad m_i = a_{m_i} + \sum_{j=1}^{i-1} b_{m_{i,j}} r_j + \sum_{j=1}^{i-1} c_{m_{i,j}} \left(\frac{r_j x + r_j m_j + 1}{y} \right)$$

Since we must have $n_i = m_i$ to have $(M_i, \tilde{N}_i) \in \widehat{\mathbb{GH}}$, we must have $a_{m_i} = a_{n_i}$, $b_{n_i} = c_{n_i} = 0$, $b_{m_{i,j}} = c_{m_{i,j}} = 0$ for all j, i.e. messages correspond to constant polynomials. Similarly, at the end of the game, (m^*, n^*) which is the discrete logarithm of the forged message $(M^*, \tilde{N}^*)$ must be of the form $m^* = n^* = a_m$.

The forgery (R^*, S^*) can only be a linear combination of the group elements from $\mathbb{G}$, i.e. a linear combination of G, $\{R_i\}_{i=1}^{q}$ and $\{S_i\}_{i=1}^{q}$. Thus, we have

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

For the forgery to be accepted, r^* and s^* must satisfy $s^* y = r^* x + r^* m^* + 1$. Therefore, we must have

$$a_s y + \sum_{i=1}^{q} b_{s,i} r_i y + \sum_{i=1}^{q} c_{s,i} \left(r_i x + r_i m_i + 1 \right) = a_r x + \sum_{i=1}^{q} b_{r,i} r_i x + \sum_{i=1}^{q} c_{r,i} \left(\frac{r_i x^2}{y} + \frac{r_i m_i x}{y} + \frac{x}{y} \right)$$
$$+ \left(a_r + \sum_{i=1}^{q} b_{r,i} r_i + \sum_{i=1}^{q} c_{r,i} \left(\frac{r_i x}{y} + \frac{r_i m_i}{y} + \frac{1}{y} \right) \right) m^* + 1$$

There is no term in y or $r_i y$ on the right-hand side so we must have $a_s = 0$, and $b_{s,i} = 0$ for all i. Also, there is no term in $\frac{r_i x^2}{y}$ or x on the left-hand side so we must have $a_r = 0$ and $c_{r,i} = 0$ for all i. Thus, we have

$$\sum_{i=1}^{q} c_{s,i} \left(r_i x + r_i m_i + 1 \right) = \sum_{i=1}^{q} b_{r,i} r_i x + \sum_{i=1}^{q} b_{r,i} r_i m^* + 1 \qquad (2)$$

The monomial $r_i x$ implies $c_{s,i} = b_{r,i}$ for all i, whereas the monomial r_i implies $c_{s,i} m_i = b_{r,i} m^*$. Since we have $c_{s,i} = b_{r,i}$, this means we have $m^* = m_i$ for some i. Hence, the signature (R^*, S^*) is on a message pair $(M_i, \tilde{N}_i)$ that was queried to the sign oracle and thus is not a forgery on a new message. □

[1] We remark that we have double verified all of our generic group proofs using the recent generic group tool of Ambrona et al. [9].

We now prove the following theorem regarding the randomizability/strong unforgeability of the scheme.

Theorem 2. *The scheme is strongly existentially-unforgeable against an adversary that queries the signing oracle on each message once at most.*

Proof. For Equality (2) in the proof of Theorem 1 to hold, it is clear that S^* (from which the left-hand side of (2) is constructed) can only be a linear combination of S_i^* part of the signature returned in response to the i-th signing query on the message $(M^*, \tilde{N}^*)$ (if any). Similarly, R^* can only be a linear combination of R_i^*. Since the adversary can make at most one signing query on each message, we have two cases. If the adversary made no signing query on $(M^*, \tilde{N}^*)$, a forgery would contradict Theorem 1. If the adversary made a signing query on $(M^*, \tilde{N}^*)$, then since in this case $q = 1$, we have $r^* = r_i$ since for (2) to hold, we must have $\sum_{i=1}^{q} c_{s,i} = 1$ which implies $b_{r,i} = 1$ and hence the signature (R^*, S^*) is not new. □

Now consider the following special randomization algorithm for the scheme:

- $\mathsf{Randomize}^{\dagger}\left(\mathsf{vk}, (M, \tilde{N}), \{\sigma_i = (R_i, S_i)\}_{i=1}^{2}\right)$: For any two distinct signatures σ_1 and σ_2, i.e. $R_1 \neq R_2$, satisfying $\mathsf{Verify}(\mathsf{vk}, (M, \tilde{N}), \sigma_i) = 1$ for all $i \in [2]$. To obtain a new signature σ' on $(M, \tilde{N})$, choose $a \leftarrow \mathbb{Z}_p$ and let $b = 1 - a$. Now compute $R' := R_1^a \cdot R_2^b$, $S' := S_1^a \cdot S_2^b$. Return $\sigma' := (R', S')$.

Theorem 3. *Signatures output by* $\mathsf{Randomize}^{\dagger}$ *are perfectly indistinguishable from those output by* Sign *on the same message.*

Proof. In the Sign algorithm, r is chosen uniformly at random from $\mathbb{Z}_p$, whereas in $\mathsf{Randomize}^{\dagger}$, a (resp. b) is also chosen uniformly at random from $\mathbb{Z}_p$. Moreover, for any possible $r \in \mathbb{Z}_p$ such that $R = G^r$, there is $a \in \mathbb{Z}_p$ such that $r = ar_1 + (1-a)r_2$ for any $r_1, r_2 \in \mathbb{Z}_p$ satisfying $r_1 \neq r_2$. Therefore, the distributions of signatures output by $\mathsf{Randomize}^{\dagger}$ and Sign are identical. □

The above observations makes it possible to achieve combined unforgeability [36] where the same scheme can allow (at the discretion of the signer) either strongly unforgeable signatures or ones that can be re-randomized.

3.2 Construction II

Here we give our second construction which yields publicly re-randomizable signatures. Given the description of Type-III bilinear groups $\mathcal{P}$ output by $\mathcal{BG}(1^\lambda)$, the scheme is as follows:

- $\mathsf{KeyGen}(\mathcal{P})$: Select $x, y \leftarrow \mathbb{Z}_p^{\times}$. Set $\mathsf{sk} := (x, y)$ and $\mathsf{vk} := (\tilde{X}, \tilde{Y}) = (\tilde{H}^x, \tilde{H}^y) \in \mathbb{H}^2$.
- $\mathsf{Sign}(\mathsf{sk}, (M, \tilde{N}))$: To sign $(M, \tilde{N}) \in \widehat{\mathbb{GH}}$, select $r \leftarrow \mathbb{Z}_p^{\times}$, and set $R := G^r$, $S := \left(G^x \cdot M\right)^{\frac{r}{y}}$. Return $\sigma := (R, S) \in \mathbb{G}^2$.

- $\mathsf{Verify}(\mathsf{vk}, (M, \tilde{N}), \sigma = (R, S))$: Return 1 iff $R \in \mathbb{G}^{\times}, S \in \mathbb{G}$, $(M, \tilde{N}) \in \widehat{\mathbb{GH}}$, and $\hat{e}(S, \tilde{Y}) = \hat{e}(R, \tilde{X} \cdot \tilde{N})$.
- $\mathsf{Randomize}(\mathsf{vk}, (M, \tilde{N}), \sigma = (R, S))$: Select $r' \leftarrow \mathbb{Z}_p^{\times}$, and set $R' := R^{r'}$, $S' := S^{r'}$. Return $\sigma' := (R', S')$.

Note that R is information-theoretically independent of the message and hence even when proving knowledge of signatures, this component of the signature can be revealed in the clear after re-randomizing it which allows one to verify that $R \neq 1_{\mathbb{G}}$.

Correctness of the scheme follows by inspection and is straightforward to verify. The scheme is perfectly randomizable as the distribution of re-randomized signatures is identical to that of fresh signatures on the same message.

The proof of the following theorem is in the full version [33].

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

4 Optimal sEUF-CMA Secure SPS One-Time Schemes

We give here new strongly unforgeable one-time Type-III schemes for unilateral messages matching the optimal one-time scheme in [6] in every measure. By transposing the groups, one can similarly sign messages in $\mathbb{H}^k$. Obtaining a scheme for a vector of Diffie-Hellman messages or a mixture of unilateral and Diffie-Hellman messages from our scheme is straightforward. The scheme for message space $\mathbb{G}^k$ is as follows:

- $\mathsf{KeyGen}(\mathcal{P})$: Select $x_1, \ldots, x_k, y \leftarrow \mathbb{Z}_p^{\times}$. Set $\mathsf{sk} := (x_1, \ldots, x_k, y)$ and $\mathsf{vk} := (\tilde{X}_1, \ldots, \tilde{X}_k, \tilde{Y}) := (\tilde{H}^{x_1}, \ldots \tilde{H}^{x_k}, \tilde{H}^{y}) \in \mathbb{H}^{k+1}$.
- $\mathsf{Sign}\big(\mathsf{sk}, (M_1, \ldots, M_k) \in \mathbb{G}^k\big)$: Return $\sigma := \big(G^{x_1} \cdot M_1 \cdot \prod_{i=2}^{k} M_i^{x_i}\big)^{\frac{1}{y}} \in \mathbb{G}$.
- $\mathsf{Verify}(\mathsf{vk}, (M_1, \ldots, M_k), \sigma)$: Return 1 iff $\sigma \in \mathbb{G}$, $M_i \in \mathbb{G}$ for $i = 1, \ldots, k$, and $\hat{e}(\sigma, \tilde{Y}) = \hat{e}(G, \tilde{X}_1)\hat{e}(M_1, \tilde{H}) \prod_{i=2}^{k} \hat{e}(M_i, \tilde{X}_i)$.

Correctness of the scheme follows by inspection. The Sign algorithm is deterministic and hence for any message there is 1 potential signature. The proof of the following theorem is in the full version [33].

Theorem 5. *The scheme is sEUF-CMA secure against a one-time chosen-message attack.*

5 Optimal Partially Structure-Preserving Signature Scheme for a Vector of Messages

We give here an optimal scheme for the message space $\widehat{\mathbb{GH}} \times \mathbb{Z}_p^k$. We call such a variant *partially structure-preserving* since other than allowing some part of the messages to not be group elements, the scheme conforms to the rest of the requirements of structure-preserving signatures.

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

- $\mathsf{KeyGen}(\mathcal{P})$: Select $x, y_1, \ldots, y_k, z \leftarrow \mathbb{Z}_p^\times$. Set $\tilde{X} := \tilde{H}^x$, $\tilde{Y}_i := \tilde{H}^{y_i}$ for all $i \in [k]$, $\tilde{Z} := \tilde{H}^z$. Set $\mathsf{sk} := (x, y_1, \ldots, y_k, z)$ and $\mathsf{vk} := (\tilde{X}, \tilde{Y}_1, \ldots, \tilde{Y}_k, \tilde{Z})$.
- $\mathsf{Sign}\Big(\mathsf{sk}, \big((M, \tilde{N}), \boldsymbol{u} = (u_1, \ldots, u_k)\big)\Big)$: To sign a Diffie-Hellman pair $(M, \tilde{N}) \in \widehat{\mathbb{GH}}$ and a vector $\boldsymbol{u} = (u_1, \ldots, u_k) \in \mathbb{Z}_p^k$, select $r \leftarrow \mathbb{Z}_p^\times$, and set $R := G^r$, $S := \big(M \cdot G^{x + \sum_{i=1}^k u_i y_i}\big)^{\frac{r}{z}}$. Return $\sigma := (R, S) \in \mathbb{G}^2$.
- $\mathsf{Verify}\Big(\mathsf{vk}, \big((M, \tilde{N}), \boldsymbol{u}\big), \sigma = (R, S)\Big)$: Return 1 iff $R \in \mathbb{G}^\times$, $(M, \tilde{N}) \in \widehat{\mathbb{GH}}$, and $\hat{e}(S, \tilde{Z}) = \hat{e}(R, \tilde{N} \cdot \tilde{X} \cdot \prod_{i=1}^k \tilde{Y}_i^{u_i})$.
- $\mathsf{Randomize}\Big(\mathsf{vk}, \big((M, \tilde{N}), \boldsymbol{u}\big), \sigma = (R, S)\Big)$: Select $r' \leftarrow \mathbb{Z}_p^\times$, and set $R' := R^{r'}$, $S' := S^{r'}$. Return $\sigma' := (R', S')$.

Correctness of the scheme is straightforward to verify. The signatures are perfectly randomizable. We now prove the following theorem.

Theorem 6. *The scheme is EUF-CMA secure.*

Proof. Let $\mathcal{A}$ be an adversary against the scheme. Using $\mathcal{A}$, we can build an adversary $\mathcal{B}$ against the unforgeability of Scheme II in Sect. 3.2. Adversary $\mathcal{B}$ gets $\mathsf{vk}' = (\tilde{X}', \tilde{Y}')$ from her game where she has access to a sign oracle. She chooses $y_1, \ldots, y_k \leftarrow \mathbb{Z}_p$ and sets $\tilde{Y}_i := \tilde{H}^{y_i}$ for $i = 1, \ldots, k$. She starts $\mathcal{A}$ on the verification key $\mathsf{vk} := (\tilde{X} := \tilde{X}', \tilde{Y}_1, \ldots, \tilde{Y}_k, \tilde{Z} := \tilde{Y}')$. When receiving a query on $\Big((M, \tilde{N})_i, \boldsymbol{u}_i\Big)$ from $\mathcal{A}$, $\mathcal{B}$ returns $\perp$ if $(M, \tilde{N})_i \notin \widehat{\mathbb{GH}}$. Otherwise, she forwards the message $(M_i', \tilde{N}_i') := \left(M_i \cdot G^{\sum\limits_{j=1}^k y_j u_{i,j}}, \tilde{N}_i \cdot \tilde{H}^{\sum\limits_{j=1}^k y_j u_{i,j}}\right) \in \widehat{\mathbb{GH}}$ to her sign oracle and returns the signature she gets to $\mathcal{A}$. Such a signature is a valid signature on the message $\Big((M, \tilde{N})_i, \boldsymbol{u}_i\Big)$.

Eventually, when $\mathcal{A}$ outputs her forgery σ^* on $\Big((M^*, \tilde{N}^*), \boldsymbol{u}^*\Big)$, $\mathcal{B}$ returns $\left(\left(M' := M^* \cdot G^{\sum\limits_{j=1}^k y_j u_j^*}, \tilde{N}' := \tilde{N}^* \cdot \tilde{H}^{\sum\limits_{j=1}^k y_j u_j^*}\right), \sigma^*\right)$ in her game. Thus, $\mathcal{B}$ wins her game with the same advantage as that of $\mathcal{A}$ in her game. □

6 Applications

Here we highlight some applications of our new schemes.

Direct Anonymous Attestation (DAA). DAA [15] is a protocol deployed in practice for realizing trusted computing. Bernhard et al. [14] introduced Randomizable Weakly Blind Signature (RwBS) schemes as one of the building blocks for their generic construction of DAA schemes. A RwBS scheme is similar to a standard blind signature scheme [22] but unlike the latter, in the former the signer never gets to see the signed message. DAA is outside of the scope of this paper but for the record we show that combining our publicly re-randomizable scheme from Sect. 3.2 with the SXDH-based Groth-Sahai proofs [37] yields more efficient RwBS schemes (and hence DAA schemes) not relying on random oracles than existing ones [13,32]. The RwBS constructions in [13,32] combine SPS schemes from [30,32], respectively, with SXDH-based Groth-Sahai proofs [37]. The underlying (less efficient) SPS schemes used in [13,32] have the same message space as ours, and similarly to our schemes, enjoy fully randomizable unilateral signatures.

The construction is based on the observation that since signing in those schemes only requires the $\mathbb{G}$ component of the message, whereas verification requires the $\mathbb{H}$ component of the message, it suffices for the user to only submit the $\mathbb{G}$ component of the message along with a zero-knowledge proof of knowledge of the $\mathbb{H}$ component when requesting signatures. The signer then has to accompany the signature she returns with a zero-knowledge proof of correctness of the returned signature. The final RwBS signature is then just a re-randomization of the signature. The RwBS construction as well as the proofs (which can be found in the full version [33]) are very similar to those in [13,32]. The difference lies in the zero-knowledge proofs used in the signing protocol. Our RwBS scheme yields signatures of size $2|\mathbb{G}|$ and require 1 PPE equation (2 pairings in total) to verify and hence is more efficient than those in [13,32].

Attribute-Based Signatures. Attribute-Based Signatures (ABS) [42] allow signers to authenticate messages while enjoying fine-grained control over identifying information. El Kaafarani et al. [24] introduced the notion of Decentralized Traceable Attribute-Based Signatures (DTABS) which adds the traceability feature to standard ABS schemes while allowing attribute authorities to operate in a decentralized manner. Ghadafi [31] revisited the latter notion and provided strengthening of some of the security requirements as well as more efficient constructions. For security definitions and applications refer to [24,31,42].

The most efficient existing DTABS construction not relying on random oracles is the one in [31] which uses the optimal structure-preserving signature scheme from [4] and yields signatures of size $(27|\mathbb{P}| + 19) \cdot |\mathbb{G}| + (22|\mathbb{P}| + 15) \cdot |\mathbb{H}| + (\beta + 3) \cdot |p|$, where $|\mathbb{P}|$ is the number of attributes in the signing policy $\mathbb{P}$, i.e. the number of rows of the span program matrix, whereas β is the number of columns. By instantiating the generic DTABS construction from [31] with the same tools as the instantiations in [31] with the exception of using our partially structure-preserving signature scheme from Sect. 5 to instantiate the tagged signature building block (where the verification key of the user is the Diffie-Hellman component of the message, whereas the attributes are the $\mathbb{Z}_p$ component), we obtain a construction of DTABS not relying on random oracles with signatures of size $(17|\mathbb{P}| + 24) \cdot |\mathbb{G}| + (14|\mathbb{P}| + 18) \cdot |\mathbb{H}| + (\beta + 3) \cdot |p|$ which is shorter than all existing constructions. Security of the instantiation follows from that of the generic construction of [31]. See the full version [33] for details.

7 Lower Bounds and Impossibility Results

Here we prove some lower bounds and impossibility results for USPSDH schemes.

Impossibility of One-Element Signatures. We prove that there is no generic-signer USPSDH scheme with one-element signatures that is EUF-RMA secure against $q > 1$ signing queries.

Theorem 7. *There is no generic-signer USPSDH scheme with one-element signatures that is unforgeable against a random-message attack for $q > 1$ signing queries.*

Proof. Consider the case where the signature $\sigma = S \in \mathbb{G}$, whereas the verification key $\mathsf{vk} = (\tilde{X}_1, \ldots, \tilde{X}_n) \in \mathbb{H}^n$. The proof for the opposite case is similar.

We first prove that it is redundant for a USPSDH scheme (for a single Diffie-Hellman pair) with one-element signatures to have more than 1 verification equation (not counting the cost for verifying the well-formedness of the message).

Lemma 1. *One verification equation is sufficient for a one-element signature scheme.*

Proof. Such a scheme has verification equations of the form of Eq. (3).

$$\prod \hat{e}(S, \tilde{X}_i)^{a_{i,\ell}} \prod \hat{e}(M, \tilde{X}_i)^{b_{i,\ell}} \hat{e}(S, \tilde{N})^{c_\ell} \hat{e}(M, \tilde{N})^{d_\ell} = Z_{\ell_{\mathbb{T}}} \tag{3}$$

Each of those equations is linear in S. Thus, we can compute a single non-trivial equation linear in S (which uniquely determines S) as a linear combination of all equations and use it for verification. If there is no such combination, the equations must be linearly dependent and hence some of them are redundant. By excluding those, we can reduce them to a single equation linear in S. □

For the scheme to be (perfectly) correct (and publicly verifiable), signatures must verify w.r.t. the (fixed) verification key and (fixed) public parameters (if any). By taking the discrete logarithms of the group elements in the (single) verification equation, we can write the verification equation as

$$s(\sum_{i=1}^{n} a_i x_i + cm) + m(\sum_{i=1}^{n} b_i x_i + dm) = z \tag{4}$$

This implies that there exists at most one potential signature for the message. Since the signing algorithm is generic, a signature σ_i on $(M_i, \tilde{N}_i)$ has the form $\sigma_i = M_i^\alpha \cdot G^\beta$ for some (fixed) $\alpha, \beta \in \mathbb{Z}_p$. Now given signatures σ_1 and σ_2 on distinct random messages $(M_1, \tilde{N}_1), (M_2, \tilde{N}_2)$, respectively, we have $\sigma_1 = M_1^\alpha \cdot G^\beta$ and $\sigma_2 = M_2^\alpha \cdot G^\beta$. By computing $\sigma^* := \sigma_1^\gamma \cdot \sigma_2^{(1-\gamma)}$ we obtain a valid forgery on the message $(M^*, \tilde{N}^*) := \big(M_1^\gamma \cdot M_2^{(1-\gamma)}, \tilde{N}_1^\gamma \cdot \tilde{N}_2^{(1-\gamma)}\big)$ for any $\gamma \in \mathbb{Z}_p$. □

Lower Bounds on the Size of the Verification Key. We prove here that a generic-signer EUF-RMA secure USPSDH scheme with one-element signatures must have at least 2 group elements (excluding the default group generators G and $\tilde{H}$) in the verification key. WLOG, we assume that any public group elements (other than the default group generators) part of the public parameters (if any) are counted as part of the verification key.

Theorem 8. *A generic-signer EUF-RMA secure one-time USPSDH scheme (with one-element signatures) must have at least* 2 *elements in the verification key.*

Proof. Consider the case where $\sigma = S \in \mathbb{G}$ and $\mathsf{vk} = \tilde{X} \in \mathbb{H}$. The proof for the opposite case is similar. Such a scheme has a verification equation (not counting the check for the well-formedness of the message) of the following form

$$\hat{e}(S, \tilde{X})^a \hat{e}(S, \tilde{H})^b \hat{e}(M, \tilde{X})^c \hat{e}(M, \tilde{H})^d \hat{e}(S, \tilde{N})^u \hat{e}(M, \tilde{N})^v = Z_{\mathbb{T}} \tag{5}$$

This means that s the discrete logarithm of the signature S has the form

$$s = \frac{z - m(cx + d + vm)}{ax + b + um}$$

A generic signer (who does not know the discrete logarithm m of the message) computes the signature S as $S := M^{\frac{\alpha(x)}{\alpha'(x)}} \cdot G^{\frac{\beta(x)}{\beta'(x)}}$ for some polynomials $\alpha, \alpha', \beta, \beta' \in \mathbb{Z}_p[x]$. Note that none of those polynomials has a term in m. Our proof strategy is to first eliminate some pairings from Eq. (5) which can not be computed by a generic signer which serves to simplify the proof. Note that without knowledge of the discrete logarithm of the message m, it is hard for a generic signer to construct a non-trivial signature S where its discrete logarithm s contains the message m in a term in the denominator. Thus, WLOG we can assume that we have $u = 0$ in Eq. (5). Similarly, it is hard for a generic signer without knowledge of m to construct a signature that contains a term with degree >1 in m (since none of the above polynomials have a term in m). Therefore, we can also WLOG assume that $v = 0$ in Eq. (5).[2]

We now show that any USPSDH scheme with a verification equation of the form of Eq. (6) cannot be secure.

$$\hat{e}(S, \tilde{X})^a \hat{e}(S, \tilde{H})^b \hat{e}(M, \tilde{X})^c \hat{e}(M, \tilde{H})^d = Z_{\mathbb{T}} \tag{6}$$

Since the verification key (and the public parameters) contain only $\tilde{X}$, G, and $\tilde{H}$, we have $Z_{\mathbb{T}} = \hat{e}(G, \tilde{H})^e \hat{e}(G, \tilde{X})^f$. Note that the exponents $a, b, c, d, e, f \in \mathbb{Z}_p$ are all public. By taking the discrete logarithms of the group elements, we can write the verification equation as

$$s(ax + b) + m(cx + d) = e + fx \tag{7}$$

[2] Refer to the full version [33] for more justification and discussions on why such assumptions do not affect the generality of our proof and how similar cases also apply to other SPS settings.

Note here if $a = b = 0$, the equation is independent of the signature S. Similarly, if $c = d = 0$, the verification equation is independent of the message $(M, \tilde{N})$. Therefore, neither of those cases should occur as otherwise it is obvious that such a scheme is not secure. We now have four cases as follows:

- **Case** $bc \neq ad$**:** Given a signature $\sigma = S$ on a random message $(M, \tilde{N})$, pick any $\alpha \leftarrow \mathbb{Z}_p \setminus \{1\}$ and let
$$a_m := \tfrac{ea(\alpha-1)-bf(\alpha-1)}{bc-ad} \qquad \text{and} \qquad a_s := -\tfrac{ec(\alpha-1)-df(\alpha-1)}{bc-ad}$$
By computing $\sigma^* = S^* := G^{a_s} \cdot S^{\alpha}$, one obtains a valid forgery on $\big(M^*, \tilde{N}^*\big) := \big(G^{a_m} \cdot M^{\alpha}, \tilde{H}^{a_m} \tilde{N}^{\alpha}\big)$.
- **Case** $bc = ad \neq 0$**:** Given a signature $\sigma = S$ on a random message $(M, \tilde{N})$, pick any $\alpha \leftarrow \mathbb{Z}_p^{\times}$ and compute $\sigma^* = S^* := G^{\alpha} \cdot S$, which is a valid forgery on $\big(M^*, \tilde{N}^*\big) := \big(G^{\frac{-b\alpha}{d}} \cdot M, \tilde{H}^{\frac{-b\alpha}{d}} \cdot \tilde{N}\big)$.
- **Case** $bc = ad = 0$, $a \neq 0$ **and** $c \neq 0$**:** Here we have that $b = d = 0$. Given a signature $\sigma = S$ on a random message $(M, \tilde{N})$, $\sigma^* = S^* := G^{\frac{-c\alpha}{a}} \cdot S$ is a valid forgery on $\big(M^*, \tilde{N}^*\big) := \big(G^{\alpha} \cdot M, \tilde{H}^{\alpha} \cdot \tilde{N}\big)$ for any $\alpha \in \mathbb{Z}_p^{\times}$.
- **Case** $bc = ad = 0$, $b \neq 0$ **and** $d \neq 0$**:** Here we have that $a = c = 0$. Given a signature $\sigma = S$ on a random message $(M, \tilde{N})$, $\sigma^* = S^* := G^{\frac{-d\alpha}{b}} \cdot S$ is a valid forgery on $\big(M^*, \tilde{N}^*\big) := \big(G^{\alpha} \cdot M, \tilde{H}^{\alpha} \cdot \tilde{N}\big)$ for any $\alpha \in \mathbb{Z}_p^{\times}$.

This concludes the proof. □

We now show that the lower bounds for the verification key proved in Theorem 8 holds even if we allow the (generic-signer) signature to have 2 elements.

Theorem 9. *There is no EUF-RMA one-time USPSDH scheme with two-element signatures,* 1 *PPE verification equation and one-element verification key.*

Proof. Consider the case where the signature $\sigma = (R, S) \in \mathbb{G}^2$ whereas the verification key $\mathsf{vk} := \tilde{X} \in \mathbb{H}$. The proof for the opposite case is similar. Such a scheme has a verification equation of the form of Eq. (8).

$$\hat{e}(R, \tilde{X})^a \hat{e}(R, \tilde{N})^b \hat{e}(R, \tilde{H})^c \hat{e}(S, \tilde{X})^d \hat{e}(S, \tilde{H})^u \hat{e}(M, \tilde{X})^v \hat{e}(M, \tilde{H})^w = Z_{\mathbb{T}} \tag{8}$$

As argued in the proof of Theorem 8, since the signing algorithm is generic, WLOG neither R nor S can have a degree >1 of m (the discrete logarithm of the message) or have a term in m in the denominator. It is obvious that a scheme with both signature components independent of the message is insecure. Thus, at least one component of the signature must depend on the message. WLOG, let's assume that S depends on the message while R is independent of the message. If it is the other way around, we just need to replace the term $\hat{e}(R, \tilde{N})^b$ with $\hat{e}(S, \tilde{N})^b$ in Eq. (8) and the proof is similar. If both components of the signature depend on the message, Eq. (8) can be simplified by setting $b = 0$ which is a special case of the cases we prove.

Since we only have $\tilde{X}, G, \tilde{H}$ in the verification key (and the public parameters), we have $Z_{\mathbb{T}} = \hat{e}(G, \tilde{H})^e \hat{e}(G, \tilde{X})^f$. Note $a, b, c, d, e, f, u, v, w \in \mathbb{Z}_p$ are all public. By taking discrete logarithms, we can write the verification equation as

$$r(ax + bm + c) + s(dx + u) + m(vx + w) = e + fx \qquad (9)$$

We start by listing 3 trivial forgery cases as follows:

1. **Case** $a = b = c = 0$ **or** $d = u = 0$**:** This means the verification equation is independent of one of the signature components and thus we are back into the one-element signature case which is already proven by Theorem 8.
2. **Case** $a = d = f = v = 0$**:** This means the verification equation is independent of the verification key (and hence σ is independent of sk).
3. **Case** $b = v = w = 0$**:** This means the verification equation is independent of the message m and hence the signature is valid on any other message.

Excluding the above obvious forgery cases, we can find a forgery by solving the following system of equations in the 9 unknowns $\alpha_m, \beta_m, \alpha_r, \beta_r, \gamma_r, \alpha_s, \beta_s, \gamma_s, \delta_s$

$$u\alpha_s + e\gamma_s - e + b\alpha_r\alpha_m + c\alpha_r + w\alpha_m = 0 \qquad d\alpha_s + f\gamma_s - f + a\alpha_r + v\alpha_m = 0$$

$$u\beta_s - w\gamma_s + b\beta_r\alpha_m + b\alpha_r\beta_m + c\beta_r + w\beta_m = 0 \qquad u\delta_s - c\gamma_s + b\gamma_r\alpha_m + c\gamma_r = 0$$

$$d\delta_s - a\gamma_s + a\gamma_r = 0 \qquad d\beta_s - v\gamma_s + a\beta_r + v\beta_m = 0$$

$$\gamma_s - \gamma_r\beta_m = 0 \qquad \beta_r\beta_m = 0$$

This is a system of 8 equations in 9 unknowns and we get two family of solutions depending on whether $\beta_m = 0$ (where forgeries require no signing queries) or $\beta_m \neq 0$ (where forgeries require a single random-message signing query). Refer to the full version [33] for the full proof. □

Impossibility of sEUF-CMA Secure Schemes. The following theorem whose proof is in the full version [33] proves that there is no generic-signer USPSDH scheme that is sEUF-CMA against an adversary making $q > 1$ signing queries. We note, however, that there exist sEUF-RMA secure schemes and sEUF-CMA secure schemes, e.g. Scheme I, against an adversary that is not allowed multiple queries on the same message.

Theorem 10. *There is no generic-signer USPSDH scheme that is sEUF-CMA secure against an adversary making $q > 1$ signing queries.*

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). doi: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). doi: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). doi: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). doi: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). doi: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). doi: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). doi: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). doi:10.1007/978-3-662-46803-6_2
9. Ambrona, M., Barthe, G., Schmidt, B.: Automated unbounded analysis of cryptographic constructions in the generic group model. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 822–851. Springer, Heidelberg (2016). doi:10.1007/978-3-662-49896-5_29
10. 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). doi:10.1007/978-3-642-34961-4_23
11. 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). doi:10.1007/978-3-662-46447-2_5
12. 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). doi:10.1007/978-3-662-46447-2_16
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). doi:10.1007/978-3-642-38980-1_33
14. Bernhard, D., Fuchsbauer, G., Ghadafi, E., Smart, N.P., Warinschi, B.: Anonymous attestation with user-controlled linkability. Int. J. Inf. Secur. **12**(3), 219–249 (2013)
15. Brickell, E., Camenisch, J., Chen, L.: Direct anonymous attestation. In: CCS 2004, pp. 132–145. ACM (2004)

16. Camenisch, J., Dubovitskaya, M., Haralambiev, K.: Efficient structure-preserving signature scheme from standard assumptions. In: Visconti, I., Prisco, R. (eds.) SCN 2012. LNCS, vol. 7485, pp. 76–94. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32928-9_5
17. 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). doi:10.1007/978-3-662-48800-3_11
18. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004). doi:10.1007/978-3-540-28628-8_4
19. Chase, M., Kohlweiss, M.: A new hash-and-sign approach and structure-preserving signatures from DLIN. In: Visconti, I., Prisco, R. (eds.) SCN 2012. LNCS, vol. 7485, pp. 131–148. Springer, Heidelberg (2012). doi:10.1007/978-3-642-32928-9_8
20. Chatterjee, S., Hankerson, D., Knapp, E., Menezes, A.: Comparing two pairing-based aggregate signature schemes. Des. Codes Crypt. **55**(2010), 141–167 (2010)
21. 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). doi:10.1007/978-3-662-48797-6_13
22. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) CRYPTO 1982. LNCS, pp. 199–203. Springer, Boston (1983). doi:10.1007/978-1-4757-0602-4_18
23. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory **31**(4), 469–472 (1985)
24. 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). doi:10.1007/978-3-319-04852-9_17
25. 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). doi:10.1007/3-540-47721-7_12
26. Fuchsbauer, G.: Automorphic Signatures in Bilinear Groups and an Application to Round-Optimal Blind Signatures. Cryptology ePrint Archive, Report 2009/320
27. Fuchsbauer, G.: Commuting signatures and verifiable encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 224–245. Springer, Heidelberg (2011). doi:10.1007/978-3-642-20465-4_14
28. 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). doi:10.1007/978-3-662-48000-7_12
29. Galbraith, S., Paterson, K., Smart, N.P.: Pairings for cryptographers. Discrete Appl. Math. **156**(2008), 3113–3121 (2008)
30. 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). doi:10.1007/978-3-642-39059-3_23
31. Ghadafi, E.: Stronger security notions for decentralized traceable attribute-based signatures and more efficient constructions. In: Nyberg, K. (ed.) CT-RSA 2015. LNCS, vol. 9048, pp. 391–409. Springer, Cham (2015). doi:10.1007/978-3-319-16715-2_21
32. Ghadafi, E.: Short structure-preserving signatures. In: Sako, K. (ed.) CT-RSA 2016. LNCS, vol. 9610, pp. 305–321. Springer, Cham (2016). doi:10.1007/978-3-319-29485-8_18

33. Ghadafi, E.: More Efficient Structure-Preserving Signatures - Or: Bypassing the Type-III Lower Bounds. Cryptology ePrint Archive, Report 2016/255. http://eprint.iacr.org/2016/255.pdf
34. Green, M., Hohenberger, S.: Universally composable adaptive oblivious transfer. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 179–197. Springer, Heidelberg (2008). doi:10.1007/978-3-540-89255-7_12
35. 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). doi:10.1007/11935230_29
36. 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). doi:10.1007/978-3-662-48797-6_11
37. Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. SIAM J. Comput. **41**(5), 1193–1232 (2012)
38. 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). doi:10.1007/978-3-642-32009-5_35
39. 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). doi:10.1007/978-3-662-54388-7_7
40. 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). doi:10.1007/978-3-662-48000-7_14
41. 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). doi:10.1007/978-3-662-48000-7_15
42. 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). doi:10.1007/978-3-642-19074-2_24
43. 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). doi:10.1007/11586821_1
44. Pointcheval, D., Sanders, O.: Short randomizable signatures. In: Sako, K. (ed.) CT-RSA 2016. LNCS, vol. 9610, pp. 111–126. Springer, Cham (2016). doi:10.1007/978-3-319-29485-8_7
45. 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). doi:10.1007/3-540-69053-0_18
46. 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). doi:10.1007/978-3-662-53890-6_16
47. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005). doi:10.1007/11426639_7