Structure-Preserving Signatures from Type II Pairings

Masayuki Abe[1], Jens Groth[2⋆], Miyako Ohkubo[3], and Mehdi Tibouchi[1]

[1] Secure Platform Laboratories, NTT Corporation, Japan
{abe.masayuki,tibouchi.mehdi}@lab.ntt.co.jp
[2] University College London, UK
j.groth@ucl.ac.uk
[3] Security Architecture Lab, NSRI, NICT, Japan
m.ohkubo@nict.go.jp

Abstract. We investigate structure-preserving signatures in asymmetric bilinear groups with an efficiently computable homomorphism from one source group to the other, i.e., the Type II setting. It has been shown that in the Type I and Type III settings (with maximal symmetry and maximal asymmetry respectively), structure-preserving signatures need at least 2 verification equations and 3 group elements. It is therefore natural to conjecture that this would also be required in the intermediate Type II setting, but surprisingly this turns out not to be the case. We construct structure-preserving signatures in the Type II setting that only require a single verification equation and consist of only 2 group elements. This shows that the Type II setting with partial asymmetry is different from the other two settings in a way that permits the construction of cryptographic schemes with unique properties.

We also investigate lower bounds on the size of the public verification key in the Type II setting. Previous work in structure-preserving signatures has explored lower bounds on the number of verification equations and the number of group elements in a signature but the size of the verification key has not been investigated before. We show that in the Type II setting it is necessary to have at least 2 group elements in the public verification key in a signature scheme with a single verification equation.

Our constructions match the lower bounds so they are optimal with respect to verification complexity, signature sizes and verification key sizes. In fact, in terms of verification complexity, they are the most efficient structure preserving signature schemes to date. Depending on the context in which a scheme is deployed it is sometimes desirable to have strong existential unforgeability, and in other cases full randomizability. We give two structure-preserving signature schemes with a single verification equation where both the signatures and the public verification keys consist of two group elements each. One signature scheme is strongly existentially unforgeable, the other is fully randomizable. Having such simple and elegant structure-preserving signatures may make the Type II setting the easiest to use when designing new structure-preserving cryptographic schemes, and lead to schemes with the greatest conceptual simplicity.

Keywords: Structure-preserving signatures, Type II pairings, strong existential unforgeability, randomizability, lower bounds.

1 Introduction

Structure-preserving signatures [3] are pairing-based signatures that consist of group elements and that are verified by testing equality of products of pairings of group elements. They are useful building blocks in modular design of cryptographic protocols, in particular in combination with non-interactive zero-knowledge (NIZK) proofs of knowledge about group elements [21]. There are numerous applications of structure-preserving signatures, such as blind signatures [3,16], group signatures [3,16,25], homomorphic signatures [24,8], delegatable anonymous credentials [15], compact verifiable shuffles [13], network encoding [7], oblivious transfer [19,11], tightly secure encryption [22,2], anonymous e-cash [27], etc.

Galbraith, Paterson and Smart [17] classify pairings $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ into three types depending on whether $\mathbb{G}_1 = \mathbb{G}_2$ (Type I), or there is an efficiently computable homomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ (Type II), or there is no efficiently

⋆ The research leading to these results has received funding from the Engineering and Physical Sciences Research Council grant EP/J009520/1 and the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 307937.

Setting	Signature	Verification key	Equations
Type III [4]	**3**	2	**2**
Type I [6]	**3**	3	**2**
Type II (this work)	**2**	**2**	**1**

Table 1. Most efficient structure-preserving signatures schemes for all three types of pairings, in terms of signature size, verification key size and number of verification equations. Boldface values are known to be optimal for their respective pairing types. Verification key size is inclusive of group elements that can be shared in a common reference string used by all signers.

computable homomorphism in either direction between $\mathbb{G}_1$ and $\mathbb{G}_2$ (Type III). Structure-preserving signatures have been analyzed in the symmetric Type I setting [4] and in the fully asymmetric Type III setting [6], and in both cases it has been shown that a structure-preserving signatures requires at least 2 verification equations and 3 group elements in the signatures.

It is thus natural to conjecture that 2 verification equations and 3 group elements would be needed in the intermediate Type II setting as well; and indeed this is the case if the messages belong to $\mathbb{G}_1$. However, when the messages belong to $\mathbb{G}_2$ we find the conjecture to be false, and give constructions of structure-preserving signatures with only one verification equation and 2 group elements in the signatures. This is significant from a high level pairing-based cryptography perspective, as it provides a concrete example of a property that can be obtained in the Type II setting but not in the other settings. Therefore, contrary to expectations, we settle Chatterjee and Menezes' open question of whether schemes based on Type II pairings can always be converted to Type III pairings at no efficiency cost [14] in the negative.

Having a single verification equation make the structure-preserving signature schemes quite efficient. As we discuss in 2.1 even though Type III pairings are more efficient in some respects with current techniques (certain group elements have a more compact representation), Type II pairings are competitive, especially in terms of speed: this makes our proposed scheme the most efficient construction to date in terms of verification complexity. Furthermore, with only one verification equation, structure-preserving signatures become conceptually simpler and easier to use for the designer of cryptographic schemes. Groth-Sahai proofs for the Type II setting [21,18] also incur a smaller overhead when there is only one verification equation.

We give two constructions of structure-preserving signatures. One is randomizable, which means that a signature on a message can be randomized to look like a new fresh signature on the message. This randomization is useful because it ensures that one of the group elements in the signature is uniformly random, which is a convenient feature when building anonymization protocols: this random group element can be revealed in the clear without showing what the original signature was. In other contexts, it is desirable that the signature cannot be tampered with, and our second construction satisfies this property: it is strongly unforgeable.

Prior work has explored lower bounds in the Type I and Type III settings, and established that 2 verification equations are required, and that signatures must consist of at least 3 group elements in both of those cases [4,6]. A third dimension of efficiency is the size of the verification key of the signature scheme. In this paper, we obtain the first lower bounds on verification key size in the literature on structure-preserving signatures: in the Type II setting, a verification key for a single verification equation signature scheme must have at least two group elements. A summary of the best known constructions and efficiency bounds for all three types of pairings is provided in Table 1.

Related work. The term "structure-preserving signatures" was first introduced by Abe et al. [3], but the notion appears in earlier works as well. Groth [20] proposed the first structure-preserving signature scheme, but the construction involves hundreds of group elements and is not practical. Green and Hohenberger [19] constructed a structure-preserving signature scheme secure against random message attacks, which is however not known to be secure against adaptive chosen message attacks. Cathalo, Libert and Yung [12] constructed a signature scheme structure-preserving in a relaxed sense that permits the verification key to include target group elements. Hofheinz and Jager [22] and Abe et al. [1,2] investigated the possibility of basing structure-preserving signatures on standard assumptions. They proposed structure-preserving signatures based on the decision linear (DLIN) assumption. The use of a nice security assumption, however, comes at the price of reduced efficiency.

Abe et al. [4] showed that structure-preserving signatures in Type III bilinear groups require at least 3 group elements and 2 verification equations. They also gave structure-preserving signatures matching those bounds that are secure in the generic bilinear group model.

Abe et al. [5] later showed that 3-element signatures cannot be proved secure under a non-interactive assumption using black-box reductions, so strong assumptions are needed to get optimal efficiency in the Type III setting. It is an open question whether a similar impossibility of basing optimal structure-preserving signatures on non-interactive assumptions also holds in the Type II setting (we conjecture it does). However, to get a more conservative non-interactive assumption we modify our first structure-preserving signature scheme in Appendix B to base it on a standard non-interactive hardness assumption. The modification requires adding an extra group element to the verification key and the signature but the scheme still has only a single verification equation.

Recently Abe et al. [6] investigated the symmetric setting (Type I) and found that the same lower bound of 3 group elements and 2 verification equations applies. They also presented a unified structure-preserving signature scheme working in all three types of settings and meeting this bound, which means a structure-preserving signature scheme with 3 group elements and 2 verification equations exists (and is the best construction published so far) in the Type II setting we investigate. They also considered the question of verification key size and their scheme requires 3 additional elements in addition to the description of the bilinear group. However, two of these group elements can be fixed in a common reference string together with the description of the bilinear group and may therefore be reused by structure-preserving signature schemes leaving only one variable group element in the verification key. It is an open question whether such a technique applies in the Type II setting.

2 Preliminaries

2.1 Bilinear groups

Let $\mathcal{G}$ be a bilinear group generator which, on input of the security parameter k, returns a bilinear group description $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi, G, H) \leftarrow \mathcal{G}(1^k)$ such that:

- $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are cyclic groups of order p, which is a k-bit prime;
- $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ is a homomorphism such that $\psi(H) = G$, hence $\psi(H^a) = G^a$ for all $a \in \mathbb{Z}$;
- H generates $\mathbb{G}_2$, G generates $\mathbb{G}_1$ and $e(G, H)$ generates $\mathbb{G}_T$;
- $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a bilinear map, i.e., $e(G^a, H^b) = e(G, H)^{ab}$ for all $a, b \in \mathbb{Z}$;
- There are efficient algorithms for computing group operations, evaluating the homomorphism ψ and the bilinear map e, comparing group elements and deciding membership of the groups.

Generic algorithms. In a bilinear group $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi, G, H)$ generated by $\mathcal{G}$ we refer to deciding group membership, computing group operations in $\mathbb{G}_1$, $\mathbb{G}_2$ or $\mathbb{G}_T$, comparing group elements and evaluating the homomorphism or the bilinear map as the generic bilinear group operations. The signature schemes we construct only use generic bilinear group operations.

As a matter of notation, we will use capital letters $G, H, M, R, S, T, U, V, W$ for group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$. We will use small letters $1, m, r, s, t, u, v, w$ for the corresponding discrete logarithms of group elements with respect to base G or H.

Type II pairings. Galbraith, Paterson and Smart [17] classify bilinear groups into three types according to the efficient morphisms that exist between the source groups $\mathbb{G}_1$ and $\mathbb{G}_2$. Type I pairings have $\mathbb{G}_1 = \mathbb{G}_2$ and $G = H$, i.e., ψ is the identity function (or equivalently, it is an efficiently computable and efficiently invertible isomorphism). Type II pairings have an efficiently computable isomorphism ψ from one source group to the other but none in the reverse direction. Type III pairings have no efficiently computable isomorphism from either source group to the other, i.e., in the definition given above ψ would not be efficiently computable. We will throughout this paper work in the Type II setting.

Type II pairings are usually constructed from the same type of pairing-friendly ordinary elliptic curves as Type III pairings; in contrast with Type III pairings, however, $\mathbb{G}_2$ is then chosen as some subgroup of order p in the p-torsion of

the curve other than the trace-zero subgroup (and the homomorphism ψ is then the trace map). As a result, there is no efficient way to hash to $\mathbb{G}_2$ in the Type II setting, but this is of course an irrelevant feature for structure-preserving cryptographic schemes since they only rely on the structure-preserving generic operations and avoid structure-destroying primitives such as cryptographic hash functions.

In terms of efficiency, Type II pairings compare quite favorably to Type I pairings (especially at higher security levels, and particularly now that low-characteristic pairings are known to be broken [23,9]), and are close to Type III pairings: in fact, a Type II pairing computation can be reduced to a Type III one at the cost of one multiplication in $\mathbb{G}_1$ [17, Note 10]. The size of the representation of elements in $\mathbb{G}_1$ is also the same in the Type II and Type III settings, and usually much smaller than in Type I pairings. However, Type II pairings do not support compression using twists for elements in $\mathbb{G}_2$, and hence their representation tends to be larger than in the Type III setting (by a factor of 1 to 6 depending on the embedding degree), and arithmetic in $\mathbb{G}_2$ is accordingly slower.

This has prompted suggestions, for example by Chatterjee and Menezes [14], that Type II pairings were "merely less efficient implementations of Type III pairings", and that cryptographic schemes designed in the Type II setting should adapt to the Type III setting at the cost of slightly different security proofs or assumptions. The present paper shows that this belief is incorrect, in the sense that certain Type II primitives (viz. structure-preserving signatures with a single verification equation) have no secure counterpart in the Type III setting.

2.2 Secure signature schemes

A digital signature scheme (with setup algorithm $\mathcal{P}$) is a quadruple of efficient algorithms $(\mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{V})$. The setup algorithm $\mathcal{P}$ takes the security parameter and outputs a public parameter PP.[4] The key generation algorithm $\mathcal{K}$ takes PP as input and returns a public verification key VK and a secret signing key SK. We will always assume that VK includes PP and that SK includes VK. The signing algorithm $\mathcal{S}$ takes a signing key SK and a message M in the message space $\mathcal{M}$ defined by PP and VK as input and returns a signature Σ. The verification algorithm $\mathcal{V}$ takes the verification key VK, a message M and the signature Σ and returns either 1 (accept) or 0 (reject).

Definition 1 (Correctness). *We say the signature scheme $(\mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ is correct if for all probabilistic polynomial time adversaries $\mathcal{A}$*

$$\Pr\left[\begin{array}{l} PP \leftarrow \mathcal{P}(1^k) \\ (VK, SK) \leftarrow \mathcal{K}(PP) \\ M \leftarrow \mathcal{A}(SK) \\ \Sigma \leftarrow \mathcal{S}_{SK}(M) \end{array} : M \in \mathcal{M} \ \wedge \ \mathcal{V}_{VK}(M, \Sigma) = 1\right] = 1 - \mathrm{negl}(k).$$

We say the signature scheme is perfectly correct if the probability is exactly 1.

All the signature schemes we construct will have perfect correctness. The lower bounds on the other hand will hold even for signature schemes that are only computationally correct as defined above.

A signature scheme is said to be existentially unforgeable if it is hard to forge a signature on a new message that has not been signed before. The adversary may see signatures on other messages before making the forgery. We distinguish between a random message attack (RMA), where the adversary gets pairs of random messages and corresponding signatures, and an adaptive chosen message attack (CMA) where the adversary can choose arbitrary messages and receive signatures on them. Our signature schemes will be existentially unforgeable against the strong adaptive chosen message attack, but our lower bounds on the complexity of signature schemes will hold even for the weaker random message attacks.

[4] Our signature schemes work over a bilinear group generated by $\mathcal{G}$. This group may be generated by the signer and included in the public verification key. In many cryptographic schemes it is convenient for the signer to work on top of a pre-existing bilinear group though. Indeed the idea behind structure-preserving cryptography is that many schemes using the same bilinear group can be composed in a modular way. In the description of our signatures, we will therefore explicitly distinguish between a setup algorithm $\mathcal{P}$ that produces a public parameter PP that includes the description of the bilinear group and a key generation algorithm the signer uses to generate her own keys.

Definition 2 (EUF-CMA). *A signature scheme $(\mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ is existentially unforgeable under adaptive chosen message attack if for all non-uniform polynomial time $\mathcal{A}$*

$$\Pr\left[\begin{array}{l} PP \leftarrow \mathcal{P}(1^k) \\ (VK, SK) \leftarrow \mathcal{K}(PP) \\ (M, \Sigma) \leftarrow \mathcal{A}^{\mathcal{S}_{SK}(\cdot)}(VK) \end{array} : M \notin Q \ \wedge \ \mathcal{V}_{VK}(M, \Sigma) = 1\right] = \mathrm{negl}(k),$$

where Q is the set of queries made by $\mathcal{A}$ to the signing oracle.

Sometimes it is also useful to prevent the adversary from issuing a new signature for a message that has already been signed. A signature scheme is strongly existentially unforgeable if it is hard to find a signature on a message that has not been signed before and also hard to find a new signature for a message that has already been signed. This notion, denoted by sEUF-CMA, is formally captured in the same way as the definition of EUF-CMA except for additionally requiring $(M, \Sigma) \notin Q$ where Q is the set of message-signature pairs from $\mathcal{A}$'s queries to the signing oracle.

We get the definition for existential unforgeability against random message attack (EUF-RMA) by modifying the signing oracle to picking $M \leftarrow \mathcal{M}$ at random, computing $\Sigma \leftarrow \mathcal{S}_{SK}(M)$ and returning (M, Σ) to the adversary whenever the signing oracle is queried.

Corresponding security notions for one-time signature schemes can be obtained by restricting the adversary to only calling the signing oracle once in the above definitions.

Randomizable signatures. In some applications it is desirable to have randomizable signatures, i.e., given a signature it is possible to randomize it such that it looks like a fresh signature on the message. The randomization is carried out by a randomization algorithm $\mathcal{R}$ that takes as input a verification key VK, a message M and a signature Σ and returns a randomized signature Σ.

Definition 3 (Randomizability). *A signature scheme $(\mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ is said to be (perfectly) randomizable if there exists a randomization algorithm $\mathcal{R}$ such that for all $k \in \mathbb{N}$ and all interactive adversaries $\mathcal{A}$*

$$\Pr\left[\begin{array}{l} PP \leftarrow \mathcal{P}(1^k) \\ (VK, SK) \leftarrow \mathcal{K}(PP) \\ (M, \Sigma) \leftarrow \mathcal{A}(SK) \\ \Sigma_0 \leftarrow \mathcal{S}_{SK}(M) \\ \Sigma_1 \leftarrow \mathcal{R}_{VK}(M, \Sigma) \\ b \leftarrow \{0, 1\} \end{array} : \mathcal{V}_{VK}(M, \Sigma) = 1 \ \wedge \ \mathcal{A}(\Sigma_b) = b\right] \leq \frac{1}{2}.$$

2.3 Structure-preserving signature schemes

We study structure-preserving signature schemes [3] on bilinear groups generated by group generator $\mathcal{G}$. In a structure preserving signature scheme the verification key, the messages and the signatures consist only of group elements from $\mathbb{G}_1$ and $\mathbb{G}_2$ and the verification algorithm evaluates the signature by deciding group membership of elements in the signature, using the homomorphism ψ and by evaluating pairing product equations, which are equations of the form

$$\prod_i \prod_j e(X_i, Y_j)^{a_{ij}} = 1,$$

where $X_1, X_2, \ldots \in \mathbb{G}_1, Y_1, Y_2, \ldots \in \mathbb{G}_2$ are group elements appearing in PP, VK, M and Σ and $a_{11}, a_{12}, \ldots \in \mathbb{Z}_p$ are constants stored in PP.[5] Structure-preserving signatures are extremely versatile because they mix well with other pairing-based protocols. Groth-Sahai proofs [21] are for instance designed with pairing product equations in mind and can therefore easily be applied to structure-preserving signatures.

[5] Our signature schemes all use small constants in $\mathbb{Z}$ that are independent of the specific bilinear group, so there are no a_{ij} values included in the public parameter. However, our lower bounds hold under the more relaxed definition where PP may include values $a_{ij} \in \mathbb{Z}_p$.

Definition 4 (Structure-preserving signatures). *A signature scheme $(\mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ is said to be structure preserving over bilinear group generator $\mathcal{G}$ if*

- *PP includes a bilinear group $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi, G, H)$ generated by $\mathcal{G}$, group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$, and constants in $\mathbb{Z}_p$,*
- *the verification key consists of PP and group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$,*
- *the messages consist of group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$,*
- *the signatures consist of group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$, and*
- *the verification algorithm only needs to decide membership in $\mathbb{G}_1$ and $\mathbb{G}_2$, use the homomorphism ψ, and evaluate pairing product equations.*

Generic signer. Abe et al. [3] did not explicitly require the signing algorithm to only use generic group operations when they defined structure-preserving signatures. However, all existing structure-preserving signatures in the literature have generic signing algorithms and we believe it would be a surprising result in itself to construct a structure-preserving signature with a non-generic signer. Our constructions have generic signer algorithms and some of our lower bounds will assume the signer is generic.

3 Randomizable Structure-Preserving Signatures

We will now show that in the Type II setting it is possible to construct an EUF-CMA secure structure-preserving signature scheme with a single verification equation. This is surprising since both in the symmetric Type I setting and the fully asymmetric Type III setting structure-preserving signature schemes require at least two verification equations [4,6].

The signature scheme is given in Fig. 1. It has a single verification equation and both signatures and verification keys consist of two group elements. This is optimal with respect to both verification complexity, signature size and verification key size as we demonstrate in Sect. 5.

As an additional benefit, the signature scheme is perfectly randomizable. We show a simple randomization algorithm that converts a signature in a new randomized signature that looks exactly like a fresh signature on the message. It is worth observing that while the natural formalization of randomizability gives both the message and the signature to the randomization algorithm our randomization algorithm does not need the message and simply ignores it and randomizes the signature directly. There may be applications where this is a feature.

Setup $\mathcal{P}(1^k)$**:** Return $PP = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi, G, H) \leftarrow \mathcal{G}(1^k)$.
Key generation $\mathcal{K}(PP)$**:** Choose $v, w \leftarrow \mathbb{Z}_p$ and compute the keys $VK = (PP, V, W)$ and $SK = (PP, v, w)$ as

$$V \leftarrow G^v \qquad W \leftarrow G^w.$$

Signing $\mathcal{S}_{SK}(M)$**:** On $M \in \mathbb{G}_2$ choose $r \leftarrow \mathbb{Z}_p$ and compute signature $\Sigma = (R, S)$ as

$$R \leftarrow H^r \qquad S \leftarrow M^v H^{r^2+w}.$$

Randomization $\mathcal{R}_{VK}(M, (R, S))$**:** Pick $\alpha \leftarrow \mathbb{Z}_p^*$ and compute the randomized signature $\Sigma' = (R', S')$ as

$$R' \leftarrow RH^\alpha \qquad S' \leftarrow SR^{2\alpha} H^{\alpha^2}.$$

Verification $\mathcal{V}_{VK}(M, (R, S))$**:** Accept if and only if $M, R, S \in \mathbb{G}_2$ and

$$e(G, S) = e(V, M)e(\psi(R), R)e(W, H).$$

Fig. 1. Randomizable structure-preserving signature scheme for messages in $\mathbb{G}_2$.

The signature scheme is designed with Groth-Sahai proofs in mind. If we randomize a signature, we may reveal the random group element R without this leaking any information about the message or the original signature from

which the randomized signature was derived. When R is public the verification equation become linear, which makes Groth-Sahai proofs very efficient.

It is easy to see that the signature scheme is perfectly correct. Randomized signatures are perfectly indistinguishable from real signatures since both types of signatures are uniquely determined by the uniformly random non-trivial group element R. We will now prove that the signature scheme is existentially unforgeable under adaptive chosen message attack.

Theorem 1. *The signature scheme in Fig. 1 is* EUF-CMA *secure in the generic bilinear group model.*

Proof. A generic adversary only uses generic group operations. This means that in $\mathbb{G}_1$ and $\mathbb{G}_2$ it can only compute linear combinations of group elements from the verification key and the signatures it has seen and use the map ψ to map elements from $\mathbb{G}_2$ to $\mathbb{G}_1$. Linear combinations on verification key elements and signature elements correspond to formal polynomials (of degree ranging from 0 to $q+1$ after q signature queries) in the discrete logarithms of the group elements. We will show that no linear combinations produce formal polynomials corresponding to a forgery. By the master theorem in [10] this means that the signature scheme is secure in the generic bilinear group model.

The group elements in VK are $G, V, W \in \mathbb{G}_1$ and $H \in \mathbb{G}_2$ with corresponding discrete logarithms $1, v, w$ and 1. On a query M_i with discrete logarithm m_i from the adversary, the signature oracle responds with a signature (R_i, S_i) with discrete logarithms

$$r_i \leftarrow \mathbb{Z}_p^* \qquad s_i = vm_i + r_i^2 + w.$$

Suppose the adversary after q queries constructs $(M, (R, S))$ in $\mathbb{G}_2$. Since the adversary is generic it can only construct them in $\mathbb{G}_2$ such that the discrete logarithms m, r, s are linear combinations of $1, r_1, s_1, \ldots, r_q, s_q$, i.e.,

$$\begin{aligned}
m =& \mu + \sum_{i=1}^{q} \mu_{r_i} r_i + \sum_{i=1}^{q} \mu_{s_i}(vm_i + r_i^2 + w) \\
r =& \rho + \sum_{i=1}^{q} \rho_{r_i} r_i + \sum_{i=1}^{q} \rho_{s_i}(vm_i + r_i^2 + w) \\
s =& \sigma + \sum_{i=1}^{q} \sigma_{r_i} r_i + \sum_{i=1}^{q} \sigma_{s_i}(vm_i + r_i^2 + w)
\end{aligned}$$

Similarly, the discrete logarithm m_i of a signing query is a linear combination of $1, r_1, s_1, \ldots, r_{i-1}, s_{i-1}$.

We will show that the signature scheme is EUF-CMA secure, i.e., an adversary cannot construct a valid signature (R, S) on M where the discrete logarithms m, r, s satisfy the verification equation

$$s = vm + r^2 + w$$

unless it reuses $M = M_j$ from a previous query.

We can write $s = vm + r^2 + w$ as

$$\begin{aligned}
&\sigma + \sum_{i=1}^{q} \sigma_{r_i} r_i + \sum_{i=1}^{q} \sigma_{s_i}(vm_i + r_i^2 + w) - v\left(\mu + \sum_{i=1}^{q} \mu_{r_i} r_i + \sum_{i=1}^{q} \mu_{s_i}(vm_i + r_i^2 + w)\right) \\
&= \left(\rho + \sum_{i=1}^{q} \rho_{r_i} r_i + \sum_{i=1}^{q} \rho_{s_i}(vm_i + r_i^2 + w)\right)^2 + w.
\end{aligned}$$

We first look at the terms r_i^4. Observe that all elements $m, r, s, m_1, \ldots, m_q$ constructed using generic bilinear group operations in $\mathbb{G}_2$, i.e., linear combinations of the discrete logarithms, can only have degree $0, 1$ or 2 in r_i. This shows that each term r_i^4 has coefficient 0 in $s - vm$. On the other side of the verification equation each term r_i^4 has coefficient $\rho_{s_i}^2$. Therefore $\rho_{s_i} = 0$ for all $i = 1, \ldots, q$.

In $s - vm$ the coefficients of all combinations $r_i r_j$ are 0 for $i \neq j$. On the other side of the verification equation in the product r^2 they have coefficients $\rho_{r_i}\rho_{r_j}$. This means for all $i \neq j$ we have $\rho_{r_i}\rho_{r_j} = 0$ and therefore there can be at most one $\rho_{r_j} \neq 0$. We now have $r = \rho + \rho_{r_j} r_j$ giving us that $s = vm + r^2 + w$ can be written as

$$\begin{aligned}&\sigma + \sum_{i=1}^{q} \sigma_{r_i} r_i + \sum_{i=1}^{q} \sigma_{s_i}(vm_i + r_i^2 + w)\\ =&v\left(\mu + \sum_{i=1}^{q} \mu_{r_i} r_i + \sum_{i=1}^{q} \mu_{s_i}(vm_i + r_i^2 + w)\right) + \left(\rho + \rho_{r_j} r_j\right)^2 + w\end{aligned}$$

for some $j \in \{1, \ldots, q\}$.

Comparing the coefficients of r_i^2 from the two sides of the verification equation we get $\sigma_{s_j} = \rho_{r_j}^2$ and $\sigma_{s_i} = 0$ for $i \neq j$. The coefficients of w on the two sides of the verification equation gives us $\sigma_{s_j} = 1$. Then the verification equation is described as

$$\begin{aligned}&v\, m_j + r_j^2 + \sigma + \sum_{i=1}^{q} \sigma_{r_i} r_i + w\\ =&v\left(\mu + \sum_{i=1}^{q} \mu_{r_i} r_i + \sum_{i=1}^{q} \mu_{s_i}(vm_i + r_i^2 + w)\right) + \left(\rho + \rho_{r_j} r_j\right)^2 + w\end{aligned}$$

for some $j \in \{1, \ldots, q\}$.

Looking at coefficient of terms that involve v we then get $vm_j = vm$, which shows us $m = m_j$ and therefore $M = M_j$. □

In some cases it is desirable to sign many group elements at once. The signature scheme we presented can easily be modified to sign n group elements at once by changing the verification equation to:

$$e(G, S) = \prod_{i=1}^{n} e(V_i, M_i) e(\psi(R), R) e(W, H)$$

and modifying the key generation and signing processes accordingly. The security proof for the generalized scheme is virtually the same as the proof for Theorem 1.

4 Strongly Unforgeable Structure-Preserving Signatures

For some applications it is desirable to use a strongly existentially unforgeable signature scheme. It is in general harder to get strong unforgeability because now also the signatures have to be immutable, but we will now present a construction that preserves optimality with respect to verification complexity, signature size and verification key size.

Fig. 2 gives a structure-preserving signature scheme with a single verification equation, 2 element verification keys and 2 element signatures. It is easy to see that it is perfectly correct. Signature verification requires only two pairing evaluations (not counting the constant factor $e(G, H)$), which makes this scheme the most efficient structure preserving signature so far in terms of verification complexity (faster than all previous Type I and Type III constructions by a significant margin). We will now prove that it is strongly existentially unforgeable under adaptive chosen message attack.

Theorem 2. *The signature scheme in Fig. 2 is* sEUF-CMA *secure in the generic bilinear group model.*

Proof. A generic adversary only uses generic group operations. This means that in $\mathbb{G}_1$ and $\mathbb{G}_2$ it can only compute linear combinations of group elements from the verification key and the signatures it has seen and use the map ψ to map elements from $\mathbb{G}_2$ to $\mathbb{G}_1$. Linear combinations on verification key elements and signature elements in $\mathbb{G}_2$ correspond to formal Laurent polynomials (of degree ranging from $-q$ to $q + 1$ after q signature queries) in the discrete logarithms of

Setup $\mathcal{P}(1^k)$**:** Return $PP = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi, G, H) \leftarrow \mathcal{G}(1^k)$.
Key generation $\mathcal{K}(PP)$**:** Choose $v, w \leftarrow \mathbb{Z}_p$ and compute $VK = (PP, V, W)$ and $SK = (PP, v, w)$ using

$$V \leftarrow G^v \qquad W \leftarrow G^w.$$

Signing $\mathcal{S}_{SK}(M)$**:** On $M \in \mathbb{G}_2$ choose $t \leftarrow \mathbb{Z}_p^*$ and compute signature $\Sigma = (R, S)$ as

$$R \leftarrow H^{t-w} \qquad S \leftarrow M^{\frac{v}{t}} H^{\frac{1}{t}}.$$

Verification $\mathcal{V}_{VK}(M, (R, S))$**:** Accept if and only if $M, R, S \in \mathbb{G}_2$ and

$$e(W\psi(R), S) = e(V, M)e(G, H).$$

Fig. 2. Strong structure-preserving signature scheme for messages in $\mathbb{G}_2$.

the group elements. We will show that no linear combinations produce formal Laurent polynomials corresponding to a forgery. By the master theorem in [10] this means that the signature scheme is secure in the generic bilinear group model.

The group elements in VK are $G, V, W \in \mathbb{G}_1$ and $H \in \mathbb{G}_2$ with corresponding discrete logarithms $1, v, w$ and 1. On a query M_i with discrete logarithm m_i from the adversary, the signature oracle responds with a signature (R_i, S_i) with discrete logarithms

$$t_i \leftarrow \mathbb{Z}_p^* \qquad r_i = t_i - w \qquad s_i = \frac{vm_i}{t_i} + \frac{1}{t_i}.$$

Suppose the adversary after q queries constructs $(M, (R, S))$ in $\mathbb{G}_2$. Since the adversary is generic it can only construct them in $\mathbb{G}_2$ such that the discrete logarithms m, r, s are linear combinations of $1, r_1, s_1, \ldots, r_q, s_q$, i.e.,

$$\begin{aligned}
m =& \mu + \sum_{i=1}^{q} \mu_{r_i}(t_i - w) + \sum_{i=1}^{q} \mu_{s_i}(\frac{vm_i}{t_i} + \frac{1}{t_i}) \\
r =& \rho + \sum_{i=1}^{q} \rho_{r_i}(t_i - w) + \sum_{i=1}^{q} \rho_{s_i}(\frac{vm_i}{t_i} + \frac{1}{t_i}) \\
s =& \sigma + \sum_{i=1}^{q} \sigma_{r_i}(t_i - w) + \sum_{i=1}^{q} \sigma_{s_i}(\frac{vm_i}{t_i} + \frac{1}{t_i})
\end{aligned}$$

Similarly, each signing query m_i is a linear combination of $1, r_1, s_1, \ldots, r_{i-1}, s_{i-1}$.

We will show that the signature scheme is sEUF-CMA secure, i.e., an adversary cannot construct a valid signature (R, S) on M where the discrete logarithms r, s, m satisfy the verification equation

$$(w + r)s = vm + 1$$

unless it reuses $M = M_j$ and $(R, S) = (R_j, S_j)$ from a previous query.

We can write $(w + r)s = vm + 1$ as

$$\left(w + \rho + \sum_{i=1}^{q} \rho_{r_i}(t_i - w) + \sum_{i=1}^{q} \rho_{s_i}(\frac{vm_i}{t_i} + \frac{1}{t_i})\right)\left(\sigma + \sum_{i=1}^{q} \sigma_{r_i}(t_i - w) + \sum_{i=1}^{q} \sigma_{s_i}(\frac{vm_i}{t_i} + \frac{1}{t_i})\right) = vm + 1.$$

Let us first show $\sigma_{r_i} = 0$ for all $i = 1, \ldots, q$. Suppose that $\sigma_{r_j} \neq 0$ for some j. The coefficient of t_j^2 then tells us $\rho_{r_j}\sigma_{r_j} = 0$ and therefore $\rho_{r_j} = 0$. Similarly, the coefficients of $t_i t_j$ tell us $\rho_{r_i}\sigma_{r_j} = 0$ and therefore $\rho_{r_i} = 0$ for all $i \neq j$ too. Since all $\rho_{r_i} = 0$ we then get from the coefficient of wt_j that $\sigma_{r_j} = 0$, which is a contradiction. Therefore we conclude that $\sigma_{r_i} = 0$ for all $i = 1, \ldots, q$.

Next, let us show $\sigma = 0$. Assume for contradiction $\sigma \neq 0$. Then the coefficients of t_i give us $\rho_{r_i} = 0$ for all $i = 1, \ldots, q$. The coefficient of w then gives us $\sigma = 0$, which yields a contradiction. We conclude $\sigma = 0$.

The coefficient of 1 now shows that there must be at least one $\sigma_{s_j} \neq 0$, since otherwise $s = 0$ and the verification equation cannot be satisfied. The coefficients of $\frac{1}{t_j^2}$ now tells us that $\rho_{s_j} = 0$. Next, the coefficients of $\frac{1}{t_i t_j}$ tell us that $\rho_{s_i} = 0$ for all $i \neq j$ as well.

Looking at the coefficients of $\frac{t_i}{t_j}$ we now get $\rho_{r_i} = 0$ for all $i \neq j$. The coefficients of $\frac{w}{t_j}$ then give us $\rho_{r_j} = 1$. The coefficients of $\frac{t_j}{t_i}$ then give us $\sigma_{s_i} = 0$ for $i \neq j$ and the coefficient 1 gives us $\sigma_{s_j} = 1$.

Combining all the information we have deduced about coefficients in s we conclude $s = s_j$. The coefficients of $\frac{1}{t_j}$ tell us $\rho = 0$ and therefore $r = r_j$. The verification equation $(w + r)s = (w + r_j)s_j = vm_j + 1 = vm + 1$ then gives us $m = m_j$. We have therefore shown that $M = M_j$ and $(R, S) = (R_j, S_j)$. □

5 Lower Bounds in the Type II Setting

We will now establish lower bounds for the complexity of structure-preserving signature schemes in the Type II setting. Unlike the Type I and the Type III settings where two verification equation are needed we have already seen in Sections 3 and 4 that it is possible to use only one verification equation in the Type II setting. However, these signature schemes only work for messages in $\mathbb{G}_2$. We start by showing this is necessarily so, a structure-preserving signature scheme for messages in $\mathbb{G}_1$ cannot have a single verification equation.

Theorem 3. *A structure-preserving signature scheme for messages in $\mathbb{G}_1$ must have at least two verification equations. This holds even for one-time signatures with security against random message attack.*

Proof. Suppose we have a structure-preserving signature scheme with a single verification equation for messages in $\mathbb{G}_1$. We will construct a one-time random message attack on the scheme. The attacker queries the signing oracle and get a signature on a random message $M \in \mathbb{G}_1$. Let S be a group element in the signature that appears non-trivially in the verification equation.

If $S \in \mathbb{G}_1$ we can write the verification equation as $e(M, X) = e(S, Y)Z$ where X, Y, Z are expression that do not include any M or S terms. We now have $e(M\psi(Y), X) = e(S\psi(X), Y)Z$, which means replacing the group element S with $S^* = S\psi(X)$ in the signature gives us a forgery on $M^* = M\psi(Y)$.

If $S \in \mathbb{G}_2$ we can write the verification equation as $e(M, S^a X) \cdot e(\psi(S)^b Y, S) = Z$ for some $a, b \in \mathbb{Z}_p$ and expressions X, Y, Z that do not have any M or S terms. Pick $r \leftarrow\in \mathbb{Z}_p^*$ and define $\Delta = (S^a X)^{\frac{1}{r}}$. Replace S with $S^* = S\Delta$ to get a signature on $M^* = M(M^a \psi(\Delta)^b Y \psi(S)^{2b})^{-\frac{1}{a+r}}$. For the signature to be non-trivial in M we must have $S^a X \neq 1$ with overwhelming probability, giving us that Δ is uniformly random in $\mathbb{G}_1^*$ and, therefore, that $M^* \neq M$ with high probability, so we do obtain a forgery. □

With Theorem 3 in mind, we will in the rest of this section only consider structure-preserving signatures on $M \in \mathbb{G}_2$. We will now show our main result in this section, which is that the verification key must have at least two group elements. The following theorem follows as a corollary to Lemmata 1, 2 and 3.

Theorem 4. *A structure-preserving signature scheme with a single verification equation and a generic signer must have at least two group elements in the verification key. This holds even for one-time signatures secure under random message attack.*

Lemma 1. *A structure-preserving signature for $M \in \mathbb{G}_2$ with a single verification equation cannot have a non-redundant signature element $S \in \mathbb{G}_1$. This holds even for one-time signatures with security under random message attack.*

Proof. We will construct an one-time random message attack similar to the one for the proof of Theorem 3 with the roles of M and S reversed. The attacker queries the signing oracle and gets a signature on a random message $M \in \mathbb{G}_2$. Let $S \in \mathbb{G}_1$ be an element in the signature that appears non-trivially in the verification equation, i.e., it does not have negligible probability of being paired with 1.

We can write the verification equation as $e(S, M^a X) \cdot e(\psi(M)^b Y, M) = Z$ for some $a, b \in \mathbb{Z}_p$ and expressions X, Y, Z that do not have any M or S terms. Pick $r \leftarrow \mathbb{Z}_p^*$ and define $\Delta = (M^a X)^{\frac{1}{r}}$. Replace S in the signature with

$S^* = S(S^a\psi(\Delta)^b Y\psi(M)^{2b})^{-\frac{1}{a+r}}$ to get a signature on $M^* = M\Delta$. For the signature scheme to be non-redundant in S the probability of $M^a X \neq 1$ has to be non-negligible and in that case Δ is uniformly random in $\mathbb{G}_1^*$, giving us $M^* \neq M$ so that we do obtain a forgery. □

Lemma 2. *There is no structure-preserving signature for $M \in \mathbb{G}_2$ with a single verification equation and a key consisting of a single group element $V \in \mathbb{G}_2$. This holds even for one-time signatures with security under random message attack.*

Proof. From Lemma 1 we can without loss of generality consider only signature schemes where all signature elements belong to $\mathbb{G}_2$. A group element $S \in \mathbb{G}_2$ from the signature appears as $e(\psi(S), S^a X)$ in the verification equation, where X is an expression that does not contain an S-term. If $a \neq 0$ we can substitute S with $S' = SX^{\frac{1}{2a}}$ to get the simpler term $e(\psi(S'), S')^a$ in the verification equation. Moreover, if $a = 0$ but X involves another signature element T^b for $b \neq 0$ we can by substituting T with $T' = TS^{-1}$ get a term $e(\psi(S), S^{a'})$ with $a' = b \neq 0$. Using these two diagonalization techniques we can without loss of generality write the single verification equation for the structure-preserving signature $(S_1, \ldots, S_n) \in \mathbb{G}_2^n$ on $M \in \mathbb{G}_2$ as

$$e(\psi(M), M^a X) \prod_{i \in I} e(\psi(S_i), M^{b_i} Y_i) \cdot \prod_{j \in J} e(\psi(S_j), S_j)^{c_j} = Z,$$

where I, J are disjoint subsets of $\{1, \ldots, n\}$, $b_i \neq 0, Y_i \neq 1$ or both for each $i \in I$, $c_j \neq 0$ for each $j \in J$, and X, Y_i and Z are expressions that only involve constant terms and the verification key.

The adversary starts by getting a signature $(S_1, \ldots, S_n)$ on a random message M. If $I \neq \emptyset$ we can use the method from the proof of Lemma 1 to modify S_i into S_i^* giving a forgery on $M^* \neq M$. If $I = \emptyset$ and $a = 0$ we can use the method from the proof of Theorem 3 to obtain a forgery on a message $M^* \neq M$.

The remaining case is when $I = \emptyset$ and $a \neq 0$, i.e., the verification equation is

$$e(\psi(M), M^a X) \cdot \prod_{j \in J} e(\psi(S_j), S_j)^{c_j} = Z,$$

with $a \neq 0$ and each $c_j \neq 0$. But in this case the equation can be seen as a quadratic equation in M with two solutions. The signature on M is also a signature on $M^* = M^{-1}X^{-\frac{1}{a}}$. This gives us an existential forgery unless $M^* = M$, which only happens in the unlikely event that $X = M^{-2a}$. □

Lemma 3. *There is no structure-preserving signature for $M \in \mathbb{G}_2$ with a single verification equation, a generic signer and a verification key consisting of a single group element $V \in \mathbb{G}_1$. This holds even for one-time signatures with security under random message attack.*

Proof. As in the proof of Theorem 2 we can rewrite the verification equation as

$$e(\psi(M), M^a H^x) \cdot \prod_{i \in I} e(\psi(S_i), M^{b_i} H^{y_i}) \cdot \prod_{j \in J} e(\psi(S_j), S_j)^{c_j} \cdot e(V, M^d \prod_{k=1}^{n} S_k^{e_k} H^f) = e(G, H)^z,$$

where I, J are disjoint subsets of $\{1, \ldots, n\}$, $x, y_i, z \in \mathbb{Z}_p$ are constant terms, $b_i \neq 0, Y_i \neq 1$ or $e_i \neq 0$ for each $i \in I$, and $c_j \neq 0$ for each $j \in J$. We will consider three cases: all $e_k = 0$ and $d = 0$ but $f \neq 0$, all $e_k = 0$ but $d \neq 0$, and without loss of generality $e_1 \neq 0$.

In the first case $d = 0$ and all $e_k = 0$ but without loss of generality $f = 1$. The adversary makes a one-time random message attack to get a signature $(S_1, \ldots, S_n)$ on a random message M. We can now make an analysis similar to the proof of Lemma 2 to create an existential forgery on a message $M^* \neq M$.

In the second case all $e_k = 0$ but $d \neq 0$. The adversary picks $M = H^{-\frac{f}{d}}$ such that the $e(V, *)$ part cancels out. If there is an $i \in I$ such that $M^{b_i} H^{y_i} = H^{-b_i \frac{f}{d} + y_i} \neq 1$, we can pick all other signature elements $S_k = 1$ for $k \neq i$ and since we know all the discrete logarithm solve for the discrete logarithm s_i of S_i to get a signature on $M = H^{\frac{f}{d}}$. Else if there is no such $i \in I$, then we have an equation in the discrete logarithms of the signature such that

$m(am+x)+\sum_{j\in J} c_j s_j^2 = z$ with $m = -\frac{d}{f}$. By the completeness of the signature scheme, this equation is solvable in the unknowns s_j and can be efficiently solved [26], which gives us a signature on M.

Finally, in the third case without loss of generality $e_1 \neq 0$. We can substitute S_1 with $(M^d \prod_{k=1}^{n} S_k^{e_k} H^f)^{-\frac{1}{e_1}}$ to get a structure-preserving signature scheme with a verification equation of the form

$$\begin{aligned} &e(\psi(M), M^a H^x) \cdot \prod_{i\in I\setminus\{1\}} e(\psi(S_i), M^{b_i} H^{y_i}) \cdot \prod_{j\in J\setminus\{1\}} e(\psi(S_j), S_j)^{c_j} \\ =&e(VG^\gamma \psi(M)^\mu \prod_{k\in I\cup J} \psi(S_k)^{\sigma_k}, S_1) \cdot e(G,H)^z, \end{aligned}$$

for some $\mu, \sigma_k \in \mathbb{Z}_p$ and with suitable modifications of a, x, b_i, y_i and z.

Our strategy now is to pick $S_1 = 1$ to eliminate the effect of the verification key V. If there is a $b_i \neq 0$ or $y_i \neq 0$, we can pick $m \leftarrow \mathbb{Z}_p$ at random and set $S_k = 1$ for $k \neq i$ and $S_i = H^{\frac{z-m(am+x)}{b_i m+y}}$ to get a signature on $M = H^m$.

If all $b_i = y_i = 0$ but there is some $j \in J \setminus \{1\}$ where $c_j \neq 0$ we instead set $S_k = 1$ for $k \neq j$ and solve the bivariate quadratic $m(am+x)+c_j s_j^2 = z$ in $\mathbb{Z}_p[m, s_j]$, which can be done efficiently [26] unless $a = x = 0$ and c_j and $z \neq 0$ have different quadratic residuosity. However, if $a = x = 0$ the adversary can use a one-time random message to get a signature on M. The adversary picks $r \leftarrow \mathbb{Z}_p^*$ and replaces S_j with $S_j^* = S_j S_k^r$ to get a signature on $M^* = M S_j^{-2c_j r} S_k^{-\sigma_j - c_j r^2}$. For the verification equation to be non-trivial in M, with overwhelming probability $S_k \neq 1$ and therefore $M^* \neq M$ so we have an existential forgery.

The remaining case is when both all $b_i = y_i = 0$ and all $c_j = 0$, i.e., the verification equation is

$$e(\psi(M), M^a H^x) = e(VG^\gamma \psi(M)^\mu \prod_{k\in I\cup J} \psi(S_k)^{\sigma_k}, S_1) \cdot e(G,H)^z.$$

If $z = 0$ we immediately get a signature $(1, \ldots, 1)$ on the message $M = 1$, so let us from now on consider the case where $z \neq 0$.

If there is a $\sigma_k \neq 0$ for $k \neq 1$ then we can substitute S_k with $G^\gamma M^\mu \prod_{\ell\in(I\cup J)} S_\ell^{\sigma_\ell}$ to get verification equation $e(\psi(M), M^a H^x) = e(VS_k, S_1) \cdot e(G,H)^z$. The adversary gets a signature on a random message M and replaces S_k with $S_k^* = S_k M^{2a} S_1^a H^x$ to get a signature on $M^* = M S_1$. With overwhelming probability $S_1 \neq 1$, since otherwise the signature would not affect any part of the equation, giving us $M^* \neq M$.

Finally, let us consider the case where we only have a single signature element S_1 that is used in a non-trivial way, i.e., the verification equation is $e(\psi(M), M^a H^x S_1^{-\mu}) = e(VG^\gamma \psi(S_1)^{\sigma_1}, S_1) \cdot e(G,H)^z$. If $a \neq 0$ the attacker can use a one-time random message attack to get a signature on a random message M, which is also a signature on $M^* = M^{-1}(H^x S_1^{-\mu})^{-\frac{1}{a}}$. We have $M^* \neq M$ unless $S_1^\mu = M^{2a} H^x$ but since a and x are known to the adversary this would mean the adversary could forge signatures on arbitrary messages. If $a = 0$ and $x \neq 0$ we can pick $S_1 = 1$ to give us a signature on $M = H^{\frac{z}{x}}$. Finally, if $a = 0$ and $x = 0$ we cannot sign the message using a generic signer. A generic signer computes $S_1 = M^\alpha H^\beta$ using known $\alpha, \beta \in \mathbb{Z}_p$ and is unlikely over the choice of the unknown discrete logarithm of M to solve the equality $-\mu(\alpha m + \beta) = (v + \gamma + \alpha m + \beta)(\alpha m + \beta) + z$ unless it is possible to use $\alpha = 0$, in which case the signature is independent of M and therefore either invalid or valid for every message. □

We have now established a lower bound of 2 group elements in the verification key for structure-preserving signatures with a single verification equation and that this lower bound even holds for one-time random message attacks. In Appendix A we give a structure-preserving one-time signature where the signature is a single group element, so such a lower bound does not hold for the signature size. However, if the adversary is allowed to obtain multiple signatures on random messages we can establish a lower bound of 2 group elements for the signatures.

Theorem 5. *A structure-preserving signature scheme with a generic signer that is existentially unforgeable against random message attacks must have at least 2 group elements for messages in $\mathbb{G}_2$ and at least 3 group elements for messages in $\mathbb{G}_1$.*

Proof. Suppose that we have a structure-preserving signature scheme with just one group element in the signature and a single verification equation. The verification equation can for any given message be seen as a quadratic or linear

equation in the discrete logarithm of the signature, so there are at most two potential signatures on the message. We conclude from Lemma 4 below that a structure-preserving signature with a single verification equation must consist of at least two group elements.

If there is more than one verification equation we now have two linear or quadratic equations in the signature elements. For messages in $\mathbb{G}_1$ we know by Theorem 3 that at least two verification equations are needed. Both equations must place non-trivial constraints on the signature or else we could reduce to a single verification equation. Again by Lemma 4, we therefore get that for messages in $\mathbb{G}_1$ at least 3 signature elements are needed, since with one or two group elements in the signature there would be at most 4 possible signatures satisfying the verification equations. □

Lemma 4. *A structure-preserving signature scheme with a generic signer that is existentially unforgeable against random message attacks must for each message have a superpolynomial number of potential signatures.*

Proof. Suppose that for a message $M \in \mathbb{G}_2$ there are only a polynomial number of signatures $\Sigma = (R_1, \ldots, R_m, S_1, \ldots, S_n) \in \mathbb{G}_1^m \times \mathbb{G}_2^n$. Since the signer is generic this means there is a set $\{(\vec{\alpha}, \vec{\beta}, \vec{\gamma}, \vec{\delta})\}_{i=1}^{\mathrm{poly}(k)}$ of vectors in $(\mathbb{Z}_p^m)^2 \times (\mathbb{Z}_p^n)^2$ creating signature vectors $\Sigma = (\psi(M)^{\vec{\alpha}} G^{\vec{\beta}}, M^{\vec{\gamma}} H^{\vec{\delta}})$ by entry-wise exponentiation. Given signatures Σ_0 and Σ_1 on random messages M_0 and M_1 we have $\frac{1}{\mathrm{poly}(k)^2}$ probability that they are constructed with the same $(\vec{\alpha}, \vec{\beta}, \vec{\gamma}, \vec{\delta})$ pair. In that case

$$\Sigma^* = \Sigma_0^r \Sigma_1^{1-r} = (\psi(M_0^r M_1^{1-r})^{\vec{\alpha}} G^{\vec{\beta}}, (M_0^r M_1^{1-r})^{\vec{\gamma}} H^{\vec{\delta}}$$

is a signature on $M^* = M_0^r M_1^{1-r}$ for all $r \in \mathbb{Z}_p$. A similar proof applies to the case where $M \in \mathbb{G}_1$. □

References

1. M. Abe, M. Chase, B. David, M. Kohlweiss, R. Nishimaki, and M. Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In X. Wang and K. Sako, editors, *ASIACRYPT*, volume 7658 of *LNCS*, pages 4–24, 2012.
2. M. Abe, B. David, M. Kohlweiss, R. Nishimaki, and M. Ohkubo. Tagged one-time signatures: Tight security and optimal tag size. In K. Kurosawa and G. Hanaoka, editors, *PKC*, volume 7778 of *LNCS*, pages 312–331. Springer, 2013.
3. M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-preserving signatures and commitments to group elements. In T. Rabin, editor, *CRYPTO*, volume 6223 of *LNCS*, pages 209–236. Springer, 2010.
4. M. Abe, J. Groth, K. Haralambiev, and M. Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In P. Rogaway, editor, *CRYPTO*, volume 6841 of *LNCS*, pages 649–666. Springer, 2011.
5. M. Abe, J. Groth, and M. Ohkubo. Separating short structure-preserving signatures from non-interactive assumptions. In D. H. Lee and X. Wang, editors, *ASIACRYPT*, volume 7073 of *LNCS*, pages 628–646, 2011.
6. M. Abe, J. Groth, M. Ohkubo, and M. Tibouchi. Unified, minimal and selectively randomizable structure-preserving signatures. In Y. Lindell, editor, *TCC*, volume 8349 of *LNCS*, pages 688–712. Springer, 2014.
7. N. Attrapadung, B. Libert, and T. Peters. Computing on authenticated data: New privacy definitions and constructions. In X. Wang and K. Sako, editors, *ASIACRYPT*, volume 7658 of *LNCS*, pages 367–385. Springer, 2012.
8. N. Attrapadung, B. Libert, and T. Peters. Efficient completely context-hiding quotable and linearly homomorphic signatures. In K. Kurosawa and G. Hanaoka, editors, *PKC*, volume 7778 of *LNCS*, pages 386–404. Springer, 2013.
9. R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT*, LNCS. Springer, 2014.
10. D. Boneh and X. Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. *J. Cryptology*, 21(2):149–177, 2008.
11. J. Camenisch, M. Dubovitskaya, R. R. Enderlein, and G. Neven. Oblivious transfer with hidden access control from attribute-based encryption. In I. Visconti and R. D. Prisco, editors, *SCN*, volume 7485 of *LNCS*, pages 559–579. Springer, 2012.
12. J. Cathalo, B. Libert, and M. Yung. Group encryption: Non-interactive realization in the standard model. In M. Matsui, editor, *ASIACRYPT*, volume 5912 of *LNCS*, pages 179–196, 2009.
13. M. Chase, M. Kohlweiss, A. Lysyanskaya, and S. Meiklejohn. Malleable proof systems and applications. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT*, volume 7237 of *LNCS*, pages 281–300. Springer, 2012.
14. S. Chatterjee and A. Menezes. On cryptographic protocols employing asymmetric pairings — The role of Ψ revisited. *Discrete Applied Mathematics*, 159(13):1311–1322, 2011.

15. G. Fuchsbauer. Commuting signatures and verifiable encryption. In K. G. Paterson, editor, *EUROCRYPT*, volume 6632 of *LNCS*, pages 224–245. Springer, 2011.
16. G. Fuchsbauer and D. Vergnaud. Fair blind signatures without random oracles. In D. J. Bernstein and T. Lange, editors, *AFRICACRYPT*, volume 6055 of *LNCS*, pages 16–33. Springer, 2010.
17. S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–3121, 2008.
18. E. Ghadafi, N. P. Smart, and B. Warinschi. Groth-Sahai proofs revisited. In *Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 177–192, 2010.
19. M. Green and S. Hohenberger. Universally composable adaptive oblivious transfer. In J. Pieprzyk, editor, *ASIACRYPT*, volume 5350 of *LNCS*, pages 179–197. Springer, 2008.
20. J. Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In X. Lai and K. Chen, editors, *ASIACRYPT*, volume 4284 of *LNCS*, pages 444–459, 2006.
21. J. Groth and A. Sahai. Efficient noninteractive proof systems for bilinear groups. *SIAM J. Comput.*, 41(5):1193–1232, 2012.
22. D. Hofheinz and T. Jager. Tightly secure signatures and public-key encryption. In *CRYPTO*, volume 7417 of *LNCS*, pages 590–607. Springer, 2012.
23. A. Joux. A new index calculus algorithm with complexity $L(1/4 + o(1))$ in very small characteristic. IACR ePrint Archive, Report 2013/095, 2013. http://eprint.iacr.org/.
24. B. Libert, T. Peters, M. Joye, and M. Yung. Linearly homomorphic structure-preserving signatures and their applications. In R. Canetti and J. Garay, editors, *CRYPTO*, LNCS. Springer, 2013.
25. B. Libert, T. Peters, and M. Yung. Group signatures with almost-for-free revocation. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO*, volume 7417 of *LNCS*, pages 571–589. Springer, 2012.
26. C. E. van de Woestijne. *Deterministic equation solving over finite fields*. PhD thesis, Leiden University, 2006.
27. J. Zhang, Z. Li, and H. Guo. Anonymous transferable conditional e-cash. In A. D. Keromytis and R. D. Pietro, editors, *SecureComm*, volume 106 of *LNICST*, pages 45–60. Springer, 2012.

A Structure-Preserving One-Time Signatures

We have seen in Sect. 5 that a secure structure-preserving signature scheme in the Type II setting must have signatures consisting of at least two group elements. The proof does not extend to one-time signatures, however. Indeed, Fig. 3 describes a one-time signature scheme with only one signature element, a single verification equation and two public key elements, which we now show is sEUF-CMA secure in the generic group model. This very compact one-time signature scheme is clearly optimal in terms of signature size and number of verification equations, and also in terms of verification key size in view of Theorem 4.

Setup $\mathcal{P}(1^k)$**:** Return $PP = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi, G, H) \leftarrow \mathcal{G}(1^k)$.
Key generation $\mathcal{K}(PP)$**:** Choose $v, w \leftarrow \mathbb{Z}_p$ and compute $VK = (PP, V, W)$ and $SK = (PP, v, w)$ using

$$V \leftarrow G^v \qquad W \leftarrow G^w.$$

Signing $\mathcal{S}_{SK}(M)$**:** On $M \in \mathbb{G}_2$ choose $t \leftarrow \mathbb{Z}_p^*$ and compute signature $S \in \mathbb{G}_2$ as

$$S \leftarrow M^v H^w.$$

Verification $\mathcal{V}_{VK}(M, S)$**:** Accept if and only if $M, S \in \mathbb{G}_2$ and

$$e(G, S) = e(V, M)e(W, H).$$

Fig. 3. Optimal strong structure-preserving one-time signature scheme for messages in $\mathbb{G}_2$.

Theorem 6. *The scheme given in Fig. 3 is an* sEUF-CMA *secure one-time signature scheme in the generic group model.*

Proof. A generic adversary can only compute linear combinations of group elements in the base groups, which means its signing query must be $M = H^m$ with known discrete logarithms m. The generic adversary gets a signature $S = H^{vm+w}$ in response.

Suppose now the generic adversary computes a message $M^* = H^{m^*}$ and a valid signature $S^* = H^{s^*}$. Since the adversary only uses linear combinations of existing group elements it knows $\mu, \mu_s, \sigma, \sigma_s \in \mathbb{Z}_p$ such that

$$\begin{aligned} m^* &= \mu + \mu_s(vm + w) \\ s^* &= \sigma + \sigma_s(vm + w). \end{aligned}$$

The verification equation then says that $s^* = vm^* + w$. This means:

$$(\sigma_s - 1)w = -\sigma + (\mu - m\sigma_s)v + \mu_s vw + \mu_s m \cdot v^2.$$

It then holds that $\sigma_s = 1$, $\sigma = 0$, $\mu = m$ and $\mu_s = 0$, hence $(m^*, s^*) = (m, s)$ and $(M^*, S^*) = (M, S)$, which is not a valid forgery. □

B Structure-Preserving Signatures from Non-interactive Assumptions

Taking a conservative stance, it is sometimes desirable to base the security of signature schemes on explicit non-interactive assumptions rather than giving direct proofs in the generic bilinear group model. The signature scheme from Sect. 3 can easily be modified to rely on a non-interactive assumption at the cost of adding an extra group element to the signature. We first define the following q-type assumption, which is equivalent to the random-message security of the scheme in Sect. 3.

Assumption 1 *For $VK = (PP, V, W)$ where $PP = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi, G, H) \leftarrow \mathcal{G}(1^k)$ and $(V, W) \leftarrow \mathbb{G}_1^2$, let θ_{VK} be the subset of all tuples $(M, R, S) \in \mathbb{G}_2^3$ such that $e(G, S) = e(V, M)e(\psi(R), R)e(W, H)$. Given VK and q uniformly chosen samples from θ_{VK}, no polynomial-time algorithm can output a tuple $(M^*, R^*, S^*) \in \theta_{VK}$ with significant probability such that M^* does not appear as the first component of any of the input samples.*

Note that Theorem 1 implies, in particular, that Assumption 1 holds in the generic group model. Based on that non-interactive assumption, we construct a scheme as follows.

Setup $\mathcal{P}(1^k)$**:** Return $PP = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, \psi, G, H) \leftarrow \mathcal{G}(1^k)$.
Key generation $\mathcal{K}(PP)$**:** Choose $u, v, w \leftarrow \mathbb{Z}_p$ and compute the keys $VK = (PP, U, V, W)$ and $SK = (PP, u, v, w)$ as

$$U \leftarrow G^u \qquad V \leftarrow G^v \qquad W \leftarrow G^w.$$

Signing $\mathcal{S}_{SK}(M)$**:** On $M \in \mathbb{G}_2$ choose $r, t \leftarrow \mathbb{Z}_p$ and compute signature $\Sigma = (R, S, T)$ as

$$R \leftarrow H^r \qquad T = H^t \qquad S \leftarrow M^v H^{tu+r^2+w}.$$

Verification $\mathcal{V}_{VK}(M, (R, S, T))$**:** Accept if and only if $M, R, S, T \in \mathbb{G}_2$ and

$$e(G, S) = e(U, T)e(V, M)e(\psi(R), R)e(W, H).$$

Fig. 4. Randomizable structure-preserving signature scheme for messages in $\mathbb{G}_2$.

Theorem 7. *The signature scheme in Fig. 4 is* EUF-CMA *secure if Assumption 1 holds.*

Proof. Given an EUF-CMA adversary $\mathcal{A}'$ against the scheme in Fig. 4, we will construct an adversary $\mathcal{A}$ that breaks Assumption 1.

Given $VK = (PP, V, W)$ and $(M_i, R_i, S_i) \leftarrow \theta_{VK}$ for $i = 1, \ldots, q$, $\mathcal{A}$ starts by setting $U = V^{\alpha} G^{\beta}$ for random $\alpha \leftarrow \mathbb{Z}_p^*$ and $\beta \leftarrow \mathbb{Z}_p$. It gives the simulated verification key $VK' = (PP, U, V, W)$ to $\mathcal{A}'$.

Whenever $\mathcal{A}'$ makes a signing query M_i', $\mathcal{A}$ takes (M_i, R_i, S_i) from the input and sets

$$R_i' = R_i \qquad S_i' = S_i (M_i / M_i')^{\frac{\beta}{\alpha}} \qquad T_i' = (M_i / M_i')^{\frac{1}{\alpha}}.$$

It then returns (R_i', S_i', T_i') as a signature for M_i'.

Finally, suppose A' after up to q queries outputs a valid forged signature (R', S', T') on a new message $M' \notin \{M_1', \ldots, M_q'\}$. $\mathcal{A}$ then sets

$$M^* = (T')^{\alpha} M' \qquad R^* = R' \qquad S^* = S' (T')^{-\beta}$$

and outputs (M^*, R^*, S^*).

The signatures returned from $\mathcal{A}$ are correct since

$$\begin{aligned}
& e(G, S_i')^{-1} e(V, M_i') e(U, T_i') e(\psi(R_i'), R_i') e(W, H) \\
&= e(G, S_i (M_i / M_i')^{\frac{\beta}{\alpha}})^{-1} e(V, M_i') e(V^{\alpha} G^{\beta}, (M_i / M_i')^{\frac{1}{\alpha}}) e(\psi(R_i), R_i) e(W, H) \\
&= e(G, S_i)^{-1} e(V, M_i) e(\psi(R_i), R_i) e(W, H) \\
&= 1.
\end{aligned}$$

We have $(M^*, R^*, S^*) \in \theta_{VK}$ since

$$\begin{aligned}
& e(G, S^*)^{-1} e(V, M^*) e(\psi(R^*), R^*) e(W, H) \\
&= e(G, S' (T')^{-\beta})^{-1} e(V, (T')^{\alpha} M') e(\psi(R'), R') e(W, H) \\
&= e(G, S')^{-1} e(V, M') e(G, (T')^{\beta}) e(V, (T')^{\alpha}) e(\psi(R'), R') e(W, H) \\
&= e(G, S')^{-1} e(V, M') e(U, T') e(\psi(R'), R') e(W, H) \\
&= 1.
\end{aligned}$$

Moreover, since $\alpha \in \mathbb{Z}_p^*$ is information theoretically hidden from the view of $\mathcal{A}'$ and $M' \notin \{M_1', \ldots, M_q'\}$, there is negligible probability that $M^* \in \{M_1, \ldots, M_q\}$. Thus if $\mathcal{A}'$ is successful with high probability, $\mathcal{A}$ breaks Assumption 1. □