Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures

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 construct a structure-preserving signature scheme that is selectively randomizable and works in all types of bilinear groups. We give matching lower bounds showing that our structure-preserving signature scheme is optimal with respect to both signature size and public verification key size.
State of the art structure-preserving signatures in the asymmetric setting consist of 3 group elements, which is known to be optimal. Our construction preserves the signature size of 3 group elements and also at the same time minimizes the verification key size to 1 group element.
Depending on the application, it is sometimes desirable to have strong unforgeability and in other situations desirable to have randomizable signatures. To get the best of both worlds, we introduce the notion of selective randomizability where the signer may for specific signatures provide randomization tokens that enable randomization.
Our structure-preserving signature scheme unifies the different pairing-based settings since it can be instantiated in both symmetric and asymmetric groups. Since previously optimal structure-preserving signatures had only been constructed in asymmetric bilinear groups this closes an important gap in our knowledge. Having a unified signature scheme that works in all types of bilinear groups is not just conceptually nice but also gives a hedge against future cryptanalytic attacks. An instantiation of our signature scheme in an asymmetric bilinear group may remain secure even if cryptanalysts later discover an efficiently computable homomorphism between the source groups.

Keywords: Structure-preserving signatures, automorphic signatures, selective randomizability.

1 Introduction

Structure-preserving signatures [3] (SPS) are signatures defined over groups with a bilinear pairing where messages, signatures and public verification keys all

⋆ The research leading to these results has received funding from the Engineering and Physical Sciences Research Council grant EP/G013829/1 and the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 307937.

consist of group elements and the verification algorithm evaluates verification equations consisting of products of pairings of these group elements. Based on such signatures, one can easily design modular cryptographic protocols with reasonable efficiency, in particular in combination with non-interactive zero-knowledge (NIZK) proofs of knowledge about group elements [21]. Numerous applications of SPS, including blind signatures [3, 17], group signatures [3, 17, 25], homomorphic signatures [24, 9], delegatable anonymous credentials [16], compact verifiable shuffles [14], network encoding [8], oblivious transfer [19, 12], tightly secure encryption [22, 2], anonymous e-cash [26], etc., have been presented in the literature.

1.1 Symmetric and asymmetric bilinear pairings

Bilinear pairing groups are usually instantiated as groups of points of certain restricted families of elliptic curves (or more rarely, other abelian varieties), and can be broadly classified into several types [18] according to the efficient morphisms that exist between the cyclic groups of prime order $\mathbb{G}_1$, $\mathbb{G}_2$ associated with the bilinear pairing $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. The two most important ones are Type I pairings, where $\mathbb{G}_1 = \mathbb{G}_2$, and Type III pairings defined as the ones that do not have an efficiently computable isomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$ in either direction. Type II parings, like Type III pairings, have $\mathbb{G}_1 \neq \mathbb{G}_2$ but with an efficiently computable isomorphism from one group to the other. We will also refer to Type I pairings as *symmetric* bilinear groups because $\mathbb{G}_1 = \mathbb{G}_2$ and refer to other types types of pairings where $\mathbb{G}_1 \neq \mathbb{G}_2$ as *asymmetric* bilinear groups.

Type I, or symmetric, pairings are obtained from supersingular curves, and have traditionally had an efficiency edge in implementations on resource-constrained devices, although recent advances on the discrete logarithm problem over finite fields of small characteristic [10] call this into question (large characteristic Type I pairings remain secure, but they are not as efficient). Pairing-based protocol designers often present their schemes in the symmetric setting, as protocol descriptions and security arguments tend to be simpler.

Type III pairings, which are the more efficient kind of asymmetric pairings, are obtained from special families of ordinary curves, and tend to be more compact, faster at least in software, and support stronger and more compact hardness assumptions such as the DDH assumption in their source groups. Thus, Type III pairings are often preferred for practical purposes. However, certain protocol descriptions given in the symmetric setting do not easily translate to the Type III setting.

1.2 Unified structure-preserving signatures

Since SPS are a relatively low-level building block, their efficiency is of crucial importance. That efficiency is usually measured in terms of the number of group elements in signatures and the number of verification equations, and a significant amount of research has been devoted to obtaining lower and upper bounds with respect to these measures. Abe et al. [4] gave a construction of an SPS with 3

group element signatures and 2 verification equations using Type III bilinear groups. They also gave a matching lower bound in Type III bilinear groups of 3 group elements for signatures and 2 verification equations, which showed that the construction is optimal with respect to signature size and verification complexity.

In contrast to the work on Type III pairings, very little is known about SPS over symmetric bilinear groups. The best known construction for Type I pairings has signatures with 7 group elements, and no non-trivial lower bounds or more efficient constructions have been proposed to date. One could hope that symmetric functions such as $e(X, X)$ that are only possible in Type I pairings would make more efficient designs possible. Besides, it seems plausible that having only one group in the symmetric case admits lower complexity than separately handling two groups as must be done in the asymmetric case. On the other hand, the ability to use elements as the input in either side of the pairing may give the adversary additional flexibility and cause additional vulnerabilities. So it is not *a priori* clear whether symmetric pairings are advantageous for designers or for attackers.

We answer this question in a strong sense by providing a unified structure-preserving signature scheme that works in all types of bilinear groups. The design of the scheme does not exploit any symmetry or maps between the source groups and can therefore be instantiated in any type of bilinear group. At the same time though, it is resistant to adversaries that are allowed to exploit symmetry. Our signature scheme has 3 group element signatures and 2 verification equations and is therefore optimal with respect to Type III pairings. We will also show similar lower bounds hold for Type I pairings and the scheme is therefore also optimal in the symmetric setting.

Designing unified structure-preserving schemes that can be used in either type of bilinear group is of course conceptually appealing since it is simpler than having separate schemes for each setting. Unified signature may also be more resistant to cryptanalysis. Currently Type III pairings are the most efficient but building cryptographic schemes in this setting may leave us vulnerable if cryptanalysts find an efficiently computable homomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$. However, if we use a unified structure-preserving signature we can even resist attacks where the adversary has an isomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$ that is efficiently computable in both directions. It is a fascinating question whether there are other cryptographic tasks for which we can construct unified structure-preserving schemes without sacrificing efficiency.

1.3 Minimal verification keys

An important efficiency measure that has not received much attention in the literature on structure-preserving signatures is the size of the public verification key. For applications that involve certification chains the public key size is of high importance. If the size of the public key exceeds the size of the messages the signature scheme can handle, it becomes difficult and cumbersome to build certification chains and in the world of structure-preserving signatures it is not

possible to use collision-resistant hash-functions to reduce the size of the messages since such hash-functions destroy the structure we are trying to preserve.

Abe et al. [4] considered only the size of the signatures and the number of verification equations but did not try to minimize the size of the public key. To sign a single group element they have a structure-preserving signature scheme with strong existential unforgeability where the public key consists of 3 group elements and a randomizable signature scheme where the public key consists of 2 group elements. This means that their schemes cannot easily be used to sign public keys. There are generic methods to extend the message space of SPS [7] but they incur a significant overhead so it is preferable to have an atomic scheme that can be used to sign verification keys.

Fuchsbauer [15, 3] defined an automorphic signature scheme as a structure-preserving signature scheme where the verification keys belong to the message space itself. This makes certification chains easy and cheap to construct and indeed automorphic signatures have been used in the construction of anonymous delegatable credentials [15, 16]. Current automorphic signatures, however, are more expensive than the most efficient structure-preserving signatures. The scheme in [3] has verification keys that consist of 2 group elements, the signatures consist of 5 group elements and the scheme uses 3 verification equations.

In contrast to these works, we also minimize the size of the verification key. As in the first construction of automorphic signatures [15, 3], we allow the setup to include some random group elements in the public parameters describing the bilinear group to help shortening the verification key. In our case, we assume that a bilinear group has been generated and a random group element X is included in these parameters. With this type of setup, it is possible to get a public verification key that consists of just one single group element.

If the signer runs the setup algorithm, she is ensured that the setup is correct. However, even if the signer uses a pre-existing setup it is a moderate trust assumption since we do not need to trust anybody to store any secret trapdoors associated with the setup; it is for instance not necessary for the signer to know the discrete logarithm of X in our scheme. If the setup is generated by a trusted third party, we therefore only need to assume the trusted third party is honest at the particular time it is generating the setup without storing a secret trapdoor at that point in time. Alternatively, we may sample the setup in an oblivious manner from a trusted source of random bits such as a multi-party coin-flipping protocol or extract it from a physical source of randomness, e.g., solar activity in a given time interval.

With a single group element as verification key, it becomes easy to build certification chains. In the symmetric setting, we get an automorphic signature scheme where the verification key space is identical to the message space. In Type III pairings, our construction is not automorphic because the message and the verification key belong to different groups. However, it is easy to create a certification ladder where we use a verification key in $\mathbb{G}_2$ to certify a verification key in $\mathbb{G}_1$, which can then be used to certify a verification key in $\mathbb{G}_2$, etc.

1.4 Selective randomizability

We introduce a new feature called *selective randomizability* that allows a strongly unforgeable signature to be randomized with the help of a randomization token. Selective randomizability reconciles the notions of strong unforgeability, where it is impossible to create new signatures on signed messages, and randomizability, where it is possible to randomize signatures. Depending on the application, different parties may hold randomization tokens corresponding to certain signatures and they may randomize the signatures, while other parties cannot randomize the signatures.

Randomizability is useful in reducing the size of the proofs when the SPS is combined with the Groth-Sahai proof system since a part of a randomized signature can be shown in the clear. There are other applications and theoretical results on (not selectively) randomizable signatures in the literature, e.g. [27, 23]. Selective randomizability may also have uses on its own; a selectively randomizable signature can for instance be used as a service token. Fee paying users get a signature on the time period they have paid for and a randomization token and can in each use reveal a fresh randomized signature. Fraudsters on the other hand do not know the randomization tokens and cannot modify the signatures and can therefore only copy previous signatures.

We show that our structure-preserving signature scheme is selectively randomizable. Our randomization tokens consist of a single group element, so also here we achieve minimal size.

1.5 Related work

Abe et al. [3] first used the term structure-preserving signatures but there are earlier works in the area. Groth [20] proposed the first structure-preserving signature but the construction involves hundreds of group elements and is not practical. Green and Hohenberger [19] gave a structure-preserving signature scheme, which is secure against random message attack, but is not known to be secure against adaptive chosen message attack. Cathalo, Libert and Yung [13] constructed a signature scheme that structure-preserving in a relaxed sense that permits the verification key to include target group elements.

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 group model. Abe et al. [5] later showed 3 element signatures cannot be proven secure under a non-interactive assumption using black-box reductions, so strong assumptions are needed to get optimal efficiency.

Hofheinz and Jager [22] and Abe et al. [1, 2] investigated the possibility of basing structure-preserving signatures on standard assumptions. They give structure-preserving signatures based on the decision linear (DLIN) assumption. The use of a nice security assumption, however, comes at the price of reducing efficiency.

Scheme	Signature	Ver. key	Equations	Type	Assumption	Notes
[20]	Many	Many	Many	I	DLIN	
[13]	11	11	9	I	HSDH, FlexDH, S2D	$*1$
[3]	7	13	2	Any	SFP	$*2$
[15, 3]	5	2	3	Any	ADH-SDH, AWF-CDH	$*3$
[4]	4	4	2	III	Non-interactive	$*1$
[4]	3	3	2	III	Interactive	$*1$
[4]	3	2	2	III	Interactive	$*2$
[1]	17	27	9	I	DLIN	
[1]	11	21	5	III	SXDH, XDLIN	
[2]	14	22	7	I	DLIN	
Ours	3	1	2	Any	Interactive	$*4$

Table 1. Comparison of structure-preserving signatures on a single group element. $*1$: Strongly unforgeable. $*2$: Randomizable. $*3$: Automorphic. $*4$: Selectively Randomizable.

1.6 Our contributions

We construct a selectively randomizable structure-preserving signature scheme with message space $\mathcal{M} = \mathbb{G}_1$, where a verification key is 1 group element, a signature is 3 group elements and the verifier uses 2 verification equations to verify the signature. The setup for the signature scheme consists of the description of a bilinear group and a single random group element. Our signature scheme is unified, i.e., it can be used in both symmetric and asymmetric bilinear groups.

We prove our signature scheme secure in the generic group model. The security of the signature scheme can therefore be viewed as an interactive security assumption. However, as shown by Abe et al. [7] it is impossible to base the security of structure-preserving signature schemes with 3 group element signatures on non-interactive intractability assumptions using black-box reductions, so at least in the Type III setting we could not hope to base security on a non-interactive assumption. On the positive side, being unified provides a hedge against cryptanalytic attacks. Even if cryptanalysts uncover efficiently computable homomorphisms between $\mathbb{G}_1$ and $\mathbb{G}_2$, our structure-preserving signature scheme may remain secure.

Table 1 compares our results to previous work on structure-preserving signatures in the symmetric and asymmetric settings. We only consider the case of a single group element and in the table we therefore compare all schemes on the same terms, i.e., the cost for signing a single group element, with the exception of Fuchsbauer's automorphic signature scheme, which is tailored to sign Diffie-Hellman pairs of group elements.

To complement our signature scheme, we provide the first analysis of lower bounds in the symmetric setting. We demonstrate that in the symmetric setting a signature must be at least 3 group elements and the verifier must use at least 2 verification equations. This matches the Type III setting previously analyzed

in [4] and shows that our signature scheme is optimal also in symmetric bilinear groups.

Interestingly it turns out that in the case of one-time signatures there is actually a difference between Type I and Type III pairings. While it is known that Type III pairings admit one-time signatures with a single verification equation, we show this is not the case for Type I pairings. The lower bound of 2 verification equations also applies to one-time signatures.

The lower bound of 3 group elements for the size of signatures does not apply though. We demonstrate this by constructing a one-time signature scheme in the symmetric setting with 2 group element signatures. We also analyze one-time signatures with respect to the size of the verification key. We show that both Type I and Type III pairings have structure-preserving one-time signature schemes with 1 group element verification keys.

2 Preliminaries

2.1 Bilinear groups

Let $\mathcal{G}$ be a bilinear group generator that returns $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G, H) \leftarrow \mathcal{G}(1^k)$ given security parameter k with the following properties:

- $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are groups of prime order p
- $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is a bilinear map s.t. $e(G^a, H^b) = e(G, H)^{ab}$ for all $a, b \in \mathbb{Z}$
- G generates $\mathbb{G}_1$, H generates $\mathbb{G}_2$, and $e(G, H)$ generates $\mathbb{G}_T$
- There are efficient algorithms for computing group operations, evaluating the bilinear map, comparing group elements and deciding membership of the groups

Bilinear groups can be classified in the 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 $G = H$. Type II pairings have an efficiently computable isomorphism 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.

2.2 Generic algorithms

In a bilinear group $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G, H)$ 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 bilinear map as the generic group operations. The signature schemes we construct only use generic 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.

2.3 Setup

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. We will therefore in the description of our signatures explicitly distinguish between a setup algorithm $\mathcal{P}$ that produces a public parameter PP and a key generation algorithm the signer uses to generate her own keys.

The setup algorithms we use generate a bilinear group $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G, H) \leftarrow \mathcal{G}(1^k)$. They may then extend the description of the bilinear group with additional random group elements. As discussed in Sect. 1.3 this is a moderate setup assumption since the signer does not need to know the discrete logarithms of the random group elements. The group elements may therefore be sampled obliviously without learning the discrete logarithms or the discrete logarithms may be erased immediately upon generation.

2.4 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. 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 (perfectly) correct if for all security parameters $k \in \mathbb{N}$*

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

A signature scheme is said to be existentially unforgeable if it is hard to forge a signature on a new message that has not been signed before. 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 signatures 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.

We now formally define existential unforgeability under adaptive chosen message attack.

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 $\mathcal{A}$*

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

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.

2.5 Selectively randomizable signatures

Some applications require signatures to be strongly unforgeable, while in other applications it is desirable that a signature on a message can be randomized into a new random signature on the same message. A randomizable signature scheme can only be EUF-CMA secure though since a randomized signature would violate sEUF-CMA security. In order to reconcile the two notions and get the best of both worlds, we define the notion of selective randomizability where the signer can select to make specific signatures randomizable by providing randomization tokens for them.

In a selectively randomizable signature scheme the signing algorithm returns both a signature and a randomization token. Furthermore, there is a randomization algorithm $\mathcal{R}$ that given a message, signature and randomization token returns a random signature on the message. We require that the randomization algorithm $\mathcal{R}$ given a message M, signature Σ and corresponding randomization token W computes a signature $\Sigma' \leftarrow \mathcal{R}_{VK}(M, \Sigma, W)$ such that for all correctly generated inputs $R_{VK}(M, \Sigma, W)$ and $\mathcal{S}_{SK}(M)$ have identical probability distributions.

Since the signatures are randomizable it is not possible to have *strong* existential unforgeability if the randomization tokens are given to the adversary. However, we can get strong existential unforgeability for signatures on messages for which the adversary does not have randomization tokens. Formally we define security against a chosen message and token attack (CMA-TA) as follows.

Definition 3 (sEUF-CMA-TA). *A selectively randomizable signature scheme* $(\mathcal{P}, \mathcal{K}, \mathcal{S}, \mathcal{R}, \mathcal{V})$ *is strongly existentially unforgeable under chosen message and token attack if for all non-uniform polynomial time* $\mathcal{A}$

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

where $\mathcal{S}$ *is a signing oracle that is given a message and returns a signature on the message,* $\mathcal{S}t$ *is a token-signing oracle that is given a message and returns both a signature and a randomization token,* Q *is the set of messages and signatures observed by the signing oracle, and* Qt *is the set of messages observed by the token-signing oracle.*

Please observe that $\mathcal{A}$ can send M to $\mathcal{S}$ and $\mathcal{S}t$ an arbitrary number of times to get (random) signatures on M so we do not need to provide the adversary with a randomization oracle in the security definition.

2.6 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 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. 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.

Definition 4 (Structure-preserving signatures). *A digital 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* $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G, H)$ *generated by* $\mathcal{G}$*, 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* $\mathbb{G}_2$ *and evaluate pairing product equations.*

When proving our lower bounds, we will relax the above definition to allow arbitrary target group elements $Z \in \mathbb{G}_T$ to be included in the verification key and to appear in the verification equations. This gives the strongest possible results: our lower bounds hold in a relaxed model of structure-preserving signatures and our constructions of signatures satisfy the strict model of structure-preserving signatures.

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 Selectively Randomizable Structure-Preserving Signatures

Fig. 1 gives a selectively randomizable structure-preserving signature scheme with 1 element verification keys, 3 group element signatures and 2 verification equations. The signature scheme is sEUF-CMA-TA secure. The lower bounds in [4] and Sect. 5 show that this construction is optimal with respect to size and verification complexity in both Type I and Type III bilinear groups.

Setup $\mathcal{P}(1^k)$**:** Run $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G, H) \leftarrow \mathcal{G}(1^k)$, pick $X \leftarrow \mathbb{G}_1$, and return $PP = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G, X, H)$.

Key generation $\mathcal{K}(PP)$**:** Choose $v \leftarrow \mathbb{Z}_p$, compute $V \leftarrow H^v$, and return $VK = (PP, V)$ and $SK = (PP, v)$.

Signing $\mathcal{S}_{SK}(M)$**:** On $M \in \mathbb{G}_1$ choose $r \leftarrow \mathbb{Z}_p^*$ and compute signature $\Sigma = (R, S, T)$ and randomization token W as:

$$R \leftarrow H^r, \qquad S \leftarrow M^{\frac{v}{r}} X^{\frac{1}{r}}, \qquad T \leftarrow S^{\frac{v}{r}} G^{\frac{1}{r}}, \qquad W \leftarrow G^{\frac{1}{r}}.$$

Randomization $\mathcal{R}_{VK}(M, (R, S, T), W)$**:** Pick $\alpha \leftarrow \mathbb{Z}_p^*$ and compute the randomized signature $\Sigma' = (R', S', T')$ given by:

$$R' \leftarrow R^{\frac{1}{\alpha}}, \qquad S' \leftarrow S^{\alpha}, \qquad T' \leftarrow T^{\alpha^2} W^{\alpha(1-\alpha)}.$$

Verification $\mathcal{V}_{VK}(M, (R, S, T))$**:** Accept if and only if $M, S, T \in \mathbb{G}_1$, $R \in \mathbb{G}_2$ and

$$e(S, R) = e(M, V)e(X, H) \quad \text{and} \quad e(T, R) = e(S, V)e(G, H).$$

Fig. 1. Minimal structure-preserving signature scheme.

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. Somebody who has a signature on a particular message and a corresponding randomization token can create as many uniformly random signatures on the message as she wants. An additional feature is that the randomization token can also be randomized together with the signature by computing $W' \leftarrow W^{\alpha}$, so the power to randomize can be delegated to others.

The signature scheme is designed with Groth-Sahai proofs in mind. If we have a secret randomization token and use it to 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 both verification equations become linear, which makes Groth-Sahai proofs very efficient.

We will now prove that the signature scheme with selective randomization is sEUF-CMA-TA secure. This implies as two special cases that the signature in Fig. 1 is EUF-CMA secure even when all randomization tokens are revealed and sEUF-CMA secure if no randomization tokens are revealed.

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

Proof. We will without loss of generality show that the signature scheme is sEUF-CMA-TA secure in the symmetric setting where $\mathbb{G}_1 = \mathbb{G}_2$ since this setting gives the adversary the most degrees of freedom and hence the best chance of breaking the scheme. Moreover, the scheme is secure in the generic group model even if the discrete logarithm $\log_G(H)$ is known to the adversary and we will therefore without loss of generality assume $H = G$.

A generic adversary only uses generic group operations. This means that in $\mathbb{G}_1$ it can only compute linear combinations of group elements from the verification key and the signatures it has seen. Linear combinations on verification key elements and signature elements correspond to formal Laurent polynomials (of degree ranging from $-2q$ to $2q + 1$ after q signature queries) in the discrete logarithms of the group elements. We will show that no linear combinations produce formal Laurent polynomials corresponding to a forgery. By the master theorem in [11] this means that the signature scheme is secure in the generic group model.

The group elements in VK are G, X, V with corresponding discrete logarithms $1, x, v$. On a query M_i with discrete logarithm m_i from the adversary, the signature oracle responds with a signature (R_i, S_i, T_i) and possibly a rerandomization token W_i with discrete logarithms

$$r_i \leftarrow \mathbb{Z}_p^* \qquad s_i = \frac{m_i v}{r_i} + \frac{x}{r_i} \qquad t_i = \frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i} \qquad w_i = \frac{1}{r_i}.$$

Suppose the adversary after q queries constructs (M, R, S, T). Since the adversary is generic it can only construct m, r, s, t that are linear combinations

of $1, x, v, r_1, s_1, t_1, w_1, \ldots, r_q, s_q, t_q, w_q$, i.e.,

$$\begin{aligned}
m =& \mu + \mu_x x + \mu_v v + \sum_{i=1}^{q} \left[\mu_{r_i} r_i + \mu_{s_i} \left(\frac{m_i v}{r_i} + \frac{x}{r_i}\right) + \mu_{t_i} \left(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}\right) + \mu_{w_i} \frac{1}{r_i} \right] \\
r =& \rho + \rho_x x + \rho_v v + \sum_{i=1}^{q} \left[\rho_{r_i} r_i + \rho_{s_i} \left(\frac{m_i v}{r_i} + \frac{x}{r_i}\right) + \rho_{t_i} \left(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}\right) + \rho_{w_i} \frac{1}{r_i} \right] \\
s =& \sigma + \sigma_x x + \sigma_v v + \sum_{i=1}^{q} \left[\sigma_{r_i} r_i + \sigma_{s_i} \left(\frac{m_i v}{r_i} + \frac{x}{r_i}\right) + \sigma_{t_i} \left(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}\right) + \sigma_{w_i} \frac{1}{r_i} \right] \\
t =& \tau + \tau_x x + \tau_v v + \sum_{i=1}^{q} \left[\tau_{r_i} r_i + \tau_{s_i} \left(\frac{m_i v}{r_i} + \frac{x}{r_i}\right) + \tau_{t_i} \left(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}\right) + \tau_{w_i} \frac{1}{r_i} \right]
\end{aligned}$$

Similarly, each query m_i is a linear combination of $1, x, v, r_1, s_1, t_1, w_1, \ldots, r_{i-1}$, s_{i-1}, t_{i-1}, w_{i-1}.

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

$$sr = mv + x \qquad tr = sv + 1 = mv^2 + xv + 1$$

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

If a randomization token has not been given for a particular message the attacker must use $\tau_{w_i} = 0$ for all indices i where this message was queried. We will show that the adversary can only randomize a signature by using some $\tau_{w_j} \neq 0$. This means the signature scheme is strong for those messages where no randomization token has been given, which gives us sEUF-CMA-TA security.

Our proof strategy is to use the first verification equation $sr = mv + x$ to simplify the descriptions of s and r by demonstrating that many of the coefficients σ_* and ρ_* are 0. After narrowing the solution space down to four distinct cases, we use the second verification equation $tr = sv + 1$ to rule out three cases and determine a single type of possible solutions. These solutions correspond exactly to randomization of signatures and if no randomization token is given then the solution must be an exact copy of a previous signature.

In order to get to the core of our proof, we delay the proof of the following claim.

Claim. The first verification equation $sr = mv + x$ can only be satisfied if the adversary picks $\sigma_{t_i} = 0, \sigma_{w_i} = 0, \rho_{t_i} = 0$ and $\rho_{w_i} = 0$ for all $i = 1, \ldots, q$.

We now know that $\sigma_{t_i}, \sigma_{w_i}, \rho_{t_i}$ and ρ_{w_i} are zero for all $i = 1, \ldots, q$. Obviously we cannot rule out the existence of some j for which $\sigma_{s_j} \neq 0$ since the adversary could simply copy a previous signature $s = s_j$ by setting $\sigma_{s_j} = 1$. We will now analyze the structure of s and r when there exists a j such that $\sigma_{s_j} \neq 0$.

We can write $sr = mv + x$ as

$$\left(\sigma + \sigma_x x + \sigma_v v + \sum_{i=1}^{q} \sigma_{r_i} r_i + \sigma_{s_i}(\frac{m_i v}{r_i} + \frac{x}{r_i})\right) \cdot \left(\rho + \rho_x x + \rho_v v + \sum_{i=1}^{q} \rho_{r_i} r_i + \rho_{s_i}(\frac{m_i v}{r_i} + \frac{x}{r_i})\right)$$
$$= \left(\mu + \mu_x x + \mu_v v + \sum_{i=1}^{q} \mu_{r_i} r_i + \mu_{s_i}(\frac{m_i v}{r_i} + \frac{x}{r_i}) + \mu_{t_i}(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}) + \mu_{w_i}\frac{1}{r_i}\right) v + x.$$

We first look at the term $\frac{x^2}{r_j^2}$. Observe that all verification key elements and signatures are linear in x and therefore all elements $m, r, s, t, m_1, \ldots, m_q$ constructed using generic group operations must also be linear in x. This shows that the term $\frac{x^2}{r_j^2}$ has coefficient 0 in $mv + x$.

Let us now determine the coefficient of $\frac{x^2}{r_j^2}$ in the product sr. Whenever the adversary makes a query m_i to get a signature (r_i, s_i, t_i) the message m_i is multiplied by v or v^2 by the signing oracle. It is not possible to decrease the degree of v, so these queries cannot contribute to the $\frac{x^2}{r_j^2}$ term. Looking at the terms in s and r we then see that the coefficient of $\frac{x^2}{r_j^2}$ in sr is $\sigma_{s_j}\rho_{s_j}$.

Comparing the coefficients of $\frac{x^2}{r_j^2}$ from the two sides of the verification equation we get $\sigma_{s_j}\rho_{r_j} = 0$. Since we assumed $\sigma_{s_j} \neq 0$ this implies $\rho_{s_j} = 0$. Using a similar analysis of the terms $\frac{x^2}{r_i r_j}$ give us $\sigma_{s_i}\rho_{s_j} + \sigma_{s_j}\rho_{s_i} = \sigma_{s_j}\rho_{s_i} = 0$ and therefore $\rho_{s_i} = 0$ for all i.

The term $\frac{x^2}{r_j}$ gives us $\sigma_{s_j}\rho_x = 0$ and therefore $\rho_x = 0$. The term $\frac{x}{r_j}$ gives us $\sigma_{s_j}\rho = 0$ and therefore $\rho = 0$. The terms $\frac{xr_i}{r_j}$ give us $\sigma_{s_j}\rho_{r_i} = 0$ and therefore $\rho_{r_i} = 0$ for all $i \neq j$. Finally, the term x gives us $\sigma_{s_j}\rho_{r_j} = 1$ and therefore $\rho_{r_j} = \frac{1}{\sigma_{s_j}}$.

We now have $r = \rho_v v + \rho_{r_j} r_j$ with $\rho_{r_j} = \frac{1}{\sigma_{s_j}} \neq 0$. Let us proceed to analyze the structure of s. The terms $\frac{xr_j}{r_i}$ give us $\sigma_{s_i}\rho_{r_j}$ and therefore $\sigma_{s_i} = 0$ for all $i \neq j$. The term r_j^2 gives us $\sigma_{r_j}\rho_{r_j} = 0$ and therefore $\sigma_{r_j} = 0$. The terms $r_i r_j$ give us $\sigma_{r_i}\rho_{r_j} + \sigma_{r_j}\rho_{r_i} = \sigma_{r_i}\rho_{r_j} = 0$ and therefore $\sigma_{r_i} = 0$ for all i. The term r_j gives us $\sigma\rho_{r_j} = 0$ and therefore $\sigma = 0$. The term xr_j gives us $\sigma_x\rho_{r_j} = 0$ and therefore $\sigma_x = 0$. We conclude that $s = \sigma_v v + \sigma_{s_j}(\frac{m_j v}{r_j} + \frac{x}{r_j})$.

By symmetry we now have two possible cases:

Case	s	r
$1:\ \sigma_{s_j} \neq 0$	$s = \sigma_v v + \sigma_{s_j}(\frac{m_j v}{r_j} + \frac{x}{r_j})$	$r = \rho_v v + \frac{1}{\sigma_{s_j}} r_j$
$2:\ \rho_{s_j} \neq 0$	$s = \sigma_v v + \frac{1}{\rho_{s_j}} r_j$	$r = \rho_v v + \rho_{s_j}(\frac{m_j v}{r_j} + \frac{x}{r_j})$

There still remains the possibility that $\sigma_{s_i} = 0$ and $\rho_{s_i} = 0$ for all i. We can then write $sr = mv + x$ as

$$\left(\sigma + \sigma_x x + \sigma_v v + \sum_{i=1}^{q} \sigma_{r_i} r_i\right) \cdot \left(\rho + \rho_x x + \rho_v v + \sum_{i=1}^{q} \rho_{r_i} r_i\right)$$
$$= \left(\mu + \mu_x x + \mu_v v + \sum_{i=1}^{q} \mu_{r_i} r_i + \mu_{s_i}\left(\frac{m_i v}{r_i} + \frac{x}{r_i}\right) + \mu_{t_i}\left(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}\right) + \mu_{w_i}\frac{1}{r_i}\right) v + x.$$

The term x^2 shows that $\rho_x \sigma_x = 0$, so they cannot both be non-zero. The term x on the other hand shows $\sigma\rho_x + \sigma_x\rho = 1$ so at least one of ρ_x or σ_x is non-zero. Let us in the following assume $\sigma_x \neq 0$ and therefore $\rho = \frac{1}{\sigma_x} \neq 0$. The constant term gives us $\sigma\rho = 0$ and therefore $\sigma = 0$. The terms r_i give us $\sigma_{r_i} = 0$ for all i and the terms xr_i give us $\rho_{r_i} = 0$ for all i. This means we have $s = \sigma_x x + \sigma_v v$ and $r = \frac{1}{\sigma_x} x + \rho_v v$. By symmetry we now have two additional cases

Case	s	r
$3:\ \sigma_x \neq 0$	$s = \sigma_x x + \sigma_v v$	$r = \frac{1}{\sigma_x} + \rho_v v$
$4:\ \rho_x \neq 0$	$s = \frac{1}{\rho_x} + \sigma_v v$	$r = \rho_x x + \rho_v v$

We will now analyze the four cases we have identified with the help of the second verification equation $tr = sv + 1$. In case 4 where $r = \rho_x x + \rho_v v$ we see that in tr all terms involve x or v. This means we do not have a constant term in either tr or sv, which makes it impossible to get $tr = sv + 1$.

A similar argument can be used in case 2 where $r = \rho_v v + \rho_{s_j}(\frac{m_j v}{r_j} + \frac{x}{r_j})$, since both in tr and in sv all terms involve x or v and therefore it is impossible to get $tr = sv + 1$.

Let us now analyze case 3 where $r = \rho + \rho_v v$ and $s = \frac{1}{\rho} x + \sigma_v v$. We get

$$\left(\tau + \tau_x x + \tau_v v + \sum_{i=1}^{q} \tau_{r_i} r_i + \tau_{s_i}\left(\frac{m_i v}{r_i} + \frac{x}{r_i}\right) + \tau_{t_i}\left(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}\right) + \tau_{w_i}\frac{1}{r_i}\right) \cdot (\rho + \rho_v v)$$
$$= \frac{1}{\rho} xv + \sigma_v v^2 + 1.$$

The constant term gives us $\tau\rho = 1$ and therefore $\rho = \frac{1}{\tau} \neq 0$. The term x gives us $\tau_x \rho = 0$ and therefore $\tau_x = 0$. But now the xv term yields a contradiction since it gives us $0 = \frac{1}{\rho} \neq 0$.

The only remaining possibility is case 1 where $r = \rho_v v + \rho_{r_j} r_j$ with $\rho_{r_j} = \frac{1}{\sigma_{s_j}}$ and $s = \sigma_v v + \sigma_{s_j}(\frac{m_j v}{r_j} + \frac{1}{r_j})$. Inserting it in the second verification equation we get

$$\left(\tau + \tau_x x + \tau_v v + \sum_{i=1}^{q} \tau_{r_i} r_i + \tau_{s_i}\left(\frac{m_i v}{r_i} + \frac{x}{r_i}\right) + \tau_{t_i}\left(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}\right) + \tau_{w_i}\frac{1}{r_i}\right) \cdot \left(\rho_v v + \rho_{r_j} r_j\right)$$
$$= \sigma_v v^2 + \sigma_{s_j}\left(\frac{m_j v^2}{r_j} + \frac{xv}{r_j}\right) + 1.$$

The terms $\frac{xvr_j}{r_i^2}$ give us $\tau_{t_i}\rho_{r_j} = 0$ and therefore $\tau_{t_i} = 0$ for $i \neq j$. The terms $\frac{1}{r_i r_j}$ give us $\tau_{w_i}\rho_{r_j} = 0$ and therefore $\tau_{w_i} = 0$ for $i \neq j$. The terms $\frac{xr_j}{r_i}$ give us $\tau_{s_i}\rho_{r_j} = 0$ and therefore $\tau_{s_i} = 0$ for all $i \neq j$. The term x gives us $\tau_{s_j}\rho_{r_j} = 0$ and therefore $\tau_{s_j} = 0$. The terms r_j^2 and $r_i r_j$ give us $\tau_{r_i} = 0$ for all i. The term xr_j gives us $\tau_x = 0$ and the term r_j gives us $\tau = 0$.

Since $\rho_{r_j} = \frac{1}{\sigma_{s_j}}$ we have now simplified the second verification equation to

$$\left(\tau_v v + \tau_{t_j}(\frac{m_j v^2}{r_j^2} + \frac{xv}{r_j^2} + \frac{1}{r_j}) + \tau_{w_j}\frac{1}{r_j}\right) \cdot \left(\rho_v v + \frac{1}{\sigma_{s_j}} r_j\right) = \sigma_v v^2 + \sigma_{s_j}(\frac{m_j v^2}{r_j} + \frac{xv}{r_j}) + 1.$$

The term $\frac{xv}{r_j}$ gives us $\tau_{t_j} \cdot \frac{1}{\sigma_{s_j}} = \sigma_{s_j}$ giving us $\tau_{t_j} = \sigma_{s_j}^2$. The constant term gives us $(\tau_{t_j} + \tau_{w_j}) \cdot \frac{1}{\sigma_{s_j}} = 1$ giving us $\tau_{w_j} = \sigma_{s_j}(1 - \sigma_{s_j})$. The vr_j term gives us $\tau_v = 0$. The $\frac{xv^2}{r_j^2}$ term gives us $\rho_v = 0$. Finally, the v^2 term gives us $\sigma_v = 0$.

The adversary can therefore only compute a valid signature by using

$$r = \frac{1}{\sigma_{s_j}} r_j \qquad s = \sigma_{s_j} s_j \qquad t = \sigma_{s_j}^2 t_j + \sigma_{s_j}(1 - \sigma_{s_j}) w_j.$$

The first verification equation then gives us $mv + x = sr = s_j r_j = m_j v + x$, showing $m = m_j$ and therefore the signature scheme is EUF-CMA secure even in the presence of randomization tokens. Furthermore, if no randomization token w_j has been provided for the message then $\tau_{w_j} = 0$. Since $\tau_{w_j} = \sigma_{s_j}(1 - \sigma_{s_j})$ and $\sigma_{s_j} \neq 0$ this shows $\sigma_{s_j} = 1$. This implies $r = r_j, s = s_j$ and $t = t_j$, which shows that the signature scheme is sEUF-CMA-TA secure.

Let us now prove Claim 3.

Proof. Starting with the first verification equation $sr = mv + x$ we have

$$\begin{aligned}
&\left(\sigma + \sigma_x x + \sigma_v v + \sum_{i=1}^{q} \sigma_{r_i} r_i + \sigma_{s_i}(\frac{m_i v}{r_i} + \frac{x}{r_i}) + \sigma_{t_i}(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}) + \sigma_{w_i}\frac{1}{r_i}\right) \\
&\cdot \left(\rho + \rho_x x + \rho_v v + \sum_{i=1}^{q} \rho_{r_i} r_i + \rho_{s_i}(\frac{m_i v}{r_i} + \frac{x}{r_i}) + \rho_{t_i}(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}) + \rho_{w_i}\frac{1}{r_i}\right) \\
=&\left(\mu + \mu_x x + \mu_v v + \sum_{i=1}^{q} \mu_{r_i} r_i + \mu_{s_i}(\frac{m_i v}{r_i} + \frac{x}{r_i}) + \mu_{t_i}(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}) + \mu_{w_i}\frac{1}{r_i}\right) v + x
\end{aligned}$$

We first show that $\sigma_{t_i} = 0$ for all i. Assume for contradiction that there exists a j such that $\sigma_{t_j} \neq 0$. We start by looking at the coefficients of $\frac{x^2 v^2}{r_j^4}$. The Laurent polynomials corresponding to r, s, m and $m_1, \ldots, m_q$ are all linear in x. Terms involving x^2 can therefore only arise in the product sr. This shows that the coefficient of $\frac{x^2 v^2}{r_j^4}$ is 0 in $mv + x$. We will in the following argue the coefficient of $\frac{x^2 v^2}{r_j^4}$ in sr is $\sigma_{t_j}\rho_{t_j}$, which by our assumption $\sigma_{t_j} \neq 0$ implies $\rho_{t_j} = 0$.

To see that indeed the coefficient of $\frac{x^2v^2}{r_j^4}$ in sr is $\sigma_{t_j}\rho_{t_j}$, we need to rule out that other cross terms in sr can be $\frac{x^2v^2}{r_j^4}$. Observe that in all terms of s and r the degree of r_j ranges from -2 to 1 and only has degree -2 in the term $t_j = \frac{m_j v^2}{r_j^2} + \frac{xv}{r_j^2} + \frac{1}{r_j}$ and in subsequent signatures on queries m_i that include a t_j term. However, if a term m_i involves t_j then the resulting signature terms s_i and t_i multiply the t_j by v or v^2. By using the fact that the degree of v never decreases, we see that all other cross terms involving $\frac{x^2}{r_j^4}$ have degree 3 or higher in v. The coefficients of $\frac{x^2v^2}{r_j^4}$ therefore do indeed give us $\sigma_{t_j}\rho_{t_j} = 0$ and therefore $\rho_{t_j} = 0$.

Next we look at the term $\frac{x^2v^2}{r_j^2 r_i^2}$ for $i \neq j$. A similar analysis shows that the coefficients satisfy $\sigma_{t_j}\rho_{t_i} + \sigma_{t_i}\rho_{t_j} = 0$. Since $\rho_{t_j} = 0$ and $\sigma_{t_j} \neq 0$ this implies $\rho_{t_i} = 0$ for all i.

We proceed to the term $\frac{x^2v}{r_j^3}$ and will show the coefficient in sr of this term is $\sigma_{t_j}\rho_{s_j}$. Since the degree of r_j is -3 in the term, we see that t_j must be used either directly, or indirectly through a signature on a subsequent query m_i involving t_j. However, whenever m_i involves t_j the degree of v is increased to at least 2 and such subsequent queries cannot contribute to the term. An inspection of the different cross terms now shows that indeed $\sigma_{t_j}\rho_{s_j}$ is the coefficient in sr for the term $\frac{x^2v}{r_j^3}$. Since cross terms involving x^2 can only arise in sr and not in $mv + x$ we then have $\sigma_{t_j}\rho_{s_j} = 0$ and since we assumed $\sigma_{t_j} \neq 0$ this means $\rho_{s_j} = 0$.

A similar analysis shows that for $i \neq j$ the terms $\frac{x^2v}{r_i r_j^2}$ have coefficient $\sigma_{t_i}\rho_{s_j} + \sigma_{t_j}\rho_{s_i} = \sigma_{t_j}\rho_{s_i} = 0$ and therefore $\rho_{s_i} = 0$ for all i.

We now look at the term $\frac{x^2v}{r_j^2}$. Again looking at the degrees of v in subsequent queries with m_i using t_j we see that they cannot contribute to the coefficient of $\frac{x^2v}{r_j^2}$ in sr and therefore the coefficient is $\sigma_{t_j}\rho_x$. Since there are no terms involving x^2 in $mv + 1$ this means $\sigma_{t_j}\rho_x = 0$ and therefore $\rho_x = 0$.

Using the term $\frac{xv}{r_j^3}$ we see that $\sigma_{t_j}\rho_{w_j} = 0$ and therefore $\rho_{w_j} = 0$. The terms $\frac{xv}{r_i r_j^2}$ give us $\sigma_{t_j}\rho_{w_i} + \sigma_{w_i}\rho_{t_j} = \sigma_{t_j}\rho_{w_i} = 0$, which implies $\rho_{w_i} = 0$ for all i.

The term $\frac{xv}{r_j^2}$ gives us $\sigma_{t_j}\rho = 0$ and therefore $\rho = 0$.

The terms $\frac{xvr_i}{r_j^2}$ give us $\sigma_{t_j}\rho_{r_i} = 0$ and therefore $\rho_{r_i} = 0$ for all $i \neq j$. The term $\frac{xv}{r_j}$ gives us $\sigma_{t_j}\rho_{r_j} = 0$ and therefore $\rho_{r_j} = 0$.

We now have $r = \rho_v v$, which means all terms in sr and mv have at least degree 1 in v. It is therefore impossible to get $sr = mv + x$ when there exists a j such that $\sigma_{t_j} \neq 0$.

By symmetry we can also rule out the existence of $\rho_{t_j} \neq 0$. We conclude that both r and s must have $\rho_{t_i} = 0$ and $\sigma_{t_i} = 0$ for all $i = 1, \ldots, q$ and will use that simplification in the rest of our proof.

Next, we will show that for all i we have $\sigma_{w_i} = 0$. Assume for contradiction $\sigma_{w_j} \neq 0$ for some j. We can write $sr = mv + x$ as

$$\left(\sigma + \sigma_x x + \sigma_v v + \sum_{i=1}^{q} \sigma_{r_i} r_i + \sigma_{s_i}(\frac{m_i v}{r_i} + \frac{x}{r_i}) + \sigma_{w_i}\frac{1}{r_i}\right)$$
$$\cdot\left(\rho + \rho_x x + \rho_v v + \sum_{i=1}^{q} \rho_{r_i} r_i + \rho_{s_i}(\frac{m_i v}{r_i} + \frac{x}{r_i}) + \rho_{w_i}\frac{1}{r_i}\right)$$
$$=\left(\mu + \mu_x x + \mu_v v + \sum_{i=1}^{q} \mu_{r_i} r_i + \mu_{s_i}(\frac{m_i v}{r_i} + \frac{x}{r_i}) + \mu_{t_i}(\frac{m_i v^2}{r_i^2} + \frac{xv}{r_i^2} + \frac{1}{r_i}) + \mu_{w_i}\frac{1}{r_i}\right)v + x.$$

The term $\frac{1}{r_j^2}$ gives us $\sigma_{w_j}\rho_{w_j} = 0$ since all other terms involving r_j^{-2} are multiplied by powers of x or v. With $\sigma_{w_j} \neq 0$ this means $\rho_{w_j} = 0$. Similarly, the terms $\frac{1}{r_i r_j}$ give us $\sigma_{w_i}\rho_{w_j} + \sigma_{w_j}\rho_{w_i} = \sigma_{w_j}\rho_{w_i} = 0$ yielding $\rho_{w_i} = 0$ for all i.

The term $\frac{x}{r_j^2}$ now gives us $\sigma_{w_j}\rho_{s_j} = 0$ and therefore $\rho_{s_j} = 0$. The terms $\frac{x}{r_i r_j}$ give us $\sigma_{w_i}\rho_{s_j} + \sigma_{w_j}\rho_{s_i} = \sigma_{w_j}\rho_{s_i} = 0$ and therefore $\rho_{s_i} = 0$ for all i.

The term $\frac{1}{r_j}$ gives us $\sigma_{w_j}\rho = 0$ and therefore $\rho = 0$. The term $\frac{x}{r_j}$ now gives us $\sigma_{w_j}\rho_x = 0$ and therefore $\rho_x = 0$.

The constant term gives us $\sigma_{w_j}\rho_{r_j} = 0$ and therefore $\rho_{r_j} = 0$. The terms $\frac{r_i}{r_j}$ give us $\sigma_{w_j}\rho_{r_i} = 0$ and therefore $\rho_{r_i} = 0$ for all i.

We now have $r = \rho_v v$ giving us $sr = \rho_v sv = mv + x$. Since signing queries only increase the degree of v this equation cannot be satisfied because of the x. The contradiction leads us to conclude $\sigma_{w_i} = 0$ for $i = 1, \ldots, q$. By symmetry this also shows $\rho_{w_i} = 0$ for all $i = 1, \ldots, q$.

4 Optimal one-time signatures

The construction of a 3-element structure-preserving signature scheme in Sect. 3 leaves open the question whether 2-element one-time signatures exist. (A one-time signature scheme with 3-element signatures already exists in the symmetric setting [6]. It is sEUF-CMA under the simultaneous double-pairing assumption.) We will now give a candidate for an sEUF-CMA secure one-time structure-preserving signature scheme in the symmetric setting, which matches the 2-element lower bound from Sect. 5. This one-time signature beats the 3-element lower bound for general structure-preserving signatures in Theorem 5. Moreover, the scheme is deterministic, so it also demonstrates that Lemma 1 requiring general structure-preserving signatures to be randomized does not apply to one-time signatures.

The case of one-time signatures also indicates a difference between the symmetric and the asymmetric Type III setting. Abe et al. [4] constructed a one-time signature scheme with a single verification equation for messages belonging exclusively to one of the groups $\mathbb{G}_1$ or $\mathbb{G}_2$ and in Sect. 4.1 we show that it is even possible to make 1 element signatures in Type III groups. On the other

hand, there is no known structure-preserving (one-time) signature scheme in the asymmetric setting for messages that contain groups elements in both $\mathbb{G}_1$ and $\mathbb{G}_2$ with signature size less than 3.

The construction of our one-time signature is given in Fig. 2. We observe that the verification key has two group elements V, W and the signer needs to know the discrete logarithm of both of these elements. It is an interesting question whether a 2-element structure-preserving one-time signature scheme can be constructed with just a single variable verification key element like we did for 3-element signatures in Fig. 1, but we have some initial indications (not included in this paper) that for some classes of one-time signature schemes this may not be possible and that the signer needs to know at least two discrete logarithms.

Setup $\mathcal{P}(1^k)$**:** Run $(p, \mathbb{G}, \mathbb{G}_T, e, G) \leftarrow \mathcal{G}(1^k)$ and return $PP = (p, \mathbb{G}, \mathbb{G}_T, e, G)$.
Key generation $\mathcal{K}(PP)$**:** Choose $v, w \leftarrow \mathbb{Z}_p$ and compute

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

Return $(VK, SK) = ((PP, V, W), (PP, v, w))$.
Signing $\mathcal{S}_{SK}(M)$**:** Given $M \in \mathbb{G}$, return the signature $\Sigma = (S, T)$ given by:

$$S = M^v G^{w^2}, \qquad T = S^v.$$

Verification $\mathcal{V}_{VK}(M, (S, T))$**:** Accept if all the input elements are in $\mathbb{G}$ and if:

$$e(S, G) = e(M, V)e(W, W) \quad \text{and} \quad e(T, G) = e(S, V).$$

Fig. 2. One-time structure-preserving signature scheme in the symmetric setting.

Theorem 2. *The scheme given in Fig. 2 is an* sEUF-CMA *secure one-time signature scheme in the generic group model.*

Proof. A generic adversary only uses generic group operations, which means that in $\mathbb{G}$ it can only compute linear combinations on group elements from the verification key or the signature from the one-time chosen message attack. We will show that linear combinations of verification key elements and signature elements correspond to formal polynomials (of degree 3 or less) in the corresponding discrete logarithms of these elements and that no linear combinations will produce formal polynomials corresponding to a forgery. By the master theorem in [11] this means that the signature scheme is secure in the generic group model.

Suppose the adversary gets a one-time signature (S, T) on a query M and then outputs a valid signature (S^*, T^*) on M^*. Since the adversary is generic it computes M^*, S^*, T^* as linear combinations of G, V, W, S, T. This means the

discrete logarithms are of the form

$$m^* = \mu + \mu_v v + \mu_w w + \mu_s(mv + w^2) + \mu_t(mv^2 + w^2 v)$$
$$s^* = \sigma + \sigma_v v + \sigma_w w + \sigma_s(mv + w^2) + \sigma_t(mv^2 + w^2 v)$$
$$t^* = \tau + \tau_v v + \tau_w w + \tau_s(mv + w^2) + \tau_t(mv^2 + w^2 v)$$

where m itself is a linear combination of $1, v, w$.

The second verification equation $t^* = s^* v = m^* v^2 + w^2 v$ gives us

$$\tau + \tau_v v + \tau_w w + \tau_s(mv + w^2) + \tau_t(mv^2 + w^2 v)$$
$$= \mu v^2 + \mu_v v^3 + \mu_w w v^2 + \mu_s(mv^3 + w^2 v^2) + \mu_t(mv^4 + w^2 v^3) + w^2 v$$

The coefficients of $w^2 v^3$ give us $\mu_t = 0$. The coefficients of $w^2 v$ give us $\tau_t = 1$. The coefficients of w^2 give us $\tau_s = 0$. The coefficients of $w^2 v^2$ give us $\mu_s = 0$. The coefficients of $1, v, w$ give us $\tau = 0, \tau_v = 0, \tau_w = 0$. This means $mv^2 = \mu v^2 + \mu_v v^3 + \mu_w w v^2$, which implies $m = \mu + \mu_v v + \mu_w w = m^*$. Since the verification equations uniquely determined the signature once the message is fixed, $m^* = m$ implies $s^* = s$ and $t^* = t$. This means $(M^*, S^*, T^*) = (M, S, T)$, which was the message and signature pair from the query. □

4.1 Optimal one-time signatures in the Type III setting

In Fig. 3, we present a one-time signature scheme over asymmetric bilinear groups with single element signatures. It can be used to sign vectors of n group elements in the second base group $\mathbb{G}_2$.

Setup $\mathcal{P}(1^k)$**:** Return $PP = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G, H)$ generated by asymmetric bilinear group generator $\mathcal{G}(1^k)$.

Key generation $\mathcal{K}(PP)$**:** Choose $v, a_1, \ldots, a_n \leftarrow \mathbb{Z}_p$ and compute:

$$V = G^v, \quad A_1 = G^{a_1}, \quad \ldots, \quad A_n = G^{a_n}.$$

Return $(VK, SK) = ((PP, V, A_1, \ldots, A_n), (PP, v, a_1, \ldots, a_n))$.

Signing $\mathcal{S}_{SK}(\boldsymbol{M})$**:** On input $\boldsymbol{M} = (M_1, \ldots, M_n) \in \mathbb{G}_2^n$, return the signature:

$$S \leftarrow H^v \prod_{i=1}^{n} M_i^{a_i}.$$

Verification $\mathcal{V}_{VK}((M_1, \ldots, M_n), S)$**:** Accept if $M_1, \ldots, M_n, S \in \mathbb{G}_2$ and if:

$$e(G, S) = e(V, H) \prod_{i=1}^{n} e(A_i, M_i).$$

Fig. 3. One-time structure-preserving signature with 1 element signatures in the Type III setting.

Theorem 3. *The scheme given in Fig. 3 is an* sEUF-CMA *secure one-time signature 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 $(M_1, \ldots, M_n) = (H^{m_1}, \ldots, H^{m_n})$ with known discrete logarithms $m_1, \ldots, m_n$. The generic adversary gets a signature $S = H^{v+\sum_{i=1}^{n} a_i m_i}$ as response.

Suppose now the generic adversary computes a message $(M_1^*, \ldots, M_n^*) = (H^{m_1^*}, \ldots, H^{m_n^*})$ and a valid signature $S^* = H^{s^*}$. Since the adversary only uses linear combinations of existing group elements it knows $\mu_1, \ldots, \sigma_s \in \mathbb{Z}_p$ such that

$$m_j^* = \mu_j + \mu_{s,j}(v + \sum_{i=1}^{n} m_i a_i) \qquad \text{for } j \in \{1, \ldots, n\}$$
$$s^* = \sigma + \sigma_s(v + \sum_{i=1}^{n} m_i a_i).$$

The verification equation gives us $s^* = v + \sum_{i=1}^{n} a_i m_i^*$. This means:

$$(\sigma_s - 1)v = -\sigma - \sigma_s \sum_{j=1}^{n} m_j a_j + \sum_{j=1}^{n} \mu_j a_j + \sum_{j=1}^{n} \mu_{s,j} a_j (v + \sum_{i=1}^{n} m_i a_i).$$

It then holds that $\sigma_s = 1$, $\sigma = 0$, $\mu_j = m_j$ and $\mu_{s,j} = 0$ for all j. This means $m_j^* = m_j$ and $s^* = s$, so $((M_1^*, \ldots, M_n^*), S^*) = ((M_1, \ldots, M_n), S)$, which is not a valid forgery. □

5 Lower Bounds in the Symmetric Setting

We will show that in the Type I setting structure-preserving signatures must have at least two verification equations and consist of at least three group elements. This matches the lower bounds in the Type III setting [4]. One-time signature can be just two group elements but still require two verification equations. Our lower bounds hold even when the verification key may also include target group elements $Z \in \mathbb{G}_T$, and the security is relaxed to random message attacks.

Theorem 4. (No one-equation signatures) *The verification algorithm $\mathcal{V}$ of a (one-time)* EUF-RMA *secure structure-preserving signature scheme over a symmetric pairing group must evaluate at least two pairing product equations.*

Proof. By diagonalizing the corresponding quadratic form, we may assume without loss of generality that the single verification equation for a signature $\Sigma = (S_1, \ldots, S_n)$ on a one-element message M has the following form:

$$e(M, M)^a \cdot e(M, U \prod_{i=1}^{n} S_i^{b_i}) \cdot \prod_{i=1}^{n} e(S_i, S_i)^{c_i} \cdot e(S_i, V_i) = Z. \tag{1}$$

Let us fix an arbitrary message $M \in \mathcal{G}$ and a signature $\Sigma = (S_1, \ldots, S_n)$ on M which is valid with respect to the verification equation (1). We will construct an explicity forgery (M^*, Σ^*) such that Σ^* coincides with Σ on all components except one. We distinguish between two cases: either all the coefficients c_i in the verification equation (1) are nonzero or at least one of the c_i's is zero.

Case 1: $c_i \neq 0$ for all i. We first assume that all the c_i's are nonzero, and fix an arbitrary index $i \in \{1, \ldots, n\}$. Let M be any message and $\Sigma = (S_1, \ldots, S_n)$ a valid signature on M. We concentrate on the component $S = S_i$ of Σ, and claim that we can find a pair $(M^*, S^*) \neq (M, S)$ such that $\Sigma^* = (S_1, \ldots, S_{i-1}, S^*, S_{i+1}, \ldots, S_n)$ is a valid signature on M^*. In terms of discrete logarithms, this is equivalent to finding $(m^*, s^*) \neq (m, s)$ such that:

$$am^2 + m(u + bs + k) + cs^2 + sv = am^{*2} + m^*(u + bs + k) + cs^{*2} + s^*v \quad (2)$$

where we let $b = b_i$, $c = c_i$, $V = V_i$, and $K = \prod_{j \neq i} S_j^{b_j}$. To find such a pair, we look for m^*, s^* of the form:

$$m^* = \mu_0 u + \mu_1 v + (1 + \mu_2)m + \mu_3 s + \mu_4 k,$$
$$s^* = \sigma_0 u + \sigma_1 v + \sigma_2 m + (1 + \sigma_3)s + \sigma_4 k.$$

such that equation (2) is satisfied regardless of the discrete logarithms, i.e. such that the corresponding coefficients of the left-hand side and right-hand side of equation (2), when regarded as polynomials in $\mathbb{Z}_p[u, v, m, s, k]$, are pairwise equal.

This gives a quadratic system of 15 equations in the 10 unknowns $\mu_0, \ldots, \mu_4$, $\sigma_0, \ldots, \sigma_4$, which we solve by computing a Gröbner basis of the corresponding ideal. We obtain, in particular, a rational one-parameter family of solutions. Let ω be any element in $\mathbb{Z}_p$ such that $\tau = b^2 - 4ac - \omega^2 \neq 0$. Then the following is a solution:

$$(\mu_0, \mu_1, \mu_2, \mu_3, \mu_4) = 2/\tau \cdot \big(2c, \omega - b, b\omega - \delta, 2c\omega, 2c\big)$$
$$(\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4) = (\omega - b)/(c\tau) \cdot \big(2c, \omega - b, b\omega - \delta, 2c\omega, 2c\big)$$

(where $\delta = b^2 - 4ac$) and defines corresponding group elements (M^*_ω, S^*_ω).

This is a successful forgery provided that we can find some ω such that $M \neq M^*_\omega$. Suppose that this is not the case. Then for all ω such that $\tau \neq 0$, we must have:

$$M^*_\omega \cdot M^{-1} = U^{\mu_0} \cdot V^{\mu_1} \cdot M^{\mu_2} \cdot S^{\mu_3} \cdot K^{\mu_4} = 1.$$

By raising to the power $\tau/2$, this gives:

$$U^{2c} V^{\omega - b} M^{b\omega - b^2 + 4ac} S^{2c\omega} K^{2c} = \big(VM^b S^{2c}\big)^\omega \cdot \big(U^{2c} V^{-b} M^{-b^2 + 4ac} K^{2c}\big) = 1,$$

and since this relation is verified for all $\omega \in \mathbb{Z}_p$ except at most two values, this implies in particular that $VM^bS^{2c} = 1$, or in other words $S = V^{-1/2c} \cdot M^{-b/2c}$. Now recall that all the c_i's are nonzero. By the previous argument, we can either carry out the previous attack for at least one index i, or the signature on a message M must be given, with overwhelming probability, by $\Sigma = (S_1, \ldots, S_n)$ where $S_i = V_i^{-1/2c_i} \cdot M^{-b_i/2c_i}$ for all i, which is obviously insecure.

Case 2: $c_i = 0$ for some i. Suppose $c_i = 0$ for some i. We concentrate on that index like before, and look again for a forgery (M^*, S^*) given a signature Σ on an arbitrary message M. With the same notation as before, we find a one-parameter family (M^*_ω, S^*_ω) of solutions, given by:

$$(\mu_0, \mu_1, \mu_2, \mu_3, \mu_4) = -\omega/(b\omega + 1) \cdot \big(0, 1, b, 0, 0\big)$$
$$(\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4) = \omega \cdot \big(1, -a\omega/(b\omega + 1), a(b\omega + 2)/(b\omega + 1), b, 1\big)$$

for all ω such that $b\omega + 1 \neq 0$. This gives a forgery unless $M^*_\omega = M$ for all such ω, namely $(VM^b)^{-\omega/(b\omega+1)} = 1$. As a result, we get a forgery on any message except $V^{-1/b}$ (or any message if $b = 0$). This completes the proof. □

Corollary 1. (Two group elements required for one-time signatures.) *A structure-preserving one-time signature scheme that is existentially unforgeable against a one-time random message attack must have at least 2 group elements.*

Proof. Suppose there is a scheme where a signature is a single group element S. If a linear combination of the verification equations give us a non-trivial equation that is linear in S, then this equation uniquely determines S and we can just use this equation as the verification equation instead of all the other verification equations. If there is no linear combination of the verification equations that yield a non-trivial linear equation in S then they must all be linearly dependent and we can again reduce to the case where there is a single verification equation. □

For structure-preserving signatures where the adversary can ask multiple signature queries there is a stronger lower bound of 3 group elements.[4]

Theorem 5. (Three group elements required for structure-preserving signatures.) *A structure-preserving signature scheme with a generic signer that is existentially unforgeable against random message attacks must have at least 3 group elements.*

Proof. We begin by proving the following lemma.

Lemma 1. *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 there are only polynomially many signature vectors Σ. Since the signer is generic this means there is a polynomial set $\{(\vec{\alpha}, \vec{\beta})\}_{i=1}^{\mathrm{poly}(k)}$ of vectors in $\mathbb{Z}_p^n$ creating signature vectors $\Sigma = G^{\vec{\alpha}} M^{\vec{\beta}}$ by entry-wise exponentiation. Given signatures Σ_0 and Σ_1 on random messages M_0 and

[4] Our proof of the lower bound is much simpler than the proof for the similar lower bound of 3 group elements in [4] in the asymmetric Type III setting and can with minor modifications be adapted to Type III groups. More generally, the proof of Theorem 5 indicates that in general if there are m verification equations, then the signature size needs to be $m + 1$.

M_1 we have $\frac{1}{\text{poly}(k)^2}$ probability that they are constructed with the same $(\vec{\alpha}, \vec{\beta})$ pair. In that case

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

is a signature on $M^* = M_0^r M_1^{1-r}$ for all $r \in \mathbb{Z}_p$. □

Now suppose that we have an SPS with just two group elements (S, T) and a minimal number of verification equations. We know there must be at least two verification equations. This means the discrete logarithms s, t of the signature elements must satisfy two quadratic equations. By using a linear combination of the two verification equations, we can without loss of generality ensure the first equation is linear in t, i.e., $t = as^2 + bs + c$ for some $a, b, c \in \mathbb{Z}_p$ determined by the message and the verification key. We can then substitute this into the second verification equation to get a quartic equation in s. If the equation is non-trivial, then there are at most 4 solutions for s and therefore at most 4 signatures in total contradicting Lemma 1. On the other hand if the equation is trivial, then the second verification equation was redundant and could be eliminated, which contradicts our initial assumption that we had a minimal number of verification equations. □

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. Springer, 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. Springer, 2011.
6. M. Abe, K. Haralambiev, and M. Ohkubo. Signing on group elements for modular protocol designs. IACR ePrint Archive, Report 2010/133, 2010. `http://eprint.iacr.org`.
7. M. Abe, K. Haralambiev, and M. Ohkubo. Efficient message space extension for automorphic signatures. In *ISC 2010*, volume 6531 of *LNCS*, pages 319–330. Springer, 2011.
8. 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.

9. 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.
10. R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé. A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. IACR ePrint Archive, Report 2013/400, 2013. `http://eprint.iacr.org/`.
11. D. Boneh and X. Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. *J. Cryptology*, 21(2):149–177, 2008.
12. 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.
13. 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. Springer, 2009.
14. 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.
15. G. Fuchsbauer. Automorphic signatures in bilinear groups. IACR ePrint Archive, Report 2009/320, 2009. `http://eprint.iacr.org`.
16. G. Fuchsbauer. Commuting signatures and verifiable encryption. In K. G. Paterson, editor, *EUROCRYPT*, volume 6632 of *LNCS*, pages 224–245. Springer, 2011.
17. 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.
18. S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–3121, 2008.
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. Springer, 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. D. Hofheinz, T. Jager, and E. Knapp. Waters signatures with optimal security reduction. In M. Fischlin, J. Buchmann, and M. Manulis, editors, *PKC*, volume 7293 of *LNCS*, pages 66–83. Springer, 2012.
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*, volume 8042 of *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. 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.
27. S. Zhou and D. Lin. Unlinkable randomizable signature and its application in group signature. In D. Pei, M. Yung, D. Lin, and C. Wu, editors, *Inscrypt*, volume 4990 of *LNCS*, pages 328–342. Springer, 2007.