Lower Bounds on Structure-Preserving Signatures for Bilateral Messages

Masayuki Abe[1(✉)], Miguel Ambrona[2], Miyako Ohkubo[3], and Mehdi Tibouchi[1]

[1] Secure Platform Laboratories, NTT Corporation, Tokyo, Japan
{abe.masayuki,tibouchi.mehdi}@lab.ntt.co.jp
[2] IMDEA Software Institute & Universidad Politécnica de Madrid, Madrid, Spain
miguel.ambrona@imdea.org
[3] Security Fundamentals Lab, CSRI, NICT, Tokyo, Japan
m.ohkubo@nict.go.jp

Abstract. Lower bounds for structure-preserving signature (SPS) schemes based on non-interactive assumptions have only been established in the case of *unilateral* messages, i.e. schemes signing tuples of group elements all from the same source group. In this paper, we consider the case of *bilateral* messages, consisting of elements from both source groups. We show that, for Type-III bilinear groups, SPS's must consist of at least 6 group elements: many more than the 4 elements needed in the unilateral case, and optimal, as it matches a known upper bound from the literature. We also obtain the first non-trivial lower bounds for SPS's in Type-II groups: a minimum of 4 group elements, whereas constructions with 3 group elements are known from interactive assumptions.

Keywords: Structure-preserving signatures · Bilateral messages
Crucial relation

1 Introduction

Background. A structure-preserving signature (SPS) scheme is a useful building block for cryptographic protocol design over bilinear groups. In SPS, signatures, messages and public-keys consist exclusively of source group elements of bilinear groups and their sizes are measured by the number of them. Since the signature size greatly impacts the efficiency of the accompanied proofs and the resulting protocol, it is of a great interest to investigate possible lower bounds for the signature size and to construct schemes that achieve these bounds. Table 1 summarizes known lower and upper bounds for the size of structure-preserving signatures over different settings.

Research on lower bounds for structure preserving signatures was initiated in [4], where the authors investigate the case of asymmetric bilinear groups (Type-III groups [16]) where no efficient morphisms are known between the source groups, $\mathbb{G}_1$ and $\mathbb{G}_2$. For schemes defined for *unilateral* messages (that belong to only one of the source groups), matching lower and upper bounds are known

D. Catalano and R. De Prisco (Eds.): SCN 2018, LNCS 11035, pp. 3–22, 2018.
https://doi.org/10.1007/978-3-319-98113-0_1

Table 1. Bounds on the signature size of structure-preserving signature schemes. See discussion in Sect. 5 for entries with †,‡,§.

Setting	Messages	Lower bounds		Upper bounds (constructions)		
		Interactive	Non-interactive	Interactive	Non-interactive	
					q-type	Static
Type-III	Unilateral	3 [4]	4 [5]	3 [4]	4 [4]	6 [22]
	Bilateral	3 [4]	6 (this work)	3 [4]	6 [4]	10 [23]
Type-II	$M \in \mathbb{G}_1$	3 [6]	4 (this work)	3 [8]	7 [3]‡	9 [22]§
	$M \in \mathbb{G}_2$	2 [6]		2 [6]	3 [6]	9 [22]§
	Bilateral	3 [8]	4 (this work)	7 [3]†	7 [3]‡	9 [22]§
Type-I	N/A	3 [8]		3 [8]	7 [3]	9 [22]

(w.r.t. both interactive and non-interactive assumptions). In the case of *bilateral* messages (that contain elements from both source groups), a construction is shown in [4] based on non-interactive assumption, but no lower bounds are provided to argue its optimality. In [8], the authors investigate the case of symmetric bilinear groups (Type-I groups) where $\mathbb{G}_1 = \mathbb{G}_2$, and present matching lower and upper bounds w.r.t. interactive assumptions. Their results are valid as well for asymmetric bilinear groups with an efficient morphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ (Type-II groups) for some message types. The analysis over Type-II groups considering interactive assumptions is continued by [6] where the authors present matching bounds for unilateral messages with an 'unexpected' gap between messages in $\mathbb{G}_1$ and $\mathbb{G}_2$. Nothing was known w.r.t. non-interactive assumptions in Type-II.

In summary, all known lower bounds are about schemes with *unilateral messages* or being secure under *interactive assumptions*. To the best of our knowledge, nothing has been shown for the case of *bilateral messages* and *non-interactive assumptions*, though this is the most general and preferred case in the context of structure-preserving signatures. Efficient and trustworthy constructions (based on *weak assumptions*) in this more general setting are desired, as they play an important role in the modular design of cryptographic primitives.

Our Results. We present lower bounds on the signature size of structure-preserving signature schemes over asymmetric bilinear groups signing bilateral messages and being secure based on non-interactive assumptions.

– **A tight lower bound for bilateral messages in Type-III groups.** As illustrated in Table 1, this constitutes the last missing piece for structure preserving signatures over Type-III groups. We show that secure signatures for bilateral messages must contain at least 6 group elements as long as the underlying assumption is non-interactive (see Sect. 3). More concretely, we show that a signature scheme signing bilateral messages cannot be proved to be EUF-CMA by a black-box algebraic reduction to any non-interactive assumption if the signatures contain less than 3 group elements in one of the

source groups and 3 in the other. Our lower bound matches an existing upper bound from [4]. Our result allows us to claim the optimality of that scheme.

– **Lower bounds for unilateral messages in $\mathbb{G}_1$ and bilateral messages in Type-II groups.** These are the first non-trivial lower bounds for Type-II groups involving non-interactive assumptions. We first show that when signing unilateral messages in $\mathbb{G}_1$, signatures must contain at least 4 group elements (see Sect. 4). Note that the lower bound for unilateral messages in $\mathbb{G}_1$ implies the same lower bound for bilateral messages That is because there exists a reduction from bilateral to unilateral messages in $\mathbb{G}_1$. However, this reduction is valid only if messages belong to $\mathbb{G}_1^{k_1} \times \mathbb{G}_2^{k_2}$ for some fixed $k_1, k_2 \in \mathbb{N}$ and the underlying scheme supports messages in $\mathbb{G}_1^{k_1+k_2}$. For our purpose, it is sufficient to show a lower bound for schemes that sign messages consisting of only one group element in $\mathbb{G}_1$ since such a result would also apply to those with larger message spaces. The result is unfortunately not known to be optimal as corresponding upper bounds are missing. We further discuss this point in Sect. 5.

Our approach follows the framework of [5], i.e., we show the existence of a *crucial relation* (see Sect. 2.3) in the algebraic model [10,14]. It is known that if such a relation exists, a meta-reduction [12] can be constructed and the considered scheme cannot be proven under non-interactive assumptions. Having messages in both source groups or having a morphism from one group to the other makes the analysis more complex. We elaborate this point as follows. We first recap the argument used in [5]. Consider a SPS scheme over Type-III groups that yields 3-element signatures, (R, S, T), for unilateral single-element message M in $\mathbb{G}_1$. For the scheme to be secure, at most two elements in the signature, say R and S, must be in the same group as M. Thus, every pairing product equation can be written as

$$e(R, U_1 T^a)\, e(S, U_2 T^b)\, e(M, U_3 T^c)\, e(V, T) \;= Z \tag{1}$$

with parameters a, b, c, and public-key elements U_i, V and Z that may be different in every equation. A reduction algorithm $\mathcal{R}$ is given an instance of a non-interactive assumption and simulates signatures for certain messages. Let G and H be generators for $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. When $\mathcal{R}$ is algebraic, the signature (R, S, T) for message M must be computed as

$$R = G^{\varphi_r} M^{\alpha_r},\; S = G^{\varphi_s} M^{\alpha_s},\; T = H^{\varphi_t} \tag{2}$$

for some variables α_r, α_s, φ_r, φ_s, and φ_t taking values in $\mathbb{Z}_p$. Actually, G^{φ_r}, G^{φ_s} and H^{φ_t} are linear combinations of group elements in the given problem instance. Therefore $\varphi_r, \varphi_s, \varphi_t$ may not be known by $\mathcal{R}$. By substituting (R, S, T) in every verification equation of the form of (1) and taking logarithm for base $e(G, H)$, we get a system of equations in the above variables. Roughly, to show that $\mathcal{R}$ will never be successful in breaking the assumption, it is necessary to show that (α_r, α_s), called the *crucial information*, is uniquely identified. If this is done, (α_r, α_s) can be extracted and used to simulate a valid forgery. The overall

argument is not extremely intricate as the obtained equations are *linear* in the crucial information (α_r, α_s). The difficulty significantly increases when applying the above procedure to show that at least 6 elements are necessary for signing bilateral messages (M, N) in $\mathbb{G}_1 \times \mathbb{G}_2$ of Type-III groups.

In the case of Type-II groups with unilateral messages in $\mathbb{G}_1$, the difficulty comes from the presence of an efficient morphism $\phi : \mathbb{G}_1 \to \mathbb{G}_2$. Observe that verification equations for 3-element signatures (R, S, T) on message $M \in \mathbb{G}_1$ will be of the form $e(R, U_1 T^a)\, e(S, U_2 T^b)\, e(M, U_3 T^c)\, e(\phi(T), U_4 T^d)\, e(U_5, T) = Z$ for $(R, S, T) \in \mathbb{G}_1^2 \times \mathbb{G}_2$. When representing (R, S, T) as in (2), the resulting system of equations w.r.t. the crucial information (α_r, α_s) is linear, although it includes the quadratic term φ_t^2, coming from $e(\phi(T), T)$, and this makes the analysis slightly more involved than the one from [5]. In our actual proof in Sect. 4, we address a more general case where the signature element T (in the opposite group to M) consists of an arbitrary number of elements $T_1, \ldots, T_\ell$. In this way, we handle all cases where signatures include less than three elements, at once.

Other Related Works. There exist variations and extensions of SPS for which the lower bounds appearing in Table 1 do not hold. For example, for one-time SPS schemes, there are constructions, e.g., [3,7], whose signature consists of one or two group elements and their security is based on static assumptions. In [19,20], the authors circumvent these bounds by considering messages in a special form (messages are bound by the Diffie-Hellman relation) and construct a SPS scheme over Type-III groups with two group elements in each signature.

Upper bounds are frequently being improved in the literature [2,22–24]. The state of the art for static assumptions and Type-III groups is a scheme from [22] with six-elements signatures for unilateral messages. For bilateral messages, a scheme presented in [23] yields 10-elements signatures. However, we point out that combining the scheme from [22] for messages in $\mathbb{G}_1$ with a partially one-time SPS from [2] for messages in $\mathbb{G}_2$, results in a scheme for bilateral messages with 9 signature elements. A randomizable SPS scheme in [18] can be seen as an alternative scheme whose signature size matches the lower bound of three group elements in Type-III groups based on an interactive assumption. For Type-I groups, the generic construction from [22] yields a scheme with the smallest signature size of 9 when the underlying MDDH assumption [13] is instantiated with the DLIN assumption [9] adjusted to Type-I groups [2].

Structure-preserving signatures over Type-II groups received less attention, even though GS-proofs had been extended to Type-II groups [21]. This may be due to [6] that shows how the one-way morphism between source groups can be exploited in cryptographic designs. Note that significant gaps in signature size exist between Type-II and Type-III settings. However, as pointed out in [11], a smaller signature size does not necessarily imply that a scheme in Type-II is computationally more advantageous than its analogues scheme in Type-III when the cost of membership testing is taken into account. That is why, comparisons should be performed within the same group setting of bilinear groups.

2 Preliminaries

2.1 Signature Schemes, Bilinear Groups, and Algebraic Algorithm

In this section we briefly review notations and standard notions used throughout the paper. Due to the page restriction, we refer to [5], which our work is based on, for more formal definitions.

Let $\mathcal{G}$ be a generator of bilinear groups that takes security parameter 1^λ as input and outputs $\Lambda := (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$, where p is a λ-bit prime and $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are groups of order p with efficiently computable group operations, membership tests, and bilinear mapping $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. An equation of the form $\prod_i \prod_j e(A_i, B_j)^{a_{ij}} = Z$ for constants $a_{ij} \in \mathbb{Z}_p, Z \in \mathbb{G}_T$, and constants or variables $A_i \in \mathbb{G}_1$, $B_j \in \mathbb{G}_2$ is called a pairing product equation (PPE). Symmetric bilinear groups refer the case where $\mathbb{G}_1 = \mathbb{G}_2$ and they are called Type-I groups. The case where $\mathbb{G}_1 \neq \mathbb{G}_2$ is known as are asymmetric groups. When no efficient morphism is provided for either direction between $\mathbb{G}_1$ and $\mathbb{G}_2$, the groups are called Type-III. If there is an efficient morphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, they are said to be in Type-II setting. See [16] for their properties.

A signature scheme consists of polynomial-time algorithms $(\mathcal{C}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ where $\mathcal{C}$ generates common parameters GK, $\mathcal{K}$ generates a pair of public and private keys, $\mathcal{S}$ is a signing algorithm and $\mathcal{V}$ is the verification algorithm. It is called structure preserving w.r.t. bilinear group generator $\mathcal{G}$ if the common parameter GK consists of a group description Λ and some constants a_{ij} in $\mathbb{Z}_p$, and public keys, messages, and signatures consist of group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$, and verification algorithm $\mathcal{V}$ evaluates membership in $\mathbb{G}_1$ and $\mathbb{G}_2$ and PPEs. A SPS scheme is considered secure if it is existentially unforgeable against adaptive chosen message attacks (EUF-CMA). It is assumed that there exists an efficiently computable key verification algorithm $TstVk$ that takes λ and VK as input and checks the validity of VK s.t. if $0 \leftarrow TstVk(1^\lambda, VK)$, then $\mathcal{V}(VK, *, *)$ always returns 0, and if $1 \leftarrow TstVk(1^\lambda, VK)$ then the message space Msp is well defined and it is efficiently and uniformly sampleable. A signature Σ is considered *valid* (w.r.t. VK and M), if $1 = \mathcal{V}(VK, M, \Sigma)$. Otherwise, it is said to be *invalid*.

An algorithm is called algebraic w.r.t. a group if it takes a vector of elements $\boldsymbol{X}$ in the group and outputs a group element Y and there is a corresponding algorithm called an extractor that can output the representation of Y w.r.t. $\boldsymbol{X}$. For instance, if the algebraic algorithm $\mathcal{R}$ takes source group elements A, B as input and outputs element C in the same group, then $\mathcal{R}$'s extractor $\mathcal{E}$ outputs (a, b) such that $C = A^a B^b$. It does not matter how $\mathcal{R}$ has computed a and b. For instance, a can be a bit-slice of some group elements like Waters' Hash [26]. The notion can also be extended naturally to oracle algorithms. Thus, it covers a wide range of algorithms and frequently used [17,25]. For a formal definition, we refer to [5], which also argues the differences from the knowledge of exponent assumption. By $\mathtt{Cls}_{alg}$ we denote the set of all algebraic algorithms with respect to $\mathcal{G}$. With respect to source groups in asymmetric bilinear groups, group elements are separated if no efficient morphism exist. Suppose that $\mathbb{G}_1$ and $\mathbb{G}_2$ are source groups of Type-III and an algorithm takes $\boldsymbol{A}$ from $\mathbb{G}_1$ and $\boldsymbol{B}$ from $\mathbb{G}_2$

as input. If the algorithm outputs $Y \in \mathbb{G}_1$, there is an extractor that outputs a representation of Y w.r.t. $\boldsymbol{A}$, i.e. Y is independent of $\boldsymbol{B}$. Also, if $\mathbb{G}_1$ and $\mathbb{G}_2$ are Type-II groups, the extractor outputs representation w.r.t. $\boldsymbol{A}$ and also $\boldsymbol{B}$ mapped to $\mathbb{G}_1$.

2.2 Non-interactive Hardness Assumptions

Typically an assumption is defined in such a way that there is no efficient algorithm $\mathcal{A}$ that returns a correct answer with better probability than random guessing. The following definition follows this intuition.

Definition 1 (Algebraic Non-interactive Hardness Assumption). *A non-interactive problem consists of a triple of algorithms $\mathcal{P} = (\mathcal{I}, \mathcal{V}, \mathcal{U})$ where $\mathcal{I} \in \mathtt{PPT}$ is an instance generator, which takes 1^λ and outputs a pair of an instance and a witness, (ins, wit), and $\mathcal{V}$ is a verification algorithm that takes ins, wit and an answer ans, and outputs 1 or 0 that represents acceptance or rejection, respectively. A non-interactive hardness assumption for problem $\mathcal{P}$ is to assume that, for any $\mathcal{A} \in \mathtt{PPT}$, the following advantage function Adv is negligible in λ.*

$$\begin{aligned} Adv_{\mathcal{A}}(1^\lambda) = &\Pr[(ins, wit) \leftarrow \mathcal{I}(1^\lambda), ans \leftarrow \mathcal{A}(ins) \ : \ 1 = \mathcal{V}(ins, ans, wit)] \\ &- \Pr[(ins, wit) \leftarrow \mathcal{I}(1^\lambda), ans \leftarrow \mathcal{U}(ins) \ : \ 1 = \mathcal{V}(ins, ans, wit)] \end{aligned}$$

$\mathcal{P}$ is called algebraic if $\mathcal{I}$ also takes Λ generated by group generator $\mathcal{G}(1^\lambda)$ with uniformly chosen default generators $G \in \mathbb{G}_1$ and $H \in \mathbb{G}_2$ as a part of input, and there exists an efficient extractor $\mathcal{E}_{\mathcal{I}}$ that, given the same input as given to $\mathcal{I}$, outputs a representation of the element w.r.t. generator G or H with overwhelming probability.

In search problems, $\mathcal{U}$ is usually set to be an algorithm that returns constant $\perp$ (or a random answer *ans* when the domain is uniformly sampleable). In decision problems, $\mathcal{U}$ typically returns 1 or 0 randomly winning only with probability 1/2.

2.3 Crucial Relation

We briefly recap the framework of [5] and restate the impossibility theorem in slightly refined and specific form. Let $\mathtt{Cls}$ be a class of algorithms (we actually consider class of algebraic algorithm in this paper) and $\mathcal{R} \in \mathtt{Cls}$ be a reduction algorithm that, given an instance *ins* of a non-interactive hardness problem $\mathcal{P}$, outputs VK and a poly-size internal state φ. Given φ and messages $\boldsymbol{M} := (M_1, \ldots, M_n)$ for some $n > 0$, $\mathcal{R}$ outputs signatures $\boldsymbol{\Sigma} := (\Sigma_1, \ldots, \Sigma_n)$. Let θ be a transcript defined as $\theta := (VK, \boldsymbol{M}, \boldsymbol{\Sigma})$. A transcript θ is valid and witness as $1 = \mathcal{V}(\theta)$ if $1 = \mathcal{V}(VK, M_i, \Sigma_i)$ for all $i = 1, \ldots, n$. ($\mathcal{V}$ is supposed to reject if $TstVk(VK) \neq 1$).

In security proofs by reduction, it is often the case that the algorithm does not actually hold the secret key but has some *crucial information* to simulate

signatures. We model such information as a witness of a binary relation $\Psi(\theta, \varpi)$ that we call a *crucial relation* and define as follows.

Definition 2 (Crucial Relation). *Let $\mathsf{Sig} = (\mathcal{C}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ be a signature scheme and TstVk be a key verification algorithm for Sig. A binary relation $\Psi : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ is a crucial relation for Sig w.r.t. a class of algorithms $\mathtt{Cls}$ and $n > 0$ if the following properties are provided.*

Uniqueness: For every $\theta := (VK, \boldsymbol{M}, \boldsymbol{\Sigma})$ s.t. $1 = \mathcal{V}(\theta)$, there exists exactly one (polynomial size) ϖ fulfilling $1 = \Psi(\theta, \varpi)$.

Extractability: For any $\mathcal{R} \in \mathtt{Cls}$, there exists $\mathcal{E} \in \mathtt{PPT}$ s.t., for any $VK \in \{0,1\}^*$ s.t. $1 \leftarrow TstVk(1^\lambda, VK)$, and any arbitrary string φ in $1^\lambda || \{0,1\}^*$, probability

$$\Pr\left[\begin{array}{l} \boldsymbol{M} \leftarrow \mathsf{Msp}^n \\ \boldsymbol{\Sigma} \leftarrow \mathcal{R}(\varphi, \boldsymbol{M}; \gamma) \\ \varpi \leftarrow \mathcal{E}(\varphi, \boldsymbol{M}; \gamma) \\ \theta := (VK, \boldsymbol{M}, \boldsymbol{\Sigma}) \end{array} : \begin{array}{l} 1 = \mathcal{V}(\theta) \wedge \\ 1 \neq \Psi(\theta, \varpi) \end{array}\right] \tag{3}$$

is negligible in λ. The probability is taken over the choice of $\boldsymbol{M}$ and random coin γ given to $\mathcal{R}$ and $\mathcal{E}$.

Usefulness: There exists an algorithm $\mathcal{B} \in \mathtt{PPT}$ s.t., for any $\theta := (VK, \boldsymbol{M}, \boldsymbol{\Sigma})$ and ϖ that satisfies $\Psi(\theta, \varpi) = 1$, the following probability is not negligible in λ.

$$\Pr\left[(M, \Sigma) \leftarrow \mathcal{B}(\theta, \varpi) \ : \ \begin{array}{l} M \notin \boldsymbol{M} \wedge \\ 1 = \mathcal{V}(VK, M, \Sigma) \end{array}\right] \tag{4}$$

The intuition behind extractability is that whenever φ is helpful for $\mathcal{R}$ to compute valid signatures, the extractor $\mathcal{E}$ should be successful in extracting ϖ from φ. This must hold even for a non-legitimate VK as long as it is functional with respect to the verification. For an $\mathcal{R}$ which is successful in producing a valid θ only with negligible probability, $\mathcal{E}$ can be an empty algorithm.

Theorem 8 of [5]. *If a crucial relation for a signature scheme exists w.r.t. algebraic algorithms, then there exists no algebraic black-box reduction from the EUF-CMA security of the signature scheme to any non-interactive algebraic problems over groups where the discrete logarithm problem is hard.*

3 Tight Lower Bound for Bilateral Messages in Type-III

Theorem 1. *Any structure preserving signature scheme over asymmetric bilinear groups that yields signatures consisting of 2 or less group elements in either of the source groups and ℓ group elements in the other (for every $\ell \leq 3$), cannot have an algebraic black-box reduction for the EUF-CMA security to non-interactive hardness assumptions if pseudo-random functions exist and the discrete logarithm problem is hard in both source groups.*

Let $\mathcal{SIG}_{\tau,\ell}$ be the set of all structure preserving signature schemes in Type-III whose signature consists of at most τ group elements from one source group and at most ℓ elements from the other source group. We prove Theorem 1 by proving the following lemma and applying Theorem 8 of [5]. Note that *the absence of morphisms between source groups is used in the proof* via the algebraic model where the source group elements returned by any algebraic algorithm depend only on the elements from the same source group that were given to the algorithm as input.

Lemma 1. *For every $\ell \leq 3$ and every scheme in $\mathcal{SIG}_{2,\ell}$, there exists a crucial relation.*

The proof of Lemma 1 will be given by explicitly presenting a crucial relation (Definition 3) and showing that it satisfies the three required properties: *uniqueness, extractability and usefulness* (Lemma 2). Our proof is valid for arbitrary values of ℓ except for arguing extractability in one sub-case, when the condition $\ell \leq 3$ is required. When analyzing Lemma 1 we will consider, without loss of generality, the case where our scheme has signatures in $\mathbb{G}_1^2 \times \mathbb{G}_2^\ell$.

Before starting, we establish some useful notation for expressing signatures schemes in $\mathcal{SIG}_{2,\ell}$. These notation will be used throughout the proofs.

Observe that in every structure preserving signature scheme with signature space $\mathbb{G}_1^2 \times \mathbb{G}_2^\ell$, the j-th verification equation can be written in the following form:

$$e(R, U_1^{(j)} N^{d_1^{(j)}} \prod_{i=1}^{\ell} T_i^{a_i^{(j)}})\, e(S, U_2^{(j)} N^{d_2^{(j)}} \prod_{i=1}^{\ell} T_i^{b_i^{(j)}})$$
$$e(M, U_3^{(j)} N^{d_3^{(j)}} \prod_{i=1}^{\ell} T_i^{c_i^{(j)}})\, e(V_0^{(j)}, N) \prod_{i=1}^{\ell} e(V_i^{(j)}, T_i) = Z^{(j)} \quad (5)$$

where $(M, N) \in \mathbb{G}_1 \times \mathbb{G}_2$ is a message, $V_0^{(j)} \in \mathbb{G}_1$, for every $i \in \{1, 2, 3\}$, $V_i^{(j)} \in \mathbb{G}_1$, $U_i^{(j)} \in \mathbb{G}_2$, and $Z^{(j)} \in \mathbb{G}_T$ are elements in the verification key, and $(R, S, T_1, \ldots, T_\ell) \in \mathbb{G}_1^2 \times \mathbb{G}_2^\ell$ is a signature. Note that exponents $d_k^{(j)}, a_i^{(j)}, b_i^{(j)}, c_i^{(j)}$ for $k \in \{1, 2, 3\}$, $i \in \{1, \ldots, \ell\}$ are determined by the description of the scheme.

Note that, to show the impossibility, it is sufficient to consider messages in $\mathbb{G}_1 \times \mathbb{G}_2$ rather than its vector form. Also, observe that we allow arbitrary $Z^{(j)} \in \mathbb{G}_T$ in every verification equation j, for more generality. These are usually set to $1_{\mathbb{G}_T}$ in the strict definition of structure preserving signatures.

We denote the discrete-log of a group element w.r.t. the default generator by its small-case letter. For instance, $M = G^m$ and $N = H^n$. For elements R and S in a signature, we consider a special representation of the form $R = G^{\varphi_r} M^{\alpha_r}$, $S = G^{\varphi_s} M^{\alpha_s}$ for some $\varphi_r, \alpha_r, \varphi_s, \alpha_s$ in $\mathbb{Z}_p$. Now, by expressing the j-th verification Eq. (5) in the exponent, we have:

$$(\varphi_r + \alpha_r\, m)(u_1^{(j)} + \Sigma_{i=1}^{\ell} a_i^{(j)}\, t_i + d_1^{(j)}\, n) + (\varphi_s + \alpha_s\, m)(u_2^{(j)} + \Sigma_{i=1}^{\ell} b_i^{(j)}\, t_i + d_2^{(j)}\, n)$$
$$+ m\,(u_3^{(j)} + \Sigma_{i=1}^{\ell} c_i^{(j)}\, t_i + d_3^{(j)}\, n) + v_0^{(j)}\, n + \Sigma_{i=1}^{\ell} v_i^{(j)}\, t_i = z \quad (6)$$

By thinking of the j-th verification Eq. (6) as a polynomial in m, we have the following equation:

$$\begin{aligned} m\,\big\{&(u_1^{(j)} + \textstyle\sum_{i=1}^{\ell} a_i^{(j)}\, t_i + d_1^{(j)}\, n)\alpha_r + (u_2^{(j)} + \textstyle\sum_{i=1}^{\ell} b_i^{(j)}\, t_i + d_2^{(j)}\, n)\alpha_s \\ &+ (u_3^{(j)} + \textstyle\sum_{i=1}^{\ell} c_i^{(j)}\, t_i + d_3^{(j)}\, n)\big\} \\ +\big\{&(u_1^{(j)} + \textstyle\sum_{i=1}^{\ell} a_i^{(j)}\, t_i + d_1^{(j)}\, n)\varphi_r + (u_2^{(j)} + \textstyle\sum_{i=1}^{\ell} b_i^{(j)}\, t_i + d_2^{(j)}\, n)\varphi_s \\ &+ (v_0^{(j)}\, n + \textstyle\sum_{i=1}^{\ell} v_i^{(j)}\, t_i - z^{(j)})\big\} = 0 \end{aligned} \tag{7}$$

Claim 1. If the discrete-logarithm problem over $\mathbb{G}_1$ is hard, for all equations j, every coefficient of (7) as polynomial in m must be zero.

Proof. We refer to the full version of this paper for a proof [1]. □

Accordingly, for every verification equation j, the following two equations are fulfilled.

$$\begin{aligned} &(u_1^{(j)} + \textstyle\sum_{i=1}^{\ell} a_i^{(j)}\, t_i + d_1^{(j)}\, n)\alpha_r + (u_2^{(j)} + \textstyle\sum_{i=1}^{\ell} b_i^{(j)}\, t_i + d_2^{(j)}\, n)\alpha_s \\ &\quad + (u_3^{(j)} + \textstyle\sum_{i=1}^{\ell} c_i^{(j)}\, t_i + d_3^{(j)}\, n) = 0 \end{aligned} \tag{8}$$

$$\begin{aligned} &(u_1^{(j)} + \textstyle\sum_{i=1}^{\ell} a_i^{(j)}\, t_i + d_1^{(j)}\, n)\varphi_r + (u_2^{(j)} + \textstyle\sum_{i=1}^{\ell} b_i^{(j)}\, t_i + d_2^{(j)}\, n)\varphi_s \\ &\quad + (v_0^{(j)}\, n + \textstyle\sum_{i=1}^{\ell} v_i^{(j)}\, t_i - z^{(j)}) = 0 \end{aligned} \tag{9}$$

Now, we focus on message N. Let $T_i = H^{\gamma_i} N^{\beta_i}$, i.e., $t_i = \gamma_i + \beta_i n$. Note that, for each verification equation j, we can rewrite the relations (8) and (9) as polynomials in n by collecting the corresponding terms:

$$\begin{aligned} &\big\{(d_1^{(j)} + \textstyle\sum_{i=1}^{\ell} a_i^{(j)}\beta_i)\alpha_r + (d_2^{(j)} + \textstyle\sum_{i=1}^{\ell} b_i^{(j)}\beta_i)\alpha_s + (d_3^{(j)} + \textstyle\sum_{i=1}^{\ell} c_i^{(j)}\beta_i)\big\}n \\ +&\big\{(u_1^{(j)} + \textstyle\sum_{i=1}^{\ell} a_i^{(j)}\gamma_i)\alpha_r + (u_2^{(j)} + \textstyle\sum_{i=1}^{\ell} b_i^{(j)}\gamma_i)\alpha_s + (u_3^{(j)} + \textstyle\sum_{i=1}^{\ell} c_i^{(j)}\gamma_i)\big\} = 0 \end{aligned} \tag{10}$$

$$\begin{aligned} &\big\{(d_1^{(j)} + \textstyle\sum_{i=1}^{\ell} a_i^{(j)}\beta_i)\varphi_r + (d_2^{(j)} + \textstyle\sum_{i=1}^{\ell} b_i^{(j)}\beta_i)\varphi_s + (v_0^{(j)} + \textstyle\sum_{i=1}^{\ell} v_i^{(j)}\beta_i)\big\}n \\ +&\big\{(u_1^{(j)} + \textstyle\sum_{i=1}^{\ell} a_i^{(j)}\gamma_i)\varphi_r + (u_2^{(j)} + \textstyle\sum_{i=1}^{\ell} b_i^{(j)}\gamma_i)\varphi_s + (-z^{(j)} + \textstyle\sum_{i=1}^{\ell} v_i^{(j)}\gamma_i)\big\} = 0 \end{aligned} \tag{11}$$

Now, for verification equation j we introduce the following more compact notation:

$$\begin{array}{lll} A_j^{\beta} = d_1^{(j)} + \sum_{i=1}^{\ell} a_i^{(j)}\beta_i & A_j^{\gamma} = u_1^{(j)} + \sum_{i=1}^{\ell} a_i^{(j)}\gamma_i & A_j^{t} = u_1^{(j)} + d_1^{(j)} n + \sum_{i=1}^{\ell} a_i^{(j)} t_i \\ B_j^{\beta} = d_2^{(j)} + \sum_{i=1}^{\ell} b_i^{(j)}\beta_i & B_j^{\gamma} = u_2^{(j)} + \sum_{i=1}^{\ell} b_i^{(j)}\gamma_i & B_j^{t} = u_2^{(j)} + d_2^{(j)} n + \sum_{i=1}^{\ell} b_i^{(j)} t_i \\ C_j^{\beta} = d_3^{(j)} + \sum_{i=1}^{\ell} c_i^{(j)}\beta_i & C_j^{\gamma} = u_3^{(j)} + \sum_{i=1}^{\ell} c_i^{(j)}\gamma_i & C_j^{t} = u_3^{(j)} + d_3^{(j)} n + \sum_{i=1}^{\ell} c_i^{(j)} t_i \\ V_j^{\beta} = v_0^{(j)} + \sum_{i=1}^{\ell} v_i^{(j)}\beta_i & V_j^{\gamma} = -z^{(j)} + \sum_{i=1}^{\ell} v_i^{(j)}\gamma_i & V_j^{t} = -z^{(j)} + v_0^{(j)} n + \sum_{i=1}^{\ell} v_i^{(j)} t_i \end{array}$$

With a similar argument as the one used in Claim 1, we can argue that if Eqs. (10) and (11) hold, then they must hold *as polynomials in* n if the discrete logarithm problem is hard. Therefore, if the above equations hold, we must have:

$$A_j^\beta \alpha_r + B_j^\beta \alpha_s + C_j^\beta = 0 \tag{12}$$
$$A_j^\gamma \alpha_r + B_j^\gamma \alpha_s + C_j^\gamma = 0 \tag{13}$$
$$A_j^\beta \varphi_r + B_j^\beta \varphi_s + V_j^\beta = 0 \tag{14}$$
$$A_j^\gamma \varphi_r + B_j^\gamma \varphi_s + V_j^\gamma = 0 \tag{15}$$

We say a verification equation j is degenerate if $A_j^t = B_j^t = C_j^t = V_j^t = 0$. Note that, $A_j^t = A_j^\gamma + nA_j^\beta$ and the same occurs for B, C and V. In general, if an equation j is degenerate, it must hold

$$A_j^\gamma = A_j^\beta = B_j^\gamma = B_j^\beta = C_j^\gamma = C_j^\beta = V_j^\gamma = V_j^\beta = 0$$

if dlog is hard (this can be shown by a similar analysis as in Claim 1).

Finally, for every pair of verification equations, say j and k, we define the determinant $\mathtt{Dt}_{j,k}(n, t_1, \ldots, t_\ell)$ as:

$$\begin{aligned}\mathtt{Dt}_{j,k}(n, t_1, \ldots, t_\ell) &:= A_j^t B_k^t - A_k^t B_j^t \\ &= (A_j^\gamma + nA_j^\beta)(B_k^\gamma + nB_k^\beta) - (A_k^\gamma + nA_k^\beta)(B_j^\gamma + nB_j^\beta)\end{aligned}$$

Hereafter we use the same conventions for matrix-representations of linear maps on finite-dimensional spaces. The *rank* of a matrix is defined to be the dimension of the vector space generated by its columns/rows. Given two vectors $\boldsymbol{v}, \boldsymbol{w}$ over $\mathbb{Z}_p^n$, we say they are linearly dependent or proportional, denoted by $\boldsymbol{v} \equiv \boldsymbol{w}$ if and only if there exist scalars $\rho, \delta \in \mathbb{Z}_p$ (not both null), s.t. $\rho\boldsymbol{v} = \delta\boldsymbol{w}$.

We prepared the notation to define a crucial relation for $\mathsf{Sig} \in \mathcal{SIG}_{2,\ell}$. We first provide some intuition about how it is defined and why.

Intuition About the Crucial Relation. The algebraic extractor associated to the reduction provides coefficients of a linear combination, linking the group elements returned by the reduction and the group elements that it received. It turns out, that if the discrete logarithm problem is hard, these coefficients must satisfy certain additional properties. When developing the crucial relation, one thinks of how to embed these coefficients in the witness, since they result extremely useful for creating a forgery. For example, knowing the pair (α_r, α_s) that was used by the reduction to create $R = G^{\varphi_r} M^{\alpha_r}$ and $S = G^{\varphi_s} M^{\alpha_s}$, a new signature can be created on a different message (see the full version of this paper for details). However, these coefficients cannot just be included in the witness. It is required that they are unique in some sense. Otherwise, using them to build a signature could potentially give extra information to the reduction. The biggest challenge when defining the crucial relation is finding cases in which we can argue usefulness and uniqueness at the same time.

Definition 3 (Crucial Relation for $\mathsf{Sig} \in \mathcal{SIG}_{2,\ell}$ for $\ell \leq 3$). *For signature scheme $\mathsf{Sig} = (\mathcal{C}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ in $\mathcal{SIG}_{\tau,\ell}$, and its transcript θ, let $(R, S, T_1, \ldots, T_\ell)$ be the first signature in θ for message (M, N). For witness $\varpi \in (\mathbb{Z}_p \cup \bot)^{\ell+2}$, the relation $\Psi(\theta, \varpi)$ is defined by the following algorithm:*

1. *If θ is invalid, return 0.*
2. *If there exist j, k s.t. $\mathtt{Dt}_{j,k}(n, t_1, \ldots, t_\ell) \neq 0$. Let $\alpha_r, \alpha_s \in \mathbb{Z}_p$ satisfy Eq. (8) for such j, k. If $\varpi = (\alpha_r, \alpha_s, \bot, \ldots, \bot)$ then return 1, else return 0.*
3. *If there exists a verification equation, j, s.t. one and only one of the following the expressions A_j^t and B_j^t is zero. Let j be the index of the first equation that satisfies the previous condition. If $A_j^t = 0$ and $\varpi = (0, \alpha_s, \bot, \ldots, \bot)$ where $B_j^t \alpha_s + C_j^t = 0$ then return 1, else if $B_j^t = 0$ and $\varpi = (\alpha_r, 0, \bot, \ldots, \bot)$ where $A_j^t \alpha_r + C_j^t = 0$ then return 1, else return 0.*
4. *If all verification equations are degenerate, i.e. for all j, $A_j^t = B_j^t = C_j^t = V_j^t = 0$, if $\varpi = (\bot, \ldots, \bot)$ return 1, else return 0.*
5. *If there exists $\beta = (\beta_1, \ldots, \beta_\ell) \in \mathbb{Z}_p^\ell$ s.t. for $\gamma_i = t_i - n\beta_i$ for $i \in \{1, \ldots, \ell\}$ and every pair of verification equations j, k the following vectors in $\mathbb{Z}_p^8$ are proportional:*

$$\left(A_j^\beta \;\; B_j^\beta \;\; C_j^\beta \;\; V_j^\beta \;\; A_j^\gamma \;\; B_j^\gamma \;\; C_j^\gamma \;\; V_j^\gamma\right) \equiv \left(A_k^\beta \;\; B_k^\beta \;\; C_k^\beta \;\; V_k^\beta \;\; A_k^\gamma \;\; B_k^\gamma \;\; C_k^\gamma \;\; V_k^\gamma\right)$$

   where, for non-degenerate equations j it holds, $A_j^\beta B_j^\gamma - A_j^\gamma B_j^\beta \neq 0$.
   If $\varpi = (\alpha_r, \alpha_s, \bot, \ldots, \bot)$ satisfying $A_j^\beta \alpha_r + B_j^\beta \alpha_s + C_j^\beta = 0$ and $A_j^\gamma \alpha_r + B_j^\gamma \alpha_s + C_j^\gamma = 0$ for every verification equation j, then return 1, else return 0.
6. *If there exists a non-degenerate equation j s.t. there exist coefficients $\mu_1, \mu_2, \mu_3 \in \mathbb{Z}_p$, which are publicly computable and verify*

$$\left(u_1^{(j)} \; d_1^{(j)} \; a_1^{(j)} \; \ldots \; a_\ell^{(j)}\right)\mu_1 + \left(u_2^{(j)} \; d_2^{(j)} \; b_1^{(j)} \; \ldots \; b_\ell^{(j)}\right)\mu_2 + \left(u_3^{(j)} \; d_3^{(j)} \; c_1^{(j)} \; \ldots \; c_\ell^{(j)}\right)\mu_3 = \mathbf{0}$$

   if it can be found $\mu_3 \neq 0$ then
   • if $\varpi = (\bot, \ldots, \bot)$ then return 1 • otherwise, return 0
   else (when μ_3 must be 0), go to clause 8.
7. *If there exists $\beta = (\beta_1, \ldots, \beta_\ell) \in \mathbb{Z}_p^\ell$ s.t. for every j, $A_j^\beta = 0 \wedge B_j^\beta = 0 \wedge C_j^\beta = 0 \wedge V_j^\beta = 0$, if $\varpi = (\beta_1, \ldots, \beta_\ell)$ then return 1, else return 0.*
8. *In any other case, if $\varpi = (\alpha_r, 0, \bot, \ldots, \bot)$ s.t., if we set $\alpha_s = 0$, for every equation j, it holds $A_j^t \alpha_r + B_j^t \alpha_s + C_j^t = 0$ then return 1, else return 0.*

Lemma 2. *For every $\ell \leq 3$, Ψ is a crucial relation for every $\mathsf{Sig} \in \mathcal{SIG}_{2,\ell}$ w.r.t. algebraic algorithms and a message sampler choosing messages uniformly.*

Proof. We show that Ψ has *uniqueness* as defined for a crucial relation. Proofs for *usefulness* and *extractability* are also technically interesting but due to the space restriction, we refer to [1] for more details.

Let k be the total number of verification equations. When analyzing scheme $\mathsf{Sig} \in \mathcal{SIG}_{2,\ell}$, we will assume without loss of generality that Sig is s.t.

$$\operatorname{rank}\begin{pmatrix} a_1^{(1)} \; b_1^{(1)} \; c_1^{(1)} \; v_1^{(1)} \; \ldots \; a_1^{(k)} \; b_1^{(k)} \; c_1^{(k)} \; v_1^{(k)} \\ \vdots \\ a_\ell^{(1)} \; b_\ell^{(1)} \; c_\ell^{(1)} \; v_\ell^{(1)} \; \ldots \; a_\ell^{(k)} \; b_\ell^{(k)} \; c_\ell^{(k)} \; v_\ell^{(k)} \end{pmatrix} = \ell \tag{16}$$

First note that the assumption is reasonable for $\ell = 1$. Otherwise the scheme would be completely trivial. For other values of ℓ, the scheme admits a transformation that makes one of the $T's$ disappear (because one of the rows of the above matrix could be expressed as a linear combination of the others) and thus, Sig would belong to $\mathcal{SIG}_{2,\ell-1}$ which is captured by the same crucial relation instantiated for $\ell - 1$. The proof is presented for a generic ℓ and we will only use the restriction $\ell \leq 3$ to argue extractability for clause 7.

Uniqueness. To argue uniqueness we show that every valid transcript θ admits one and only one witness ϖ s.t. $1 = \Psi(\theta, \varpi)$. First, note that every valid θ falls in one of the clauses 2–8 (clause 8 accepts every θ that did not fall in an earlier clause). We analyze clause by clause the uniqueness of ϖ in case θ fall in it.

Assume that θ falls into clause 2, i.e., for some (j, k), $\mathtt{Dt}_{j,k}(n, t_1, \ldots, t_\ell) \neq 0$. Note that, there can only exist a *unique* pair (α_r, α_s) satisfying Eq. (8) for both j and k, because $\mathtt{Dt}_{j,k}(n, t_1, \ldots, t_\ell) \neq 0$. That makes the witness unique.

When θ falls in clause 3, let j be the first verification equation for which one and only one of A_j^t, B_j^t is zero. Uniqueness holds because if $A_j^t = 0$ then $B_j^t \neq 0$ and there exists exactly one α_s s.t. $B_j^t \alpha_s + C_j^t = 0$. On the other hand, if $A_j^t \neq 0$, there exists exactly one α_r satisfying $A_j^t \alpha_r + C_j^t = 0$.

In case of clauses 4 or 6, uniqueness holds immediately.

For clause 5, it is clear that in case of existing a valid witness, it must be unique. That is because, due to $A_j^\beta B_j^\gamma - A_j^\gamma B_j^\beta \neq 0$, there exists exactly one pair (α_r, α_s) satisfying $A_j^\beta \alpha_r + B_j^\beta \alpha_s + C_j^\beta = 0$ and $A_j^\gamma \alpha_r + B_j^\gamma \alpha_s + C_j^\gamma = 0$ as clause 5 requires. However, we need to show that this (α_r, α_s) exists, independently of the β that has been chosen (as long as the β satisfies the conditions of the clause). To do so, we consider a different vector of β, defined by $\beta'_i = \beta_i + \delta_i$ (we denote $\gamma'_i = t'_i - n\beta'_i$) for $i \in \{1, \ldots, \ell\}$ and we prove that the value of (α_r, α_s) must be the same. Because $A_j^\beta B_j^\gamma - A_j^\gamma B_j^\beta \neq 0$, the equations we can give a explicit formula for (α_r, α_s) satisfying the equations $A_j^\beta \alpha_r + B_j^\beta \alpha_s + C_j^\beta = 0$ and $A_j^\gamma \alpha_r + B_j^\gamma \alpha_s + C_j^\gamma = 0$ for some j. That is,

$$\alpha_r = \frac{B_j^\gamma C_j^\beta - B_j^\beta C_j^\gamma}{A_j^\gamma B_j^\beta - A_j^\beta B_j^\gamma} \qquad \alpha_s = \frac{A_j^\beta C_j^\gamma - A_j^\gamma C_j^\beta}{A_j^\gamma B_j^\beta - A_j^\beta B_j^\gamma}$$

Now, assume that α_r and α_s are derived from the same equations induced by a different β, i.e., $\beta' = \beta + \delta$. Expanding the equations and rearranging terms, we can express the above equation as (we omit indices j for simplicity)

$$\alpha_r = \frac{B_j^\gamma C_j^\beta - B_j^\beta C_j^\gamma - n\Delta_1 + \Delta_2}{A_j^\gamma B_j^\beta - A_j^\beta B_j^\gamma - n\Delta_3 + \Delta_4}$$

where

$$\begin{aligned}
\Delta_1 &= (\textstyle\sum_{i=1}^{\ell} b_i\delta_i)(d_3 + \sum_{i=1}^{\ell} c_i\beta_i) - (\sum_{i=1}^{\ell} c_i\delta_i)(d_2 + \sum_{i=1}^{\ell} b_i\beta_i)\\
\Delta_2 &= (\textstyle\sum_{i=1}^{\ell} c_i\delta_i)(u_2 + \sum_{i=1}^{\ell} b_i\gamma_i) - (\sum_{i=1}^{\ell} b_i\delta_i)(u_3 + \sum_{i=1}^{\ell} c_i\gamma_i)\\
\Delta_3 &= (\textstyle\sum_{i=1}^{\ell} a_i\delta_i)(d_2 + \sum_{i=1}^{\ell} b_i\beta_i) - (\sum_{i=1}^{\ell} b_i\delta_i)(d_1 + \sum_{i=1}^{\ell} a_i\beta_i)\\
\Delta_4 &= (\textstyle\sum_{i=1}^{\ell} b_i\delta_i)(u_1 + \sum_{i=1}^{\ell} a_i\gamma_i) - (\sum_{i=1}^{\ell} a_i\delta_i)(u_2 + \sum_{i=1}^{\ell} b_i\gamma_i)
\end{aligned}$$

Our goal is to show that α_r is unique and therefore, increments $-n\Delta_1 + \Delta_2$ and $-n\Delta_3 + \Delta_4$ are zero. Observe that, the new β' must also satisfy the equation

$$(d_1 + \sum_{i=1}^{\ell} a_i\beta_i + \sum_{i=1}^{\ell} a_i\delta_i)\alpha_r + (d_2 + \sum_{i=1}^{\ell} b_i\beta_i + \sum_{i=1}^{\ell} b_i\delta_i)\alpha_s + (d_3 + \sum_{i=1}^{\ell} c_i\beta_i + \sum_{i=1}^{\ell} c_i\delta_i) = 0$$

which also satisfies $(d_1 + \sum_{i=1}^{\ell} a_i\beta_i)\alpha_r + (d_2 + \sum_{i=1}^{\ell} b_i\beta_i)\alpha_s + (d_3 + \sum_{i=1}^{\ell} c_i\beta_i) = 0$. Assume that α_r, α_s is not unique, in that case, it must be

$$(d_1 + \sum_{i=1}^{\ell} a_i\beta_i)(d_2 + \sum_{i=1}^{\ell} b_i\beta_i + \sum_{i=1}^{\ell} b_i\delta_i) - (d_2 + \sum_{i=1}^{\ell} b_i\beta_i)(d_1 + \sum_{i=1}^{\ell} a_i\beta_i + \sum_{i=1}^{\ell} a_i\delta_i) = 0$$

which leads to $(\sum_{i=1}^{\ell} a_i\delta_i)(d_2 + \sum_{i=1}^{\ell} b_i\beta_i) - (\sum_{i=1}^{\ell} b_i\delta_i)(d_1 + \sum_{i=1}^{\ell} a_i\beta_i) = 0$ and observe that the previous expression corresponds to Δ_3. A similar analysis, using the following equations (from the requirements of clause 5):

$$(u_1 + \sum_{i=1}^{\ell} a_i\gamma_i)\alpha_r + (u_2 + \sum_{i=1}^{\ell} b_i\gamma_i)\alpha_s + (u_3 + \sum_{i=1}^{\ell} c_i\gamma_i) = 0$$
$$(u_1 + \sum_{i=1}^{\ell} a_i\gamma_i + \sum_{i=1}^{\ell} a_i\gamma_i)\alpha_r + (u_2 + \sum_{i=1}^{\ell} b_i\gamma_i + \sum_{i=1}^{\ell} b_i\gamma_i)\alpha_s + (u_3 + \sum_{i=1}^{\ell} c_i\gamma_i + \sum_{i=1}^{\ell} c_i\gamma_i) = 0$$

leads to $(\sum_{i=1}^{\ell} b_i\delta_i)(u_1 + \sum_{i=1}^{\ell} a_i\gamma_i) - (\sum_{i=1}^{\ell} a_i\delta_i)(u_2 + \sum_{i=1}^{\ell} b_i\gamma_i) = 0$ and observe that the previous expression corresponds to Δ_4. By a similar analysis, it can be shown that the increments in the numerator of α_r are zero and eventually, that the same thing occurs for α_s.

If θ falls into clause 7, and the witness ϖ satisfies Ψ, it must be $\varpi = (\beta_1, \ldots, \beta_\ell)$, with $A_j^\beta = 0 \wedge B_j^\beta = 0 \wedge C_j^\beta = 0 \wedge V_j^\beta = 0$. Or equivalently, $(\beta_1, \ldots, \beta_\ell)$ is a solution of the following linear system

$$\left(\beta_1 \ldots \beta_\ell\right) \mathsf{M} = \left(-d_1^{(1)} \; -d_2^{(1)} \; -d_3^{(1)} \; -v_0^{(1)} \; -d_1^{(2)} \ldots -d_1^{(k)} \; -d_2^{(k)} \; -d_3^{(k)} \; -v_0^{(k)}\right)$$

where M is the matrix from Eq. (16). Because the rank of M is ℓ, there exists at most one solution to the system and therefore, the witness is unique.

For arguing about the missing clause, 8, we prove the following Claim.

Claim 2. Any transcript θ that did not fall in clause 5 or before is s.t. all Eq. $(12)^{(*)}$ are be proportional between them and to all Eq. $(13)^{(*)}$ (when considering them as linear equations in α_r, α_s).

Proof. Assume that the groups of Eqs. $(12)^{(*)}$ and $(13)^{(*)}$ are not proportional. We show that θ should have fallen into clause 5 or earlier.

Note that at this point (and because we did not enter in clause 3), for every pair of verification equations j, k the determinant $\mathtt{Dt}_{j,k}(n, t_1, \ldots, t_\ell)$ is zero. Also note that, if we consider as before, $t_i = \gamma_i + n\beta_i$ for every $i \in \{1, \ldots, \ell\}$, such a determinant can be seen as a degree-2 polynomial in n,

$$n^2(A_j^\beta B_k^\beta - A_k^\beta B_j^\beta) + n\,(A_j^\beta B_k^\gamma - A_k^\gamma B_j^\beta \; + \; A_j^\gamma B_k^\beta - A_k^\beta B_j^\gamma) + (A_j^\gamma B_k^\gamma - A_k^\gamma B_j^\gamma)$$

which is zero for every pair j, k. In a similar way as done in the proof of Claim 1, we can prove that $\mathtt{Dt}_{j,k}(n, t_1, \ldots, t_\ell) = 0$ happens only if every coefficient of the above polynomial in n is zero (otherwise, $\mathcal{R}$ can be used to solve the discrete-logarithm problem in $\mathbb{G}_2$). We therefore have

$$A_j^\beta B_k^\beta - A_k^\beta B_j^\beta = 0 \tag{17}$$
$$A_j^\gamma B_k^\gamma - A_k^\gamma B_j^\gamma = 0 \tag{18}$$
$$A_j^\beta B_k^\gamma - A_k^\gamma B_j^\beta + A_j^\gamma B_k^\beta - A_k^\beta B_j^\gamma = 0 \tag{19}$$

Let $(\mathsf{x})^{(j)}$ denote equation (x) w.r.t. j-th verification equation. Equation (17) implies that, when considering the relations $(12)^{(j)}$ for all j as equations in α_r, α_s, they are all proportional. The same happens with Eq. $(13)^{(j)}$ due to (18).

First, note that if all verification equations are degenerate, we would have entered in clause 4. On the other hand, if there is just one non-degenerate verification equation the condition on clause 5 holds and we would have fallen in there. Now, pick two non-degenerate equations, say (j, k). Note that, since $A_j^\beta B_k^\beta = A_k^\beta B_j^\beta$ and they are non-degenerate, there must exist a constant $\rho \in \mathbb{Z}_p$ s.t. $A_j^\beta = \rho A_k^\beta$ and $B_j^\beta = \rho B_k^\beta$. Analogously, since $A_j^\gamma B_k^\gamma = A_k^\gamma B_j^\gamma$ and they are non-degenerate, there exists a constant $\delta \in \mathbb{Z}_p$ s.t. $A_j^\gamma = \delta A_k^\gamma$ and $B_j^\gamma = \delta B_k^\gamma$. Now, substituting in Eq. (19) we have

$$\rho A_k^\beta B_k^\gamma - A_k^\gamma \rho B_k^\beta + \delta A_k^\gamma B_k^\beta - A_k^\beta \delta B_k^\gamma = (\rho - \delta)(A_k^\beta B_k^\gamma - A_k^\gamma B_k^\beta) = 0 \tag{20}$$

Because the groups of Eqs. $(12)^{(*)}$ and $(13)^{(*)}$ are not proportional between them, it must be $(A_k^\beta B_k^\gamma - A_k^\gamma B_k^\beta) \neq 0$ for any pair of non-degenerate equations j, k, and thus, it must be $\rho - \delta = 0$. Therefore, the linear factor between Eq. $(12)^{(j)}$ and $(12)^{(k)}$ is the same as the linear factor between Eq. $(13)^{(j)}$ and $(13)^{(k)}$. With similar techniques, it can be shown that in this situation happens between A and C and so on. In fact, it must hold

$$\left(A_j^\beta \;\; B_j^\beta \;\; C_j^\beta \;\; V_j^\beta \;\; A_j^t \;\; B_j^t \;\; C_j^t \;\; V_j^t \right) \equiv \left(A_k^\beta \;\; B_k^\beta \;\; C_k^\beta \;\; V_k^\beta \;\; A_k^t \;\; B_k^t \;\; C_k^t \;\; V_k^t \right)$$

for any pair of non-degenerate verification equations j, k. If j or k are degenerate, the above equations hold and the transcript θ would have entered in clause 5.

Therefore, if clause 8 is reached, all equations in $(12)^{(*)}$ must be proportional to all Eq. $(13)^{(*)}$. □

At this point, we know that all equations of the form $A_j^\beta \alpha_r + B_j^\beta \alpha_s + C_j^\beta = 0$ are proportional between them for all j (looking at them as linear equations in α_r, α_s) and they are all proportional to $A_j^\gamma \alpha_r + B_j^\gamma \alpha_s + C_j^\gamma = 0$ for all j. This implies that they are also all proportional to $A_j^t \alpha_r + B_j^t \alpha_s + C_j^t = 0$ for every j.

Pick a non-degenerate equation, say j^*. If α_r, α_s satisfy this equation, they satisfy them all. On the other hand, because it is non-degenerate, $A_{j^*}^t \neq 0$ and therefore, there exists a unique value $\alpha_r \in \mathbb{Z}_p$ s.t. $A_{j^*}^t \alpha_r + B_{j^*}^t \cdot 0 + C_{j^*}^t = 0$. Therefore, the witness is unique in this branch. □

From Theorem 1, the following corollary is immediate. It implies that at least six group elements are necessary as claimed in Table 1.

Corollary 1. *If there exists a structure preserving signature scheme that signs bilateral messages over Type-III bilinear groups and its EUF-CMA security is proved by algebraic black-box reductions to a non-interactive problem, then its signature must include at least 6 group elements.*

It is worth to point out that the above result brings new insights to the case of unilateral messages in Type-III under non-interactive assumptions. Recall that the 4-element construction in [5] outputs signatures in $\mathbb{G}_1^3 \times \mathbb{G}_2$ for messages in $\mathbb{G}_1$. It was unknown whether other structures such as $\mathbb{G}_1^2 \times \mathbb{G}_2^2$ are possible. Corollary 1 states that $\mathbb{G}_1^3 \times \mathbb{G}_2$ is the only possible choice and it justifies the optimality of the construction from [5].

The following corollary restricts the number of schemes for bilateral messages with signatures in $\mathbb{G}_1^2 \times \mathbb{G}_2^\ell$ for arbitrary ℓ, by imposing a condition without which it would be easy to argue extractability for clause 7.

Corollary 2. *If Sig is a signature scheme for messages $(M, N) \in \mathbb{G}_1 \times \mathbb{G}_2$ with signature elements $(R, S, T_1, \ldots, T_\ell) \in \mathbb{G}_1^2 \times \mathbb{G}_2^\ell$ is proven EUF-CMA under a non-interactive assumption, it must be s.t. all the k verification equations satisfy:*

$$\operatorname{rank}\begin{pmatrix} d_1^{(1)} & d_2^{(1)} & d_3^{(1)} & \ldots & d_1^{(k)} & d_2^{(k)} & d_3^{(k)} \\ a_1^{(1)} & b_1^{(1)} & c_1^{(1)} & \ldots & a_1^{(k)} & b_1^{(k)} & c_1^{(k)} \\ & & & \vdots & & & \\ a_\ell^{(1)} & b_\ell^{(1)} & c_\ell^{(1)} & \ldots & a_\ell^{(k)} & b_\ell^{(k)} & c_\ell^{(k)} \end{pmatrix} < \ell$$

4 Lower Bounds in Type-II

In Type-II, there are three cases, i.e., (1) messages exist only in $\mathbb{G}_1$, (2) messages exist only in $\mathbb{G}_2$, and (3) messages exist in both $\mathbb{G}_1$ and $\mathbb{G}_2$. Below, we give a bound for the first case. Note that it directly implies a lower bound for bilateral messages (case 3) as well.

Theorem 2. *Any structure preserving signature scheme over Type-II groups with message space $\mathcal{M} \subset \mathbb{G}_1$ that yields signatures consisting of 3 group elements cannot have an algebraic black-box reduction from the EUF-CMA security to non-interactive hardness assumptions if pseudo-random functions exist and the discrete logarithm problem is hard in $\mathbb{G}_1$.*

Let $M \in \mathbb{G}_1$ be a message and $(R, S, T_1, \ldots, T_\ell)$ be a signature. We first consider two extreme cases where signatures include elements from one group. If $(R, S, T_1, \ldots, T_\ell) \in \mathbb{G}_1^{2+\ell}$, the verification equations are in the form of $e(R, U_1)$ $e(S, U_2)\, e(M, U_3) \prod_{j=1}^{\ell} e(T_j, U_{3+j}) = Z$ where U_i and Z are public-keys. Thus, given two signatures on two messages, one can easily obtain a valid signature on a new message by linearly combining two messages and signatures. Therefore, such signatures are vulnerable to random message attacks.

We now consider the case where the number of signature elements in $\mathbb{G}_1$ is at most 2. Say, $(R, S) \in \mathbb{G}_1^2$, $T_1, \ldots, T_\ell \in \mathbb{G}_2^\ell$. Let $\mathcal{SIG}_\ell$ be the set of all structure

preserving signature schemes whose signature consists of 2 group elements from $\mathbb{G}_1$ and other ℓ elements from $\mathbb{G}_2$. We denote by $\tilde{A}$ the group element in $\mathbb{G}_1$ that was mapped from $A \in \mathbb{G}_2$.

Theorem 2 is shown by combining our Lemma 3 with Theorem 8 from [5].

Lemma 3. *For every scheme in $\mathcal{SIG}_\ell$, there exists a crucial relation.*

Proof. According to [6], at least 2 verification equations are required in Type-II for secure signature with $(R, S) \in \mathbb{G}_1^2$, $T_1, \ldots, T_\ell \in \mathbb{G}_2^\ell \in \mathcal{SIG}_\ell$. Observe that in every structure preserving signature scheme with signature space $\mathbb{G}_1^2 \times \mathbb{G}_2^\ell$, the j-th verification equation can be written in the following form, where $M \in \mathbb{G}_1$ is a message, $U_i^{(j)}, V_i^{(j)}$ are elements in VK, $a_i^{(j)}, b_i^{(j)}, c_i^{(j)}, d_i^{(j)} \in \mathbb{Z}_p$ for $i = 1, \ldots, \ell$ are public parameters, and $(R, S, T_1, \ldots, T_\ell) \in \mathbb{G}_1^2 \times \mathbb{G}_2^\ell$ are signatures,

$$e(R, U_1^{(j)} \prod_{i=1}^{\ell} T_i^{a_i^{(j)}})\, e(S, U_2^{(j)} \prod_{i=1}^{\ell} T_i^{b_i^{(j)}})\, e(M, U_3^{(j)} \prod_{i=1}^{\ell} T_i^{c_i^{(j)}}) \prod_{j=1}^{\ell} \prod_{i=1}^{\ell} e(\tilde{T}_j, T_i^{d_i^{(j)}}) \prod_{i=1}^{\ell} e(V_i^{(j)}, T_i) = Z^{(j)}. \quad (21)$$

Note that, to show the impossibility, it is sufficient to consider a single-element message in $\mathbb{G}_1$ rather than its vector form.

For elements R, S, T_i $(i = 1, \ldots, \ell)$ in a signature, we consider a special representation of the form $R = G^{\varphi_r} M^{\alpha_r}$, $S = G^{\varphi_s} M^{\alpha_s}$, $T_i = H^{\varphi_{t_i}}$ for some $\varphi_r, \alpha_r, \varphi_s, \alpha_s, \varphi_{t_i}$ in $\mathbb{Z}_p$. Now, consider Eq. (21) in the exponent:

$$\begin{aligned}(\varphi_r + \alpha_r\, m)\,(\textstyle\sum_{i=1}^{\ell} a_i^{(j)}\, \varphi_{t_i} + u_1^{(j)}) + (\varphi_s + \alpha_s\, m)\,(\sum_{i=1}^{\ell} b_i^{(j)}\, \varphi_{t_i} + u_2^{(j)}) \\ + m\,(\textstyle\sum_{i=1}^{\ell} c_i^{(j)}\, \varphi_{t_i} + u_3^{(j)}) + \sum_{j=1}^{\ell} \varphi_{t_j} \sum_{i=1}^{\ell} d_i^{(j)}\, \varphi_{t_i} + \sum_{j=1}^{\ell} v_i^{(j)} \varphi_{t_i} = z \end{aligned} \quad (22)$$

By considering (22) as a polynomial in m, it can be shown that

$$(\textstyle\sum_{i=1}^{\ell} a_i^{(j)} \varphi_{t_i} + u_1^{(j)})\alpha_r + (\sum_{i=1}^{\ell} b_i^{(j)} \varphi_{t_i} + u_2^{(j)})\alpha_s + (\sum_{i=1}^{\ell} c_i^{(j)} \varphi_{t_i} + u_3^{(j)}) = 0 \quad (23)$$

if the discrete logarithm problem is hard in $\mathbb{G}_1$. We denote by $\mathtt{Dt}_{j,k}(t_1, \ldots, t_\ell)$ the determinant of Eq. (23) for j and $k \neq j$, when considered as polynomials in (α_r, α_s). There exists a unique solution (α_r, α_s) if and only if $\mathtt{Dt}_{j,k}(t_1, \ldots, t_\ell) \neq 0$. Let θ denote a transcript $\theta := (VK, (M^{(1)}, R^{(1)}, S^{(1)}, T_1^{(1)}, \ldots, T_\ell^{(1)}), \ldots, (M^{(n)}, R^{(n)}, S^{(n)}, T_1^{(n)}, \ldots, T_\ell^{(n)}))$. We construct a crucial relation for $\mathsf{Sig} \in \mathcal{SIG}_\ell$.

Definition 4 (Crucial Relation for $\mathsf{Sig} \in \mathcal{SIG}_\ell$). *Let $\varpi := (\omega_1, \omega_2)$ and given θ, let $(R, S, T_1, \ldots, T_\ell)$ be the first signature in θ, for message M. The relation $\Psi(\theta, \varpi)$ is decided as follows.*

1. *If θ is invalid, return 0.*
2. *Else if there exist verification equations j and k s.t. $\mathtt{Dt}_{j,k}(t_1, \ldots, t_\ell) \neq 0$,*
   - *if $\varpi = (\alpha_r, \alpha_s)$ where α_r and α_s satisfy (23) for both verification equations j and k, return 1,*

– *else return 0.*

3. *Else if* $\varpi = (\bot, \bot)$ *then return* 1*, else return* 0*.*

Lemma 4. *The relation* Ψ *in Definition 4 is a crucial relation for any* $\mathsf{Sig} \in \mathcal{SIG}_\ell$ *w.r.t. algebraic algorithms and a message sampler choosing* M *uniformly.*

We show that the relation Ψ in Definition 4 satisfies usefulness, omitting proofs for uniqueness and extractability (see [1] for further details).

USEFULNESS. Given $\varpi = (\alpha_r, \alpha_s) \in \mathbb{Z}_p^2$, we forge a signature on arbitrary fresh message as follows:

Choose $\hat{M} \in \mathbb{G}_1$ randomly. Compute $(M^\star, R^\star, S^\star, T_1^\star, \ldots, T_\ell^\star) = (M \cdot \hat{M}, R \cdot \hat{M}^{-\alpha_r}, S \cdot \hat{M}^{-\alpha_s}, T_1, \ldots, T_\ell)$ and output $(R^\star, S^\star, T_1^\star, \ldots, T_\ell^\star)$ as a forgery for $M^\star$. Since it uses the actual α_r and α_s that were used by the reduction, it constitutes a valid signature because it satisfies (21) for every verification equation.

On the other hand, if $\varpi = (\bot, \bot)$, it means that Eq. (23) is proportional (as an equation in α_r and α_s) for every verification equation j. We say a verification equation is *degenerate* if $\sum_{i=1}^{\ell} a_i^{(j)} \varphi_{t_i} + u_1^{(j)} = 0$ and $\sum_{i=1}^{\ell} b_i^{(j)} \varphi_{t_i} + u_2^{(j)} = 0$. Otherwise, it is called *non-degenerate*. Note that, if $T_1, \ldots, T_\ell$ are reused, if a non-degenerate verification equation holds for certain M, R, S, all verification equations will also hold (because they are all proportional). This observation allows us to define the following forgery:

Pick a non-degenerate verification equation j s.t. $\sum_{i=1}^{\ell} a_i^{(j)} \varphi_{t_i} + u_1^{(j)} \neq 0$. Compute $M^\star = M \cdot \big(U_1^{(j)} \prod_{i=1}^{\ell} \tilde{T}_i^{a_i^{(j)}}\big)^{-1}$ and $R^\star = R \cdot \big(U_3^{(j)} \prod_{i=1}^{\ell} \tilde{T}_i^{c_i^{(j)}}\big)$. Observe that $(R^\star, S, T_1, \ldots, T_\ell)$ is a valid signature for $M^\star$: it satisfies the non-degenerate equation j and, because it reuses $T_1, \ldots, T_\ell$, it must satisfy all the others too.

If no non-degenerate verification equation satisfies the previous condition, pick one, say j, s.t. $\sum_{i=1}^{\ell} b_i^{(j)} \varphi_{t_i} + u_2^{(j)} \neq 0$. Analogously, compute $M^\star = M \cdot \big(U_2^{(j)} \prod_{i=1}^{\ell} \tilde{T}_i^{b_i^{(j)}}\big)^{-1}$ and $S^\star = S \cdot \big(U_3^{(j)} \prod_{i=1}^{\ell} \tilde{T}_i^{c_i^{(j)}}\big)$ and observe that $(R, S^\star, T_1, \ldots, T_\ell)$ is a valid signature for $M^\star$.

Finally, if the above is not possible, all verification equations are degenerate for such $T_1, \ldots, T_\ell$. In that case, $(*, *, T_1, \ldots, T_\ell)$ is a valid signature for every message in $\mathbb{G}_1$, where placeholders $*$ can be filled with arbitrary $\mathbb{G}_1$ elements. □

The above implies that constructions with signature elements $R \in \mathbb{G}_1$ and $S, T_1, \ldots, T_{\ell-1} \in \mathbb{G}_2$ are impossible. Additionally, we can say that no secure SPS based on non-interactive assumption with all signature elements in $\mathbb{G}_2$ can exist.

5 Discussion and Open Problems

On the Tightness of Our Bound for Type-III. We have shown that 6 elements are necessary and the construction from [5] shows that 6 elements are also sufficient. This construction requires 3 signature elements in every source group. A small remaining question would be whether a construction is possible with 2 elements on one side and 4 elements on the other. Our Corollary 2 gives necessary conditions on the shape of the verification equations of such a scheme.

On Constructions Over Type-II Groups. We next discuss the current status of constructions in the setting marked as †, ‡, § in Table 1 and (non-)optimality of the lower bounds obtained in this paper.

- († *Bilateral messages, interactive assumptions*). The optimal scheme for unilateral messages in $\mathbb{G}_1$ (and the scheme in Type-I) from [8] cannot be straightforwardly used for signing bilateral messages since the scheme can sign only a single group element. The best existing scheme for this setting is the 7-element scheme in [3] originally designed for Type-I groups. It can be securely used for bilateral messages in Type-II groups since the construction and security proofs do not use the symmetry of the pairing, and the underlying q-type assumption is justified in the Type-I generic group model where an efficient morphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ does exist. To close the gap between lower and upper bounds in this setting, finding a 3-element scheme that signs messages consisting of two group elements in $\mathbb{G}_1$ is desired.
- (‡ *Unilateral messages in* $\mathbb{G}_1$ *and bilateral messages, q-type assumptions*). The 7-element scheme from [3] is not known to be optimal, since the current lower bound is 4. We want to note that some straightforward approaches to get closer to the lower bound fail: First, observe that the 4-element scheme [4] based on a q-type assumption cannot be used, because it is defined over Type-III bilinear groups and the assumption does not hold in the Type-II setting. Second, the technique of converting a SPS scheme from an interactive to a non-interactive assumption by using the first group element in a message as a random element in a signature (as used in [4,6,15]) does not work because the existing 3-element scheme [8] based on an interactive assumption has a limited message space consisting only of one group element. Closing the gap in this case remains as an open problem.
- (§ *All message types, static assumptions*). The construction in [22] instantiated with the DLIN assumption can be adapted to Type-II groups. It yields in signatures with 9 group elements for messages consisting of an arbitrary (but preliminary fixed) number of group elements in $\mathbb{G}_1$, and hence can be used to sign unilateral messages in $\mathbb{G}_2$ or bilateral messages as well. To the best of our knowledge, that is currently the smallest scheme (according to the signature size) and it is still far from our lower bound of 4 signature elements.

On the Possibility of Showing a Lower Bound for Unilateral Messages in $\mathbb{G}_2$ *in Type-II Groups.* The authors of [6] have constructed a SPS scheme over Type-II groups for messages in $\mathbb{G}_2$ based on a non-interactive assumption, with 3 signature elements. This gives an upper bound of 3, while there is a lower bound of 2. Extrapolating from known lower bounds in different settings, it is natural to conjecture that 3-element construction is indeed optimal in this case. However, the fact that secure constructions with a *single* verification equation exist in Type-II, makes our techniques inapplicable for this case. Finding a scheme with 2 signature elements in this setting or proving that 3 group elements are needed remains as an open problem. We conjecture that a 2-element construction based on non-interactive assumptions does not exist and lean towards the optimality of 3 signature elements.

References

1. Abe, M., Ambrona, M., Ohkubo, M., Tibouchi, M.: Lower bounds on structurepreserving signatures for bilateral messages. IACR Cryptology ePrint Archive 2018/640 (2018). https://eprint.iacr.org/2018/640
2. Abe, M., Chase, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Constant-size structure-preserving signatures: generic constructions and simple assumptions. J. Cryptol. **29**(4), 833–878 (2016)
3. Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., Ohkubo, M.: Structure-preserving signatures and commitments to group elements. J. Cryptol. **29**(2), 363–421 (2016)
4. Abe, M., Groth, J., Haralambiev, K., Ohkubo, M.: Optimal structure-preserving signatures in asymmetric bilinear groups. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 649–666. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22792-9_37
5. Abe, M., Groth, J., Ohkubo, M.: Separating short structure-preserving signatures from non-interactive assumptions. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 628–646. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_34
6. Abe, M., Groth, J., Ohkubo, M., Tibouchi, M.: Structure-preserving signatures from type II pairings. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 390–407. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44371-2_22. Full version: IACR Cryptology ePrint Archive 2014/312
7. Abe, M., Groth, J., Ohkubo, M., Tibouchi, M.: Structure-preserving signatures from type II pairings. IACR Cryptology ePrint Archive, 2014/312 (2014)
8. Abe, M., Groth, J., Ohkubo, M., Tibouchi, M.: Unified, minimal and selectively randomizable structure-preserving signatures. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 688–712. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54242-8_29
9. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-28628-8_3
10. Boneh, D., Venkatesan, R.: Breaking RSA may not be equivalent to factoring. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 59–71. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0054117
11. Chatterjee, S., Menezes, A.: Type 2 structure-preserving signature schemes revisited. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 286–310. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48797-6_13
12. Coron, J.-S.: Optimal security proofs for PSS and other signature schemes. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 272–287. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_18
13. Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40084-1_8
14. Fuchsbauer, G., Kiltz, E., Loss, J.: The algebraic group model and its applications. Cryptology ePrint Archive, Report 2017/620 (2017). https://eprint.iacr.org/2017/620

15. Fuchsbauer, G., Hanser, C., Slamanig, D.: Practical round-optimal blind signatures in the standard model. IACR Cryptology ePrint Archive 2015/626 (2015). https://eprint.iacr.org/2015/626
16. Galbraith, S.D., Paterson, K.G., Smart, N.P.: Pairings for cryptographers. Discrete Appl. Math. **156**(16), 3113–3121 (2008). Applications of Algebra to Cryptography
17. Garg, S., Bhaskar, R., Lokam, S.V.: Improved bounds on security reductions for discrete log based signatures. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 93–107. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_6
18. Ghadafi, E.: Short structure-preserving signatures. In: Sako, K. (ed.) CT-RSA 2016. LNCS, vol. 9610, pp. 305–321. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-29485-8_18
19. Ghadafi, E.: How low can you go? Short structure-preserving signatures for Diffie-Hellman vectors. In: O'Neill, M. (ed.) IMACC 2017. LNCS, vol. 10655, pp. 185–204. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-71045-7_10
20. Ghadafi, E.: More efficient structure-preserving signatures - or: bypassing the type-III lower bounds. In: Foley, S.N., Gollmann, D., Snekkenes, E. (eds.) ESORICS 2017. LNCS, vol. 10493, pp. 43–61. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66399-9_3
21. Ghadafi, E., Smart, N.P., Warinschi, B.: Groth–sahai proofs revisited. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 177–192. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13013-7_11
22. Jutla, C.S., Roy, A.: Improved structure preserving signatures under standard bilinear assumptions. In: Fehr, S. (ed.) PKC 2017. LNCS, vol. 10175, pp. 183–209. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54388-7_7
23. Kiltz, E., Pan, J., Wee, H.: Structure-preserving signatures from standard assumptions, revisited. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 275–295. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_14
24. Libert, B., Peters, T., Yung, M.: Short group signatures via structure-preserving signatures: standard model security from simple assumptions. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 296–316. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_15
25. Paillier, P., Vergnaud, D.: Discrete-log-based signatures may not be equivalent to discrete log. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 1–20. Springer, Heidelberg (2005). https://doi.org/10.1007/11593447_1
26. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_7