Lower Bounds on Structure-Preserving Signatures for Bilateral Messages

Masayuki Abe[1], Miguel Ambrona[2,3], Miyako Ohkubo[4], and Mehdi Tibouchi[1]

[1] Secure Platform Laboratories, NTT Corporation, Japan
{abe.masayuki,tibouchi.mehdi}@lab.ntt.co.jp
[2] IMDEA Software Institute, Spain
[3] Universidad Politécnica de Madrid, Spain
miguel.ambrona@imdea.org
[4] Security Fundamentals Lab, CSRI, NICT, 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. As its signature size significantly impacts the efficiency of the resulting protocols, finding the optimal size is of great concern. For example, showing one's possession of a valid signature in non-interactive zero-knowledge manner plays an essential role in the construction of cryptographic protocols concerning privacy. A typical approach for efficient instantiation of non-interactive zero-knowledge primitives consists of combining structure-preserving signature schemes [2] over bilinear groups with non-interactive proofs, e.g., [9, 23–25, 27, 30, 32], for relations defined over the same 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 [3], where the authors investigate the case of asymmetric bilinear groups (Type-III groups [18]) 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 (for reductions based on both interactive and non-interactive assumptions). In the case of *bilateral* messages (that contain elements from both source groups), a construction is shown in [3] based on non-interactive assumption, but no lower bounds are provided to argue its optimality. In [7], 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 with respect to 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 [5], 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 with respect to 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

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

		Lower bounds		Upper Bounds (Constructions)		
Setting	Messages	Interactive	Non-interactive	Interactive	Non-interactive	
					q-type	Static
Type-III	Unilateral	3 [3]	4 [4]	3 [3]	4 [3]	6 [28]
	Bilateral	3 [3]	6 (this work)	3 [3]	6 [3]	10 [29]
Type-II	$M \in \mathbb{G}_1$	3 [5]	4 (this work)	3 [7]	7 [2]‡	9 [28]§
	$M \in \mathbb{G}_2$	2 [5]		2 [5]	3 [5]	9 [28]§
	Bilateral	3 [7]	4 (this work)	7 [2]†	7 [2]‡	9 [28]§
Type-I	N/A	3 [7]		3 [7]	7 [2]	9 [28]

bilateral messages and *non-interactive assumptions*, though this is the most general and preferred case in the context of structure-preserving signatures. Note that SPS schemes are often used as a building block of more complex cryptographic primitives. Therefore, in order to be combined with other constructions, and handling *bilateral messages* may be necessary. 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 Section 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 [3], where the authors propose a scheme that includes exactly 3 group elements in every source group. 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 Section 4). Note that the lower bound for unilateral messages in $\mathbb{G}_1$ implies the same lower bound for bilateral messages since messages in $\mathbb{G}_2$ can be efficiently translated into those in $\mathbb{G}_1$ when signing and verifying them. That is because there exists a reduction from bilateral to unilateral messages in $\mathbb{G}_1$. However, this reduction is valid only if the message size is fixed to some $k_1, k_2 \in \mathbb{N}$, i.e., messages belong to $\mathbb{G}_1^{k_1} \times \mathbb{G}_2^{k_2}$, 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 Section 5.

Our approach follows the framework of [4], i.e., we show the existence of a *crucial relation* (see Section 2.7) in the algebraic model [11, 17]. It is known that if such a relation exists, a meta-reduction [13] can be constructed and therefore, 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 compared to the previous cases in [4]. We elaborate this point as follows. We first recap the argument used in [4]. 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

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

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 message M 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 with respect to 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 [4].

In our actual proof in Section 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., [2, 6], whose signature consists of one or two group elements and their security is based on static assumptions. In [20, 21], 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 [1, 28, 29, 31]. The state of the art for static assumptions and Type-III groups is a scheme from [28] with six-element signatures for unilateral messages. For bilateral messages, a scheme presented in [29] yields 10-element signatures. However, we point out that combining the scheme from [28] for messages in $\mathbb{G}_1$ with a partially one-time SPS from [1] for messages in $\mathbb{G}_2$, results in a scheme for bilateral messages with 9 signature elements. A randomizable SPS scheme in [19] 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 [28] yields a scheme with the smallest signature size of 9 when the underlying MDDH assumption [15] is instantiated with the DLIN assumption [10] adjusted to Type-I groups [1].

Structure-preserving signatures over Type-II groups received less attention, even though GS-proofs had been extended to Type-II groups [22]. This may be due to recent results [5] 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 [12], 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

The definitions in this section are mostly borrowed from [4] which our work is based on.

2.1 Notation

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), such that $\rho\boldsymbol{v} = \delta\boldsymbol{w}$.

2.2 Digital Signature Scheme

Definition 1 (Digital Signature Scheme). *A digital signature scheme* Sig *is a set of efficient algorithms* $(\mathcal{C}, \mathcal{K}, \mathcal{S}, \mathcal{V})$*. The* $\mathcal{C}$ *algorithm is the common-parameter generator that takes security parameter* 1^λ *as input and outputs a common parameter* GK*. The* $\mathcal{K}$ *algorithm is the key generator that takes* GK *as input and outputs a signing key* SK *and verification key* VK*. The keys include* GK *and the public key defines a message space* Msp*. The* $\mathcal{S}$ *algorithm is the signature generation algorithm that computes a signature* Σ *for input message* M *by using* SK*. The* $\mathcal{V}$ *algorithm is the verification algorithm that takes* VK*,* M*, and* Σ *and outputs* 1 *or* 0*, which represent acceptance and rejection, respectively.*

A signature scheme must be correct, i.e., it is required that for any key generated using $\mathcal{K}$ and for any message in Msp, it holds that $1 = \mathcal{V}(VK, M, \mathcal{S}(SK, M))$. 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 such that 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* (with respect to VK and M), if $1 = \mathcal{V}(VK, M, \Sigma)$. Otherwise, it is said to be *invalid.*

Definition 2 (EUF-CMA). *A signature scheme* $\mathsf{Sig} = (\mathcal{C}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ *is existentially unforgeable against adaptive chosen message attacks if, for any* $\mathcal{A} \in \mathsf{PPT}$*, the probability*

$$\Pr\left[\begin{array}{l} GK \leftarrow \mathcal{C}(1^\lambda), \\ (VK, SK) \leftarrow \mathcal{K}(GK), \\ (M^\star, \Sigma^\star) \leftarrow \mathcal{A}^{\mathcal{O}}(VK) \end{array} : \begin{array}{l} M^\star \notin Q \wedge \\ 1 \leftarrow \mathcal{V}(VK, M^\star, \Sigma^\star) \end{array}\right]$$

is negligible in λ*. Here,* $\mathcal{O}$ *is a signing oracle that takes message* M *and returns signatures* $\Sigma \leftarrow \mathcal{S}(SK, M)$*. The term* Q *is the set of messages submitted to the signing oracle.*

2.3 Bilinear Groups

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 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$,
- $\forall G \in \mathbb{G}_1 \setminus \{1\}, H \in \mathbb{G}_2 \setminus \{1\}$, $e(G, H)$ generates $\mathbb{G}_T$, and
- $\forall A \in \mathbb{G}_1$, $\forall B \in \mathbb{G}_2$, $\forall x, y \in \mathbb{Z}$: $e(A^x, B^y) = e(A, B)^{xy}$.

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 [18] for their properties.

2.4 Structure Preserving Signatures

For a description of bilinear groups $\Lambda = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$, 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).

Definition 3 (Structure-Preserving Signatures). *A signature scheme $(\mathcal{C}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ is called structure preserving with respect to bilinear group generator $\mathcal{G}$ if*

- *The common parameter GK consists of a group description Λ. Constants a_{ij} in $\mathbb{Z}_p$ are also included in GK if any,*
- *VK includes GK and group elements in $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$,*
- *M consists of group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$,*
- *Σ consists of group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$, and*
- *$\mathcal{V}$ evaluates membership in $\mathbb{G}_1$ and $\mathbb{G}_2$ and PPEs.*

In a narrow sense, structure preserving signature can be further restricted to the case when $Z = 1$ and VK excluding elements in $\mathbb{G}_T$ so that accompanying witness-indistinguishable Groth-Sahai proofs can have the zero-knowledge property.

2.5 Algebraic Algorithms

An algorithm is called algebraic with respect to 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 with respect to $\boldsymbol{X}$. For instance, if the algebraic algorithm $\mathcal{R}$ takes $A, B \in \mathbb{G}_1$ as input and outputs $C \in \mathbb{G}_1$, then $\mathcal{R}$'s extractor $\mathcal{E}$ outputs (a, b) such that $C = A^a B^b$.

In the following, we give a formal definition of the minimal case where an algorithm takes group elements from one group as input and outputs only one group element.

Definition 4 (Algebraic Algorithms for $\mathcal{G}$). *Let $\mathcal{R}$ be a probabilistic polynomial time algorithm that takes $\Lambda = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ generated by $\mathcal{G}$, group elements $\boldsymbol{X}_1 \in \mathbb{G}_1^{k_1}$ and $\boldsymbol{X}_2 \in \mathbb{G}_2^{k_2}$ for some $k_1, k_2 \geq 0$, and a string $aux \in \{0,1\}^*$ as input. It outputs group elements $\boldsymbol{Y}_1$ in $\mathbb{G}_1^{n_1}$, $\boldsymbol{Y}_2$ in $\mathbb{G}_1^{n_2}$ and a string $ext \in \{0,1\}^*$. $\mathcal{R}$ is called algebraic with respect to $\mathcal{G}$ if there exists $\mathcal{E} \in$ PPT such that, given the same input as $\mathcal{R}$ including the same random coins, for any $\Lambda \leftarrow \mathcal{G}(1^\lambda)$ and for all polynomial size $\boldsymbol{X}_1$, $\boldsymbol{X}_2$ and aux, the following probability is negligible in λ.*

$$\Pr\left[\begin{array}{l}(Y_1, Y_2, ext) \leftarrow \mathcal{R}(\Lambda, \boldsymbol{X}_1, \boldsymbol{X}_2, aux\ ; r); \\ (\boldsymbol{y}_1, \boldsymbol{y}_2, ext) \leftarrow \mathcal{E}(\Lambda, \boldsymbol{X}_1, \boldsymbol{X}_2, aux\ ; r)\end{array} \ :\ Y_1 \neq \boldsymbol{X}_1^{\boldsymbol{y}_1} \vee Y_2 \neq \boldsymbol{X}_2^{\boldsymbol{y}_2}\right].$$

It is important to see that elements in $\mathbb{G}_1$ and $\mathbb{G}_2$ are isolated when $\mathcal{R}$ computes Y_1 and Y_2. For notational simplicity, however, we may wrap X_i and Y_i simply by X and Y if the separated treatment is not important for the context.

We stress that, unlike the case of the knowledge of exponent assumptions [14, 26, 8] that assumes the presence of $\mathcal{E}$ for *any malicious* $\mathcal{R}$, here we try to capture the limitation of current technology in building reduction algorithms. It is in fact easy to imagine an algorithm $\mathcal{R}$ that may not be algebraic as defined above; $\mathcal{R}$ takes a string from aux and directly translates it as a group element. For such $\mathcal{R}$ there may not be an efficient extractor $\mathcal{E}$. However, a reduction algorithm that chooses Y in this way will typically not be more useful than one that chooses Y with a known discrete logarithm with respect to $\boldsymbol{X}$. Accordingly, we consider algorithms that compute on explicitly given group elements.

The above definition extends naturally to $\mathcal{R}$ that outputs multiple group elements in both groups. It also extends to interactive and oracle algorithms as follows. We describe interactive algebraic algorithm $\mathcal{R}$ as a sequence of execution $(Y^{(i)}, ext^{(i)}) \leftarrow \mathcal{R}(\Lambda, X^{(i-1)}, aux^{(i-1)})$ for $i = 0$ to n that is some polynomial in λ. Initial input $X^{(0)}$ should be defined appropriately, and every succeeding input $X^{(i)}$ is defined as concatenation of $X^{(i-1)}$ from the previous step and the group elements obtained from the interaction.

(Note that output $Y^{(i)}$ is not included in $X^{(i)}$ as it is redundant with this formulation.) We define $aux^{(i)}$ in the same manner. The total running time of $\mathcal{R}$ should be in a polynomial in λ. We then define interactive extractor $\mathcal{E}$ that takes $(\Lambda, X^{(0)}, aux^{(0)})$ as initial input (with the same randomness as given to $\mathcal{R}$), interacts as well as $\mathcal{R}$ does, and outputs a representation of every $Y^{(i)}$ with respect to bases in $X^{(i-1)}$.

2.6 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 a trivial algorithm $\mathcal{U}$ giving random answers. The following definition follows this intuition.

Definition 5 (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.*

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

Problem $\mathcal{P}$ is called algebraic if algorithm $\mathcal{I}$ is algebraic. That is, $\mathcal{I}$ 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 with respect to 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.

2.7 Crucial Relation

In [4], it is shown that for a certain class of signature schemes and a certain class of reduction algorithms, there exist no reductions from their EUF-CMA security to any non-interactive hardness assumptions if pseudo-random functions exist. That class of signature schemes is characterized by the notion of *crucial relation*. More concretely, it is the class of schemes for which there exists a *crucial relation*. This notion conveniently abstracts sufficient properties on the reduction algorithms so that a meta-reduction algorithm can be built to show the impossibility of the reduction. We briefly recap the framework 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 6 (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 with respect to a class of algorithms $\mathtt{Cls}$ and $n > 0$ if the following properties are provided.*

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

Extractability: For any $\mathcal{R} \in \texttt{Cls}$, there exists $\mathcal{E} \in \texttt{PPT}$ such that, for any $VK \in \{0,1\}^*$ such that $1 \leftarrow TstVk(1^\lambda, VK)$, 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 $\mathcal{B} \in \texttt{PPT}$ such that, 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 [4]. *If a crucial relation for a signature scheme exists with respect to 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 [4]. 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 7) 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:

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

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 public parameters, 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 with respect to 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 equation (5) in the exponent, we have:

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

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

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

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. Without loss of generality, we focus on a verification equation and drop superscript (j) from the notation of public-key elements and relevant variables used in the equation. Let $\mathcal{G}$ be a group generator and $\mathcal{P} = (\mathcal{I}, \mathcal{V}, \mathcal{U})$ be an algebraic non-interactive hard problem over $\mathcal{G}$. Since the instance generator $\mathcal{I}$ is algebraic, an instance *ins* produced by $\mathcal{I}$ is of the form $ins = (Y_1, \ldots, Y_{k_1}, W_1, \ldots, W_{k_2}, ext)$ where $k_1, k_2 \geq 0$, $Y_j \in \mathbb{G}_1$, $W_j \in \mathbb{G}_2$, and *ext* is an arbitrary string that may include the group description Λ (the default generators G and H can be present among Y_j and W_j). Consider an algebraic algorithm $\mathcal{R}$ that first takes *ins* and outputs VK and a state σ. Then, it takes a message (M, N) and state σ and outputs a signature $(R, S, T_1, \ldots, T_\ell)$. For such $\mathcal{R}$, there exists an extractor $\mathcal{E}_{\mathcal{R}}$ that takes the same input (ins, M, N) and the same randomness and outputs representations $(\varphi_{v_i,1}, \ldots, \varphi_{v_i,k_1})$ for $i = \{0,1,2,3\}$, and $(\gamma_{u_i,1}, \ldots, \gamma_{u_i,k_2})$ for $i = \{1,2,3\}$, that satisfy

$$V_i = \textstyle\prod_{j=1}^{k_1} Y_j^{\varphi_{v_i,j}}, \quad U_i = \prod_{j=1}^{k_2} W_j^{\gamma_{u_i,j}}, \tag{8}$$

and $(\varphi_{z_1,1}, \ldots, \varphi_{z_1,k_1})$, $(\gamma_{z_2,1}, \ldots, \gamma_{z_2,k_2})$ that satisfy

$$Z = e(\textstyle\prod_{j=1}^{k_1} Y_j^{\varphi_{z_1,j}}, \prod_{j=1}^{k_2} W_j^{\gamma_{z_2,j}}), \tag{9}$$

and $(\alpha_r, \varphi_r^{(1)}, \ldots, \varphi_r^{(k_1)})$, $(\alpha_s, \varphi_s^{(1)}, \ldots, \varphi_s^{(k_1)})$, $(\beta_i, \gamma_{t_i}^{(1)}, \ldots, \gamma_{t_i}^{(k_2)})$ that satisfy

$$R = \textstyle\prod_{j=1}^{k_1} Y_j^{\varphi_r^{(j)}} M^{\alpha_r}, \quad S = \prod_{j=1}^{k_1} Y_j^{\varphi_s^{(j)}} M^{\alpha_s}, \quad T_i = \prod_{j=1}^{k_2} W_j^{\gamma_{t_i}^{(j)}} N^{\beta_i} \tag{10}$$

for all $i \in \{1, \ldots, \ell\}$. By using $y_j = \log_G Y_j$ and $w_j = \log_H W_j$, we can write

$$v_i = \textstyle\sum_{j=1}^{k_1} \varphi_{v_i,j} y_j, \quad u_i = \sum_{j=1}^{k_2} \varphi_{u_i,j} w_j, \quad z = (\sum_{j=1}^{k_1} \varphi_{z_1,j} y_j)(\sum_{j=1}^{k_2} \varphi_{z_2,j} w_j), \tag{11}$$

$$\varphi_r = \textstyle\sum_j \varphi_r^{(j)} y_j, \quad \varphi_s = \sum_j \varphi_s^{(j)} y_j, \quad \text{and} \quad t_i = \sum_j \gamma_{t_i}^{(j)} w_j + \beta_i n. \tag{12}$$

These u_i, v_i, z, $\alpha_r, \alpha_s, \varphi_r, \varphi_s, t_1, \ldots, t_\ell, n$, and m satisfy (7) for every verification equation j.

For algebraic instance generator $\mathcal{I}$, there exists an extractor $\mathcal{E}_{\mathcal{I}}$ that outputs a representation $(y_1, \ldots, y_{k_1}, w_1, \ldots, w_{k_2})$ for the group elements in *ins*. Given $\mathcal{R}$, $\mathcal{E}_{\mathcal{R}}$, $\mathcal{I}$, and $\mathcal{E}_{\mathcal{I}}$, we construct algorithm $\mathcal{D}$ that takes a discrete-log instance (Λ, G, Y) in $\mathbb{G}_1$ and outputs x such that $Y = G^x$. Algorithm $\mathcal{D}$ selects a default generator $H \in \mathbb{G}_2$, runs $\mathcal{I}$ with input (Λ, G, H), and receives an instance *ins*. Then it runs $\mathcal{R}$ with input *ins* and receives VK. It selects a random n and sets $M := Y$, $N := H^n$, gives (M, N) to $\mathcal{R}$, and receives a signature $(R, S, T_1, \ldots, T_\ell)$. Since *ins* and (M, N) distribute as expected by $\mathcal{R}$, $\mathcal{R}$ must work correctly and $(R, S, T_1, \ldots, T_\ell)$ must be a valid signature with non-negligible probability in λ. Algorithm $\mathcal{D}$ now runs extractors $\mathcal{E_I}$ and $\mathcal{E_R}$. From their outputs, $\mathcal{D}$ obtains all u_i, v_i, z and $(\alpha_r, \alpha_s, \varphi_r, \varphi_s, t_1, \ldots, t_\ell)$. If $\mathcal{E_R}$ is successful, they satisfy (7) with respect to $m = \log_G M$. Therefore, if (7) is not trivial, $\mathcal{D}$ solves the linear equation in m and returns it as $\log_G Y$. □

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

$$(u_1^{(j)} + \textstyle\sum_{i=1}^{\ell} a_i^{(j)} t_i + d_1^{(j)} n)\alpha_r + (u_2^{(j)} + \sum_{i=1}^{\ell} b_i^{(j)} t_i + d_2^{(j)} n)\alpha_s + (u_3^{(j)} + \sum_{i=1}^{\ell} c_i^{(j)} t_i + d_3^{(j)} n) = 0 \quad (13)$$

$$(u_1^{(j)} + \textstyle\sum_{i=1}^{\ell} a_i^{(j)} t_i + d_1^{(j)} n)\varphi_r + (u_2^{(j)} + \sum_{i=1}^{\ell} b_i^{(j)} t_i + d_2^{(j)} n)\varphi_s + (v_0^{(j)} n + \sum_{i=1}^{\ell} v_i^{(j)} t_i - z^{(j)}) = 0 \quad (14)$$

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 (13) and (14) as polynomials in n by collecting the corresponding terms:

$$\begin{aligned}&\big\{(d_1^{(j)}+\textstyle\sum_{i=1}^{\ell} a_i^{(j)}\beta_i)\alpha_r+(d_2^{(j)}+\sum_{i=1}^{\ell} b_i^{(j)}\beta_i)\alpha_s+(d_3^{(j)}+\sum_{i=1}^{\ell} c_i^{(j)}\beta_i)\big\}n\\ &+\big\{(u_1^{(j)}+\textstyle\sum_{i=1}^{\ell} a_i^{(j)}\gamma_i)\alpha_r+(u_2^{(j)}+\sum_{i=1}^{\ell} b_i^{(j)}\gamma_i)\alpha_s+(u_3^{(j)}+\sum_{i=1}^{\ell} c_i^{(j)}\gamma_i)\big\} = 0 \quad (15)\\ &\big\{(d_1^{(j)}+\textstyle\sum_{i=1}^{\ell} a_i^{(j)}\beta_i)\varphi_r+(d_2^{(j)}+\sum_{i=1}^{\ell} b_i^{(j)}\beta_i)\varphi_s+(v_0^{(j)}+\sum_{i=1}^{\ell} v_i^{(j)}\beta_i)\big\}n\\ &+\big\{(u_1^{(j)}+\textstyle\sum_{i=1}^{\ell} a_i^{(j)}\gamma_i)\varphi_r+(u_2^{(j)}+\sum_{i=1}^{\ell} b_i^{(j)}\gamma_i)\varphi_s+(-z^{(j)}+\sum_{i=1}^{\ell} v_i^{(j)}\gamma_i)\big\} = 0 \quad (16)\end{aligned}$$

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 equations (15) and (16) 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:

$$(d_1^{(j)}+\textstyle\sum_{i=1}^{\ell} a_i^{(j)}\beta_i)\alpha_r+(d_2^{(j)}+\sum_{i=1}^{\ell} b_i^{(j)}\beta_i)\alpha_s+(d_3^{(j)}+\sum_{i=1}^{\ell} c_i^{(j)}\beta_i) = 0 \quad (17)$$

$$(u_1^{(j)}+\textstyle\sum_{i=1}^{\ell} a_i^{(j)}\gamma_i)\alpha_r+(u_2^{(j)}+\sum_{i=1}^{\ell} b_i^{(j)}\gamma_i)\alpha_s+(u_3^{(j)}+\sum_{i=1}^{\ell} c_i^{(j)}\gamma_i) = 0 \quad (18)$$

$$(d_1^{(j)}+\textstyle\sum_{i=1}^{\ell} a_i^{(j)}\beta_i)\varphi_r+(d_2^{(j)}+\sum_{i=1}^{\ell} b_i^{(j)}\beta_i)\varphi_s+(v_0^{(j)}+\sum_{i=1}^{\ell} v_i^{(j)}\beta_i) = 0 \quad (19)$$

$$(u_1^{(j)}+\textstyle\sum_{i=1}^{\ell} a_i^{(j)}\gamma_i)\varphi_r+(u_2^{(j)}+\sum_{i=1}^{\ell} b_i^{(j)}\gamma_i)\varphi_s+(-z^{(j)}+\sum_{i=1}^{\ell} v_i^{(j)}\gamma_i) = 0 \quad (20)$$

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 the discrete logarithm 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:

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

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 as we will show in (27) or (29) in case of the $\mathbb{G}_2$ part of the signature. 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 7 (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 such that $\mathtt{Dt}_{j,k}(n, t_1, \ldots, t_\ell) \neq 0$. Let $\alpha_r, \alpha_s \in \mathbb{Z}_p$ satisfy equation (13) 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, such that one and only one of the following the expressions A^t_j and B^t_j is zero. Let j be the index of the first equation that satisfies the previous condition. If $A^t_j = 0$ and $\varpi = (0, \alpha_s, \bot, \ldots, \bot)$ where $B^t_j \alpha_s + C^t_j = 0$ then return 1, else if $B^t_j = 0$ and $\varpi = (\alpha_r, 0, \bot, \ldots, \bot)$ where $A^t_j \alpha_r + C^t_j = 0$ then return 1, else return 0.*
4. *If all verification equations are degenerate, i.e. for all j, $A^t_j = B^t_j = C^t_j = V^t_j = 0$, if $\varpi = (\bot, \ldots, \bot)$ return 1, else return 0.*
5. *If there exists $\beta = (\beta_1, \ldots, \beta_\ell) \in \mathbb{Z}_p^\ell$ such that 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:*

$$\begin{pmatrix} A^\beta_j & B^\beta_j & C^\beta_j & V^\beta_j & A^\gamma_j & B^\gamma_j & C^\gamma_j & V^\gamma_j \end{pmatrix} \equiv \begin{pmatrix} A^\beta_k & B^\beta_k & C^\beta_k & V^\beta_k & A^\gamma_k & B^\gamma_k & C^\gamma_k & V^\gamma_k \end{pmatrix}$$

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

$$\begin{pmatrix} u_1^{(j^*)} & d_1^{(j^*)} & a_1^{(j^*)} & \ldots & a_\ell^{(j^*)} \end{pmatrix} \mu_1 + \begin{pmatrix} u_2^{(j^*)} & d_2^{(j^*)} & b_1^{(j^*)} & \ldots & b_\ell^{(j^*)} \end{pmatrix} \mu_2 + \begin{pmatrix} u_3^{(j^*)} & d_3^{(j^*)} & c_1^{(j^*)} & \ldots & c_\ell^{(j^*)} \end{pmatrix} \mu_3 = 0$$

   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 $\beta = (\beta_1, \ldots, \beta_\ell) \in \mathbb{Z}_p^\ell$ such that for every verification equation j,*

$$A^\beta_j = 0 \wedge B^\beta_j = 0 \wedge C^\beta_j = 0 \wedge V^\beta_j = 0$$

   if $\varpi = (\beta_1, \ldots, \beta_\ell)$ then return 1, else return 0.
8. *In any other case, if $\varpi = (\alpha_r, 0, \bot, \ldots, \bot)$ such that, if we set $\alpha_s = 0$, for every verification equation j, it holds $A^t_j \alpha_r + B^t_j \alpha_s + C^t_j = 0$ then return 1, else return 0.*

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

Proof. We show that Ψ has *uniqueness*, *usefulness*, and *extractability* as defined for a crucial relation. 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 such that

$$\operatorname{rank} \begin{pmatrix} a_1^{(1)} \, b_1^{(1)} \, c_1^{(1)} \, v_1^{(1)} \ldots a_1^{(k)} \, b_1^{(k)} \, c_1^{(k)} \, v_1^{(k)} \\ \vdots \\ a_\ell^{(1)} \, b_\ell^{(1)} \, c_\ell^{(1)} \, v_\ell^{(1)} \ldots a_\ell^{(k)} \, b_\ell^{(k)} \, c_\ell^{(k)} \, v_\ell^{(k)} \end{pmatrix} = \ell \qquad (21)$$

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 need to show that every valid transcript θ admits one and only one witness ϖ such that $1 = \Psi(\theta, \varpi)$. 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), $\mathtt{Dt}_{j,k}(n, t_1, \dots, t_\ell) \neq 0$. Note that, there can only exist a *unique* pair (α_r, α_s) satisfying equation (13) for both j and k, because $\mathtt{Dt}_{j,k}(n, t_1, \dots, t_\ell) \neq 0$. 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 such that $B_j^t \alpha_s + C_j^t = 0$. 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 $i \in \{1, \dots, \ell\}$ 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,

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

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, we would have (we omit indices j for simplicity),

$$\alpha_r = \frac{(u_2 + \sum_{i=1}^\ell b_i \gamma_i')(u_3 + \sum_{i=1}^\ell c_i(\beta_i + \delta_i)) - (d_2 + \sum_{i=1}^\ell b_i(\beta_i + \delta_i))(u_3 + \sum_{i=1}^\ell c_i \gamma_i')}{(u_1 + \sum_{i=1}^\ell a_i \gamma_i')(d_2 + \sum_{i=1}^\ell b_i(\beta_i + \delta_i)) - (d_1 + \sum_{i=1}^\ell a_i(\beta_i + \delta_i))(u_2 + \sum_{i=1}^\ell b_i \gamma_i')}$$

where we use γ_i' instead of $(t_i - (\beta_i + \delta_i)n$ for brevity. By rearranging terms we can express the above equation as

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

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

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

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

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

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):

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

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

$$\begin{pmatrix}\beta_1 \ldots \beta_\ell\end{pmatrix} \mathsf{M} = \begin{pmatrix} -d_1^{(1)} & -d_2^{(1)} & -d_3^{(1)} & -v_0^{(1)} & -d_1^{(2)} & \ldots & -d_1^{(k)} & -d_2^{(k)} & -d_3^{(k)} & -v_0^{(k)}\end{pmatrix}$$

where M is the matrix from equation (21). 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 such that all equations $(17)^{(*)}$ are be proportional between them and to all equations $(18)^{(*)}$ (when considering them as linear equations in α_r, α_s).

Proof. Assume that the groups of equations $(17)^{(*)}$ and $(18)^{(*)}$ are not proportional. We will show that under this condition 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

$$A_j^\beta B_k^\beta - A_k^\beta B_j^\beta = 0 \tag{22}$$

$$A_j^\beta B_k^\gamma - A_k^\gamma B_j^\beta \,+\, A_j^\gamma B_k^\beta - A_k^\beta B_j^\gamma = 0 \tag{23}$$

$$A_j^\gamma B_k^\gamma - A_k^\gamma B_j^\gamma = 0 \tag{24}$$

Let $(\mathsf{x})^{(j)}$ denote equation (x) with respect to j-th verification equation. Equation (22) implies that, when considering the relations $(17)^{(j)}$ for all j as equations in α_r, α_s, they are all proportional. The same happens with equations $(18)^{(j)}$ due to (24).

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 $\rho \in \mathbb{Z}_p$ such that $A_j^\beta = \rho A_k^\beta$ 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 $\delta \in \mathbb{Z}_p$ such that $A_j^\gamma = \delta A_k^\gamma$ and $B_j^\gamma = \delta B_k^\gamma$. Now, substituting in equation (23) we have

$$\rho A_k^\beta B_k^\gamma - A_k^\gamma \rho B_k^\beta \,+\, \delta A_k^\gamma B_k^\beta - A_k^\beta \delta B_k^\gamma = (\rho - \delta)(A_k^\beta B_k^\gamma - A_k^\gamma B_k^\beta) = 0 \tag{25}$$

Because the groups of equations $(17)^{(*)}$ and $(18)^{(*)}$ 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 equations $(17)^{(j)}$ and $(17)^{(k)}$ is the same as the linear factor between equations $(18)^{(j)}$ and $(18)^{(k)}$. With similar techniques, it can be shown that in this situation happens between A and C and so on. In fact, it must hold

$$\begin{pmatrix} A^\beta_j & B^\beta_j & C^\beta_j & V^\beta_j & A^t_j & B^t_j & C^t_j & V^t_j \end{pmatrix} \equiv \begin{pmatrix} A^\beta_k & B^\beta_k & C^\beta_k & V^\beta_k & A^t_k & B^t_k & C^t_k & V^t_k \end{pmatrix}$$

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

Therefore, if clause 8 is reached, all equations in $(17)^{(*)}$ must be proportional to all equations $(18)^{(*)}$. □

At this point, we know that all equations of the form $A^\beta_j \alpha_r + B^\beta_j \alpha_s + C^\beta_j = 0$ are proportional between them for all j (looking at them as linear equations in α_r, α_s) and they are all proportional to $A^\gamma_j \alpha_r + B^\gamma_j \alpha_s + C^\gamma_j = 0$ for all j. This implies that they are also all proportional to $A^t_j \alpha_r + B^t_j \alpha_s + C^t_j = 0$ 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, $A^t_{j^*} \neq 0$ and therefore, there exists a unique value $\alpha_r \in \mathbb{Z}_p$ such that $A^t_{j^*} \alpha_r + B^t_{j^*} \cdot 0 + C^t_{j^*} = 0$. Therefore, the witness is unique in this branch.

Usefulness. If the relation $\Psi(\theta, \varpi)$ is satisfied in clause 4, then all the equations are degenerate and a forgery can be created by reusing the elements from $\mathbb{G}_2$. This is, $(*, *, T_1, \dots, T_\ell) \in \mathbb{G}_1^2 \times \mathbb{G}_2^\ell$ is a valid signature on message $(*, N) \in \mathbb{G}_1 \times \mathbb{G}_2$, where placeholders $*$ can be filled with arbitrary elements from $\mathbb{G}_1$.

If the relation is satisfied in clauses $2, 3, 5, 8$ note that in all of them the witness must be of the form $(\alpha_r, \alpha_s, \perp, \dots, \perp)$, where $\alpha_r, \alpha_s \in \mathbb{Z}_p$ and they satisfy $A^t_j \alpha_r + B^t_j \alpha_s + C^t_j = 0$ for all verification equations j. Or equivalently,

$$(u_1^{(j)} + d_1^{(j)} n + \textstyle\sum_{i=1}^\ell a_i^{(j)} t_i)\alpha_r + (u_2^{(j)} + d_2^{(j)} n + \sum_{i=1}^\ell b_i^{(j)} t_i)\alpha_s + (u_3^{(j)} + d_3^{(j)} n + \sum_{i=1}^\ell c_i^{(j)} t_i) = 0 \tag{26}$$

Under these conditions, we can build a forgery as follows. Select an arbitrary fresh message $M^\star \in \mathbb{G}_1$ and compute $R^\star = R(M^\star/M)^{\alpha_r}$, $S^\star = S(M^\star/M)^{\alpha_s}$. Then output $(R^\star, S^\star, T_1, \dots, T_\ell)$ for forged messages $(M^\star, N)$. To verify that the forgery is valid, examine a generic verification predicate:

$$\begin{aligned}
&e(R^\star, U_1 N^{d_1} \textstyle\prod_{i=1}^\ell T_i^{a_i})\, e(S^\star, U_2 N^{d_2} \prod_{i=1}^\ell T_i^{b_i})\, e(M^\star, U_3 N^{d_3} \prod_{i=1}^\ell T_i^{c_i})\, e(V_0, N) \prod_{i=1}^\ell e(V_i, T_i) \\
&= e(R(M^\star/M)^{\alpha_r}, U_1 N^{d_1} \textstyle\prod_{i=1}^\ell T_i^{a_i})\, e(S(M^\star/M)^{\alpha_s}, U_2 N^{d_2} \prod_{i=1}^\ell T_i^{b_i}) \\
&\qquad e(M^\star/M, U_3 N^{d_3} \textstyle\prod_{i=1}^\ell T_i^{c_i})\, e(M, U_3 N^{d_3} \prod_{i=1}^\ell T_i^{c_i})\, e(V_0, N) \prod_{i=1}^\ell e(V_i, T_i) \\
&= e(R, U_1 N^{d_1} \textstyle\prod_{i=1}^\ell T_i^{a_i})\, e(S, U_2 N^{d_2} \prod_{i=1}^\ell T_i^{b_i})\, e(M, U_3 N^{d_3} \prod_{i=1}^\ell T_i^{c_i})\, e(V_0, N) \prod_{i=1}^\ell e(V_i, T_i) \\
&\qquad e(M^\star/M, \{U_1 N^{d_1} \textstyle\prod_{i=1}^\ell T_i^{a_i}\}^{\alpha_r} \{U_2 N^{d_2} \prod_{i=1}^\ell T_i^{b_i}\}^{\alpha_s} \{U_3 N^{d_3} \prod_{i=1}^\ell T_i^{c_i}\}) \\
&= Z e(M^\star/M, H)^{\Phi} = Z,
\end{aligned} \tag{27}$$

where $\Phi = (u_1 + d_1 n + \sum_{i=1}^\ell a_i t_i)\alpha_r + (u_2 + d_2 n + \sum_{i=1}^\ell b_i t_i)\alpha_s + (u_3 + d_3 n + \sum_{i=1}^\ell c_i t_i)$, and $\Phi = 0$ due to (26).

Now, consider the case where Ψ is satisfied in clause 6. There must exist a non-degenerate verification equation, j^* such that there exist $\mu_1, \mu_2, \mu_3 \in \mathbb{Z}_p$, which are *publicly computable* and verify

$$\begin{pmatrix} u_1^{(j^*)} & d_1^{(j^*)} & a_1^{(j^*)} & \dots & a_\ell^{(j^*)} \end{pmatrix} \mu_1 + \begin{pmatrix} u_2^{(j^*)} & d_2^{(j^*)} & b_1^{(j^*)} & \dots & b_\ell^{(j^*)} \end{pmatrix} \mu_2 + \begin{pmatrix} u_3^{(j^*)} & d_3^{(j^*)} & c_1^{(j^*)} & \dots & c_\ell^{(j^*)} \end{pmatrix} \mu_3 = 0$$

In these conditions, we can attack by first finding such coefficients μ_1, μ_2, μ_3, with $\mu_3 \neq 0$ (note that clause 6 guarantees that μ_3 can be taken not null). We set $R^\star = RG^{\mu_1}$, $S^\star = SG^{\mu_2}$, $M^\star = MG^{\mu_3}$ and $(R^\star, S^\star, T_1, \dots, T_\ell)$ is a valid forgery for message $(M^\star, N)$. Note that $M^\star \neq M$ because $\mu_3 \neq 0$. This signature clearly satisfies the j^*-th verification equation. Note that the rest of verification also hold because j^* is a non-degenerate equation and Claim 2 guarantees that at this point all must the verification equations be proportional between them (when $T_1, \dots, T_\ell, N$ are reused).

Finally, if the relation Ψ is satisfied in clause 7, the witness $\varpi = (\beta_1, \dots, \beta_\ell)$ is such that for every verification equation j,

$$d_1^{(j)} + \textstyle\sum_{i=1}^\ell a_i^{(j)} \beta_i = 0 \quad d_2^{(j)} + \sum_{i=1}^\ell b_i^{(j)} \beta_i = 0 \quad d_3^{(j)} + \sum_{i=1}^\ell c_i^{(j)} \beta_i = 0 \quad v_0^{(j)} + \sum_{i=1}^\ell v_i^{(j)} \beta_i = 0 \tag{28}$$

A forgery can be built as follows. Select an arbitrary $\delta \in \mathbb{Z}_p^*$ and compute $N^\star = N^{\delta+1}$ and $T_i{}^\star = T_i N^{\delta\beta_i}$, for $i \in \{1, \ldots, \ell\}$. Then output $(R, S, T_1{}^\star, \ldots, T_\ell{}^\star)$ for forged messages $(M, N^\star)$. To see that it is a valid forgery, consider the following generic verification equation:

$$\begin{aligned}
& e(R, U_1 N^{\star d_1} \textstyle\prod_{i=1}^{\ell} T_i{}^{\star a_i})\, e(S, U_2 N^{\star d_2} \prod_{i=1}^{\ell} T_i{}^{\star b_i})\, e(M, U_3 N^{\star d_3} \prod_{i=1}^{\ell} T_i{}^{\star c_i})\, e(V_0, N^\star) \prod_{i=1}^{\ell} e(V_i, T_i{}^\star) \\
&= e(R, U_1 N^{d_1} N^{d_1\delta} \textstyle\prod_{i=1}^{\ell} T_i^{a_i} N^{a_i\beta_i\delta})\, e(S, U_2 N^{d_2} N^{d_2\delta} \prod_{i=1}^{\ell} T_i^{b_i} N^{b_i\beta_i\delta}) \\
&\quad \cdot e(M, U_3 N^{d_3} N^{d_3\delta} \textstyle\prod_{i=1}^{\ell} T_i^{c_i} N^{c_i\beta_i\delta})\, e(V_0, N^{1+\delta}) \prod_{i=1}^{\ell} e(V_i, T_i N^{v_i\beta_i\delta}) \\
&= Z e(R, N^{\delta(d_1+\Sigma_{i=1}^{\ell} a_i\beta_i)}) e(S, N^{\delta(d_2+\Sigma_{i=1}^{\ell} b_i\beta_i)}) e(M, N^{\delta(d_3+\Sigma_{i=1}^{\ell} c_i\beta_i)}) e(G, N^{\delta(v_0+\Sigma_{i+1}^{\ell} v_i\beta_i)}) = Z
\end{aligned} \tag{29}$$

where the last step is due to (28).

Extractability. We extract $(\alpha_r, \alpha_s, \beta_1, \ldots, \beta_\ell)$ from the first signature $(R, S, T_1, \ldots, T_\ell)$ in θ for message (M, N) by using the algebraic extractor. Note that these extracted values must satisfy equations (17)-(20) when we set $\gamma_i = t_i - n\beta_i$ for every $i \in \{1, \ldots, \ell\}$ and we set $\varphi_r = r - m\alpha_r$ and $\varphi_s = s - m\alpha_s$.

We need to identify if there exist two verification equations j, k such that $\mathtt{Dt}_{j,k}(n, t_1, \ldots, t_\ell) \neq 0$. Remember that the determinant can be expressed like:

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

Note that for the extracted values, the above polynomial is zero if an only if all the coefficients of n are zero (as argued in above). First observe that parameters in the coefficients of $(17)^{(j)}$ and $(17)^{(k)}$ are $d_i^{(j)}$, $a_i^{(j)}$, $b_i^{(j)}$, $c_i^{(j)}$, $d_i^{(k)}$, $a_i^{(k)}$, $b_i^{(k)}$, $c_i^{(k)}$ and β_i. Since they are all public or available after the extraction, verifying $A_j^\beta B_k^\beta - A_k^\beta B_j^\beta = 0$ can be easily done. Next, $A_j^\beta B_k^\gamma - A_k^\gamma B_j^\beta \, + \, A_j^\gamma B_k^\beta - A_k^\beta B_j^\gamma = 0$ can be verified by evaluating:

$$\begin{aligned}
&\left(U_1^{(k)} N^{d_1} \textstyle\prod_{i=1}^{\ell} (T_i N^{-\beta_i})^{a_i^{(k)}}\right)^{B_j^\beta} \left(U_2^{(j)} N^{d_2} \prod_{i=1}^{\ell} (T_i N^{-\beta_i})^{b_i^{(j)}}\right)^{A_k^\beta} \\
&\stackrel{?}{=} \left(U_2^{(k)} N^{d_2} \textstyle\prod_{i=1}^{\ell} (T_i N^{-\beta_i})^{b_i^{(k)}}\right)^{A_j^\beta} \left(U_1^{(j)} N^{d_1} \prod_{i=1}^{\ell} (T_i N^{-\beta_i})^{a_i^{(j)}}\right)^{B_k^\beta}
\end{aligned} \tag{30}$$

Finally, to verify $A_j^\gamma B_k^\gamma - A_k^\gamma B_j^\gamma = 0$, pick two distinct pairs of (α_r, α_s) that satisfy (17). Then check if both of them satisfy $(18)^{(j)}$ and $(18)^{(k)}$. In that case, it must be $A_j^\gamma B_k^\gamma - A_k^\gamma B_j^\gamma = 0$. If any of the checks failed for a pair of equations j, k, we conclude that $\mathtt{Dt}_{j,k}(n, t_1, \ldots, t_\ell) \neq 0$ and output $\varpi = (\alpha_r, \alpha_s, \perp, \ldots, \perp)$.

Now we check clause 3, if there exists j such that $U_1^{(j)} N^{d_1} \prod_{i=1}^{\ell} (T_i)^{a_i^{(j)}} = 1_{\mathbb{G}_2}$ and $U_2^{(j)} N^{d_2} \prod_{i=1}^{\ell} (T_i)^{b_i^{(j)}} \neq 1_{\mathbb{G}_2}$ then output $\varpi = (0, \alpha_s, \perp, \ldots, \perp)$. Else if $U_1^{(j)} N^{d_1} \prod_{i=1}^{\ell} (T_i)^{a_i^{(j)}} \neq 1_{\mathbb{G}_2}$ and $U_2^{(j)} N^{d_2} \prod_{i=1}^{\ell} (T_i)^{b_i^{(j)}} = 1_{\mathbb{G}_2}$ for some j, output $\varpi = (\alpha_r, 0, \perp, \ldots, \perp)$. Otherwise, continue to the next clause.

Now, if for all verification equations j, $U_1^{(j)} N^{d_1} \prod_{i=1}^{\ell} (T_i)^{a_i^{(j)}} = U_2^{(j)} N^{d_2} \prod_{i=1}^{\ell} (T_i)^{b_i^{(j)}} = 1_{\mathbb{G}_2}$ we are in the condition of clause 4 and we can set the witness to $\varpi = (\perp, \ldots, \perp)$.

For clause 5, first observe that A_j^β, B_j^β, C_j^β for any j can be computed in $\mathbb{Z}_p$ using β_i and public parameters. Thus checking $(A_j^\beta \;\; B_j^\beta \;\; C_j^\beta) \equiv (A_k^\beta \;\; B_k^\beta \;\; C_k^\beta)$ is trivial. For V_j^β and V_k^β, it suffices to check $A_k^\beta V_j^\beta = A_j^\beta V_k^\beta$ by verifying

$$(V_0^{(j)} \textstyle\prod_{i=1}^{\ell} (V_i^{(j)})^{\beta_i})^{(d_1^{(k)} + \Sigma_{i=1}^{\ell} a_i^{(k)} \beta_i)} = (V_0^{(k)} \prod_{i=1}^{\ell} (V_i^{(k)})^{\beta_i})^{(d_1^{(j)} + \Sigma_{i=1}^{\ell} a_i^{(j)} \beta_i)}$$

in $\mathbb{G}_1$. For A_j^t, B_j^t, C_j^t, A_k^t , B_k^t, C_k^t, a similar verification can be done in $\mathbb{G}_2$. For instance, for A_j^t and A_k^t, it suffices to check relation $A_k^\beta A_j^t = A_j^\beta A_k^t$ by verifying

$$(U_1^{(j)} N^{d_1^{(j)}} \textstyle\prod_{i=1}^{\ell} T_i^{a_i^{(j)}})^{(d_1^{(k)} + \Sigma_{i=1}^{\ell} a_i^{(k)} \beta_i)} = (U_1^{(k)} N^{d_1^{(k)}} \prod_{i=1}^{\ell} T_i^{a_i^{(k)}})^{(d_1^{(j)} + \Sigma_{i=1}^{\ell} a_i^{(j)} \beta_i)}$$

in $\mathbb{G}_2$. Finally, for V_j^t and V_k^t, we check relation $A_k^\beta V_j^t = A_j^\beta V_k^t$ by verifying

$$\{e(V_0^{(j)}, N) \textstyle\prod_{i=1}^{\ell} e(V_i^{(j)}, T_i)/Z^{(j)}\}^{(d_1^{(k)} + \Sigma_{i=1}^{\ell} a_i^{(k)} \beta_i)} = \{e(V_0^{(k)}, N) \prod_{i=1}^{\ell} e(V_i^{(k)}, T_i)/Z^{(k)}\}^{(d_1^{(j)} + \Sigma_{i=1}^{\ell} a_i^{(j)} \beta_i)}.$$

Condition $A_j^\beta B_k^\beta - A_k^\beta B_j^\beta = 0$ is indeed $(d_1^{(j)} + \Sigma_{i=1}^\ell a_i^{(j)}\beta_i)(d_2^{(k)} + \Sigma_{i=1}^\ell b_i^{(k)}\beta_i) - (d_1^{(k)} + \Sigma_{i=1}^\ell a_i^{(k)}\beta_i)(d_2^{(j)} + \Sigma_{i=1}^\ell b_i^{(j)}\beta_i) = 0$ which can be verified easily in $\mathbb{Z}_p$. $A_j^\beta B_k^\gamma - A_k^\gamma B_j^\beta \neq 0$ is verified by

$$\{U_1^{(j)} \textstyle\prod_{i=1}^\ell (T_i/N^{\beta_i})^{a_i^{(j)}}\}^{d_2^{(k)} + \Sigma_{i=1}^\ell b_i^{(k)}\beta_i} \,/\, \{U_2^{(j)} \textstyle\prod_{i=1}^\ell (T_i/N^{\beta_i})^{b_i^{(j)}}\}^{d_1^{(k)} + \Sigma_{i=1}^\ell a_i^{(k)}\beta_i} \neq 1_{\mathbb{G}_2}.$$

Similarly, we can check $A_j^\gamma B_k^\beta - A_k^\beta B_j^\gamma \neq 0$ by

$$\{U_2^{(k)} \textstyle\prod_{i=1}^\ell (T_i/N^{\beta_i})^{b_i^{(k)}}\}^{d_1^{(j)} + \Sigma_{i=1}^\ell a_i^{(j)}\beta_i} \,/\, \{U_1^{(k)} \textstyle\prod_{i=1}^\ell (T_i/N^{\beta_i})^{a_i^{(k)}}\}^{d_2^{(j)} + \Sigma_{i=1}^\ell b_i^{(j)}\beta_i} \neq 1_{\mathbb{G}_2}.$$

Once the above verifications succeed, condition $A_j^\gamma B_k^\gamma - A_k^\gamma B_j^\gamma = 0$ holds as well. We then set $\varpi = (\alpha_r, \alpha_s, \perp, \dots, \perp)$.

Checking the condition on clause 6 can be done by solving the system of equations and finding the publicly computable μ_1, μ_2, μ_3 if it exists. In case $\mu_3 \neq 0$ can be found, we set $\varpi = (\perp, \dots, \perp)$. Otherwise, the values values μ_1, μ_2 are not null and such that for every verification equation j, $A_j^t \mu_1 + B_j^t \mu_2 = 0$. Note that, in that case, for every $\delta \in \mathbb{Z}_p$, we can combine (μ_1, μ_2) with the extracted (α_r, α_s) and get

$$A_j^t(\alpha_r + \delta\mu_1) + B_j^t(\alpha_s + \delta\mu_2) + C_j^t = 0$$

and therefore, we can choose $\delta = -\alpha_s/\mu_2$ and set the witness $\varpi = (\alpha_r - \alpha_s\mu_1/\mu_2, 0, \perp, \dots, \perp)$ that satisfies clause 8 (when coming from clause 6).

Now we examine clause 7. It is in this clause when we use the restriction $\ell \leq 3$. If there exists an equation j such that

$$\operatorname{rank} \begin{pmatrix} d_1^{(j)} & a_1^{(j)} & \dots & a_\ell^{(j)} \\ d_2^{(j)} & b_1^{(j)} & \dots & b_\ell^{(j)} \\ d_3^{(j)} & c_1^{(j)} & \dots & c_\ell^{(j)} \end{pmatrix} = 3$$

we can solve the system $A_j^{\hat\beta}$ for $\hat\beta_1, \dots, \hat\beta_\ell$ (if there exists a solution) and in case there is a solution, check whether it satisfies $A_j^{\hat\beta} = 0 \wedge B_j^{\hat\beta} = 0 \wedge C_j^{\hat\beta} = 0 \wedge V_j^{\hat\beta} = 0$ for all equations j. We note that, because the above range is 3 and the dimension of β is at most 3, either there do not exist the mentioned $\hat\beta_i$ or they are unique and can be extracted by solving a linear system with known coefficients. If the answer is affirmative, we are in clause 7 and we output $\varpi = (\hat\beta_1, \dots, \hat\beta_\ell)$, otherwise we go to check clause 8. In case the above rank is 2 for every verification equation we will show that the extracted $(\beta_1, \dots, \beta_\ell)$ from the extractor algorithm is a solution to the system of clause 7 for all equations. It is clear that the system is satisfied for all degenerated equations. Now, pick a non-degenerate equation j. There exist coefficients $\rho_1, \rho_2, \rho_3 \in \mathbb{Z}_p$, not all null, such that

$$\begin{pmatrix} d_1^{(j)} & a_1^{(j)} & \dots & a_\ell^{(j)} \end{pmatrix} \rho_1 + \begin{pmatrix} d_2^{(j)} & b_1^{(j)} & \dots & b_\ell^{(j)} \end{pmatrix} \rho_2 + \begin{pmatrix} d_3^{(j)} & c_1^{(j)} & \dots & c_\ell^{(j)} \end{pmatrix} \rho_3 = 0$$

assume ρ_3 is not zero (the other cases are analogous). And set $\hat\rho_1 = -\rho_1/\rho_3$ and $\hat\rho_2 = -\rho_2/\rho_3$. Because at this point, equations (17) and (18) must be proportional, we have $\begin{pmatrix} A_j^\beta & B_j^\beta & C_j^\beta \end{pmatrix} \equiv \begin{pmatrix} A_j^\gamma & B_j^\gamma & C_j^\gamma \end{pmatrix}$. Therefore, there exist constants δ_1, δ_2 not both null such that $\delta_1 A_j^\beta = \delta_2 A_j^\gamma$ and $\delta_1 B_j^\beta = \delta_2 B_j^\gamma$ and $\delta_1 C_j^\beta = \delta_2 C_j^\gamma$. Note that, additionally,

$$C_j^\beta = \hat\rho_1 A_j^\beta + \hat\rho_2 B_j^\beta \qquad \text{and} \qquad C_j^\gamma = u_3 + \hat\rho_1(A_j^\gamma - u_1) + \hat\rho_2(B_j^\gamma - u_2)$$

multiplying by δ_1 and δ_2 respectively and comparing the previous equations we get,

$$\delta_1\hat\rho_1 A_j^\beta + \delta_1\hat\rho_2 B_j^\beta = \delta_2 u_3 + \delta_2\hat\rho_1(A_j^\gamma - u_1) + \delta_2\hat\rho_2(B_j^\gamma - u_2)$$

but note that $\delta_1\hat\rho_1 A_j^\beta + \delta_1\hat\rho_2 B_j^\beta = \delta_2\hat\rho_1 A_j^\gamma + \delta_2\hat\rho_2 B_j^\gamma$, and simplifying, $\delta_2(u_3 - \hat\rho_1 u_1 - \hat\rho_2 u_2) = 0$. But it cannot be $u_3 - \hat\rho_1 u_1 - \hat\rho_2 u_2 = 0$ or we would have entered in clause 6. Therefore, it must be $\delta_2 = 0$ and thus, $A_j^\beta = B_j^\beta = C_j^\beta = 0$ for the extracted β, which also implies $V_j^\beta = 0$. This shows that the extracted β satisfies the conditions of clause 7 and we can set $\varpi = (\beta_1, \dots, \beta_\ell)$.

Finally, if we reached this point, we must be in clause 8. Note that, since we did not enter in clause 7, there exists a verification equation j such that for the extracted β, $A_j^\beta \alpha_r + B_j^\beta \alpha_s + C_j^\beta = 0$ is a non-trivial equation in (α_r, α_s) for which its coefficients can be computed. Moreover, all the verification equations are proportional to it, and since we did not enter in clause 3, it must be $A_j^\beta \neq 0$. It is clear that we can compute all solutions over $\mathbb{Z}_p$ to the equation and in particular the only solution of the form $(\alpha_r^*, 0)$ at this point we return the witness $\varpi = (\alpha_r^*, 0, \perp, \dots, \perp)$. This completes the proof of extractability. □

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 [4] outputs signatures in $\mathbb{G}_1^3 \times \mathbb{G}_2$ for messages in $\mathbb{G}_1$. Although the total number of elements matches the lower bound given in [3], it has not been known 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 [4].

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 $(R, S, T_1, \dots, T_\ell) \in \mathbb{G}_1^2 \times \mathbb{G}_2^\ell$ is proven EUF-CMA under a non-interactive assumption, it must be such that all the k verification equations satisfy:*

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

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 $(R, S, T_1, \dots, T_\ell)$ be a signature. We first consider two extreme cases where signatures include elements from one group. If $(R, S, T_1, \dots, T_\ell) \in \mathbb{G}_1^{2+\ell}$, 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, $(R, S) \in \mathbb{G}_1^2$, $T_1, \dots, T_\ell \in \mathbb{G}_2^\ell$. Let $\mathcal{SIG}_\mu$ 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 [4].

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

Proof. According to [5], at least 2 verification equations are required in Type-II for secure signature with $(R, S) \in \mathbb{G}_1^2$, $T_1, \dots, T_\ell \in \mathbb{G}_2^\ell \in \mathcal{SIG}_\mu$. 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 $i = 1, \dots, \ell$ are public parameters, and $(R, S, T_1, \dots, T_\ell) \in \mathbb{G}_1^2 \times \mathbb{G}_2^\ell$ are signatures,

$$e(R, U_1^{(j)} \textstyle\prod_{i=1}^{\ell} T_i^{a_i^{(j)}})\, e(S, U_2^{(j)} \prod_{i=1}^{\ell} T_i^{b_i^{(j)}})\, e(M, U_3^{(j)} \prod_{i=1}^{\ell} T_i^{c_i^{(j)}}) \\ \textstyle\prod_{j=1}^{\ell} \prod_{i=1}^{\ell} e(\tilde{T}_j, T_i^{d_i^{(j)}}) \prod_{i=1}^{\ell} e(V_i^{(j)}, T_i) = Z^{(j)}. \tag{31}$$

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 $(i = 1, \dots, \ell)$ in a signature, we consider a special representation of the form

$$R = G^{\varphi_r} M^{\alpha_r}, \quad S = G^{\varphi_s} M^{\alpha_s}, \quad T_i = H^{\varphi_{t_i}} \tag{32}$$

for some $\varphi_r, \alpha_r, \varphi_s, \alpha_s, \varphi_{t_i}$ in $\mathbb{Z}_p$. Now, consider equation (31) in the exponent:

$$(\varphi_r + \alpha_r\, m)\, (\textstyle\sum_{i=1}^{\ell} a_i^{(j)}\, \varphi_{t_i} + u_1^{(j)}) + (\varphi_s + \alpha_s\, m)\, (\sum_{i=1}^{\ell} b_i^{(j)}\, \varphi_{t_i} + u_2^{(j)}) \\ + m\, (\textstyle\sum_{i=1}^{\ell} c_i^{(j)}\, \varphi_{t_i} + u_3^{(j)}) + \sum_{j=1}^{\ell} \varphi_{t_j} \sum_{i=1}^{\ell} d_i^{(j)}\, \varphi_{t_i} + \sum_{j=1}^{\ell} v_i^{(j)} \varphi_{t_i} = z \tag{33}$$

By considering (33) as a polynomial in m, it can be shown that

$$(\textstyle\sum_{i=1}^{\ell} a_i^{(j)} \varphi_{t_i} + u_1^{(j)})\alpha_r + (\sum_{i=1}^{\ell} b_i^{(j)} \varphi_{t_i} + u_2^{(j)})\alpha_s + (\sum_{i=1}^{\ell} c_i^{(j)} \varphi_{t_i} + u_3^{(j)}) = 0 \tag{34}$$

if the discrete logarithm problem is hard in $\mathbb{G}_1$. We denote by $\mathtt{Dt}_{j,k}(t_1, \dots, t_\ell)$ the determinant of equation (34) for j and k, when considered as polynomials in (α_r, α_s). There exists a unique solution (α_r, α_s) if and only if $\mathtt{Dt}_{j,k}(t_1, \dots, t_\ell) \neq 0$ for two different equations j and k.

We construct a crucial relation for $\mathsf{Sig} \in \mathcal{SIG}_\mu$.

Let θ denote a transcript $\theta := (VK, (M^{(1)}, R^{(1)}, S^{(1)}, T_1^{(1)}, \dots, T_\ell^{(1)}), \dots, (M^{(n)}, R^{(n)}, S^{(n)}, T_1^{(n)}, \dots, T_\ell^{(n)}))$.

Definition 8 (Crucial Relation for $\mathsf{Sig} \in \mathcal{SIG}_\mu$). *Let $\varpi := (\omega_1, \omega_2)$ and given θ, let $(R, S, T_1, \dots, T_\ell)$ 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 such that* $\mathtt{Dt}_{j,k}(t_1, \dots, t_\ell) \neq 0$,
   - *if $\varpi = (\alpha_r, \alpha_s)$ where α_r and α_s satisfy (34) 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 8 is a crucial relation for any $\mathsf{Sig} \in \mathcal{SIG}_\mu$ with respect to algebraic algorithms and a message sampler choosing M uniformly.*

We show that the relation Ψ in Definition 8 satisfies uniqueness, usefulness, and extractability.

Uniqueness. Uniqueness for clauses 1 and 3 is immediate. We focus on clause 2. In that case, because $\mathtt{Dt}_{j,k}(t_1, \dots, t_\ell) \neq 0$, there exists a unique pair (α_r, α_s) satisfying equation (34) for both j and k.

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 $(M^\star, R^\star, S^\star, T_1^\star, \dots, T_\ell^\star) = (M \cdot \hat{M}, R \cdot \hat{M}^{-\alpha_r}, S \cdot \hat{M}^{-\alpha_s}, T_1, \dots, T_\ell)$ and output $(R^\star, S^\star, T_1^\star, \dots, T_\ell^\star)$ 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 (31) for every verification equation.

On the other hand, if $\varpi = (\bot, \bot)$, it means that equation (34) is proportional (as an equation in α_r and α_s) for every verification equation j. We say a verification equation is *degenerate* if

$$\textstyle\sum_{i=1}^{\ell} a_i^{(j)} \varphi_{t_i} + u_1^{(j)} = 0 \qquad \text{and} \qquad \sum_{i=1}^{\ell} b_i^{(j)} \varphi_{t_i} + u_2^{(j)} = 0.$$

Otherwise, it is called *non-degenerate.* Note that, if $T_1, \dots, T_\ell$ 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 such that $\sum_{i=1}^{\ell} a_i^{(j)} \varphi_{t_i} + u_1^{(j)} \neq 0$. Compute $M^\star = M \cdot \left(U_1^{(j)} \prod_{i=1}^{\ell} \tilde{T}_i^{a_i^{(j)}} \right)^{-1}$ and $R^\star = R \cdot \left(U_3^{(j)} \prod_{i=1}^{\ell} \tilde{T}_i^{c_i^{(j)}} \right)$. Observe that $(R^\star, S, T_1, \ldots, T_\ell)$ is a valid signature for $M^\star$, because it satisfies the non-degenerate verification 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, such that $\sum_{i=1}^{\ell} b_i^{(j)} \varphi_{t_i} + u_2^{(j)} \neq 0$. Analogously, compute $M^\star = M \cdot \left(U_2^{(j)} \prod_{i=1}^{\ell} \tilde{T}_i^{b_i^{(j)}} \right)^{-1}$ and $S^\star = S \cdot \left(U_3^{(j)} \prod_{i=1}^{\ell} \tilde{T}_i^{c_i^{(j)}} \right)$ 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, it is because all verification equations are degenerate for such $T_1, \ldots, T_\ell$. In this case, $(*, *, T_1, \ldots, T_\ell)$ is a valid signature for every message in $\mathbb{G}_1$, where placeholders $*$ can be filled with arbitrary elements in $\mathbb{G}_1$.

Extractability. The problem reduces to verifying $\mathtt{Dt}_{j,k}(t_1, \ldots, t_\ell) = 0$ for every pair of verification equations j and k. This can be done by exploiting the efficient morphism. Concretely $\mathtt{Dt}_{j,k}(t_1, \ldots, t_\ell) = 0$ holds if and only if

$$e(\tilde{U}_1^{(j)}, U_2^{(k)}) / e(\tilde{U}_1^{(k)}, U_2^{(j)}) \cdot \prod_{i_1=1}^{\ell} \prod_{i_2=1}^{\ell} e(\tilde{T}_{i_2}, T_{i_1})^{(a_{i_2}^{(j)} b_{i_1}^{(k)} - b_{i_2}^{(j)} a_{i_1}^{(k)})}$$
$$\cdot \prod_{i=1}^{\ell} e(\tilde{T}_i, (U_2^{(k)})^{a_i^{(j)}} (U_1^{(j)})^{b_i^{(k)}} (U_2^{(j)})^{-a_i^{(k)}} (U_1^{(k)})^{-b_i^{(j)}}) = 1_{\mathbb{G}_T}. \qquad (35)$$

If equation (35) holds for some pair j,k, output the extracted (α_r, α_s) otherwise, output $(\perp, \perp)$. □

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

Corollary 3. *If there exists a structure preserving signature schemes that signs messages in $\mathbb{G}_1$ over Type-II groups and its EUF-CMA security is proved by algebraic black-box reductions to any non-interactive problems, then its signature must include at least 4 group elements.*

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 [4] 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. We believe that the techniques used in the crucial relation presented in our Definition 7 get us closer to answering to this question.

On q-type and static assumptions. We have closed the gap between lower and upper bounds in Type-III groups with respect to non-interactive assumptions. However, considering a more detailed classification of non-interactive assumptions, there exists a gap between those based on q-type and those based on static assumptions. The framework from [4] falls short of capturing such a difference in the assumptions. Although seeking for better constructions based on static assumptions is a natural direction in the design of SPS, it is not known how small their signatures can be. Therefore, closing the gap with respect to static assumptions is an important open problem.

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 [7] 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 [2] 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 [2] 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 [3] 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 [3, 5, 16]) does not work because the existing 3-element scheme [7] 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 [28] 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 [5] 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. M. Abe, M. Chase, B. David, M. Kohlweiss, R. Nishimaki, and M. Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. *J. Cryptology*, 29(4):833–878, 2016.
2. M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-preserving signatures and commitments to group elements. *J. Cryptology*, 29(2):363–421, 2016.
3. M. Abe, J. Groth, K. Haralambiev, and M. Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In P. Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 649–666, Santa Barbara, CA, USA, Aug. 14–18, 2011. Springer, Heidelberg, Germany.
4. M. Abe, J. Groth, and M. Ohkubo. Separating short structure-preserving signatures from non-interactive assumptions. In D. H. Lee and X. Wang, editors, *Advances in Cryptology – ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 628–646, Seoul, South Korea, Dec. 4–8, 2011. Springer, Heidelberg, Germany.
5. M. Abe, J. Groth, M. Ohkubo, and M. Tibouchi. Structure-preserving signatures from type II pairings. In J. A. Garay and R. Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 390–407. Springer, 2014. Full version: IACR Cryptology ePrint Archive 2014/312.
6. M. Abe, J. Groth, M. Ohkubo, and M. Tibouchi. Structure-preserving signatures from type II pairings. *IACR Cryptology ePrint Archive*, 2014:312, 2014.
7. M. Abe, J. Groth, M. Ohkubo, and M. Tibouchi. Unified, minimal and selectively randomizable structure-preserving signatures. In Y. Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume

8349 of *Lecture Notes in Computer Science*, pages 688–712, San Diego, CA, USA, Feb. 24–26, 2014. Springer, Heidelberg, Germany.

8. M. Bellare and A. Palacio. The knowledge-of-exponent assumptions and 3-round zero-knowledge protocols. In *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, pages 273–289, 2004.
9. E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza. Scalable zero knowledge via cycles of elliptic curves. In J. A. Garay and R. Gennaro, editors, *Advances in Cryptology – CRYPTO 2014, Part II*, volume 8617 of *Lecture Notes in Computer Science*, pages 276–294, Santa Barbara, CA, USA, Aug. 17–21, 2014. Springer, Heidelberg, Germany.
10. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55, Santa Barbara, CA, USA, Aug. 15–19, 2004. Springer, Heidelberg, Germany.
11. D. Boneh and R. Venkatesan. Breaking RSA may not be equivalent to factoring. In K. Nyberg, editor, *Advances in Cryptology – EUROCRYPT'98*, volume 1403 of *Lecture Notes in Computer Science*, pages 59–71, Espoo, Finland, May 31 – June 4, 1998. Springer, Heidelberg, Germany.
12. S. Chatterjee and A. Menezes. Type 2 structure-preserving signature schemes revisited. In T. Iwata and J. H. Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 286–310. Springer, 2015.
13. J.-S. Coron. Optimal security proofs for PSS and other signature schemes. In L. R. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 272–287, Amsterdam, The Netherlands, Apr. 28 – May 2, 2002. Springer, Heidelberg, Germany.
14. I. Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, pages 445–456, 1991.
15. A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie-Hellman assumptions. In R. Canetti and J. A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 129–147, Santa Barbara, CA, USA, Aug. 18–22, 2013. Springer, Heidelberg, Germany.
16. G. Fuchsbauer, C. Hanser, and D. Slamanig. Euf-cma-secure structure-preserving signatures on equivalence classes. *IACR Cryptology ePrint Archive*, 2014:944, 2014.
17. G. Fuchsbauer, E. Kiltz, and J. Loss. The algebraic group model and its applications. Cryptology ePrint Archive, Report 2017/620, 2017. `https://eprint.iacr.org/2017/620`.
18. S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113 – 3121, 2008. Applications of Algebra to Cryptography.
19. E. Ghadafi. Short structure-preserving signatures. In K. Sako, editor, *Topics in Cryptology - CT-RSA 2016 - The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, February 29 - March 4, 2016, Proceedings*, volume 9610 of *Lecture Notes in Computer Science*, pages 305–321. Springer, 2016.
20. E. Ghadafi. How low can you go? short structure-preserving signatures for diffie-hellman vectors. In M. O'Neill and J. Groth, editors, *16th IMA International Conference on Cryptography and Coding (IMACC)*, volume 10655 of *Lecture Notes in Computer Science*, pages 185–204. Springer, 2017.
21. E. Ghadafi. More efficient structure-preserving signatures - or: Bypassing the type-iii lower bounds. In S. N. Foley, D. Gollmann, and E. Snekkenes, editors, *Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II*, volume 10493 of *Lecture Notes in Computer Science*, pages 43–61. Springer, 2017.
22. E. Ghadafi, N. P. Smart, and B. Warinschi. Groth-Sahai proofs revisited. In P. Q. Nguyen and D. Pointcheval, editors, *PKC 2010: 13th International Conference on Theory and Practice of Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 177–192, Paris, France, May 26–28, 2010. Springer, Heidelberg, Germany.
23. J. Groth. Short pairing-based non-interactive zero-knowledge arguments. In M. Abe, editor, *Advances in Cryptology – ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 321–340, Singapore, Dec. 5–9, 2010. Springer, Heidelberg, Germany.
24. J. Groth. On the size of pairing-based non-interactive arguments. In M. Fischlin and J. Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 305–326. Springer, 2016.
25. J. Groth and A. Sahai. Efficient noninteractive proof systems for bilinear groups. *SIAM J. Comput.*, 41(5):1193–1232, 2012.
26. S. Hada and T. Tanaka. On the existence of 3-round zero-knowledge protocols. In *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, pages 408–423, 1998.

27. C. S. Jutla and A. Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In K. Sako and P. Sarkar, editors, *Advances in Cryptology – ASIACRYPT 2013, Part I*, volume 8269 of *Lecture Notes in Computer Science*, pages 1–20, Bengalore, India, Dec. 1–5, 2013. Springer, Heidelberg, Germany.
28. C. S. Jutla and A. Roy. Improved structure preserving signatures under standard bilinear assumptions. In S. Fehr, editor, *Public-Key Cryptography - PKC 2017 - 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, The Netherlands, March 28-31, 2017, Proceedings, Part II*, volume 10175 of *Lecture Notes in Computer Science*, pages 183–209. Springer, 2017.
29. E. Kiltz, J. Pan, and H. Wee. Structure-preserving signatures from standard assumptions, revisited. In R. Gennaro and M. Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 275–295. Springer, 2015.
30. B. Libert, T. Peters, M. Joye, and M. Yung. Compactly hiding linear spans - tightly secure constant-size simulation-sound QA-NIZK proofs and applications. In T. Iwata and J. H. Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 681–707, Auckland, New Zealand, Nov. 30 – Dec. 3, 2015. Springer, Heidelberg, Germany.
31. B. Libert, T. Peters, and M. Yung. Short group signatures via structure-preserving signatures: Standard model security from simple assumptions. In R. Gennaro and M. Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 296–316. Springer, 2015.
32. H. Lipmaa. Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments. In R. Cramer, editor, *TCC 2012: 9th Theory of Cryptography Conference*, volume 7194 of *Lecture Notes in Computer Science*, pages 169–189, Taormina, Sicily, Italy, Mar. 19–21, 2012. Springer, Heidelberg, Germany.