Structure-Preserving Signatures from Standard Assumptions, Revisited *

Eike Kiltz **, Jiaxin Pan, and Hoeteck Wee ***

[1] Ruhr-Universität Bochum
[2] Ruhr-Universität Bochum
[3] ENS, Paris
{eike.kiltz,jiaxin.pan}@rub.de, wee@di.ens.fr

Abstract. Structure-preserving signatures (SPS) are pairing-based signatures where all the messages, signatures and public keys are group elements, with numerous applications in public-key cryptography. We present new, simple and improved SPS constructions under standard assumptions via a conceptually different approach. Our constructions significantly narrow the gap between existing constructions from standard assumptions and optimal schemes in the generic group model.

1 Introduction

Structure-preserving signatures (SPS) [4] are pairing-based signatures where all the messages, signatures and public keys are group elements, verified by testing equality of products of pairings of group elements. They are useful building blocks in modular design of cryptographic protocols, in particular in combination with non-interactive zero-knowledge (NIZK) proofs for algebraic relations in a group [29]. Structure-preserving signatures have found numerous applications in public-key cryptography, such as blind signatures [4, 25], group signatures [27, 28, 4, 25, 39], homomorphic signatures [37], delegatable anonymous credentials [24, 11], compact verifiable shuffles [18], network encoding [9], oblivious transfer [26] and e-cash [13].

A systematic treatment of structure-preserving signatures was initiated by Abe et al. in 2010 [4], building upon previous constructions in [27, 26, 17]. In the past few years, substantial and rapid progress were made in our understanding of the construction of structure-preserving signatures, yielding both efficient schemes under standard assumptions [4, 2, 30, 3] as well as "optimal" schemes in the generic group model with matching upper and lower bounds on the efficiency of the schemes [5, 6, 8, 7, 10]. The three important measures of efficiency in structure-preserving signatures are (i) signature size, (ii) public key size (also per-user public key size for applications like delegatable credentials where we need to sign user public keys), and (iii) number of pairing equations during verification, which in turn affects the efficiency of the NIZK proofs.

One of the main advantages of designing cryptographic protocols starting from structure-preserving signatures is that we can obtain efficient protocols that are secure under standard cryptographic assumptions without the use of random oracles. Ideally, we want to build efficient SPS based on the well-understood k-Lin assumption, which can then be used in conjunction with Groth-Sahai proofs [29] to derive protocols based on the same assumption. In contrast, if we start with SPS that are only secure in the generic group model, then the ensuing protocols would also only be secure in the generic group model, which offer little theoretical or practical benefits over alternative – and typically more efficient and pairing-free – solutions in the random oracle model.

* An extended abstract of this work appeared in the proceedings of CRYPTO 2015. This is the full version

** Supported by a Sofja Kovalevskaja Award of the Alexander von Humboldt Foundation, the German Israel Foundation, and ERC Project ERCC (FP7/615074).

*** CNRS, INRIA and Columbia University. Partially supported by the Alexander von Humboldt Foundation, NSF Award CNS-1445424 and ERC Project aSCEND (639554).

Unfortunately, there is still a big efficiency gap between existing constructions of structure-preserving signatures from the k-Lin assumption and the optimal schemes in the generic group model. For instance, to sign a single group element, the best construction under the SXDH (1-Lin) assumption contains 11 and 21 group elements in the signature and the public key [2], whereas the best construction in the generic group model contains 3 and 3 elements (moreover, this is "tight") [5]. The goal of this work is to bridge this gap.

1.1 Our Results

We present clean, simple, and improved constructions of structure-preserving signatures via a conceptually novel approach. Our constructions are secure under the k-Lin assumption; under the SXDH assumption (i.e., $k = 1$), we achieve 7 group elements in the signature.

Previous constructions use fairly distinct techniques, resulting in a large family of schemes with incomparable efficiency and security guarantees. We obtain a family of schemes that simultaneously match – and in many settings, improve upon – the efficiency, assumptions, and security guarantees of all the previous constructions. Figure 1 summarizes the efficiency of our constructions. (The work of [40] is independent and concurrent.) Our schemes are fully explicit and simple to describe. Furthermore, our schemes have a natural derivation from a symmetric-key primitive, and the derivation even extends to a modular and intuitive proof of security.

We highlight two results:

- For Type III asymmetric pairings, under the SXDH assumption, we can sign a vector of n elements in $\mathbb{G}_1$ with 7 group elements. This improves upon the prior SXDH-based scheme in [2] which requires 11 group elements, and matches the signature size of the scheme in [4] based on (non-standard) q-type assumptions;
- For Type I symmetric pairings, under the 2-Lin assumption, we can sign a vector of n elements with 10 group elements, improving upon that in [3] which requires 14 group elements.

In each of these cases, we also improve the size of the public key, as well as the number of equations used in verification. Finally, we extend our schemes to obtain efficient SPS for signing bilateral messages in $\mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$ for Type III asymmetric pairings. Particularly, under the SXDH assumption, our scheme can sign messages in $\mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$ with 10 group elements in the signature, 4 pairing product equations for verification, and $(n_1 + n_2 + 8)$ group elements in the public key. Prior SXDH-based scheme from [2] required 14 group elements in the signature, 5 pairing product equations, and $(n_1 + n_2 + 22)$ elements in the public key.

At a high level, our constructions and techniques borrow heavily from the recent work of Kiltz and Wee [35] which addresses a different problem of constructing pairing-based non-interactive zero-knowledge arguments [29, 33]. We exploit recent developments in obtaining adaptively secure identity-based encryption (IBE) schemes, notably the use of pairing groups to "compile" a symmetric-key primitive into an asymmetric-key primitive [14, 43, 19], and the dual system encryption methodology for achieving adaptive security against unbounded collusions [42, 36]. Along the way, we have to overcome a new technical hurdle which is specific to structure-preserving cryptography.

1.2 Our Approach: SPS from MACs

We provide an overview of our construction of structure-preserving signatures. Throughout this overview, we fix a pairing group $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ with $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, and rely on implicit representation notation

	Security	Assumption	$\|\mathbf{m}\|$	$\|\sigma\|$	$\|\mathsf{pk}\|$	# (PPEs)
AFGHO10 [4]	OT	2-KerLin ($\mathbb{G}_2$)	$(n_1, 0)$	$(3, 0)$	$2n_1 + 5$	2
$\mathsf{SPS}_{\mathsf{ot}}$ (Fig 2)	OT	$\mathcal{D}_k$-KerMDH ($\mathbb{G}_2$)	$(n_1, 0)$	$(k + 1, 0)$	$(n_1 + 1)k + \mathsf{RE}(\mathcal{D}_k)$	k
AGHO11 [5]	full	Interactive (Generic)	(n_1, n_2)	$(2, 1)$	$n_1 + n_2 + 2$	2
AGHO11 [5]	full	Non-interactive (Generic)	(n_1, n_2)	$(3, 3)$	$n_1 + n_2 + 2$	2
AGHO11 [5]	full	Non-interactive (Generic)	$(n_1, 0)$	$(3, 1)$	$n_1 + 2$	2
ACDKNO12 [2]	full	SXDH, XDLIN	$(n_1, 0)$	$(7, 4)$	$20 + n_1$	4
ACDKNO12 [2]	full	SXDH, XDLIN	(n_1, n_2)	$(8, 6)$	$22 + n_1 + n_2$	5
ADKNO13 [3]	full	2-Lin ($\mathbb{G}_1 = \mathbb{G}_2$)	n	14	$22 + n$	7
AFGHO10 [4]	full	q-SFP	$(n_1, 0)$	$(5, 2)$	$13 + n_1$	2
LPY15 [40]	full	SXDH, XDLIN	$(n_1, 0)$	$(9, 1)$	$2n_1 + 21$	5
$\mathsf{SPS}_{\mathsf{full}}$ (Fig 3)	full	$\mathcal{D}_k$-MDDH ($\mathbb{G}_1, \mathbb{G}_2$)	$(n_1, 0)$	$(3k + 3, 1)$	$(n_1 + 2k + 3)k + \mathsf{RE}(\mathcal{D}_k)$	$2k + 1$
$\mathsf{BSPS}_{\mathsf{full}}$ (Fig 9)	full	$\mathcal{D}_k$-MDDH ($\mathbb{G}_1, \mathbb{G}_2$)	(n_1, n_2)	$(4k + 3, k + 2)$	$(n_1 + n_2 + 3k + 3)k + 2\mathsf{RE}(\mathcal{D}_k)$	$3k + 1$

Fig. 1. Structure-preserving signatures for message space $\mathcal{M} = \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$ or $\mathcal{M} = \mathbb{G}^n$ if $\mathbb{G} = \mathbb{G}_1 = \mathbb{G}_2$. Notation (x, y) means x elements in $\mathbb{G}_1$ and y elements in $\mathbb{G}_2$. $\mathsf{RE}(\mathcal{D}_k)$ denotes the number of group elements needed to represent $[\mathbf{A}]$. In case of k-Lin, we have $\mathsf{RE}(\mathcal{D}_k) = k$. Recall that k-Lin is a special case of $\mathcal{D}_k$-MDDH (decisional assumptions) and k-KerLin is a special case of $\mathcal{D}_k$-KerMDH (search assumptions), for $\mathcal{D}_k = \mathcal{L}_k$, the linear distribution. For $k = 1$ (SXDH) and $n_1 = 1$, we obtain $(|\mathsf{pk}|, |\sigma|, \#\text{equations}) = (7, 7, 3)$ for $\mathcal{M} = \mathbb{G}_1^{n_1}$. For comparison, the known lower bound [5, 6] is $(|\sigma|, \#\text{equations}) \geq (4, 2)$.

for group elements, as explained in Section 2.1.[4] As a warm-up, we explain in some detail how to build a one-time structure-preserving signature scheme, following closely the exposition in [35]. While we do not obtain significant improvement in this setting (nonetheless, we do simplify and generalize prior one-time schemes [4]), we believe it already illustrates the conceptual simplicity and novelty of our approach over previous constructions of structure-preserving signatures.

Warm-up: One-Time SPS. We want to build a one-time signature scheme for signing a vector $[\mathbf{m}]_1 \in \mathbb{G}_1^n$ of group elements. The starting point of our construction is a one-time "structure-preserving" information-theoretic MAC for vectors of group elements. We pick a secret MAC key $\mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times(k+1)}$ known to the verifier ($k \geq 1$ is a parameter of the security assumption), and the MAC on $[\mathbf{m}]_1$ is given by

$$\sigma := [(1, \mathbf{m}^\top)\mathbf{K}]_1 \in \mathbb{G}_1^{1\times(k+1)}$$

Verification is straight-forward: check if

$$\sigma \overset{?}{=} (1, \mathbf{m}^\top)\mathbf{K} \tag{1}$$

Security follows readily from the fact that for any pair of distinct vectors $\mathbf{m}, \mathbf{m}^* \in \mathbb{Z}_q^n$, the vectors $(1, \mathbf{m}^\top)$ and $(1, \mathbf{m}^{*\top})$ are linearly independent, and therefore the quantities

$$(1, \mathbf{m}^\top)\mathbf{K}, (1, \mathbf{m}^{*\top})\mathbf{K} \in \mathbb{Z}_q^{(k+1)}$$

are two independently random values; this holds even if $\mathbf{m}^* \neq \mathbf{m}$ is chosen adaptively after seeing $(1, \mathbf{m}^\top)\mathbf{K}$.

To achieve public verifiability as is required for a signature scheme, we publish a "partial commitment" to $\mathbf{K}$ in $\mathbb{G}_2$ as given by $[\mathbf{A}]_2, [\mathbf{KA}]_2$, where the choice of $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$ is defined by the security assumption. The signature on $[\mathbf{m}]_1$ is the same as the MAC value, and verification is the natural analogue of (1) with the pairing:

$$e(\sigma, [\mathbf{A}]_2) \overset{?}{=} e([(1, \mathbf{m}^\top)]_1, [\mathbf{KA}]_2)$$

[4] For fixed generators g_1 and g_2 of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively, and for a matrix $\mathbf{M} \in \mathbb{Z}_q^{n\times t}$, we define $[\mathbf{M}]_1 := g_1^{\mathbf{M}}$ and $[\mathbf{M}]_2 := g_2^{\mathbf{M}}$ (componentwise).

As $[\mathbf{A}]_2, [\mathbf{KA}]_2$ leaks additional information about the secret MAC key $\mathbf{K}$, we can only prove computational adaptive soundness. In particular, we rely on the $\mathcal{D}_k$-KerMDH Assumption [41], which stipulates that given a random $[\mathbf{A}]_2$ drawn from a matrix distribution $\mathcal{D}_k$, it is hard to find a non-zero $[\mathbf{s}]_1 \in \mathbb{G}_1^{k+1}$ such that $\mathbf{s}^\top\mathbf{A} = \mathbf{0}$; this is implied by the $\mathcal{D}_k$-MDDH Assumption [22], a generalization of the k-Lin Assumption.[5] Therefore, for any $([\mathbf{m}^*]_1, [\sigma]_1)$ produced by an efficient adversary,

$$\sigma\mathbf{A} = (1, \mathbf{m}^{*\top})\mathbf{KA} \Longrightarrow (\sigma - (1, \mathbf{m}^{*\top})\mathbf{K})\mathbf{A} = \mathbf{0}$$
$$\overset{\text{using assumption}}{\Longrightarrow} \sigma - (1, \mathbf{m}^{*\top})\mathbf{K} = \mathbf{0} \Longrightarrow \sigma = (1, \mathbf{m}^{*\top})\mathbf{K}.$$

That is, security of the signature reduces to the security for the MAC, with a little more work to account for the leakage from $\mathbf{KA}$. Moreover, adaptive security for the MAC (which is easy to analyze via a purely information-theoretic argument) carries over to adaptive security for the signature.

General SPS. To achieve unforgeability against multiple signature queries, we move from a one-time MAC to a randomized MAC that is secure against multiple queries. As shown in [35, 14], we know that under the $\mathcal{D}_k$-MDDH assumption in $\mathbb{G}_1$, the following construction is a randomized PRF

$$\tau \mapsto \big([\mathbf{t}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1)]_1, [\mathbf{t}^\top]_1\big) \in (\mathbb{G}_1^{1\times(k+1)})^2, \tag{2}$$

where $\mathbf{K}_0, \mathbf{K}_1$ is the seed and $\mathbf{t}$ is the randomness. We now use the randomized PRF to additively mask the one-time MAC value $[(1, \mathbf{m}^\top)\mathbf{K}]_1$. The new randomized MAC takes as input a vector of group elements $[\mathbf{m}]_1 \in \mathbb{G}_1^n$ as before, picks a random tag $\tau \in \mathbb{Z}_q$ and a fresh $\mathbf{t}$ and outputs

$$(\sigma_1, \sigma_2) := ([(1, \mathbf{m}^\top)\mathbf{K}]_1 + \boxed{[\mathbf{t}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1)]_1}, \boxed{[\mathbf{t}^\top]_1}) \in (\mathbb{G}_1^{1\times(k+1)})^2 \tag{3}$$

where $\mathbf{K}$ and $\mathbf{K}_0, \mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times(k+1)}$ constitute the key. The boxed terms correspond to the additive mask from (2). We want to argue that an adversary upon obtaining MAC values on Q message vectors $[\mathbf{m}_1]_1, \ldots, [\mathbf{m}_Q]_1$, cannot compute the MAC value on a new message vector $[\mathbf{m}^*]_1$. First, we may assume that the MAC values on $[\mathbf{m}_1]_1, \ldots, [\mathbf{m}_Q]_1$ use distinct tags $\tau_1, \ldots, \tau_Q$. Then, we consider two cases:

- case 1: the adversary uses a fresh tag for $[\mathbf{m}^*]_1$. This immediately breaks the pseudorandomness of the security of the construction in (2);
- case 2: the adversary reuses tag τ_i. Again, we know from pseudorandomness that the MAC values on the remaining $Q - 1$ tags do not leak any information $\mathbf{K}$; therefore, the only leakage about $\mathbf{K}$ in the Q queries comes from $(1, \mathbf{m}_i^\top)\mathbf{K}$. We may then rely on the security of the one-time MAC to argue that given only $(1, \mathbf{m}_i^\top)\mathbf{K}$, it is hard to compute $(1, \mathbf{m}^{*\top})\mathbf{K}$.

As before, to obtain a signature scheme, we then publish $[\mathbf{A}]_2, [\mathbf{KA}]_2, [\mathbf{K}_0\mathbf{A}]_2, [\mathbf{K}_1\mathbf{A}]_2$ for public verification:

$$e(\sigma_1, [\mathbf{A}]_2) \stackrel{?}{=} e([(1, \mathbf{m}^\top)]_1, [\mathbf{KA}]_2) \cdot e(\sigma_2, [\mathbf{K}_0\mathbf{A}]_2 \cdot [\tau\mathbf{K}_1\mathbf{A}]_2)$$

Note that the above verification requires knowledge of $\tau \in \mathbb{Z}_q$ to compute $[\tau\mathbf{K}_1\mathbf{A}]_2$.

To obtain a structure-preserving signature, we cannot publish $\tau \in \mathbb{Z}_q$ in the signature. The main technical challenge in this work is to find a way to embed τ as a group element that enables both verification and a security reduction. The natural work-around is to add $[\tau\mathbf{K}_1\mathbf{A}]_2$ and $[\tau]_1$ to the signature, but the proof breaks down as we can no longer transform a forgery for the signature to a forgery to the randomized MAC.

[5] We refer the reader to Section 2.2 for a more detailed treatment of the assumptions.

Instead, we add $[\tau]_2$ and $[\tau \mathbf{t}^\top]_1$ to the signature to enable verification. This yields a signature with $3k+4$ group elements.

An alternative interpretation. Linearly homomorphic signatures (LHS) [15, 21, 32] are signatures where the messages consist of vectors over group $\mathbb{G}_1$ such that from any set of signatures on $[\mathbf{m}_i]_1 \in \mathbb{G}_1^n$, one can efficiently derive a signature σ on any element message $[\mathbf{m}]_1 := [\sum \omega_i \mathbf{m}_i]_1$ in the span of $\mathbf{m}_1, \ldots, \mathbf{m}_Q$. For security, one requires that it is infeasible to produce a signature on a message outside of the span of all previously signed messages. Linearly homomorphic structure preserving signatures (LHSPS) [37, 16, 35] have the additional property that signatures and public keys are all elements of the groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$, while allowing the use of a tag which is a scalar.

We can construct a SPS with message space $\mathbb{G}_1^n$ from a LHSPS with message space $\mathbb{G}_1^{n+1}$ as follows: to sign a message $[\mathbf{m}]_1$, we use a LHSPS to sign the $(n+1)$-dimensional vector $[1, \mathbf{m}^\top]_1$ on a random tag. Suppose the SPS adversary forges a signature on $[\mathbf{m}^*]_1$. First, we may assume that all the signatures from the signing queries $[\mathbf{m}_1]_1, \ldots, [\mathbf{m}_Q]_1$ are on distinct tags $\tau_1, \ldots, \tau_Q$. Then, we consider two cases:

- case 1: the adversary uses a fresh tag. Then, security of LHSPS tells us that the adversary can only sign the vector $\mathbf{0} \in \mathbb{G}_1^{n+1}$, which does not correspond to a valid message in the SPS.
- case 2: the adversary reuses tag τ_i. Then, $(1, \mathbf{m}^{*\top})$ must lie in the span of $(1, \mathbf{m}_i^\top)$, which means $\mathbf{m}^* = \mathbf{m}_i$. Here, we crucially rely on the fact that $\tau_1, \ldots, \tau_Q$ are distinct, which ensures that the adversary has seen at most one signature corresponding to τ_i.

At this point, we can then embed $\tau \in \mathbb{Z}_q$ as a group element as described earlier. Our constructions may also be viewed as instantiating the above paradigm with the state-of-the-art LHSPS in [35].

1.3 Discussion

Optimality. The linearity in the verification equation of SPS poses severe restrictions on the efficiency of such constructions. In both Type I and III bilinear groups, it was proved in [5, 8] that any fully secure SPS requires at least 2 verification equations, at least 3 group elements, the 3 elements not all the same group (for Type III asymmetric pairings). In fact, [5] shows the above lower bounds by giving attacks the weaker security model of unforgeability against two random message queries. Furthermore, one-time secure SPS against random message attack (RMA) in Type I bilinear groups require at least 2 group elements and 2 equations [8]. Furthermore, SPSs in Type III bilinear groups require at least 4 group elements [6] for unforgeability against adaptive chosen message attack under *non-interactive assumptions* (such as k-Lin).

Interestingly, for one-time RMA-security, we can match the lower bounds. By combining our main result on the one-time CMA-secure SPS and the techniques used in [35] to obtain shorter QANIZK, we obtain an optimal RMA-secure one-time SPS (Section 5). In Type III asymmetric groups, under the SXDH assumption, signatures requires 1 group element and 1 verification equation which is clearly optimal; in Type I symmetric groups, under the 2-Lin assumption, our scheme requires 2 elements and 2 verification equations, matching the lower bound for one-time RMA-secure SPS from [8].

Comparison with previous approaches. The prior works of Abe, et al. [2, 3] presented two generic approaches for constructing SPS from SXDH and 2-Lin assumptions: both constructions combine a structure-preserving one-time signature and random-message secure signatures ala [23], with slightly different syntax and security notions for the two underlying building blocks; the final signature is the concatenation of the two underlying signatures. Our construction has a similar flavor in that we combine a one-time MAC with a randomized PRF. However, we are able to exploit the common structure in both building blocks to compress the output; interestingly, working with the matrix Diffie-Hellman framework [22] makes it easier to identity such common structure. In particular, the output length of the randomized MAC with unbounded security is that of the PRF and not the sum of the output lengths of the one-time MAC and the PRF; this is akin to combining a one-time signature and a random-message secure signature in such a way that the combined signature size is that of the latter rather than the sum of the two.

Signatures from IBE. While our construction of signatures exploits techniques from the literature on IBE, it is quite different from the well-known Naor's derivation of a signature scheme from an IBE. There, the signature on a message $m \in \mathbb{Z}_q$ corresponds to an IBE secret key for the identity m. This approach seems to inherently fail for structure-preserving signatures as all known pairings-based IBE schemes need to treat the identity as a scalar. In our construction, a signature on $[\mathbf{m}]_1$ also corresponds to an IBE secret key: the message vector (specifically, a one-time MAC applied to the message vector) is embedded into the master secret key component of an IBE, and a fresh random tag $\tau \in \mathbb{Z}_q$ is chosen and used as the identity. The idea of embedding $[\mathbf{m}]_1$ into the master secret key component of an IBE also appeared in earlier constructions of linearly homomorphic structure-preserving schemes [37, 38, 35]; a crucial difference is that these prior constructions allow the use of a scalar tag in the signature.

Towards shorter SPS? One promising approach to get even shorter SPS against adaptive chosen message attack by using our approach is to improve upon the underlying MAC in the computational core lemma (Lemma 3). Currently, the MAC achieves security against chosen message attacks, whereas it suffices to use one that is secure against random message attacks. Saving one group element in this MAC would likely yield a saving of two group elements in the SPS, which would in turn yield a SXDH-based signature with 5 group elements. Note that the state-of-the-art standard signature from SXDH contains 4 group elements [20]. Together with existing lower bounds for SPS, this indicates a barrier of 5 group elements for SXDH-based SPS; breaking this barrier would likely require improving upon the best standard signatures from SXDH.

Perspective. As noted at the beginning of the introduction, structure-preserving signatures have been a target of intense scrutiny in recent years. We presented a conceptually different yet very simple approach for building structure-preserving signatures. We are optimistic that our approach will yield further insights into structure-preserving signatures as well as concrete improvements to the numerous applications that rely on such signatures.

2 Definitions

Notation. If $\mathbf{x} \in \mathcal{B}^n$, then $|\mathbf{x}|$ denotes the length n of the vector. Further, $x \leftarrow_{\mathrm{R}} \mathcal{B}$ denotes the process of sampling an element x from set $\mathcal{B}$ uniformly at random. If $\mathbf{A} \in \mathbb{Z}_q^{n \times k}$ is a matrix with $n > k$, then $\overline{\mathbf{A}} \in \mathbb{Z}_q^{k \times k}$ denotes the upper square matrix of $\mathbf{A}$ and then $\underline{\mathbf{A}} \in \mathbb{Z}_q^{(n-k) \times k}$ denotes the remaining $n-k$ rows of $\mathbf{A}$. We use $span()$ to denote the column span of a matrix.

2.1 Pairing Groups

Let GGen be a probabilistic polynomial time (PPT) algorithm that on input 1^λ returns a description $\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, g_1, g_2, e)$ of asymmetric pairing groups where $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ are cyclic groups of order q for a λ-bit prime q, g_1 and g_2 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2$ is an efficiently computable (non-degenerate) bilinear map. Define $g_T := e(g_1, g_2)$, which is a generator in $\mathbb{G}_T$.

We use implicit representation of group elements as introduced in [22]. For $s \in \{1, 2, T\}$ and $a \in \mathbb{Z}_q$, define $[a]_s = g_s^a \in \mathbb{G}_s$ as the *implicit representation* of a in $\mathbb{G}_s$. More generally, for a matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_q^{n \times m}$ we define $[\mathbf{A}]_s$ as the implicit representation of $\mathbf{A}$ in $\mathbb{G}_s$:

$$[\mathbf{A}]_s := \begin{pmatrix} g_s^{a_{11}} \dots g_s^{a_{1m}} \\ \\ g_s^{a_{n1}} \dots g_s^{a_{nm}} \end{pmatrix} \in \mathbb{G}_s^{n \times m}$$

We will always use this implicit notation of elements in $\mathbb{G}_s$, i.e., we let $[a]_s \in \mathbb{G}_s$ be an element in $\mathbb{G}_s$. Note that from $[a]_s \in \mathbb{G}_s$ it is generally hard to compute the value a (discrete logarithm problem in $\mathbb{G}_s$). Further, from $[b]_T \in \mathbb{G}_T$ it is hard to compute the value $[b]_1 \in \mathbb{G}_1$ and $[b]_2 \in \mathbb{G}_2$ (pairing inversion problem). Obviously, given $[a]_s \in \mathbb{G}_s$ and a scalar $x \in \mathbb{Z}_q$, one can efficiently compute $[ax]_s \in \mathbb{G}_s$. Further, given $[a]_1, [a]_2$ one can efficiently compute $[ab]_T$ using the pairing e. For two matrices $\mathbf{A}, \mathbf{B}$ with matching dimensions define $e([\mathbf{A}]_1, [\mathbf{B}]_2) := [\mathbf{AB}]_T \in \mathbb{G}_T$.

2.2 Matrix Diffie-Hellman Assumption

We recall the definitions of the Matrix Decision Diffie-Hellman (MDDH) and the Kernel Diffie-Hellman assumptions [22, 41].

Definition 1 (Matrix Distribution). *Let $k \in \mathbb{N}$. We call $\mathcal{D}_k$ a matrix distribution if it outputs matrices in $\mathbb{Z}_q^{(k+1) \times k}$ of full rank k in polynomial time.*

Without loss of generality, we assume the first k rows of $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k$ form an invertible matrix. The $\mathcal{D}_k$-Matrix Diffie-Hellman problem is to distinguish the two distributions $([\mathbf{A}], [\mathbf{Aw}])$ and $([\mathbf{A}], [\mathbf{u}])$ where $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, $\mathbf{w} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k$ and $\mathbf{u} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}$.

Definition 2 ($\mathcal{D}_k$-Matrix Diffie-Hellman Assumption $\mathcal{D}_k$-MDDH). *Let $\mathcal{D}_k$ be a matrix distribution and $s \in \{1, 2, T\}$. We say that the $\mathcal{D}_k$-Matrix Diffie-Hellman ($\mathcal{D}_k$-MDDH) Assumption holds relative to* GGen *in group $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$,*

$$\mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{A}) := |\Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}]_s, [\mathbf{Aw}]_s) = 1] - \Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}]_s, [\mathbf{u}]_s) = 1]| = \mathrm{negl}(\lambda),$$

where the probability is taken over $\mathcal{G} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$, $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k, \mathbf{w} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k, \mathbf{u} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}$.

The Kernel-Diffie-Hellman assumption $\mathcal{D}_k$-KerMDH [41] is a natural *computational analogue* of the $\mathcal{D}_k$-MDDH Assumption.

Definition 3 ($\mathcal{D}_k$-Kernel Diffie-Hellman Assumption $\mathcal{D}_k$-KerMDH). *Let $\mathcal{D}_k$ be a matrix distribution and $s \in \{1, 2\}$. We say that the $\mathcal{D}_k$-Kernel Diffie-Hellman ($\mathcal{D}_k$-KerMDH) Assumption holds relative to* GGen *in group $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$,*

$$\mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{A}) := \Pr[\mathbf{c}^\top \mathbf{A} = \mathbf{0} \wedge \mathbf{c} \neq \mathbf{0} \mid [\mathbf{c}]_{3-s} \leftarrow_{\mathrm{R}} \mathcal{A}(\mathcal{G}, [\mathbf{A}]_s)] = \mathrm{negl}(\lambda),$$

where the probability is taken over $\mathcal{G} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$, $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k$.

Note that we can use a non-zero vector in the kernel of $\mathbf{A}$ to test membership in the column space of $\mathbf{A}$. This means that the $\mathcal{D}_k$-KerMDH assumption is a relaxation of the $\mathcal{D}_k$-MDDH assumption, as captured in the following lemma from [41].

Lemma 1. *For any matrix distribution $\mathcal{D}_k$, $\mathcal{D}_k$-*$\mathsf{MDDH} \Rightarrow \mathcal{D}_k$-$\mathsf{KerMDH}$.

For each $k \geq 1$, [22, 41] specify distributions $\mathcal{L}_k$, $\mathcal{SC}_k$, $\mathcal{U}_k$ (and others) such that the corresponding $\mathcal{D}_k$-MDDH and $\mathcal{D}_k$-KerMDH assumptions are generically secure in bilinear groups and form a hierarchy of increasingly weaker assumptions.

$$\mathcal{SC}_k : \mathbf{A} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ a & 1 & 0 & \dots & 0 \\ 0 & a & 1 & & 0 \\ 0 & 0 & a & & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & 0 & 0 & \dots & a \end{pmatrix}, \; \mathcal{L}_k : \mathbf{A} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ 0 & 0 & a_3 & & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & 0 & 0 & \dots & a_k \end{pmatrix}, \; \mathcal{U}_k : \mathbf{A} = \begin{pmatrix} a_{1,1} & \dots & a_{1,k} \\ \vdots & \ddots & \vdots \\ a_{k+1,1} & \dots & a_{k+1,k} \end{pmatrix},$$

where $a, a_i, a_{i,j} \leftarrow \mathbb{Z}_q$. We define the *representation size* $\mathsf{RE}(\mathcal{D}_k)$ of a given matrix distribution $\mathcal{D}_k$ as the minimal number of group elements needed to represent $[\mathbf{A}]_s$, where $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k$. Then $\mathsf{RE}(\mathcal{SC}_k) = 1$, $\mathsf{RE}(\mathcal{L}_k) = k$ and $\mathsf{RE}(\mathcal{U}_k) = k(k+1)$. As shown in [22], $\mathcal{SC}_k$-MDDH offers the same security guarantees as $\mathcal{L}_k$-MDDH (k-Linear Assumption of [31]), while having the advantage of a more compact representation. We define k-$\mathsf{Lin} := \mathcal{L}_k$-$\mathsf{MDDH}$ and k-$\mathsf{KerLin} := \mathcal{L}_k$-$\mathsf{KerMDH}$. Note that 2-$\mathsf{KerLin} = \mathsf{SDP}$ (Simultaneous Double Pairing Assumption of [17]). The relations between the different assumptions for $\mathcal{D}_k = \mathcal{L}_k$ are as follows:

$$\begin{tikzcd}
\mathsf{DDH} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & 2\text{-}\mathsf{Lin} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & 3\text{-}\mathsf{Lin} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \dots & \\
1\text{-}\mathsf{KerLin} \arrow[r, Rightarrow] & 2\text{-}\mathsf{KerLin} = \mathsf{SDP} \arrow[r, Rightarrow] & 3\text{-}\mathsf{KerLin} \arrow[r, Rightarrow] & \dots \arrow[r, Rightarrow] & \mathsf{CDH}
\end{tikzcd}$$

2.3 Structure-Preserving Signatures

Let par be some parameters that contain a pairing group $\mathcal{PG}$. In a structure-preserving signature (SPS) [4], both the messages and signatures are group elements, verification proceeds via a pairing-product equation.

Definition 4 (Structure-preserving signature). *A structure-preserving signature scheme* SPS *is defined as a triple of probabilistic polynomial time (PPT) algorithms* $\mathsf{SPS} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$*:*

- *The probabilistic key generation algorithm* $\mathsf{Gen}(\mathsf{par})$ *returns the public/secret key* $(\mathsf{pk}, \mathsf{sk})$*, where* $\mathsf{pk} \in \mathbb{G}^{n_{\mathsf{pk}}}$ *for some* $n_{\mathsf{pk}} \in \mathrm{poly}(\lambda)$*. We assume that* pk *implicitly defines a message space* $\mathcal{M} := \mathbb{G}^n$ *for some* $n \in \mathrm{poly}(\lambda)$.
- *The probabilistic signing algorithm* $\mathsf{Sign}(\mathsf{sk}, [\mathbf{m}])$ *returns a signature* $\sigma \in \mathbb{G}^{n_\sigma}$ *for* $n_\sigma \in \mathrm{poly}(\lambda)$.
- *The deterministic verification algorithm* $\mathsf{Verify}(\mathsf{pk}, [\mathbf{m}], \sigma)$ *only consists of pairing product equations and returns 1 (accept) or 0 (reject).*

(Perfect correctness.) *for all* $(\mathsf{pk}, \mathsf{sk}) \leftarrow_{\mathrm{R}} \mathsf{Gen}(\mathsf{par})$ *and all messages* $[\mathbf{m}] \in \mathcal{M}$ *and all* $\sigma \leftarrow_{\mathrm{R}} \mathsf{Sign}(\mathsf{sk}, [\mathbf{m}])$ *we have* $\mathsf{Verify}(\mathsf{pk}, [\mathbf{m}], \sigma) = 1$.

Definition 5 (Unforgeablility against chosen message attack). *To an adversary* $\mathcal{A}$ *and* SPS *we associate the advantage function*

$$\mathbf{Adv}^{\mathrm{cma}}_{\mathsf{SPS}}(\mathcal{A}) := \Pr\left[[\mathbf{m}^*] \notin \mathcal{Q}_{\mathrm{msg}} \wedge \mathsf{Verify}(\mathsf{pk}, [\mathbf{m}^*], \sigma^*) = 1 \;\middle|\; \begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow_{\mathrm{R}} \mathsf{Gen}(\mathsf{par}) \\ ([\mathbf{m}^*], \sigma^*) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathsf{SignO}(\cdot)}(\mathsf{pk}) \end{array} \right],$$

where $\mathsf{SignO}([\mathbf{m}])$ *runs* $\sigma \leftarrow_{\mathrm{R}} \mathsf{Sign}(\mathsf{sk}, [\mathbf{m}])$*, adds the vector* $[\mathbf{m}]$ *to* $\mathcal{Q}_{\mathrm{msg}}$ *(initialized with* $\emptyset$*) and returns* σ *to* $\mathcal{A}$*.* SPS *is said to be (unbounded)* CMA-secure *if for all PPT adversaries* $\mathcal{A}$*,* $\mathbf{Adv}^{\mathrm{cma}}_{\mathsf{SPS}}(\mathcal{A})$ *is negligible.* SPS *is said to be* one-time CMA-secure *with corresponding advantage function* $\mathbf{Adv}^{\text{ot-cma}}_{\mathsf{SPS}}(\mathcal{A})$*, if* $\mathcal{A}$ *is restricted to make at most one query to oracle* SignO.

3 One-Time CMA-Secure SPS

The scheme is given in Figure 2 and its parameters are:

$$|\mathsf{pk}| = (n+1)k + \mathsf{RE}(\mathcal{D}_k), \qquad |\sigma| = k+1.$$

As defined in Section 2.2, $\mathsf{RE}(\mathcal{D}_k)$ denotes the number of group elements needed to represent $[\mathbf{A}]_s$, where $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k$. For k-Lin, we achieve 2 group elements in the signature for $k = 1$ and 3 group elements for $k = 2$. Moreover, we note that the verification needs k pairing product equations: for $e(\sigma, [\mathbf{A}]_2) = e([(1, \mathbf{m})]_1, [\mathbf{C}]_2)$ we need to pair the vector σ with every column of $[\mathbf{A}]_2$ and thus this check needs k pairing product equations.

```
Gen(par):                                          Sign(sk, $[\mathbf{m}]_1$):
$\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k; \mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times(k+1)}$     $\sigma := \left[(1, \mathbf{m}^\top)\mathbf{K}\right]_1$
$\mathbf{C} := \mathbf{K}\mathbf{A} \in \mathbb{Z}_q^{(n+1)\times k}$                     Return $\sigma \in \mathbb{G}_1^{1\times(k+1)}$
$\mathsf{sk} := \mathbf{K}$
$\mathsf{pk} := ([\mathbf{C}]_2, [\mathbf{A}]_2)$                         Verify(pk, $[\mathbf{m}]_1, \sigma$):
Return (pk, sk)                                    Check: $e(\sigma, [\mathbf{A}]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{C}]_2)$
```

Fig. 2. One-time CMA-secure structure-preserving signature $\mathsf{SPS}_{\mathsf{ot}}$ with message-space $\mathcal{M} = \mathbb{G}_1^n$.

We will exploit the following lemma in the analysis of our scheme. Informally, the lemma says that $\mathbf{m} \mapsto (1, \mathbf{m}^\top)\mathbf{K}$ is a secure information-theoretic one-time MAC even if the adversary first sees $(\mathbf{A}, \mathbf{K}\mathbf{A})$.

Lemma 2 (Core lemma for adaptive soundness). *Let* n, k *be integers. For any* $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$ *and any (possibly unbounded) adversary* $\mathcal{A}$*,*

$$\Pr\left[\mathbf{m}^* \neq \mathbf{m} \wedge \mathbf{z}^\top = (1, \mathbf{m}^{*\top})\mathbf{K} \,\middle|\, \begin{array}{l} \mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times(k+1)} \\ (\mathbf{z}, \mathbf{m}^*) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathcal{O}(\cdot)}(\mathbf{K}\mathbf{A}) \end{array}\right] \leq \frac{1}{q}, \tag{4}$$

where $\mathcal{O}(\mathbf{m} \in \mathbb{Z}_q^n)$ *returns* $(1, \mathbf{m}^\top)\mathbf{K}$ *and* $\mathcal{A}$ *only gets a single call to* $\mathcal{O}$*.*

This lemma can be seen as an adaptive version of a special case of [35, Lemma 2] in that we fix $t = 1$, $\mathbf{M}$ to be the matrix $(1, \mathbf{m}^\top) \in \mathbb{Z}_q^{1\times(n+1)}$, and we use the fact that if $\mathbf{m}^* \neq \mathbf{m}$, then $(1, \mathbf{m}^*) \notin \mathit{span}(\mathbf{M})$. In our adaptive version, $\mathbf{m}$ may depend on $\mathbf{K}\mathbf{A}$ but the proof is essentially the same as in [35].

Proof. First, fix any $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$ and any pair of distinct $\mathbf{m}, \mathbf{m}^* \in \mathbb{Z}_q^n$, along with a non-zero vector $\hat{\mathbf{a}} \notin \mathit{span}(\mathbf{A})$. Observe that the following distributions

$$((1, \mathbf{m}^\top)\mathbf{K}, \mathbf{K}\mathbf{A}, (1, \mathbf{m}^{*\top})\mathbf{K}\hat{\mathbf{a}}) \text{ and } ((1, \mathbf{m}^\top)\mathbf{K}, \mathbf{K}\mathbf{A}, u) \tag{5}$$

are the same, where $\mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times(k+1)}, u \leftarrow_{\mathrm{R}} \mathbb{Z}_q$. Here, we use the fact that if $\mathbf{m} \neq \mathbf{m}^*$, then $(1, \mathbf{m}^{*\top})$ and $(1, \mathbf{m}^\top)$ are linearly independent. By a standard argument (e.g. complexity leveraging[6]), this means that the two distributions are the same even if $\mathbf{m}, \mathbf{m}^*$ are adaptively chosen, that is, seeing $\mathbf{KA}$ for $\mathbf{m}$, after seeing $(\mathbf{KA}, (1, \mathbf{m}^\top)\mathbf{K})$ for $\mathbf{m}^*$. Therefore, for any adversary $\mathcal{A}$, we have

$$\Pr\left[\mathbf{m}^* \neq \mathbf{m} \wedge \mathbf{z}^\top \hat{\mathbf{a}} = (1, \mathbf{m}^{*\top})\mathbf{K}\hat{\mathbf{a}} \,\middle|\, \begin{array}{l} \mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times(k+1)} \\ (\mathbf{z}, \mathbf{m}^*) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathcal{O}(\cdot)}(\mathbf{KA}) \end{array}\right] \leq \frac{1}{q},$$

since $(1, \mathbf{m}^{*\top})\mathbf{K}\hat{\mathbf{a}}$ is uniformly random from the adversary's view-point. The lemma then follows from the fact that $\mathbf{z}^\top = (1, \mathbf{m}^{*\top})\mathbf{K}$ implies $\mathbf{z}^\top \hat{\mathbf{a}} = (1, \mathbf{m}^{*\top})\mathbf{K}\hat{\mathbf{a}}$. □

Theorem 1. *Under the $\mathcal{D}_k$-KerMDH Assumption in $\mathbb{G}_2$, $\mathsf{SPS_{ot}}$ from Figure 2 is a one-time CMA-secure structure-preserving signature scheme.*

Proof. Perfect correctness and the structure-preserving property are straight-forward. We proceed to establish one-time CMA-security based on the $\mathcal{D}_k$-KerMDH assumption. We will show that for all adversaries $\mathcal{A}$, there exists an adversary $\mathcal{B}$ with $\mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B})$ and

$$\mathbf{Adv}^{\text{ot-cma}}_{\mathsf{SPS_{ot}}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}) + 1/q. \tag{6}$$

Adversary $\mathcal{B}(\mathcal{PG}, [\mathbf{A}]_2 \in \mathbb{G}_2^{(k+1)\times k})$ generates $\mathsf{pk} = ([\mathbf{C}]_2, [\mathbf{A}]_2)$ as in the real scheme by picking $\mathbf{K} \in \mathbb{Z}_q^{(n+1)\times(k+1)}$ and computing $\mathbf{C} := \mathbf{KA}$. Next, $\mathcal{B}$ runs $\mathcal{A}$ on pk, simulates a signature on $[\mathbf{m}]_1$ honestly using $\mathbf{K}$, and obtains $([\mathbf{m}^*]_1, \sigma^*)$ satisfying $\mathbf{m}^* \neq \mathbf{m}$ and $e(\sigma^*, [\mathbf{A}]_2) = e([(1, \mathbf{m}^{*\top})]_1, [\mathbf{KA}]_2)$ with probability $\mathbf{Adv}^{\text{ot-cma}}_{\mathsf{SPS_{ot}}}(\mathcal{A})$. Finally, $\mathcal{B}$ returns $[\mathbf{s}]_1$ computed as

$$[\mathbf{s}]_1 = \sigma^* - [(1, \mathbf{m}^{*\top})]_1\mathbf{K}.$$

Clearly, $\mathbf{s} \cdot \mathbf{A} = \mathbf{0}$ and $\Pr[\mathbf{s} = \mathbf{0}] \leq 1/q$ by Lemma 2. This proves equation (6). □

4 Unbounded CMA-Secure SPS

4.1 Computational Core Lemma

We present a variant of the computational core lemma from [35, Lemma 3].

Lemma 3 (Computational core lemma for unbounded CMA-security). *For all adversaries $\mathcal{A}$, there exists an adversary $\mathcal{B}$ with $\mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B})$ and*

$$\Pr\left[\begin{array}{c} \tau^* \notin \mathcal{Q}_{\text{tag}} \\ \wedge\, b' = b \end{array} \,\middle|\, \begin{array}{l} \mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k \\ \mathbf{K}_0, \mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times(k+1)} \\ (\mathbf{P}_0, \mathbf{P}_1) := (\mathbf{B}^\top\mathbf{K}_0, \mathbf{B}^\top\mathbf{K}_1) \\ \mathsf{pk} := ([\mathbf{P}_0]_1, [\mathbf{P}_1]_1, [\mathbf{B}]_1, \mathbf{K}_0\mathbf{A}, \mathbf{K}_1\mathbf{A}, \mathbf{A}) \\ b \leftarrow_{\mathrm{R}} \{0,1\}; b' \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathcal{O}_b(\cdot), \mathcal{O}^*(\cdot)}(\mathsf{pk}) \end{array}\right]$$
$$\leq \frac{1}{2} + 2Q \cdot \mathbf{Adv}^{\text{mddh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}) + Q/q,$$

where

[6] Using complexity leveraging, we can transform any adaptive distinguisher into a non-adaptive one with an exponential loss in the distinguishing advantage. If the optimal non-adaptive distinguishing advantage is 0 as is the case for two identical distributions, then the optimal adaptive distinguishing advantage must also be 0.

- *$\mathcal{O}_b(\tau)$ returns $\left(\left[b\mu\mathbf{a}^{\perp} + \mathbf{r}^{\top}(\mathbf{P}_0 + \tau\mathbf{P}_1)\right]_1, [\mathbf{r}^{\top}\mathbf{B}^{\top}]_1\right) \in (\mathbb{G}_1^{1\times(k+1)})^2$ with $\mu \leftarrow_{\mathrm{R}} \mathbb{Z}_q, \mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k$ and adds τ to $\mathcal{Q}_{\mathrm{msg}}$. Here, $\mathbf{a}^{\perp}$ is non-zero vector in $\mathbb{Z}_q^{1\times(k+1)}$ that satisfies $\mathbf{a}^{\perp}\mathbf{A} = \mathbf{0}$.*
- $\boxed{\mathcal{O}^*([\tau^*]_2) \text{ returns } [\mathbf{K}_0 + \tau^*\mathbf{K}_1]_2}$*. $\mathcal{A}$ only gets a single call τ^* to $\mathcal{O}^*$.*
- *Q is the number of queries $\mathcal{A}$ makes to $\mathcal{O}_b$.*

Compared to [35, Lemma 3], oracle $\mathcal{O}^*$ is modified as follows. Instead of getting tag τ^* and returning $\mathbf{K}_0 + \tau^*\mathbf{K}_1$ in the clear, both the query and the output are encoded in $\mathbb{G}_2$. The change is boxed in the lemma. It is straight-forward to check that the proof goes through as in [35]:

- the security reduction knows $\mathbf{K}_0, \mathbf{K}_1$, and therefore it can compute $[\mathbf{K}_0 + \tau^*\mathbf{K}_1]_2$ given $[\tau^*]_2$;
- the quantity $[\mathbf{K}_0 + \tau^*\mathbf{K}_1]_2$ does not reveal any additional information about $\mathbf{K}_0, \mathbf{K}_1$ beyond $\mathbf{K}_0 + \tau^*\mathbf{K}_1$.

For completeness, we reproduce the proof of [35, Lemma 3] and mark the modifications with †'s below.

Proof. We proceed via a series of games, exactly as in the proof of [35, Lemma 3]. For $i = 0, 1, \ldots, Q$, in Game i, we answer the first i queries to $\mathcal{O}_b$ using $\mathcal{O}_0$, and the last $Q - i$ queries using $\mathcal{O}_1$. Let $\mathbf{Adv}_i$ denote the probability that $\mathcal{A}$ wins the game, that is, $\tau^* \notin \mathcal{Q}_{\mathrm{msg}} \wedge\ b' = b$. It suffices to show that for all $i = 0, 1, \ldots, Q-1$,

$$|\mathbf{Adv}_i - \mathbf{Adv}_{i+1}| \leq 2\mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}) + 1/q.$$

The main difference between Game i and Game $i+1$ is that we answer the i'th query τ to $\mathcal{O}_b$ using $\mathcal{O}_0$ in Game i and $\mathcal{O}_1$ in Game $i+1$, where $\mathcal{O}_b$ returns:

$$\left(\left[b\mu\mathbf{a}^{\perp} + \mathbf{r}^{\top}\mathbf{B}^{\top}(\mathbf{K}_0 + \tau\mathbf{K}_1)\right]_1, [\mathbf{r}^{\top}\mathbf{B}^{\top}]_1\right), \text{where } \mu \leftarrow_{\mathrm{R}} \mathbb{Z}_q, \mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k.$$

Using the MDDH assumption twice, we may switch $[\mathbf{Br}]_1$ with $[\mathbf{w}]_1 \leftarrow_{\mathrm{R}} \mathbb{G}_1^{k+1}$ and then reverse the switch. Here, we use the fact that the security reduction on input either $([\mathbf{B}]_1, [\mathbf{Br}]_1)$ or $([\mathbf{B}]_1, [\mathbf{w}]_1)$, picks $\mathbf{K}_0, \mathbf{K}_1$ at random, and can compute $[\mathbf{K}_0 + \tau^*\mathbf{K}_1]_2$ given $[\tau^*]_2$ while simulating $\mathcal{O}^*$.†

To complete the proof, we need to bound the advantage of $\mathcal{A}$ in an experiment where we answer the i'th query τ to $\mathcal{O}_b$ with

$$\left(\left[b\mu\mathbf{a}^{\perp} + \mathbf{w}^{\top}(\mathbf{K}_0 + \tau\mathbf{K}_1)\right]_1, [\mathbf{w}^{\top}]_1\right), \text{where } \mu \leftarrow_{\mathrm{R}} \mathbb{Z}_q, \mathbf{w} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1};$$

and the remaining $q-1$ queries are handled using the normal $\mathcal{O}_0, \mathcal{O}_1$ as before. We may then proceed via an information-theoretic argument to bound the advantage for this experiment. As shown in [35], for all $\mathbf{A}, \mathbf{B} \leftarrow \mathcal{D}_k$, with probability $1 - 1/q$ over $\mathbf{w} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}$: for all $\tau \neq \tau^*$, the following distributions

$$(\mathsf{pk}, \mathbf{w}^{\top}(\mathbf{K}_0 + \tau\mathbf{K}_1), \mathbf{K}_0 + \tau^*\mathbf{K}_1) \text{ and } (\mathsf{pk}, \mu\mathbf{a}^{\perp} + \mathbf{w}^{\top}(\mathbf{K}_0 + \tau\mathbf{K}_1), \mathbf{K}_0 + \tau^*\mathbf{K}_1)$$

are the same, where $\mathbf{K}_0, \mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times(k+1)}$. This implies that for all $\tau \neq \tau^*$, the following distributions

$$(\mathsf{pk}, [\mathbf{w}^{\top}(\mathbf{K}_0 + \tau\mathbf{K}_1)]_1, [\mathbf{K}_0 + \tau^*\mathbf{K}_1]_2) \text{ and } (\mathsf{pk}, [\mu\mathbf{a}^{\perp} + \mathbf{w}^{\top}(\mathbf{K}_0 + \tau\mathbf{K}_1)]_1, [\mathbf{K}_0 + \tau^*\mathbf{K}_1]_2)$$

are the same†. The quantities in the distributions above correspond to the answers for the i'th query to $\mathcal{O}_b$ and the query to $\mathcal{O}^*$; moreover, given pk, we can compute $\mathbf{a}^{\perp}$ and simulate the remaining $Q-1$ queries to $\mathcal{O}_0$ and $\mathcal{O}_1$. This completes the proof. □

4.2 Our Scheme

The parameters are:

$$|\mathsf{pk}| = (n+1)k + 2(k+1)k + \mathsf{RE}(\mathcal{D}_k), \qquad |\sigma| = (3(k+1), 1),$$

where notation (x, y) means x elements in $\mathbb{G}_1$ and y elements in $\mathbb{G}_2$. For k-Lin, this yields $(n+6, (6,1))$ for $k = 1$ and $(2n+16, (9,1))$ for $k = 2$. Moreover, we note that the verification needs $2k+1$ pairing product equations: for $e(\sigma_1, [\mathbf{A}]_2) = e([(1, \mathbf{m})]_1, [\mathbf{C}]_2) \cdot e(\sigma_2, [\mathbf{C}_0]_2) \cdot e(\sigma_3, [\mathbf{C}_1]_2)$ we need to pair the vector σ_1 with every column of $[\mathbf{A}]_2$ and thus this check needs k pairing product equations; and for $e(\sigma_2, [\tau]_2) = e(\sigma_3, [1]_2)$ we need to pair every element from σ_2 with $[\tau]_2 \in \mathbb{G}_2$ and thus this requires $k+1$ pairing product equations.

```
$\mathsf{Gen}(\mathsf{par})$:
$\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k; \mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times(k+1)}$
$\mathbf{K}_0, \mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times(k+1)}$
$\mathbf{C} := \mathbf{K}\mathbf{A} \in \mathbb{Z}_q^{(n+1)\times k}$
$(\mathbf{C}_0, \mathbf{C}_1) := (\mathbf{K}_0\mathbf{A}, \mathbf{K}_1\mathbf{A}) \in (\mathbb{Z}_q^{(k+1)\times k})^2$
$(\mathbf{P}_0, \mathbf{P}_1) := (\mathbf{B}^\top\mathbf{K}_0, \mathbf{B}^\top\mathbf{K}_1) \in (\mathbb{Z}_q^{k\times(k+1)})^2$
$\mathsf{sk} := (\mathbf{K}, [\mathbf{P}_0]_1, [\mathbf{P}_1]_1, [\mathbf{B}]_1)$
$\mathsf{pk} := ([\mathbf{C}_0]_2, [\mathbf{C}_1]_2, [\mathbf{C}]_2, [\mathbf{A}]_2)$
Return $(\mathsf{pk}, \mathsf{sk})$
```

```
$\mathsf{Sign}(\mathsf{sk}, [\mathbf{m}]_1)$:
$\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k; \tau \leftarrow_{\mathrm{R}} \mathbb{Z}_q;$
$\sigma_1 := \left[(1, \mathbf{m}^\top)\mathbf{K} + \mathbf{r}^\top(\mathbf{P}_0 + \tau\mathbf{P}_1)\right]_1 \in \mathbb{G}_1^{1\times(k+1)}$
$\sigma_2 := \left[\mathbf{r}^\top\mathbf{B}^\top\right]_1 \in \mathbb{G}_1^{1\times(k+1)}$
$\sigma_3 := \left[\mathbf{r}^\top\mathbf{B}^\top\tau\right]_1 \in \mathbb{G}_1^{1\times(k+1)}$
$\sigma_4 := [\tau]_2 \in \mathbb{G}_2$
Return $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$

$\mathsf{Verify}(\mathsf{pk}, [\mathbf{m}]_1, \sigma)$:
Parse $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4 = [\tau]_2)$
Check:
$e(\sigma_1, [\mathbf{A}]_2) = e([(1, \mathbf{m})]_1, [\mathbf{C}]_2) \cdot e(\sigma_2, [\mathbf{C}_0]_2) \cdot e(\sigma_3, [\mathbf{C}_1]_2)$
$\wedge \quad e(\sigma_2, [\tau]_2) = e(\sigma_3, [1]_2)$
```

Fig. 3. Structure-preserving signature $\mathsf{SPS}_{\mathsf{full}}$ with message-space $\mathcal{M} = \mathbb{G}_1^n$.

Theorem 2. *Under the $\mathcal{D}_k$-MDDH Assumption in $\mathbb{G}_1$ and $\mathcal{D}_k$-KerMDH Assumption in $\mathbb{G}_2$, $\mathsf{SPS}_{\mathsf{full}}$ from Figure 3 is an unbounded CMA-secure structure-preserving signature scheme.*

Proof. Perfect correctness and the structure-preserving property are straight-forward. We proceed to establish the unbounded CMA-security. We will show that for any adversary $\mathcal{A}$ that makes at most Q signing queries, there exists adversaries $\mathcal{B}_0, \mathcal{B}_1$ with $\mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B}_0) \approx \mathbf{T}(\mathcal{B}_1)$ and

$$\mathbf{Adv}^{\mathrm{cma}}_{\mathsf{SPS}_{\mathsf{full}}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_0) + 2Q(Q+1) \cdot \mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) + (Q+1)^2/q + Q^2/2q. \tag{7}$$

We proceed via a series of games and we use $\mathbf{Adv}_i$ to denote the advantage of $\mathcal{A}$ in Game i.

Game 0. This is the CMA-security experiment from Definition 5.

$$\mathbf{Adv}^{\mathrm{cma}}_{\mathsf{SPS}_{\mathsf{full}}}(\mathcal{A}) = \mathbf{Adv}_0$$

Game 1. Switch Verify to Verify*:

```
$\mathsf{Verify}^*(\mathsf{pk}, [\mathbf{m}]_1, \sigma)$:
Parse $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4 = [\tau]_2)$
Check: $e(\sigma_1, [1]_2) = e([(1, \mathbf{m}^\top)\mathbf{K}]_1, [1]_2) \cdot e(\sigma_2, [\mathbf{K}_0 + \tau\mathbf{K}_1]_2)$
$\wedge \quad e(\sigma_2, [\tau]_2) = e(\sigma_3, [1]_2)$
```

Suppose $e(\sigma_2, [\tau]_2) = e(\sigma_3, [1]_2)$. We note that

$$\begin{aligned}
& e(\sigma_1, [\mathbf{A}]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{C}]_2) \cdot e(\sigma_2, [\mathbf{C}_0]_2) \cdot e(\sigma_3, [\mathbf{C}_1]_2) \\
\Longleftrightarrow\ & e(\sigma_1, [\mathbf{A}]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{K}\mathbf{A}]_2) \cdot e(\sigma_2, [\mathbf{K}_0\mathbf{A}]_2) \cdot e(\sigma_3, [\mathbf{K}_1\mathbf{A}]_2) \\
\Longleftarrow\ & e(\sigma_1, [1]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{K}]_2) \cdot e(\sigma_2, [\mathbf{K}_0]_2) \cdot e(\sigma_3, [\mathbf{K}_1]_2) \\
\Longleftrightarrow\ & e(\sigma_1, [1]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{K}]_2) \cdot e(\sigma_2, [\mathbf{K}_0 + \tau\mathbf{K}_1]_2)
\end{aligned}$$

Hence, for any $([\mathbf{m}]_1, \sigma)$ that passes Verify but not Verify^*, the value

$$\sigma_1 - ([(1, \mathbf{m}^\top)\mathbf{K}]_1 + \sigma_2\mathbf{K}_0 + \sigma_3\mathbf{K}_1) \in \mathbb{G}_1^{1\times(k+1)}$$

is a non-zero vector in the kernel of $\mathbf{A}$, which is hard to be computed under the $\mathcal{D}_k$-KerMDH assumption in $\mathbb{G}_2$. This means that

$$|\mathbf{Adv}_0 - \mathbf{Adv}_1| \leq \mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_0).$$

Game 2. Let $\tau_1, \ldots, \tau_Q$ denote the randomly chosen tags in the Q queries to SignO. We abort if $\tau_1, \ldots, \tau_Q$ are not all distinct.

$$\mathbf{Adv}_2 \geq \mathbf{Adv}_1 - Q^2/2q.$$

Game 3. We define $\tau_{Q+1} := \tau^*$. Now, pick $i^* \leftarrow_{\mathrm{R}} [Q+1]$ and abort if i^* is not the smallest index i for which $\tau^* = \tau_i$. In the rest of the proof, we focus on the case we do not abort, which means that $\tau^* = \tau_{i^*}$ and $\tau_1, \ldots, \tau_{i^*-1}$ are all different from τ^*. This means that given τ, SignO can check whether τ^* equals τ: for the rest $i^* - 1$ queries, answer NO, and starting from the i^*'th query, we know τ^*. It is easy to see that

$$\mathbf{Adv}_3 \geq \frac{1}{Q+1}\mathbf{Adv}_2.$$

Game 4. Switch SignO to SignO^* where

```
$\underline{\mathsf{SignO}^*([\mathbf{m}]_1)}$:                                    // adds $\mu\mathbf{a}^\perp$ for $\tau \neq \tau^*$
$\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k$; $\tau \leftarrow_{\mathrm{R}} \mathbb{Z}_q$; $\mu \leftarrow_{\mathrm{R}} \mathbb{Z}_q$;
if $\tau = \tau^*$ then $\mu := 0$
$\sigma_1 := \left[(1, \mathbf{m}^\top)\mathbf{K} + \mu\mathbf{a}^\perp + \mathbf{r}^\top(\mathbf{P}_0 + \tau\mathbf{P}_1)\right]_1$
$\sigma_2 := \left[\mathbf{r}^\top\mathbf{B}^\top\right]_1$
$\sigma_3 := \left[\mathbf{r}^\top\mathbf{B}^\top\tau\right]_1$
$\sigma_4 := [\tau]_2$
Return $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) \in \mathbb{G}_1^{1\times(k+1)} \times \mathbb{G}_1^{1\times(k+1)} \times \mathbb{G}_1^{1\times(k+1)} \times \mathbb{G}_2$
```

Here $\mathbf{a}^\perp \in \mathbb{Z}_q^{1\times(k+1)}$ is non-zero vector in the kernel of $\mathbf{A}$ such that $\mathbf{a}^\perp\mathbf{A} = \mathbf{0}$. We will use Lemma 3 to show that

$$|\mathbf{Adv}_3 - \mathbf{Adv}_4| \leq 2Q\mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) + Q/q$$

Basically, we pick $\mathbf{K}$ ourselves and use $\mathcal{O}_b$ to simulate either SignO or SignO^* and $\mathcal{O}^*$ to simulate Verify^* as follows:

- For the i'th signing query $[\mathbf{m}]_1$ where $i \neq i^*$,we query $\mathcal{O}_b$ at $\tau \leftarrow_{\mathrm{R}} \mathbb{Z}_q$ to obtain

$$(\sigma_1', \sigma_2) := (\left[b\mu\mathbf{a}^\perp + \mathbf{r}^\top(\mathbf{P}_0 + \tau\mathbf{P}_1)\right]_1, [\mathbf{r}^\top\mathbf{B}^\top]_1),$$

  and we return

$$(\sigma_1 := [(1, \mathbf{m}^\top)\mathbf{K}]_1 \cdot \sigma_1',\ \sigma_2,\ \sigma_3 := \sigma_2\tau,\ \sigma_4 := [\tau]_2)$$

- For the i^*'th signing query $[\mathbf{m}]_1$ where $i^* \le Q$, we run Sign honestly using our knowledge of $\mathbf{K}, [\mathbf{P}_0]_1, [\mathbf{P}_1], [\mathbf{B}]_1$.
- For Verify*, we will query $\mathcal{O}^*$ on $[\tau^*]_2$ to get $[\mathbf{K}_0 + \tau^* \mathbf{K}_1]_2$. The latter is sufficient to simulate the Verify* query by computing $e(\sigma_2, [\mathbf{K}_0 + \tau^* \mathbf{K}_1]_2)$.

This allows us to then build a distinguisher for Lemma 3.

Game 5. Switch $\mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times(k+1)}$ in Gen to $\mathbf{K} := \mathbf{K}' + \mathbf{u}\mathbf{a}^{\perp}$, where $\mathbf{K}' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times(k+1)}$, $\mathbf{u} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n+1}$. Since $\mathbf{u}\mathbf{a}^{\perp}$ is masked by a uniform matrix $\mathbf{K}'$, $\mathbf{K}$ in Game 5 is still uniformly random and thus Game 4 and 5 are identical. We have

$$\mathbf{Adv}_5 = \mathbf{Adv}_4.$$

To conclude the proof, we bound the adversarial advantage in Game 5 via an information-theoretic argument. We first consider the information about $\mathbf{u}$ leaked from pk and signing queries:

- $\mathbf{C} = (\mathbf{K}' + \mathbf{u}\mathbf{a}^{\perp})\mathbf{A} = \mathbf{K}'\mathbf{A}$ completely hides $\mathbf{u}$;
- the output of SignO* on $(\mathbf{m}, \tau)$ for $\tau \neq \tau^*$ completely hides $\mathbf{u}$, since $(1, \mathbf{m}^{\top})(\mathbf{K}' + \mathbf{u}\mathbf{a}^{\perp}) + \mu\mathbf{a}^{\perp}$ is identically distributed to $(1, \mathbf{m}^{\top})\mathbf{K}' + \mu\mathbf{a}^{\perp}$ (namely, $(1, \mathbf{m}^{\top})\mathbf{u}$ is masked by $\mu \leftarrow_{\mathrm{R}} \mathbb{Z}_q$).
- the output of SignO* on τ^* leaks $(1, \mathbf{m}^{\top})(\mathbf{K}' + \mathbf{u}\mathbf{a}^{\perp})$, which is captured by $(1, \mathbf{m}^{\top})\mathbf{u}$.

To convince Verify* to accept a signature σ^* on $\mathbf{m}^*$, the adversary must correctly compute

$$(1, \mathbf{m}^{*\top})(\mathbf{K}' + \mathbf{u}\mathbf{a}^{\perp})$$

and thus $(1, \mathbf{m}^{*\top})\mathbf{u} \in \mathbb{Z}_q$. Given $(1, \mathbf{m}^{\top})\mathbf{u}$, for any adaptively chosen $\mathbf{m}^* \neq \mathbf{m}$, we have that $(1, \mathbf{m}^{*\top})\mathbf{u}$ is uniformly random over $\mathbb{Z}_q$ from the adversary's view-point. Therefore, $\mathbf{Adv}_5 \le 1/q$.

□

5 Security against Random Message Attacks

In this section, we consider possible efficiency improvements on the structure-preserving signatures (SPS) from Sections 3 and 4 for the weaker security notion of *unforgeability against random message attacks* (RMA). Precisely, we obtain a one-time RMA-secure SPS with signature size one less than that from Figure 2 and an unbounded RMA-secure SPS with signature size $k + 1$ less than that from Figure 3. Figure 4 summarizes our results.

Our rSPS$_{\mathsf{ot}}$ is optimal for both the Type I and III settings: in the Type I setting, under the 2-Lin assumption, rSPS$_{\mathsf{ot}}$ requires 2 elements and 2 verification equations, matching the lower bound for one-time RMA-secure SPS from [8]; in the Type III setting, under the SXDH assumption, rSPS$_{\mathsf{ot}}$ requires 1 element and 1 verification equation, which is clearly optimal.

	Security	Assumption	$\lvert\mathbf{m}\rvert$	$\lvert\sigma\rvert$	$\lvert$pk$\rvert$	# equations
AGOT14 (Fig. 2) [8]	OT	Generic (Type I)	1	2	3	2
AGOT14 (Fig. 3) [8]	OT	Generic (Type III)	n	$(1,0)$	$n+3$	1
ACDKNO12 [2]	full	2-Lin	6	8	13	7
rSPS$_{\mathsf{ot}}$ (Fig 5)	OT	$\mathcal{D}_k$-KerMDH ($\mathbb{G}_2$)	n	$(k,0)$	$(n+1)k + \mathsf{RE}(\mathcal{D}_k)$	k
rSPS$_{\mathsf{full}}$ (Fig 6)	full	$\mathcal{D}_k$-MDDH ($\mathbb{G}_1, \mathbb{G}_2$)	n	$(2k+2,1)$	$(n+2k+3)k + \mathsf{RE}(\mathcal{D}_k)$	$2k+1$

Fig. 4. Structure-preserving signatures secure against random message attacks for $\mathcal{M} = \mathbb{G}_1^n$ in the Type I and III setting. For the Type I setting we have $\mathbb{G} = \mathbb{G}_1 = \mathbb{G}_2$. Notation (x, y) represents x elements in $\mathbb{G}_1$ and y elements in $\mathbb{G}_2$.

5.1 Unforgeability against Random Message Attacks

RMA-security states that it is hard for an adversary to forge a signature even if he sees many signatures on randomly chosen messages. The security is formally defined as follows:

Definition 6 (Unforgeability against random message attacks). *To an adversary $\mathcal{A}$ and* SPS *we associate the advantage function*

$$\mathbf{Adv}^{\mathrm{rma}}_{\mathsf{SPS}}(\mathcal{A}) := \Pr\left[[\mathbf{m}^*] \notin \mathcal{Q}_{\mathrm{msg}} \wedge \mathsf{Verify}(\mathsf{pk}, [\mathbf{m}^*], \sigma^*) = 1 \,\middle|\, \begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow_{\mathrm{R}} \mathsf{Gen}(\mathsf{par}) \\ ([\mathbf{m}^*], \sigma^*) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathsf{SignO}()}(\mathsf{pk}) \end{array} \right],$$

where $\mathsf{SignO}()$ *chooses a random message* $[\mathbf{m}] \leftarrow_{\mathrm{R}} \mathbb{G}^n$*, runs* $\sigma \leftarrow_{\mathrm{R}} \mathsf{Sign}(\mathsf{sk}, [\mathbf{m}])$*, adds the vector* $[\mathbf{m}]$ *to* $\mathcal{Q}_{\mathrm{msg}}$ *(initialized with* $\emptyset$*) and returns* $([\mathbf{m}], \sigma)$ *to* $\mathcal{A}$. SPS *is said to be* RMA-secure *if for all PPT adversaries* $\mathcal{A}$*,* $\mathbf{Adv}^{\mathrm{rma}}_{\mathsf{SPS}}(\mathcal{A})$ *is negligible.* SPS *is said to be* one-time RMA-secure *with corresponding advantage function* $\mathbf{Adv}^{\mathrm{ot\text{-}rma}}_{\mathsf{SPS}}(\mathcal{A})$*, if* $\mathcal{A}$ *is restricted to make at most one query to oracle* SignO.

5.2 One-Time RMA-Secure SPS

Motivated by the techniques used in [34, 1, 35] to obtain shorter QANIZK proofs for linear subspaces, we construct a one-time RMA-secure SPS in Figure 5 with the following parameters:

$$|\mathsf{pk}| = (n+1)k + \mathsf{RE}(\mathcal{D}_k), \qquad |\sigma| = k.$$

For k-Lin, this yields $(|\mathsf{pk}|, |\sigma|) = (n+2, 1)$ for $k = 1$ and $(2n+4, 2)$ for $k = 2$. Moreover, we note that verification needs k pairing product equations for $e(\sigma_1, \left[\overline{\mathbf{A}}\right]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{C}]_2)$. Compared with $\mathsf{SPS}_{\mathsf{ot}}$, we reduce the signature size by one element.

```
Gen(par):
    $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k; \mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times k}$
    $\mathbf{C} := \mathbf{K}\overline{\mathbf{A}} \in \mathbb{Z}_q^{(n+1)\times k}$
    $\mathsf{sk} := \mathbf{K}$
    $\mathsf{pk} := ([\mathbf{C}]_2, [\overline{\mathbf{A}}]_2)$
    Return $(\mathsf{pk}, \mathsf{sk})$

Sign(sk, $[\mathbf{m}]_1$):
    $\sigma := \left[(1, \mathbf{m}^\top)\mathbf{K}\right]_1$
    Return $\sigma \in \mathbb{G}_1^{1\times k}$

Verify(pk, $[\mathbf{m}]_1, \sigma$):
    Check: $e(\sigma, \left[\overline{\mathbf{A}}\right]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{C}]_2)$
```

Fig. 5. One-time RMA-secure structure-preserving signature $\mathsf{rSPS}_{\mathsf{ot}}$ with message-space $\mathcal{M} = \mathbb{G}_1^n$. Recall that $\overline{\mathbf{A}}$ denotes the upper $k \times k$ submatrix of $\mathbf{A}$.

Theorem 3. *Under the* $\mathcal{D}_k$-KerMDH *Assumption in* $\mathbb{G}_2$*,* $\mathsf{rSPS}_{\mathsf{ot}}$ *from Figure 5 is a one-time* RMA-*secure structure-preserving signature scheme.*

Our proof is similar to that in [35, Theorem 2]. As we choose $\mathbf{m} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^n$ in the security game ourselves, we can compute the kernel basis $\mathbf{M}^\perp \in \mathbb{Z}_q^{(n+1)\times n}$ of $(1, \mathbf{m}^\top)$ such that $(1, \mathbf{m}^\top) \cdot \mathbf{M}^\perp = \mathbf{0}$ and then we embed $\mathbf{M}^\perp$ in the secret key $\mathbf{K}$. This way we do not need to compute the kernel of $[\mathbf{A}]_2$ when answering the signing query. However, for the forgery $\mathbf{m}^* \neq \mathbf{m}$, since $(1, \mathbf{m}^{*\top})\mathbf{M}^\perp \neq \mathbf{0}$, the adversary has to compute an element from the kernel to break RMA-security, which is infeasible under the $\mathcal{D}_k$-KerMDH Assumption.

Proof. Perfect correctness and the structure-preserving property are straight-forward to verify. We proceed to establish one-time RMA-security based on the $\mathcal{D}_k$-KerMDH assumption. We will show that for all adversaries $\mathcal{A}$, there exists an adversary $\mathcal{B}$ with $\mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B})$ and

$$\mathbf{Adv}^{\text{ot-rma}}_{\mathsf{rSPS_{ot}}}(\mathcal{A}) \le \mathbf{Adv}^{\text{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}) + 1/q. \tag{8}$$

Adversary $\mathcal{B}(\mathcal{PG}, [\mathbf{A}]_2 \in \mathbb{G}_2^{(k+1)\times k})$ chooses $\mathbf{m} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^n$ before generating the public and secret keys; $\mathbf{m}$ corresponds to the random message $[\mathbf{m}]_1$ chosen by $\mathsf{SignO}(\cdot)$. Let $\mathbf{M}^{\perp} \in \mathbb{Z}_q^{(n+1)\times n}$ be a basis for the kernel of $(1, \mathbf{m}^\top)$ such that $(1, \mathbf{m}^\top)\mathbf{M}^{\perp} = \mathbf{0} \in \mathbb{Z}_q^{1\times n}$. $\mathbf{M}^{\perp} = (-\mathbf{m}||\mathbf{I}_n)^\top$ can be efficiently computed by $\mathcal{B}$, as he knows $\mathbf{m}$ over $\mathbb{Z}_q$. Next, $\mathcal{B}$ picks $\mathbf{K}' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times k}$, $\mathbf{R} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n-1)\times(k+1)}$ and defines

$$\mathbf{A}' := \begin{pmatrix} \mathbf{A} \\ \mathbf{R}\cdot\mathbf{A} \end{pmatrix} \in \mathbb{Z}_q^{(k+n)\times k}.$$

Let $\mathbf{T}_{\mathbf{A}'} := \underline{\mathbf{A}'} \cdot (\overline{\mathbf{A}'})^{-1} \in \mathbb{Z}_q^{n\times k}$, where $\overline{\mathbf{A}'}$ denotes the first k rows of $\mathbf{A}'$ (i.e., $\overline{\mathbf{A}'} = \overline{\mathbf{A}}$) and $\underline{\mathbf{A}'}$ denotes the last n rows of $\mathbf{A}'$. By defining $\mathbf{K} := \mathbf{K}' + \mathbf{M}^{\perp}\mathbf{T}_{\mathbf{A}'}$, $\mathcal{B}$ can compute

$$[\mathbf{C}]_2 = [\mathbf{K}\cdot\overline{\mathbf{A}}]_2 = [(\mathbf{K}' + \mathbf{M}^{\perp}\mathbf{T}_{\mathbf{A}'})\cdot\overline{\mathbf{A}}]_2 = [\mathbf{K}'\overline{\mathbf{A}'} + \mathbf{M}^{\perp}\underline{\mathbf{A}'}]_2 = [(\mathbf{K}'||\mathbf{M}^{\perp})\mathbf{A}']_2$$

and runs $\mathcal{A}(\mathsf{pk} := ([\mathbf{C}]_2, [\overline{\mathbf{A}}]_2))$. Upon the single random message signing query, $\mathcal{B}$ computes

$$\sigma := [(1,\mathbf{m}^\top)\mathbf{K}]_1 = [(1,\mathbf{m}^\top)(\mathbf{K}' + \mathbf{M}^{\perp}\mathbf{T}_{\mathbf{A}'})]_1 = [(1,\mathbf{m}^\top)\mathbf{K}' + \mathbf{0}]_1 = [(1,\mathbf{m}^\top)\mathbf{K}']_1$$

and returns $([\mathbf{m}]_1, \sigma)$. We note that the simulated distribution is identical to the real distribution.

Let $([\mathbf{m}^*]_1, \sigma^* := [\mathbf{z}^\top]_1)$ be a valid forgery from $\mathcal{A}$ and $\mathbf{y}^\top := (1, \mathbf{m}^{*\top})$, i.e., $\mathbf{z}^\top \cdot \overline{\mathbf{A}} = \mathbf{y}^\top \cdot \mathbf{C}$. By the definitions of $\mathbf{C}$ and $\mathbf{A}'$,

$$\mathbf{z}^\top\overline{\mathbf{A}} = (\mathbf{z}^\top||\mathbf{0})\mathbf{A}' = \mathbf{y}^\top\cdot\mathbf{C} = \mathbf{y}^\top(\mathbf{K}'||\mathbf{M}^{\perp})\cdot\mathbf{A}'$$

such that $[\mathbf{c}]_1$ with

$$\mathbf{c}^\top = ((\mathbf{z}^\top - \mathbf{y}^\top\mathbf{K}')|| - \mathbf{y}^\top\mathbf{M}^{\perp})$$

satisfies $\mathbf{c}^\top\mathbf{A}' = \mathbf{0}$. As $\mathbf{m}^* \neq \mathbf{m}$, $\mathbf{y}^\top \notin \mathit{span}(1, \mathbf{m}^\top)$ and thus $\mathbf{y}^\top \cdot \mathbf{M}^{\perp} \neq \mathbf{0}$. That implies $\mathbf{c} \neq \mathbf{0}$. Finally, $\mathcal{B}$ can extract a solution $[\mathbf{s}]_1$ to the $\mathcal{D}_k$-KerMDH problem in $\mathbb{G}_2$, from $[\mathbf{c}^\top]_1 = [\mathbf{c}_1^\top||\mathbf{c}_2^\top]_1 \in \mathbb{G}_1^{1\times(k+1)} \times \mathbb{G}_1^{1\times(n-1)}$. Define $\mathbf{s}^\top := \mathbf{c}_1^\top + \mathbf{c}_2^\top\mathbf{R} \in \mathbb{Z}_q^{1\times(k+1)}$ such that

$$\mathbf{s}^\top\mathbf{A} = \mathbf{c}_1^\top\mathbf{A} + \mathbf{c}_2^\top\mathbf{R}\mathbf{A} = (\mathbf{c}_1^\top||\mathbf{c}_2^\top)\cdot\begin{pmatrix} \mathbf{A} \\ \mathbf{R}\cdot\mathbf{A} \end{pmatrix} = \mathbf{c}^\top\mathbf{A}' = \mathbf{0}.$$

As $\mathcal{B}$ knows $\mathbf{R}, \mathbf{K}'$ and $\mathbf{M}^{\perp}$ over $\mathbb{Z}_q$, he can efficiently compute $[\mathbf{s}]_1$. It remains to show that $\mathbf{s} \neq 0$, with high probability. As $\mathbf{c} \neq \mathbf{0}$ and matrix $\mathbf{R}$ is only leaked through $\mathbf{A}'$ via $\mathbf{R}\mathbf{A}$, we have

$$\Pr_{\mathbf{R}\leftarrow_{\mathrm{R}}\mathbb{Z}_q^{(n-1)\times(k+1)}}[\mathbf{c}_1^\top + \mathbf{R}\mathbf{c}_2^\top = \mathbf{0}|\mathbf{R}\mathbf{A}] \le \frac{1}{q}.$$

This proves equation (8).

5.3 Unbounded RMA-Secure SPS

Consider the scheme $\mathsf{SPS}_{\mathsf{full}}$ from Figure 3 with the modification that in the signing algorithm, vector $\mathbf{Br}$ is chosen as a random vector as $\mathbf{t} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}$. Clearly, under the $\mathcal{D}_k$-MDDH Assumption, this modified scheme is also a CMA-secure SPS. Suppose that the message space is $\mathbb{G}_1^n$ with $n = n' + k + 1 \geq k + 1$. Then we can view the random vector $[\mathbf{t}]_1 \in \mathbb{G}_1^{k+1}$ as part of the message space which reduces the signature size from $3k + 4$ elements to $2k + 3$. The modified scheme is presented in Figure 6. Its parameters are:

$$|\mathsf{pk}| = (n+1)k + 2(k+1)k + \mathsf{RE}(\mathcal{D}_k), \qquad |\sigma| = (2(k+1), 1),$$

where notation (x, y) means x elements in $\mathbb{G}_1$ and y elements in $\mathbb{G}_2$. For k-Lin, $(|\mathsf{pk}|, |\sigma|) = (n + 6, (4, 1))$ for $k = 1$ and $(2n + 16, (6, 1))$ for $k = 2$. Moreover, we note that the verification needs $2k + 1$ pairing product equations. Compared with the $\mathsf{SPS}_{\mathsf{full}}$ from Figure 3, $\mathsf{rSPS}_{\mathsf{full}}$ requires $(k + 1)$ elements less in the signature.

```
$\underline{\mathsf{Gen}(\mathsf{par})}$:
$\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k; \mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times(k+1)}$
$\mathbf{K}_0, \mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times(k+1)}$
$\mathbf{C} := \mathbf{KA} \in \mathbb{Z}_q^{(n+1)\times k}$
$(\mathbf{C}_0, \mathbf{C}_1) := (\mathbf{K}_0\mathbf{A}, \mathbf{K}_1\mathbf{A}) \in (\mathbb{Z}_q^{(k+1)\times k})^2$
$\mathsf{sk} := (\mathbf{K}, \mathbf{K}_0, \mathbf{K}_1)$
$\mathsf{pk} := ([\mathbf{C}_0]_2, [\mathbf{C}_1]_2, [\mathbf{C}]_2, [\mathbf{A}]_2)$
Return $(\mathsf{pk}, \mathsf{sk})$
```

```
$\underline{\mathsf{Sign}(\mathsf{sk}, [\mathbf{m}]_1)}$:
Parse $[\mathbf{m}]_1 = ([\mathbf{s}]_1, [\mathbf{t}]_1) \in \mathbb{G}_1^{n'} \times \mathbb{G}_1^{k+1}$
$\tau \leftarrow_{\mathrm{R}} \mathbb{Z}_q$;
$\sigma_1 := \left[(1, \mathbf{m}^\top)\mathbf{K} + \mathbf{t}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1)\right]_1$
$\sigma_2 := \left[\tau\mathbf{t}^\top\right]_1$
$\sigma_3 := [\tau]_2$
Return $(\sigma_1, \sigma_2, \sigma_3) \in \mathbb{G}_1^{1\times(k+1)} \times \mathbb{G}_1^{1\times(k+1)} \times \mathbb{G}_2$

$\underline{\mathsf{Verify}(\mathsf{pk}, [\mathbf{m}]_1, \sigma)}$:
Parse $\sigma = (\sigma_1, \sigma_2, \sigma_3 = [\tau]_2)$
Parse $[\mathbf{m}]_1 = ([\mathbf{s}]_1, [\mathbf{t}]_1)$
Check:
$e(\sigma_1, [\mathbf{A}]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{C}]_2) \cdot e([\mathbf{t}^\top]_1, [\mathbf{C}_0]_2) \cdot e(\sigma_2, [\mathbf{C}_1]_2)$
$\wedge \quad e(\sigma_2, [1]_2) = e([\mathbf{t}^\top]_1, [\tau]_2)$
```

Fig. 6. An unbounded RMA-secure structure-preserving signature $\mathsf{rSPS}_{\mathsf{full}}$ with message-space $\mathcal{M} = \mathbb{G}_1^n$ where $n = n' + k + 1 \geq k + 1$.

Theorem 4. *Under the $\mathcal{D}_k$-*MDDH *Assumption in $\mathbb{G}_1$ and $\mathcal{D}_k$-*KerMDH *Assumption in $\mathbb{G}_2$,* $\mathsf{rSPS}_{\mathsf{full}}$ *from Figure 6 is an unbounded* RMA*-secure structure-preserving signature scheme.*

The proof is given in Appendix A.

6 Structure-Preserving Signatures for Bilateral Message Spaces

Let $\mathcal{M} := \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$ be a message space. In Type III pairing groups, $\mathcal{M}$ is bilateral if both $n_1 \neq 0$ and $n_2 \neq 0$; otherwise, $\mathcal{M}$ is unilateral. In this section, we extend the construction from Section 4 to sign bilateral message spaces.

The main idea of our construction is to use the Even-Goldreich-Micali (EGM) framework [23] and a method of Abe *et al.* [2]: for $\mathbf{m} = ([\mathbf{m}_1]_1, [\mathbf{m}_2]_2) \in \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$ we sign $[\mathbf{m}_1]_1$ by using a one-time SPS with a fresh public key $\mathsf{pk}_{\mathsf{ot}}$ over $\mathbb{G}_2$ and then sign message $([\mathbf{m}_2]_2, \mathsf{pk}_{\mathsf{ot}})$ using an unbounded CMA-secure SPS; the signature on $([\mathbf{m}_1]_1, [\mathbf{m}_2]_2)$ is $\mathsf{pk}_{\mathsf{ot}}$ together with the concatenation of both signatures. However, this yields long signatures as $\mathsf{pk}_{\mathsf{ot}}$ contains $O(n_1 k)$ group element for the best known one-time SPS. Next, we observe that our one-time SPS is in fact a so-called "two-tier" signature scheme, i.e. opk can decomposed into a reusable long *primary key* plus a one-time short *secondary key* which contains only k group elements. For the transformation sketched above it is sufficient to put the short secondary key in the signature which leads to short signatures.

Concretely, under the SXDH assumption, our signature on messages in $\mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$ contain $(7, 3)$ group elements (7 elements in $\mathbb{G}_1$ and 3 elements in $\mathbb{G}_2$), 4 pairing product equations for verification and $(n_1 + n_2 + 8)$ group elements in public keys. A previous SXDH-based construction from [2] required $(8, 6)$ group elements in the signature, 5 pairing product equations, and $(n_1 + n_2 + 22)$ elements in the public key.

We note that our idea gives a generic way to extend message space $\mathcal{M}_1$ to $\mathcal{M}_1 \times \mathcal{M}_2$ for signature schemes, where $\mathcal{M}_1$ and $\mathcal{M}_2$ are arbitrary message spaces. In Subsection 6.1, we present our transformation for arbitrary (not necessarily structure-preserving) signatures and show that $\mathsf{SPS}_{\mathsf{ot}}$ from Figure 2 satisfies the stronger notion of two-tier signatures. Finally, in Subsection 6.2, we instantiate the transformation with the above two-tier SPS and the unbounded CMA-secure $\mathsf{SPS}_{\mathsf{full}}$ from Figure 3. By our generic composition theorem the resulting scheme is unbounded CMA secure. Furthermore, it can be verified to be structure-preserving for bilateral message spaces.

6.1 Two-Tier Signatures

The notion of two-tier signatures was firstly proposed by Bellare and Shoup [12] and considered to the structure-preserving setting by Abe *et al.* [2] (called partial one-time signatures in [2]). A two-tier signature scheme is like a standard signature scheme except that the public (secret) key is split into a fixed primary part pk (sk) and a variable secondary part opk (osk). We recall the definition of a two-tier signature scheme and its security.

Definition 7 (Two-tier signature). *A two-tier signature scheme* TTS *is defined as a tuple of probabilistic polynomial time (PPT) algorithms* $\mathsf{TTS} := (\mathsf{PGen}, \mathsf{SGen}, \mathsf{TTSign}, \mathsf{TTVerify})$*:*

- *The probabilistic primary key generation algorithm* $\mathsf{PGen}(\mathsf{par})$ *returns the primary public/secret key* $(\mathsf{pk}, \mathsf{sk})$. *We assume that* pk *implicitly defines a message space* $\mathcal{M}$ *and a secondary public key space* $\mathcal{OPK}$.
- *The probabilistic secondary key generation algorithm* $\mathsf{SGen}(\mathsf{pk}, \mathsf{sk})$ *returns the secondary public/secret key* $(\mathsf{opk}, \mathsf{osk})$.
- *The probabilistic signing algorithm* $\mathsf{TTSign}(\mathsf{sk}, \mathsf{osk}, \mathsf{m})$ *returns a signature* σ.
- *The deterministic verification algorithm* $\mathsf{TTVerify}(\mathsf{pk}, \mathsf{opk}, \mathsf{m}, \sigma)$ *returns 1 (accept) or 0 (reject).*

(Perfect correctness.) *for all* $(\mathsf{pk}, \mathsf{sk}) \leftarrow_{\mathrm{R}} \mathsf{PGen}(\mathsf{par})$*, all* $(\mathsf{opk}, \mathsf{osk}) \leftarrow_{\mathrm{R}} \mathsf{SGen}(\mathsf{pk}, \mathsf{sk})$*, all messages* $\mathsf{m} \in \mathcal{M}$ *and all* $\sigma \leftarrow_{\mathrm{R}} \mathsf{TTSign}(\mathsf{sk}, \mathsf{osk}, \mathsf{m})$ *we have* $\mathsf{TTVerify}(\mathsf{pk}, \mathsf{opk}, \mathsf{m}, \sigma) = 1$.

In the following, we define two-tier CMA security (TT-CMA-security) for TTS (which was called OT-NACMA-security in [2]). It is weaker than the original security notion from [12] but sufficient for our application. (We note that our two-tier SPS in Figure 7 satisfies the stronger security from [12].)

Definition 8 (TT-CMA**-security).** *To an adversary* $\mathcal{A}$ *and* TTS *we associate the advantage function*

$$\mathbf{Adv}_{\mathsf{TTS}}^{\text{tt-cma}}(\mathcal{A}) := \Pr\left[\begin{array}{l} (i^*, \mathsf{m}, \sigma) \in \mathcal{Q}_{\text{msg}} \wedge \mathsf{m}^* \neq \mathsf{m} \\ \wedge \mathsf{TTVerify}(\mathsf{pk}, \mathsf{opk}_{i^*}, \mathsf{m}^*, \sigma^*) = 1 \end{array} \middle| \begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow_{\mathrm{R}} \mathsf{PGen}(\mathsf{par}) \\ (i^*, \mathsf{m}^*, \sigma^*) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathsf{TTSignO}(\cdot)}(\mathsf{pk}) \end{array}\right],$$

where

- $\mathsf{TTSignO}(\mathsf{m})$*:* $i = i + 1$ *(initialized with* 0*), generates* $(\mathsf{opk}_i, \mathsf{osk}_i) \leftarrow_{\mathrm{R}} \mathsf{SGen}(\mathsf{pk}, \mathsf{sk})$*, computes* $\sigma \leftarrow_{\mathrm{R}} \mathsf{TTSign}(\mathsf{sk}, \mathsf{osk}_i, \mathsf{m})$*, adds* (i, m, σ) *to* $\mathcal{Q}_{\mathrm{msg}}$ *(initialized with* $\emptyset$*) and returns* (opk_i, σ)*.*

TTS *is said to be* TT-CMA-secure *if for all PPT adversaries* $\mathcal{A}$*,* $\mathbf{Adv}^{\text{tt-cma}}_{\mathsf{TTS}}(\mathcal{A})$ *is negligible.*

Our two-tier signature scheme. We now show that $\mathsf{SPS}_{\mathsf{ot}}$ from Figure 2 can be modified to be a two-tier signature scheme with message space $\mathcal{M} = \mathbb{G}_1^n$ in Figure 7. We split the secret key of $\mathsf{SPS}_{\mathsf{ot}}$ (matrix $\mathbf{K}$) into the first row $\mathbf{k}^\top$ and the lower n rows $\mathbf{K}'$. Matrix $\mathbf{K}'$ is the primary secret key and vector $\mathbf{k}$ is the secondary secret key. The reason why we can reuse $\mathbf{K}'$ is that in each signing query a fresh $\mathbf{k}_i$ is chosen which hides $\mathbf{m}^\top\mathbf{K}'$. The only information leaked from signing queries is $(1, \mathbf{m}^\top)\binom{\mathbf{k}_{i^*}^\top}{\mathbf{K}'}$. Given that, $(1, \mathbf{m}^{*\top})\binom{\mathbf{k}_{i^*}^\top}{\mathbf{K}'}$ is uniform for $\mathbf{m}^* \neq \mathbf{m}$ by the same arguments as in Section 3. Lemma 4 formalizes the above intuition and security of $\mathsf{TTSPS}_{\mathsf{ot}}$ is shown in Theorem 5. We note that $\mathsf{TTSPS}_{\mathsf{ot}}$ is a generalization of $\mathsf{POSu2}$ from [2].

```
PGen(par):
  $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k; \mathbf{K}' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}$
  $\mathbf{C}' := \mathbf{K}'\mathbf{A} \in \mathbb{Z}_q^{n\times k}$
  Return $(\mathsf{pk} := ([\mathbf{C}']_2, [\mathbf{A}]_2), \mathsf{sk} := \mathbf{K}')$

SGen(pk, sk)
  $\mathbf{k} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}; \mathbf{c} := \mathbf{k}^\top\mathbf{A} \in \mathbb{Z}_q^{1\times k}$
  Return $(\mathsf{opk} := [\mathbf{c}]_2, \mathsf{osk} := \mathbf{k})$
```

```
TTSign(sk, osk, $[\mathbf{m}]_1$):
  $\mathbf{K} := \begin{pmatrix}\mathbf{k}^\top \\ \mathbf{K}'\end{pmatrix}$
  $\sigma := \big[(1, \mathbf{m}^\top)\mathbf{K}\big]_1$
  Return $\sigma \in \mathbb{G}_1^{1\times(k+1)}$

TTVerify(pk, opk $= [\mathbf{c}]_2, [\mathbf{m}]_1, \sigma$):
  $\mathbf{C} := \begin{pmatrix}\mathbf{c} \\ \mathbf{C}'\end{pmatrix}$
  Check: $e(\sigma, [\mathbf{A}]_2) = e([1, \mathbf{m}^\top]_1, [\mathbf{C}]_2)$
```

Fig. 7. Two-tier signature scheme $\mathsf{TTSPS}_{\mathsf{ot}}$ with message-space $\mathcal{M} = \mathbb{G}_1^n$.

The following is the main computational core lemma required for the proof of $\mathsf{TTSPS}_{\mathsf{ot}}$.

Lemma 4. *Let* n, k *be integers. For any* $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$ *and any (possibly unbounded) adversary* $\mathcal{A}$*,*

$$\Pr\left[\begin{array}{l} (i^*, \mathbf{m}) \in \mathcal{Q}_{\mathrm{msg}} \wedge \mathbf{m}^* \neq \mathbf{m} \\ \wedge(\mathbf{z}^\top = (1, \mathbf{m}^{*\top}) \cdot \binom{\mathbf{k}_{i^*}^\top}{\mathbf{K}'}) \end{array}\middle| \begin{array}{l} \mathbf{K}' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)} \\ (i^*, \mathbf{m}^*, \mathbf{z}) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathcal{O}(\cdot)}(\mathbf{K}'\mathbf{A}) \end{array}\right] \leq \frac{1}{q}, \tag{9}$$

where:

- $\mathcal{O}(\mathbf{m})$*:* $i = i + 1$ *(initialized with 0), picks* $\mathbf{k}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}$*, adds* $(i, \mathbf{m})$ *to* $\mathcal{Q}_{\mathrm{msg}}$ *(initialized with* $\emptyset$*) and returns* $\mathbf{k}_i^\top\mathbf{A}$ *and* $(1, \mathbf{m}^\top) \cdot \binom{\mathbf{k}_i^\top}{\mathbf{K}'}$*.*

Proof. Fix any $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$. Let $\mathbf{a}^\perp \in \mathbb{Z}_q^{1\times(k+1)}$ be a non-zero vector in the kernel of $\mathbf{A}$ such that $\mathbf{a}^\perp \cdot \mathbf{A} = \mathbf{0} \in \mathbb{Z}_q^{1\times k}$. We make the following changes to the distribution of the experiment:

- Switch $\mathbf{K}' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}$ to $\mathbf{K}' = \mathbf{K}'' + \mathbf{u}\mathbf{a}^\perp$, where $\mathbf{K}'' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}$ and $\mathbf{u} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^n$.
- Switch $\mathbf{k}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}$ in $\mathcal{O}$ to $\mathbf{k}_i = \mathbf{k}_i' + (u_i\mathbf{a}^\perp)^\top$, where $\mathbf{k}_i' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}$ and $u_i \leftarrow_{\mathrm{R}} \mathbb{Z}_q$.

We note that the modified distribution is identical to the real distribution of the experiment, since $\mathbf{K}''$ and $\mathbf{k}_i'$ are uniformly chosen, In the following, we consider the information about $(u_{i^*}, \mathbf{u})$ leaked from $\mathbf{K}'\mathbf{A}$ and the answers of the $\mathcal{O}$ queries in order to argue that equation (9) holds for any (possibly unbounded) adversary $\mathcal{A}$:

- Since $\mathbf{K}'\mathbf{A} = (\mathbf{K}'' + \mathbf{u}\mathbf{a}^\perp)\mathbf{A} = \mathbf{K}''\mathbf{A}$, the matrix $\mathbf{K}'\mathbf{A}$ leaks nothing about $\mathbf{u}$. By the same argument, the values $\mathbf{k}_i^\top\mathbf{A}$ from the $\mathcal{O}$ queries leak nothing about the u_i.
- The output of the j-th query to $\mathcal{O}$ on $\mathbf{m}_j$ for $j \neq i^*$ hides $\mathbf{u}$. The reason is that $(1, \mathbf{m}_j^\top)\binom{\mathbf{k}_j^\top}{\mathbf{K}'} = \mathbf{k}_j^\top + \mathbf{m}_j^\top\mathbf{K}' = \mathbf{k}_j'^\top + u_j\mathbf{a}^\perp + \mathbf{m}_j^\top(\mathbf{K}'' + \mathbf{u}\mathbf{a}^\perp)$ is identically distributed to $\mathbf{k}_j'^\top + u_j\mathbf{a}^\perp + \mathbf{m}_j^\top\mathbf{K}''$, since $\mathbf{m}_j^\top\mathbf{u} \in \mathbb{Z}_q$ is masked by fresh randomness $u_j \leftarrow_{\mathrm{R}} \mathbb{Z}_q$.
- The output of the i^*-th $\mathcal{O}$ query on $\mathbf{m}$ leaks $(1, \mathbf{m}^\top)\begin{pmatrix} u_{i^*} \\ \mathbf{u} \end{pmatrix}$, since $(1, \mathbf{m}^\top)\binom{\mathbf{k}_{i^*}^\top}{\mathbf{K}'} = (1, \mathbf{m}^\top)\binom{\mathbf{k}_{i^*}'^\top}{\mathbf{K}''} + (1, \mathbf{m}^\top)\binom{u_{i^*}}{\mathbf{u}} \cdot \mathbf{a}^\perp$.

To compute $(i^*, \mathbf{m}^*, \mathbf{z})$ such that $\mathbf{z}^\top = (1, \mathbf{m}^{*\top})\begin{pmatrix} \mathbf{k}_{i^*}^\top \\ \mathbf{K}' \end{pmatrix} = (1, \mathbf{m}^{*\top})\binom{\mathbf{k}_{i^*}'^\top}{\mathbf{K}''} + (1, \mathbf{m}^{*\top})\binom{u_{i^*}}{\mathbf{u}} \cdot \mathbf{a}^\perp$ holds, $\mathcal{A}$ has to compute $(1, \mathbf{m}^{*\top})\begin{pmatrix} u_{i^*} \\ \mathbf{u} \end{pmatrix}$. Given $(1, \mathbf{m}^\top)\begin{pmatrix} u_{i^*} \\ \mathbf{u} \end{pmatrix}$, for any adaptively chosen $\mathbf{m}^* \neq \mathbf{m}$, we have that $(1, \mathbf{m}^{*\top})\begin{pmatrix} u_{i^*} \\ \mathbf{u} \end{pmatrix}$ is uniformly random over $\mathbb{Z}_q$ from the adversary's view. This shows equation (9). □

Theorem 5. *Under the $\mathcal{D}_k$-*KerMDH *Assumption in $\mathbb{G}_2$,* TTSPS$_{\mathsf{ot}}$ *from Figure 7 is a* TT-CMA*-secure two-tier signature scheme.*

Proof. Perfect correctness is straight-forward to verify. We proceed to establish TT-CMA-security based on the $\mathcal{D}_k$-KerMDH assumption. We will show that for all adversaries $\mathcal{A}$, there exists an adversary $\mathcal{B}$ with $\mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B})$ and

$$\mathbf{Adv}^{\text{tt-cma}}_{\mathsf{TTSPS_{ot}}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}) + 1/q. \tag{10}$$

Adversary $\mathcal{B}(\mathcal{PG}, [\mathbf{A}]_2 \in \mathbb{G}_2^{(k+1)\times k})$ generates $\mathsf{pk} = ([\mathbf{C}']_2, [\mathbf{A}]_2)$ as in the real scheme by picking $\mathbf{K}' \in \mathbb{Z}_q^{n\times(k+1)}$ and computing $[\mathbf{C}']_2 := [\mathbf{K}'\mathbf{A}]_2$. Next, $\mathcal{B}$ runs $\mathcal{A}$ on pk and simulates TTSignO as in the real scheme:

- TTSignO$([\mathbf{m}]_1)$: $i = i + 1$, picks $\mathbf{k}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}$, computes $\mathsf{opk}_i := [\mathbf{k}_i^\top\mathbf{A}]_2$, computes $\sigma := [(1, \mathbf{m}^\top) \cdot \binom{\mathbf{k}_i^\top}{\mathbf{K}'}]_1$, adds $(i, [\mathbf{m}]_1, \sigma)$ to $\mathcal{Q}_{\mathrm{msg}}$ and returns σ.

With probability $\mathbf{Adv}^{\text{tt-cma}}_{\mathsf{TTSPS_{ot}}}(\mathcal{A})$, $\mathcal{B}$ obtains $(i^*, [\mathbf{m}^*]_1, \sigma^*)$ such that there exists $(i^*, [\mathbf{m}]_1, \sigma) \in \mathcal{Q}_{\mathrm{msg}}$ and $\mathbf{m}^* \neq \mathbf{m}$ and $e(\sigma^*, [\mathbf{A}]_2) = e([1, \mathbf{m}^{*\top}]_1, [\mathbf{K}^*\mathbf{A}]_2)$, where $\mathbf{K}^* := \binom{\mathbf{k}_{i^*}^\top}{\mathbf{K}'}$. Then $\mathcal{B}$ returns $[\mathbf{s}]_1$ computed as

$$[\mathbf{s}]_1 = \sigma^* - [1, \mathbf{m}^{*\top}]_1\mathbf{K}^*.$$

Clearly, $\mathbf{s} \cdot \mathbf{A} = \mathbf{0}$. The information-theoretic argument of Lemma 4 captures the fact that, for any $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$ and any adversary $\mathcal{A}$, given $(\mathbf{A}, \mathbf{K}'\mathbf{A})$ over $\mathbb{Z}_q$ and Q-many $(1, \mathbf{m}_i^\top)\binom{\mathbf{k}_i^\top}{\mathbf{K}'}$ for adversarial chosen $\mathbf{m}_i$ ($\mathbf{K}' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}, \mathbf{k}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}$), $\mathcal{A}$ can not come up with $(\mathbf{z}, \mathbf{m}^*)$ such that $\mathbf{z} - (1, \mathbf{m}^{*\top})\binom{\mathbf{k}_{i^*}^\top}{\mathbf{K}'} = 0$ ($i^* \in \{1, \ldots, Q\}$). Thus, $\Pr[\mathbf{s} = \mathbf{0}] \leq 1/q$ by Lemma 4. □

Transformation. Let TTS := (PGen, SGen, TTSign, TTVerify) be a two-tier signature scheme with message space over $\mathcal{M}_1$ and secondary public key space over $\mathcal{OPK}$. Let S := (Gen$'$, Gen$'$, Verify$'$) be an unbounded CMA-secure signature scheme with message space $\mathcal{M}_2 \times \mathcal{OPK}$. Our transformed signature scheme TS[S, TTS] with message space $\mathcal{M} = \mathcal{M}_1 \times \mathcal{M}_2$ is defined as in Figure 8.

```
$\underline{\mathsf{Gen}(\mathsf{par}):}$
$(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow_{\mathrm{R}} \mathsf{PGen}(\mathsf{par})$
$(\mathsf{pk}_2, \mathsf{sk}_2) \leftarrow_{\mathrm{R}} \mathsf{Gen}'(\mathsf{par})$
$\mathsf{pk} := (\mathsf{pk}_1, \mathsf{pk}_2)$; $\mathsf{sk} := (\mathsf{sk}_1, \mathsf{sk}_2)$
Return $(\mathsf{pk}, \mathsf{sk})$
```

```
$\underline{\mathsf{Sign}(\mathsf{sk}, (\mathbf{m}_1, \mathbf{m}_2)):}$
$(\mathsf{opk}, \mathsf{osk}) \leftarrow_{\mathrm{R}} \mathsf{SGen}(\mathsf{pk}, \mathsf{sk})$
$\sigma_1 \leftarrow_{\mathrm{R}} \mathsf{TTSign}(\mathsf{sk}_1, \mathsf{osk}, \mathbf{m}_1)$
$\sigma_2 \leftarrow_{\mathrm{R}} \mathsf{Sign}'(\mathsf{sk}_2, (\mathbf{m}_2, \mathsf{opk}))$
Return $(\mathsf{opk}, \sigma_1, \sigma_2)$
```

```
$\underline{\mathsf{Verify}(\mathsf{pk}, (\mathbf{m}_1, \mathbf{m}_2), \sigma):}$
Parse $\sigma = (\mathsf{opk}, \sigma_1, \sigma_2)$
Check:
$\mathsf{TTVerify}(\mathsf{pk}_1, \mathsf{opk}, \mathbf{m}_1, \sigma_1) = 1$
$\wedge \mathsf{Verify}'(\mathsf{pk}_2, (\mathbf{m}_2, \mathsf{opk}), \sigma_2) = 1$
```

Fig. 8. Generic construction of a signature scheme $\mathsf{TS}[\mathsf{S}, \mathsf{TTS}]$ with message space $\mathcal{M} = \mathcal{M}_1 \times \mathcal{M}_2$ from a two-tier signature scheme with message space $\mathcal{M}_1$ and secondary public key space $\mathcal{OPK}$. and signature scheme S with message space $\mathcal{M}_2 \times \mathcal{OPK}$.

Theorem 6. *Under the* $\mathsf{TT\text{-}CMA}$*-security of* TTS *and unbounded* CMA*-security of* S*,* $\mathsf{TS}[\mathsf{S}, \mathsf{TTS}]$ *is an unbounded* CMA*-secure signature scheme.*

Perfect correctness is implied by perfect correctness of TTS and S. We will show that for any adversary $\mathcal{A}$, there exist adversaries $\mathcal{B}_1$ and $\mathcal{B}_2$ with $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B}_2)$ and

$$\mathbf{Adv}^{\mathrm{cma}}_{\mathsf{TS}[\mathsf{S},\mathsf{TTS}]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{tt\text{-}cma}}_{\mathsf{TTS}}(\mathcal{B}_1) + \mathbf{Adv}^{\mathrm{cma}}_{\mathsf{S}}(\mathcal{B}_2). \tag{11}$$

Since the proof is similar to that for the EGM framework [23, 2], we only sketch the proof. Let $(\mathbf{m}_1^*, \mathbf{m}_2^*, \sigma^* = (\mathsf{opk}^*, \sigma_1^*, \sigma_2^*))$ be a forgery from $\mathcal{A}$. $\mathcal{A}$ can make at most Q signing queries to SignO for $\mathsf{TS}[\mathsf{S}, \mathsf{TTS}]$ and we denote the i-th query by $(\mathbf{m}_1^{(i)}, \mathbf{m}_2^{(i)})$ and its answer as $(\mathsf{opk}^{(i)}, \sigma_1^{(i)}, \sigma_2^{(i)})$. There are two complementary cases:

- There exists an $i \in \{1, \ldots, Q\}$ such that $(\mathbf{m}_2^*, \mathsf{opk}^*) = (\mathbf{m}_2^{(i)}, \mathsf{opk}^{(i)})$. As $(\mathbf{m}_1^*, \mathbf{m}_2^*) \notin \mathcal{Q}_{\mathrm{msg}}$, $\mathbf{m}_1^* \neq \mathbf{m}_1^{(i)}$. Thus, $(i, \mathbf{m}_1^*, \sigma_1^*)$ is a valid forgery that breaks the $\mathsf{TT\text{-}CMA}$-security of TTS.
- $(\mathbf{m}_2^*, \mathsf{opk}^*) \neq (\mathbf{m}_2^{(i)}, \mathsf{opk}^{(i)})$ for all $i \in \{1, \ldots, Q\}$. Clearly, $((\mathbf{m}_2^*, \mathsf{opk}^*), \sigma_2^*)$ is a valid forgery that breaks the unbounded CMA-security of S.

6.2 Instantiation

Combining $\mathsf{TTSPS}_{\mathsf{ot}}$ from Figure 7 and $\mathsf{SPS}_{\mathsf{full}}$ from Figure 3 we obtain an UFCMA-secure signature scheme $\mathsf{BSPS}_{\mathsf{full}}$, see Figure 9. One can verify that it is structure preserving with bilateral message space $\mathcal{M} = \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$ and the following parameters:

$$|\mathsf{pk}| = (n_1 + n_2)k + 3(k+1)k + 2\mathsf{RE}(\mathcal{D}_k), \qquad |\sigma| = (k+2, 4k+3), \qquad \#\text{equations} = 3k+1.$$

Notation (x, y) means x elements in $\mathbb{G}_1$ and y elements in $\mathbb{G}_2$. We note that the representation of $\mathbb{G}_2$ elements is longer than that of $\mathbb{G}_1$ elements. To simplify the efficiency comparison, one can use $\mathsf{TTSPS}_{\mathsf{ot}}$ to sign $[\mathbf{m}_2]_2$ and $\mathsf{SPS}_{\mathsf{full}}$ to sign $([\mathbf{m}_1]_1, [\mathbf{z}]_1)$, which gives us a scheme with $|\sigma| = (4k+3, k+2)$. Under the SXDH assumption, our scheme achieves $(|\mathsf{pk}|, |\sigma|, \#\text{equations}) = (n_1 + n_2 + 8, (7, 3), 4)$. Compared with $(n_1 + n_2 + 22, (8, 6), 5)$ of [2], we obtain better efficiency under standard assumptions.

Acknowledgments. We thank Olivier Blazy and Georg Fuchsbauer for helpful discussions.

References

[1] M. Abdalla, F. Benhamouda, and D. Pointcheval. Disjunctions for hash proof systems: New constructions and applications. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 69–100. Springer, Apr. 2015.

```
$\underline{\mathsf{Gen}(\mathsf{par})\text{:}}$
// Generate the primary key pair of $\mathsf{TTSPS_{ot}}$
$\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k; \mathbf{X} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n_1 \times (k+1)}$
$\mathbf{Z} = \mathbf{X}\mathbf{A} \in \mathbb{Z}_q^{n_1 \times k}$
// Generate the key pair of $\mathsf{SPS_{full}}$
$\mathbf{A}', \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k; \mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(1+n_2+k) \times (k+1)}$
$\mathbf{K}_0, \mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1) \times (k+1)}$
$\mathbf{C} := \mathbf{K}\mathbf{A}' \in \mathbb{Z}_q^{(1+n_2+k) \times k}$
$(\mathbf{C}_0, \mathbf{C}_1) := (\mathbf{K}_0\mathbf{A}', \mathbf{K}_1\mathbf{A}') \in (\mathbb{Z}_q^{(k+1) \times k})^2$
$(\mathbf{P}_0, \mathbf{P}_1) := (\mathbf{B}^\top\mathbf{K}_0, \mathbf{B}^\top\mathbf{K}_1) \in (\mathbb{Z}_q^{k \times (k+1)})^2$
$\mathsf{sk} := (\mathbf{X}, \mathbf{K}, [\mathbf{P}_0]_2, [\mathbf{P}_1]_2, [\mathbf{B}]_2)$
$\mathsf{pk} := ([\mathbf{Z}]_2, [\mathbf{C}_0]_1, [\mathbf{C}_1]_1, [\mathbf{C}]_1, [\mathbf{A}]_2, [\mathbf{A}']_1)$
Return $(\mathsf{pk}, \mathsf{sk})$

$\underline{\mathsf{Sign}(\mathsf{sk}, ([\mathbf{m}_1]_1, [\mathbf{m}_2]_2))\text{:}}$
// Use $\mathsf{TTSPS_{ot}}$ to sign $[\mathbf{m}_1]_1$
$\mathbf{x} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}; \mathbf{z} := \mathbf{x}^\top\mathbf{A} \in \mathbb{Z}_q^{1 \times k}$
$\sigma_1 := [\mathbf{x}^\top + \mathbf{m}_1^\top\mathbf{X}]_1 \in \mathbb{G}_1^{1 \times (k+1)}$
// Use $\mathsf{SPS_{full}}$ to sign $([\mathbf{m}_2]_2, [\mathbf{z}]_2)$
$\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k; \tau \leftarrow_{\mathrm{R}} \mathbb{Z}_q;$
$\sigma_2 := \big[(1, \mathbf{m}_2^\top, \mathbf{z})\mathbf{K} + \mathbf{r}^\top(\mathbf{P}_0 + \tau\mathbf{P}_1)\big]_2 \in \mathbb{G}_2^{1 \times (k+1)}$
$\sigma_3 := [\mathbf{B}\mathbf{r}]_2 \in \mathbb{G}_2^{k+1}$
$\sigma_4 := [\tau\mathbf{B}\mathbf{r}]_2 \in \mathbb{G}_2^{k+1}$
$\sigma_5 := [\tau]_1 \in \mathbb{G}_1$
Return $([\mathbf{z}]_2, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$

$\underline{\mathsf{Verify}(\mathsf{pk}, ([\mathbf{m}_1]_1, [\mathbf{m}_2]_2), \sigma)\text{:}}$
Parse $\sigma = ([\mathbf{z}]_2, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$
Check:
$e(\sigma_1, [\mathbf{A}]_2) = e([1, \mathbf{m}_1^\top]_1, \left[\begin{smallmatrix}\mathbf{z}\\ \mathbf{Z}\end{smallmatrix}\right]_2)$
$\wedge e([\mathbf{A}']_1^\top, \sigma_2^\top) = e([\mathbf{C}]_1^\top, \left[\begin{smallmatrix}1\\ \mathbf{m}_2\\ \mathbf{z}^\top\end{smallmatrix}\right]_2) \cdot e([\mathbf{C}_0]_1^\top, \sigma_3) \cdot e([\mathbf{C}_1]_1^\top, \sigma_4)$
$\wedge e(\sigma_5, \sigma_3) = e([1]_1, \sigma_4)$
```

Fig. 9. Structure-preserving signature $\mathsf{BSPS_{full}}$ with bilateral message spaces $\mathcal{M} = \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$.

[2] M. Abe, M. Chase, B. David, M. Kohlweiss, R. Nishimaki, and M. Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In X. Wang and K. Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 4–24. Springer, Dec. 2012.

[3] M. Abe, B. David, M. Kohlweiss, R. Nishimaki, and M. Ohkubo. Tagged one-time signatures: Tight security and optimal tag size. In K. Kurosawa and G. Hanaoka, editors, *PKC 2013*, volume 7778 of *LNCS*, pages 312–331. Springer, Feb. / Mar. 2013.

[4] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-preserving signatures and commitments to group elements. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236. Springer, Aug. 2010.

[5] M. Abe, J. Groth, K. Haralambiev, and M. Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In P. Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 649–666. Springer, Aug. 2011.

[6] M. Abe, J. Groth, and M. Ohkubo. Separating short structure-preserving signatures from non-interactive assumptions. In D. H. Lee and X. Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 628–646. Springer, Dec. 2011.

[7] M. Abe, J. Groth, M. Ohkubo, and M. Tibouchi. Structure-preserving signatures from type II pairings. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 390–407. Springer, Aug. 2014.

[8] M. Abe, J. Groth, M. Ohkubo, and M. Tibouchi. Unified, minimal and selectively randomizable structure-preserving signatures. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 688–712. Springer, Feb. 2014.

[9] N. Attrapadung, B. Libert, and T. Peters. Efficient completely context-hiding quotable and linearly homomorphic signatures. In K. Kurosawa and G. Hanaoka, editors, *PKC 2013*, volume 7778 of *LNCS*, pages 386–404. Springer, Feb. / Mar. 2013.

[10] G. Barthe, E. Fagerholm, D. Fiore, A. Scedrov, B. Schmidt, and M. Tibouchi. Strongly-optimal structure preserving signatures from type II pairings: Synthesis and lower bounds. In J. Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 355–376. Springer, Mar. / Apr. 2015.

[11] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham. Randomizable proofs and delegatable anonymous credentials. In S. Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 108–125. Springer, Aug. 2009.

[12] M. Bellare and S. Shoup. Two-tier signatures, strongly unforgeable signatures, and Fiat-Shamir without random oracles. In T. Okamoto and X. Wang, editors, *PKC 2007*, volume 4450 of *LNCS*, pages 201–216. Springer, Apr. 2007.

[13] O. Blazy, S. Canard, G. Fuchsbauer, A. Gouget, H. Sibert, and J. Traoré. Achieving optimal anonymity in transferable e-cash with a judge. In A. Nitaj and D. Pointcheval, editors, *AFRICACRYPT 11*, volume 6737 of *LNCS*, pages 206–223. Springer, July 2011.

[14] O. Blazy, E. Kiltz, and J. Pan. (Hierarchical) identity-based encryption from affine message authentication. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 408–425. Springer, Aug. 2014.

[15] D. Boneh, D. Freeman, J. Katz, and B. Waters. Signing a linear subspace: Signature schemes for network coding. In S. Jarecki and G. Tsudik, editors, *PKC 2009*, volume 5443 of *LNCS*, pages 68–87. Springer, Mar. 2009.

[16] D. Catalano, A. Marcedone, and O. Puglisi. Authenticating computation on groups: New homomorphic primitives and applications. In P. Sarkar and T. Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of *LNCS*, pages 193–212. Springer, Dec. 2014.

[17] J. Cathalo, B. Libert, and M. Yung. Group encryption: Non-interactive realization in the standard model. In M. Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 179–196. Springer, Dec. 2009.

[18] M. Chase, M. Kohlweiss, A. Lysyanskaya, and S. Meiklejohn. Malleable proof systems and applications. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 281–300. Springer, Apr. 2012.

[19] J. Chen, R. Gay, and H. Wee. Improved dual system ABE in prime-order groups via predicate encodings. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 595–624. Springer, Apr. 2015.

[20] J. Chen, H. W. Lim, S. Ling, H. Wang, and H. Wee. Shorter IBE and signatures via asymmetric pairings. In M. Abdalla and T. Lange, editors, *PAIRING 2012*, volume 7708 of *LNCS*, pages 122–140. Springer, May 2013.

[21] Y. Desmedt. Computer security by redefining what a computer is. In New Security Paradigms Workshop (NSPW), 1993.

[22] 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, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Aug. 2013.

[23] S. Even, O. Goldreich, and S. Micali. On-line/off-line digital signatures. *Journal of Cryptology*, 9(1):35–67, 1996.

[24] G. Fuchsbauer. Commuting signatures and verifiable encryption. In K. G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 224–245. Springer, May 2011.

[25] G. Fuchsbauer and D. Vergnaud. Fair blind signatures without random oracles. In D. J. Bernstein and T. Lange, editors, *AFRICACRYPT 10*, volume 6055 of *LNCS*, pages 16–33. Springer, May 2010.

[26] M. Green and S. Hohenberger. Universally composable adaptive oblivious transfer. In J. Pieprzyk, editor, *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 179–197. Springer, Dec. 2008.

[27] J. Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In X. Lai and K. Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 444–459. Springer, Dec. 2006.

[28] J. Groth. Fully anonymous group signatures without random oracles. In K. Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 164–180. Springer, Dec. 2007.

[29] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, Apr. 2008.

[30] D. Hofheinz and T. Jager. Tightly secure signatures and public-key encryption. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 590–607. Springer, Aug. 2012.

[31] D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. In A. Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 553–571. Springer, Aug. 2007.

[32] R. Johnson, D. Molnar, D. X. Song, and D. Wagner. Homomorphic signature schemes. In B. Preneel, editor, *CT-RSA 2002*, volume 2271 of *LNCS*, pages 244–262. Springer, Feb. 2002.

[33] C. S. Jutla and A. Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In K. Sako and P. Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 1–20. Springer, Dec. 2013.

[34] C. S. Jutla and A. Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 295–312. Springer, Aug. 2014.

[35] E. Kiltz and H. Wee. Quasi-adaptive NIZK for linear subspaces revisited. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128. Springer, Apr. 2015.

[36] A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In D. Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 455–479. Springer, Feb. 2010.

[37] B. Libert, T. Peters, M. Joye, and M. Yung. Linearly homomorphic structure-preserving signatures and their applications. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 289–307. Springer, Aug. 2013.

[38] B. Libert, T. Peters, M. Joye, and M. Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 514–532. Springer, May 2014.

[39] B. Libert, T. Peters, and M. Yung. Group signatures with almost-for-free revocation. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 571–589. Springer, Aug. 2012.

[40] B. Libert, T. Peters, and M. Yung. Short group signatures via structure-preserving signatures: Standard model security from simple assumptions. In *CRYPTO*, 2015.

[41] P. Morillo, C. Ràfols, and J. L. Villar. Matrix computational assumptions in multilinear groups. Cryptology ePrint Archive, Report 2015/353, 2015.

[42] B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In S. Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636. Springer, Aug. 2009.

[43] H. Wee. Dual system encryption via predicate encodings. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 616–637. Springer, Feb. 2014.

A Proof of Theorem 4

Our proof requires the Q-fold $\mathcal{D}_k$-MDDH problem, which is tightly related to the standard $\mathcal{D}_k$-MDDH problem by Lemma 1 in [22]. Let $Q \geq 1$. For $\mathbf{W} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k \times Q}, \mathbf{U} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1) \times Q}$, consider the Q-fold $\mathcal{D}_k$-MDDH problem which is distinguishing the distributions $([\mathbf{B}], [\mathbf{BW}])$ and $([\mathbf{B}], [\mathbf{U}])$ for $\mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$. That is, the Q-fold $\mathcal{D}_k$-MDDH problem contains Q independent instances of the $\mathcal{D}_k$-MDDH problem (with the same $\mathbf{B}$ but different $\mathbf{w}_i$). By the random self reducibility (Lemma 1 in [22]), the Q-fold $\mathcal{D}_k$-MDDH problem is tightly related to the standard $\mathcal{D}_k$-MDDH problem. For completeness, we recall Lemma 1 in [22] as follows:

Lemma 5 (Random self reducibility [22]). *For any matrix distribution $\mathcal{D}_k$, $\mathcal{D}_k$-MDDH is random self-reducible. In particular, for any $Q \geq 1$,*

$$\mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) + \frac{1}{q-1} \geq \mathbf{Adv}^{Q\text{-}\mathsf{MDDH}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}') := \Pr[\mathcal{D}'(\mathcal{G}, [\mathbf{B}], [\mathbf{BW}]) \Rightarrow 1] - \Pr[\mathcal{D}'(\mathcal{G}, [\mathbf{B}], [\mathbf{U}]) \Rightarrow 1],$$

with $\mathcal{G} \leftarrow \mathsf{GGen}(1^\lambda)$, $\mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k, \mathbf{W} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k \times Q}, \mathbf{U} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1) \times Q}$.

Proof (of Theorem 4). Perfect correctness and the structure-preserving property are straight-forward. We proceed to establish RMA-security. We will show that for any adversary $\mathcal{A}$ that makes at most Q random message signing queries, there exists adversaries $\mathcal{B}_0, \mathcal{B}_1$ with $\mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B}_0) \approx \mathbf{T}(\mathcal{B}_1)$ and

$$\mathbf{Adv}^{\mathrm{rma}}_{\mathsf{rSPS}_{\mathsf{full}}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_0) + O(Q^2) \cdot \mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) + O(Q^2)/q. \tag{12}$$

We proceed via a series of games and we use $\mathbf{Adv}_i$ to denote the advantage of $\mathcal{A}$ in Game i.

Game 0. This is the RMA-experiment from Definition 6.

Game 1. Switch Verify to Verify^* for the forgery:

```
$\mathsf{Verify}^*(\mathsf{pk}, [\mathbf{m}]_1, \sigma)$:
Parse $\sigma = (\sigma_1, \sigma_2, \sigma_3 = [\tau]_2)$
Parse $[\mathbf{m}]_1 = ([\mathbf{s}]_1, [\mathbf{t}]_1)$
Check: $e(\sigma_1, [1]_2) = e([(1, \mathbf{m}^\top)\mathbf{K}]_1, [1]_2) \cdot e([\mathbf{t}^\top]_1, [\mathbf{K}_0 + \tau\mathbf{K}_1]_2)$
$\wedge \quad e(\sigma_2, [1]_2) = e([\mathbf{t}^\top]_1, [\tau]_2)$
```

Suppose $e(\sigma_2, [1]_2) = e([\mathbf{t}^\top]_1, [\tau]_2)$. We note that

$$\begin{aligned}
& e(\sigma_1, [\mathbf{A}]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{C}]_2) \cdot e([\mathbf{t}^\top]_1, [\mathbf{C}_0]_2) \cdot e(\sigma_2, [\mathbf{C}_1]_2) \\
\Longleftrightarrow\; & e(\sigma_1, [\mathbf{A}]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{KA}]_2) \cdot e([\mathbf{t}^\top]_1, [\mathbf{K}_0\mathbf{A}]_2) \cdot e(\sigma_2, [\mathbf{K}_1\mathbf{A}]_2) \\
\Longleftarrow\; & e(\sigma_1, [1]_2) = e([(1, \mathbf{m}^\top)]_1, [\mathbf{K}]_2) \cdot e([\mathbf{t}^\top]_1, [\mathbf{K}_0]_2) \cdot e(\sigma_2, [\mathbf{K}_1]_2) \\
\Longleftrightarrow\; & e(\sigma_1, [1]_2) = e([(1, \mathbf{m}^\top)\mathbf{K}]_1, [1]_2) \cdot e([\mathbf{t}^\top]_1, [\mathbf{K}_0 + \tau\mathbf{K}_1]_2)
\end{aligned}$$

By the same argument in Game 3 of Theorem 2, if any $([\mathbf{m}]_1, \sigma)$ passes Verify but not Verify^*, then the value

$$\mathbf{x}^\top := \sigma_1 - ([(1, \mathbf{m}^\top)\mathbf{K}]_1 + [\mathbf{t}^\top\mathbf{K}_0]_1 + \sigma_2\mathbf{K}_1) \in \mathbb{G}_1^{1 \times (k+1)}$$

is a non-zero vector in the kernel of $\mathbf{A}$, which is hard to be computed under the $\mathcal{D}_k$-KerMDH assumption in $\mathbb{G}_2$. We note that the vector $\mathbf{x}$ can be computed by $\mathcal{B}_0$, since $\mathcal{B}_0$ knows $\mathbf{K}, \mathbf{K}_0, \mathbf{K}_1$ over $\mathbb{Z}_q$ and $[\mathbf{m}]_1, , \sigma_1$ and σ_2 are from the forgery of $\mathcal{A}$. This means that

$$|\mathbf{Adv}_0 - \mathbf{Adv}_1| \leq \mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_0).$$

Game 2. Let $\tau_1, \ldots, \tau_Q$ denote the randomly chosen tags in the Q queries to $\mathsf{SignO}()$. We abort if $\tau_1, \ldots, \tau_Q$ are not all distinct.

$$\mathbf{Adv}_2 \geq \mathbf{Adv}_1 - Q^2/2q.$$

Game 3. We define $\tau_{Q+1} := \tau^*$. Now, pick $i^* \leftarrow_{\mathrm{R}} [Q+1]$ and abort if i^* is not the smallest index i for which $\tau^* = \tau_i$. In the rest of the proof, we focus on the case we do not abort, which means that $\tau^* = \tau_{i^*}$ and $\tau_1, \ldots, \tau_{i^*-1}$ are all different from τ^*. This means that given τ, SignO can check whether τ^* equals τ: for the rest $i^* - 1$ queries, answer NO, and starting from the i^*'th query, we know τ^*. It is easy to see that

$$\mathbf{Adv}_3 \geq \frac{1}{Q+1} \mathbf{Adv}_2.$$

Game 4. By choosing the matrix $\mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$ in the key generation, we switch SignO to SignO$'$ where

```
SignO'():
$\tau \leftarrow_{\mathrm{R}} \mathbb{Z}_q$
$\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k; \mathbf{t} := \mathbf{Br} \in \mathbb{Z}_q^{k+1}$
$\mathbf{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n'}; \mathbf{m} := (\mathbf{s}, \mathbf{t})$
$\sigma_1 := \left[(1, \mathbf{m}^\top)\mathbf{K} + \mathbf{t}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1)\right]_1$
$\sigma_2 := \left[\tau\mathbf{t}^\top\right]_1$
$\sigma_3 := [\tau]_2$
$\sigma := (\sigma_1, \sigma_2, \sigma_3) \in \mathbb{G}_1^{1\times(k+1)} \times \mathbb{G}_1^{1\times(k+1)} \times \mathbb{G}_2$
Return $([\mathbf{m}]_1, \sigma)$
```

The only difference between SignO and SignO$'$ is that we compute $\mathbf{t} = \mathbf{Br}$ instead of picking a random vector $\mathbf{t}$. It is easy to see that the difference is bounded by the $\mathcal{D}_k$-MDDH Assumption in $\mathbb{G}_1$.
Precisely, we construct an adversary $\mathcal{B}_1$ to break the Q-fold $\mathcal{D}_k$-MDDH Assumption if $\mathcal{A}$ can distinguish Game 0 and 1. Let $([\mathbf{B}]_1, [\mathbf{H}]_1)$ be the Q-fold $\mathcal{D}_k$-MDDH challenge. $\mathcal{B}_1$ picks $\mathbf{K}, \mathbf{K}_0$ and $\mathbf{K}_1$ over $\mathbb{Z}_q$ and runs $\mathsf{Gen}(\mathsf{par})$ honestly. On answering the i-th SignO$'$ query, $\mathcal{B}_1$ defines $[\mathbf{t}]_1 := [\mathbf{H}_i]_1$ and the rest is simulated by using the explicit expressions of $\tau, \mathbf{K}, \mathbf{K}_0$ and $\mathbf{K}_1$ over $\mathbb{Z}_q$.
One can see that if $[\mathbf{H}]_2 = [\mathbf{BW}]_2$ then the simulation is identical to Game 4; and, otherwise, the simulation is identical to Game 3. By Lemma 5, we can tightly bound $\mathbf{Adv}_3$ and $\mathbf{Adv}_4$

$$|\mathbf{Adv}_3 - \mathbf{Adv}_4| \leq \mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) + 1/(q-1).$$

Game 5. Switch SignO$'$ to SignO*, where

```
SignO*():                                                   // adds $\mu\mathbf{a}^\perp$ for $\tau \neq \tau^*$
$\tau \leftarrow_{\mathrm{R}} \mathbb{Z}_q; \mu \leftarrow_{\mathrm{R}} \mathbb{Z}_q;$
$\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k; \mathbf{t} = \mathbf{Br} \in \mathbb{Z}_q^{k+1}$
$\mathbf{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n'}; \mathbf{m} := (\mathbf{s}, \mathbf{t})$
if $\tau = \tau^*$ then $\mu := 0$
$\sigma_1 := \left[(1, \mathbf{m}^\top)\mathbf{K} + \mu\mathbf{a}^\perp + \mathbf{t}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1)\right]_1$
$\sigma_2 := \left[\tau\mathbf{t}^\top\right]_1$
$\sigma_3 := [\tau]_2$
$\sigma := (\sigma_1, \sigma_2, \sigma_3) \in \mathbb{G}_1^{1\times(k+1)} \times \mathbb{G}_1^{1\times(k+1)} \times \mathbb{G}_2$
Return $([\mathbf{m}]_1, \sigma)$
```

We will use Lemma 3 to show that

$$|\mathbf{Adv}_4 - \mathbf{Adv}_5| \leq 2Q\mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_2) + Q/q.$$

Basically, in the reduction $\mathcal{B}_2$ picks $\mathbf{K}$ itself and uses $\mathcal{O}_b$ to simulate either SignO$'$ or SignO* and $\mathcal{O}^*$ to simulate Verify*:

- For the i'th signing query where $i \neq i^*$,we query $\mathcal{O}_b$ at $\tau \leftarrow_{\mathrm{R}} \mathbb{Z}_q$ to obtain

$$(\sigma_1' = \Big[b\mu\mathbf{a}^\perp + \mathbf{r}^\top\mathbf{B}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1)\Big]_1, \quad [\mathbf{t}^\top]_1 = [\mathbf{r}^\top\mathbf{B}^\top]_1),$$

  We pick $\mathbf{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n'}$, define $\mathbf{m} = (\mathbf{s}, \mathbf{t})$ and return

$$([\mathbf{m}]_1, (\sigma_1 := [(1, \mathbf{m}^\top)\mathbf{K}]_1 \cdot \sigma_1',\ \sigma_2 := \tau[\mathbf{t}^\top]_1,\ \sigma_3 := [\tau]_2))$$

- For the i^*'th signing query where $i^* \leq Q$, $\mathcal{B}_2$ picks $\tau \leftarrow_{\mathrm{R}} \mathbb{Z}_q$, $\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k$ and computes $[\mathbf{t}]_1 := [\mathbf{Br}]_1$. With the knowledge of $\mathbf{r}, \mathbf{K}, [\mathbf{P}_0]_1 := [\mathbf{B}^\top\mathbf{K}_0]_1, [\mathbf{P}_1]_1 := [\mathbf{B}^\top\mathbf{K}_1]_1, [\mathbf{B}]_1$, $\mathcal{B}_2$ can compute $(\sigma_1, \sigma_2, \sigma_3)$ honestly:

$$\sigma_1 := [(1, \mathbf{m}^\top)\mathbf{K} + \mathbf{r}^\top(\mathbf{P}_0 + \mathbf{P}_1)]_1$$
$$\sigma_2 := [\tau\mathbf{r}^\top\mathbf{B}^\top]_1, \sigma_3 := [\tau]_2$$

- For Verify^*, we will query $\mathcal{O}^*$ on $[\tau^*]_2$ to get $[\mathbf{K}_0 + \tau^*\mathbf{K}_1]_2$. The latter is sufficient to simulate the Verify^* query by computing $e([\mathbf{t}^{*\top}]_1, [\mathbf{K}_0 + \tau^*\mathbf{K}_1]_2)$.

This allows us to then build a distinguisher for for Lemma 3, since $\mathcal{B}_2$ simulates Game 5 if $b = 1$, or Game 4 if $b = 0$.

Game 6. Switch $\mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times(k+1)}$ in Gen to $\mathbf{K} := \mathbf{K}' + \mathbf{ua}^\perp$, where $\mathbf{K}' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(n+1)\times(k+1)}$, $\mathbf{u} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n+1}$. Since $\mathbf{ua}^\perp$ is masked by a uniform matrix $\mathbf{K}'$, $\mathbf{K}$ in Game 6 is still uniformly random and thus Game 5 and 6 are identical. We have

$$\mathbf{Adv}_6 = \mathbf{Adv}_5.$$

To conclude the proof, we bound the adversarial advantage in Game 6 via an information-theoretic argument. We first consider the information about $\mathbf{u}$ leaked from pk and signing queries:

- $\mathbf{C} = (\mathbf{K}' + \mathbf{ua}^\perp)\mathbf{A} = \mathbf{K}'\mathbf{A}$ completely hides $\mathbf{u}$;
- the output of SignO^* on $(\mathbf{m}, \tau)$ for $\tau \neq \tau^*$ completely hides $\mathbf{u}$, since $(1, \mathbf{m}^\top)(\mathbf{K}' + \mathbf{ua}^\perp) + \mu\mathbf{a}^\perp$ is identically distributed to $(1, \mathbf{m}^\top)\mathbf{K}' + \mu\mathbf{a}^\perp$ (namely, $(1, \mathbf{m}^\top)\mathbf{u}$ is masked by $\mu \leftarrow_{\mathrm{R}} \mathbb{Z}_q$).
- the output of SignO^* on τ^* leaks $(1, \mathbf{m}^\top)(\mathbf{K}' + \mathbf{ua}^\perp)$, which is captured by $(1, \mathbf{m}^\top)\mathbf{u}$;

To convince Verify^* to accept a signature σ^* on $\mathbf{m}^*$, the adversary must correctly compute

$$(1, \mathbf{m}^{*\top})(\mathbf{K}' + \mathbf{ua}^\perp)$$

and thus $(1, \mathbf{m}^{*\top})\mathbf{u} \in \mathbb{Z}_q$. Given $(1, \mathbf{m}^\top)\mathbf{u}$, for any adaptively chosen $\mathbf{m}^* \neq \mathbf{m}$, we have that $(1, \mathbf{m}^{*\top})\mathbf{u}$ is uniformly random over $\mathbb{Z}_q$ from the adversary's view-point. Therefore, $\mathbf{Adv}_6 \leq 1/q$. □