Quasi-Adaptive NIZK for Linear Subspaces Revisited

Eike Kiltz* and Hoeteck Wee**

[1] Ruhr-Universität Bochum
[2] ENS, Paris

Abstract. Non-interactive zero-knowledge (NIZK) proofs for algebraic relations in a group, such as the Groth-Sahai proofs, are an extremely powerful tool in pairing-based cryptography. A series of recent works focused on obtaining very efficient NIZK proofs for linear spaces in a weaker quasi-adaptive model. We revisit recent quasi-adaptive NIZK constructions, providing clean, simple, and improved constructions via a conceptually different approach inspired by recent developments in identity-based encryption. We then extend our techniques also to linearly homomorphic structure-preserving signatures, an object both of independent interest and with many applications.

1 Introduction

Non-interactive zero-knowledge (NIZK) proofs for efficiently proving algebraic relations in a group [38, 37, 35, 14] have had a profound impact on pairing-based cryptography, notably in (i) improving the concrete efficiency of non-interactive cryptography schemes like group signatures [36], (ii) realizing stronger security guarantees in applications like anonymous credentials [10, 9, 33], and (iii) minimizing interaction in secure computation and two-party protocols [44, 31].

A recent fruitful line of works has focused in obtaining very efficient NIZK proofs for proving membership in a linear subspace over a group, which is an important subset of the algebraic relations supported by the Groth-Sahai NIZK [38]. For linear subspaces, the Groth-Sahai proofs were linear in the dimensions of the (sub)space. The first substantial improvement was obtained by Jutla and Roy [42] in a weaker *quasi-adaptive* model, where the CRS may depend on the linear subspace, and the soundness guarantee is computational but adaptive. In addition, they used quasi-adaptive NIZK (QANIZK) for linear subspaces to obtain improved KDM-CCA2-secure encryption as well as CCA2-secure IBE scheme with short, publicly verifiable ciphertexts [18, 19]. Further efficiency improvements were subsequently obtained in [48, 43, 1], leading to constant-size proofs, independent of the dimensions of space and subspace; several of these constructions also realized stronger notions of soundness like one-time simulation soundness and unbounded simulation soundness [51, 27], which in turn enable new applications.

1.1 Our Results and Techniques: QANIZK

We present clean, simple, and improved constructions of QANIZK protocols via a conceptually novel approach. 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 of the

* 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, ANR-14-CE28-0003 (Project EnBid) and ERC Project CryptoCloud (FP7/2007-2013 Grant Agreement no. 339563).

previous constructions. Figure 1 summarizes the efficiency of our constructions. Like the earliest Jutla-Roy scheme [42], our schemes are fully explicit and simple to describe: the prover and verifier carry out simple matrix-vector products in the exponent, and both correctness and zero-knowledge follow readily from one simple equation. Furthermore, our schemes have a natural derivation from a symmetric-key setting, and the derivation even extends to a modular and intuitive proof of security. Finally, in all but the settings with unbounded security, we obtain a qualitative improvement in the underlying assumptions from decisional to computational (search) assumptions; specifically, security relies on a natural computational analogue of the decisional k-Lin assumption.

Our constructions and techniques are inspired by recent developments in obtaining adaptively secure identity-based encryption schemes, notably the use of pairing groups to "compile" a symmetric-key primitive into an asymmetric-key primitive [13, 54, 23], and the dual system encryption methodology for achieving adaptive security against unbounded collusions [52, 46]. We then extend our techniques to linearly homomorphic structure-preserving signatures [47, 48], an object both of independent interest and with many applications.

Overview of our constructions. Fix a pairing group $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ with $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. We present a very simple non-interactive argument system for linear subspaces over $\mathbb{G}_1$ as defined by a matrix[3] $[\mathbf{M}]_1 := g_1^{\mathbf{M}} \in \mathbb{G}_1^{n \times t}$ $(n > t)$ and captured by the language:

$$\mathcal{L}_{\mathbf{M}} = \Big\{ [\mathbf{y}]_1 \in \mathbb{G}_1^n : \exists\, \mathbf{x} \in \mathbb{Z}_q^t \text{ s.t. } \mathbf{y} = \mathbf{M}\mathbf{x} \Big\}.$$

The starting point of our construction is a hash proof system [26] for the language, which is essentially a symmetric-key analogue of NIZK with a designated verifier. Namely, we pick a secret hash key $\mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n \times (k+1)}$ known to the verifier ($k \geq 1$ is a parameter of the security assumption) and publish the projection $[\mathbf{P}]_1 := [\mathbf{M}^\top \mathbf{K}]_1$ in the CRS. The proof is given by $[\pi]_1 := [\mathbf{x}^\top \mathbf{P}]_1$, and verification works by checking whether $\pi \stackrel{?}{=} \mathbf{y}^\top \mathbf{K}$. Completeness and perfect zero-knowledge follow readily from the fact that for all $\mathbf{y} = \mathbf{M}\mathbf{x}$ and $\mathbf{P} = \mathbf{M}^\top \mathbf{K}$:

$$\mathbf{x}^\top \mathbf{P} = \mathbf{x}^\top (\mathbf{M}^\top \mathbf{K}) = \mathbf{y}^\top \mathbf{K}.$$

Next, observe that if $\mathbf{y}$ is outside the span of $\mathbf{M}$, then $\mathbf{y}^\top \mathbf{K}$ is completely random given $\mathbf{M}^\top \mathbf{K}$; this is the case even if such a $\mathbf{y}$ is adaptively chosen after seeing $\mathbf{M}^\top \mathbf{K}$. Thus, the construction achieves statistical adaptive soundness: namely, a computationally unbounded cheating prover, upon seeing $\mathbf{P}$, still cannot produce a vector outside $\mathcal{L}_{\mathbf{M}}$ along with an accepting proof.

To achieve public verifiability, we carry out the hash proof system in $\mathbb{G}_1$ and publish a "partial commitment" to $\mathbf{K}$ in $\mathbb{G}_2$ as given by $[\mathbf{A}]_2, [\mathbf{K}\mathbf{A}]_2$, where the choice of $\mathbf{A} \in \mathbb{Z}_q^{(k+1) \times k}$ is defined by the security assumption. Instead of checking whether $\pi \stackrel{?}{=} \mathbf{y}^\top \mathbf{K}$ as before, anyone can now publicly check whether $\pi \mathbf{A} \stackrel{?}{=} \mathbf{y}^\top \mathbf{K}\mathbf{A}$ via a pairing. As $[\mathbf{A}]_2, [\mathbf{K}\mathbf{A}]_2$ leaks additional information about the secret hash key $\mathbf{K}$, we can only prove computational adaptive soundness. In particular, we rely on the $\mathcal{D}_k$-KerMDH Assumption [49], 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 [30], a

[3] We use implicit representation notation for group elements, as explained in Section 2.1.

generalization of the k-Lin Assumption.[4] Therefore, for any $([\mathbf{y}]_1, [\pi]_1)$ produced by an efficient adversary,

$$\pi\mathbf{A} = \mathbf{y}^\top\mathbf{K}\mathbf{A} \Longrightarrow (\pi - \mathbf{y}^\top\mathbf{K})\mathbf{A} = \mathbf{0} \overset{\text{using assumption}}{\Longrightarrow} \pi - \mathbf{y}^\top\mathbf{K} = \mathbf{0} \Longrightarrow \pi = \mathbf{y}^\top\mathbf{K},$$

upon which we are back in the symmetric-key setting, with a little more work to account for the leakage from $\mathbf{KA}$. Moreover, adaptive security in the symmetric-key setting (which is easy to analyze via a purely information-theoretic argument) carries over to adaptive security in the public-key setting.

Two simple extensions. We extend this simple construction in two simple ways:

- First, we show that we can use $\mathbf{A}$ with the bottom row deleted, which saves one element to obtain proofs of size k, albeit at the cost of a more intricate security reduction and a restriction to witness-sampleable (WS) distributions for $[\mathbf{M}]_1$ [42]. The latter means that we are given an explicit description of $\mathbf{M}$ in the security reduction, which we need to program the CRS as with prior works [43, 1] that achieve the same proof size. In the case $k = 1$, the proof consists of 1 element and the CRS only contains $n + t$ group elements, which seems optimal.
- Second, we show how to achieve one-time simulation soundness, by replacing $\mathbf{K}$ with 2-wise independent hash function $\mathbf{K}_0 + \tau\mathbf{K}_1$ where τ is a tag, and we publish $[\mathbf{A}]_2, [\mathbf{K}_0\mathbf{A}]_2, [\mathbf{K}_1\mathbf{A}]_2$ for public verification. A single simulated proof reveals only an evaluation of the hash function at a single point, while its evaluation at every other point remains hidden, upon which we are back in the setting of standard adaptive soundness.

Unbounded simulation-soundness. To achieve unbounded simulation-soundness, we move from a 2-wise independent hash function to an affine pseudo-random MAC (or, a randomized PRF) [13, 29, 25], which guarantees pseudorandomness at a single point even upon giving out evaluations for polynomially many other points. Here, we require a decisional assumption over $\mathbb{G}_1$. Our construction may also be viewed as an instantiation of the dual system encryption methodology, whereas prior constructions in [47, 48] rely on the random partitioning technique in [53, 12]. This allows us to immediately bypass two of the main limitations of random partitioning: long public parameters and a polynomial-time but inefficient security reduction.

1.2 Extension: Linearly Homomorphic Structure Preserving Signatures

Linearly homomorphic signatures (LHS) [15, 28, 40] 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 derives 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. In recent years, LHS have drawn considerable attentions from the community with a wide range of constructions under different assumptions [34, 6, 17, 16, 20, 32, 7, 8]. Linearly homomorphic structure preserving signatures (LHSPS) [47] have the additional property that signatures and public keys are all elements of the groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$. This is a useful property when combined with other algebraic tools such as Groth-Sahai NIZK systems. Applications beyond the algebraic compatibility include IND-CCA1-secure encryption with publicly verifiable ciphertexts and verifiable computation for encrypted cloud

[4] That is, $\mathcal{D}_k$-MDDH $\Rightarrow$ $\mathcal{D}_k$-KerMDH; for the specific linear distribution $\mathcal{D}_k = \mathcal{L}_k$ we have k-Lin := $\mathcal{L}_k$-MDDH $\Rightarrow$ $\mathcal{L}_k$-KerMDH =: k-KerLin. We refer the reader to Section 2.2 for a more detailed treatment of the assumptions.

	Soundness	WS?	Assumption	Proof	CRS	#pairings
GS08 [38]	AS		2-Lin $(\mathbb{G}_2)$	$2n+3t$	6	$3n(t+3)$
LPJY14 [48]	AS		2-KerLin $(\mathbb{G}_2)$	3	$2n+3t+3$	$2n+4$
ABP14 [1]	AS		k-Lin $(\mathbb{G}_2)$	$k+1$	$kn+(k+1)t+k$	$kn+k+1$
Π_{as} (Fig 4)	AS		$\mathcal{D}_k$-KerMDH $(\mathbb{G}_2)$ ✓	$k+1$	$kn+(k+1)t+\mathsf{RE}(\mathbf{A})$	$kn+\mathsf{RE}(\mathbf{A})$ ✓
JR13 [42]	AS	yes	k-KerLin $(\mathbb{G}_2)$	$k(n-t)$	$2kt(n-t)+k+1$	$k(n-t)(t+2)$
JR14 [43]	AS	yes	k-Lin $(\mathbb{G}_2)$	k	$kn+kt+k^2$	$kn+k^2$
ABP14 [1]	AS	yes	k-Lin $(\mathbb{G}_2)$	k	$kn+kt+k$	$kn+k$
Π'_{as} (Fig 5)	AS	yes	$\mathcal{D}_k$-KerMDH $(\mathbb{G}_2)$ ✓	k	$kn+kt+\overline{\mathsf{RE}}(\overline{\mathbf{A}})$ ✓	$kn+\overline{\mathsf{RE}}(\overline{\mathbf{A}})$ ✓
ABP14 [1]	OTSS		k-Lin $(\mathbb{G}_2)$	$k+1$	$2kn+2(k+1)t+k$	$kn+k+1$
$\Pi_{\mathsf{ot\text{-}ss}}$ (Fig 6)	OTSS		$\mathcal{D}_k$-KerMDH $(\mathbb{G}_2)$ ✓	$k+1$	$2kn+2(k+1)t+\mathsf{RE}(\mathbf{A})$	$kn+\mathsf{RE}(\mathbf{A})$ ✓
ABP14 [1]	OTSS	yes	k-Lin $(\mathbb{G}_2)$	k	$2\lambda(kn+(k+1)t)+k$	$\lambda kn+k$
$\Pi'_{\mathsf{ot\text{-}ss}}$ (Fig 9)	OTSS	yes	$\mathcal{D}_k$-KerMDH $(\mathbb{G}_2)$ ✓	k	$2\lambda(kn+(k+1)t)+\overline{\mathsf{RE}}(\overline{\mathbf{A}})$ ✓	$\lambda kn+\overline{\mathsf{RE}}(\overline{\mathbf{A}})$ ✓
CCS09 [18]	USS		2-Lin $(\mathbb{G}_2,\mathbb{G}_2)$	$2n+6t+52$	18	$O(tn)$
LPJY14 [48]	USS	yes	2-Lin $(\mathbb{G}_1,\mathbb{G}_2)$	20	$2n+3t+3\lambda+10$	$2n+30$
Π_{uss} (Fig 7)	USS	yes	$\mathcal{D}_k$-MDDH $(\mathbb{G}_1,\mathbb{G}_2)$ ✓	$2k+2$ ✓	$kn+4(k+t+1)k+2\mathsf{RE}(\mathbf{A})$ ✓	$k(n+k+1)+\mathsf{RE}(\mathbf{A})$ ✓

Fig. 1. QANIZK for linear subspaces of $\mathbb{Z}_q^n$ of dimension t and tag-space $\mathcal{T}=\{0,1\}^\lambda$. For the soundness column we use AS for adaptive soundness, OTSS for one-time simulation soundness, and USS for unbounded simulation soundness. WS stands for witness sampleability [42] and slightly restricts the class of languages, cf. Section 3.2. We omit the generators for the group when computing the CRS size. $\mathsf{RE}(\mathbf{A})$ and $\overline{\mathsf{RE}}(\overline{\mathbf{A}})$ depend on the assumption and denote the number of group elements needed to represent $[\mathbf{A}]$ and $[\overline{\mathbf{A}}]$ (the top k rows of $[\mathbf{A}]$), respectively. In case of k-Lin, we have $\mathsf{RE}(\mathbf{A})=k$ and $\overline{\mathsf{RE}}(\overline{\mathbf{A}})=k-1$. 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. In all settings, we improve upon either the assumption (c.f. Figure 3), the CRS size, or # pairings used in verification (which can be further reduced using randomized verification), as indicated by a ✓.

storage [4, 47], non-malleable trapdoor commitments to group elements [47] and QANIZK [48]. The first constructions of LHSPS were given in [47, 21].

We show how to extend our QANIZK techniques to LHSPS. Concretely, for our one-time secure LHSPS, we define a signature σ on message $[\mathbf{m}]_1 \in \mathbb{G}_1^n$ as

$$\sigma = [\mathbf{m}^\top \mathbf{K}]_1,$$

and publish $[\mathbf{A}]_2, [\mathbf{K}\mathbf{A}]_2$ for verification. Security follows by the same argument as in our QANIZK construction. Our construction can also be seen as a generalization of a 2-KerLin based scheme from [47] to $\mathcal{D}_k$-KerMDH. Similarly, the construction of unbounded simulation-sound QANIZK gives rise to a fully secure LHSPS scheme. In the latter, the signatures on previously signed messages $([\mathbf{m}_i]_1)_{1\le i\le q}$ reveal $\mathbf{M}^\top\mathbf{K}$ to the adversary, where $\mathbf{M}=(\mathbf{m}_1,\ldots,\mathbf{m}_q)$. The winning condition of LHSPS is to produce a valid signature on a message outside of the language $\mathcal{L}_\mathbf{M}$, which corresponds to breaking simulation-soundness in the QANIZK. Here, we do have to address an additional complication arising from the fact that the LHSPS adversary is allowed to have previously requested signatures for the challenge tag. Our constructions improve upon the efficiency of the prior schemes; see Figure 2. Moreover, our techniques also offer two qualitative advantages over those in [48]: first, they immediately yield fully randomizable linearly homomorphic signatures, which means they are strongly context-hiding [7, 4], and second, we completely eliminate the additional restriction that adversary only query linearly independent vectors on each tag [47, §2.1].

In fact, our constructions follow a more general and natural (in hindsight) methodology for constructing LHSPS from any QANIZK: the signing key is the simulation trapdoor; a signature on $[\mathbf{m}]_1$ is a simulated proof on the vector $[\mathbf{m}]_1$; verifying a signature is the same as verifying a proof. The proof of LHSPS security uses the honest prover to simulate signatures. When a LHSPS adversary requests signatures on $([\mathbf{m}_i]_1)_{1\le i\le q}$, it gets QANIZK proofs for the vectors lying in the span of the matrix $\mathbf{M}:=(\mathbf{m}_1,\ldots,\mathbf{m}_q)$. Soundness for

	Security	Restrictions on adv.	Assumption	signature	pk
LPJY13 [47, §3.1]:	OT	none	2-KerLin ($\mathbb{G}_2$)	3	$2n+3$
LPJY14 [48, §D]:	OT	none	$\mathcal{L}_k$-KerMDH ($\mathbb{G}_2$)	$k+1$	$kn+2k-1$
$\mathsf{LHSPS}_{\mathsf{ot}}$ (Fig 10)	OT	none	$\mathcal{D}_k$-KerMDH ($\mathbb{G}_2$)	$k+1$	$kn+\mathsf{RE}(\mathcal{D}_k)$
LPJY13 [47, §3.2]:	full	indep.	2-KerLin ($\mathbb{G}_1=\mathbb{G}_2$)	4	$2n+\lambda+5$
LPJY13 [47, §B.2]:	full, rand	indep., targeting	2-Lin ($\mathbb{G}_1=\mathbb{G}_2$)	15	$2n+\lambda+7$
$\mathsf{LHSPS}_{\mathsf{full}}$ (Fig 8)	full, rand	targeting	$\mathcal{D}_k$-MDDH ($\mathbb{G}_1,\mathbb{G}_2$)	$2k+2$	$kn+4(k+1)k+2\mathsf{RE}(\mathcal{D}_k)$

Fig. 2. Linearly homomorphic structure-preserving signatures for $\mathcal{M}=\mathbb{G}_1^n$ and tag-space $\mathcal{T}=\{0,1\}^\lambda$. In the security column, OT stands for one-time security and full for full security; rand stands for full randomizability. The restrictions column describes the restrictions required on the adversary. An independent adversary is restricted to querying linearly independent vectors on each tag; a targeting adversary is required to provide a certificate that its output vector is outside the span of previous queried messages.

QANIZK tells us that it is infeasible to produce an accepting proof for a vector outside the span of $\mathbf{M}$; this means that it is infeasible to produce a valid signature for a vector outside the span of $([\mathbf{m}_i]_1)_{1\le i\le q}$. For the above construction to work, we require that proof verification does not depend on $\mathbf{M}$, which is indeed satisfied by all of our QANIZK protocols. The main qualitative difference between QANIZK and LHSPS security is that in QANIZK, the entire $\mathbf{M}$ is fixed in advance, whereas in signatures, the corresponding matrix is chosen adaptively and incrementally row by row. This means that QANIZK proof techniques that require WS and that program an explicit description of $\mathbf{M}$ into the CRS (which is the case for the QANIZK schemes with the shortest proofs) do not yield LHSPS schemes.

1.3 Discussion

Comparison with previous approaches. We briefly outline previous approaches for obtaining constant-size QANIZK proofs for linear subspaces. The constructions in [43, 1] both derive their basic QANIZK with adaptive soundness from a more general framework: a switching lemma in [43] and hash proof system for disjunctions in [1]. Both frameworks seem inherently limited to decisional assumptions, whereas our constructions enable the use of computational search assumptions. Moreover, the switching lemma framework appears to be limited to applications where the adversary's winning condition is efficiently checkable, and therefore seems unlikely to extend beyond WS distributions or to LHSPS even in the one-time setting. On the other hand, these more general frameworks could enable other new applications.

Previous QANIZK constructions achieving one-time simulation-soundness as well as the weaker notion of single-theorem relatively soundness [41] proceed by combining a basic adaptively secure QANIZK scheme with either a hash proof system [42, 48, 43] or some strengthening thereof [1]. Our approach for one-time simulation-soundness by replacing a single key with the output of a 2-wise independent hash function is arguably simpler and more natural.

The constructions of Libert et al. in [48] used LHSPS in the constructions of QANIZK. Interestingly, while this prior work [48] used LHSPS to build QANIZK, we reverse the connection in this work, and as a result, obtained even more efficient QANIZK and LHSPS. Their basic QANIZK with adaptive soundness builds upon on an existing one-time structure-preserving signature in [2, 3]. Their QANIZK scheme with unbounded simulation-soundness as well as the fully secure LHSPS in [47] relies on Waters' random partitioning technique [53, 12], which originated in the context of adaptively secure IBE; the final QANIZK scheme is fairly complex, require a long CRS, an inefficient security reduction, and in addition the use of Groth-Sahai NIWI proofs. Our schemes for unbounded simulation-soundness and full security rely on the more powerful dual system encryption methodology [52] for building adaptively secure IBE, and are largely self-contained.

Other related work. The idea of compiling symmetric to asymmetric cryptography also appeared in several prior works. In 1989, Bellare and Goldwasser [11] gave a transformation from a message authentication code (originally, a PRF) and a NIZK to a signature scheme; interestingly, their transformation requires NIZK as a building block, whereas NIZK is the target of our compiler. To the best of our knowledge, the first works to explicitly point out that we can directly compile a symmetric primitive into an asymmetric one in pairing groups came from the literature on attribute-based and identity-based encryption [54, 24, 5, 13]. These latter works can be viewed as an instantiation of the dual system encryption methodology [52, 46]. In the specific case of (H)IBE, they can also be viewed as an algebraic MAC plus a Groth-Sahai NIZK [13].

Perspective. As noted at the beginning of the introduction, Groth-Sahai NIZK have been widely used in many cryptographic applications in recent years. We presented a conceptually different yet very simple approach for building NIZK with extremely short proofs for linear subspaces, and also to improve one of the applications. We are optimistic that our approach will yield concrete improvements to many constructions that currently rely on Groth-Sahai proofs.

2 Definitions

Notation. If $\mathbf{x} \in \mathcal{B}^n$, then $|\mathbf{x}|$ denotes the length n of the vector. Further, $x \leftarrow_R \mathcal{B}$ 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 [30]. 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 [30, 49].

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 $([\mathbf{A}], [\mathbf{A}\mathbf{w}])$ 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 $\mathcal{A}$,*

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

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 [49] 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 [49].

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

For each $k \geq 1$, [30, 49] 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 $\mathsf{Lin}_k := \mathcal{L}_k$-MDDH ($k$-Linear Assumption of [39]) and $\mathsf{KerLin}_k := \mathcal{L}_k$-KerMDH. Note that $\mathsf{KerLin}_2 = \mathsf{SDP}$ (Simultaneous Double Pairing Assumption of [22]). The relations between the different assumptions for $\mathcal{D}_k = \mathcal{L}_k$ are as follows:

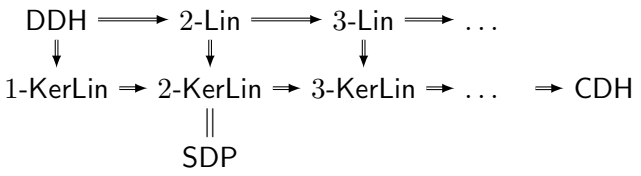

Fig. 3. The relation between k-KerLin and k-Lin.

2.3 Quasi-adaptive Non-Interactive Zero-Knowledge

Quasi-Adaptive NIZK (QA-NIZK) proofs are NIZK proofs where the CRS is allowed to depend on the specific language for which proofs have to be generated [42]. The common reference string crs is generated in a specific way and contains a fixed part par, produced by an algorithm $\mathsf{Gen}_{\mathsf{par}}$, and a language-dependent part crs_l. However, for the zero-knowledge property there should be a single simulator for the entire class of languages.

For public parameters par produced by $\mathsf{Gen}_{\mathsf{par}}$, let $\mathcal{D}_{\mathsf{par}}$ be a probability distribution over a collection of relations $R = \{R_\rho\}$ parametrized by a string ρ with an associated language $\mathcal{L}_\rho = \{y : \exists x \text{ s.t. } R_\rho(y, x) = 1\}$.

We now give a formal definition of QANIZK for $\mathcal{D}_{\mathsf{par}}$ in its tag-based variant.

Definition 4 (Quasi-adaptive Non-Interactive Zero Knowledge Argument). *A* Quasi-adaptive Non-Interactive Zero Knowledege Argument *(QANIZK) Π for a language distribution $\mathcal{D}_{\mathsf{par}}$ consists of five PPT algorithms $\Pi = (\mathsf{Gen}_{\mathsf{par}}, \mathsf{Gen}_{\mathsf{crs}}, \mathsf{Prove}, \mathsf{Sim}_\pi, \mathsf{Verify})$:*

- *The probabilistic key generation algorithm $\mathsf{Gen}_{\mathsf{par}}(\lambda)$ returns the public parameters par.*
- *The probabilistic algorithm $\mathsf{Gen}_{\mathsf{crs}}(\mathsf{par}, \rho)$ returns a common reference string crs and a trapdoor trap. We assume that crs implicitly contains par and ρ and that it defines a tag-space $\mathcal{T}$. (This is the classical QANIZK setting.) If $\mathcal{T}$ is not specified then $\mathcal{T} = \{\varepsilon\}$ and tags can be ignored in all algorithms.*
- *The probabilistic proving algorithm $\mathsf{Prove}(\mathsf{crs}, \tau, x, y)$ returns a proof π with respect to tag $\tau \in \mathcal{T}$.*
- *The deterministic verification algorithm $\mathsf{Verify}(\mathsf{crs}, \tau, y, \pi)$ returns 1 or 0, where 1 means that π is a valid proof of $y \in \mathcal{L}_\rho$.*
- *The probabilistic proving algorithm $\mathsf{Sim}_\pi(\mathsf{crs}, \mathsf{trap}, \tau, y)$ returns a proof π for some y (not necessarily in $\mathcal{L}_\rho$) with respect to tag $\tau \in \mathcal{T}$.*

We require that the algorithms satisfy the following properties:

(Perfect completeness). *For all λ, all par output by $\mathsf{Gen}_{\mathsf{par}}(\lambda)$, all ρ output by $\mathcal{D}_{\mathsf{par}}$, all (x, y) with $R_\rho(y, x) = 1$, all $\tau \in \mathcal{T}$, we have*

$$\Pr\left[\mathsf{Verify}(\mathsf{crs}, \tau, y, \pi) = 1 \;\middle|\; \begin{array}{l}|(\mathsf{crs}, \mathsf{trap}) \leftarrow_{\mathrm{R}} \mathsf{Gen}_{\mathsf{crs}}(\mathsf{par}, \rho) \\ \pi \leftarrow_{\mathrm{R}} \mathsf{Prove}(\mathsf{crs}, \tau, x, y)\end{array}\right] = 1.$$

(Perfect zero-knowledge). *For all λ, all par output by $\mathsf{Gen}_{\mathsf{par}}(\lambda)$, all ρ output by $\mathcal{D}_{\mathsf{par}}$, all $(\mathsf{crs}, \mathsf{trap})$ output by $\mathsf{Gen}_{\mathsf{crs}}(\mathsf{par}, \rho)$, all (x, y) with $R_\rho(y, x) = 1$, all $\tau \in \mathcal{T}$, the distributions*

$$\mathsf{Prove}(\mathsf{crs}, \tau, x, y) \text{ and } \mathsf{Sim}_\pi(\mathsf{crs}, \mathsf{trap}, \tau, y)$$

are the same (where the coin tosses are taken over $\mathsf{Prove}, \mathsf{Sim}_\pi$).

(Computational adaptive soundness). *For all PPT adversaries* $\mathcal{A}$, $\mathbf{Adv}^{\mathrm{as}}_{\Pi}(\mathcal{A}) :=$

$$\Pr\left[\begin{array}{l} y^\star \notin \mathcal{L}_\rho \\ \wedge \mathsf{Verify}(\mathsf{crs}, \tau^\star, y^\star, \pi^\star) = 1 \end{array} \middle| \begin{array}{l} \mathsf{par} \leftarrow_{\mathrm{R}} \mathsf{Gen}_{\mathsf{par}}(\lambda); \rho \leftarrow_{\mathrm{R}} \mathcal{D}_{\mathsf{par}} \\ (\mathsf{crs}, \mathsf{trap}) \leftarrow_{\mathrm{R}} \mathsf{Sim}_{\mathsf{crs}}(\mathsf{par}, \rho) \\ (\tau^\star, y^\star, \pi^\star) \leftarrow_{\mathrm{R}} \mathcal{A}(\mathsf{par}, \mathsf{crs}, \rho) \end{array}\right]$$

is negligible.

Note that our formalization of perfect knowledge is similar to that of composable zero knowledge in [38] and requires indistinguishability even for adversaries that get access to $(\mathsf{crs}, \mathsf{trap})$. In particular, the formalization implies composability (namely, the adversary may see multiple proofs for many adaptively chosen instances in the language). We also consider simulation soundness [51, 27], which is a strengthening of adaptive soundness, and stipulates that an adversary cannot prove a false statement, even if it can see simulated proofs for instances y of its choice.

Definition 5 (Simulation soundness). *A QANIZK system* Π *is said to be* (unbounded) simulation-sound *if for all PPT adversaries* $\mathcal{A}$, $\mathbf{Adv}^{\mathrm{uss}}_{\Pi}(\mathcal{A}) :=$

$$\Pr\left[\begin{array}{l} y^\star \notin \mathcal{L}_\rho \wedge \tau^\star \notin \mathcal{Q}_{\mathrm{tags}} \\ \wedge \mathsf{Verify}(\mathsf{crs}, \tau^\star, y^\star, \pi^\star) = 1 \end{array} \middle| \begin{array}{l} \mathsf{par} \leftarrow_{\mathrm{R}} \mathsf{Gen}_{\mathsf{par}}(\lambda); \rho \leftarrow_{\mathrm{R}} \mathcal{D}_{\mathsf{par}} \\ (\mathsf{crs}, \mathsf{trap}) \leftarrow_{\mathrm{R}} \mathsf{Sim}_{\mathsf{crs}}(\mathsf{par}, \rho) \\ (\tau^\star, y^\star, \pi^\star) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathsf{ProveO}(\cdot,\cdot)}(\mathsf{par}, \mathsf{crs}, \rho) \end{array}\right]$$

is negligible, where $\mathsf{ProveO}(\tau, y)$ *returns* $\mathsf{Sim}_\pi(\mathsf{crs}, \mathsf{trap}, \tau, y)$ *and adds* τ *to the set* $\mathcal{Q}_{\mathrm{tags}}$. Π *is said to be* one-time simulation-sound *with corresponding advantage function* $\mathbf{Adv}^{\text{ot-ss}}_{\Pi}(\mathcal{A})$*, if* $\mathcal{A}$ *is restricted to make at most one query to the oracle* ProveO.

We remark that a QANIZK with exponential tag-space can be transformed into a classical QANIZK with $\mathcal{T} = \{\varepsilon\}$ using a one-time signature scheme or a MAC. Other security properties remain the same.

2.4 Linearly homomorphic structure-preserving signatures

We now define syntax and security of a linearly homomorphic structure-preserving signature (LHSPS) scheme [47, 32, 15], where the signatures are fully randomizable and also strongly context-hiding [7, 4]. We assume the existence of $\mathsf{Gen}_{\mathsf{par}}(\lambda)$, a probabilistic key generation algorithm that returns public parameters par containing the description of a group $\mathbb{G}$.

Definition 6 (Linearly homomorphic structure-preserving signature). *A* linearly homomorphic structure-preserving signature *(LHSPS) scheme* LHSPS *consists of four PPT algorithms* $\mathsf{LHSPS} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{SignDerive}, \mathsf{Verify})$ *with the following properties.*

- *The probabilistic key generation algorithm* $\mathsf{Gen}(\mathsf{par})$ *returns the (master) 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* $n \in \mathrm{poly}(\lambda)$*, and a tag space* $\mathcal{T}$*.*
- *The probabilistic signing algorithm* $\mathsf{Sign}(\mathsf{sk}, \tau, [\mathbf{m}])$ *returns a signature* $\sigma \in \mathbb{G}^{n_\sigma}$ *on message* $[\mathbf{m}] \in \mathbb{G}^n$ *with respect to tag* τ*.*
- *The probabilistic signature derivation algorithm* $\mathsf{SignDerive}(\mathsf{pk}, \tau, (\omega_i, \sigma_i)_{1 \le i \le \ell})$ *returns a signature* $\sigma \in \mathbb{G}^{n_\sigma}$ *on the vector* $[\sum \omega_i \mathbf{m}_i]$*, where* $\omega_i \in \mathbb{Z}_q$ *and* σ_i *is a valid signature on* $[\mathbf{m}_i]$ *with respect to tag* τ*.*

– *The deterministic verification algorithm* $\mathsf{Verify}(\mathsf{pk}, \tau, [\mathbf{m}], \sigma)$ *returns 1 or* 0*, where* 1 *means that* σ *is a valid signature in* $[\mathbf{m}]$.

We require that for all $\lambda \in \mathbb{N}$*, all pairs* $(\mathsf{pk}, \mathsf{sk})$ *generated by* $\mathsf{Gen}(\mathsf{par})$*, all tags* $\tau \in \mathcal{T}$*, the following holds:*

(Perfect correctness.) *for all messages* $[\mathbf{m}] \in \mathbb{G}^n$*, all* σ *generated by* $\mathsf{Sign}(\mathsf{sk}, \tau, [\mathbf{m}])$ *we have*

$$\mathsf{Ver}(\mathsf{pk}, \tau, [\mathbf{m}], \sigma) = 1.$$

(Full randomizability.) *for all messages* $[\mathbf{m}_1], \ldots, [\mathbf{m}_\ell] \in \mathbb{G}^n$*, all* $\omega_1, \ldots, \omega_\ell \in \mathbb{Z}_q$*, for all* $\sigma_1, \ldots, \sigma_\ell$ *where* $\sigma_i \leftarrow \mathsf{Sign}(\mathsf{sk}, \tau, [\mathbf{m}_i])$*, the distributions*

$$\mathsf{Sign}(\mathsf{sk}, \tau, [\sum \omega_i \mathbf{m}_i]) \text{ and } \mathsf{SignDerive}(\mathsf{pk}, \tau, (\omega_i, \sigma_i)_{1 \le i \le \ell})$$

are the same.

Note that our requirement of full randomizability implies strongly context hiding as considered in [7, 4]. We now define security for LHSPS schemes.

Definition 7. *To an adversary* $\mathcal{A}$ *and* LHSPS *we associate the advantage function* $\mathbf{Adv}^{\mathrm{ufcma}}_{\mathsf{LHSPS}}(\mathcal{A}) :=$

$$\Pr\left[\begin{array}{l|l} \mathbf{m}^* \notin span(\mathbf{M}_{\tau^*}) & (\mathsf{pk}, \mathsf{sk}) \leftarrow_{\mathrm{R}} \mathsf{Gen}(\mathsf{par}) \\ \wedge \mathsf{Verify}(\mathsf{pk}, \tau^*, [\mathbf{m}^*], \sigma^*) = 1 & (\tau^*, [\mathbf{m}^*], \sigma^*) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathsf{SignO}(\cdot,\cdot)}(\mathsf{pk}) \end{array}\right],$$

where $\mathsf{SignO}(\tau, [\mathbf{m}])$ *runs* $\sigma \leftarrow_{\mathrm{R}} \mathsf{Sign}(\mathsf{sk}, \tau, [\mathbf{m}])$*, appends the vector* $\mathbf{m}$ *(as a new column) to the matrix* $\mathbf{M}_\tau$ *(initialized with* $\mathbf{0}$*) and returns* σ *to* $\mathcal{A}$*.*

Note that the winning condition $\mathbf{m}^* \notin span(\mathbf{M}_{\tau^*})$ may not be efficiently verifiable. We will also consider security against a restricted class of "targeting adveraries" [47] which provide a certificate $\mathbf{c}^*$ for $\mathbf{m}^* \notin span(\mathbf{M}_{\tau^*})$.

Definition 8. *To an adversary* $\mathcal{A}$ *and* LHSPS *we associate the advantage function* $\mathbf{Adv}^{\mathrm{ufcma-t}}_{\mathsf{LHSPS}}(\mathcal{A}) :=$

$$\Pr\left[\begin{array}{l|l} \mathbf{c}^{*\top}\mathbf{m}^* \neq 0 \wedge \mathbf{c}^{*\top}\mathbf{M}_{\tau^*} = \mathbf{0} & (\mathsf{pk}, \mathsf{sk}) \leftarrow_{\mathrm{R}} \mathsf{Gen}(\mathsf{par}) \\ \wedge \mathsf{Verify}(\mathsf{pk}, \tau^*, [\mathbf{m}^*], \sigma^*) = 1 & (\tau^*, [\mathbf{m}^*], \sigma^*, [\mathbf{c}^*]) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathsf{SignO}(\cdot,\cdot)}(\mathsf{pk}) \end{array}\right],$$

where $\mathsf{SignO}(\tau, [\mathbf{m}])$ *runs* $\sigma \leftarrow_{\mathrm{R}} \mathsf{Sign}(\mathsf{sk}, \tau, [\mathbf{m}])$*, appends the vector* $\mathbf{m}$ *(as a new column) to the matrix* $\mathbf{M}_\tau$ *(initialized with* $\mathbf{0}$*) and returns* σ *to* $\mathcal{A}$*.*

Observe that $\mathbf{c}^{*\top}\mathbf{m}^* \neq 0 \wedge \mathbf{c}^{*\top}\mathbf{M}_{\tau^*} = \mathbf{0}$ (which we can check via the pairing) implies $\mathbf{m}^* \notin span(\mathbf{M}_{\tau^*})$.

3 Quasi-Adaptive Zero Knowledge for Linear Spaces

In this section we will describe a number of Quasi-Adaptive Zero Knowledge Proofs for linear spaces. From now on and for the rest of this paper we will use $\mathsf{Gen}_{\mathsf{par}} = \mathsf{GGen}$. That is, $\mathsf{Gen}_{\mathsf{par}}(1^\lambda)$ returns $\mathsf{par} = \mathcal{PG}$, where $\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, g_1, g_2, e)$ is a pairing group. The probability distribution $\mathcal{D}_{\mathsf{par}}$ returns a matrix $\rho = [\mathbf{M}]_1 \in \mathbb{G}_1^{n \times t}$, for integers $n > t$. Given par and ρ, the language $\mathcal{L}_{\mathbf{M}}$ is defined as

$$\mathcal{L}_{\mathbf{M}} = \Big\{ [\mathbf{y}]_1 \in \mathbb{G}_1^n : \exists\, \mathbf{x} \in \mathbb{Z}_q^t \text{ s.t. } \mathbf{y} = \mathbf{M}\mathbf{x} \Big\}.$$

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

$$\Pr\left[\mathbf{y} \notin \mathit{span}(\mathbf{M}) \wedge \mathbf{z}^\top = \mathbf{y}^\top\mathbf{K} \;\middle|\; \begin{array}{l}\mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)} \\ (\mathbf{z},\mathbf{y}) \leftarrow_{\mathrm{R}} \mathcal{A}(\mathbf{M}^\top\mathbf{K}, \mathbf{K}\mathbf{A})\end{array}\right] \leq \frac{1}{q}$$

$$\Pr\left[\begin{array}{l}\mathbf{y} \notin \mathit{span}(\mathbf{M}) \wedge \tau \neq \hat{\tau} \\ \wedge\, \mathbf{z}^\top = \mathbf{y}^\top(\mathbf{K}_0 + \hat{\tau}\mathbf{K}_1)\end{array} \;\middle|\; \begin{array}{l}\mathbf{K}_0, \mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}; \\ (\mathbf{z},\mathbf{y},\tau) \leftarrow_{\mathrm{R}} \mathcal{A}^{\mathcal{O}(\cdot)}(\mathbf{M}^\top\mathbf{K}_0, \mathbf{M}^\top\mathbf{K}_1, \mathbf{K}_0\mathbf{A}, \mathbf{K}_1\mathbf{A})\end{array}\right] \leq \frac{1}{q},$$

where $\mathcal{O}(\hat{\tau})$ may only be called one time and returns $\mathbf{K}_0 + \hat{\tau}\mathbf{K}_1$.

Proof. To prove the first equation of the lemma, fix $\mathbf{M} \in \mathbb{Z}_q^{n\times t}, \mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$, and fix a non-zero vector $\hat{\mathbf{a}} \notin \mathit{span}(\mathbf{A})$. Then, for any $\mathbf{y} \notin \mathit{span}(\mathbf{M})$, the following distributions

$$(\mathbf{M}^\top\mathbf{K}, \mathbf{K}\mathbf{A}, \mathbf{y}^\top\mathbf{K}\hat{\mathbf{a}}) \text{ and } (\mathbf{M}^\top\mathbf{K}, \mathbf{K}\mathbf{A}, u) \tag{1}$$

are the same, where $\mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}, u \leftarrow_{\mathrm{R}} \mathbb{Z}_q$. By a standard argument (e.g. complexity leveraging[5]), this means that the two distributions are the same even if $\mathbf{y} \notin \mathit{span}(\mathbf{M})$ is adaptively chosen after seeing $(\mathbf{M}^\top\mathbf{K}, \mathbf{K}\mathbf{A})$. Therefore, for any adversary $\mathcal{A}$, we have

$$\Pr_{\mathbf{K}\leftarrow_{\mathrm{R}}\mathbb{Z}_q^{n\times(k+1)}}[\mathbf{y} \notin \mathit{span}(\mathbf{M}) \wedge \mathbf{z}^\top\hat{\mathbf{a}} = \mathbf{y}^\top\mathbf{K}\hat{\mathbf{a}} \mid (\mathbf{z},\mathbf{y}) \leftarrow_{\mathrm{R}} \mathcal{A}(\mathbf{M}^\top\mathbf{K}, \mathbf{K}\mathbf{A})] \leq 1/q$$

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

To prove the second equation of the lemma, observe that $(\mathbf{K}_0 + \tau\mathbf{K}_1, \mathbf{K}_0 + \hat{\tau}\mathbf{K}_1)$ are pairwise-independent, so we can essentially give away $\mathbf{K}_0 + \tau\mathbf{K}_1$ to $\mathcal{A}$ and still carry out the preceding proof with $\mathbf{K}_0 + \hat{\tau}\mathbf{K}_1$ in place of $\mathbf{K}$. More formally, for any $\tau \neq \hat{\tau}$ and any $\mathbf{y} \notin \mathit{span}(\mathbf{M})$, the following distributions

$$\begin{array}{c}(\mathbf{M}^\top\mathbf{K}_0, \mathbf{M}^\top\mathbf{K}_1, \mathbf{K}_0\mathbf{A}, \mathbf{K}_1\mathbf{A}, \mathbf{K}_0 + \tau\mathbf{K}_1, \mathbf{y}^\top(\mathbf{K}_0 + \hat{\tau}\mathbf{K}_1)\hat{\mathbf{a}}) \\ \text{and } (\mathbf{M}^\top\mathbf{K}_0, \mathbf{M}^\top\mathbf{K}_1, \mathbf{K}_0\mathbf{A}, \mathbf{K}_1\mathbf{A}, \mathbf{K}_0 + \tau\mathbf{K}_1, u)\end{array}$$

are the same, where $\mathbf{K}_0, \mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}, u \leftarrow_{\mathrm{R}} \mathbb{Z}_q$. Upon eliminating the terms involving $\mathbf{K}_0 + \tau\mathbf{K}_1$, the preceding claim follows from the fact that the following distributions

$$(\mathbf{M}^\top\mathbf{K}_1, \mathbf{K}_1\mathbf{A}, (\hat{\tau} - \tau)\mathbf{y}^\top\mathbf{K}_1\hat{\mathbf{a}}) \text{ and } (\mathbf{M}^\top\mathbf{K}_1, \mathbf{K}_1\mathbf{A}, u)$$

are the same, where $\mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}, u \leftarrow_{\mathrm{R}} \mathbb{Z}_q$, as considered earlier in (1). The proof then proceeds as before.

3.1 Simple QANIZK with Adaptive Soundness

Let $\mathcal{D}_k$ be any matrix distribution from Definition 1. Consider protocol Π_{as} from Figure 4.

[5] 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.

$\underline{\mathsf{Gen}(\mathsf{par}, [\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t})}$:
$\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k; \mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}$
$\mathbf{P} := \mathbf{M}^\top\mathbf{K}; \mathbf{C} := \mathbf{K}\mathbf{A}$
$\mathsf{crs} := ([\mathbf{P}]_1, [\mathbf{C}]_2, [\mathbf{A}]_2) \in \mathbb{G}_1^{t\times(k+1)} \times \mathbb{G}_2^{n\times k} \times \mathbb{G}_2^{(k+1)\times k}$
Return $(\mathsf{crs}, \mathsf{trap} = \mathbf{K})$

$\underline{\mathsf{Prove}(\mathsf{crs}, [\mathbf{y}]_1, \mathbf{x})}$: // $\mathbf{y} = \mathbf{M}\mathbf{x}$
Return $\pi := \left(\left[\mathbf{x}^\top\mathbf{P}\right]_1\right) \in \mathbb{G}_1^{k+1}$

$\underline{\mathsf{Sim}(\mathsf{crs}, \mathsf{trap} = \mathbf{K}, [\mathbf{y}]_1)}$:
Return $\pi := \left(\left[\mathbf{y}^\top\mathbf{K}\right]_1\right)$

$\underline{\mathsf{Verify}(\mathsf{crs}, [\mathbf{y}]_1, \pi)}$:
Check: $e(\pi, [\mathbf{A}]_2) = e(\left[\mathbf{y}^\top\right]_1, [\mathbf{C}]_2)$

Fig. 4. QANIZK Π_{as} with adaptive soundness under $\mathcal{D}_k$-KerMDH Assumption.

Theorem 1. *Protocol Π_{as} from Figure 4 is a Quasi-adaptive Non-Interactive Zero Knowledege Argument. Furthermore, under the $\mathcal{D}_k$-KerMDH Assumption in $\mathbb{G}_2$, it has adaptive soundness.*

Proof. Perfect completeness and perfect zero-knowledge follow readily from the fact that for all $\mathbf{y} = \mathbf{M}\mathbf{x}$ and $\mathbf{P} = \mathbf{M}^\top\mathbf{K}$:

$$\mathbf{x}^\top\mathbf{P} = \mathbf{x}^\top(\mathbf{M}^\top\mathbf{K}) = \mathbf{y}^\top\mathbf{K}.$$

We proceed to establish adaptive soundness 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

$$\mathbf{Adv}^{\mathrm{as}}_{\Pi_{\mathsf{as}}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}) + 1/q. \tag{2}$$

Adversary $\mathcal{B}(\mathcal{PG}, [\mathbf{A}]_2 \in \mathbb{G}_2^{(k+1)\times k})$ generates $[\mathbf{M}]_1 \leftarrow_{\mathrm{R}} \mathcal{D}_{\mathsf{par}}$, and the rest of the CRS as in the real scheme by picking $\mathbf{K} \in \mathbb{Z}_q^{n\times(k+1)}$ and computing

$$\mathsf{crs} = ([\mathbf{P}]_1 = \left[\mathbf{M}^\top\mathbf{K}\right]_1 \in \mathbb{G}_1^{t\times k}, \quad [\mathbf{C}]_2 = [\mathbf{K}\cdot\mathbf{A}]_2 \in \mathbb{G}_2^{n\times k}, \quad [\mathbf{A}]_2 \in \mathbb{G}_2^{(k+1)\times k}).$$

Next, $\mathcal{B}$ runs $\mathcal{A}$ on crs and obtains a proof $\pi = [\mathbf{z}^\top]_1 \in \mathbb{G}_1^{1\times k}$ and $[\mathbf{y}]_1 \in \mathbb{G}_1^n$ satisfying $\mathbf{y} \notin \mathit{span}(\mathbf{M})$ and $\mathbf{z}^\top\cdot\mathbf{A} = \mathbf{y}^\top\cdot\mathbf{C} = \mathbf{y}^\top\mathbf{K}\cdot\mathbf{A}$ with probability $\mathbf{Adv}^{\mathrm{as}}_{\Pi_{\mathsf{as}}}(\mathcal{A})$. Finally, $\mathcal{B}$ returns $[\mathbf{s}]_1$ computed as

$$\mathbf{s}^\top = \mathbf{z}^\top - \mathbf{y}^\top\mathbf{K}.$$

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

3.2 More Efficient QANIZK with Adaptive Soundness for WS distributions

Recall that we are considering a probability distribution $\mathcal{D}_{\mathsf{par}}$ that outputs a matrix $[\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t}$. Such distributions are called *witness sampleable* (WS) [42] if there exist an efficiently sampleable distribution $\mathcal{D}'_{\mathsf{par}}$ that outputs $\mathbf{M}' \in \mathbb{Z}_q^{n\times t}$ such that $[\mathbf{M}']_1$ has the same distribution as $[\mathbf{M}]_1$. Note that this slightly restricts the set of languages which can be handled. Whereas the techniques used in QANIZK protocols for WS distributions pose no restrictions for most applications, are not applicable to structure-preserving signatures (for the latter, $[\mathbf{M}]_1$ is chosen adaptively by an adversary).

In Figure 5 we give an efficiency improvement of Π_{as} from Figure 4 which only works for WS distributions.

$\underline{\mathsf{Gen}(\mathsf{par}, [\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t})}$:
$\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k; \mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times k}$
$\mathbf{P} := \mathbf{M}^\top \mathbf{K}; \mathbf{C} := \mathbf{K}\bar{\mathbf{A}}$
$\mathsf{crs} := ([\mathbf{P}]_1, [\mathbf{C}]_2, [\bar{\mathbf{A}}]_2) \in \mathbb{G}_1^{t\times k} \times \mathbb{G}_2^{n\times k} \times \mathbb{G}_2^{k\times k}$
Return $(\mathsf{crs}, \mathsf{trap} = \mathbf{K})$

$\underline{\mathsf{Prove}(\mathsf{crs}, [\mathbf{y}]_1, \mathbf{x})}$: // $\mathbf{y} = \mathbf{M}\mathbf{x}$
Return $\pi := \left[\mathbf{x}^\top \mathbf{P}\right]_1 \in \mathbb{G}_1^{1\times k}$

$\underline{\mathsf{Sim}_\pi(\mathsf{crs}, \mathsf{trap} = \mathbf{K}, [\mathbf{y}]_1)}$:
Return $\pi := \left[\mathbf{y}^\top \mathbf{K}\right]_1$

$\underline{\mathsf{Verify}(\mathsf{crs}, [\mathbf{y}]_1, \pi)}$:
Check: $e(\pi, \left[\bar{\mathbf{A}}\right]_2) = e(\left[\mathbf{y}^\top\right]_1, [\mathbf{C}]_2)$

Fig. 5. More efficient QANIZK Π'_{as} with adaptive soundness for WS distributions under $\mathcal{D}_k$-KerMDH Assumption. Recall that $\overline{\mathbf{A}} \in \mathbb{Z}_q^{k\times k}$ denotes the upper square matrix of $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$.

Theorem 2. *Protocol Π'_{as} from Figure 5 is a Quasi-adaptive Non-Interactive Zero Knowledege Argument. Suppose in addition that $\mathcal{D}_{\mathsf{par}}$ is a witness sampleable distribution. Then, under the $\mathcal{D}_k$-KerMDH Assumption in $\mathbb{G}_2$, the protocol has adaptive soundness.*

Proof. Perfect completeness and perfect zero-knowledge follow readily from the fact that for all $\mathbf{y} = \mathbf{M}\mathbf{x}$ and $\mathbf{P} = \mathbf{M}^\top \mathbf{K}$:

$$\mathbf{x}^\top \mathbf{P} = \mathbf{x}^\top (\mathbf{M}^\top \mathbf{K}) = \mathbf{y}^\top \mathbf{K}.$$

We proceed to establish adaptive soundness 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

$$\mathbf{Adv}^{\mathrm{as}}_{\Pi'_{\mathsf{as}}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{B}) + 1/q. \tag{3}$$

Adversary $\mathcal{B}(\mathcal{PG}, [\mathbf{A}]_2 \in \mathbb{G}_2^{(k+1)\times k})$ generates $\mathbf{M} \leftarrow_{\mathrm{R}} \mathcal{D}'_{\mathsf{par}}$. (The latter algorithm exists since $\mathcal{D}_{\mathsf{par}}$ is witness sampleable.) Let $\mathbf{M}^\perp \in \mathbb{Z}_q^{n\times(n-t)}$ be a basis for the kernel of $\mathbf{M}^\top$, that is, $\mathbf{M}^\perp$ is a full-rank matrix such that $\mathbf{M}^\top \mathbf{M}^\perp = \mathbf{0}$. Next, it picks $\mathbf{K}' \in \mathbb{Z}_q^{n\times k}, \mathbf{R} \in \mathbb{Z}_q^{(n-t-1)\times(k+1)}$ and defines

$$\mathbf{A}' := \begin{pmatrix} \mathbf{A} \\ \mathbf{R}\cdot\mathbf{A} \end{pmatrix} \in \mathbb{Z}_q^{(k+n-t)\times k}.$$

Let $\mathbf{T}_{\mathbf{A}'} \in \mathbb{Z}_q^{(n-t)\times k}$ be such that $\mathbf{T}_{\mathbf{A}'}\overline{\mathbf{A}'} = \underline{\mathbf{A}}'$. By implicitly defining $\mathbf{K} = \mathbf{K}' + \mathbf{M}^\perp \mathbf{T}_{\mathbf{A}'}$, $\mathcal{B}$ can compute

$$[\mathbf{C}]_2 = [\mathbf{K}\overline{\mathbf{A}}]_2 = [(\mathbf{K}' + \mathbf{M}^\perp \mathbf{T}_{\mathbf{A}'})\overline{\mathbf{A}}]_2 = [\mathbf{K}'\overline{\mathbf{A}}' + \mathbf{M}^\perp \underline{\mathbf{A}}']_2 = [(\mathbf{K}' \| \mathbf{M}^\perp)\cdot \mathbf{A}']_2$$
$$[\mathbf{P}]_1 = [\mathbf{M}^\top \mathbf{K}]_1 = [\mathbf{M}^\top \mathbf{K}']_1.$$

(The way we program the CRS is similar to that in [43, Theorem 13].)

Next, $\mathcal{B}$ runs $\mathcal{A}$ on $\mathsf{crs} := ([\mathbf{P}]_1, [\mathbf{C}]_2, [\bar{\mathbf{A}}]_2)$ and obtains a proof $\pi = [\mathbf{z}^\top]_1 \in \mathbb{G}_1^{1\times k}$ and $[\mathbf{y}]_1 \in \mathbb{G}_1^n$ satisfying $\mathbf{y}^\top \mathbf{M}^\perp \neq \mathbf{0}$ and

$$\mathbf{z}^\top \cdot \overline{\mathbf{A}} = \mathbf{y}^\top \cdot \mathbf{C}. \tag{4}$$

By the definitions of $\mathbf{C}$ and $\mathbf{A}'$,

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

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

$$\mathbf{c}^\top = ((\mathbf{z}^\top - \mathbf{y}^\top \mathbf{K}')\| - \mathbf{y}^\top \mathbf{M}^\perp) \neq \mathbf{0}$$

satisfies $\mathbf{c}^\top \mathbf{A}' = \mathbf{0}$. From $\mathbf{c}^\top = (\mathbf{c}_1^\top \| \mathbf{c}_2^\top) \in \mathbb{Z}_q^{1\times(k+1)} \times \mathbb{Z}_q^{1\times(n-t-1)}$ we will now extract a solution $\mathbf{s}$ to the $\mathcal{D}_k$-KerMDH problem. Define $\mathbf{s}^\top = \mathbf{c}_1^\top + \mathbf{c}_2^\top \mathbf{R}$ such that $\mathbf{s}^\top \mathbf{A} = \mathbf{c}_1^\top \mathbf{A} + \mathbf{c}_2^\top \mathbf{R}\mathbf{A} = \mathbf{c}^\top \mathbf{A}' = \mathbf{0}$. Since $\mathbf{c} \neq \mathbf{0}$ and matrix $\mathbf{R}$ only leaks through $\mathbf{A}'$ as $\mathbf{R}\mathbf{A}$,

$$\Pr_{\mathbf{R}\leftarrow_R \mathbb{Z}_q^{(n-t-1)\times(k+1)}}[\mathbf{c}_1^\top + \mathbf{c}_2^\top \mathbf{R} = \mathbf{0} \mid \mathbf{R}\mathbf{A}] \leq 1/q.$$

This proves equation (3).

3.3 Simple QANIZK with Adaptive One-Time Simulation Soundness

Protocol $\Pi_{\mathsf{ot\text{-}ss}}$ from Figure 6 with one-time simulation soundness is based on Π_{as} from Figure 4 with the hash key $\mathbf{K}$ replaced by the 2-wise independent hash function $h(\tau) := \mathbf{K}_0 + \tau \mathbf{K}_1$. This allows arguing for one-time simulation soundness. We remark that the protocol can be easily extending to ℓ-time simulation soundness by using the ℓ-wise independent hash function $h(\tau) = \sum_{i=0}^{\ell} \tau^i \mathbf{K}_i$. The size of crs would grow with ℓ, but the proof size remains the same.

$\underline{\mathsf{Gen}(\mathsf{par}, [\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t})}$:	$\underline{\mathsf{Prove}(\mathsf{crs}, \tau, [\mathbf{y}]_1, \mathbf{x})}$: // $\mathbf{y} = \mathbf{M}\mathbf{x}$
$\mathbf{A} \leftarrow_R \mathcal{D}_k; \mathbf{K}_0, \mathbf{K}_1 \leftarrow_R \mathbb{Z}_q^{n\times(k+1)}$	Return $\pi := \left[\mathbf{x}^\top(\mathbf{P}_0 + \tau \mathbf{P}_1)\right]_1 \in \mathbb{G}_1^{k+1}$
$(\mathbf{P}_0, \mathbf{P}_1) := (\mathbf{M}^\top \mathbf{K}_0, \mathbf{M}^\top \mathbf{K}_1) \in (\mathbb{Z}_q^{t\times(k+1)})^2$	
$(\mathbf{C}_0, \mathbf{C}_1) := (\mathbf{K}_0\mathbf{A}, \mathbf{K}_1\mathbf{A}) \in (\mathbb{Z}_q^{n\times k})^2$	$\underline{\mathsf{Sim}_\pi(\mathsf{crs}, \mathsf{trap} = (\mathbf{K}_0, \mathbf{K}_1), \tau, [\mathbf{y}]_1)}$:
$\mathsf{crs} := ([\mathbf{P}_0]_1, [\mathbf{P}_1]_1, [\mathbf{C}_0]_2, [\mathbf{C}_1]_2, [\mathbf{A}]_2)$	Return $\pi := \left[\mathbf{y}^\top(\mathbf{K}_0 + \tau \mathbf{K}_1)\right]_1$
Return $(\mathsf{crs}, \mathsf{trap} = (\mathbf{K}_0, \mathbf{K}_1))$	
//crs defines tag-space $\mathcal{T} = \mathbb{Z}_q$	$\underline{\mathsf{Verify}(\mathsf{crs}, \tau, [\mathbf{y}]_1, \pi)}$:
	Check: $e(\pi, [\mathbf{A}]_2) = e(\left[\mathbf{y}^\top\right]_1, [\mathbf{C}_0 + \tau \mathbf{C}_1]_2)$

Fig. 6. QANIZK $\Pi_{\mathsf{ot\text{-}ss}}$ protocol with adaptive one-time simulation-soundness under $\mathcal{D}_k$-KerMDH Assumption.

Theorem 3. *Protocol $\Pi_{\mathsf{ot\text{-}ss}}$ from Figure 6 is a Quasi-adaptive Non-Interactive Zero Knowledege Argument. Furthermore, under the $\mathcal{D}_k$-KerMDH Assumption in $\mathbb{G}_2$, it has adaptive one-time simulation soundness.*

The proof of Theorem 3 is the same as that for Theorem 1 instantiated with the second part of Lemma 2.

Proof. Perfect completeness and perfect zero-knowledge follow readily from the fact that for all $\mathbf{y} = \mathbf{M}\mathbf{x}$ and $(\mathbf{P}_0, \mathbf{P}_1) = (\mathbf{M}^\top \mathbf{K}_0, \mathbf{M}^\top \mathbf{K}_1)$ and all τ:

$$\mathbf{x}^\top(\mathbf{P}_0 + \tau P_1) = \mathbf{x}^\top(\mathbf{M}^\top \mathbf{K}_0 + \tau \mathbf{M}^\top \mathbf{K}_1) = \mathbf{y}^\top(\mathbf{K}_0 + \tau \mathbf{K}_1).$$

We proceed to establish adaptive soundness 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

$$\mathbf{Adv}^{\text{ot-ss}}_{\Pi_{\mathsf{ot\text{-}ss}}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{kmdh}}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{B}) + 1/q. \tag{5}$$

Adversary $\mathcal{B}(\mathcal{PG}, [\mathbf{A}]_2 \in \mathbb{G}_2^{(k+1)\times k})$ generates $[\mathbf{M}]_1 \leftarrow_{\mathrm{R}} \mathcal{D}_{\mathsf{par}}$, and the rest of the CRS as in the real scheme by picking $\mathbf{K}_0, \mathbf{K}_1 \in \mathbb{Z}_q^{n\times(k+1)}$ and computing crs as before. Next, $\mathcal{B}$ runs $\mathcal{A}$ on crs, simulates Sim_π once using $(\mathbf{K}_0, \mathbf{K}_1)$, and obtains a tag τ, a proof $\pi = [\mathbf{z}^\top]_1 \in \mathbb{G}_1^{1\times k}$ and $[\mathbf{y}]_1 \in \mathbb{G}_1^n$ satisfying $\mathbf{y} \notin \mathit{span}(\mathbf{M})$ and $\mathbf{z}^\top \cdot \mathbf{A} = \mathbf{y}^\top \cdot (\mathbf{C}_0 + \tau\mathbf{C}_1) = \mathbf{y}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1) \cdot \mathbf{A}$. Finally, $\mathcal{B}$ returns $[\mathbf{s}]_1$ computed as

$$\mathbf{s}^\top = \mathbf{z}^\top - \mathbf{y}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1).$$

Clearly, $\mathbf{s}^\top\mathbf{A} = \mathbf{0}$ and $\Pr[\mathbf{s} = \mathbf{0}] \leq 1/q$ by the second part of Lemma 2. This proves equation (5).

4 QANIZK with Unbounded Simulation Soundness for WS distributions

In this section, we present a QANIZK with unbounded simulation soundness. For unbounded simulation-soundness, we can no longer rely on information-theoretic techniques for the core lemma (Lemma 2) as in the previous section. Instead, we introduce a computational variant of the core lemma based on the $\mathcal{D}_k$-MDDH assumption in $\mathbb{G}_1$, which we will use again for the fully secure LHSPS in Section 5.

4.1 Computational Core Lemma

In the computational core lemma, instead of giving out zero/one copy of $\mathbf{K}_0 + \tau\mathbf{K}_1$ to the adversary as in Lemma 2, we give out unbounded copies of

$$([\mathbf{r}^\top\mathbf{B}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1)]_1, [\mathbf{r}^\top\mathbf{B}^\top]_1) \in (\mathbb{G}_1^{1\times(k+1)})^2 \tag{6}$$

where $\mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k, \mathbf{K}_0, \mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times(k+1)}$ are fixed and a fresh $\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k$ is chosen for each sample. Under the $\mathcal{D}_k$-MDDH assumption in $\mathbb{G}_1$ w.r.t. the matrix $\mathbf{B}$, this essentially yields a pseudorandom MAC (or randomized PRF) [13, 23, 29, 25]. Note that we can verify these pairs given $(\mathbf{K}_0, \mathbf{K}_1)$. As before, we then publish $[\mathbf{A}]_2, [\mathbf{K}_0\mathbf{A}]_2, [\mathbf{K}_1\mathbf{A}]_2$ for public verification. For completeness, we use the fact that for all $\mathbf{A}, \mathbf{B}, \mathbf{r}, \mathbf{K}_0, \mathbf{K}_1$:

$$e([\mathbf{r}^\top\mathbf{B}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1)]_1, [\mathbf{A}]_2) = e([\mathbf{r}^\top\mathbf{B}^\top]_1, [\mathbf{K}_0\mathbf{A} + \tau\mathbf{K}_1\mathbf{A}]_2). \tag{7}$$

The computational core lemma says that random samples in (6) are pseudorandom subject to the preceding verification equation, in the sense that the first component hides any vector in the kernel of $\mathbf{A}$. The construction and proof strategy build upon those used in recent $\mathcal{D}_k$-MDDH-based fully secure IBE schemes in [13, 23], which in turn build upon earlier dual system IBE schemes in [52, 50, 45, 24].

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

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

where

– $\mathcal{O}_b(\tau)$ *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* $\mathcal{Q}_{\mathrm{tags}}$. *Here,* $\mathbf{a}^\perp \neq \mathbf{0}$ *satisfies* $\mathbf{a}^\perp\mathbf{A} = \mathbf{0}$.
– $\mathcal{O}^*(\tau^*)$ *returns* $\mathbf{K}_0 + \tau^*\mathbf{K}_1$. $\mathcal{A}$ *only gets a single call* τ^* *to* $\mathcal{O}^*$.
– Q *is the number of queries* $\mathcal{A}$ *makes to* $\mathcal{O}_b$.

Proof. We proceed via a series of games. 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, $\tau^* \notin \mathcal{Q}_{\mathrm{tags}} \wedge\ b' = b$. 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. Then, we just 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 (similar to that used in Lemma 2) to bound the advantage for this experiment. Specifically, it suffices to show that 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

$$(\mathsf{pk}, \mathbf{w}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1), \mathbf{K}_0 + \tau^*\mathbf{K}_1) \text{ and } (\mathsf{pk}, \mu\mathbf{a}^\perp + \mathbf{w}^\top(\mathbf{K}_0 + \tau\mathbf{K}_1), \mathbf{K}_0 + \tau^*\mathbf{K}_1) \tag{8}$$

are the same, where $\mathbf{K}_0, \mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times(k+1)}$. (As in Lemma 2, we may use complexity leveraging to handle adaptive choices of τ, τ^*.) 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 $\mathcal{O}_1$. Upon eliminating the terms involving $\mathbf{K}_0 + \tau^*\mathbf{K}_1$, it suffices to show that with probability $1 - 1/q$ over $\mathbf{w} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k+1}$, the following distributions

$$((\tau - \tau^*)\mathbf{w}^\top\mathbf{K}_1, \mathbf{K}_1\mathbf{A}, \mathbf{B}^\top\mathbf{K}_1) \text{ and } (\mu\mathbf{a}^\perp + (\tau - \tau^*)\mathbf{w}^\top\mathbf{K}_1, \mathbf{K}_1\mathbf{A}, \mathbf{B}^\top\mathbf{K}_1)$$

where $\mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times(k+1)}$ are the same. To establish the last statement, let us sample $\mathbf{K}_1$ as $\mathbf{K}' + \mu'\mathbf{b}^{\perp\top}\mathbf{a}^\perp$ where $\mathbf{K}' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times(k+1)}, \mu' \leftarrow_{\mathrm{R}} \mathbb{Z}_q$ and $\mathbf{b}^\perp \neq \mathbf{0}$ satisfies $\mathbf{b}^\perp\mathbf{B} = \mathbf{0}$. Observe that $(\mathbf{K}_1\mathbf{A}, \mathbf{B}^\top\mathbf{K}_1) = (\mathbf{K}'\mathbf{A}, \mathbf{B}^\top\mathbf{K}')$ and that with probability $1 - 1/q$ over $\mathbf{w}$, we have $\mathbf{b}^\perp\mathbf{w} \neq 0$. Fix such a $\mathbf{w}$, and the last statement follows from the fact that for all μ, the following distributions

$$((\tau - \tau^*)\mu'\mathbf{w}^\top\mathbf{b}^{\perp\top}\mathbf{a}^\perp) \text{ and } (\mu\mathbf{a}^\perp + (\tau - \tau^*)\mu'\mathbf{w}^\top\mathbf{b}^{\perp\top}\mathbf{a}^\perp)$$

are the same, where $\mu' \leftarrow_{\mathrm{R}} \mathbb{Z}_q$.

4.2 Our QANIZK Construction

Our protocol Π_{uss} with unbounded simulation soundness for witness sampleable distributions (c.f. Section 3.2) is given in Figure 7. We basically combine Π_{as} with the pseudorandom MAC given in the computational core lemma. The (simulated) proofs, instead of being $[\mathbf{y}^\top \mathbf{K}]_1$ as in Π_{as}, are now given by

$$\left([\mathbf{y}^\top \mathbf{K} + \mathbf{r}^\top \mathbf{B}^\top (\mathbf{K}_0 + \tau \mathbf{K}_1)]_1 , [\mathbf{r}^\top \mathbf{B}^\top]_1\right)$$

Roughly speaking, the pseudo-random MAC allows us to hide partial information about $\mathbf{K}$ across all the simulated proofs, upon which we can use an information-theoretic argument as before.

The WS requirement basically means that we may assume that we know an explicit representation of the matrix $\mathbf{M}$ in the proof of security. For the protocol in Section 3.2, we need an explicit representation of $\mathbf{M}^\perp$ (a basis for the kernel of $\mathbf{M}$) in the proof of security. For the protocol in this section, it suffices to know $[\mathbf{M}^\perp]_2$, with which we can efficiently verify the winning condition for (simulation) soundness; the latter is necessary in order to build a distinguisher for the pseudorandom MAC.

$\underline{\mathsf{Gen}(\mathsf{par}, [\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t})}$:
$\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$
$\mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}; \mathbf{K}_0, \mathbf{K}_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times(k+1)}$
$\mathbf{P} := \mathbf{M}^\top \mathbf{K}; \mathbf{C} := \mathbf{K}\mathbf{A}$
$(\mathbf{C}_0, \mathbf{C}_1) := (\mathbf{K}_0\mathbf{A}, \mathbf{K}_1\mathbf{A}) \in (\mathbb{Z}_q^{(k+1)\times k})^2$
$(\mathbf{P}_0, \mathbf{P}_1) := (\mathbf{B}^\top \mathbf{K}_0, \mathbf{B}^\top \mathbf{K}_1) \in (\mathbb{Z}_q^{k\times(k+1)})^2$
$\mathsf{crs} := ([\mathbf{P}]_1, [\mathbf{C}]_2, [\mathbf{A}]_2, [\mathbf{B}]_1, [\mathbf{C}_0]_2, [\mathbf{C}_1]_2, [\mathbf{P}_0]_1, [\mathbf{P}_1]_1)$
$\mathsf{trap} := \mathbf{K}$
Return $(\mathsf{crs}, \mathsf{trap})$
//crs defines tag-space $\mathcal{T} = \mathbb{Z}_q$

$\underline{\mathsf{Prove}(\mathsf{crs}, \tau, [\mathbf{y}]_1, \mathbf{x})}$: // $\mathbf{y} = \mathbf{M}\mathbf{x}$
$\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k$
$\pi := \left(\left[\mathbf{x}^\top \mathbf{P} + \mathbf{r}^\top (\mathbf{P}_0 + \tau \mathbf{P}_1)\right]_1 , \left[\mathbf{r}^\top \mathbf{B}^\top\right]_1\right) \in (\mathbb{G}_1^{1\times(k+1)})^2$
Return π

$\underline{\mathsf{Verify}(\mathsf{crs}, \tau, [\mathbf{y}]_1, \pi)}$:
Parse $\pi = (\pi_1, \pi_2)$
Check: $e(\pi_1, [\mathbf{A}]_2) = e([\mathbf{y}^\top]_1, [\mathbf{C}]_2) \cdot e(\pi_2, [\mathbf{C}_0 + \tau \mathbf{C}_1]_2)$

$\underline{\mathsf{Sim}_\pi(\mathsf{crs}, \mathsf{trap} = \mathbf{K}, \tau, [\mathbf{y}]_1)}$:
$\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k$
Return $\pi := \left(\left[\mathbf{y}^\top \mathbf{K} + \mathbf{r}^\top (\mathbf{P}_0 + \tau \mathbf{P}_1)\right]_1 , \left[\mathbf{r}^\top \mathbf{B}^\top\right]_1\right)$

Fig. 7. QANIZK Π_{uss} protocol with (adaptive) unbounded simulation-soundness for WS distributions under $\mathcal{D}_k$-MDDH Assumption.

Theorem 4. *Protocol Π_{uss} from Figure 7 is a Quasi-adaptive Non-Interactive Zero Knowledege Argument. Suppose in addition that $\mathcal{D}_{\mathsf{par}}$ is a witness sampleable distribution. Then, under the $\mathcal{D}_k$-MDDH Assumption in $\mathbb{G}_1$ and $\mathcal{D}_k$-KerMDH Assumption in $\mathbb{G}_2$, the protocol has adaptive unbounded simulation soundness.*

Proof. Perfect completeness and perfect zero-knowledge follow readily from the fact that for all $\mathbf{y} = \mathbf{M}\mathbf{x}$ and $\mathbf{P} = \mathbf{M}^\top \mathbf{K}$:

$$\mathbf{x}^\top \mathbf{P} = \mathbf{x}^\top (\mathbf{M}^\top \mathbf{K}) = \mathbf{y}^\top \mathbf{K},$$

along with (7).

We proceed to establish adaptive unbounded simulation soundness. We will show that for any adversary $\mathcal{A}$ that makes at most Q queries to Sim_π, 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

$$\mathbf{Adv}^{\mathrm{uss}}_{\Pi_{\mathsf{uss}}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{B}_0) + 2Q \cdot \mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{B}_1) + (Q+1)/q. \tag{9}$$

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 real experiment from Definition 5.

Game 1. Switch Verify to Verify^*:

$\underline{\mathsf{Verify}^*(\mathsf{crs}, \tau, [\mathbf{y}]_1, \pi):}$
Parse $\pi = (\pi_1, \pi_2)$
Check: $\pi_1 = [\mathbf{y}]_1^\top \mathbf{K} + \pi_2(\mathbf{K}_0 + \tau \mathbf{K}_1)$

To bound $|\mathbf{Adv}_0 - \mathbf{Adv}_1|$, it suffices to bound the probability that $\mathcal{A}$ produces $([\mathbf{y}]_1, \pi_1, \pi_2)$ that passes Verify but not Verify^*. We may rewrite the verification equation in Verify as

$$\begin{aligned} & e(\pi_1, [\mathbf{A}]_2) = e([\mathbf{y}]_1^\top \mathbf{K}, [\mathbf{A}]_2) \cdot e(\pi_2(\mathbf{K}_0 + \tau \mathbf{K}_1), [\mathbf{A}]_2) \\ \iff & e(\pi_1 - [\mathbf{y}]_1^\top \mathbf{K} + \pi_2(\mathbf{K}_0 + \tau \mathbf{K}_1), [\mathbf{A}]_2) = 0 \end{aligned}$$

Observe that for any $([\mathbf{y}]_1, \pi_1, \pi_2)$ that passes Verify but not Verify^*, the value

$$\pi_1 - [\mathbf{y}]_1^\top \mathbf{K} + \pi_2(\mathbf{K}_0 + \tau \mathbf{K}_1) \in \mathbb{G}_1^{1 \times (k+1)}$$

is a non-zero vector in the kernel of $\mathbf{A}$, which is hard to sample under the $\mathcal{D}$-KerMDH assumption. 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 $\mathbf{a}^\perp$ be an element from the kernel of $\mathbf{A}$. Switch Sim_π to Sim^*_π where

$\underline{\mathsf{Sim}^*_\pi(\mathsf{crs}, \mathsf{trap} = \mathbf{K}, \tau, [\mathbf{y}]_1):}$ // adds $\mu \mathbf{a}^\perp$
$\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k; \mu \leftarrow_{\mathrm{R}} \mathbb{Z}_q$
Return $\pi := \left(\left[\mathbf{y}^\top \mathbf{K} + \mu \mathbf{a}^\perp + \mathbf{r}^\top (\mathbf{P}_0 + \tau \mathbf{P}_1) \right]_1, \left[\mathbf{r}^\top \mathbf{B}^\top \right]_1 \right)$

It follows readily from Lemma 3 and the fact that we can efficiently verify the winning condition for $\mathcal{A}$ that

$$|\mathbf{Adv}_1 - \mathbf{Adv}_2| \leq 2Q \mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{B}_1) + Q/q.$$

Basically, we pick $\mathbf{K}$ ourselves and proceed as follows:

- when $\mathcal{A}$ makes a query $(\tau, [\mathbf{y}]_1)$ and $\tau \neq \tau^*$, query $\mathcal{O}_b$ at τ to simulate either Sim_π or Sim^*_π, where $b = 0$ corresponds to Sim_π and $b = 1$ to Sim^*_π;
- when $\mathcal{A}$ makes a query $(\tau, [\mathbf{y}]_1)$ and $\tau = \tau^*$, pick $\mathbf{r} \leftarrow \mathbb{Z}_q^k$, return $\left([\mathbf{y}^\top \mathbf{K} + \mathbf{r}^\top (\mathbf{P}_0 + \tau \mathbf{P}_1)]_1, [\mathbf{r}^\top \mathbf{B}^\top]_1 \right)$;
- we query $\mathcal{O}^*$ at τ^* to simulate Verify^*.

The winning condition of $\mathcal{A}$ can be efficiently verified because $\mathcal{D}_{\mathsf{par}}$ is a witness sampleable distribution: given $[\mathbf{y}]_1$ and $\mathbf{M} \in \mathbb{Z}_q^{n \times t}$ we can verify $[\mathbf{y}]_1 \in \mathcal{L}_{\mathbf{M}} \Leftrightarrow [\mathbf{y}^\top]_1 \mathbf{M}^\perp \neq [\mathbf{0}]_1$.

Game 3. Switch $\mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n \times (k+1)}$ in Gen to $\mathbf{K} := \mathbf{K}' + \mathbf{u}\mathbf{a}^\perp$, where $\mathbf{K}' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n \times (k+1)}, \mathbf{u} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^n$.

We will bound the advantage of the adversary $\mathcal{A}$ in Game 3 via an information-theoretic argument. We first look at what the adversary's view together with $\mathbf{K}'$ leaks about $\mathbf{u}$:

- $\mathbf{C} = (\mathbf{K}' + \mathbf{u}\mathbf{a}^\perp)\mathbf{A} = \mathbf{K}'\mathbf{A}$ completely hides $\mathbf{u}$;
- $\mathbf{P} = \mathbf{M}^\top (\mathbf{K}' + \mathbf{u}\mathbf{a}^\perp)$ leaks $\mathbf{M}^\top \mathbf{u}$;
- the output of Sim^*_π completely hides $\mathbf{u}$, since $\mathbf{y}^\top (\mathbf{K}' + \mathbf{u}\mathbf{a}^\perp) + \mu \mathbf{a}^\perp$ is identically distributed to $\mathbf{y}^\top \mathbf{K}' + \mu \mathbf{a}^\perp$ (namely, $\mathbf{y}^\top \mathbf{u}$ is masked by $\mu \leftarrow_{\mathrm{R}} \mathbb{Z}_q$).

To convince Verify^* to accept a proof (π_1, π_2) on $\mathbf{y}^*$, the adversary must correctly compute

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

and thus $(\mathbf{y}^*)^\top \mathbf{u} \in \mathbb{Z}_q$. Given $\mathbf{M}^\top \mathbf{u}$, for any adaptively chosen $\mathbf{y}^*$ not in the span of $\mathbf{M}$, we have that $(\mathbf{y}^*)^\top \mathbf{u}$ is uniformly random over $\mathbb{Z}_q$ from the adversary's view-point. Therefore, $\mathbf{Adv}_3 \leq 1/q$.

5 Linearly Homomorphic Structure-Preserving Signatures

We show how to extend our QANIZK techniques to LHSPS (linearly homomorphic structure-preserving signature), via a general methodology outlined in Section 1.2. The simplest example of our techniques as applied to the QANIZK protocol Π_{as} from Figure 4 yields a one-time LHSPS, presented in Section A.2. Next, we modify the QANIZK protocol Π_{uss} from Figure 7 into a fully secure LHSPS: we use $\mathsf{sk} = \mathsf{trap}$ and define a signature on $[\mathbf{m}]_1$ as the "simulated proof" $\mathsf{Sim}_\pi(\mathsf{trap}, [\mathbf{m}]_1)$. We only achieve security against targeting adversaries (c.f. Definition 8), namely adversaries for which the winning condition is efficiently verifiable; the latter is necessary in order to build a distinguisher for the pseudorandom MAC in the security proof.

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

$\underline{\mathsf{Sign}(\mathsf{pk}, \mathsf{sk}, \tau, [\mathbf{m}]_1)}$:
$\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k$;
$\sigma := \left(\left[\mathbf{m}^\top\mathbf{K} + \mathbf{r}^\top(\mathbf{P}_0 + \tau\mathbf{P}_1)\right]_1, \left[\mathbf{r}^\top\mathbf{B}^\top\right]_1\right)$
Return $\sigma \in (\mathbb{G}_1^{1\times(k+1)})^2$

$\underline{\mathsf{SignDerive}(\mathsf{pk}, \tau, (\omega_i, \sigma_i)_{1\le i\le \ell})}$:
$\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k$;
Parse $\sigma_i = ([\mathbf{s}_i], [\mathbf{t}_i])$
$\sigma := \left(\left[\mathbf{r}^\top(\mathbf{P}_0 + \tau\mathbf{P}_1) + \sum_{i=1}^{\ell}\omega_i\mathbf{s}_i\right]_1, \left[\mathbf{r}^\top\mathbf{B}^\top + \sum_{i=1}^{\ell}\omega_i\mathbf{t}_i\right]_1\right)$
Return $\sigma \in (\mathbb{G}_1^{1\times(k+1)})^2$

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

Fig. 8. Linearly homomorphic structure-preserving signature $\mathsf{LHSPS}_{\mathsf{full}}$ with message-space $\mathcal{M} = \mathbb{G}_1^n$ and tag-space $\mathcal{T} = \mathbb{Z}_q$.

Theorem 5. *Under the $\mathcal{D}_k$-MDDH Assumption in $\mathbb{G}_1$ and $\mathcal{D}_k$-KerMDH Assumption in $\mathbb{G}_2$, $\mathsf{LHSPS}_{\mathsf{full}}$ from Figure 8 is a linearly homomorphic structure-preserving signature scheme secure against targeting adversaries.*

The proof is similar to that in Theorem 4, with a complication and an additional $1/(Q+1)$ factor security loss arising from the fact that the adversary is allowed to have previously requested signatures for the challenge tag τ^*.

Proof. Perfect correctness and full randomizability are straight-forward. We proceed to establish security against targeting adversaries. 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

$$\mathbf{Adv}^{\mathrm{ufcma-t}}_{\mathsf{LHSPS}_{\mathsf{full}}}(\mathcal{A}) \le (Q+1)(\mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_0) + 2Q\mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) + \frac{Q+1}{q}). \tag{10}$$

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 real experiment from Definition 8.

Game 1. Suppose the adversary makes at most Q queries to SignO with tags $\tau_1, \ldots, \tau_Q$. In addition, 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

$$\mathbf{Adv}_1 \geq \frac{1}{Q+1}\mathbf{Adv}_0.$$

Game 2. Switch Verify to Verify^*:

$\underline{\mathsf{Verify}^*(\mathsf{pk}, \tau, [\mathbf{m}]_1, \sigma)}$:
Parse $\sigma = (\sigma_1, \sigma_2)$
Check: $\sigma_1 = [\mathbf{m}]_1^\top \mathbf{K} + \sigma_2(\mathbf{K}_0 + \tau\mathbf{K}_1)$

As in the proof of Theorem 4, observe that for any $([\mathbf{m}]_1, \sigma_1, \sigma_2)$ that passes Verify but not Verify^*, the value

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

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

$$|\mathbf{Adv}_1 - \mathbf{Adv}_2| \leq \mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_0).$$

Game 3. Switch Sign to Sign^* where

$\underline{\mathsf{Sign}^*(\mathsf{pk}, \mathsf{sk}, \tau, [\mathbf{m}]_1)}$: // adds $\mu\mathbf{a}^\perp$ for $\tau \neq \tau^*$
$\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^k; \mu \leftarrow_{\mathrm{R}} \mathbb{Z}_q$
if $\tau = \tau^*$, $\mu := 0$
Return $\sigma := \left(\left[\mathbf{m}^\top\mathbf{K} + \mu\mathbf{a}^\perp + \mathbf{r}^\top(\mathbf{P}_0 + \tau\mathbf{P}_1)\right]_1, \left[\mathbf{r}^\top\mathbf{B}^\top\right]_1\right)$

As in the proof of Theorem 4, it follows readily from Lemma 3 and the fact that the adversary is targeting that

$$|\mathbf{Adv}_2 - \mathbf{Adv}_3| \leq 2Q\mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) + Q/q$$

Basically, we pick $\mathbf{K}$ ourselves and use $\mathcal{O}_b$ to simulate either Sign or Sign^* for $\tau \neq \tau^*$; compute the signature directly to simulate Sign or Sign^* for $\tau = \tau^*$; and $\mathcal{O}^*$ to simulate Verify^*. The winning condition of $\mathcal{A}$ can be efficiently verified since $\mathcal{A}$ is a targeting adversary.

Game 4. Switch $\mathbf{K} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}$ in Gen to $\mathbf{K} := \mathbf{K}' + \mathbf{u}\mathbf{a}^\perp$, where $\mathbf{K}' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times(k+1)}, \mathbf{u} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^n$.

We will bound the advantage of the adversary in Game 4 via an information-theoretic argument, similar to that in Theorem 4. We first look at what the adversary's view together with $\mathbf{K}'$ leaks about $\mathbf{u}$:

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

To convince Verify^* to accept a signature (σ_1, σ_2) on $\mathbf{m}^*$, the adversary must correctly compute

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

and thus $(\mathbf{m}^*)^\top \mathbf{u} \in \mathbb{Z}_q$. Given $\mathbf{M}_{\tau^*}^\top \mathbf{u}$, for any adaptively chosen $\mathbf{m}^*$ not in the span of $\mathbf{M}_{\tau^*}$, we have that $(\mathbf{m}^*)^\top \mathbf{u}$ is uniformly random over $\mathbb{Z}_q$ from the adversary's view-point. Therefore, $\mathbf{Adv}_4 \leq 1/q$.

Acknowledgments. We thank Fabrice Benhamouda, Olivier Blazy, and Carla Ràfols for helpful discussions on prior works and the reviewers for detailed and constructive feedback.

References

[1] M. Abdalla, F. Benhamouda, and D. Pointcheval. Disjunctions for hash proof systems: New constructions and applications. In *Eurocrypt*, 2015. Also, Cryptology ePrint Archive, Report 2014/483.

[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] J. H. Ahn, D. Boneh, J. Camenisch, S. Hohenberger, a. shelat, and B. Waters. Computing on authenticated data. In R. Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 1–20. Springer, Mar. 2012.

[5] N. Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 557–577. Springer, May 2014.

[6] N. Attrapadung and B. Libert. Homomorphic network coding signatures in the standard model. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 17–34. Springer, Mar. 2011.

[7] N. Attrapadung, B. Libert, and T. Peters. Computing on authenticated data: New privacy definitions and constructions. In X. Wang and K. Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 367–385. Springer, Dec. 2012.

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

[9] 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.

[10] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya. P-signatures and noninteractive anonymous credentials. In R. Canetti, editor, *TCC 2008*, volume 4948 of *LNCS*, pages 356–374. Springer, Mar. 2008.

[11] M. Bellare and S. Goldwasser. New paradigms for digital signatures and message authentication based on non-interative zero knowledge proofs. In G. Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 194–211. Springer, Aug. 1989.

[12] M. Bellare and T. Ristenpart. Simulation without the artificial abort: Simplified proof and improved concrete security for Waters' IBE scheme. In A. Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 407–424. Springer, Apr. 2009.

[13] 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.

[14] M. Blum, P. Feldman, and S. Micali. Non-interactive zero-knowledge and its applications (extended abstract). In *20th ACM STOC*, pages 103–112. ACM Press, May 1988.

[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. Boneh and D. M. Freeman. Homomorphic signatures for polynomial functions. In K. G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 149–168. Springer, May 2011.

[17] D. Boneh and D. M. Freeman. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 1–16. Springer, Mar. 2011.

[18] J. Camenisch, N. Chandran, and V. Shoup. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In A. Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 351–368. Springer, Apr. 2009.

[19] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In C. Cachin and J. Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 207–222. Springer, May 2004.

[20] D. Catalano, D. Fiore, and B. Warinschi. Efficient network coding signatures in the standard model. In M. Fischlin, J. Buchmann, and M. Manulis, editors, *PKC 2012*, volume 7293 of *LNCS*, pages 680–696. Springer, May 2012.

[21] D. Catalano, A. Marcedone, and O. Puglisi. Authenticating computation on groups: New homomorphic primitives and applications. In *Asiacrypt*, pages 193–212, 2014.

[22] 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.

[23] J. Chen, R. Gay, and H. Wee. Improved dual system ABE in prime-order groups via predicate encodings. In *Eurocrypt*, 2015. To appear.

[24] J. Chen and H. Wee. Fully, (almost) tightly secure IBE and dual system groups. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 435–460. Springer, Aug. 2013.

[25] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In H. Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 13–25. Springer, Aug. 1998.

[26] R. Cramer and V. Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In L. R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 45–64. Springer, Apr. / May 2002.

[27] A. De Santis, G. Di Crescenzo, R. Ostrovsky, G. Persiano, and A. Sahai. Robust non-interactive zero knowledge. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 566–598. Springer, Aug. 2001.

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

[29] Y. Dodis, E. Kiltz, K. Pietrzak, and D. Wichs. Message authentication, revisited. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 355–374. Springer, Apr. 2012.

[30] 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.

[31] M. Fischlin, B. Libert, and M. Manulis. Non-interactive and re-usable universally composable string commitments with adaptive security. In D. H. Lee and X. Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 468–485. Springer, Dec. 2011.

[32] D. M. Freeman. Improved security for linearly homomorphic signatures: A generic framework. In M. Fischlin, J. Buchmann, and M. Manulis, editors, *PKC 2012*, volume 7293 of *LNCS*, pages 697–714. Springer, May 2012.

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

[34] R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin. Secure network coding over the integers. In P. Q. Nguyen and D. Pointcheval, editors, *PKC 2010*, volume 6056 of *LNCS*, pages 142–160. Springer, May 2010.

[35] 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.

[36] 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.

[37] J. Groth, R. Ostrovsky, and A. Sahai. Perfect non-interactive zero knowledge for NP. In S. Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 339–358. Springer, May / June 2006.

[38] 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.

[39] 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.

[40] 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.

[41] C. S. Jutla and A. Roy. Relatively-sound NIZKs and password-based key-exchange. In M. Fischlin, J. Buchmann, and M. Manulis, editors, *PKC 2012*, volume 7293 of *LNCS*, pages 485–503. Springer, May 2012.

[42] 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.

[43] 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.

[44] J. Katz and V. Vaikuntanathan. Round-optimal password-based authenticated key exchange. In Y. Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 293–310. Springer, Mar. 2011.

[45] A. B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 318–335. Springer, Apr. 2012.

[46] 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.

[47] 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.

[48] 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.

[49] P. Morillo, C. Ràfols, and J. L. Villar. Matrix computational assumptions in multilinear groups. Manuscript, 2015.

[50] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208. Springer, Aug. 2010.

[51] A. Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In *40th FOCS*, pages 543–553. IEEE Computer Society Press, Oct. 1999.

[52] 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.

[53] B. R. Waters. Efficient identity-based encryption without random oracles. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127. Springer, May 2005.

[54] 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 Appendix

A.1 More efficient QANIZK with one-time simulation soundness for WS distributions

In Figure 9 we give a one-time simulation-sound QANIZK for WS distributions. It is a variant of $\Pi_{\mathsf{ot\text{-}ss}}$ from Figure 9 with shorter proofs as with Π'_{as}. The result is inspired by the prior construction in [1]. Recall that in $\Pi_{\mathsf{ot\text{-}ss}}$, we replaced $\mathbf{K}$ in Π_{as} with a 2-wise independent hash function $\mathbf{K}_0 + \tau\mathbf{K}_1$, which serves also as a one-time MAC. Unfortunately, we cannot apply the same modification to Π'_{as}. Roughly speaking, in the proof of security for Π'_{as}, we need to program $\mathbf{K}$. In the setting for one-time simulation soundness, we would need to program $\mathbf{K}_0 + \tau^*\mathbf{K}_1$, which we cannot do since τ^* is adaptively chosen.

Instead, we replace $\mathbf{K}$ in Π'_{as} with a different 2-wise independent hash function

$$\tau \mapsto \sum\nolimits_{i=1}^{\ell} \mathbf{K}_{i,\tau_i}$$

as in Lamport's one-time signature. As in the security proof for Lamport's one-time signature, we would guess $i' \leftarrow_{\mathrm{R}} [\lambda], b' \leftarrow_{\mathrm{R}} \{0,1\}$ so that $\tau^*_{i'} \neq \tau_{i'}$ and $\tau^*_{i'} = b'$ (such a (i', b') exists since $\tau \neq \tau^*$) and then program $\mathbf{K}_{i',b'}$.

$\underline{\mathsf{Gen}(\mathsf{par}, [\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t})}$:
$\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k; \mathbf{K}_{i,b} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times k}, i = 1, \ldots, \lambda, b = 0, 1$
$\mathbf{P}_{i,b} := \mathbf{M}^\top \mathbf{K}_{i,b}; \mathbf{C}_{i,b} := \mathbf{K}_{i,b}\bar{\mathbf{A}}$
$\mathsf{crs} := ([\mathbf{P}_{i,b}]_1, [\mathbf{C}_{i,b}]_2, [\bar{\mathbf{A}}]_2) \in (\mathbb{G}_1^{t\times k})^{2\lambda} \times (\mathbb{G}_2^{n\times k})^{2\lambda} \times \mathbb{G}_2^{k\times k}$
Return $(\mathsf{crs}, \mathsf{trap} = (\mathbf{K}_{i,b})_{1\le i\le \ell, 0\le b\le 1})$
//crs defines tag-space $\mathcal{T} = \{0,1\}^\lambda$

$\underline{\mathsf{Prove}(\mathsf{crs}, \tau, [\mathbf{y}]_1, \mathbf{x})}$: // $\mathbf{y} = \mathbf{M}\mathbf{x}$
Return $\pi := \left[\mathbf{x}^\top \sum_{i=1}^{\ell} \mathbf{P}_{i,\tau_i}\right]_1 \in \mathbb{G}_1^{1\times k}$

$\underline{\mathsf{Sim}_\pi(\mathsf{crs}, \mathsf{trap} = (\mathbf{K})_{i,b}, \tau, [\mathbf{y}]_1)}$:
Return $\pi := \left[\mathbf{y}^\top \sum_{i=1}^{\ell} \mathbf{K}_{i,\tau_i}\right]_1$

$\underline{\mathsf{Verify}(\mathsf{crs}, \tau, [\mathbf{y}]_1, \pi)}$:
Check: $e(\pi, [\bar{\mathbf{A}}]_2) = e([\mathbf{y}^\top]_1, \left[\sum_{i=1}^{\ell} \mathbf{C}_{i,\tau_i}\right]_2)$

Fig. 9. QANIZK $\Pi'_{\mathsf{ot\text{-}ss}}$ protocol with adaptive one-time simulation-soundness for WS distributions under $\mathcal{D}_k$-KerMDH Assumption.

Theorem 6. *The protocol from Figure 9 is a Quasi-adaptive Non-Interactive Zero Knowledege Argument. Suppose in addition that $\mathcal{D}_{\mathsf{par}}$ is a witness sampleable distribution. Then, under the $\mathcal{D}_k$-KerMDH Assumption in $\mathbb{G}_2$, the protocol has adaptive one-time simulation soundness.*

The proof is similar to that for Theorem 2, along with ideas from the security proof for Lamport's one-time signature scheme.

Proof. Perfect completeness and perfect zero-knowledge are straight-forward as before. We proceed to establish adaptive soundness 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

$$\mathbf{Adv}^{\mathrm{ot\text{-}ss}}_{\Pi'_{\mathsf{ot\text{-}ss}}}(\mathcal{A}) \le \frac{1}{2\lambda}(\mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}) + 1/q).$$

$\mathcal{B}$ begins by choosing $i' \leftarrow_{\mathrm{R}} [\lambda], b' \leftarrow_{\mathrm{R}} \{0,1\}$ and abort later if it is not the case that $\tau^*_{i'} \neq \tau_{i'}$ and $\tau^*_{i'} = b'$. $\mathcal{B}$ then selects $(\mathbf{K}_{i,b})_{1\le i\le \ell, 0\le b\le 1})$ as follows:

– if $(i,b) \neq (i',b')$, pick $\mathbf{K}_{i,b} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times k}$;
– if $(i,b) = (i',b')$, pick $\mathbf{K}' \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{n\times k}$ and implicitly define $\mathbf{K}_{i',b'} = \mathbf{K}' + \mathbf{M}^{\perp}\mathbf{T}_{\mathbf{A}'}$ (as in the proof of Theorem 2). This yields $[\mathbf{C}_{i',b'}]_2 = [(\mathbf{K}'\|\mathbf{M}^{\perp})\cdot\mathbf{A}']_2$.

Suppose $\tau^*_{i'} \neq \tau_{i'}$ and $\tau^*_{i'} = b'$, which happens with probability $\frac{1}{2\lambda}$. Then, $\mathcal{B}$ can simulate Sim_π on τ since it knows $(\mathbf{K}_{i,\tau_i})_{1\le i\le\lambda}$ explicitly. In addition, upon obtaining from $\mathcal{A}$ an accepting proof $\pi = [\mathbf{z}^\top]_1 \in \mathbb{G}_1^{1\times k}$ for τ^* and $[\mathbf{y}]_1 \in \mathbb{G}_1^n$ satisfying $\mathbf{y}^\top\mathbf{M}^{\perp} \neq 0$, we have

$$(\mathbf{z}^\top - \sum\nolimits_{i\neq i'} \mathbf{K}_{i,\tau^*_i})\cdot\overline{\mathbf{A}} = \mathbf{y}^\top\cdot\mathbf{C}_{i',b'} = \mathbf{y}^\top(\mathbf{K}'\|\mathbf{M}^{\perp})\cdot\mathbf{A}'.$$

We may then proceed as in Theorem 2 to extract a solution to the $\mathcal{D}_k$-KerMDH problem.

A.2 One-time Linearly Homomorphic Structure-Preserving Signatures

We now modify the QANIZK protocol Π_{as} from Figure 4 into a one-time structure-preserving linearly homomorphic signature scheme. One-time basically means that the tag space is a singleton set, upon which we may omit the tag from the signature algorithms. Following the general methodology outlined in Section 1.2, we use $\mathsf{sk} = \mathsf{trap}$ and define a signature on $[\mathbf{m}]_1$ as the "simulated proof" $\mathsf{Sim}_\pi(\mathsf{trap}, [\mathbf{m}]_1)$. The scheme can also be seen as a generalization of the one-time LHSPS scheme from [47] from $\mathcal{D}_k = \mathcal{L}_2$ to arbitrary matrix distributions. It serves as a warm-up for our unbounded construction in the next section.

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

Fig. 10. One-time linearly homomorphic structure-preserving signature $\mathsf{LHSPS}_{\mathsf{ot}}$ with message-space $\mathcal{M} = \mathbb{G}_1^n$.

Theorem 7. *Under the $\mathcal{D}_k$-KerMDH Assumption in $\mathbb{G}_2$, $\mathsf{LHSPS}_{\mathsf{ot}}$ from Figure 10 is a one-time linearly homomorphic structure-preserving signature scheme.*

The proof of Theorem 7 is essentially the same as the one of Theorem 1 with the difference that $[\mathbf{P}]_1 = [\mathbf{M}^\top\mathbf{K}]_1$ from crs of Π_{as} is being constructed adaptively "on the fly", where $\mathbf{M} = (\mathbf{m}_1,\ldots,\mathbf{m}_q) \in \mathbb{Z}_q^{n\times q}$ and $[\mathbf{m}_i]_1 \in \mathbb{Z}_q^n$ is the message of the i-th signing query. (This adaptivity is also the reason why one cannot use the more efficient QANIZK protocol Π'_{as} from Figure 5.)

Proof. Perfect correctness and full randomizability are straight-forward. We proceed to establish 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

$$\mathbf{Adv}^{\mathrm{ufcma}}_{\mathsf{LHSPS}_{\mathsf{ot}}}(\mathcal{A}) \le \mathbf{Adv}^{\mathrm{kmdh}}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}) + 1/q. \tag{11}$$

Adversary $\mathcal{B}(\mathcal{PG}, [\mathbf{A}]_2 \in \mathbb{G}_2^{(k+1)\times k})$ generates pk as in the real scheme by picking $\mathbf{K} \in \mathbb{Z}_q^{n\times(k+1)}$. Next, $\mathcal{B}$ runs $\mathcal{A}$ on pk, answers signing queries on messages $[\mathbf{m}_1]_1, \ldots, [\mathbf{m}_Q]_1$ as in the real scheme using $\mathbf{K}$, and obtains a signature $\sigma = [\mathbf{z}^\top]_1 \in \mathbb{G}_1^{1\times k}$ on $[\mathbf{m}^*]_1 \in \mathbb{G}_1^n$ such that $\mathbf{m}^* \notin \mathit{span}(\mathbf{M})$, where $\mathbf{M} = (\mathbf{m}_1, \ldots, \mathbf{m}_Q) \in \mathbb{Z}_q^{n\times Q}$. Finally, $\mathcal{B}$ returns $[\mathbf{s}]_1$ computed as

$$\mathbf{s}^\top = \mathbf{z}^\top - \mathbf{m}^{*\top}\mathbf{K}.$$

As before in Theorem 7, $\mathbf{s}^\top\mathbf{A} = \mathbf{0}$ and $\Pr[\mathbf{s} = \mathbf{0}] \leq 1/q$ by Lemma 2, since the signing queries only leak $\mathbf{M}^\top\mathbf{K}$. This proves equation (11).