Matrix Computational Assumptions in Multilinear Groups

Paz Morillo[1], Carla Ràfols[2], and Jorge L. Villar[1⋆]

[1] Universitat Politècnica de Catalunya, Spain
{paz,jvillar}@ma4.upc.edu
[2] Horst Görtz Institut für IT Sicherheit, Ruhr-Universität Bochum, Germany
carla.rafols@rub.de

Abstract. We put forward a new family of computational assumptions, the Kernel Matrix Diffie-Hellman Assumption. This family abstracts and includes as a special case several assumptions used in the literature under different names. Given some matrix $\mathbf{A}$ sampled from some distribution $\mathcal{D}_{\ell,k}$, the kernel assumption says that it is hard to find "in the exponent" a nonzero vector in the kernel of $\mathbf{A}^\top$. Our assumption is the natural computational analogue of the Matrix Decisional Diffie-Hellman Assumption (MDDH), proposed by Escala *et al.*

We show that the $\mathcal{D}_{\ell,k}$ Kernel DH Assumption is a strictly increasing family of weaker computational assumptions when k grows. This requires ruling out the existence of some black-box reductions between flexible problems (*i.e.*, computational problems with a non unique solution), which is specially subtle. As opposed to the decisional MDDH Assumption, our kernel assumption might hold in the recent candidate multilinear groups.

Kernel assumptions have implicitly been used in recent works on QA-NIZK and structure-preserving signatures. We also provide a new construction of commitments to group elements in the multilinear setting, based on any kernel assumption.

1 Introduction

It is always desirable to base security of cryptographic protocols on the weakest possible assumptions, like discrete logarithm or factoring. Although this is possible in many scenarios, it usually limits either the efficiency or the functionality of the protocols. This is the main reason why stronger assumptions like DDH are broadly used. However, such a strong assumption is not always true, like in the case of symmetric bilinear groups. Therefore, it is important to have a thorough understanding of the hardness of computational assumptions and the relations among them.

This issue has been treated extensively in the cryptographic literature, *i.e.*, in [6,17,24,25,26,27,28] just to name a few. On the computational side, many of the proposed assumptions are often shown to be equivalent [6,17,27]. Typically, most computational problems related to prime order groups are equivalent or reducible to CDH. However, on the stronger side, it is difficult to find relations between decisional assumptions [6,10,11,27] which makes it hard to compare the security achieved by different cryptographic protocols based on different assumptions.

On the other hand, security notions can be classified mainly in hiding and unforgeability ones. The former typically appear in encryption schemes and commitments, while the latter corresponds to signature schemes and soundness in zero knowledge proofs. Although it is theoretically possible to base the hiding property on computational problems, most of the practical schemes achieve this notion either information theoretically or based on decisional assumptions, at least in the standard model. Likewise, unforgeability naturally comes from computational assumptions (obviously implied by stronger decisional assumptions).

Most computational problems considered in the literature are search problems with a unique solution like discrete logarithm or CDH. But, unforgeability actually means the inability to produce one among many solutions to a given problem (*e.g.*, in many signature schemes or zero knowledge proofs). Thus, unforgeability is more naturally captured by a *flexible computational problem*, namely, a problem which admits several solutions. Unfortunately, flexible problems have received less attention until recently

⋆ This work has been partially supported by the Spanish research project MTM2013-41426-R.

[2,7,9,14,15,21,23]. This is probably due to the difficulty of finding reductions among them, or even fully understanding the meaning of a black-box reduction between two flexible problems.

A better knowledge and understanding flexible problems, which are weaker than non-flexible computational ones and harder than decisional ones would have a great impact on the design of efficient signature and zero knowledge protocols with extended functionalities, similarly what happened with decisional problems and encryption schemes.

Recently, Escala *et al.* [12] have put forward a new family of decisional assumptions in a prime order group $\mathbb{G}$, the *Matrix Diffie-Hellman* Assumption ($\mathcal{D}_{\ell,k}$-MDDH). The assumption says that given some matrix $\mathbf{A} \in \mathbb{Z}_q^{\ell \times k}$ sampled from some matrix distribution $\mathcal{D}_{\ell,k}$, it is hard to decide membership in $\operatorname{Im} \mathbf{A}$ in "the exponent". Rather than as a new assumption, the Matrix DH Assumption should be seen as an algebraic framework for describing several decisional assumptions which includes as a special case the widely used k-Lin family of assumptions. This abstraction is useful in several ways. First, schemes based on any $\mathcal{D}_{\ell,k}$-MDDH Assumption, tend to highlight the algebraic structure of the construction. Further, many instantiations of the given scheme can be written in a compact way. This abstraction points out to a tradeoff between security and efficiency, since on one hand, the uniform assumption is the weakest of all possible assumptions but has the worst representation size, while the symmetric cascade has optimal representation size but is a stronger assumption.

In this paper we propose a computational analogue of the Matrix DH Assumption: the *Kernel Matrix DH Assumption*. This new flexible assumption states that it is hard to find "in the exponent" an element in the kernel of a matrix $\mathbf{A}^\top$, for $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$. For some special instances of $\mathcal{D}_{\ell,k}$, these assumptions have appeared in the literature under different and sometimes confusing names.

Our new algebraic framework is useful to abstract and understand existing constructions of schemes in the literature, leading to simplified/more efficient constructions of existing schemes or to new constructions based on weaker computational assumptions, as in the decisional case. For instance, the recent paper of Jutla and Roy [19] presents a construction of a QA-NIZK of size k based on a variant of the decisional k-Lin assumption. A close look at the proof reveals that in fact it is actually based on an instance of our kernel assumption, which is weaker. Recently, Kiltz and Wee [20] have shown that one can achieve the same functionality based on the kernel assumption for any matrix distribution.

Matrix DH Assumptions are a natural match for a recent line of work on structure-preserving cryptography [1,2,5,22]. In a structure-preserving cryptographic primitive defined over some group G, essentially all the elements are group elements. Thus, most algorithms of some structure preserving primitive admit a natural algebraic interpretation. For instance, in a structure-preserving signature scheme, both the verification key and the message are group elements. A signature which verifies the verification equation can be naturally interpreted as an orthogonal vector to some public information [5]. This has naturally led to lower bounds on the size of a structure preserving signature. Recent works on structure-preserving signatures and QA-NIZK proofs of membership in linear spaces use assumptions which are special cases of our new family of kernel assumptions.

Our Results. We define a new class of flexible problems over a primer order group, *Kernel Matrix DH Problem*, inspired by the matrix DDH family. Indeed, for any matrix distribution $\mathcal{D}_{\ell,k} \subset \mathbb{Z}_q^{\ell \times k}$, we define the $\mathcal{D}_{\ell,k}$-KerMDH problem, which is the natural computational version of $\mathcal{D}_{\ell,k}$-MDDH problem, defined in [12], since the former is reducible to the latter, as happens with CDH and DDH. We show the new class includes, as particular instances, the problems introduced in [2,9,14,15,21,23]. We also present a generalization of the kernel problem in multilinear maps where the solution must be in one of the intermediate groups.

We also propose new interesting families. Namely, we define the circulant matrix distribution, $\mathcal{CI}_{k,d}$, which generalizes the $\mathcal{SC}_k$ in [12] to the case $\ell = k+d > k+1$ and we prove its generic hardness in k-linear maps. We prove that it has optimal representation size d independent of k (even in multilinear groups), which is an important parameter for applications. The case $\ell > k+1$ typically arises when one considers commitments/encryption in which the message is a vector of group elements instead of a single group element and the representation size of the assumptions typically affects the size of the public parameters. Analyzing the security of a family of decisional assumptions (depending on a parameter k) can be rather involved. This is why in [12], the authors gave a criterion for generic hardness when $\ell = k+1$ in terms of

irreducibility of some polynomials involved in the description of the assumption. This criterion was used then to prove the generic hardness of several families of assumptions. To analyze the generic hardness of the $\mathcal{CI}_{k,d}$ for any k, we need to extend the techniques of [12] to the case $\ell > k+1$. To the best of our knowledge, the generic hardness criterion of [12] was not used so far to analyze families of assumptions in this case.

Then we show that the families of matrix distributions in [12], $\mathcal{U}_{\ell,k}$, $\mathcal{L}_k$, $\mathcal{SC}_k$, $\mathcal{C}_k$ and $\mathcal{RL}_k$, as well as $\mathcal{CI}_{k,d}$, define families of kernel problems with strictly increasing hardness. That is, we show reduction from the smaller to the larger problems in each family, likewise we prove that there is no black-box meta-reduction from the larger to the smaller problems in the multilinear generic group model.

The last step requires dealing with the notion of black-box reduction between flexible problems. A black-box reduction must work for any possible behavior of the oracle, but, on the contrary to the normal (unique answer) black-box reductions, here the oracle has to choose among the set of valid answers in every call. Ruling out the existence of a reduction implies that for any reduction there is an oracle behavior for which the reduction fails. This is specially subtle when dealing with multiple oracle calls. The proof technique used in this paper can be considered as a contribution in itself as it can potentially be used in future works.

We show that the kernel assumption is not only generically hard in k-linear maps, but we also discuss if in the current candidate k-linear maps [13], the assumption is not immediately broken. We propose it as a candidate for a computational assumption in k-linear maps.

We then show how to construct commitments to any element in level $m < k$ in k-linear groups under the kernel assumption for any matrix distribution, generalizing the Pedersen commitment and the commitment in Abe *et al.* [2]. In particular when the construction is instantiated with the new circulant matrix distribution we have commitments with very short representation size.

2 Preliminaries

For $\lambda \in \mathbb{N}$, we write 1^λ for the string of λ ones. For a set S, $s \leftarrow S$ denotes the process of sampling an element s from S uniformly at random. For an algorithm $\mathcal{A}$, we write $z \leftarrow \mathcal{A}(x, y, \ldots)$ to indicate that $\mathcal{A}$ is a (probabilistic) algorithm that outputs z on input $(x, y, \ldots)$.

2.1 Multilinear Maps

Let Gen be a probabilistic polynomial time (PPT) algorithm that on input 1^λ returns a description $\mathcal{G} = (\mathbb{G}, q, \mathcal{P})$ of a cyclic group $\mathbb{G}$ of order q for a λ-bit prime q and a generator $\mathcal{P}$ of $\mathbb{G}$.

For any fixed $k \geq 1$, let MGen_k be a PPT algorithm that on input 1^λ returns a description of an (ideal) graded encoding $\mathcal{MG}_k = (e, \mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k, q, \mathcal{P}_1, \ldots, \mathcal{P}_k)$, where $\mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k$ are cyclic groups of prime-order q, $\mathcal{P}_i$ is a generator of $\mathbb{G}_i$ and e is a non-degenerate efficiently computable bilinear map. Sometimes $\mathbb{G}_0$ is used to refer to $\mathbb{Z}_q$. For group elements we use the following implicit notation: for all $i = 1, \ldots, k$, $[a]_i := a\mathcal{P}_i$. The notation extends in a natural way to vectors and matrices and to linear algebra operations. We sometimes drop the index when referring to elements in $\mathbb{G}_1$, *i.e.*, $[a] := [a]_1 = a\mathcal{P}_1$. The map e is defined as $e([a]_i, [b]_j) = [ab]_{i+j}$, for all i, j such that $i + j \leq k$.

Additionally, let AGen_2 be a PPT algorithm that on input 1^λ returns a description of an asymmetric bilinear map $\mathcal{AG}_2 = (e, \mathbb{G}, \mathbb{H}, \mathbb{T}, q, \mathcal{P}, \mathcal{Q})$, where $\mathbb{G}, \mathbb{H}, \mathbb{T}$ are cyclic groups of prime-order q, $\mathcal{P}$ is a generator of $\mathbb{G}$, $\mathcal{Q}$ is a generator of $\mathbb{H}$ and $e : \mathbb{G} \times \mathbb{H} \to \mathbb{T}$ is a non-degenerate, efficiently computable bilinear map. In this case we refer to group elements as: $[a]_G := a\mathcal{P}$, $[a]_H := a\mathcal{Q}$ and $[a]_T := e(\mathcal{P}, \mathcal{Q})^a$.

2.2 The Matrix Decisional Diffie-Hellman Assumption

We recall here the definition of the decisional assumptions introduced in [12], which are the starting point of our flexible computational matrix problems.

Definition 1. *[12], Let $\ell, k \in \mathbb{N}$ with $\ell > k$. We call $\mathcal{D}_{\ell,k}$ a matrix distribution if it outputs (in polynomial time, with overwhelming probability) matrices in $\mathbb{Z}_q^{\ell \times k}$ of full rank k. We denote $\mathcal{D}_k := \mathcal{D}_{k+1,k}$.*

Definition 2 ($\mathcal{D}_{\ell,k}$-MDDH Assumption). *[12] Let $\mathcal{D}_{\ell,k}$ be a matrix distribution. We say that the $\mathcal{D}_{\ell,k}$-Matrix Diffie-Hellman ($\mathcal{D}_{\ell,k}$-MDDH) Assumption holds relative to* Gen *if for all PPT adversaries $\mathcal{D}$,*

$$\mathbf{Adv}_{\mathcal{D}_{\ell,k},\mathsf{Gen}}(\mathcal{D}) = \Pr[\mathcal{D}(\mathcal{G},[\mathbf{A}],[\mathbf{A}\boldsymbol{w}])=1] - \Pr[\mathcal{D}(\mathcal{G},[\mathbf{A}],[\boldsymbol{u}])=1] \in negl(\lambda),$$

where the probability is taken over $\mathcal{G}=(\mathbb{G},q,\mathcal{P}) \leftarrow \mathsf{Gen}(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}, \boldsymbol{w} \leftarrow \mathbb{Z}_q^k, \boldsymbol{u} \leftarrow \mathbb{Z}_q^\ell$ and the coin tosses of adversary $\mathcal{D}$.

Definition 3. *A matrix distribution $\mathcal{D}_{\ell,k}$ is hard if the corresponding $\mathcal{D}_{\ell,k}$-MDDH problem is hard in the generic k-linear group model.*

(A)symmetric Multilinear Groups. In this paper we will consider both symmetric and asymmetric k-linear groups. In the symmetric case, we will say that the $\mathcal{D}_{\ell,k}$-MDDH Assumption holds relative to $\mathcal{G}=(\mathbb{G},q,\mathcal{P})$ when the distribution of $\mathcal{G}$ is the one induced by running the symmetric bilinear map generator. In the asymmetric case, we will say that the $\mathcal{D}_{\ell,k}$-MDDH Assumption holds in the left (similarly, in the right) if it holds in the group $\mathbb{G}$ (similarly in $\mathbb{H}$) with the distribution of the group $\mathbb{G}$ being the one induced by the asymmetric bilinear map generator AGen_2.

2.3 Examples of $\mathcal{D}_{\ell,k}$-MDDH

Some particular families of matrix distributions were presented in [12]. Namely,

$$\mathcal{SC}_k : \mathbf{A} = \begin{pmatrix} a & & 0 \\ 1 & \ddots & \\ & \ddots & a \\ 0 & & 1 \end{pmatrix} \quad \mathcal{C}_k : \mathbf{A} = \begin{pmatrix} a_1 & & 0 \\ 1 & \ddots & \\ & \ddots & a_k \\ 0 & & 1 \end{pmatrix} \quad \mathcal{L}_k : \mathbf{A} = \begin{pmatrix} a_1 & \cdots & 0 \\ & & \\ 0 & & a_k \\ 1 & \cdots & 1 \end{pmatrix},$$

where $a, a_i \leftarrow \mathbb{Z}_p$, and $\mathcal{U}_{\ell,k}$ which is simply the uniform distribution in $\mathbb{Z}_p^{\ell\times k}$. The $\mathcal{SC}_k$-MDDH Assumption is the Symmetric Cascade Assumption, the $\mathcal{C}_k$-MDDH Assumption is the Cascade Assumption, which were proposed for the first time. $\mathcal{U}_{\ell,k}$-MDDH and $\mathcal{L}_k$-MDDH were implicitly used in some previous works. Actually, $\mathcal{L}_k$-MDDH is the Decisional Linear Assumption in [8].

2.4 Computational Assumptions in Multilinear Groups

In this section we recall some computational problems in the cryptographic literature, that appear as unrelated but we unify as particular instances of our framework. There is some confusion about the terminology for the problems listed below. In this section we merely write the computational problems as they appear in the literature.

Definition 4. *In the following, all parameters a_i and b_i are assumed to be randomly chosen in $\mathbb{Z}_q$.*

1. *Find-Rep [9]: Given $([a_1],\ldots,[a_\ell])$, find a nonzero tuple $(x_1,\ldots,x_\ell)$ such that $x_1a_1+\ldots+a_\ell x_\ell = 0$.*
2. *Simultaneous Double Pairing (SDP) [2]: Given the two tuples, $([a_1],[b_1])$ and $([a_2],[b_2])$, find a nonzero tuple $([x_1],[x_2],[x_3])$ such that $x_1b_1+x_2a_1=0$, $x_1b_2+x_3a_2=0$.*
3. *Simultaneous Triple Pairing [14]: Given the two tuples, $([a_1],[a_2],[a_3])$ and $([b_1],[b_2],[b_3])$, find a nonzero tuple $([x_1],[x_2],[x_3])$ such that $x_1a_1+x_2a_2+x_3a_3=0$, $x_1b_1+x_2b_2+x_3b_3=0$.*
4. *Simultaneous Pairing [15]: Given $([a_1],[a_2],\ldots,[a_\ell])$ and $([a_1^2],[a_2^2],\ldots,[a_\ell^2])$, find a nonzero tuple $([x_1],\ldots,[x_\ell])$ such that $\sum_{i=1}^\ell x_ia_i=0$, $\sum_{i=1}^\ell x_ia_i^2=0$.*
5. *1-Flexible Diffie-Hellman (1-FlexDH) [23]: Given $([1],[a],[b])$, find a triple $([r],[ra],[rab])$ with $r\neq 0$.*
6. *1-Flexible Square Diffie-Hellman (1-FlexSDH) [21]: Given $([1],[a])$, find a triple $([r],[ra],[ra^2])$ with $r\neq 0$.*
7. *ℓ-Flexible Diffie-Hellman (ℓ-FlexDH) [23]: Given $([1],[a],[b])$, find a $(2\ell+1)$-tuple $([r_1],\ldots,[r_\ell],[r_1a],[r_1r_2a],\ldots,[(\prod_{i=1}^\ell r_i)a],[(\prod_{i=1}^\ell r_i)ab])$ such that $r_j\neq 0$ for all $j=1,\ldots,\ell$.*
8. *Double Pairing (DP) [14]: In an asymmetric group $(\mathbb{G},\mathbb{H},\mathbb{T})$, given a pair of random elements $([a_1]_H,[a_2]_H)\in\mathbb{H}^2$, find a nonzero tuple $([x_1]_G,[x_2]_G)$ such that $[x_1a_1+x_2a_2]_T=[0]_T$.*

3 New Matrix DDH Assumptions

In this section we give examples of matrix distributions which did not appear in [12]. The two distributions given in the next definition appear naturally when one considers the natural decisional versions of the computational problems 2 and 4 in Definition 4.

Definition 5. *The Randomized Linear and the Square Polynomial distributions are:*

$$\mathcal{RL}_k : \mathbf{A} = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_k \\ b_1 & \cdots & b_k \end{pmatrix} \qquad \mathcal{P}_{\ell,2} : \mathbf{A} = \begin{pmatrix} a_1 & a_1^2 \\ a_2 & a_2^2 \\ \vdots & \vdots \\ a_\ell & a_\ell^2 \end{pmatrix}$$

where $a_i \leftarrow \mathbb{Z}_q$ *and* $b_i \leftarrow \mathbb{Z}_q^\times$.

Jutla and Roy [19] referred to $\mathcal{RL}_k$-MDDH Assumption as the k-lifted Assumption. From the results in Section 4.5 it is easy to see that $\mathcal{RL}_k$ is a hard matrix distribution. The hardness of the $\mathcal{P}_{\ell,2}$ matrix distribution is partially analyzed, under the name of Simultaneous Pairing Assumption, by Groth and Lu [15]. However, they actually prove that the associated flexible problem ($\mathcal{P}_{\ell,2}$-KerMDH, in our notation) is generically hard.

For some applications it would be useful having at hand some $\mathcal{D}_{\ell,k}$-MDDH assumptions in which $\ell > k+1$, and for this case, the only example considered in [12] is one corresponding to the uniform matrix distribution $\mathcal{U}_{\ell,k}$. Although every other $\mathcal{D}_{\ell,k}$-MDDH problem reduces to the $\mathcal{U}_{\ell,k}$-MDDH problem, it is also interesting to have matrix distributions with a smaller description size. A natural way to construct such a distribution is to pick one of the known distributions $\mathcal{D}_{k+1,k}$ (*e.g.*, $\mathcal{L}_k$) and add $\ell - k - 1$ new random rows. It can be easily seen that the obtained $\mathcal{D}_{\ell,k}$-MDDH assumption is equivalent to the original $\mathcal{D}_{k+1,k}$-MDDH assumption. Again, for efficiency reasons, we are interested in matrix distributions with an even smaller representation size. This motivates us to introduce a new family of matrix distributions, the $\mathcal{CI}_{k,d}$ family.

Definition 6 (Circulant Matrix Distribution). *We define the distribution* $\mathcal{CI}_{k,d}$ *as follows*

$$\mathbf{A} = \begin{pmatrix} a_1 & & & 0 \\ \vdots & a_1 & & \\ a_d & \vdots & \ddots & \\ 1 & a_d & & a_1 \\ & 1 & \ddots & \vdots \\ & & \ddots & a_d \\ 0 & & & 1 \end{pmatrix} \in \mathbb{Z}_q^{(k+d)\times k}, \qquad \text{where } a_i \leftarrow \mathbb{Z}_q$$

Matrix $\mathbf{A}$ is such that each column can be obtained by rotating one position the previous column, which explains the name. Notice that when $d = 1$, $\mathcal{CI}_{k,d}$ is exactly the symmetric cascade distribution $\mathcal{SC}_k$, introduced in [12].

Following [16, Thm. 5.15 and corollaries], for the special case that all matrices produced by the matrix distribution are full-rank, we can prove that $\mathcal{CI}_{k,d}$ is a hard matrix distribution. Indeed, an algorithm solving the $\mathcal{CI}_{k,d}$-MDDH problem in the generic k-linear group model must be able to compute a polynomial in the ideal $\mathfrak{H} \subset \mathbb{Z}_q[a_1, \ldots, a_d, z_1, \ldots, z_{k+d}]$ generated by all the $(k+1)$-minors of $\mathbf{A}\|\boldsymbol{z}$ as polynomials in $a_1, \ldots, a_d, z_1, \ldots, z_{k+d}$. Although this ideal can actually be generated using only a few of the minors, we need to build a Gröbner basis of $\mathfrak{H}$ to reason about the minimum degree a nonzero polynomial in $\mathfrak{H}$ can have. We show that, carefully selecting a monomial order, the set of all $(k+1)$-minors of $\mathbf{A}\|\boldsymbol{z}$ form a Gröbner basis, and all these minors have total degree exactly $k+1$. Therefore, all nonzero polynomials in $\mathfrak{H}$ have degree at least $k+1$, and then they cannot be evaluated by any algorithm in the generic k-linear group model.

On the other hand, it can also be shown that the representation size of $\mathcal{CI}_{k,d}$, which is the number of parameters d, is the optimal among all hard matrix distributions $\mathcal{D}_{k,k+d}$ defined by linear polynomials in the parameters. The proofs of optimality and generic hardness of $\mathcal{CI}_{k,d}$ can be found in the appendix.

4 The Matrix Diffie-Hellman Computational Problems

In this section we introduce two families of search problems naturally related to the Matrix Decisional Diffie-Hellman problems. Given a matrix distribution, $\mathcal{D}_{\ell,k}$, the first family consists of the problems of given a matrix $[\mathbf{A}]$, where $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, and the first k components of a vector $[\boldsymbol{z}]$, complete it so that $\boldsymbol{z} \in \operatorname{Im} \mathbf{A}$. The second family consists of the problems of finding $[\boldsymbol{x}]$ such that $\boldsymbol{x} \in \ker \mathbf{A}^\top \setminus \{\mathbf{0}\}$. It is noticeable that the computational problems listed in Definition 4 are particular cases of this second family.

We next show that any solution of the new search problems is enough to solve the corresponding decisional MDDH problem. Finally, we study the existence of reductions between the kernel problems for the matrix distributions previously given: for different sizes within the same distribution, and also between different distributions with the same size.

Definition 7 ($\mathcal{D}_{\ell,k}$-MCDH). *Given a matrix distribution $\mathcal{D}_{\ell,k}$ in a group $\mathbb{G}$, the computational matrix Diffie-Hellman Problem is given $([\mathbf{A}], [\boldsymbol{z}_0])$, with $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, $\boldsymbol{z}_0 \leftarrow \mathbb{Z}_q^k$, compute $[\boldsymbol{z}_1] \in \mathbb{G}^{\ell-k}$ such that $(\boldsymbol{z}_0 \| \boldsymbol{z}_1) \in Im\, \mathbf{A}$.*

Notice that CDH and the computational k-Lin problems are particular examples of MCDH problems. Namely, CDH is exactly $\mathcal{L}_1$-MCDH and the computational k-Lin problem is $\mathcal{L}_k$-MCDH. MCDH are computational problems with unique solution. It appears naturally when using MDDH Assumptions, for instance, the one-wayness of the encryption scheme in [12] is equivalent to this problem. However, this problem amounts to computing some polynomial on the elements of $\mathbf{A}$ and it is equivalent to CDH ([6,17]), although the tightness of the reduction depends on the degree of these polynomials.

The second family is more interesting. It is a family of flexible problems. Flexible computational problems are the natural way to model the adversarial capability is some scenarios like unforgeability, and finding reductions between flexible problems is not an obvious task. This new problem family is closely related to the various flavors of "simultaneous pairing" assumptions in the literature.

Definition 8 ($\mathcal{D}_{\ell,k}$-KerMDH). *Given a matrix distribution $\mathcal{D}_{\ell,k}$ in a group $\mathbb{G}$, the Kernel Diffie-Hellman Problem is given $[\mathbf{A}]$, with $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, find a nonzero vector $[\boldsymbol{x}] \in \mathbb{G}^\ell$ such that $\boldsymbol{x}$ is orthogonal to $Im\, \mathbf{A}$, that is, $\boldsymbol{x} \in \ker \mathbf{A}^\top \setminus \{\mathbf{0}\}$.*

Note that one can efficiently test if a vector $[\boldsymbol{x}]$ is a solution to the problem KerMDH in a bilinear group, by checking whether $e([\boldsymbol{x}^\top], [\mathbf{A}]) = [\mathbf{0}]_2$.

Definition 8 naturally generalizes to asymmetric bilinear groups. There, given $[\mathbf{A}]_H$, the problem is to find $[\boldsymbol{x}]_G$ such that $\boldsymbol{x} \in \ker \mathbf{A}^\top \setminus \{\mathbf{0}\}$. A solution can be obviously verified by checking if $e([\boldsymbol{x}^\top]_G, [\mathbf{A}]_H) = [\mathbf{0}]_T$. We can also consider a generalization of this problem in which the goal is to solve the same problem but giving the solution in a different group $\mathbb{G}_r$, in some ideal graded encoding $\mathcal{MG}_m$, for some $0 \leq r \leq \min(m, k-1)$. The case $r = 1$ corresponds to the previous problem defined in a m-linear group.

Definition 9 ($(r, m, \mathcal{D}_{\ell,k})$-KerMDH). *Given a matrix distribution $\mathcal{D}_{\ell,k}$ over a m-linear group $\mathcal{MG}_m$ and r an integer $0 \leq r \leq \min(m, k-1)$, the $(r, m, \mathcal{D}_{\ell,k})$-KerMDH Problem is to find $[\boldsymbol{x}]_r \in \mathbb{G}_r^\ell$ such that $\boldsymbol{x} \in \ker \mathbf{A}^\top \setminus \{\mathbf{0}\}$.*

When the precise degree of multilinearity m is not an issue, we will write $(r, \mathcal{D}_{\ell,k})$-KerMDH instead of $(r, m, \mathcal{D}_{\ell,k})$-KerMDH, for any $m \geq r$.

Again, we note that if $m \geq r+1$ one can efficiently test if a vector $[\boldsymbol{x}]_r$ solves the $(r, m, \mathcal{D}_{\ell,k})$-KerMDH by checking whether $e([\boldsymbol{x}^\top]_r, [\mathbf{A}]) = [\mathbf{0}]_{r+1}$. However, if $m = r$ the solution of the problem cannot be checked as it would require the use of a $(m+1)$-linear map.

Notice that we do not consider the case $r \geq k$ because it makes the problem easy.

Lemma 1. *The* $(r, m, \mathcal{D}_{\ell,k})$-KerMDH *Problem for* $k \leq r \leq m$ *is easy.*

Proof. If $\ell = k+1$, a solution to the problem is the vector $[(A_1, -A_2, \ldots, (-1)^k A_{k+1})]_r$ where A_i is the minor of $\mathbf{A}$ obtained by deleting the i-th row, computed by means of the m-linear map, as $m \geq r$. In the case $\ell > k+1$ the solution can be obtained with a similar trick applied to any full-rank $(k+1) \times k$ submatrix of $\mathbf{A}$.

4.1 Decisional vs. Computational Matrix Problems

In this section we detail the relation between the new search problems given in definitions 7 and 8 and the Matrix Decisional Diffie-Hellman Problems. Specifically, any solution to the computational problems allows to tell apart the real and the random instances of the corresponding MDDH problem.

The first lemma states the obvious relation between MCDH and MDDH.

Lemma 2. *In a* k*-linear group,* $\mathcal{D}_{\ell,k}$-MDDH $\Rightarrow$ $\mathcal{D}_{\ell,k}$-MCDH.

The kernel problem is also harder than the corresponding decisional problem, in multilinear groups.

Lemma 3. *In a* m*-linear group with* $m \geq 2$, $\mathcal{D}_{\ell,k}$-MDDH $\Rightarrow$ $\mathcal{D}_{\ell,k}$-KerMDH.

Proof. Given an instance of the $\mathcal{D}_{\ell,k}$-MDDH problem $([\mathbf{A}], [\boldsymbol{z}])$, a solution to test membership in $\operatorname{Im} \mathbf{A}$ is simply checking whether $e([\boldsymbol{x}^\top], [\boldsymbol{z}]) = [\boldsymbol{x}^\top \boldsymbol{z}]_2 \stackrel{?}{=} [0]_2$, where $[\boldsymbol{x}]$ is the output of the $\mathcal{D}_{\ell,k}$-KerMDH solver on input $[\mathbf{A}]$.

Analogously, we have

Lemma 4. *In a* m*-linear group,* $\mathcal{D}_{\ell,k}$-MDDH $\Rightarrow$ $(r, m, \mathcal{D}_{\ell,k})$-KerMDH *for any* $0 \leq r \leq m-1$.

4.2 The Kernel DH Assumptions in Real Multilinear Maps

We have shown that for any hard matrix distribution $\mathcal{D}_{\ell,k}$ the $\mathcal{D}_{\ell,k}$-KerMDH problem is generically hard in m-linear groups. However, in the only candidate multilinear groups which have resisted cryptanalysis [13], every $\mathcal{D}_{\ell,k}$-MDDH Assumption is false (see [13], full version, Section 4.4). Indeed, every matrix problem amounts to deciding whether a matrix has full rank or not.

Roughly speaking, in an m-linear group $\mathcal{MG}_m$, given a matrix $[\mathbf{A}]_r$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, $0 \leq r \leq m-1$ and the zero-test given in the multilinear group description (which allows to decide if two encodings in $\mathbb{G}_m$ correspond to the same element), one can compute a matrix of "weak discrete logarithms", *i.e.*, a noisy encoding at level 0 of the matrix which has full rank if and only if the original matrix has full rank. This can be determined easily at level 0 (without multilinear maps, so independently of ℓ, k).

However, this attack does not apply in a straightforward way to break the Kernel DH Assumption. With the matrix of "weak discrete logarithms" of $\mathbf{A}$, one can compute a noisy version of a vector of the kernel, but this vector is not in $\mathbb{G}_i$ for any $i = 1, \ldots, m$. Thus, this attack does not immediately apply to break the $(r, m, \mathcal{D}_{\ell,k})$-KerMDH, which means that the Kernel DH Assumptions could be still used to build cryptographic protocols in the multilinear group setting. We leave it as an open question to examine this issue further.

4.3 A Unifying View on Computational Matrix Problems

We show that the KerMDH problem family includes as particular instances the problems defined in Section 2.4, giving an unifying view of many previously unrelated flexible computational problems in the literature. Namely, Find-Rep (Def. 4.1) is just $(0, \mathcal{U}_{\ell,1})$-KerMDH, SDP in Definition 4.2 is $\mathcal{RL}_2$-KerMDH, the Simultaneous Triple Pairing problem (Def. 4.3) is $\mathcal{U}_2$-KerMDH, the Simultaneous Pairing problem (Def. 4.4) is $\mathcal{P}_{\ell,2}$-KerMDH. DP in Definition 4.8 corresponds to $\mathcal{U}_1$-KerMDH in an asymmetric bilinear setting. On the other hand, 1-FlexDH is $\mathcal{C}_2$-KerMDH, 1-FlexSDH problem is $\mathcal{SC}_2$-KerMDH and ℓ-FlexDH for $\ell > 1$ is the only one which is not in the KerMDH problem family. However, ℓ-FlexDH $\Rightarrow$ $\mathcal{C}_{\ell+1}$-KerMDH. Getting the last three results require a bit more work, as we show in the next two lemmas.

Lemma 5. 1-*FlexDH* $= \mathcal{C}_2$-KerMDH *and* 1-*FlexSDH* $= \mathcal{SC}_2$-KerMDH.

Proof. The proof of the first statement is obvious from the fact that the solutions $([r], [ra], [rab])$ of the 1-FlexDH problem instance $([1], [a], [b])$ correspond exactly to the nonzero vectors in $\ker \mathbf{A}^\top$ for $\mathbf{A} = \begin{pmatrix} -a & 0 \\ 1 & -b \\ 0 & 1 \end{pmatrix}$. The second statement is proven in a similar way.

Lemma 6. ℓ-*FlexDH* $\Rightarrow \mathcal{C}_{\ell+1}$-KerMDH.

Proof. Given a ℓ-FlexDH problem instance $([1], [a], [b])$, pick random $r_2, \ldots, r_\ell \in \mathbb{Z}_q^*$ and compute the matrix $[\mathbf{A}]$ where

$$\mathbf{A} = \begin{pmatrix} -a & & & & 0 \\ 1 & -r_2 & & & \\ & \ddots & \ddots & & \\ & & 1 & -r_\ell & \\ & & & 1 & -b \\ 0 & & & & 1 \end{pmatrix}$$

Then, run the $\mathcal{C}_{\ell+1}$-KerMDH solver on $[\mathbf{A}]$, obtaining the vector $([r_1], [r_1 a], [r_1 r_2 a], \ldots, [r_1 \cdots r_\ell a], [r_1 \cdots r_\ell ab])$ for some $r_1 \in \mathbb{Z}_q^*$, which along with $([r_2], \ldots, [r_\ell])$ solves the ℓ-FlexDH problem.

Notice that simply reformulating existing problems as Kernel DH problem instances, not only gives a homogeneous naming but also it shows up the existing relations among them. For example, it is now self evident that Triple Pairing and SDP problems are essentially the same.

4.4 Increasing Families of KerMDH Problems

Most matrix distributions are indeed families parameterized by their size. In this section we show that the examples described in previous sections, namely $\mathcal{U}_{\ell,k}$, $\mathcal{L}_k$, $\mathcal{CI}_{k,d}$, $\mathcal{SC}_k$, $\mathcal{C}_k$ and $\mathcal{RL}_k$, define families of kernel problems with increasing hardness. We provide specific reductions for each family, as they require different techniques.

Lemma 7. $\mathcal{U}_{\widetilde{\ell},\widetilde{k}}$-KerMDH $\Rightarrow \mathcal{U}_{\ell,k}$-KerMDH *for* $\widetilde{k} \leq k$ *and* $\widetilde{\ell} \leq \ell$.

Proof. Given an instance $[\widetilde{\mathbf{A}}]$, with $\widetilde{\mathbf{A}} \leftarrow \mathcal{U}_{\widetilde{\ell},\widetilde{k}}$, we choose random invertible matrices $\mathbf{L} \in \mathbb{Z}_q^{\ell \times \ell}$ and $\mathbf{R} \in \mathbb{Z}_q^{k \times k}$ and define $\mathbf{A} = \mathbf{L}(\widetilde{\mathbf{A}} \oplus \mathbf{B})\mathbf{R}$, where $\mathbf{B}$ is any full-rank matrix in $\mathbb{Z}_q^{(\ell-\widetilde{\ell}) \times (k-\widetilde{k})}$ and $\oplus$ operation denotes diagonal block matrix concatenation. Clearly, the new matrix is uniformly distributed in $\mathbb{Z}_q^{\ell \times k}$.

Any vector $[\boldsymbol{x}]$ such that $\boldsymbol{x} \in \ker \mathbf{A}^\top \setminus \{\mathbf{0}\}$ can be transformed into $[\widetilde{\boldsymbol{x}}]$ such that $\widetilde{\boldsymbol{x}} \in \ker \widetilde{\mathbf{A}}^\top \setminus \{\mathbf{0}\}$ by just letting $[\widetilde{x}] = \mathbf{L}^\top [\boldsymbol{x}]$.

Lemma 8. $\mathcal{L}_k$-KerMDH $\Rightarrow \mathcal{L}_{k+1}$-KerMDH.

Proof. Observe that given a matrix $\mathbf{A} \in \mathcal{L}_{k+1}$, with parameters $a_1, \ldots, a_{k+1}$, we can obtain a matrix $\widetilde{\mathbf{A}} \in \mathcal{L}_k$ by deleting the row and the column corresponding to a_{k+1}. Moreover, given $\boldsymbol{x} = (x_1, \ldots, x_{k+2}) \in \ker \mathbf{A}^\top \setminus \{\mathbf{0}\}$, the vector $\widetilde{\boldsymbol{x}} = (x_1, \ldots, x_k, x_{k+2})$ is in $\ker \widetilde{\mathbf{A}}^\top \setminus \{\mathbf{0}\}$.

The reduction consists of choosing a random a_{k+1}, then building $[\mathbf{A}]$ from $[\widetilde{\mathbf{A}}]$ as above, and finally obtaining $[\widetilde{\boldsymbol{x}}]$ from $[\boldsymbol{x}]$ by deleting the $(k+1)$-th coordinate.

Lemma 9. $\mathcal{CI}_{k,d}$-KerMDH $\Rightarrow \mathcal{CI}_{k+1,d}$-KerMDH.

Proof. From a matrix $\mathbf{A} \in \mathcal{CI}_{k+1,d}$, with parameters $a_1, \ldots, a_d$, we can obtain a matrix $\widetilde{\mathbf{A}} \in \mathcal{CI}_{k,d}$ by deleting the last row and the last column. Now given $\boldsymbol{x} = (x_1, \ldots, x_{k+d+1}) \in \ker \mathbf{A}^\top \setminus \{\mathbf{0}\}$, it is easy to see that the vector $\widetilde{\boldsymbol{x}} = (x_1, \ldots, x_{k+d})$ is in $\ker \widetilde{\mathbf{A}}^\top \setminus \{\mathbf{0}\}$.

The reduction proceeds analogously as in the linear matrix distribution.

This lemma also shown that $\mathcal{SC}_k$-KerMDH $\Rightarrow \mathcal{SC}_{k+1}$-KerMDH as a particular case. The proofs of $\mathcal{C}_k$-KerMDH $\Rightarrow \mathcal{C}_{k+1}$-KerMDH and $\mathcal{RL}_k$-KerMDH $\Rightarrow \mathcal{RL}_{k+1}$-KerMDH directly follow from the same ideas.

4.5 Algebraic Reductions

Now we analyze the possible reductions among different families of KerMDH problems of the same size. Thanks to the algebraic nature of matrix distributions it is easy to find some generic reductions among the corresponding problems.

Definition 10. *We say that $\mathcal{D}^1_{\ell,k}$ is algebraically reducible to $\mathcal{D}^2_{\ell,k}$ if there exist two efficiently samplable matrix distributions, $\mathcal{L}$ which outputs a matrix $\mathbf{L} \in \mathbb{Z}_q^{\ell\times\ell}$ matrix and $\mathcal{R}$ which outputs a matrix $\mathbf{R} \in \mathbb{Z}_q^{k\times k}$, such that given $\mathbf{A} \leftarrow \mathcal{D}^1_{\ell,k}$ the distribution of the matrix $\mathbf{LAR}$ is negligibly close to $\mathcal{D}^2_{\ell,k}$. In this case we write $\mathcal{D}^1_{\ell,k} \overset{a}{\Rightarrow} \mathcal{D}^2_{\ell,k}$.*

We note that since we assume that the matrices output by either of the distributions $\mathcal{D}^1_{\ell,k}$, $\mathcal{D}^2_{\ell,k}$ have full rank with overwhelming probability, the distributions $\mathcal{L}, \mathcal{R}$ must output full rank matrices also with overwhelming probability.

Next, we show two examples of algebraic reductions. Using random $\mathbf{L}$ and $\mathbf{R}$ we obtain $\mathcal{D}_{\ell,k}$, $\mathcal{D}_{\ell,k} \overset{a}{\Rightarrow} \mathcal{U}_{\ell,k}$, for any matrix distribution $\mathcal{D}_{\ell,k}$, and considering $\mathbf{L}$ the identity matrix and $\mathbf{R}$ a random invertible diagonal matrix, $\mathcal{L}_k \overset{a}{\Rightarrow} \mathcal{R}\mathcal{L}_k$ holds.

The notion of algebraic reducibility is useful to find reductions among the MDDH problems and also the Kernel problems.

Lemma 10. *$\mathcal{D}^1_{\ell,k} \overset{a}{\Rightarrow} \mathcal{D}^2_{\ell,k}$ implies both $\mathcal{D}^1_{\ell,k}$-MDDH $\Rightarrow \mathcal{D}^2_{\ell,k}$-MDDH and $\mathcal{D}^1_{\ell,k}$-KerMDH $\Rightarrow \mathcal{D}^2_{\ell,k}$-KerMDH.*

Proof. Given instance of the $\mathcal{D}^1_{\ell,k}$-MDDH problem, $([\mathbf{A}], [\boldsymbol{z}])$, the tuple $([\mathbf{LAR}], [\mathbf{L}\boldsymbol{z}])$, with $\mathbf{L} \leftarrow \mathcal{L}$, $\mathbf{R} \leftarrow \mathcal{R}$ is a properly distributed instance of the $\mathcal{D}^2_{\ell,k}$-MDDH problem. Indeed, it is easy to see that 'real' instances are transformed into 'real' instances, and 'random' instances into 'random' ones.

On the other hand, we show that given an algorithm $\mathcal{A}$ which solves $\mathcal{D}^2_{\ell,k}$-KerMDH there exists another algorithm which solves $\mathcal{D}^1_{\ell,k}$-KerMDH with the same probability. Given $\mathbf{A} \leftarrow \mathcal{D}^1_{\ell,k}$-KerMDH problem, sample two matrices $\mathbf{L} \leftarrow \mathcal{L}$, $\mathbf{R} \leftarrow \mathcal{R}$ and construct an instance $\mathbf{LAR}$ of $\mathcal{D}^2_{\ell,k}$. Let $[\boldsymbol{x}]$ be the output of $\mathcal{A}$ on input $[\mathbf{LAR}]$, that is, $\boldsymbol{x}$ is a nonzero vector such that $\boldsymbol{x}^\top \mathbf{LAR} = \mathbf{0}^\top$. Since $\mathbf{L}$ and $\mathbf{R}$ are invertible with overwhelming probability, $\boldsymbol{x}^\top \mathbf{LA} = \mathbf{0}^\top$ also holds. Then output the nonzero vector $[\mathbf{L}^\top \boldsymbol{x}]$ as a solution to the $\mathcal{D}^1_{\ell,k}$-KerMDH problem.

From the above results, it is straightforward that $\mathcal{D}_{\ell,k}$-KerMDH $\Rightarrow \mathcal{U}_{\ell,k}$-KerMDH, for any matrix distribution $\mathcal{D}_{\ell,k}$, and $\mathcal{L}_k$-KerMDH $\Rightarrow \mathcal{R}\mathcal{L}_k$-KerMDH.

5 Separation of Kernel Diffie-Hellman Problems

One can easily prove that any family of hard matrix distributions $\mathcal{D}_{\ell,k}$ of increasing k defines a decisional problem family $\mathcal{D}_{\ell,k}$-MDDH of strictly increasing hardness. Indeed, any efficient m-linear map can efficiently solve any $\mathcal{D}_{\ell,k}$-MDDH problem with $k \leq m-1$, and therefore every two $\mathcal{D}_{\ell,k}$-MDDH and $\mathcal{D}_{\widetilde{\ell},\widetilde{k}}$-MDDH problems with $\widetilde{k} < k$ are separated by an oracle computing a k-linear map.

When dealing with the computational $\mathcal{D}_{\ell,k}$-KerMDH family, no such a trivial argument is known to exist. Actually, a m-linear map does not seem to help at all solving any $\mathcal{D}_{\ell,k}$-KerMDH problem with $k > 1$. Therefore, without further analysis there is no reason for using $k > 2$, and this is why there are so many works which use the $\mathcal{R}\mathcal{L}_2$-KerMDH Assumption.

In this section we show a separation result for KerMDH problems. Namely, we show that there is no black-box reduction in the generic group model from $\mathcal{D}_{\ell,k}$-KerMDH to $\mathcal{D}_{\widetilde{\ell},\widetilde{k}}$-KerMDH for $k > \widetilde{k}$, assuming that the corresponding $\mathcal{D}_{\ell,k}$-MDDH problems are generically hard on a multilinear group. We will consider only the (plain) generic group model in the analysis, since the solution of the $\mathcal{D}_{\ell,k}$-KerMDH problem over a group $\mathbb{G}$ is a particular vector of elements in $\mathbb{G}$, while the result of computing any multilinear map is an element of a different group $\mathbb{G}_m$, and no efficient map from $\mathbb{G}_m$ to $\mathbb{G}$ is supposed to exist.

In order to achieve this goal, we prove some lemmas and we introduce a new concept on a family of subspaces of a vector space, named *t-Elusiveness*.

The natural reductions between kernel DH problems defined over a group are algebraic black-box reductions that transform an instance of a problem into an instance of the other by means of a (randomized) linear map. In the first lemma in this section we show that natural reductions between kernel DH problems have a very special form. Observe that a black-box reduction to a flexible problem must work for any adversary solving it. In particular, the reduction should work for **any** solution given by this adversary, or for **any** probability distribution of the solutions given by it. The lemma is very technical but it mainly states that the output of a successful reduction can be computed in essentially two ways:

- by just applying a (randomized) linear map to the answer given by the adversary in the last call. Therefore, all possibly existing previous calls to the adversary are just used to prepare the last one.
- by just ignoring the last call to the adversary.

Let $\mathcal{R}$ be a black-box reduction of $\mathcal{D}_{\ell,k}$-KerMDH to $\mathcal{D}_{\widetilde{\ell},\widetilde{k}}$-KerMDH, in the generic group $\mathbb{G}$, for some matrix distributions $\mathcal{D}_{\ell,k}$ and $\mathcal{D}_{\widetilde{\ell},\widetilde{k}}$. Namely, $\mathcal{R}$ solves $\mathcal{D}_{\ell,k}$-KerMDH with a non-negligible probability by making $Q \geq 1$ queries to an oracle solving $\mathcal{D}_{\widetilde{\ell},\widetilde{k}}$-KerMDH with probability one. As we aim at ruling out the existence of some reductions, we consider the best possible case any black-box reduction must be able to deal with. Now consider the splitting $\mathcal{R} = (\mathcal{R}_0, \mathcal{R}_1)$ defined by the last oracle call, depicted in Figure 1. That is, $\mathcal{R}_0$ stops by outputting the last query to the oracle together with some state information s for $\mathcal{R}_1$, while $\mathcal{R}_1$ resumes the execution from the state information and the answer $[\boldsymbol{w}] \in \mathbb{G}^{\widetilde{l}}$ given by the oracle. Without loss of generality, we assume that both stages $\mathcal{R}_0$ and $\mathcal{R}_1$ receive the same random tape (and perhaps $\mathcal{R}_1$ will redo some of the computations performed by $\mathcal{R}_0$).

In the generic group model, following Maurer's model [24,25], the output of the reduction $[\boldsymbol{v}] \in \mathbb{G}^l$ is computed as linear combinations of the group elements received from the input or from the oracle answers. In particular, we can write $\boldsymbol{v} = \boldsymbol{u} + \eta(\boldsymbol{w})$, for some vector $\boldsymbol{u} \in \mathbb{Z}_q^l$ depending on s (*i.e.*, depending on the input, the random tape and the first $Q-1$ oracle answers), and some (randomized) linear map $\eta : \mathbb{Z}_q^{\widetilde{l}} \to \mathbb{Z}_q^l$ depending only on the random tape of $\mathcal{R}$. Actually, $[\boldsymbol{u}]$ is computed by $\mathcal{R}_1$ as linear combinations of the group elements contained in s, but the explicit linear combination is not relevant here.

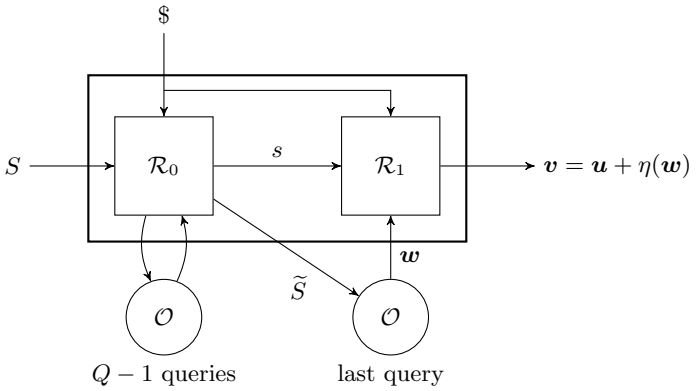

Fig. 1. Splitting of the black-box reduction.

Let us denote $S = \ker \mathbf{A}^\top$, where $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$ and $S' = S \setminus \{\mathbf{0}\}$. Analogously, $\widetilde{S} = \ker \widetilde{\mathbf{A}}^\top$, where $\widetilde{\mathbf{A}} \leftarrow \mathcal{D}_{\widetilde{\ell},\widetilde{k}}$ and $\widetilde{S}' = \widetilde{S} \setminus \{\mathbf{0}\}$.

Lemma 11. *Let $\mathcal{R} = (\mathcal{R}_0, \mathcal{R}_1)$ be a black-box reduction from $\mathcal{D}_{\ell,k}$-KerMDH to $\mathcal{D}_{\widetilde{\ell},\widetilde{k}}$-KerMDH, in the generic group $\mathbb{G}$, making $Q \geq 1$ calls to an oracle solving the latter with probability one. If $\mathcal{R}$ is successful then, for all behaviour of the oracle, either $\Pr(\eta(\boldsymbol{w}) \in S \setminus \{\mathbf{0}\}) > negl$ or $\Pr(\boldsymbol{u} \in S \setminus \{\mathbf{0}\}) > negl$, where the output of the reduction is $[\boldsymbol{u} + \eta(\boldsymbol{w})]$, $\boldsymbol{u}$ only depends on the state output by $\mathcal{R}_0$, $[\boldsymbol{w}]$ is the answer*

to the last oracle query, and $\eta : \mathbb{Z}_q^{\widetilde{l}} \to \mathbb{Z}_q^l$ *is a (randomized) linear map that only depends on the random tape of* $\mathcal{R}$.

Proof. As a black-box reduction, $\mathcal{R}$ is successful means that it is successful for all possible behaviours of the oracle in its Q queries. We arbitrarily fix its behaviour in the first $Q-1$ queries. Then concerning the last one, for all $\boldsymbol{w} \in \widetilde{S}'$, $\Pr(\boldsymbol{u} + \eta(\boldsymbol{w}) \in S') > negl$, where the probability is computed with respect the random tape of $\mathcal{R}$ and the randomness of the $\mathcal{D}_{\ell,k}$-KerMDH input instance. Now, defining

$$p_{\boldsymbol{w}} = \Pr(\boldsymbol{u} \in S \wedge \boldsymbol{u} + \eta(\boldsymbol{w}) \in S')$$

$$r_{\boldsymbol{w}} = \Pr(\boldsymbol{u} \notin S \wedge \boldsymbol{u} + \eta(\boldsymbol{w}) \in S')$$

we have $p_{\boldsymbol{w}} + r_{\boldsymbol{w}} > negl$. But not all $r_{\boldsymbol{w}}$ can be non-negligible since the corresponding events are disjoint. Indeed, for every nonzero vector $\boldsymbol{w}$ and any different $\alpha_1, \alpha_2 \in \mathbb{Z}_q^\times$,

$$\boldsymbol{u} + \eta(\alpha_1 \boldsymbol{w}) \in S,\ \boldsymbol{u} + \eta(\alpha_2 \boldsymbol{w}) \in S \quad \Rightarrow \quad (\alpha_2 - \alpha_1)\boldsymbol{u} \in S \quad \Rightarrow \quad \boldsymbol{u} \in S$$

and then $\sum_{\alpha \in \mathbb{Z}_q^\times} r_{\alpha \boldsymbol{w}} \leq 1$. Therefore, there is some α_m such that $r_{\alpha_m \boldsymbol{w}} \leq \frac{1}{q-1}$, which in turn implies $p_{\alpha_m \boldsymbol{w}} > negl$. Now, we can split $p_{\alpha_m \boldsymbol{w}}$ depending on whether $\boldsymbol{u} \in S'$ or $\boldsymbol{u} = \boldsymbol{0}$, obtaining

$$\begin{aligned} p_{\alpha_m \boldsymbol{w}} &= \Pr(\eta(\boldsymbol{w}) \in S') + \Pr(\boldsymbol{u} \in S' \wedge \boldsymbol{u} + \eta(\alpha_m \boldsymbol{w}) \in S') \leq \\ &\leq \Pr(\eta(\boldsymbol{w}) \in S') + \Pr(\boldsymbol{u} \in S') \end{aligned}$$

and concluding that either $\Pr(\boldsymbol{u} \in S') > negl$ or for all nonzero $\boldsymbol{w} \in \widetilde{S}'$, $\Pr(\eta(\boldsymbol{w}) \in S') > negl$. However, which one is true could depend on the particular behaviour of the oracle in the first $Q-1$ calls.

In some cases, one of the two strategies of the reduction mentioned above can be ruled out. Namely, we can prove that $\Pr(\eta(\boldsymbol{w}) \in S \setminus \{\boldsymbol{0}\}) \in negl$.

Lemma 12. *Consider integers* $l = k + d$, $\widetilde{l} = \widetilde{k} + \widetilde{d}$ *such that* $l, \widetilde{l} > 0$ *and* $k > \widetilde{k}$. *Let* $\eta : \mathbb{Z}_q^{\widetilde{l}} \to \mathbb{Z}_q^l$ *be a linear map, exists a subspace* F *of* $Im\,\eta$ *of dimension at most* k *such that for all* $\widetilde{S}$ *subspaces of* $\mathbb{Z}_q^{\widetilde{l}}$ *of dimension* $\widetilde{d}$, *either* $\widetilde{S} \subset \ker \eta$ *or* $\dim F \cap \eta(\widetilde{S}) \geq 1$.

Proof. If $\operatorname{rank} \eta \leq k$ it suffices to take $F = \operatorname{Im} \eta$. Indeed, if $\widetilde{S} \not\subset \ker \eta$, *i.e.*, $\eta(\widetilde{S}) \neq \{\boldsymbol{0}\}$, then $\dim F \cap \eta(\widetilde{S}) = \dim \eta(\widetilde{S}) \geq 1$.

Otherwise, $\operatorname{rank} \eta > k$, let F a subspace of $\operatorname{Im} \eta$ of dimension k, using the Grassman's formula,

$$\begin{aligned} \dim F \cap \eta(\widetilde{S}) &= \dim F + \dim \eta(\widetilde{S}) - \dim(F + \eta(\widetilde{S})) \geq \\ &\geq k + \dim \eta(\widetilde{S}) - \operatorname{rank} \eta \geq k + \dim \widetilde{S} - \dim \ker \eta - \operatorname{rank} \eta = \\ &= k + \widetilde{d} - \widetilde{l} = k - \widetilde{k} \geq 1 \end{aligned}$$

Definition 11 (t-Elusiveness). *A family of subspaces* $\mathcal{S}$ *of a vector space* X *over the finite field* $\mathbb{Z}_q$ *is called* t*-elusive for some* $t < \dim X$ *if for all* t*-dimensional subspaces* $F \subset X$, $\Pr(F \cap S \neq \{\boldsymbol{0}\}) \in negl$, *where the probability is computed with respect to the choice of* $S \in \mathcal{S}$.

A matrix distribution $\mathcal{D}_{\ell,k}$ *is called* t*-elusive if the family* $\{\ker \mathbf{A}^\top\}_{\mathbf{A} \in \mathcal{D}_{\ell,k}}$ *is* t*-elusive.*

Lemma 13. *If a matrix distribution* $\mathcal{D}_{\ell,k}$ *is hard (as given in Definition 3) then* $\mathcal{D}_{\ell,k}$ *is* k*-elusive.*

Proof. By definition, given a non-k-elusive matrix distribution $\mathcal{D}_{\ell,k}$, there exists a k-dimensional vector subspace $F \subset \mathbb{Z}_q^\ell$ such that $\Pr_{\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}}(F \cap \ker \mathbf{A}^\top \neq \{\boldsymbol{0}\}) > negl$. F can be efficiently computed from the description of $\mathcal{D}_{\ell,k}$ with standard tools from linear algebra.

Let $\mathbf{M} \in \mathbb{Z}_q^{k \times \ell}$ be a maximal rank matrix such that $\operatorname{Im} \mathbf{M}^\top = F$. Then, $\dim(F \cap \ker \mathbf{A}^\top) = \dim(\operatorname{Im} \mathbf{M}^\top \cap \ker \mathbf{A}^\top) \leq \dim \ker(\mathbf{A}^\top \mathbf{M}^\top) = \dim \ker(\mathbf{MA})^\top = \dim \ker(\mathbf{MA})$, as $\mathbf{MA}$ is a $k \times k$ square matrix. Thus, we know that

$$\Pr_{\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}}(\operatorname{rank}(\mathbf{MA}) < k) > negl$$

Now we show how to solve the $\mathcal{D}_{\ell,k}$-MDDH problem on some k-linear group $\mathbb{G}$, by means of a k-linear map. Let $[(\mathbf{A}\|\boldsymbol{z})]$ be an instance of the $\mathcal{D}_{\ell,k}$-MDDH problem. In a 'real' instance $\boldsymbol{z} = \mathbf{A}\boldsymbol{x}$ for a uniformly distributed vector $\boldsymbol{x} \in \mathbb{Z}_q^k$, while in a 'random' instance, $\boldsymbol{z}$ is uniformly distributed $\mathbb{Z}_q^\ell$. A distinguisher can efficiently compute $[\mathbf{MA}]$ and $[\mathbf{M}\boldsymbol{z}]$. Observe that in a 'real' instance $\operatorname{rank}(\mathbf{MA}\|\mathbf{M}\boldsymbol{z}) = \operatorname{rank}(\mathbf{MA}\|\mathbf{MA}\boldsymbol{x}) = \operatorname{rank}(\mathbf{MA})$, while in a 'random' instance $\mathbf{M}\boldsymbol{z}$ is uniformly distributed in $\mathbb{Z}_q^k$. Therefore, for a 'random' instance there is a non-negligible probability that $\operatorname{rank}(\mathbf{MA}) < k$ and $\operatorname{rank}(\mathbf{MA}\|\mathbf{M}\boldsymbol{z}) = \operatorname{rank}(\mathbf{MA}) + 1$, because $\mathbf{M}\boldsymbol{z} \in \operatorname{Im}(\mathbf{MA})$ occurs only with a negligible probability $< \frac{1}{q}$. Then, the distinguisher can efficiently tell apart the two cases because with a k-linear map at hand computing the rank of a $k \times k$ or a $k \times k+1$ matrix can be done efficiently.

Theorem 1. *Let $\mathcal{D}_{\ell,k}$ be k-elusive. If there exists a black-box reduction in the generic group model from $\mathcal{D}_{\ell,k}$-KerMDH to another problem $\mathcal{D}_{\widetilde{\ell},\widetilde{k}}$-KerMDH with $\widetilde{k} < k$, then $\mathcal{D}_{\ell,k}$-KerMDH is easy.*

Proof. Let us assume the existence of the claimed reduction, $\mathcal{R} = (\mathcal{R}_0, \mathcal{R}_1)$, making $Q \geq 1$ oracle queries, where Q is minimal. Then, by Lemma 11, its output can be written as $[\boldsymbol{u} + \eta(\boldsymbol{w})]$, where $\eta : \mathbb{Z}_q^{\widetilde{l}} \to \mathbb{Z}_q^l$ is a (randomized) linear map that does not depend on the particular choice of the matrix $\mathbf{A}$ in the $\mathcal{D}_{\ell,k}$-KerMDH input instance.

Let us denote as above $S = \ker \mathbf{A}^\top$, and $S' = S \setminus \{\mathbf{0}\}$. Analogously, $\widetilde{S} = \ker \widetilde{\mathbf{A}}^\top$, where $\widetilde{\mathbf{A}} \leftarrow \mathcal{D}_{\widetilde{\ell},\widetilde{k}}$ and $\widetilde{S}' = \widetilde{S} \setminus \{\mathbf{0}\}$.

We now proof that in Lemma 11, for any possible behaviour of the oracle in the first $Q-1$ calls, there exists a particular behaviour in the last call such that $\Pr(\eta(\boldsymbol{w}) \in S')$ is negligible. Specifically, the answer of the oracle, $\boldsymbol{w}$, is uniformly distributed in $\widetilde{S}'$.

$$\Pr(\eta(\boldsymbol{w}) \in S') = \Pr(\eta(\boldsymbol{w}) \in S) - \Pr(\eta(\boldsymbol{w}) = 0)$$

Now, developing the second term,

$$\begin{aligned}
\Pr(\eta(\boldsymbol{w}) = 0) &= \Pr(\eta(\boldsymbol{w}) = 0 \mid \widetilde{S} \subset \ker\eta)\Pr(\widetilde{S} \subset \ker\eta) + \\
&\quad + \Pr(\eta(\boldsymbol{w}) = 0 \mid \widetilde{S} \not\subset \ker\eta)\Pr(\widetilde{S} \not\subset \ker\eta) = \\
&= \Pr(\widetilde{S} \subset \ker\eta) + \Pr(\boldsymbol{w} \in \widetilde{S} \cap \ker\eta \mid \widetilde{S} \not\subset \ker\eta)\Pr(\widetilde{S} \not\subset \ker\eta) = \\
&= \Pr(\widetilde{S} \subset \ker\eta) + \mathit{negl}
\end{aligned}$$

where the last equality uses that the probability that a vector uniformly distributed in $\widetilde{S}'$ belongs to a proper subspace of $\widetilde{S}'$ is negligible.

And, analogously for the first term,

$$\begin{aligned}
\Pr(\eta(\boldsymbol{w}) \in S) &= \Pr(\eta(\boldsymbol{w}) \in S \mid \eta(\widetilde{S}) \subset S)\Pr(\eta(\widetilde{S}) \subset S) + \\
&\quad + \Pr(\eta(\boldsymbol{w}) \in S \mid \eta(\widetilde{S}) \not\subset S)\Pr(\eta(\widetilde{S}) \not\subset S) = \\
&= \Pr(\eta(\widetilde{S}) \subset S) + \Pr(\boldsymbol{w} \in \widetilde{S} \cap \eta^{-1}(S) \mid \eta(\widetilde{S}) \not\subset S)\Pr(\eta(\widetilde{S}) \not\subset S) = \\
&= \Pr(\eta(\widetilde{S}) \subset S) + \mathit{negl}
\end{aligned}$$

Thus,

$$\Pr(\eta(\boldsymbol{w}) \in S') = \Pr(\eta(\widetilde{S}) \subset S) - \Pr(\widetilde{S} \subset \ker\eta) + \mathit{negl}$$

Now, using Lemma 12, we know that there exists a subspace F such that if $\widetilde{S} \not\subset \ker\eta$, then $\dim F \cap \eta(\widetilde{S}) \geq 1$. Therefore $\Pr(\eta(\widetilde{S}) \subset S) - \Pr(\widetilde{S} \subset \ker\eta) \leq \Pr(\eta(\widetilde{S}) \subset S \wedge \dim F \cap \eta(\widetilde{S}) \geq 1) \leq \Pr(\dim F \cap S \geq 1)$. Since $\dim F \leq k$, the last probability is negligible due to the k-elusiveness of $\mathcal{D}_{\ell,k}$.

Now applying Lemma 11 we know that $\Pr(\boldsymbol{u} \in S \setminus \{\mathbf{0}\}) > \mathit{negl}$ for any possible behaviour of the oracle in the first $Q-1$ calls. Therefore, we can modify the reduction $\mathcal{R}$ to output $\boldsymbol{u}$, without making the Q-th oracle call. The modified reduction is also successful, with only $Q-1$ oracle calls, which contradicts the assumption that Q is minimal. In summary, if the claimed reduction exists then there also exists an algorithm (a "reduction with $Q = 0$") directly solving $\mathcal{D}_{\ell,k}$-KerMDH without the help of any oracle.

Corollary 1. *If a matrix distribution family $\{\mathcal{D}_{\ell,k}\}$ is hard then for any $\mathcal{D}_{\ell,k}$ and $\mathcal{D}_{\widetilde{\ell},\widetilde{k}}$ in the family with $k > \widetilde{k}$ there is no black-box reduction in the generic group model from $\mathcal{D}_{\ell,k}$-KerMDH to $\mathcal{D}_{\widetilde{\ell},\widetilde{k}}$-KerMDH.*

Proof. As all $\mathcal{D}_{\ell,k}$-MDDH problems in the family are generically hard on a k-linear group, we know that $\mathcal{D}_{\ell,k}$ is k-elusive by Lemma 13, and also $\mathcal{D}_{\ell,k}$-KerMDH is hard in that group (otherwise, any solution to $\mathcal{D}_{\ell,k}$-KerMDH can be used to solve $\mathcal{D}_{\ell,k}$-MDDH in a straightforward way). By the above theorem, no black-box reduction in the generic group model from $\mathcal{D}_{\ell,k}$-KerMDH to $\mathcal{D}_{\widetilde{\ell},\widetilde{k}}$-KerMDH can exist for $k > \widetilde{k}$.

To conclude, combining the above corollary and the results in the previous section, all $\mathcal{U}_{\ell,k}$, $\mathcal{L}_k$, $\mathcal{CI}_{k,d}$, $\mathcal{SC}_k$, $\mathcal{C}_k$ and $\mathcal{RL}_k$ define families of kernel problems with **strictly** increasing hardness. Thus, it makes sense relying on $\mathcal{D}_{\ell,k}$-KerMDH Assumption for larger k.

6 Applications

The Double Pairing Assumption (in asymmetric groups) and the Simultaneous Double Pairing Assumption (in symmetric groups) correspond in our language to, respectively, the $\mathcal{U}_1$-KerMDH Assumption and the $\mathcal{RL}_2$-KerMDH Assumption. They are used in a large number of protocols, most notably in the design of structure preserving cryptographic primitives [1,2,5,22] (to name a few). We expect that these protocols can all be generalized to work with the Kernel DH Assumption and to lead to simplified constructions and/or constructions based on weaker assumptions.

QA-NIZK for Linear Spaces. All the recent constant-size arguments of membership in linear spaces [18,19,20,22] are based on some $\mathcal{D}_{\ell,k}$-KerMDH Assumption (*e.g.* the SP or SDP Assumptions). Among them we are particularly interested in the work of [19,20], who give a family of instances of their scheme. More specifically, [20] give an instance of proof size k based on our new family of computational assumptions, the $\mathcal{D}_k$-KerMDH. On the other hand, Jutla and Roy [19] achieve the same proof size under what they call the "Switching Lemma", which is proven under a decisional assumption, the $\mathcal{RL}_k$-MDDH Assumption. However, a close look at the proof reveals that in fact it is based on (the weaker, computational) $\mathcal{RL}_k$-KerMDH Assumption [3]

In either case, as the proof size grows with k, the only reason to construct these arguments based on such a family of computational assumptions ($k = 1$ would suffice in the asymmetric case groups) is if the assumptions are *strictly* increasingly weaker, which was unknown prior to this work. So our results fundament the general constructions of [19,20].

Lower Bounds for Structure-Preserving Cryptography. A number of works investigate lower bounds for structure-preserving signatures. For instance, [3,4] investigate (among others) lower bounds for the number of (pairing-product) equations necessary to verify a structure preserving signature, and [5] deals with the minimal number of (pairing-product) equations necessary to verify an opening of a structure-preserving commitment. Implicitly, these works use the inexistence of kernel assumptions of a certain size, *e.g* the inexistence of $\mathcal{D}_1$-KerMDH Assumption in symmetric bilinear groups.

6.1 Generalized Pedersen Commitments in Multilinear Groups

In a group $(\mathbb{G}, q, \mathcal{P})$ where the discrete logarithm is hard, the Pedersen commitment is a statistically hiding and computationally binding commitment to a scalar. It can be naturally generalized to several scalars. Abe *et al.* [2] show how to do similar Pedersen type commitments to group elements in bilinear groups under what they call the SDP Assumption, which in our language is the $\mathcal{RL}_2$-KerMDH Assumption. With our new assumption family we can write both the Pedersen commitment and the commitment of [2] as a single construction and generalize it to graded encodings.

[3] To see this, note that in the proof of their "Switching Lemma" on which soundness is based, they use the output of the adversary to decide if $\boldsymbol{f} \stackrel{?}{\in} \operatorname{Im} \mathbf{A}$, $\mathbf{A} \leftarrow \mathcal{RL}_k$, by checking whether $[\boldsymbol{f}]$ is orthogonal to the adversary's output (equation (1), proof of Lemma 1, [19], full version).

– $\mathsf{Setup}(1^\lambda, k, n)$: Let $\mathcal{MG}_k = (e, \mathbb{G}_1, \mathbb{G}_2, \ldots, \mathbb{G}_k, q, \mathcal{P}_1, \ldots, \mathcal{P}_k) \leftarrow \mathsf{MGen}_k(1^\lambda)$. Sample $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$. Output $ck := (\mathcal{MG}_k, [\mathbf{A}]_1)$, $tk := (\mathbf{A})$.
– $\mathsf{Commit}(ck, [\boldsymbol{m}]_r)$: To commit to a vector $[\boldsymbol{m}]_r \in \mathbb{G}_r^n$, $r < k$, pick $[\boldsymbol{s}]_r \leftarrow \mathbb{G}_r^k$, and output

$$[\boldsymbol{c}]_{r+1} := e([(\boldsymbol{s}^\top || \boldsymbol{m}^\top]_r, [\mathbf{A}]_1) = [(\boldsymbol{s}^\top || \boldsymbol{m}^\top)\mathbf{A}]_{r+1} \in \mathbb{G}_{r+1}^k.$$

– $\mathsf{TrapdoorCommit}(ck, tk, r)$: Generate an equivocal commitment $[\boldsymbol{c}]_{r+1} \in \mathbb{G}_{r+1}^k$ by picking $[\boldsymbol{s}]_r \leftarrow \mathbb{G}_r^k$ and computing $[\boldsymbol{c}]_{r+1} = e([\boldsymbol{s}^\top]_r, [\mathbf{A}]_1) \in \mathbb{G}_{r+1}^k$.
– $\mathsf{TrapdoorOpen}(\mathbf{A}, [\boldsymbol{c}]_{r+1})$: On an equivocal commitment $[\boldsymbol{c}]_{r+1} \in \mathbb{G}_{r+1}^k$, compute and return the trapdoor opening to some message $[\boldsymbol{m}]_r \in \mathbb{G}_r^n$ as follows. Pick $\boldsymbol{s} \leftarrow \mathbb{Z}_q^k$. Let $\boldsymbol{f}_i$, $i \in [k]$, be the ith column of $\mathbf{A}$. For each $i \in [k]$, let:

$$[a_i]_r := [(\boldsymbol{s}^\top || \boldsymbol{m}^\top)]_r \boldsymbol{f}_i = [(\boldsymbol{s}^\top || \boldsymbol{m}^\top) \boldsymbol{f}_i]_r \in \mathbb{G}_r.$$

Let $\mathbf{A}_0$ be the minor of $\mathbf{A}$ consisting of the first k rows. W.l.o.g. we can assume $\mathbf{A}_0^{-1}$ exists. Output $[\boldsymbol{s}]_r$ as the opening of $[\boldsymbol{c}]_{r+1}$ to $[\boldsymbol{m}]_r$, where:

$$\boldsymbol{s} := \mathbf{A}_0^{-1} \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}.$$

The proof for the general case is almost identical to [2]. The hiding property of the commitment is unconditional, while the soundness (at level r) is based on the $(r, k, \mathcal{D}_{\ell,k})$-$\mathsf{KerMDH}$ Assumption. The correctness of the trapdoor opening property follows easily from an algebraic argument.

Existing constructions. The Pedersen commitment (to multiple elements) corresponds to $m = 0$ and $\mathbf{A} \leftarrow \mathcal{U}_{n+1,1}$ and soundness is based on the $(0, \mathcal{U}_{n+1,1})$-KerMDH. The construction proposed in [2] to commit to group elements corresponds to $m = 1$ and $\mathbf{A} \leftarrow \mathcal{U}_{n+1,1}$, and to $m = 2$ (in symmetric bilinear maps) and $\mathbf{A} \leftarrow \mathcal{U}_{n+2,2}$. Soundness (binding property) is proven based on the corresponding kernel problems.

Tradeoff Efficiency - Security. With our family of assumptions we can describe in a compact-way many instances of the scheme to commit to messages $[\boldsymbol{m}]_i$ at different levels under any family of $\mathcal{D}_{\ell,k}$-KerMDHAssumption. In particular, this highlights that there is a tradeoff between the size of the public parameters and security. That is, while $\mathcal{U}_{n+k,k}$-KerMDH is the weakest possible Assumption, the number of elements necessary to represent $[\mathbf{A}]$ is $k(n+k)$. On the other hand, if $\mathbf{A} \leftarrow \mathcal{CI}_{k,d}$, soundness is based on the stronger $\mathcal{CI}_{k,d}$-KerMDH Assumption, but the representation size of the public parameters is just $n + k$.

Multilinear maps. As we discussed in Section 4.2, the Kernel Assumption might be a good candidate assumption in multilinear groups. The commitment scheme described above could be an interesting construction there, because the hiding property of the commitment is unconditional and there are no interesting decisional assumptions in $\mathbb{G}_i$, $i < m$, so one should expect to achieve the hiding property only unconditionally.

7 Acknowledgement

The authors thank E. Kiltz and G. Herold for improving this work through very fruitful discussions. Also G. Herold gave us the insight and guidelines to prove the hardness of the circulant matrix distribution.

References

1. M. Abe, M. Chase, B. David, M. Kohlweiss, R. Nishimaki, and M. Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In X. Wang and K. Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 4–24, Beijing, China, Dec. 2–6, 2012. Springer, Berlin, Germany. 2, 13
2. M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-preserving signatures and commitments to group elements. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236, Santa Barbara, CA, USA, Aug. 15–19, 2010. Springer, Berlin, Germany. 2, 3, 4, 13, 14
3. M. Abe, J. Groth, K. Haralambiev, and M. Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In P. Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 649–666, Santa Barbara, CA, USA, Aug. 14–18, 2011. Springer, Berlin, Germany. 13
4. M. Abe, J. Groth, M. Ohkubo, and M. Tibouchi. Structure-preserving signatures from type II pairings. In *CRYPTO 2014, Part I*, LNCS, pages 390–407, Santa Barbara, CA, USA, Aug. 2014. Springer, Berlin, Germany. 13
5. M. Abe, K. Haralambiev, and M. Ohkubo. Group to group commitments do not shrink. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 301–317, Cambridge, UK, Apr. 15–19, 2012. Springer, Berlin, Germany. 2, 13
6. F. Bao, R. H. Deng, and H. Zhu. Variations of Diffie-Hellman problem. In S. Qing, D. Gollmann, and J. Zhou, editors, *ICICS 03*, volume 2836 of *LNCS*, pages 301–312, Huhehaote, China, Oct. 10–13, 2003. Springer, Berlin, Germany. 1, 6
7. N. Bari and B. Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. In W. Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 480–494, Konstanz, Germany, May 11–15, 1997. Springer, Berlin, Germany. 2
8. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55, Santa Barbara, CA, USA, Aug. 15–19, 2004. Springer, Berlin, Germany. 4
9. S. Brands. Untraceable off-line cash in wallets with observers (extended abstract). In D. R. Stinson, editor, *CRYPTO'93*, volume 773 of *LNCS*, pages 302–318, Santa Barbara, CA, USA, Aug. 22–26, 1994. Springer, Berlin, Germany. 2, 4
10. E. Bresson, Y. Lakhnech, L. Mazaré, and B. Warinschi. A generalization of DDH with applications to protocol analysis and computational soundness. In A. Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 482–499, Santa Barbara, CA, USA, Aug. 19–23, 2007. Springer, Berlin, Germany. 1
11. M. Chase and S. Meiklejohn. Déjà Q: Using dual systems to revisit q-type assumptions. In *EUROCRYPT 2014*, LNCS, pages 622–639. Springer, Berlin, Germany, 2014. 1
12. 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, Santa Barbara, CA, USA, Aug. 18–22, 2013. Springer, Berlin, Germany. 2, 3, 4, 5, 6, 17
13. S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In T. Johansson and P. Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 1–17, Athens, Greece, May 26–30, 2013. Springer, Berlin, Germany. 3, 7
14. J. Groth. Homomorphic trapdoor commitments to group elements. *Manuscript.*, 2010. 2, 4
15. J. Groth and S. Lu. A non-interactive shuffle with pairing based verifiability. In K. Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 51–67, Kuching, Malaysia, Dec. 2–6, 2007. Springer, Berlin, Germany. 2, 4, 5
16. G. Herold. Applications of classical algebraic geometry to cryptography. *PhD Thesis, Ruhr-Universität Bochum*, 2014. 5, 16, 17
17. A. Joux and A. Rojat. Security ranking among assumptions within the uber assumption framework. Cryptology ePrint Archive, Report 2013/291, 2013. `http://eprint.iacr.org/`. 1, 6
18. C. S. Jutla and A. Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In *ASIACRYPT 2013*, LNCS, pages 1–20. Springer, Berlin, Germany, Dec. 2013. 13
19. C. S. Jutla and A. Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In *CRYPTO 2014, Part II*, LNCS, pages 295–312, Santa Barbara, CA, USA, Aug. 2014. Springer, Berlin, Germany. 2, 5, 13
20. E. Kiltz and H. Wee. Quasi-adaptive nizk for linear subspaces revisited. *To appear in Eurocrypt 2015*, 2015. 2, 13
21. F. Laguillaumie, P. Paillier, and D. Vergnaud. Universally convertible directed signatures. In B. K. Roy, editor, *ASIACRYPT 2005*, volume 3788 of *LNCS*, pages 682–701, Chennai, India, Dec. 4–8, 2005. Springer, Berlin, Germany. 2, 4

22. 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 *EUROCRYPT 2014*, LNCS, pages 514–532. Springer, Berlin, Germany, 2014. 2, 13
23. B. Libert and D. Vergnaud. Multi-use unidirectional proxy re-signatures. In P. Ning, P. F. Syverson, and S. Jha, editors, *ACM CCS 08*, pages 511–520, Alexandria, Virginia, USA, Oct. 27–31, 2008. ACM Press. 2, 4
24. U. M. Maurer. Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete algorithms. In Y. Desmedt, editor, *CRYPTO'94*, volume 839 of *LNCS*, pages 271–281, Santa Barbara, CA, USA, Aug. 21–25, 1994. Springer, Berlin, Germany. 1, 10
25. U. M. Maurer. Abstract models of computation in cryptography (invited paper). In N. P. Smart, editor, *10th IMA International Conference on Cryptography and Coding*, volume 3796 of *LNCS*, pages 1–12, Cirencester, UK, Dec. 19–21, 2005. Springer, Berlin, Germany. 1, 10
26. U. M. Maurer and S. Wolf. Lower bounds on generic algorithms in groups. In K. Nyberg, editor, *EUROCRYPT'98*, volume 1403 of *LNCS*, pages 72–84, Espoo, Finland, May 31 – June 4, 1998. Springer, Berlin, Germany. 1
27. A.-R. Sadeghi and M. Steiner. Assumptions related to discrete logarithms: Why subtleties make a real difference. In B. Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 244–261, Innsbruck, Austria, May 6–10, 2001. Springer, Berlin, Germany. 1
28. V. Shoup. Lower bounds for discrete logarithms and related problems. In W. Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266, Konstanz, Germany, May 11–15, 1997. Springer, Berlin, Germany. 1

A More Details About the Circulant Matrix Distribution

In this appendix we give more details about both the hardness and the optimality of the representation size of the circulant matrix distribution.

A.1 Optimality of the Representation Size

Lemma 14. *A matrix distribution $\mathcal{D}_{\ell,k}$ defined by linear polynomials in the parameters, $\mathbf{A}(t_1,\ldots,t_d) = \mathbf{A}_0 + \mathbf{A}_1 t_1 + \ldots + \mathbf{A}_d t_d$, where $\mathbf{A}_1,\ldots,\mathbf{A}_d$ are linearly independent matrices, can only be hard if the number of parameters d is at least $\ell - k$.*

Proof. Assume for contradiction that $d < \ell - k$. Then, by gaussian elimination in $\mathbf{A}$ we can transform the matrix into another one, $\mathbf{B}(t_1,\ldots,t_d) = \mathbf{L}\mathbf{A}(t_1,\ldots,t_d)$ for a constant invertible matrix $\mathbf{L}$, such that the first column of $\mathbf{B}$ has zeroes in the lower $\ell - d - 1 \geq k$ positions (as at most $d+1$ entries can be linearly independent as polynomials in $t_1,\ldots,t_d$). Now, it is straightforward to see that this can be used to solve the associated $\mathcal{D}_{\ell,k}$-MDDH problem. Indeed, if $\widehat{\mathbf{L}}$ denotes the lowest k rows of $\mathbf{L}$, given an instance $([\mathbf{A}],[\boldsymbol{z}])$, we transform it into $([\widehat{\mathbf{L}}\mathbf{A}],[\widehat{\mathbf{L}}\boldsymbol{z}])$ and then compare the ranks of $\widehat{\mathbf{L}}\mathbf{A}$ and $\widehat{\mathbf{L}}\mathbf{A}\|\widehat{\mathbf{L}}\boldsymbol{z}$ (computed by means of the k-linear map). The ranks are equal for 'real' instances, while they are different with overwhelming probability for 'random' instances of the $\mathcal{D}_{\ell,k}$-MDDH problem, which contradicts the hardness of $\mathcal{D}_{\ell,k}$.

The linear independency requirement in the lemma just means that there is no redundancy among the d parameters (that is, the map $(t_1,\ldots,t_d) \mapsto \mathbf{A}(t_1,\ldots,t_d)$ is injective). The representation of $\mathbf{A}$ must contain at least d group elements, due to the previous injectivity. Therefore, $\mathcal{CI}_{k,d}$ has optimal representation size.

A.2 Hardness

Here we prove that $\mathcal{CI}_{k,d}$ is a hard matrix distribution (*i.e.*, the $\mathcal{CI}_{k,d}$-MDDH problem is generically hard in k-linear groups), using Theorem 5.15 and specially its Corollary 5.16 in [16] in the linear polynomial case, and Gröbner basis computations in some polynomial ideal.

Intuitively, an algorithm solving $\mathcal{CI}_{k,d}$-MDDH problem in the generic k-linear group model must know some nonzero polynomial in $t_1,\ldots,t_d,z_1,\ldots,z_{k+d}$ vanishing whenever $\boldsymbol{z} \in \operatorname{Im}\mathbf{A}(\boldsymbol{t})$. But this can only

happen if such polynomial belongs to the ideal $\mathfrak{H} \in \overline{\mathbb{Z}}_q[t_1, \ldots, t_d, z_1, \ldots, z_{k+d}]$[4] generated by the relations between $t_1, \ldots, t_d, z_1, \ldots, z_{k+d}$ obtained by elimination of the variables $w_1, \ldots, w_k$ in the equation $\boldsymbol{z} = \mathbf{A}(\boldsymbol{t})\boldsymbol{w}$.

$\mathcal{CI}_{k,d}$ has some interesting properties that makes possible the generic hardness proof. Namely, it is defined by linear polynomials (*i.e.*, $\mathbf{A}(\boldsymbol{t})$ is made of polynomials of degree one in the parameters $t_1, \ldots, t_d$), and $\operatorname{rank} \mathbf{A}(\boldsymbol{t}) = k$ for all possible choices of $t_1, \ldots, t_d \in \overline{\mathbb{Z}}_q$ (*i.e.*, in the algebraic closure of $\mathbb{Z}_q$). This second property comes from the fact that the lowest k-minor of $\mathbf{A}(\boldsymbol{t})$ is constant and equal to 1. With these two properties, Theorem 5.15 and its Corollary 5.16 in [16] essentially state that $\mathfrak{H}$ is precisely the ideal generated by all the $(k+1)$-minors of $\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z}$ as polynomials in $t_1, \ldots, t_d, z_1, \ldots, z_{k+d}$. More precisely,

Theorem 2 (from Theorem 5.15 and its Corollary 5.16 in [16]). *Let $\mathcal{D}_{\ell,k} = \{\mathbf{A}(\boldsymbol{t}) \mid \boldsymbol{t} \leftarrow \mathbb{Z}_q^d\}$ be a polynomial matrix distribution of degree one such that the matrices $\mathbf{A}(\boldsymbol{t})$ in the distribution have always full rank, for all choices of the parameters $t_1, \ldots, t_d$ in the algebraic closure of $\mathbb{Z}_q$. Let*

$$\mathfrak{H} = I(\{(\boldsymbol{t}, \mathbf{A}(\boldsymbol{t})\boldsymbol{w}) \mid \boldsymbol{t} \in \mathbb{Z}_q^d,\ \boldsymbol{w} \in \mathbb{Z}_q^k\})$$

that is the ideal of the polynomials in $\overline{\mathbb{Z}}_q[\boldsymbol{t}, \boldsymbol{z}]$ vanishing at all (rational) points such that $\boldsymbol{z} = \mathbf{A}(\boldsymbol{t})\boldsymbol{w}$, for some $\boldsymbol{w} \in \mathbb{Z}_q^k$, and

$$\mathfrak{D} = (\{\det{}_{i_1,\ldots,i_{k+1}}(\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z}) \mid 1 \le i_1 < i_2 < \cdots < i_{k+1} \le \ell\})$$

the ideal generated by all $(k+1)$-minors of $\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z}$. Then $\mathfrak{H} = \mathfrak{D}$ and it is a prime ideal.

At this point, proving the generic hardness of $\mathcal{CI}_{k,d}$ amounts to proving that there is no nonzero polynomial of total degree less that $k+1$ in $\mathfrak{H}$. Indeed, this means that the only way to generically solve the $\mathcal{CI}_{k,d}$-MDDH problem is computing a polynomial of degree strictly greater than k, which is not feasible in k-linear groups. Notice that in the general case $d \ge 1$, finding a lower bound for the total degree in $\mathfrak{H}$ is a nontrivial task, while in the case $\ell = k+1$ or $d = 1$, as seen in [12], it is as easy as computing the degree of the determinant polynomial $\det(\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z})$. The main reason for that difficulty is the fact that the ideal $\mathfrak{H}$ is not principal. Therefore, we need to compute a Gröbner basis of $\mathfrak{H}$, and show that all the polynomials in it have total degree at least $k+1$.

Gröbner bases can be computed quite easily for specific ideals by means of a computer, but here we will build bases for an infinite collection of ideals, that is for arbitrary values of the size parameters k and d. Thus, we have to compute them by hand. Fortunately, we manage to show that the set of all $(k+1)$-minors of $\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z}$ as polynomials in $t_1, \ldots, t_d, z_1, \ldots, z_{k+d}$, where $\mathbf{A} \leftarrow \mathcal{CI}_{k,d}$, is a Gröbner basis of $\mathfrak{H}$.

We recall some basic notions related to ideals and Gröbner basis. An admissible monomial order $\prec$ in the polynomial ring $\mathbb{Z}_q[t_1, \ldots, t_d, z_1, \ldots, z_{k+d}]$ is a total order among the monomials in it such that for any monomials $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{m}_3$

1. $\mathfrak{m}_1 \neq 1 \ \Rightarrow\ 1 \prec \mathfrak{m}_1$
2. $\mathfrak{m}_1 \prec \mathfrak{m}_2 \ \Rightarrow\ \mathfrak{m}_1\mathfrak{m}_3 \prec \mathfrak{m}_2\mathfrak{m}_3$

The leading monomial of a polynomial $\mathfrak{p}$, denoted by $\mathrm{LM}(\mathfrak{p})$ is defined as the greatest of its monomials (without the coefficient)[5] with respect of the monomial order. We recall that a Gröbner basis of $\mathfrak{H} \subset \mathbb{Z}_q[t_1, \ldots, t_d, z_1, \ldots, z_{k+d}]$ with respect of an admissible monomial order is a set of nonzero polynomials $G = \{\mathfrak{g}_1, \ldots, \mathfrak{g}_s\} \subset \mathfrak{H}$ with the following properties

1. for every $\mathfrak{f} \in \mathfrak{H}$ there exist $\mathfrak{c}_1, \ldots, \mathfrak{c}_s \in \mathbb{Z}_q[t_1, \ldots, t_d, z_1, \ldots, z_{k+d}]$ such that $\mathfrak{f} = \mathfrak{c}_1\mathfrak{g}_1 + \ldots + \mathfrak{c}_s\mathfrak{g}_s$,
2. for every $\mathfrak{f} \in \mathfrak{H}$, $\mathrm{LM}(\mathfrak{f})$ is divisible by $\mathrm{LM}(\mathfrak{g})$ for some $\mathfrak{g} \in G$.

The following lemma comes in a straightforward way from the previous definition

[4] $\overline{\mathbb{Z}}_q$ denotes the algebraic closure of the field $\mathbb{Z}_q$. We define the ideal in the algebraic closure for technical reasons, although the polynomial used by the algorithm will necessarily have its coefficients in $\mathbb{Z}_q$.

[5] We call *leading term* to the leading monomial multiplied by the corresponding coefficient.

Lemma 15. *The minimal degree of nonzero polynomials in an ideal $\mathfrak{H}$ is the minimal degree of the polynomials in any Gröbner basis of $\mathfrak{H}$ with respect to any admissible monomial order compatible with the total degree.*

From now on we fix the following admissible monomial order:

1. $\deg \mathfrak{m}_1 < \deg \mathfrak{m}_2 \Rightarrow \mathfrak{m}_1 \prec \mathfrak{m}_2$, where deg denotes the total degree of the monomial,
2. $z_1 \prec \ldots \prec z_{k+d} \prec t_1 \prec \ldots \prec t_d$,
3. if $\deg \mathfrak{m}_1 = \deg \mathfrak{m}_2$, $\prec$ is the lexicographical order. That is, we write $\mathfrak{m}_1 = z_1^{\alpha_1} \cdots z_{k+d}^{\alpha_{k+d}} t_1^{\alpha_{k+d+1}} \cdots t_d^{\alpha_{k+2d}}$ and $\mathfrak{m}_2 = z_1^{\beta_1} \cdots z_{k+d}^{\beta_{k+d}} t_1^{\beta_{k+d+1}} \cdots t_d^{\beta_{k+2d}}$. Then, for the same total degree, $\mathfrak{m}_1 \prec \mathfrak{m}_2$ if and only if the first nonzero difference $\beta_i - \alpha_i$ is positive.

Given $\mathbf{A} \leftarrow \mathcal{CI}_{k,d}$ we denote by $\Delta(\boldsymbol{i}) = \Delta(i_1, \ldots, i_{k+1}) = \det_{i_1,\ldots,i_{k+1}}(\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z})$ the $(k+1)$-minor of $\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z}$ defined by the rows $1 \leq i_1 < i_2 < \cdots < i_{k+1} \leq k+d$. From now on we will use $\boldsymbol{i} \in \binom{k+d}{k+1}$ as a shorthand for the previous inequalities. These determinants have very special properties. Indeed, we show that with respect to the previous monomial order the main diagonal defines their leading monomial.

Lemma 16. *For all $\boldsymbol{i} \in \binom{k+d}{k+1}$, $LM(\Delta(\boldsymbol{i})) = z_{i_{k+1}} t_{i_1} t_{i_2-1} \cdots t_{i_k-k+1}$.*

Proof. In order to simplify the notation, we can always write the $(k+1)$-minors of $\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z}$ as

$$\Delta(\boldsymbol{i}) = \begin{vmatrix} t_{i_1} & t_{i_1-1} & \cdots & t_{i_1-k+1} & z_{i_1} \\ t_{i_2} & t_{i_2-1} & \cdots & t_{i_2-k+1} & z_{i_2} \\ \vdots & \vdots & \vdots\vdots & \vdots & \vdots \\ t_{i_k} & t_{i_k-1} & \cdots & t_{i_k-k+1} & z_{i_k} \\ t_{i_{k+1}} & t_{i_{k+1}-1} & \cdots & t_{i_{k+1}-k+1} & z_{i_{k+1}} \end{vmatrix}$$

assuming that $t_{d+1} = 1$, and $t_i = 0$ for any i outside the range $i = 1, \ldots, d+1$. Then we show that in the development of the determinant, the monomial corresponding to the main diagonal $\mathfrak{m}_{\text{diag}} = z_{i_{k+1}} t_{i_1} t_{i_2-1} \cdots t_{i_k-k+1}$ is the leading monomial. Firstly, notice that all the terms occurring in the main diagonal are proper terms (*i.e.*, neither 0 nor 1). Indeed, $1 \leq i_1 \leq i_2 - 1 \leq \cdots \leq i_k - k + 1 \leq i_{k+1} - k \leq d$, which is something that deeply depends on the circulant structure of the matrix $\mathbf{A}$.

Now, assume by contradiction that there is another term in the development of the determinant, $\mathfrak{m} = z_{i_{\sigma(k+1)}} t_{i_{\sigma(1)}} t_{i_{\sigma(2)}-1} \cdots t_{i_{\sigma(k)}-k+1}$ (written in a possibly unsorted way), for a permutation $\sigma \in S_{k+1}$, such that $\mathfrak{m}_{\text{diag}} \prec \mathfrak{m}$. Due to the monomial order, the last column must contribute to this term with the variable z_{k+1} (that is $\sigma(k+1) = k+1$). Otherwise, $z_{i_{\sigma(k+1)}} \prec z_{i_{k+1}}$, which contradicts $\mathfrak{m}_{\text{diag}} \prec \mathfrak{m}$.

We can rewrite $\mathfrak{m}$ in terms of the inverse permutation $\pi = \sigma^{-1}$ as

$$\mathfrak{m} = z_{i_{k+1}} t_{i_1-\pi(1)+1} t_{i_2-\pi(2)+1} \cdots t_{i_k-\pi(k)+1}$$

Then, $\pi(1) \neq 1$ would imply $a_{i_1-\pi(1)+1} \prec a_{i_1}$, which is also in contradiction with $\mathfrak{m}_{\text{diag}} \prec \mathfrak{m}$. Therefore, $\sigma(1) = 1$. Observe that it could happen that $i_1 - \pi(1) + 1 \leq 0$, which means that $t_{i_1-\pi(1)+1}$ is actually 0, which also contradicts $\mathfrak{m}_{\text{diag}} \prec \mathfrak{m}$.

Proceeding similarly with subsequent indexes (rows) in increasing order, we easily show that σ can only be the identity permutation, which concludes the proof.

Now we prove that the set of all $(k+1)$-minors of $\mathbf{A}\|\boldsymbol{z}$ is a Gröbner basis. The proof of this result is rather technical and deeply relies on the properties of determinants.

Theorem 3. *The set $G = \{\Delta(\boldsymbol{i}) \mid \boldsymbol{i} \in \binom{k+d}{k+1}\}$ is a Gröbner basis of $\mathfrak{H}$ with respect to the monomial order $\prec$.*

Proof. The usual way to prove that a set $G = \{\mathfrak{g}_1, \ldots, \mathfrak{g}_s\}$ is a Gröbner basis is by means of the so-called S-polynomials. The S-polynomial of a pair $\mathfrak{g}_i, \mathfrak{g}_j \in G$ for $i \neq j$ is defined by

$$\mathfrak{s}_{i,j} = \text{SPOL}(\mathfrak{g}_i, \mathfrak{g}_j) = \frac{\mathfrak{m}_{i,j}}{\mathfrak{m}_i} \mathfrak{g}_i - \frac{\mathfrak{m}_{i,j}}{\mathfrak{m}_j} \mathfrak{g}_j \tag{1}$$

where $\mathfrak{m}_i = \mathrm{LM}(\mathfrak{g}_i)$, $\mathfrak{m}_j = \mathrm{LM}(\mathfrak{g}_j)$, and $\mathfrak{m}_{i,j}$ denotes the least common multiple of $\mathfrak{m}_i$ and $\mathfrak{m}_j$. Then, G is a Gröbner basis if and only if for all $i \neq j$, $\mathrm{RED}_G(\mathfrak{s}_{i,j}) = 0$, where $\mathrm{RED}_G(\mathfrak{p})$ denotes the reduction of a polynomial $\mathfrak{p}$ by repeatedly taking the remainder of the division by elements in G until no further division can be properly performed[6]. Indeed, the famous Buchberger's algorithm for computing Gröbner basis iteratively uses the previous computation to either verify that a pair $\mathfrak{g}_i, \mathfrak{g}_j \in G$ passes the check, or to add its reduced S-polynomial to G.

Observe that any expression of the form $\mathfrak{p} = \mathfrak{c}_1\mathfrak{g}_1 + \ldots + \mathfrak{c}_s\mathfrak{g}_s$, where all the leading monomials $\mathfrak{n}_j = \mathrm{LM}(\mathfrak{c}_j\mathfrak{g}_j)$, $j = 1, \ldots, s$, are different, shows that $\mathrm{RED}_G(\mathfrak{p}) = 0$. Indeed, without loss off generality we can sort the previous terms to ensure that $\mathfrak{n}_1 \prec \ldots \prec \mathfrak{n}_s$. Clearly, $\mathrm{LM}(\mathfrak{p}) = \mathfrak{n}_s$ and reducing $\mathfrak{p}$ by $\mathfrak{g}_s$ gives the remainder $\mathfrak{c}_1\mathfrak{g}_1 + \ldots + \mathfrak{c}_{s-1}\mathfrak{g}_{s-1}$. Therefore, by induction, we get $\mathrm{RED}_G(\mathfrak{p}) = 0$.

Buchberger also provided two optimization rules to speed up the algorithm. In particular, the second one (Buchberger's chain criterion) says that if for some indexes i, j, v, $\mathrm{RED}_G(\mathfrak{s}_{i,v}) = \mathrm{RED}_G(\mathfrak{s}_{j,v}) = 0$ and $\mathfrak{m}_v$ divides $\mathfrak{m}_{i,j}$, then also $\mathrm{RED}_G(\mathfrak{s}_{i,j}) = 0$. We use this criterion to inductively show that in our case, we only need to deal with pairs of $(k+1)$-minors differing only in one row.

We now split the proof into several technical claims. The idea is drawing a path between any two $(k+1)$-minors in which at each step we only change one row of the minor.

The first claim says that from any two $(k+1)$-minors with the same upper $\alpha - 1$ rows but that differ in the α-th row, we can build a third "hybrid" minor by moving the α-th row from one determinant to the other, and the corresponding three leading monomials are related in a suitable way for the chain criterion described above.

Claim 1. For any two sequences $\boldsymbol{i}, \boldsymbol{i^*} \in \binom{k+d}{k+1}$ such that the first difference occurs at position α, for $1 \leq \alpha \leq k$, that is $i_j = i^*_j$ if $j < \alpha$ and $i_\alpha < i^*_\alpha$,

$$\mathrm{LM}(\Delta(i_1, \ldots, i_\alpha, i^*_{\alpha+1} \ldots, i^*_{k+1})) \quad \text{divides} \quad \mathrm{lcm}(\mathrm{LM}(\Delta(\boldsymbol{i})), \mathrm{LM}(\Delta(\boldsymbol{i^*})))$$

Proof (of Claim 1). According to Lemma 16,

$$\mathrm{LM}(\Delta(i_1, \ldots, i_\alpha, i^*_{\alpha+1} \ldots, i^*_{k+1})) = \begin{cases} z_{i^*_{k+1}} t_{i_1} \cdots t_{i_\alpha - \alpha + 1} t_{i^*_{\alpha+1} - \alpha} \cdots t_{i^*_k - k + 1} & \text{if } \alpha < k \\ z_{i^*_{k+1}} t_{i_1} \cdots t_{i_k - k + 1} & \text{if } \alpha = k \end{cases}$$

Then the claim directly comes from the fact that this monomial can be split into two coprime factors $t_{i_1} \cdots t_{i_\alpha - \alpha + 1}$ and $z_{i^*_{k+1}} t_{i^*_{\alpha+1} - \alpha} \cdots t_{i^*_k - k + 1}$, each dividing $\mathrm{LM}(\Delta(\boldsymbol{i}))$ and $\mathrm{LM}(\Delta(\boldsymbol{i^*}))$, respectively. Indeed, both factors are coprime because $i_1 \leq \cdots \leq i_\alpha - \alpha + 1 < i^*_\alpha - \alpha + 1 \leq i^*_{\alpha+1} - \alpha \leq \cdots \leq i^*_{k+1} - k$. □

We call *adjacent pair* to any pair of minors $\Delta(\boldsymbol{i})$ and $\Delta(\boldsymbol{i^*})$ such that $\boldsymbol{i}$ and $\boldsymbol{i^*}$ differ only at position α, for some $1 \leq \alpha \leq k+1$, that is $i_j = i^*_j$ if $j \neq \alpha$ and $i_\alpha < i^*_\alpha$. This pair can be actually described by an increasing sequence of length $k+2$, $1 \leq i_1 < \cdots < i_\alpha < i^*_\alpha < \cdots < i_{k+1} \leq k + d \in \binom{k+d}{k+2}$ and the index α. The previous claim allows us to build a path connecting any two $(k+1)$-minors such that every consecutive pairs of minors in the path is an adjacent pair. An example for $k = 5$ is depicted below. The numbers in every column in the table correspond to the indices of the rows in every minor in the path connecting $\Delta(1, 5, 6, 9, 12, 13)$ and $\Delta(2, 4, 7, 8, 11, 14)$.

i_1	1	1	1	1	1	**1**	**2**
i_2	**5**	**4**	4	4	4	4	4
i_3	6	6	6	6	**6**	**7**	7
i_4	9	**9**	**8**	8	8	8	8
i_5	12	12	**12**	**11**	11	11	11
i_6	13	13	13	**13**	**14**	14	14

[6] The reduction algorithm repeatedly takes a polynomial $\mathfrak{p}$ and checks whether some $\mathrm{LM}(\mathfrak{g}_i)$ divides $\mathrm{LM}(\mathfrak{p})$. If so, the algorithm cancels out the leading term of $\mathfrak{p}$ by substracting from it the appropriate multiple of $\mathfrak{g}_i$, and repeats the procedure with the resulting polynomial. Otherwise, the algorithm adds the leading term of $\mathfrak{p}$ to the output polynomial and proceeds with the remaining terms of $\mathfrak{p}$, until they are exhausted. The output has the property that none of its monomials is divisible by any $\mathrm{LM}(\mathfrak{g}_i)$.

Using the above path we show that, according to Buchberger's chain criterion, to prove that G is a Gröbner basis it suffices to check only the S-polynomials of adjacent pairs.

Claim 2. If the S-polynomial of every adjacent pair of $(k+1)$-minors is reducible to 0, then so are all the other S-polynomials (and therefore G is a Gröbner basis of $\mathfrak{H}$).

Proof (of Claim 2). We prove the claim by (descending) induction in α, the index of the first row-difference between two $(k+1)$-minors. For $\alpha = k+1$ (*i.e.*, the minors only differ in the last row) the statement is obviously true, as the two minors form an adjacent pair. Now, let us assume that the statement is true for $\alpha = \alpha_0$, where $1 < \alpha_0 \leq k+1$. Then for any two minors with the first row-difference occurring at row $\alpha_0 - 1$, say $\mathfrak{g} = \Delta(i_1, \ldots, i_{\alpha_0-2}, i_{\alpha_0-1}, \ldots, i_{k+1})$ and $\mathfrak{g}^* = \Delta(i_1, \ldots, i_{\alpha_0-2}, i^*_{\alpha_0-1}, \ldots, i^*_{k+1})$ with $i_{\alpha_0-1} < i^*_{\alpha_0-1}$, we define as in the first claim the "hybrid" minor $\mathfrak{h} = \Delta(i_1, \ldots, i_{\alpha_0-1}, i^*_{\alpha_0}, \ldots, i^*_{k+1})$. Then, by Claim 1 we know that $\mathrm{LM}(\mathfrak{h})$ divides $\mathrm{lcm}(\mathrm{LM}(\mathfrak{g}), \mathrm{LM}(\mathfrak{g}^*))$. On the other hand, the induction assumption implies $\mathrm{RED}_G(\mathrm{SPOL}(\mathfrak{h}, \mathfrak{g})) = 0$, since the first row-difference between $\mathfrak{g}$ and $\mathfrak{h}$ occurs at row α_0. Moreover, $\mathrm{RED}_G(\mathrm{SPOL}(\mathfrak{h}, \mathfrak{g}^*)) = 0$ because $(\mathfrak{h}, \mathfrak{g}^*)$ is an adjacent pair. Thus, by Buchberger's chain criterion, $\mathrm{RED}_G(\mathrm{SPOL}(\mathfrak{g}, \mathfrak{g}^*)) = 0$, concluding the proof of the second claim. □

The last step in the proof of the theorem is showing that the S-polynomial of every adjacent pair of $(k+1)$-minors is reducible to 0. Actually, the S-polynomial of an adjacent pair of minors can be embedded into the determinant of a $(k+2) \times (k+2)$ matrix. This matrix gives us a syzygy (*i.e.*, a linear relation with polynomial coefficients among elements in G) that allows to manually reduce the S-polynomial to 0.

Claim 3. For any adjacent pair of $(k+1)$-minors given by the sequence $\boldsymbol{i} \in \binom{k+d}{k+2}$ and the index $1 \leq \alpha \leq k+1$, that is $\mathfrak{g} = \Delta(i_1, \ldots, i_\alpha, i_{\alpha+2} \ldots, i_{k+2})$ and $\mathfrak{g}^* = \Delta(i_1, \ldots, i_{\alpha-1}, i_{\alpha+1} \ldots, i_{k+2})$, $\mathrm{RED}_G(\mathrm{SPOL}(\mathfrak{g}, \mathfrak{g}^*)) = 0$.

Proof (of Claim 3). Let us consider for the case $\alpha \leq k$ the extended matrix

$$\mathbf{B} = \begin{pmatrix} t_{i_1} & t_{i_1-1} & \cdots & t_{i_1-k+1} & z_{i_1} & t_{i_1-\alpha+1} \\ \vdots & \vdots & \vdots\vdots & \vdots & \vdots & \vdots \\ t_{i_\alpha} & t_{i_\alpha-1} & \cdots & t_{i_\alpha-k+1} & z_{i_\alpha} & t_{i_\alpha-\alpha+1} \\ t_{i_{\alpha+1}} & t_{i_{\alpha+1}-1} & \cdots & t_{i_{\alpha+1}-k+1} & z_{i_{\alpha+1}} & t_{i_{\alpha-1}-\alpha+1} \\ \vdots & \vdots & \vdots\vdots & \vdots & \vdots & \vdots \\ t_{i_{k+2}} & t_{i_{k+2}-1} & \cdots & t_{i_{k+2}-k+1} & z_{i_{k+2}} & t_{i_{k+2}-\alpha+1} \end{pmatrix}$$

which is a $(k+2) \times (k+2)$ matrix[7] with two repeated columns: the α-th and the last columns. Thus, $\det \mathbf{B} = 0$, and using Laplace expansion of the determinant along the last column we obtain the following syzygy:

$$\sum_{\substack{j=1 \\ j \neq \alpha, \alpha+1}}^{k+2} (-1)^{k+j} t_{i_j-\alpha+1} \mathfrak{h}_j + (-1)^{k+\alpha} \left(t_{i_\alpha-\alpha+1} \mathfrak{g}^* - t_{i_{\alpha+1}-\alpha+1} \mathfrak{g} \right) = 0 \tag{2}$$

where $\mathfrak{h}_j = \Delta(i_1, \ldots, i_{j-1}, i_{j+1}, \ldots, i_{k+2})$. Actually, $\mathfrak{g} = \mathfrak{h}_\alpha$ and $\mathfrak{g}^* = \mathfrak{h}_{\alpha+1}$.

Notice that the S-polynomial $\mathfrak{s} = \mathrm{SPOL}(\mathfrak{g}, \mathfrak{g}^*)$, as given by Equation 1, is exactly $t_{i_{\alpha+1}-\alpha+1}\mathfrak{g} - t_{i_\alpha-\alpha+1}\mathfrak{g}^*$, since

$$\mathrm{LM}(\mathfrak{g}) = z_{i_{k+2}} t_{i_1} \cdots t_{i_\alpha-\alpha+1} t_{i_{\alpha+2}-\alpha} \cdots t_{i_{k+1}-k+1}$$

and

$$\mathrm{LM}(\mathfrak{g}^*) = z_{i_{k+2}} t_{i_1} \cdots t_{i_{\alpha-1}-\alpha+2} t_{i_{\alpha+1}-\alpha+1} \cdots t_{i_{k+1}-k+1}$$

[7] Recall that we are using the notational convention introduced in Lemma 16. Thus, some entries in the matrix can be equal to 0 or 1.

As a consequence, Equation 2 gives an explicit reduction of $\mathfrak{s}$ to 0. Namely,

$$\mathfrak{s} = \sum_{\substack{j=1 \\ j\neq\alpha,\alpha+1}}^{k+2} (-1)^{\alpha+j} t_{i_j-\alpha+1}\mathfrak{h}_j \tag{3}$$

Actually, to see that Equation 3 implies $\mathrm{RED}_G(\mathfrak{s}) = 0$, we only need to show that all leading monomials $\mathfrak{n}_{\alpha,j} = \mathrm{LM}(t_{i_j-\alpha+1}\mathfrak{h}_j) = t_{i_j-\alpha+1}\mathrm{LM}(\mathfrak{h}_j)$, for $j = 1,\ldots,k+2$, $j \neq \alpha, \alpha+1$, corresponding to nonzero terms[8] are different. We now compute all leading monomials $\mathfrak{n}_{\alpha,j}$ for any $j \neq \alpha, \alpha+1$ (written as possibly unsorted products):

$$\mathfrak{n}_{\alpha,j} = \begin{cases} z_{i_{k+2}} t_{i_1-\alpha+1} t_{i_2} \cdots t_{i_{k+1}-k+1} & \text{for } j = 1 \\ z_{i_{k+2}} t_{i_1} \cdots t_{i_{j-1}-j+2} t_{i_j-\alpha+1} t_{i_{j+1}-j+1} \cdots t_{i_{k+1}-k+1} & \text{for } 1 < j < k+1 \\ z_{i_{k+2}} t_{i_1} \cdots t_{i_k-k+1} t_{i_{k+1}-\alpha+1} & \text{for } j = k+1 \\ z_{i_{k+1}} t_{i_1} \cdots t_{i_k-k+1} t_{i_{k+2}-\alpha+1} & \text{for } j = k+2 \end{cases}$$

Clearly, $\mathfrak{n}_{\alpha,k+2}$ is different to the others, and the only coincidence can be $\mathfrak{n}_{\alpha,j} = \mathfrak{n}_{\alpha,j^*}$ for some $1 \leq j < j^* \leq k+1$. But this would imply (removing all common terms)

$$t_{i_j-\alpha+1} t_{i_{j+1}-j+1} \cdots t_{i_{j^*-1}-j^*+3} t_{i_j^*-j^*+2} = t_{i_j-j+1} t_{i_{j+1}-j} \cdots t_{i_{j^*-1}-j^*+2} t_{i_j^*-\alpha+1}$$

But due to the inequalities of the indices, the least index in the righthand side, $i_j - j + 1$, can only be cancelled out with the term $i_j - \alpha + 1$ in the lefthand side, thus implying $j = \alpha$. Similarly, $i_j^* - j^* + 2$ on the left must be the same as $i_j^* - \alpha + 1$ on the right, and then $j^* = \alpha + 1$. But these values of j, j^* are out of the correct range, what shows that no collision among the $\mathfrak{n}_{\alpha,j}$ is actually possible.

For the remaining case, $\alpha = k+1$, we proceed similarly, defining

$$\mathbf{B} = \begin{pmatrix} t_{i_1} & t_{i_1-1} & \cdots & t_{i_1-k+1} & z_{i_1} & z_{i_1} \\ \vdots & \vdots & \vdots\vdots & \vdots & \vdots & \vdots \\ t_{i_{k+1}} & t_{i_{k+1}-1} & \cdots & t_{i_{k+1}-k+1} & z_{i_{k+1}} & z_{i_{k+1}} \\ t_{i_{k+2}} & t_{i_{k+2}-1} & \cdots & t_{i_{k+2}-k+1} & z_{i_{k+2}} & z_{i_{k+2}} \end{pmatrix}$$

Now, the syzygy is

$$\sum_{j=1}^{k} (-1)^{k+j} z_{i_j}\mathfrak{h}_j - z_{i_{k+1}}\mathfrak{g}^* + z_{i_{k+2}}\mathfrak{g} = 0$$

where $\mathfrak{h}_j = \Delta(i_1,\ldots,i_{j-1},i_{j+1},\ldots,i_{k+2})$. Then

$$\mathfrak{s} = \mathrm{SPOL}(\mathfrak{g},\mathfrak{g}^*) = z_{i_{k+2}}\mathfrak{g} - z_{i_{k+1}}\mathfrak{g}^* = -\sum_{j=1}^{k} (-1)^{k+j} z_{i_j}\mathfrak{h}_j \tag{4}$$

and for any $j < k+1$

$$\mathfrak{n}_{k+1,j} = \mathrm{LM}(z_{i_j}\mathfrak{h}_j) = z_{i_j}\mathrm{LM}(\mathfrak{h}_j) = \begin{cases} z_{i_1} z_{i_{k+2}} t_{i_2} t_{i_3-1} \cdots t_{i_{k+1}-k+1} & \text{for } j = 1 \\ z_{i_j} z_{i_{k+2}} t_{i_1} \cdots t_{i_{j-1}-j+2} t_{i_{j+1}-j+1} \cdots t_{i_{k+1}-k+1} & \text{for } 1 < j < k+1 \end{cases}$$

which are clearly different. This shows that again Equation 4 is a reduction to 0 of $\mathrm{SPOL}(\mathfrak{g},\mathfrak{g}^*)$, which covers all the remaining adjacent pairs of $(k+1)$-minors. □

Now, the theorem statement is a direct consequence of Claims 2 and 3.

[8] Some terms in Equation 3 can be zero due to $t_{i_j-\alpha+1} = 0$, what happens exactly when $i_j - \alpha + 1 \leq 0$ or $i_j - \alpha + 1 \geq d + 2$

The next corollary finally proves that $\mathcal{CI}_{k,d}$ is a hard matrix distribution, that is, the $\mathcal{CI}_{k,d}$-MDDH problem is generically hard in k-linear groups.

Corollary 2. *All nonzero polynomials in $\mathfrak{H}$ have degree at least $k+1$.*

Proof. According to Lemma 16 the degree of all polynomials $\Delta(\boldsymbol{i})$ for $\boldsymbol{i} \in \binom{k+d}{k+1}$ is exactly $k+1$. Thus, by Lemma 15 and Theorem 3 the statement follows directly.