Equivalences and Black-Box Separations of Matrix Diffie-Hellman Problems

Jorge L. Villar[1] *

Universitat Politècnica de Catalunya, Spain
jorge.villar@upc.edu

Abstract. In this paper we provide new algebraic tools to study the relationship between different Matrix Diffie-Hellman (MDDH) Problems, which are recently introduced as a natural generalization of the so-called Linear Problem. Namely, we provide an algebraic criterion to decide whether there exists a generic black-box reduction, and in many cases, when the answer is positive we also build an explicit reduction with the following properties: it only makes a single oracle call, it is tight and it makes use only of operations in the base group.
It is well known that two MDDH problems described by matrices with a different number of rows are separated by an oracle computing certain multilinear map. Thus, we put the focus on MDDH problems of the same size. Then, we show that MDDH problems described with a different number of parameters are also separated (meaning that a successful reduction cannot decrease the amount of randomness used in the problem instance description).
When comparing MDDH problems of the same size and number of parameters, we show that they are either equivalent or incomparable. This suggests that a complete classification into equivalence classes could be done in the future. In this paper we give some positive and negative partial results about equivalence, in particular solving the open problem of whether the Linear and the Cascade MDDH problems are reducible to each other.
The results given in the paper are limited by some technical restrictions in the shape of the matrices and in the degree of the polynomials defining them. However, these restrictions are also present in most of the work dealing with MDDH Problems. Therefore, our results apply to all known instances of practical interest.

Keywords: Matrix Diffie-Hellman problems, Black-box reductions, Decisional linear assumption, Black-box separations.

1 Introduction

Matrix Decisional Diffie-Hellman (MDDH) Problems were recently introduced in [9] as a natural generalization of the Linear Problem, and they have found

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

many applications (see, for instance [1–9]) and they are further generalized to computational problems in [13, 15]. A MDDH problem is defined as a set of matrices $\mathbf{A} \in \mathbb{Z}_q^{\ell \times k}$, for $\ell > k$, sampled from a probability distribution $\mathcal{D}_{\ell,k}$. Informally, the $\mathcal{D}_{\ell,k}$-MDDH problem is telling apart the two probability distributions $([\mathbf{A}], [\mathbf{A}\boldsymbol{w}])$ and $([\mathbf{A}], [\boldsymbol{z}])$, where $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, $\boldsymbol{w} \leftarrow \mathbb{Z}_q^k$ and $\boldsymbol{z} \leftarrow \mathbb{Z}_q^\ell$. The bracket notation (also called 'implicit' notation) means giving the vectors and matrices "in the exponent" (see Sect. 2). Most interesting examples correspond to the case $\ell = k + 1$, and usually $\mathcal{D}_{\ell,k}$ is defined by evaluating a degree-one polynomial map $\mathbf{A}(\boldsymbol{t})$ on a random point $\boldsymbol{t} \in \mathbb{Z}_q^d$ (we denote this problem as $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$). [1]

The broadly used DDH and k-Lin problems are indeed instances of MDDH problems (namely, $\mathcal{L}_1$-MDDH and $\mathcal{L}_k$-MDDH problems). Other useful instances were introduced in [9, 15], like the Cascade ($\mathcal{C}_k$-MDDH) and the Symmetric Cascade ($\mathcal{SC}_k$-MDDH) problems (see Sect. 2.3 for more details on these examples). This wide range of decisional problems is typically organized into families of increasing hardness, allowing us to trade compactness for hardness. In particular, $\mathcal{C}_k$-MDDH and $\mathcal{L}_k$-MDDH both depend on k parameters, and they offer the same security guarantees (generically), while $\mathcal{SC}_k$-MDDH has optimal representation size (only one parameter) but it is supposed to be easier than $\mathcal{C}_k$-MDDH. The applications of the MDDH problems that appeared in the papers listed above suggest that, in most scenarios, the k-Lin problem can be successfully replaced by any other hard MDDH problem.

Using tools from algebraic geometry, in [9] a general criterion for the hardness of $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ in the (symmetric) k-linear generic group model is given, based on the properties of the so-called determinant polynomial $\mathfrak{d}_{\mathbf{A}}$ associated to the MDDH problem. This criterion is one of the few known general theorems that transforms the problem of proving the generic hardness of a computational problem, chosen from a wide family, into a simple algebraic problem. This can be done thanks to a purely algebraic reformulation of the generic group model formalized by Maurer in [14], including also the multilinear map functionality. A clear and detailed reference for this algebraic reformulation, applied to a very general generic group model supporting several groups and homomorphisms among them, can be found in [4].

Although proving the hardness of a problem in a generic model does not give all the guarantees about the security of the protocols based on it, at least, it constitutes a proof that the protocol is well-designed. Indeed, the meaning of a

[1] MDDH problems beyond these technical limitations are hard to use because, firstly, there are no known efficient algebraic tools to show the generic hardness of unbounded families of $\mathcal{D}_{\ell,k}$-MDDH problems with $\ell > k+1$, meaning that the hardness must be proven individually for every instance in the family. Secondly, dealing with MDDH problems defined by non-linear polynomial maps produces the same effect in the generic hardness analysis, and in addition, it limits the practical applicability of the MDDH problem instances. Indeed, in the linear case, $[\mathbf{A}]$ (typically required to be publicly known) can be easily recovered by evaluating the polynomial map in the exponent, given only the parameters $[\boldsymbol{t}]$. This compression of the public information is partially lost when using polynomial maps of higher degree.

problem being hard on a generic group is that the only possible successful algorithms solving it are specific to a particular choice of the base group. Moreover, even when a specific attack against a protocol based on such problem is found, there is still the possibility to avoid it by properly changing the base group. For instance, the subexponential algorithms solving the Discrete Logarithm problem in certain groups have no known equivalent in the realm of random elliptic curves. On the other hand, even if we know that two problems are generically hard, it still makes sense looking for reductions (or separations) between them, because they have implications about the impact of solving one of the problems implemented on a specific group family.

Indeed, in the current candidates for multilinear maps (or the richer structure called graded encodings) considered in the literature, most decisional problems inspired on DDH (including the MDDH problems) are easy. However, these attacks are specific to the platforms considered in the constructions, and they do not rule out the existence of other constructions in the future. Therefore, the research on general results about the hardness and relationship of decisional problems related to DDH remains to be of great theoretical interest.

Finding reductions between decisional problems is a rather difficult task: A decisional problem typically specifies two probability distributions that are hard to tell apart, and then the reduction has to transform the two specific probability distributions defining one of the problems into the two distributions defining the other, tolerating only a negligible error probability. One can find many subtleties when trying to build such reductions, or to rule out their existence, as shown for example in [16]. Most known reductions fall in the class of black-box reductions, and they typically use the base groups in a generic way. This suggests the possibility of finding an algebraic formulation that captures the notion of generic black-box reducibility for a wide family of decisional problems, assuming that their description is uniform enough. A natural candidate is the family of MDDH problems. However, known results about equivalence or separation of MDDH problems essentially reduce to:

- [9]. $\mathcal{D}_{\ell,k}$-MDDH and $\mathcal{D}_{\ell',k'}$-MDDH problems with $k < k'$ are separated by an oracle that computes a $(k+1)$-linear map.[2] Namely, $\mathcal{D}_{\ell,k}$-MDDH is easily solved by means of the oracle, while $\mathcal{D}_{\ell',k'}$-MDDH could remain hard (*e.g.*, it can still be hard in the generic k'-linear group model).
- [10]. All hard $\mathcal{D}^{\mathbf{A}}_{\ell,k}$-MDDH problems with $\ell = k+1$, described by a univariate degree-one polynomial map $\mathbf{A}(t)$ are equivalent.
- [10]. By using randomization and "algebraic reductions" one can obtain reductions between some known families of MDDH problems. For instance, $\mathcal{SC}_k$-MDDH is reduced to $\mathcal{C}_k$-MDDH, and all $\mathcal{D}_{\ell,k}$-MDDH problems reduce to $\mathcal{U}_{\ell,k}$-MDDH problems (based on the uniform matrix distribution).

[2] This is actually valid in the general case provided that k is constant (*i.e.*, independent of the security parameter). However, for some compact matrix distributions, including $\mathcal{L}_k$, $\mathcal{C}_k$ and $\mathcal{SC}_k$), a $(k+1)$-linear map can efficiently solve the $\mathcal{D}_{\ell,k}$-MDDH problem even when k grows linearly in the complexity parameter.

Many other questions remain unanswered. For instance, it is an open problem whether a reduction between $\mathcal{C}_k$-MDDH and $\mathcal{L}_k$-MDDH exists, in either way.

In this paper we focus on the general problem of finding a simple algebraic criterion for the existence of reductions between two MDDH problems with the same size k. When the answer is positive, we also try to build a simple reduction. The results we provide here are a first step of the big project of classifying all MDDH assumptions (or at least a wide family of them) into equivalence classes.

1.1 Our Results

The main theorem in [9, 10] gives sufficient conditions for the hardness, in the generic k-linear group model, of a wide family of MDDH problems defined by polynomial matrix distributions $\mathcal{D}_k^{\mathbf{A}}$, based on some properties (degree and irreducibility) of the determinant polynomial $\mathfrak{d}_{\mathbf{A}}$ (*i.e.*, the determinant of $\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z}$ as a polynomial in $(\boldsymbol{t}, \boldsymbol{z})$, see Definition 8). In the particular case of one-parameter polynomial matrix distributions, the converse theorem is also proved in [10]. We prove that a similar converse also holds for matrix distributions with many parameters in Theorem 3, by using different techniques. We also give additional technical properties that any $\mathfrak{d}_{\mathbf{A}}$ must fulfil when $\mathcal{D}_k^{\mathbf{A}}$ is hard (*i.e.*, the $\mathcal{D}_k^{\mathbf{A}}$-MDDH problem is hard in the generic k-linear group model), and they are based on the geometric notion called elusiveness, recently introduced in [15].

Our main contribution is giving positive and negative results about the existence of black-box reductions between the two generically hard problems $\mathcal{D}_k^{\mathbf{A}}$-MDDH and $\mathcal{D}_k^{\mathbf{B}}$-MDDH defined by degree-one polynomial matrix distributions with d and e parameters, respectively. The first result shows how to extract from any successful generic black-box reduction with polynomially-many oracle calls a polynomial map f of degree one fulfilling the simple polynomial equation

$$\lambda \mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f \qquad (1)$$

(Informal) Theorem 4 *If there exists a generic black-box reduction from the $\mathcal{D}_k^{\mathbf{A}}$-MDDH problem to the $\mathcal{D}_k^{\mathbf{B}}$-MDDH problem, then Eq. 1 is satisfied by some polynomial map f, for some nonzero constant λ.*

This polynomial map is also shown to be injective, which means that necessarily $e \geq d$, that is, a successful generic black-box reduction cannot decrease the number of parameters, or equivalently, it cannot derandomize the instance of $\mathcal{D}_k^{\mathbf{A}}$-MDDH to build an instance of $\mathcal{D}_k^{\mathbf{B}}$-MDDH. This result itself is enough to show a black-box separation between MDDH problems defined from the distributions $\mathcal{SC}_k$ and $\mathcal{C}_k$, and also $\mathcal{L}_k$ and $\mathcal{U}_k$, for the same size k. At this point, we know many black-box separations between MDDH problems. Informally, bigger problems do not reduce to smaller problems, and problems with many parameters do not reduce to problems with fewer parameters.

To gain a deeper understanding of the reducibility of MDDH problems, we show that Eq. 1 captures it by proving the converse of Theorem 4.

(Informal) Theorem 5 *If there exists a solution to Eq. 1, then*

1. *there exists a black-box deterministic reduction from* $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ *to* $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$*, using a single oracle call, that succeeds with overwhelming probability if the oracle is perfect.*
2. *if in addition* f *is surjective, then the reduction is actually a tight black-box reduction, and it works for any imperfect oracle.*
3. *otherwise, if* $\mathcal{D}_k^{\mathbf{B}}$ *is random self-reducible, then there also exists a (probabilistic) tight black-box reduction with the same properties.*

The last item requires a stronger notion of random self-reducibility, compared to the one used in [9, 10], in which not only the vector $\boldsymbol{z}$, but also the matrix $\mathbf{A}$ is randomized. We prove in this paper that the usual matrix distributions $\mathcal{C}_k$, $\mathcal{SC}_k$, $\mathcal{L}_k$, $\mathcal{RL}_k$ and the uniform one are random self-reducible in this stronger way. These results directly show that, among other relations, $\mathcal{SC}_k$-MDDH reduces to $\mathcal{C}_k$-MDDH, and $\mathcal{L}_k$-MDDH reduces to $\mathcal{RL}_k$-MDDH, as one can expect.

The previous theorem is extremely powerful when $e = d$, since then any possible solution f to Eq. 1 must be a bijective map. Thus, using the inverse map we also show in Theorem 6 that $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ and $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$ are either equivalent (by simple tight reductions involving only operations in the base group), or they are incomparable by generic black-box reductions. This fact opens the possibility to build an entire classification of all degree-one polynomial MDDH problems into equivalence classes. Although we leave the general problem open, we also provide some partial results and tools to carry out the classification. Recall that all MDDH problems in an equivalence class must have the same size and number of parameters.

In the positive way, we give two easy-to-check sufficient conditions for equivalence: the first one directly uses the determinant polynomial, while the second is related to a polynomial vector space $X_{\mathbf{A}}$ associated to any polynomial matrix distribution (in the way defined in [12]),

(Informal) Corollary 2 *If* $\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}}$*, then* $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH} \Leftrightarrow \mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$*.*

(Informal) Corollary 3 *If* $X_{\mathbf{A}} = X_{\mathbf{B}}$*, then* $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH} \Leftrightarrow \mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$*.*

Actually, the second result implies the first, since the polynomial vector space $X_{\mathbf{A}}$ is determined by $\mathfrak{d}_{\mathbf{A}}$. However, the equality of determinant polynomials can be checked trivially, while the equality of two vector spaces (given by generating sets) involves some linear algebra computations.

Although most natural algebraic reductions of matrix problems keep $X_{\mathbf{A}}$ invariant, there are other less natural reductions that do not, and therefore the equality of polynomial vector spaces does not solve the equivalence problem completely. Nevertheless, the special case of the one-parameter family of degree-one polynomial matrix distributions is completely solved since there is only one possible choice for the vector space $X_{\mathbf{A}}$, and then all hard one-parameter MDDH problems are equivalent. This result has proved in [10] in a rather different way.

Next, we address the problem of showing separations between $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ and $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$ with $e = d \geq 1$, like for instance $\mathcal{C}_k$-MDDH and $\mathcal{L}_k$-MDDH.

Although one can try to show directly that Eq. 1 has no solutions, it is a cumbersome task when k and d grow. This kind of problem is often solved by looking for invariant objects. Namely, we look for easy-to compute objects associated to matrix distributions, such that they are constant within an equivalence class, while they typically change between different equivalence classes. In this paper, we propose two invariant objects: the singular locus and the automorphism group. Roughly speaking, for every matrix distribution $\mathcal{D}_k^{\mathbf{A}}$ we can define the algebraic variety $V_{\mathbf{A}}$ containing all the zeros of the determinant polynomial, and also the automorphism group $\mathrm{Aut}_{\mathbf{A}}$ containing all bijective polynomial maps that leave $V_{\mathbf{A}}$ invariant. Then,

(Informal) Lemma 6 *If* $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH} \Leftrightarrow \mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$*, then* $V_{\mathbf{A}}$ *and* $V_{\mathbf{B}}$ *have the same number of (rational) singular points.*

(Informal) Lemma 7 *If* $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH} \Leftrightarrow \mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$*, then* $\mathrm{Aut}_{\mathbf{A}} \cong \mathrm{Aut}_{\mathbf{B}}$.

The singular locus turns to be quite easy to compute for matrix distributions. Indeed we use it to solve the open problem of the black-box separation between $\mathcal{L}_k$-MDDH and $\mathcal{C}_k$-MDDH. Namely, we show that the variety associated to $\mathcal{L}_k$ has singular points, while the one corresponding to $\mathcal{C}_k$ has not. This suggests that $\mathcal{C}_k$ is "cleaner" than $\mathcal{L}_k$, so the former would be a preferable choice (as singular points are associated to easy problem instances).

However, the singular locus is a too coarse invariant, meaning that many non-equivalent matrix distributions have no singular points, and then they cannot be separated using this technique. We propose a second invariant which is presumably finer that the singular locus, the group of black-box self-reductions, or the group of automorphisms of the matrix distribution. Although computing the whole group is a hard task, we could compute only some property of the group, like the number of elements of order two. However, we could not give any concrete example such that this technique is simpler than directly showing the nonexistence of solutions to Eq. 1.

1.2 Roadmap

In Sect. 2 we describe the basics about MDDH problems, the known generic hardness results, and a new more general "converse" theorem is given in Sect. 3. The main contributions are in Sect. 4 and 5. In the former we show the importance of Eq. 1 for the reducibility of MDDH problems, while the latter deals with the classification of MDDH problems with the same number of parameters. In particular, we give the separation result between of the most used MDDH problems: the $\mathcal{C}_k$-MDDH and the $\mathcal{L}_k$-MDDH problems.

2 Preliminaries

2.1 Additive Notation for Group Elements

In this paper we adopt the additive notation for group operations, as it is now a *de facto* standard for papers dealing with matrix problems. Let $\mathbb{G}$ be a cyclic group of prime-order q and g a generator of $\mathbb{G}$. We will denote every group element $h \in \mathbb{G}$ by its (possibly unknown) discrete logarithm with respect to the generator g. More precisely, we will write $h = [x]$, where $x \in \mathbb{Z}_q$ such that $h = g^x$. We naturally extend this notation to vectors and matrices. Thus, for a matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_q^{n\times m}$, we will write $[\mathbf{A}] = (g^{a_{ij}}) \in \mathbb{G}^{n\times m}$.

Notice that computing $x \in \mathbb{Z}_q$ from $[x] \in \mathbb{G}$ is hard, since it means solving the Discrete Logarithm Problem in $\mathbb{G}$. Similarly, given $[x], [y] \in \mathbb{G}$ and $z \in \mathbb{Z}_q$, one can efficiently compute $[x + y], [xz], [yz] \in \mathbb{G}$ but not $[xy] \in \mathbb{G}$, since the latter would mean solving the Computational Diffie-Hellman Problem in $\mathbb{G}$.

For a non-degenerated bilinear symmetric pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ we use a similar notation. For $[x], [y] \in \mathbb{G}$ we will write $[z]_T = [xy]_T = e([x], [y])$, where, as one would expect, $[z]_T = g_T^z \in \mathbb{G}_T$ and $[1]_T = g_T = e(g, g)$ is a generator of G_T. Similarly, for a k-linear map $e : \mathbb{G}^k \to \mathbb{G}_T$ we will write $[z]_T = [x_1 \cdots x_k]_T = e([x_1], \ldots, [x_k])$.

2.2 A Generic Model for Groups With a Multilinear Map

In this section we sketch the random-encodings based and the purely-algebraic generic models for groups with a multilinear map, used in the paper. The latter is similar to the model used in [4, 9, 11], and it is a purely algebraic version of Maurer's generic group model [14] including the k-linear map functionality.

As we are dealing with decisional problems entirely described by group elements, we can notably simplify the exposition. Consider first Maurer's model, in which an algorithm $\mathcal{A}$ does not deal with proper group elements in $\mathbb{G}$ or $\mathbb{G}_T$, but only with labels, and it has access to an additional oracle internally performing the group operations. Namely, on start $\mathcal{A}$ receives the labels $(X_1, 1), \ldots, (X_n, 1)$, corresponding to some group elements $[x_1], \ldots, [x_n] \in \mathbb{G}$ (along with some additional labels $(0, 1), (1, 1), (0, T), (1, T)$ corresponding to $[0], [1], [0]_T, [1]_T$, which we assume are implicitly given to $\mathcal{A}$). Then $\mathcal{A}$ can adaptively make the following queries to the generic group oracle:

- GroupOp$((Y_1, i), (Y_2, i))$, $i \in \{1, T\}$: group operation in $\mathbb{G}$ or $\mathbb{G}_T$ for two previously issued labels, resulting in a new label (Y_3, i).
- GroupInv$((Y_1, i))$, $i \in \{1, T\}$: group inversion in $\mathbb{G}$ or $\mathbb{G}_T$, resulting in a new label (Y_2, i).
- GroupML$((Y_1, 1), \ldots, (Y_k, 1))$: k-linear map of k previously issued labels in $\mathbb{G}$, resulting in a new label (Y_{k+1}, T).
- GroupEqTest$((Y_1, i), (Y_2, i))$, $i \in \{1, T\}$: test two previously issued labels in $\mathbb{G}$ or $\mathbb{G}_T$ for equality of the corresponding group elements, resulting in a bit (1 indicates equality). Here, the oracle stores the actual input group elements and the results of the operations corresponding to the oracle calls.

Every badly formed query (for instance, containing an unknown label) is answered with a special rejection symbol $\perp$. Similarly, the output of $\mathcal{A}$ consists of some labels $(Z_1, 1), \ldots, (Z_a, 1), (Z_{a+1}, T), \ldots, (Z_{a+b}, T)$ representing group elements in either $\mathbb{G}$ or $\mathbb{G}_T$, and perhaps some non-group elements $\widetilde{z}$.

In a generic group model based on random encodings, every group element handled by the algorithm is replaced by a random label (just a string selected from a large enough set, in order to prevent guessing a valid label from scratch). The generic oracle keeps the real group elements (or elements in an isomorphic copy of the group) associated to the labels, and carries out all group operations queried by the algorithm. The label mapping is injective, meaning that equal group elements (perhaps resulting from different computations) are assigned to the same label. Therefore, only the first three oracle queries ($\mathsf{GroupOp}$, $\mathsf{GroupInv}$ and $\mathsf{GroupML}$) are necessary in this generic group model. The $\mathsf{GroupEqTest}$ query is now trivial due to the mentioned injectivity.

On the other hand, in the purely algebraic generic model, the labels are indeed polynomials in $\boldsymbol{X} = (X_1, \ldots, X_n)$. More precisely the labels are (Y, i) for $Y \in \mathbb{Z}_q[\boldsymbol{X}]$ and $i \in \{1, T\}$. The oracle no longer performs group operations but only polynomial operations in the labels. As a consequence, the labels received by $\mathcal{A}$ are completely predictable to it, that is, $\mathcal{A}$ knows the coefficients of every label Y as a polynomial in $\boldsymbol{X}$, for every intermediate group element handled during the computations, including the group elements in the output. Observe that due to the limitation in the oracle syntax, the elements in $\mathbb{G}$ correspond to polynomials of degree at most 1, while the elements in $\mathbb{G}_T$ correspond to polynomials of degree at most k. And these are the only polynomials that can appear in the labels.

To model the possible constraints in the inputs $[x_1], \ldots, [x_n]$, we assume that $\boldsymbol{x} = (x_1, \ldots, x_n)$ is sampled by evaluating a polynomial map $\mathfrak{h}$ at a a uniformly distributed random point $\boldsymbol{s} \in \mathbb{Z}_q^d$. Thus, the generic group oracle formally assigns polynomials $X_1, \ldots, X_n \in \mathbb{Z}_q[\boldsymbol{S}]$ to the input labels. Then, the oracle call $\mathsf{GroupEqTest}$ is modified and it just compares the labels as polynomials in $\boldsymbol{S}$. This modification in the oracle only amounts into a negligible difference between the models. Indeed, as a usual step in generic model proofs, detecting the model difference means finding a (bounded degree) polynomial that vanishes at a random point $\boldsymbol{s}$, and this probability is shown to be negligible by using Schwartz-Zippel Lemma and the union bound.

All the information $\mathcal{A}$ can obtain from the purely algebraic generic group oracle is via the equality test queries, since for any intermediate group element $\mathcal{A}$ knows the corresponding polynomial in $\boldsymbol{X}$, but not necessarily the associated polynomial in $\boldsymbol{S}$. When dealing with a decisional problem, there are two different sampling polynomial maps $\mathfrak{h}_0, \mathfrak{h}_1$, and $\mathcal{A}$'s goal is guessing which one is used by the generic group oracle. In this setting, $\mathcal{A}$ wins if it finds two different "computable" polynomials (i.e., of degree at most k) in $\boldsymbol{X}$ such that they are equal when composed to $\mathfrak{h}_0$, but they are different when composed to $\mathfrak{h}_1$, or vice versa. Proving that the decisional problem is generically hard exactly means proving that such polynomials do not exist.

When dealing with algorithms in the generic group model with access to extra oracles (e.g. reductions), the transition between a generic group model based on random encodings to its purely algebraic counterpart is a bit more subtle. This is mainly due to the interaction of the generic model with the extra oracle, which can leak some information about the group elements themselves. For the reducibility results given in Sect. 4, we will use in the proofs both the random encodings based generic model and the purely algebraic one.

2.3 The Matrix DDH Problem Family

We recall some definitions from [9, 10, 15].

Definition 1 (Matrix Distribution). *Let $\ell, k \in \mathbb{N}$ with $\ell > k$.*[3] *We call $\mathcal{D}_{\ell,k}$ a matrix distribution if it is a probabilistic algorithm that, given any large enough prime q* [4]*, it outputs matrices in $\mathbb{Z}_q^{\ell \times k}$, in time polynomial in $\log q$, that have full rank k with overwhelming probability. We actually identify $\mathcal{D}_{\ell,k}$ to the probability distribution of its output. For simplicity, we write $\mathcal{D}_k = \mathcal{D}_{k+1,k}$.*

Definition 2 (Polynomial Matrix Distribution). *We call $\mathcal{D}_{\ell,k}$ a polynomial matrix distribution with d parameters if there exists a polynomial map $\mathbf{A} : \mathbb{Z}_q^d \to \mathbb{Z}_q^{\ell \times k}$ of constant degree (i.e., not depending on q) such that for a uniformly sampled $\boldsymbol{t} \in \mathbb{Z}_q^d$, the matrix $\mathbf{A}(\boldsymbol{t})$ follows the distribution $\mathcal{D}_{\ell,k}$. We will write $\mathcal{D}_{\ell,k}^{\mathbf{A}}$ to emphasize that the matrix distribution is defined via a polynomial map. We call the degree of $\mathcal{D}_{\ell,k}^{\mathbf{A}}$ to the minimum possible degree of a polynomial map $\mathbf{A}$ producing the distribution $\mathcal{D}_{\ell,k}$.*

We define the $\mathcal{D}_{\ell,k}$-matrix decision problem as to distinguish the two distributions $([\mathbf{A}], [\mathbf{A}\boldsymbol{w}])$ and $([\mathbf{A}], [\boldsymbol{z}])$, where $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, $\boldsymbol{w} \leftarrow \mathbb{Z}_q^k$ and $\boldsymbol{z} \leftarrow \mathbb{Z}_q^\ell$.

Definition 3 ($\mathcal{D}_{\ell,k}$-MDDH Problem). *Let $\mathcal{D}_{\ell,k}$ be a matrix distribution and* IG *an instance generator algorithm. The $\mathcal{D}_{\ell,k}$-Matrix Decision Diffie-Hellman ($\mathcal{D}_{\ell,k}$-*MDDH*) Problem, defined with respect to* IG*, is telling apart the two probability distributions*

$$D_{real} = (q, \mathbb{G}, g, [\mathbf{A}], [\mathbf{A}\boldsymbol{w}]), \qquad D_{random} = (q, \mathbb{G}, g, [\mathbf{A}], [\boldsymbol{z}]),$$

where $(q, \mathbb{G}, g) \leftarrow \mathsf{IG}(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, $\boldsymbol{w} \leftarrow \mathbb{Z}_q^k$ and $\boldsymbol{z} \leftarrow \mathbb{Z}_q^\ell$.

The $\mathcal{D}_{\ell,k}$-MDDH Assumption for an instance generator IG says that for all probabilistic polynomial time distinguishers A,

$$|\Pr[\mathsf{A}(D_{\text{real}}) = 1] - \Pr[\mathsf{A}(D_{\text{random}}) = 1]| \in negl.$$

Definition 4 (Hard Matrix Distribution). *We say that a matrix distribution $\mathcal{D}_{\ell,k}$ is hard if the $\mathcal{D}_{\ell,k}$-*MDDH *Problem is hard in the generic k-linear group model.*[5]

[3] We assume that k and ℓ are constant (*i.e.*, independent of the security parameter).

[4] From now on we assume that q is implicitly given as input to $\mathcal{D}_{\ell,k}$.

[5] This is the maximum level of generic security achievable, since a $(k+1)$-linear map solves all $\mathcal{D}_{\ell,k}$-MDDH problem instances.

Some particular families of matrix distributions were presented in [9, 15]. Namely,

$$\mathcal{L}_k : \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_k \\ 1 & \cdots & 1 \end{pmatrix}, \qquad \mathcal{C}_k : \begin{pmatrix} a_1 & & 0 \\ 1 & \ddots & \\ & \ddots & a_k \\ 0 & & 1 \end{pmatrix}, \qquad \mathcal{RL}_k : \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_k \\ b_1 & \cdots & b_k \end{pmatrix},$$

where $a_i, b_i \leftarrow \mathbb{Z}_q$. $\mathcal{L}_k$, $\mathcal{C}_k$ and $\mathcal{RL}_k$ are respectively called the Linear, the Cascade and the Randomized Linear matrix distributions. The Symmetric Cascade distribution, $\mathcal{SC}_k$, is defined from $\mathcal{C}_k$ by taking $a_1 = \cdots = a_k = a$, and similarly the Incremental Linear distribution, $\mathcal{IL}_k$, is defined from $\mathcal{L}_k$ by taking $a_i = a + i - 1$. The Uniform matrix distribution $\mathcal{U}_{\ell,k}$ is simply taking uniformly distributed matrices in $\mathbb{Z}_q^{\ell \times k}$. Also from the same source, the Circulant matrix distribution is defined as follows

$$\mathcal{CI}_{k,d} : \begin{pmatrix} a_1 & & & 0 \\ \vdots & a_1 & & \\ a_d & \vdots & \ddots & \\ 1 & a_d & & a_1 \\ & 1 & \ddots & \vdots \\ & & \ddots & a_d \\ 0 & & & 1 \end{pmatrix} \in \mathbb{Z}_q^{(k+d)\times k}, \qquad \text{where } a_i \leftarrow \mathbb{Z}_q.$$

2.4 Algebraic Reductions and Random Self-Reducibility

The algebraic nature of matrix distributions makes it easy to find some natural generic reductions among the corresponding problems. The following set of transformations were introduced in [10].

Definition 5 (Algebraic Reductions[6]). *We say that a matrix distribution $\mathcal{D}^1_{\ell,k}$ is algebraically reducible to another one $\mathcal{D}^2_{\ell,k}$ if there exists an efficiently samplable distribution $\mathcal{T}$ that, on the input of a large prime q, it outputs a pair of matrices $(\mathbf{L}, \mathbf{R})$, $\mathbf{L} \in \mathbb{Z}_q^{\ell\times\ell}$ and $\mathbf{R} \in \mathbb{Z}_q^{k\times k}$, with the following property: Given $\mathbf{A} \leftarrow \mathcal{D}^1_{\ell,k}$ the distribution of $\mathbf{LAR}$ is statistically close to $\mathcal{D}^2_{\ell,k}$. In this case we write $\mathcal{D}^1_{\ell,k} \overset{alg}{\Rightarrow} \mathcal{D}^2_{\ell,k}$, or simply $\mathcal{D}^2_{\ell,k} = \mathcal{T}^*(\mathcal{D}^1_{\ell,k})$.*

As shown in [10] and later in [15], algebraic reductions between matrix distributions also imply generic reductions between the MDDH problems.

Lemma 1 (from [15]). $\mathcal{D}^1_{\ell,k} \overset{alg}{\Rightarrow} \mathcal{D}^2_{\ell,k}$ *implies* $\mathcal{D}^1_{\ell,k}$-$\mathsf{MDDH} \Rightarrow \mathcal{D}^2_{\ell,k}$-$\mathsf{MDDH}$.

[6] This definition can be extended to deal with matrix distributions of different sizes, by adding some restrictions to the shapes of $\mathbf{R}$ and $\mathbf{L}$. However, here we are mainly focusing on self-reductions.

By taking $\mathcal{T}$ to produce independent uniformly distributed invertible matrices, it is easy to see that for any matrix distribution $\mathcal{D}_{\ell,k}$, $\mathcal{D}_{\ell,k} \overset{alg}{\Rightarrow} \mathcal{U}_{\ell,k}$, which implies that $\mathcal{U}_{\ell,k}$-MDDH is the hardest of the MDDH problems of size $\ell \times k$. It is also easy to prove that $\mathcal{L}_k \overset{alg}{\Rightarrow} \mathcal{RL}_k$ and $\mathcal{SC}_k \overset{alg}{\Rightarrow} \mathcal{C}_k$.

As mentioned in [9], MDDH problems show some random self-reducibility properties. In particular, all variants of the $\mathcal{D}_k$-MDDH problems (that is, with $\ell = k+1$) with a nonuniform distribution of the vector $\boldsymbol{z}$ (either in the real or the random instances) can be reduced to the corresponding proper $\mathcal{D}_k$-MDDH problem (*i.e.*, with $\boldsymbol{z}$ distributed as in Definition 3). Indeed, it suffices to apply the map $(\mathbf{A}, \boldsymbol{z}) \mapsto (\mathbf{A}, \lambda\boldsymbol{z} + \mathbf{A}\boldsymbol{w})$ for random $\boldsymbol{w} \leftarrow \mathbb{Z}_q^k$ and $\lambda \leftarrow \mathbb{Z}_q^\times$, which works fine for both real and random instances.

Stronger self-reducibility properties of the $\mathcal{D}_k$-MDDH problems (*i.e.*, including also the distribution of the matrix $\mathbf{A}$) are known for specific matrix distributions, like $\mathcal{C}_k$, $\mathcal{SC}_k$, $\mathcal{RL}_k$, $\mathcal{RL}_k$ or the uniform distribution. To this end, we can use the algebraic reductions, given in Definition 5, to explicitly build random self-reductions (according to Lemma 1) transforming any probability distribution of the parameters $\boldsymbol{t} \in \mathbb{Z}_q^d$ into some probability distribution statistically close to the uniformly one. In particular, for $\mathcal{C}_k$ we can choose an algebraic reduction $\mathcal{T}$ producing diagonal matrices

$$\mathbf{L}(\boldsymbol{\lambda}) = \begin{pmatrix} 1 & & & 0 \\ & \lambda_1^{-1} & & \\ & & \ddots & \\ 0 & & & \lambda_k^{-1} \end{pmatrix} \qquad \mathbf{R}(\boldsymbol{\lambda}) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_k \end{pmatrix}$$

where $\lambda_1, \dots, \lambda_k \leftarrow \mathbb{Z}_q^\times$ are taken at random. Observe that $\mathcal{T}$ can be seen as the transformation in the parameter space $(a_1, \dots, a_k) \mapsto (\lambda_1 a_1, \dots, \lambda_k a_k)$. Using now $\lambda_1 = \cdots = \lambda_k$, we can show the strong random self-reducibility of $\mathcal{SC}_k$-MDDH. Similarly, for $\mathcal{RL}_k$ we can take

$$\mathbf{L}(\boldsymbol{\lambda}) = \begin{pmatrix} \lambda_1 & & & 0 \\ & \ddots & & \\ & & \lambda_k & \\ 0 & & & 1 \end{pmatrix} \qquad \mathbf{R}(\boldsymbol{\mu}) = \begin{pmatrix} \mu_1 & & 0 \\ & \ddots & \\ 0 & & \mu_k \end{pmatrix}$$

for random $\lambda_1, \dots, \lambda_k, \mu_1, \dots, \mu_k \leftarrow \mathbb{Z}_q^\times$, corresponding to the map $(a_1, \dots, a_k, b_1, \dots, b_k) \mapsto (\lambda_1\mu_1 a_1, \dots, \lambda_k\mu_k a_k, \mu_1 b_1, \dots, \mu_k b_k)$. Finally, for $\mathcal{L}_k$ we just set $\mu_1 = \cdots = \mu_k = 1$.[7] We formally define this stronger notion of self-reducibility.

Definition 6 (Random Self-Reducibility). *A matrix distribution $\mathcal{D}_k$ (or the $\mathcal{D}_k$-*MDDH *problem) is defined to be random self-reducible if there exists a probabilistic polynomial-time transformation $\mathcal{R}$ such that on the input of any possible*

[7] Actually, these transformations do not randomize some 'badly selected' parameters, that is, when some $a_i = 0$ or $b_i = 0$. In practice, we can discard these values in the sampling algorithm, incurring only in a negligible difference, but here we are forced to include them due to the algebraic framework.

instance[8] $(q, \mathbb{G}, g, [\mathbf{A}], [\boldsymbol{z}])$ *of the* $\mathcal{D}_k$-MDDH *problem, it outputs* $([\widetilde{\mathbf{A}}], [\widetilde{\boldsymbol{z}}])$ *with the following properties*

1. *if there exists* $\boldsymbol{w} \in \mathbb{Z}_q^k$ *such that* $\boldsymbol{z} = \mathbf{A}\boldsymbol{w}$*, then the probability distribution of* $(q, \mathbb{G}, g, [\widetilde{\mathbf{A}}], [\widetilde{\boldsymbol{z}}])$ *is statistically close to* D_{real}.
2. *otherwise, the probability distribution is statistically close to* D_{random}.

where D_{real} *and* D_{random} *are given in Definition 3.*

Definition 7 (Quasi Random Self-Reducibility). *We say that* $\mathcal{D}_k$ *is quasi random self-reducible if there exists a transformation* $\mathcal{R}$ *fulfiling the properties required in Definition 6 only when the matrix* $\mathbf{A}$ *in the input instance of* $\mathcal{R}$ *belongs to a subset* $\mathcal{X} \subset \mathbb{Z}_q^{(k+1)\times k}$ *such that* $\Pr[\mathbf{A} \notin \mathcal{X};\ \mathbf{A} \leftarrow \mathcal{D}_k] \in negl$.

Clearly, for the above families, the composition of $\mathcal{T}$ and the map $(\mathbf{A}, \boldsymbol{z}) \mapsto (\mathbf{A}, \lambda\boldsymbol{z} + \mathbf{A}\boldsymbol{w})$, for random $\boldsymbol{w} \leftarrow \mathbb{Z}_q^k$ and $\lambda \leftarrow \mathbb{Z}_q^\times$, behaves as the transformation $\mathcal{R}$ in the previous definitions. This proves the following result.

Theorem 1. *The matrix distributions* $\mathcal{C}_k$, $\mathcal{SC}_k$, $\mathcal{L}_k$, $\mathcal{RL}_k$ *and the uniform distribution are quasi random self-reducible*[9] *in the sense of Definition 7.*

2.5 Generic Hardness of the MDDH Problems

Here we will focus on the case $\ell = k+1$, as presented in [9]. However, in [11] more general results for the case $\ell > k+1$ are given, and they are applied to the particular family $\mathcal{CI}_{k,d}$ in [15].

Given a polynomial matrix distribution $\mathcal{D}_k^{\mathbf{A}}$, the hardness of the $\mathcal{D}_k^{\mathbf{A}}$-MDDH problem in the k-linear generic group model (*i.e.*, the hardness of $\mathcal{D}_k^{\mathbf{A}}$) is tightly related to the properties of the so-called *determinant polynomial* corresponding to $\mathcal{D}_k^{\mathbf{A}}$.

Definition 8 (Determinant Polynomial). *Given a polynomial matrix distribution* $\mathcal{D}_k^{\mathbf{A}}$*, described by the polynomial map* $\mathbf{A} : \mathbb{Z}_q^d \to \mathbb{Z}_q^{(k+1)\times k}$*, the associated determinant polynomial* $\mathfrak{d}_{\mathbf{A}} \in \mathbb{Z}_q[t_1, \ldots, t_d, z_1, \ldots, z_{k+1}]$ *is defined as the determinant* $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \boldsymbol{z}) = \det(\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z})$.

Observe that developing the determinant by its last column, we can write

$$\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \boldsymbol{z}) = \sum_{i=1}^{k+1} \mathfrak{d}_{\mathbf{A},i}(\boldsymbol{t}) z_i \tag{2}$$

which means that $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \boldsymbol{z})$ is linear (*i.e.*, homogeneous of degree one) in $\boldsymbol{z}$.

[8] That is, $\mathcal{R}$ transforms every particular real instance into a randomly distributed real one, and the same for random instances. Therefore, $([\widetilde{\mathbf{A}}], [\widetilde{\boldsymbol{z}}])$ is independent of $([\mathbf{A}], [\boldsymbol{z}])$ for real and random instances.

[9] Indeed, $\mathcal{SC}_k$ can be shown to be random self-reducible by using a more sophisticated transformation leading to $a \mapsto a + \lambda$ for $\lambda \in \mathbb{Z}_q$.

Once we associate a polynomial $\mathfrak{d}_{\mathbf{A}}$ to the polynomial matrix distribution $\mathcal{D}_k^{\mathbf{A}}$, other mathematical objects are automatically defined, like the principal ideal $\mathfrak{I}_{\mathbf{A}} = (\mathfrak{d}_{\mathbf{A}}) \subset \mathbb{Z}_q[\boldsymbol{t}, \boldsymbol{z}]$ or the associated algebraic variety $V_{\mathbf{A}} = V(\mathfrak{I}_{\mathbf{A}}) = \{(\boldsymbol{t}, \boldsymbol{z}) \in \mathbb{Z}_q^d \times \mathbb{Z}_q^{k+1} \mid \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \boldsymbol{z}) = 0\}$[10]. It is precisely using these objects how the following hardness criterion is derived.

Theorem 2 (Determinant Hardness Criterion (from [9])). *Let $\mathcal{D}_k^{\mathbf{A}}$ be a polynomial matrix distribution, which outputs matrices $\mathbf{A}(\boldsymbol{t})$ for uniform $\boldsymbol{t} \in \mathbb{Z}_q^d$. Let $\mathfrak{d}_{\mathbf{A}}$ be the associated determinant polynomial.*

1. *If all matrices $\mathbf{A}(\boldsymbol{t})$ have full rank even for t_i in the algebraic closure $\overline{\mathbb{Z}}_q$, then the determinant polynomial $\mathfrak{d}_{\mathbf{A}}$ is irreducible over $\overline{\mathbb{Z}}_q$.*
2. *If $\mathbf{A}(\boldsymbol{t})$ has degree one, $\mathfrak{d}_{\mathbf{A}}$ is irreducible over $\overline{\mathbb{Z}}_q$, and the total degree of $\mathfrak{d}_{\mathbf{A}}$ is $k+1$, then $\mathcal{D}_k^{\mathbf{A}}$ is a hard matrix distribution (i.e., $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ problem is hard in the generic k-linear group model). In particular, for any polynomial $\mathfrak{h} \in \mathbb{Z}_q[\boldsymbol{t}, \boldsymbol{z}]$, if $\mathfrak{h}((\boldsymbol{t}, \mathbf{A}(\boldsymbol{t})\boldsymbol{w})) = 0$ for all $\boldsymbol{t} \in \mathbb{Z}_q^d$ and $\boldsymbol{w} \in \mathbb{Z}_q^k$, then $\mathfrak{h} \in \mathfrak{I}_{\mathbf{A}}$ (i.e., $\mathfrak{h}$ is a multiple of $\mathfrak{d}_{\mathbf{A}}$).*

The intuition behind this result is that in the generic k-linear group model[11], any successful strategy to solve the $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ problem amounts to evaluate a known nonzero polynomial $\mathfrak{h}$ of degree at most k that vanishes at all points $(\boldsymbol{t}, \mathbf{A}(\boldsymbol{t})\boldsymbol{w})$, for $\boldsymbol{t} \in \mathbb{Z}_q^d$ and $\boldsymbol{w} \in \mathbb{Z}_q^k$. The irreducibility of $\mathfrak{d}_{\mathbf{A}}$ is used to show that $\mathfrak{h}$ must belong to the principal ideal $\mathfrak{I}_{\mathbf{A}}$. Finally, the degree requirement for $\mathfrak{d}_{\mathbf{A}}$ just shows that no such polynomial $\mathfrak{h}$ exists.

This powerful result allows to directly prove at once the generic hardness of a whole family of MDDH problems, by just analyzing the properties of a particular polynomial, or a family of polynomials. For instance, in [9] the criterion is applied to the $\mathcal{SC}$, $\mathcal{C}$ and $\mathcal{L}$ families (actually, the hardness of $\mathcal{C}_k$ is implied by the hardness of $\mathcal{SC}_k$, and similarly with $\mathcal{RL}_k$ and $\mathcal{L}_k$, from the results on algebraic reductions given above).

3 A Partial Converse of Theorem 2

From now on, we restrict the study to the particular case of polynomial matrix distributions $\mathcal{D}_{\ell,k}^{\mathbf{A}}$ of degree one with $\ell = k+1$, as considered also in Theorem 2. Namely, $\mathcal{D}_{\ell,k}^{\mathbf{A}}$ can be sampled by the map $\mathbf{A}(\boldsymbol{t}) = \mathbf{A}_0 + \mathbf{A}_1 t_1 + \ldots + \mathbf{A}_d t_d$ for uniformly distributed $\boldsymbol{t} = (t_1, \ldots, t_d) \in \mathbb{Z}_q^d$, and fixed matrices $\mathbf{A}_0, \ldots, \mathbf{A}_d \in \mathbb{Z}_q^{(k+1)\times k}$. This family covers the most useful instances among the matrix distributions, including $\mathcal{C}_k$, $\mathcal{L}_k$, $\mathcal{SC}_k$, $\mathcal{RL}_k$ and the uniform one. We also assume that the parameters $t_1, \ldots, t_d$ are all meaningful, that is, the map $\mathbf{A} : \mathbb{Z}_q^d \to \mathbb{Z}_q^{(k+1)\times k}$ is injective, or equivalently, $\mathbf{A}_1, \ldots, \mathbf{A}_d$ are linearly independent matrices. This in particular implies that the parameters $t_1, \ldots, t_d$ can be expressed as linear

[10] To properly define the variety we need to consider the algebraic closure of the field. But here we only consider the subset of rational points, *i.e.*, with coordinates in $\mathbb{Z}_q$.

[11] See Sect. 2.2 for details.

combinations of the entries of the matrix $\mathbf{A}(\boldsymbol{t})$. Therefore, there exist efficient (generic) algorithms computing $[\boldsymbol{t}]$ from $[\mathbf{A}(\boldsymbol{t})]$, and vice versa. We call these polynomial matrix distributions *compact degree-one*.

Recall that the determinant polynomial $\mathfrak{d}_{\mathbf{A}}$ is defined as the determinant of $(\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z})$ as a polynomial in $\mathbb{Z}_q[\boldsymbol{t},\boldsymbol{z}]$, $\mathfrak{I}_{\mathbf{A}}$ is the ideal generated by $\mathfrak{d}_{\mathbf{A}}$, and $V_{\mathbf{A}}$ is the set of (rational) zeros of $\mathfrak{d}_{\mathbf{A}}$. For notational convenience, we also define the set $V_{\mathbf{A}}^{\mathrm{def}} = \{\boldsymbol{t} \in \mathbb{Z}_q^d \mid \operatorname{rank}\mathbf{A}(\boldsymbol{t}) < k\}$ (which is also the set of rational points in an algebraic variety).

We start the exposition with a few technical lemmas stating additional properties of the compact degree-one matrix distributions.

Lemma 2. *Define* $r = \max_{\boldsymbol{t}\in\mathbb{Z}_q^d} \operatorname{rank}\mathbf{A}(\boldsymbol{t})$*. Then* $\operatorname{rank}\mathbf{A}(\boldsymbol{t}) = r$ *with overwhelming probability, and there exists a nonzero polynomial* $\mathfrak{h} \in \mathbb{Z}_q[\boldsymbol{t},\boldsymbol{z}]$ *of total degree at most* $r+1$ *such that* $\mathfrak{h}(\boldsymbol{t},\mathbf{A}(\boldsymbol{t})\boldsymbol{w}) = 0$ *for all* $\boldsymbol{t} \in \mathbb{Z}_q^d$ *and* $\boldsymbol{w} \in \mathbb{Z}_q^k$*.*

Proof. Clearly, there exists a r-minor of $\mathbf{A}(\boldsymbol{t})$ that is nonzero, as a polynomial in $\mathbb{Z}_q[\boldsymbol{t}]$. By Schwartz-Zippel Lemma [17] this polynomial, whose degree cannot exceed $r < k$, can only vanish at a negligible fraction of $\mathbb{Z}_q^d$ (a fraction $\frac{r}{q}$), which proves that $\operatorname{rank}\mathbf{A}(\boldsymbol{t}) = r$ with overwhelming probability. Let $\widehat{\mathbf{A}}(\boldsymbol{t})$ be any $(r+1)\times r$ submatrix of $\mathbf{A}(\boldsymbol{t})$ containing the previous r-minor, and let $(\widehat{\mathbf{A}}(\boldsymbol{t})\|\widehat{\boldsymbol{z}})$ be the same matrix but adding as an extra column the part of $\boldsymbol{z}$ corresponding to the rows of $\widehat{\mathbf{A}}(\boldsymbol{t})$. As before, $\operatorname{rank}\widehat{\mathbf{A}}(\boldsymbol{t}) = r$ with overwhelming probability. In addition, $\operatorname{rank}(\widehat{\mathbf{A}}(\boldsymbol{t})\|\widehat{\boldsymbol{z}}) = r+1$ with overwhelming probability if $\boldsymbol{z} \leftarrow \mathbb{Z}_q^\ell$, while $\operatorname{rank}(\widehat{\mathbf{A}}(\boldsymbol{t})\|\widehat{\boldsymbol{z}}) \le \operatorname{rank}(\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z}) \le r$ when $\boldsymbol{z} = \mathbf{A}(\boldsymbol{t})\boldsymbol{w}$. Therefore $\mathfrak{h} = \det(\widehat{\mathbf{A}}(\boldsymbol{t})\|\widehat{\boldsymbol{z}})$ fulfils the required properties: $\mathfrak{h}$ is a nonzero polynomial of total degree at most $r+1$, and $\mathfrak{h}(\boldsymbol{t},\mathbf{A}(\boldsymbol{t})\boldsymbol{w}) = 0$ for all $\boldsymbol{t} \in \mathbb{Z}_q^d$ and $\boldsymbol{w} \in \mathbb{Z}_q^k$. □

Another interesting property of a hard matrix distribution $\mathcal{D}_{\ell,k}$ is the so-called k-elusiveness, introduced in [15].

Definition 9 (m-Elusiveness (from [15])). *A matrix distribution* $\mathcal{D}_{\ell,k}$ *is called* m*-elusive for some* $m < \ell$ *if for all* m*-dimensional subspaces* $F \subset \mathbb{Z}_q^\ell$*,* $\Pr(F \cap \ker\mathbf{A}^\top \neq \{\mathbf{0}\}) \in$ *negl, where the probability is computed with respect to* $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$*.*

Lemma 3 (proved in [15]). *All hard matrix distributions* $\mathcal{D}_{\ell,k}$ *are* k*-elusive.*

We will need another technical lemma about the determinant polynomial of a hard compact degree-one matrix distribution, which essentially states that $\mathfrak{d}_{\mathbf{A}}$ cannot be constant along any line in the space $\mathbb{Z}_q^d \times \mathbb{Z}_q^{k+1}$.

Lemma 4. *Let* $\mathcal{D}_k^{\mathbf{A}}$ *be a hard compact degree-one matrix distribution with* d *parameters. If there exist vectors* $\boldsymbol{\tau} \in \mathbb{Z}_q^d$ *and* $\boldsymbol{\zeta} \in \mathbb{Z}_q^{k+1}$ *such that* $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}+\boldsymbol{\tau},\boldsymbol{z}+\boldsymbol{\zeta}) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t},\boldsymbol{z})$*, for all* $\boldsymbol{t} \in \mathbb{Z}_q^d$ *and* $\boldsymbol{z} \in \mathbb{Z}_q^{k+1}$*, then necessarily* $(\boldsymbol{\tau},\boldsymbol{\zeta}) = (\mathbf{0},\mathbf{0})$*.*

Proof. Recall the linearity property of the determinant polynomial $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t},\boldsymbol{z_1}+\boldsymbol{z_2}) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t},\boldsymbol{z_1}) + \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t},\boldsymbol{z_2})$. In particular, $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t},\boldsymbol{z}+\mathbf{A}(\boldsymbol{t})\boldsymbol{w}) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t},\boldsymbol{z})$ for any $\boldsymbol{w} \in \mathbb{Z}_q^k$, since clearly $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t},\mathbf{A}(\boldsymbol{t})\boldsymbol{w}) = 0$.

Using now that $\mathbf{A}(\boldsymbol{t}+\boldsymbol{\tau}) = \mathbf{A}(\boldsymbol{t}) + \mathbf{B}$, where $\mathbf{B} = \sum_{i=1}^{d} \tau_i \mathbf{A}_i$, and $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}+\boldsymbol{\tau}, \boldsymbol{z}+\boldsymbol{\zeta}) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \boldsymbol{z})$ for any $\boldsymbol{z} \in \mathbb{Z}_q^{k+1}$, we have for any $\boldsymbol{w} \in \mathbb{Z}_q^k$,

$$\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}+\boldsymbol{\tau}, \mathbf{A}(\boldsymbol{t}+\boldsymbol{\tau})\boldsymbol{w}+\boldsymbol{\zeta}) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \mathbf{A}(\boldsymbol{t}+\boldsymbol{\tau})\boldsymbol{w}) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \mathbf{A}(\boldsymbol{t})\boldsymbol{w}+\mathbf{B}\boldsymbol{w}) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \mathbf{B}\boldsymbol{w})$$

and, on the other hand, by the linearity property

$$\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}+\boldsymbol{\tau}, \mathbf{A}(\boldsymbol{t}+\boldsymbol{\tau})\boldsymbol{w}+\boldsymbol{\zeta}) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}+\boldsymbol{\tau}, \boldsymbol{\zeta}) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \mathbf{0}) = 0$$

Thus, $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \mathbf{B}\boldsymbol{w}) = 0$ which implies that $\mathbf{B}\boldsymbol{w} \in \operatorname{Im}\mathbf{A}(\boldsymbol{t})$ for all $\boldsymbol{w} \in \mathbb{Z}_q^k$ and $\boldsymbol{t} \in \mathbb{Z}_q^d \setminus V_{\mathbf{A}}^{\text{def}}$. Therefore, for all such $\boldsymbol{t}$ we have $\operatorname{Im}\mathbf{B} \subseteq \operatorname{Im}\mathbf{A}(\boldsymbol{t})$ or equivalently $\ker \mathbf{A}(\boldsymbol{t})^\top \subseteq \ker \mathbf{B}^\top$.

By the k-elusiveness property, this is only possible if $\dim\ker\mathbf{B}^\top > k$, that is, $\mathbf{B} = \mathbf{0}$. In addition, by the compactness property, necessarily $\boldsymbol{\tau} = \mathbf{0}$. But now, for all $\boldsymbol{t} \in \mathbb{Z}_q^d$, $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \boldsymbol{\zeta}) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \mathbf{0}) = 0$ which implies $\boldsymbol{\zeta} \in \operatorname{Im}\mathbf{A}(\boldsymbol{t})$ for all $\boldsymbol{t} \in \mathbb{Z}_q^d \setminus V_{\mathbf{A}}^{\text{def}}$. Then, $\ker\mathbf{A}(\boldsymbol{t})^\top$ is included in the orthogonal subspace $\{\boldsymbol{\zeta}\}^\perp$, which contradicts again the k-elusiveness property, unless $\dim\{\boldsymbol{\zeta}\}^\perp > k$ or equivalently $\boldsymbol{\zeta} = \mathbf{0}$. □

Now we state and prove a partial converse of Theorem 2.[12]

Theorem 3. *Let $\mathcal{D}_k^{\mathbf{A}}$ be a hard compact degree-one matrix distribution, producing matrices $\mathbf{A}(\boldsymbol{t}) = \mathbf{A}_0 + \mathbf{A}_1 t_1 + \ldots + \mathbf{A}_d t_d$. Then, the set $V_{\mathbf{A}}^{def}$ is a negligible fraction of $\mathbb{Z}_q^d$, and the determinant polynomial $\mathfrak{d}_{\mathbf{A}}$ has the following properties:*

1. *$\mathfrak{d}_{\mathbf{A}}$ is irreducible in $\overline{\mathbb{Z}}_q[\boldsymbol{t}, \boldsymbol{z}]$ with total degree $k+1$.*
2. *$\mathfrak{d}_{\mathbf{A}}$ cannot be constant along any direction in the space $\mathbb{Z}_q^d \times \mathbb{Z}_q^{k+1}$, i.e., $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}+\boldsymbol{\tau}, \boldsymbol{z}+\boldsymbol{\zeta}) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \boldsymbol{z})$ for all $\boldsymbol{t} \in \mathbb{Z}_q^d$ and all $\boldsymbol{z} \in \mathbb{Z}_q^{k+1}$ only if $(\boldsymbol{\tau}, \boldsymbol{\zeta}) = (\mathbf{0}, \mathbf{0})$.*
3. *The polynomials $\mathfrak{d}_{\mathbf{A},1}, \ldots, \mathfrak{d}_{\mathbf{A},k+1}$ in Eq. 2 are linearly independent*[13].

Proof. If $\mathcal{D}_k^{\mathbf{A}}$ is hard then no nonzero polynomial $\mathfrak{h} \in \mathbb{Z}_q[\boldsymbol{t}, \boldsymbol{z}]$ of degree at most k fulfils $\mathfrak{h}(\boldsymbol{t}, \mathbf{A}(t)\boldsymbol{w}) = 0$ for all $\boldsymbol{t} \in \mathbb{Z}_q^d$ and $\boldsymbol{w} \in \mathbb{Z}_q^k$. Otherwise, a distinguisher only needs to check whether $\mathfrak{h}(\boldsymbol{t}, \boldsymbol{z}) = 0$ (using the k-linear map) to tell apart 'real' and 'random' instances of the $\mathcal{D}_k^{\mathbf{A}}$-MDDH problem.

Consider the maximal rank $r = \max_{\boldsymbol{t}\in\mathbb{Z}_q^d} \operatorname{rank}\mathbf{A}(\boldsymbol{t})$. If $r < k$ then, according to Lemma 2, the $\mathcal{D}_k^{\mathbf{A}}$-MDDH problem is easy in a k-linear group (as shown also in [9]). Thus, it must be $r = k$, and the same lemma states in addition that $\operatorname{rank}\mathbf{A}(\boldsymbol{t}) = k$ with overwhelming probability, or equivalently, $V_{\mathbf{A}}^{\text{def}}$ only holds a negligible fraction of the parameter space $\mathbb{Z}_q^d$. Actually, all instances $(\boldsymbol{t}, \boldsymbol{z})$ of the $\mathcal{D}_k^{\mathbf{A}}$-MDDH problem with $\boldsymbol{t} \in V_{\mathbf{A}}^{\text{def}}$ are easy.

Moreover, the total degree of the determinant polynomial $\mathfrak{d}_{\mathbf{A}}$ must be $k+1$ (it cannot be larger because the degree of $\mathbf{A}$ is one). Otherwise, we could let

[12] A more limited converse of the same theorem appeared in [10], but for the special case of $d = 1$. It is worth mentioning that for $d = 1$, $V_{\mathbf{A}}^{\text{def}}$ is not only a negligible fraction of $\mathbb{Z}_q^d$, but it is the empty set.

[13] In [12] this property is named irredundancy of the matrix distribution.

$\mathfrak{h} = \mathfrak{d}_{\mathbf{A}}$ and solve the $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ problem, as explained in the first paragraph of the proof. Notice that $\mathfrak{d}_{\mathbf{A}}$ cannot be the zero polynomial because it would contradict the fact that rank $\mathbf{A}(\boldsymbol{t}) = k$ with overwhelming probability.

Consider now the irreducibility of the determinant polynomial. If $\mathfrak{d}_{\mathbf{A}}$ were reducible in $\overline{\mathbb{Z}}_q[\boldsymbol{t}, \boldsymbol{z}]$, it follows that $\mathfrak{d}_{\mathbf{A}}$ can be split as $\mathfrak{d}_{\mathbf{A}} = \mathfrak{c}\mathfrak{d}_0$, where $\mathfrak{c} \in \mathbb{Z}_q[\boldsymbol{t}]$ and $\mathfrak{d}_0 \in \mathbb{Z}_q[\boldsymbol{t}, \boldsymbol{z}]$ are nonconstant. Indeed, the degree of $\mathfrak{d}_{\mathbf{A}}$ in $\boldsymbol{z}$ is one. Thus, only one of the irreducible factors of $\mathfrak{d}_{\mathbf{A}}$ can depend explicitly on $\boldsymbol{z}$, and its coefficients must be elements in the base field $\mathbb{Z}_q$ (as there is no other conjugate irreducible factor)[14]. Clearly, for any $\boldsymbol{t}$ such that $\mathfrak{c}(\boldsymbol{t}) \neq 0$, we know that $\mathfrak{d}_0(\boldsymbol{t}, \mathbf{A}(t)\boldsymbol{w}) = 0$ for all $\boldsymbol{w} \in \mathbb{Z}_q^k$. Hence, by Schwartz-Zippel lemma, as a polynomial in $\mathbb{Z}_q[\boldsymbol{t}, \boldsymbol{w}]$, $\mathfrak{d}_0(\boldsymbol{t}, \mathbf{A}(\boldsymbol{t})\boldsymbol{w})$ is the zero polynomial. Again, we could use $\mathfrak{h} = \mathfrak{d}_0$ to solve the $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ problem, since $\deg \mathfrak{d}_0 < \deg \mathfrak{d}_{\mathbf{A}} = k + 1$.

On the other hand, under the conditions of the theorem Lemma 4 ensures that $\mathfrak{d}_{\mathbf{A}}$ cannot be constant along any direction in the space $\mathbb{Z}_q^d \times \mathbb{Z}_q^{k+1}$.

We now proceed in a similar way with the last item in the theorem statement. According to Eq. 2, any nontrivial linear dependency relation of the polynomials $\mathfrak{d}_{\mathbf{A},1}, \ldots, \mathfrak{d}_{\mathbf{A},k+1}$ can be written as

$$\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \boldsymbol{\zeta}) = \sum_{i=1}^{k+1} \mathfrak{d}_{\mathbf{A},i}(\boldsymbol{t})\zeta_i = 0$$

for a fixed nonzero $\boldsymbol{\zeta} \in \mathbb{Z}_q^{k+1}$ and for all $\boldsymbol{t} \in \mathbb{Z}_q^d$. Again, Lemma 4 implies that such nonzero vector $\boldsymbol{\zeta}$ does not exist. □

Notice that the last item in the theorem statement allow us to associate every hard polynomial matrix distribution of degree one $\mathcal{D}_k^{\mathbf{A}}$ with a polynomial vector space $X_{\mathbf{A}} \subset \mathbb{Z}_q[\boldsymbol{t}]$ of dimension $k+1$, generated by $\mathfrak{d}_{\mathbf{A},1}, \ldots, \mathfrak{d}_{\mathbf{A},k+1}$. This association is actually at the heart of the polynomial view of MDDH problems, introduced in [12]. Moreover, since the total degree of $\mathfrak{d}_{\mathbf{A}}$ is $k+1$ then the maximum of the degrees of $\mathfrak{d}_{\mathbf{A},1}, \ldots, \mathfrak{d}_{\mathbf{A},k+1}$ is exactly k. Clearly, for $d = 1$ the only possible choice is $X_{\mathbf{A}} = \mathbb{Z}_q[\boldsymbol{t}]_{\leq k}$, the vector space of all polynomials of degree at most k. We will show later that this actually means that there is essentially a unique hard polynomial matrix distribution of degree one with only one parameter, and this matrix distribution is the symmetric cascade distribution $\mathcal{SC}_k$. This was proved for the first time in [10] by means of completely different algebraic tools, more related to matrix Jordan normal forms. This uniqueness does not directly extend to the case $d \geq 2$, because the number of possible choices for the vector space $X_{\mathbf{A}}$ increases fast with d.

4 MDDH Problems of the Same Size

The goal of this section is to obtain some criteria to analyze in a compact way the possible black-box reductions between MDDH problems, in terms of the

[14] All these facts are indeed used in [9] to prove Theorem 2.

determinant polynomials or other mathematical objects associated to the matrix distributions. The idea is then to avoid the classical case-by-case approach to show reductions or separation results between computational problems, and deal instead with large families of problems at once. As explained in the previous section, we restrict ourselves to the study of compact degree-one matrix distributions, but we also restrict to the case of reductions between $\mathcal{D}_k$-MDDH problems, that is with the same size and with $\ell = k + 1$.

In a more general approach we would take into consideration the possible reductions between two $\mathcal{D}_{k_1}$-MDDH and $\mathcal{D}_{k_2}$-MDDH problems with $k_1 < k_2$. However, since any $\mathcal{D}_k$-MDDH problem is easy in a m-linear group with $m > k$, then $\mathcal{D}_{k_1}$-MDDH and $\mathcal{D}_{k_2}$-MDDH are separated by an oracle computing a (k_1+1)-linear map, meaning that the large problem could remain hard while the small one is clearly easy. Therefore, we focus only on the case $k_2 = k_1$, in which there is no a priori hardness implication.

Recall that the determinant polynomial $\mathfrak{d}_{\mathbf{A}}$ is defined as the determinant of $(\mathbf{A}(\boldsymbol{t})\|\boldsymbol{z})$ as a polynomial in $\mathbb{Z}_q[\boldsymbol{t}, \boldsymbol{z}]$, $\mathfrak{I}_{\mathbf{A}}$ is the ideal generated by $\mathfrak{d}_{\mathbf{A}}$, $V_{\mathbf{A}}$ is the set of (rational) zeros of $\mathfrak{d}_{\mathbf{A}}$, and $V_{\mathbf{A}}' \overset{\text{def}}{=} \{\boldsymbol{t} \in \mathbb{Z}_q^d \mid \operatorname{rank} \mathbf{A}(\boldsymbol{t}) < k\}$.

Once the properties of the determinant polynomials of hard polynomial matrix distributions of degree one are understood, we can find a purely algebraic criterion for the existence of generic reductions among them. Indeed, as usually in the generic algebraic models, the criterion either gives an explicit reduction or completely rules out its existence.

Theorem 4. *Let $\mathcal{D}_k^{\mathbf{A}}$ and $\mathcal{D}_k^{\mathbf{B}}$ be hard compact degree-one matrix distributions, producing matrices $\mathbf{A}(\boldsymbol{t}) = \mathbf{A}_0 + \mathbf{A}_1 t_1 + \ldots + \mathbf{A}_d t_d$ and $\mathbf{B}(\boldsymbol{s}) = \mathbf{B}_0 + \mathbf{B}_1 s_1 + \ldots + \mathbf{B}_e s_e$, and let $\mathfrak{d}_{\mathbf{A}}$ and $\mathfrak{d}_{\mathbf{B}}$ be the corresponding determinant polynomials. If there exists a generic black-box reduction from the $\mathcal{D}_k^{\mathbf{A}}$-MDDH problem to the $\mathcal{D}_k^{\mathbf{B}}$-MDDH problem, then there exists a polynomial map $f : \mathbb{Z}_q^{d+k+1} \to \mathbb{Z}_q^{e+k+1}$ of degree one such that $\lambda \mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ for some nonzero constant $\lambda \in \mathbb{Z}_q$.*

Proof. Because of the compactness of the two matrix distributions we know that the matrices $\mathbf{A}_1, \ldots, \mathbf{A}_d$ are linearly independent, and so are $\mathbf{B}_1, \ldots, \mathbf{B}_e$. Then there are efficient linear maps computing $[\boldsymbol{t}]$ from $[\mathbf{A}(\boldsymbol{t})]$, and $[\boldsymbol{s}]$ from $[\mathbf{B}(\boldsymbol{s})]$. Thus, we can consider the instances of the two $\mathcal{D}_k^{\mathbf{A}}$-MDDH and $\mathcal{D}_k^{\mathbf{B}}$-MDDH problems respectively defined by $([\boldsymbol{t}], [\boldsymbol{z}])$ and $([\boldsymbol{s}], [\boldsymbol{u}])$.

Let $\mathcal{R}$ be a black-box reduction in the generic k-linear group model from the $\mathcal{D}_k^{\mathbf{A}}$-MDDH problem to the $\mathcal{D}_k^{\mathbf{B}}$-MDDH problem, and assume that $\mathcal{D}_k^{\mathbf{A}}$ is a hard matrix distribution, and there is no polynomial map $f : \mathbb{Z}_q^{d+k+1} \to \mathbb{Z}_q^{e+k+1}$ of degree one such that $\lambda \mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ for some nonzero constant $\lambda \in \mathbb{Z}_q$. We use a sequence of games in order to prove that $\mathcal{R}$ can only have a negligible advantage even when it has access to an oracle solving the $\mathcal{D}_k^{\mathbf{B}}$-MDDH problem with overwhelming probability. Each game in the sequence, Game G_i, is played by the reduction $\mathcal{R}$ and a (possibly inefficient) challenger $\mathcal{C}_i$, specific for that game, that simulates all the environment for $\mathcal{R}$. Namely it provides the input for $\mathcal{R}$, and simulates the oracle $\mathcal{O}$ solving the $\mathcal{D}_k^{\mathbf{B}}$-MDDH problem with overwhelming probability and the generic group oracle.

Notice that in the generic k-linear group model $\mathcal{R}$'s input is an encoding of an instance of $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$, $([\boldsymbol{t}],[\boldsymbol{z}])$, consisting only of elements in $\mathbb{G}$. These group elements are generated by evaluating a polynomial map $\mathfrak{h}$ at a random point. Namely, for a 'real' instance $\mathfrak{h}_1(\boldsymbol{t},\boldsymbol{w}) = (\boldsymbol{t},\mathbf{A}(\boldsymbol{t})\boldsymbol{w}) = (\boldsymbol{t},\boldsymbol{z})$, and for a 'random' instance, $\mathfrak{h}_0$ is the identity map. Observe that both polynomials $\mathfrak{h}_0$, $\mathfrak{h}_1$ have degree 1. For notational convenience, we will denote 'real' instances by $b = 1$ and 'random' instances by $b = 0$, where b is a variable defined by the challenger. Thus, in the generic k-linear group model every group element $[y] \in \mathbb{G}$ or $[y]_T \in \mathbb{G}_T$ handled by $\mathcal{R}$ can be seen as a polynomial in the formal variables $(\boldsymbol{T},\boldsymbol{W})$ or $(\boldsymbol{T},\boldsymbol{Z})$, depending on the type of input instance given to $\mathcal{R}$. To give more notational uniformity to the proof we will consider that the polynomial Y associated to a group element $[y]$ or $[y]_T$ depends on the variables $(\boldsymbol{T},\boldsymbol{Z})$, formally representing the entries of $(\boldsymbol{t},\boldsymbol{z})$. Thus, $Y \in \mathbb{Z}_q[\boldsymbol{T},\boldsymbol{Z}]$ but then composing Y with the sampling polynomial, $\mathfrak{y} = Y \circ \mathfrak{h}_b$ is either in $\mathbb{Z}_q[\boldsymbol{T},\boldsymbol{W}]$ if $b = 1$, or it is in $\mathbb{Z}_q[\boldsymbol{T},\boldsymbol{Z}]$ if $b = 0$.[15]

The combination of the generic k-linear group model with algorithms with additional oracle access is not a trivial task, since depending of the oracle definition, some essential information about the representation of the group elements can be leaked to the algorithm, thus breaking the usual arguments in the generic model proofs. For this reason we give a more detailed proof that analyzes step-by-step the transition between a generic k-linear group model based on random encodings to its purely algebraic counterpart. It is worth noticing that the methodology used here is specific for the MDDH problem structure, and therefore it cannot be directly applied to other scenarios.

In the proof we will consider two different simulation strategies for both the generic group oracle and the oracle $\mathcal{O}$. We describe them before detailing the sequence of games.

Real (value-based) simulation of the generic group oracle. This is the usual strategy for the simulation. The challenger maintains two tables $\mathcal{T}_1$, $\mathcal{T}_k$ with entries $(y, Y, \mathfrak{y}, L_y)$, where $y \in \mathbb{Z}_q$, $Y \in \mathbb{Z}_q[\boldsymbol{T},\boldsymbol{Z}]$ is a polynomial representing y, $\mathfrak{y} = Y \circ \mathfrak{h}_b$ ($\mathfrak{h}_b$ is the sampling polynomial defined above), and L_y is a string called 'label', randomly drawn from a large enough set (making hard for $\mathcal{R}$ to guess a valid label).[16] The tuple $(y, Y, \mathfrak{y}, L_y)$ represents either the group element $[y]$ or $[y]_T$, depending on the table it belongs to. The tables are initialized with $(0,0,0,L_0)$ and $(1,1,1,L_1)$ and $(0,0,0,L_{0,k})$ and $(1,1,1,L_{1,k})$, for the neutral element and generator of $\mathbb{G}$ and $\mathbb{G}_T$. Group elements in the input of $\mathcal{R}$, $([\boldsymbol{t}],[\boldsymbol{z}])$, are replaced by freshly generated labels, which are stored in the table $\mathcal{T}_1$ along with their discrete logarithms $(\boldsymbol{t},\boldsymbol{z})$ and the corresponding formal variables $\boldsymbol{T},\boldsymbol{Z}$ and their composition with $\mathfrak{h}_b$.

All operations queried by $\mathcal{R}$ to the generic group oracle are performed on the discrete logarithms stored in the tables and on the associated polynomials. For

[15] Indeed, the polynomial Y models what $\mathcal{R}$ knows about $[y]$ in the generic k-linear group model, while the challenger also knows $\mathfrak{y}$, or even the discrete logarithm y.

[16] It suffices, for instance, taking a set of size greater than q^5.

instance, for a query $\mathsf{GroupOp}(L_1, L_2)$, two tuples $(y_1, Y_1, \mathfrak{y}_1, L_1)$, $(y_2, Y_2, \mathfrak{y}_2, L_2)$ are located at either one of the tables $\mathcal{T}_1$ or $\mathcal{T}_k$. If a tuple $(y_1 + y_2, Y_3, \mathfrak{y}_3, L_3)$ already exists in the same table then L_3 is answered to $\mathcal{R}$. Otherwise, a fresh random label L_3 is generated, the tuple $(y_1 + y_2, Y_1 + Y_2, \mathfrak{y}_1 + \mathfrak{y}_2, L_3)$ is added to the table and L_3 is answered to $\mathcal{R}$. The other oracle queries $\mathsf{GroupInv}(L_1)$ and $\mathsf{GroupML}(L_1, \ldots, L_k)$ work similarly, except that in the last case labels $L_1, \ldots, L_k$ are looked only at table $\mathcal{T}_1$ and the resulting tuple is added to table $\mathcal{T}_k$. Any improper query (e.g., containing an unknown or invalid label) made by $\mathcal{R}$ is rejected by the oracle.

Observe that the polynomials stored in the tables are unused in this simulation. But always in any tuple $(y, Y, \mathfrak{y}, L_y)$, y is the result of evaluating Y at the point $(\boldsymbol{t}, \boldsymbol{z})$ sampled by the challenger (or evaluating $\mathfrak{y}$ at either $(\boldsymbol{t}, \boldsymbol{w})$ if $b = 1$ or $(\boldsymbol{t}, \boldsymbol{z})$ if $b = 0$).

Algebraic (polynomial-based) simulation of the generic group oracle. In this simulation the discrete logarithms stored in the tables are no longer used, and the polynomial components are used instead. Namely, in a query $\mathsf{GroupOp}(L_1, L_2)$, instead of looking for a tuple $(y_1+y_2, Y_3, \mathfrak{y}_3, L_3)$, it looks for $(y_3, Y_3, \mathfrak{y}_1+\mathfrak{y}_2, L_3)$. Notice that now a label is not associated to a true group element, but to an algebraic relation with the parameters used in the sampling procedure. Therefore, the two simulations will differ when after some query to the real generic group oracle there exist two different tuples $(y_1, Y_1, \mathfrak{y}_1, L_1)$, $(y_2, Y_2, \mathfrak{y}_2, L_2)$ in the same table such that $y_1 = y_2$ while $\mathfrak{y}_1 \neq \mathfrak{y}_2$. This implies that the non-zero polynomial $\mathfrak{y}_2 - \mathfrak{y}_1$ vanishes at the random point ($(\boldsymbol{t}, \boldsymbol{w})$ if $b = 1$ or $(\boldsymbol{t}, \boldsymbol{z})$ if $b = 0$) used in the sampling procedure.

In a standard proof in the generic k-linear group model we can easily upper bound the probability that such a difference occurs between the two simulation strategies, by just considering the degree of the polynomials and applying Schwartz-Zippel lemma. However, things are not so simple when $\mathcal{R}$ has access to extra oracles, that could leak some information about the group elements outside of the generic k-linear group model. We then consider also an algebraic simulation of the additional oracle $\mathcal{O}$.

For technical reasons, we need to ensure that only 'good' instances of $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ and $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$ are handled by $\mathcal{R}$, i.e., instances with $\operatorname{rank} \mathbf{A}(\boldsymbol{t}) = \operatorname{rank} \mathbf{B}(\boldsymbol{s}) = k$. This is not an issue since for any black-box reduction $\mathcal{R}$ there exists another one $\mathcal{R}'$ with at least the same advantage solving $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$, and running essentially within the same time, fulfilling the previous requirement. The only differences between both reductions are that $\mathcal{R}'$ directly solves any instance $([\boldsymbol{t}], [\boldsymbol{z}])$ of $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ with $\operatorname{rank} \mathbf{A}(\boldsymbol{t}) < k$ via the k-linear map (as already described in the proof of Theorem 3), and all queries $([\boldsymbol{s}], [\boldsymbol{u}])$ to the oracle $\mathcal{O}$ made by $\mathcal{R}$ with $\operatorname{rank} \mathbf{B}(\boldsymbol{s}) < k$ are directly solved by $\mathcal{R}'$ itself, also with the k-linear map. From now on, we will assume that $\mathcal{R} = \mathcal{R}'$.

Real (value-based) simulation of the oracle $\mathcal{O}$. We will simulate an oracle $\mathcal{O}$ that solves the $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$ problem with overwhelming probability. Since we are considering $\mathcal{R} = \mathcal{R}'$, we only deal with instances $([\boldsymbol{s}], [\boldsymbol{u}])$ such that $\operatorname{rank} \mathbf{B}(\boldsymbol{s}) = k$.

With this restriction, $\boldsymbol{u} \in \operatorname{Im} \mathbf{B}(\boldsymbol{s})$ if and only if $\det(\mathbf{B}(\boldsymbol{s}) \| \boldsymbol{u}) = 0$, or equivalently, $\mathfrak{d}_{\mathbf{B}}(\boldsymbol{s}, \boldsymbol{u}) = 0$. Thus, we define $\mathcal{O}$ to output 1 if and only if $\mathfrak{d}_{\mathbf{B}}(\boldsymbol{s}, \boldsymbol{u}) = 0$. Notice that 'real' instances are correctly solved with probability one, while 'random' instances are solved correctly only with probability $1 - 1/q$, because the latter instances include the former ones.[17] In this simulation, in order to compute $\mathfrak{d}_{\mathbf{B}}(\boldsymbol{s}, \boldsymbol{u})$ the challenger needs the real values of $([\boldsymbol{s}], [\boldsymbol{u}])$. But in the generic k-linear group model (either value-based or polynomial-based one) the simulator can recover the discrete logarithms $(\boldsymbol{s}, \boldsymbol{u})$ from the labels queried by $\mathcal{R}$ and the table $\mathcal{T}_1$, maintained by the generic group oracle. As before, any improper query (e.g., containing an unknown or invalid label) made by $\mathcal{R}$ is rejected by the oracle. Once $(\boldsymbol{s}, \boldsymbol{u})$ are known, the challenger directly evaluates $\mathfrak{d}_{\mathbf{B}}(\boldsymbol{s}, \boldsymbol{u})$ and obtains the oracle answer.

Algebraic (polynomial-based) simulation of the oracle $\mathcal{O}$. Similarly as happens to the generic group oracle, in the algebraic version the challenger retrieves from the table $\mathcal{T}_1$ the polynomials $(\boldsymbol{S}, \boldsymbol{U})$ corresponding to the labels queried by $\mathcal{R}$, and not the discrete logarithms. This means that the simulator obtains a polynomial map f of degree one,[18] expressing the variables $(\boldsymbol{S}, \boldsymbol{U})$ as polynomials in $(\boldsymbol{T}, \boldsymbol{Z})$. Now the challenger computes the composition $\mathfrak{g} = \mathfrak{d}_{\mathbf{B}} \circ f \circ \mathfrak{h}_b$, which is also a polynomial. If $\mathfrak{g} = 0$ (as a polynomial) then the oracle answer is set to 1, otherwise the answer is 0. Again, both simulations can differ only when $\mathfrak{g}$ is a non-zero polynomial but it vanishes at the random point ($(\boldsymbol{t}, \boldsymbol{w})$ or $(\boldsymbol{t}, \boldsymbol{z})$) used in the sampling procedure.

Essentially, switching from the value-based simulation to the polynomial-based one means delaying the sampling of the parameters, which could cause some inconsistencies in the simulation. We introduce a sequence of games such that the oracles switch gradually from one model to the other, and we bound the error probability in each step in the sequence. Let Q be the number of calls to $\mathcal{O}$ made by $\mathcal{R}$, let n_i for $i = 1, \ldots, Q$ be the number of calls to the generic group oracle made by $\mathcal{R}$ before the i-th oracle call to $\mathcal{O}$, and let n_∞ be the total number of calls to the generic group oracle made by $\mathcal{R}$.

Game $\mathsf{G}_{\mathsf{real},b}$, $b \in \{0,1\}$: This game perfectly simulates the environment for $\mathcal{R}$ as a distinguisher for the $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ problem (fed with a 'real' instance if $b = 1$, and a 'random' instance if $b = 0$), with oracle access to a solver for the $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$ problem, that answers correctly with an overwhelming probability. In this game, the challenger $\mathcal{C}_{\mathrm{real},b}$ initializes the tables $\mathcal{T}_1$ and $\mathcal{T}_k$ and computes the input labels for $\mathcal{R}$, as explained in the previous paragraph "Real (value-based) simulation of the generic group oracle". Then $\mathcal{C}_{\mathrm{real},b}$ uses the real simulation of both the generic group oracle and the oracle $\mathcal{O}$. Finally, $\mathcal{C}_{\mathrm{real},b}$ just forwards $\mathcal{R}$'s output bit.

[17] This problem could be overcome by redefining the MDDH problems as telling apart 'real' from non-'real' instances.

[18] Observe that all the group elements considered here are in $\mathbb{G}$, and the group operation in $\mathbb{G}$ corresponds to linear combinations of the associated polynomials.

Game $G_{i,b}$*,* $i = 1, \dots, Q$*,* $b \in \{0,1\}$*:* The challenger performs the same initialization as $\mathcal{C}_{\mathrm{real},b}$, but it uses instead the algebraic simulation of both the generic group oracle and the oracle $\mathcal{O}$, until $\mathcal{R}$ makes the i-th query to $\mathcal{O}$. Then, $\mathcal{C}_{i,b}$ switches to the real simulation to answer this query and all subsequent queries to the two oracles. Finally, $\mathcal{C}_{i,b}$ just forwards $\mathcal{R}$'s output bit.

Game $G'_{i,b}$*,* $i = 1, \dots, Q$*,* $b \in \{0,1\}$*:* The challenger $\mathcal{C}'_{i,b}$ only differs from $\mathcal{C}_{i,b}$ in that it uses the algebraic simulation also to answer the i-th query to $\mathcal{O}$ (thus, the switching point is moved to just after answering that query).

Game $G_{\mathsf{alg},b}$*,* $b \in \{0,1\}$*:* The challenger performs the same initialization as $\mathcal{C}_{\mathrm{real},b}$, but it uses instead the algebraic simulation of both the generic group oracle and the oracle $\mathcal{O}$ all the time. Finally, $\mathcal{C}_{i,b}$ just forwards $\mathcal{R}$'s output bit.

Now we analyze the differences between the games. It should be mentioned that during the simulation, $\mathcal{R}$ itself can partially maintain the tables $\mathcal{T}_1$ and $\mathcal{T}_k$. Namely, it can associate each label L_y to the corresponding polynomial Y.

Step $G_{real,b} \to G_{1,b}$*,* $b \in \{0,1\}$*:* The only possible difference between games can occur if in some query to the generic group oracle before the first query to $\mathcal{O}$ it happens that there exist two different tuples $(y_1, Y_1, \mathfrak{y}_1, L_1)$, $(y_2, Y_2, \mathfrak{y}_2, L_2)$ in the same table ($\mathcal{T}_1$ or $\mathcal{T}_k$) such that $y_1 = y_2$ while $\mathfrak{y}_1 \neq \mathfrak{y}_2$, which implies that the non-zero polynomial $\mathfrak{y}_2 - \mathfrak{y}_1$ vanishes at the random point ($(\boldsymbol{t}, \boldsymbol{w})$ if $b = 1$ or $(\boldsymbol{t}, \boldsymbol{z})$ if $b = 0$) used in the sampling procedure. Lets call this event $F_{1,b}$. Then, by Schwartz-Zippel lemma,

$$\Pr[F_{1,b}] \leq \binom{n_1}{2} \frac{k}{q}$$

since there are at most $\binom{n_1}{2}$ different pairs of polynomials $(\mathfrak{y}_1, \mathfrak{y}_2)$ in the tables. Indeed, the degree of the polynomial $\mathfrak{y}_2 - \mathfrak{y}_1$ is upper bounded by k, since the sampling polynomial $\mathfrak{h}_b$ has degree 1.

Step $G_{i,b} \to G'_{i,b}$*,* $b \in \{0,1\}$*,* $1 \leq i \leq Q$*:* The games are identical until the i-th query to $\mathcal{O}$ is made. Moreover, at this point, conditioned to b, the view of $\mathcal{R}$ is independent of the true values $(\boldsymbol{t}, \boldsymbol{z})$ if $b = 0$, or $(\boldsymbol{t}, \boldsymbol{w})$ if $b = 1$. The only difference between the two games can occur because of the simulation of $\mathcal{O}$ in this query. Namely, there exists a nonzero polynomial $\mathfrak{g} = \mathfrak{d}_{\mathbf{B}} \circ f \circ \mathfrak{h}_b$, of degree at most $\deg \mathfrak{d}_{\mathbf{B}} = k + 1$ that vanishes at the random point ($(\boldsymbol{t}, \boldsymbol{w})$ or $(\boldsymbol{t}, \boldsymbol{z})$) used in the sampling procedure. Lets call this event $F'_{i,b}$. Again, by Schwartz-Zippel lemma,

$$\Pr[F'_{i,b}] \leq \frac{k+1}{q}.$$

Step $G'_{i,b} \to G_{i+1,b}$*,* $b \in \{0,1\}$*,* $1 \leq i \leq Q - 1$*:* The games proceed identically until the i-th query to $\mathcal{O}$ is answered. Again, at this point, conditioned to b, the view of $\mathcal{R}$ is independent of the true values $(\boldsymbol{t}, \boldsymbol{z})$ if $b = 0$, or $(\boldsymbol{t}, \boldsymbol{w})$ if $b = 1$.

As in the step $G_{\mathrm{real},b} \to G_{1,b}$, the only difference between games is due to the simulation of the generic group oracle. Lets call $F_{i+1,b}$ to the event that between the i-th and the $(i+1)$-th calls to $\mathcal{O}$, as a consequence of a query to the generic group oracle, there exist two different tuples $(y_1, Y_1, \mathfrak{y}_1, L_1)$, $(y_2, Y_2, \mathfrak{y}_2, L_2)$ in the same table ($\mathcal{T}_1$ or $\mathcal{T}_k$) such that $y_1 = y_2$ while $\mathfrak{y}_1 \neq \mathfrak{y}_2$, but at least one of them is generated within this period. By Schwartz-Zippel lemma,

$$\Pr[F_{i+1,b}] \leq \left(\binom{n_{i+1}}{2} - \binom{n_i}{2} \right) \frac{k}{q}.$$

Step $G'_{Q,b} \to G_{alg,b}$, $b \in \{0,1\}$: This step follows exactly the same argument as any other $G'_{i,b} \to G_{i+1,b}$ with $i < Q$. Therefore, we define $F_{\mathrm{alg},b}$ accordingly, and

$$\Pr[F_{\mathrm{alg},b}] \leq \left(\binom{n_\infty}{2} - \binom{n_Q}{2} \right) \frac{k}{q}.$$

Step $G_{alg,0} \to G_{alg,1}$: As a final step, we argue that the two games must be identical. Otherwise, either $\mathcal{D}_k^{\mathbf{A}}$ is not a hard matrix distribution, or there exists a polynomial map $f : \mathbb{Z}_q^{d+k+1} \to \mathbb{Z}_q^{e+k+1}$ of degree one such that $\lambda \mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ for some nonzero constant $\lambda \in \mathbb{Z}_q$. Firstly let us assume that the first difference in the oracle answers given to $\mathcal{R}$ occurs in a query to the generic group oracle. Then there exists two different tuples $(y_1, Y_1, \mathfrak{y}_1, L_1)$, $(y_2, Y_2, \mathfrak{y}_2, L_2)$ in the same table ($\mathcal{T}_1$ or $\mathcal{T}_k$) such that $\mathfrak{y}_1 = \mathfrak{y}_2$ in one game while $\mathfrak{y}_1 \neq \mathfrak{y}_2$ in the other. But this can only happen if $Y_1 \neq Y_2$ and $Y_1 \circ \mathfrak{h}_1 = Y_2 \circ \mathfrak{h}_1$, because $\mathfrak{h}_0$ is the identity map. Therefore, by Theorem 2 the existence of the polynomial $Y_2 - Y_1$, which has degree at most k, contradicts the fact that $\mathcal{D}_k^{\mathbf{A}}$ is a hard matrix distribution.

Suppose now that the first difference between games occur in a query to $\mathcal{O}$. This implies that there exists a polynomial map f of degree one such that the composition $\mathfrak{g} = \mathfrak{d}_{\mathbf{B}} \circ f \circ \mathfrak{h}_b$ is the zero polynomial only in one of the games. Again, using that $\mathfrak{h}_0$ is the identity, it must happen that $\mathfrak{d}_{\mathbf{B}} \circ f \neq 0$ and $\mathfrak{d}_{\mathbf{B}} \circ f \circ \mathfrak{h}_1 = 0$. But then, Theorem 2 applied to the hard matrix distribution $\mathcal{D}_k^{\mathbf{A}}$ implies that $\mathfrak{d}_{\mathbf{B}} \circ f$ is a multiple of $\mathfrak{d}_{\mathbf{A}}$. Finally, $k+1 = \deg \mathfrak{d}_{\mathbf{A}} \leq \deg(\mathfrak{d}_{\mathbf{B}} \circ f) \leq \deg \mathfrak{d}_{\mathbf{B}} = k+1$ and then $\mathfrak{d}_{\mathbf{B}} \circ f$ can only be a nonzero scalar multiple of $\mathfrak{d}_{\mathbf{A}}$, which contradicts the assumption about the nonexistence of such map f.

Summing up, using the triangle inequality, the advantage of $\mathcal{R}$ solving the $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ problem is

$$\begin{aligned}
&|\Pr[G_{\mathrm{real},1}[\mathcal{R}] = 1] - \Pr[G_{\mathrm{real},0}[\mathcal{R}] = 1]| \leq \\
&\quad \leq \Pr[F_{\mathrm{alg},1}] + \Pr[F_{\mathrm{alg},0}] + \sum_{i=1}^{Q} \left(\Pr[F'_{i,1}] + \Pr[F_{i,1}] + \Pr[F_{i,0}] + \Pr[F'_{i,0}] \right) \leq \\
&\quad \leq \frac{n_\infty^2 k}{q} + \frac{2Q(k+1)}{q} \in negl
\end{aligned}$$

□

Not all polynomial maps of degree one can actually fulfil the equation $\lambda \mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$. In particular, any such f must be injective.

Lemma 5. *Let $\mathcal{D}_k^{\mathbf{A}}$ and $\mathcal{D}_k^{\mathbf{B}}$ be as in Theorem 4. Any polynomial map of degree one such that $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ for a nonzero $\lambda \in \mathbb{Z}_q$ is injective.*

Proof. For any non-injective map f there exists $(\boldsymbol{\tau}, \boldsymbol{\zeta}) \in \mathbb{Z}_q^d \times \mathbb{Z}_q^{k+1} \setminus \{(\mathbf{0}, \mathbf{0})\}$ such that $f(\boldsymbol{\tau}, \boldsymbol{\zeta}) = f(\mathbf{0}, \mathbf{0})$. Indeed, since f is a polynomial map of degree one, we can write $f(\boldsymbol{t}, \boldsymbol{z}) = f(\mathbf{0}, \mathbf{0}) + g(\boldsymbol{t}, \boldsymbol{z})$ where the map g is linear. Then, for all $\boldsymbol{t}, \boldsymbol{\tau} \in \mathbb{Z}_q^d$ and all $\boldsymbol{z}, \boldsymbol{\zeta} \in \mathbb{Z}_q^{k+1}$,

$$f(\boldsymbol{t}+\boldsymbol{\tau}, \boldsymbol{z}+\boldsymbol{\zeta}) - f(\boldsymbol{t}, \boldsymbol{z}) = g(\boldsymbol{t}+\boldsymbol{\tau}, \boldsymbol{z}+\boldsymbol{\zeta}) - g(\boldsymbol{t}, \boldsymbol{z}) = g(\boldsymbol{\tau}, \boldsymbol{\zeta}) = f(\boldsymbol{\tau}, \boldsymbol{\zeta}) - f(\mathbf{0}, \mathbf{0})$$

Then, any collision $f(\boldsymbol{t_1}, \boldsymbol{z_1}) = f(\boldsymbol{t_2}, \boldsymbol{z_2})$ implies $f(\boldsymbol{\tau}, \boldsymbol{\zeta}) = f(\mathbf{0}, \mathbf{0})$ for $\boldsymbol{\tau} = \boldsymbol{t_1} - \boldsymbol{t_2}$ and $\boldsymbol{\zeta} = \boldsymbol{z_1} - \boldsymbol{z_2}$. Conversely, $f(\boldsymbol{\tau}, \boldsymbol{\zeta}) = f(\mathbf{0}, \mathbf{0})$ implies $f(\boldsymbol{t}+\boldsymbol{\tau}, \boldsymbol{z}+\boldsymbol{\zeta}) = f(\boldsymbol{t}, \boldsymbol{z})$ for all $\boldsymbol{t} \in \mathbb{Z}_q^d$ and $\boldsymbol{z} \in \mathbb{Z}_q^{k+1}$. Now, from the equation $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ we know that $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}+\boldsymbol{\tau}, \boldsymbol{z}+\boldsymbol{\zeta}) = \lambda\mathfrak{d}_{\mathbf{B}}(f(\boldsymbol{t}+\boldsymbol{\tau}, \boldsymbol{z}+\boldsymbol{\zeta})) = \lambda\mathfrak{d}_{\mathbf{B}}(f(\boldsymbol{t}, \boldsymbol{z})) = \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \boldsymbol{z})$ for all $\boldsymbol{t} \in \mathbb{Z}_q^d$ and $\boldsymbol{z} \in \mathbb{Z}_q^{k+1}$, which contradicts Lemma 4 unless $(\boldsymbol{\tau}, \boldsymbol{\zeta}) = (\mathbf{0}, \mathbf{0})$. This finally proves the injectivity of f. □

The necessary injectivity of the map f gives us the following result, that essentially claims that a successful generic black-box reduction between MDDH problems cannot reduce the amount of randomness in the problem instance.

Corollary 1. *Let $\mathcal{D}_k^{\mathbf{A}}$ and $\mathcal{D}_k^{\mathbf{B}}$ be as in Theorem 4. If there exists a generic black-box reduction from the $\mathcal{D}_k^{\mathbf{A}}$-*MDDH *problem to the $\mathcal{D}_k^{\mathbf{B}}$-*MDDH *problem, then $e \geq d$.*

We now address the natural question about whether the converse of Theorem 4 is also true. We easily show that the converse actually holds, but for reductions using a perfect oracle (*i.e.*, that correctly solves all instances of the problem). Building a more general reduction from the map f, working with imperfect oracles, is a bit more involved. Indeed, it requires some extra properties of f, or some random self-reducibility properties of the MDDH problems.

Theorem 5. *Let $\mathcal{D}_k^{\mathbf{A}}$ and $\mathcal{D}_k^{\mathbf{B}}$ be as in Theorem 4. If there exists a degree one polynomial map $f : \mathbb{Z}_q^{d+k+1} \to \mathbb{Z}_q^{e+k+1}$ such that $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ for some nonzero constant $\lambda \in \mathbb{Z}_q$, then*

1. *there exists a black-box deterministic reduction from the $\mathcal{D}_k^{\mathbf{A}}$-*MDDH *problem to the $\mathcal{D}_k^{\mathbf{B}}$-*MDDH *problem, using a single oracle call, that succeeds with overwhelming probability if the oracle is perfect.*
2. *if in addition f is surjective, then the above reduction is actually a tight black-box reduction using a single oracle call, for any imperfect oracle.*
3. *otherwise, if $\mathcal{D}_k^{\mathbf{B}}$ is random self-reducible (see Definition 6)*[19]*, then there also exists a (probabilistic) tight black-box reduction with the same properties.*

[19] If it is only quasi random self-reducible, then one have to additionally check whether the image of f intersects properly with the set $\mathcal{X}$ of randomizable instances (see again Definition 7 for more details).

Proof. To prove the theorem, we just show a reduction $\mathcal{R}$ making a single oracle call, based on the map f. Namely, on the input of an instance $([\boldsymbol{t}],[\boldsymbol{z}])$ of $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$, $\mathcal{R}$ computes $([\boldsymbol{s}],[\boldsymbol{u}])$ by applying f to it. Observe that these computations only involve group operations in $\mathbb{G}$, since $\deg f = 1$. Then $\mathcal{R}$ queries the oracle on $([\boldsymbol{s}],[\boldsymbol{u}])$ and just forwards its answer.

For convenience, we classify the problem instances $([\boldsymbol{t}],[\boldsymbol{z}])$ of $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ (we omit here $(q,\mathbb{G},g)$ for simplicity) into four types: 'good real', 'bad real', 'good non-real', 'bad non-real'. Here 'real' refers to instances such that $\boldsymbol{z} \in \operatorname{Im} \mathbf{A}(\boldsymbol{t})$, while 'bad' corresponds to $\boldsymbol{t} \in V_{\mathbf{A}}^{\text{def}}$. Let $\mathcal{Y}_{\mathbf{A}}$ and $\mathcal{N}_{\mathbf{A}}$ respectively denote the sets of good real and good non-real instances, and $\mathsf{U}_{\mathcal{Y}_{\mathbf{A}}}$ and $\mathsf{U}_{\mathcal{N}_{\mathbf{A}}}$ the corresponding uniform probability distributions. Notice that $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t},\boldsymbol{z}) \neq 0$ if and only if $(\boldsymbol{t},\boldsymbol{z}) \in \mathcal{N}_{\mathbf{A}}$. On the other hand, the probability distribution $D_{\text{real}}^{\mathbf{A}}$ given in Definition 3 produces both good and bad real instances, while $D_{\text{random}}^{\mathbf{A}}$ produces the four types. Theorem 3 ensures that $V_{\mathbf{A}}^{\text{def}}$ is a negligible fraction of the set $\mathbb{Z}_q^d$, that is, there exists a negligible function $\varepsilon_{\mathbf{A}}$ such that $\left|V_{\mathbf{A}}^{\text{def}}\right| = \varepsilon_{\mathbf{A}} q^d$ (where $|\mathcal{X}|$ denotes the cardinality of a set $\mathcal{X}$). Thus $D_{\text{random}}^{\mathbf{A}}$ produces elements in $\mathcal{N}_{\mathbf{A}}$ with overwhelming probability, while $D_{\text{real}}^{\mathbf{A}}$ produces elements in $\mathcal{Y}_{\mathbf{A}}$ with overwhelming probability. Therefore, we can replace the distributions $D_{\text{real}}^{\mathbf{A}}$ and $D_{\text{random}}^{\mathbf{A}}$ by $\mathsf{U}_{\mathcal{Y}_{\mathbf{A}}}$ and $\mathsf{U}_{\mathcal{N}_{\mathbf{A}}}$ without any noticeable change in Definition 3. We also apply the same considerations to the $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$ problem.

The map f transforms $\mathcal{N}_{\mathbf{A}}$ into $\mathcal{N}_{\mathbf{B}}$, since $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ and then $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t},\boldsymbol{z}) \neq 0$ if and only if $\mathfrak{d}_{\mathbf{B}}(\boldsymbol{s},\boldsymbol{u}) \neq 0$. The case of good real instances is not so easy, as f can map the elements in $\mathcal{Y}_{\mathbf{A}}$ into either of the three types: good real, bad real and bad non-real. However, we can show that f maps uniformly distributed elements in $\mathcal{Y}_{\mathbf{A}}$ into $\mathcal{Y}_{\mathbf{B}}$ with overwhelming probability. Namely, consider a generic distinguisher A solving the $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ problem in the following way: First, A computes $([\boldsymbol{s}],[\boldsymbol{u}])$ from $([\boldsymbol{t}],[\boldsymbol{z}])$ using f. Then, A checks whether $\boldsymbol{s} \in V_{\mathbf{B}}^{\text{def}}$, that is, $\operatorname{rank} \mathbf{B}(\boldsymbol{s}) < k$ using the k-linear map. If so, A decides that $([\boldsymbol{t}],[\boldsymbol{z}]) \in \mathcal{Y}_{\mathbf{A}}$. Otherwise, it decides $([\boldsymbol{t}],[\boldsymbol{z}]) \in \mathcal{N}_{\mathbf{A}}$. It is easy to see that the advantage of A is $\Pr[f(\boldsymbol{t},\boldsymbol{z}) \notin \mathcal{Y}_{\mathbf{B}}; (\boldsymbol{t},\boldsymbol{z}) \leftarrow \mathcal{Y}_{\mathbf{A}}]$, since bad $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$ instances never come from $\mathcal{N}_{\mathbf{A}}$. Then A breaks the generic hardness of $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ unless f maps uniformly distributed elements in $\mathcal{Y}_{\mathbf{A}}$ into $\mathcal{Y}_{\mathbf{B}}$ with overwhelming probability.

With these ideas in mind we consider now the three cases in the theorem separately. Since f preserves good real and good non-real instances with overwhelming probability, the reduction $\mathcal{R}$ succeeds with overwhelming probability for a perfect oracle solving the $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$ problem. However, the general case of an imperfect oracle is harder, because we need to show that $f(\mathsf{U}_{\mathcal{Y}_{\mathbf{A}}}) \approx \mathsf{U}_{\mathcal{Y}_{\mathbf{B}}}$ and $f(\mathsf{U}_{\mathcal{N}_{\mathbf{A}}}) \approx \mathsf{U}_{\mathcal{N}_{\mathbf{B}}}$, where $\approx$ denotes that two distributions are statistically close.

Let us assume that f is surjective (*i.e.*, the second case in the theorem). According to Lemma 5, f is injective, so it is a bijection and then $e = d$. Therefore, $f(\mathsf{U}_{\mathcal{N}_{\mathbf{A}}}) = \mathsf{U}_{\mathcal{N}_{\mathbf{B}}}$.[20] Similarly, consider the subset $\mathcal{Y}'_{\mathbf{A}} = \mathcal{Y}_{\mathbf{A}} \cap f^{-1}(\mathcal{Y}_{\mathbf{B}})$, containing all good real instances of $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ transformed by f into good real instances of $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$. Because of the above discussion, $\mathsf{U}_{\mathcal{Y}'_{\mathbf{A}}} \approx \mathsf{U}_{\mathcal{Y}_{\mathbf{A}}}$. In

[20] An injective map f always transforms the uniform probability distribution on a subset $\mathcal{X}$ into the uniform distribution on the image subset $\mathcal{Y} = f(\mathcal{X})$.

particular, there exists a negligible function ε such that $|\mathcal{Y}'_{\mathbf{A}}| = (1-\varepsilon)\,|\mathcal{Y}_{\mathbf{A}}|$. We also claim that $f(\mathsf{U}_{\mathcal{Y}'_{\mathbf{A}}}) \approx \mathsf{U}_{\mathcal{Y}_{\mathbf{B}}}$. Indeed, $|\mathcal{Y}_{\mathbf{A}}| = (1-\varepsilon_{\mathbf{A}})q^d q^k$, since every good real instance can be uniquely written as $(\boldsymbol{t}, \mathbf{A}(\boldsymbol{t})\boldsymbol{w})$ for $\boldsymbol{t} \in \mathbb{Z}_q^d \setminus V_{\mathbf{A}}^{\text{def}}$ and $\boldsymbol{w} \in \mathbb{Z}_q^k$, and similarly $|\mathcal{Y}_{\mathbf{B}}| = (1-\varepsilon_{\mathbf{B}})q^d q^k$ for some negligible function $\varepsilon_{\mathbf{B}}$. Moreover, by definition, $f(\mathcal{Y}'_{\mathbf{A}}) \subset \mathcal{Y}_{\mathbf{B}}$, and by the injectivity of f, $|f(\mathcal{Y}'_{\mathbf{A}})| = |\mathcal{Y}'_{\mathbf{A}}| = (1-\varepsilon)\,|\mathcal{Y}_{\mathbf{A}}| = (1-\varepsilon)(1-\varepsilon_{\mathbf{A}})q^d q^k$, that differs from $|\mathcal{Y}_{\mathbf{B}}|$ only in a negligible fraction. Finally, we have that $\mathsf{U}_{\mathcal{Y}_{\mathbf{A}}} \approx \mathsf{U}_{\mathcal{Y}'_{\mathbf{A}}}$ implies $f(\mathsf{U}_{\mathcal{Y}_{\mathbf{A}}}) \approx f(\mathsf{U}_{\mathcal{Y}'_{\mathbf{A}}})$, and along with $f(\mathsf{U}_{\mathcal{Y}'_{\mathbf{A}}}) \approx \mathsf{U}_{\mathcal{Y}_{\mathbf{B}}}$ imply that $f(\mathsf{U}_{\mathcal{Y}_{\mathbf{A}}}) \approx \mathsf{U}_{\mathcal{Y}_{\mathbf{B}}}$. This proves that $\mathcal{R}$ has the same advantage as the oracle, up to a negligible function.

Concerning the third part of the theorem, if f is not surjective then we would need to randomize it. This is actually possible when $\mathcal{D}_k^{\mathbf{B}}$ is random self-reducible (according to Definition 6). Indeed, we have seen that except for a negligible error probability f maps real instances into real instances, and also non-real instances into non-real instances. Therefore, the composition of the reduction in Definition 6 and the map f produces the right distributions (except for a negligible statistical distance) for real and random instances, even when f is not surjective. Therefore, a tight reduction from the $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ problem to the $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$ problem is obtained also in this case. □

It is easy to see that when $\mathcal{D}_k^{\mathbf{B}}$ is only quasi random self-reducible, if the images $(\boldsymbol{s}, \boldsymbol{u}) = f(\boldsymbol{t}, \boldsymbol{z})$ both for $(\boldsymbol{t}, \boldsymbol{z}) \leftarrow D_{\text{real}}^{\mathbf{A}}$ and $(\boldsymbol{t}, \boldsymbol{z}) \leftarrow D_{\text{random}}^{\mathbf{A}}$ fulfil $\boldsymbol{s} \in \mathcal{X}$ with overwhelming probability, where $\mathcal{X}$ is the set of rerandomizable matrices in Definition 7, then we can also prove the existence of the reduction.

It is noticeable that, as a byproduct of the last two theorems, whenever a generic black-box reduction from $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ to $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$ exists, and either $d = e$ or $\mathcal{D}_k^{\mathbf{B}}$-$\mathsf{MDDH}$ is random self-reducible, then there also exists a simple reduction with the following properties: 1) The reduction only makes a single oracle query. 2) It never uses the multilinear map, and then it only performs some group operations in the base group $\mathbb{G}$. 3) It is probabilistic only when the random self-reducibility property is needed. Intuitively, this means that there is little hope in that making many oracle calls or trying to use the multilinear map helps finding a reduction between two reasonable MDDH problems.

Some examples of reductions from MDDH families can be easily obtained by combining the previous theorem and the quasi random self-reducibility of $\mathcal{C}_k$, $\mathcal{L}_k$ and $\mathcal{RL}_k$. In particular, using the trivial inclusions as the map f, one obtains $\mathcal{IL}_k \Rightarrow \mathcal{L}_k \Rightarrow \mathcal{RL}_k$ and $\mathcal{SC}_k \Rightarrow \mathcal{C}_k$. It is also known that $\mathcal{IL}_k$ and $\mathcal{SC}_k$ are equivalent. Thus, $\mathcal{SC}_k \Rightarrow \mathcal{L}_k$.

5 MDDH Problems of the Same Size and Randomness

We now focus on the case $e = d$, that is, the two MDDH problems have the same (minimal) number of parameters. From Corollary 1 this is the only case in which two MDDH problems can be equivalent by generic black-box reductions. Notice that $e = d$ implies that any injective polynomial map $f : \mathbb{Z}_q^{d+k+1} \to \mathbb{Z}_q^{d+k+1}$ of degree one is indeed a bijection, and its inverse map g is also a polynomial map of degree one. Therefore, if there exists a generic black-box reduction from the $\mathcal{D}_k^{\mathbf{A}}$-MDDH problem to the $\mathcal{D}_k^{\mathbf{B}}$-MDDH problem then there exists a bijective polynomial map $f : \mathbb{Z}_q^{d+k+1} \to \mathbb{Z}_q^{d+k+1}$ (of degree one) such that $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ for $\lambda \in \mathbb{Z}_q^{\times}$, which also implies $\lambda^{-1}\mathfrak{d}_{\mathbf{B}} = \mathfrak{d}_{\mathbf{A}} \circ g$, where g is the inverse of f. As a consequence of the previous results, this shows the existence of a generic black-box reduction in the opposite way (observe that we are in the case g is bijective). In summary, we conclude that either the two problems are equivalent or they are incomparable via generic black-box reductions.

Theorem 6. *Let $\mathcal{D}_k^{\mathbf{A}}$ and $\mathcal{D}_k^{\mathbf{B}}$ be hard polynomial degree one matrix distributions, both with d parameters. Then either $\mathcal{D}_k^{\mathbf{A}}$-MDDH and $\mathcal{D}_k^{\mathbf{B}}$-MDDH are equivalent or they are incomparable, by generic black-box reductions.*

This result suggests the possibility of classifying all MDDH problems of the same size and number of parameters into equivalence classes. In particular, we can consider the following positive consequences of the previous theorems.

Corollary 2. *Let $\mathcal{D}_k^{\mathbf{A}}$ and $\mathcal{D}_k^{\mathbf{B}}$ be hard polynomial matrix distributions of degree one. If $\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}}$ then $\mathcal{D}_k^{\mathbf{A}}$-MDDH and $\mathcal{D}_k^{\mathbf{B}}$-MDDH are equivalent.*

Proof. The identity map is a particular bijective degree one polynomial map f, and we just need to apply Theorem 5. □

This means that the determinant polynomials hold enough information about the MDDH problems to decide their equivalence. However, $\mathfrak{d}_{\mathbf{A}} \neq \mathfrak{d}_{\mathbf{B}}$ does not mean the separation of the MDDH problems. The following result using the polynomial vector spaces is more complete, since $\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}}$ implies $X_{\mathbf{A}} = X_{\mathbf{B}}$, but the converse is not true in general.

Corollary 3. *Let $\mathcal{D}_k^{\mathbf{A}}$ and $\mathcal{D}_k^{\mathbf{B}}$ be hard polynomial matrix distributions of degree one. If the polynomial vector spaces $X_{\mathbf{A}}$ and $X_{\mathbf{B}}$ are equal, then $\mathcal{D}_k^{\mathbf{A}}$-MDDH and $\mathcal{D}_k^{\mathbf{B}}$-MDDH are equivalent.*

Proof. The equality of the two vector spaces implies the existence of an invertible matrix $M \in \mathbb{Z}_q^{d\times d}$ such that $\mathfrak{d}_{\mathbf{A},i} = \sum_{j=1}^{d} m_{i,j}\mathfrak{d}_{\mathbf{B},j}$. Then

$$\begin{aligned}\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t},\boldsymbol{z}) = \sum_{i=1}^{d}\mathfrak{d}_{\mathbf{A},i}(\boldsymbol{t})z_i = \sum_{i=1}^{d}\sum_{j=1}^{d}\mathfrak{d}_{\mathbf{B},j}(\boldsymbol{t})z_i m_{i,j} =\\ = \sum_{j=1}^{d}\mathfrak{d}_{\mathbf{B},j}(\boldsymbol{t})\sum_{i=1}^{d} z_i m_{i,j} = \mathfrak{d}_{\mathbf{B}}(\boldsymbol{t}, M^{\top}\boldsymbol{z})\end{aligned}$$

and finally $\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ for $f(\boldsymbol{t},\boldsymbol{z}) = (\boldsymbol{t}, M^{\top}\boldsymbol{z})$, which is a bijective polynomial map of degree one. □

As pointed out in previous section, for $d = 1$ there is a unique choice for the vector space $X_{\mathbf{A}}$. Thus, there exists a unique hard one-parameter polynomial matrix distribution of degree one, up to equivalence of the corresponding MDDH problems, which is the symmetric cascade distribution $\mathcal{SC}_k$.

The story does not end here, as still equivalent MDDH problems could have different vector spaces, $X_{\mathbf{A}} \neq X_{\mathbf{B}}$. We failed to provide a simple and efficient way to show the equivalence of two MDDH problems in the general case. Although we managed to notably simplify the set of possible reductions between MDDH problems, it is still hard taking into account all possible bijective polynomial maps f fulfiling the equation $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$, specially for large k and d, or for large problem subfamilies. Observe that some maps f transform only the z_i (as in the last corollary), or only the t_i, or they can mix both types of variables, as in the following toy example. Consider the self-reduction of $\mathcal{C}_2$-MDDH induced by the map $f(a_1, a_2, z_1, z_2, z_3) = (a_1, z_3, z_1, z_2, a_2)$, that exchanges the second parameter a_2 and z_3. It solves the equation $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{A}} \circ f$ for $\lambda = 1$, due to the symmetry of $\mathfrak{d}_{\mathbf{A}}$. Namely, $\mathfrak{d}_{\mathbf{A}}(a_1, a_2, z_1, z_2, z_3) = a_1a_2z_3 - a_1z_2 + z_1$, and a_2 and z_3 only appear in one of the monomials. A similar construction could be used to show a reduction between two more complex but differently looking MDDH problems. At this point, we can consider the complementary approach of proving separations between (families of) MDDH problems.

5.1 Invariants, Singularities and Separations

When the goal is obtaining a separation between two MDDH problems, one has to rule out the existence of any map f satisfying the equation $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$. Trying to show the nonexistence of solutions directly form the equation is not an impossible task for well-structured determinant polynomials, but it takes a lot of computations and one have to deal with many unknowns (in principle, the description of f requires $(k+1+d)(k+2+d)$ unknowns).

However, we can consider the following simple example with $k = 3$ and $d = 2$, for two variants of $\mathcal{C}_3$, one $\mathbf{A}$ with parameters (a_1, a_2, a_2) and the other $\mathbf{B}$ with parameters (b_1, b_1, b_2),

$$\mathbf{A}(a_1, a_2) = \begin{pmatrix} a_1 & 0 & 0 \\ 1 & a_1 & 0 \\ 0 & 1 & a_2 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{B}(b_1, b_2) = \begin{pmatrix} b_1 & 0 & 0 \\ 1 & b_2 & 0 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix}$$

where $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{a}, \boldsymbol{z}) = a_1^2a_2z_4 - a_1^2z_3 + a_1z_2 - z_1$ and $\mathfrak{d}_{\mathbf{B}}(\boldsymbol{b}, \boldsymbol{u}) = b_1b_2^2u_4 - b_1b_2u_3 + b_1u_2 - u_1$. Here, $\mathfrak{d}_{\mathbf{A}}$ has only one monomial of total degree 4. Therefore if the equation $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ holds for a degree one polynomial map f, then necessarily $\lambda a_1^2a_2z_4$ comes from the terms of degree 4 of $b_1b_2^2u_4$. Since we are in a unique factorization domain, this means that b_1 can only depend on one of a_1, a_2 or z_4, and the same happens to b_2 and u_4. Actually, because of the square, b_2 can only depend on a_1 (*i.e.*, $b_2 = \beta_{20} + \beta_{21}a_1$, for some constants β_{20}, β_{21}), while we can still choose whether b_1 depends only on a_2 and u_4 depends only on z_4, or vice versa. But now, moving to the degree 3 terms, $b_1b_2^2u_4$ does not depend on z_3 and the monomial $a_1^2z_3$ can only come from $b_1b_2u_3$, and u_3 must depend (among other variables) on z_3. But then the degree of $b_1 b_2$ in a_1 must be at least 2, which contradicts what happened with the degree 4 terms. Therefore, we conclude that no such f exists, and the two MDDH problems are incomparable. This approach can be applied to obtain more general separation results, but the computations scale badly with the size and the number of parameters of the matrix distribution, and also depends heavily on the configuration of the matrix itself. Thus, we look for a different strategy.

Another natural way separate two MDDH problems is looking for some easy to compute invariants associated to the determinant polynomial (or to other mathematical objects related to it), where 'invariant' means here a quantity that is preserved by all bijective polynomial maps f of degree one. If the invariant takes different values for two MDDH problems, then no such map f can exist, and both problems are incomparable. One possible candidate for invariant is the singular locus, *i.e.*, the set of points $(\boldsymbol{t}, \boldsymbol{z}) \in \mathbb{Z}_q^d \times \mathbb{Z}_q^{k+1}$ such that both $\mathfrak{d}_{\mathbf{A}}$ and its gradient $\nabla \mathfrak{d}_{\mathbf{A}}$ are zero.

Lemma 6. *Given two hard polynomial matrix distributions $\mathcal{D}_k^{\mathbf{A}}$ and $\mathcal{D}_k^{\mathbf{B}}$ of degree 1 such that there exists a bijective polynomial map f and $\lambda \neq 0$ such that $\lambda \mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$, then $V_{\mathbf{A}}$ and $V_{\mathbf{B}}$ have the same number of rational singular points.*

Proof. It is easy to see that any bijective polynomial f satisfying $\lambda \mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ maps singular points to singular points. Indeed, the map f can be written as $(\boldsymbol{s}, \boldsymbol{u}) = f(\boldsymbol{t}, \boldsymbol{z}) = f(\mathbf{0}, \mathbf{0}) + M(\boldsymbol{t} \| \boldsymbol{z})$ for an invertible matrix M. Thus, $\nabla \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \boldsymbol{z}) = \lambda^{-1} \nabla \mathfrak{d}_{\mathbf{B}}(\boldsymbol{s}, \boldsymbol{u}) \cdot M$ and $\nabla \mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \boldsymbol{z}) = 0$ if and only if $\nabla \mathfrak{d}_{\mathbf{B}}(\boldsymbol{s}, \boldsymbol{u}) = 0$. Therefore, the number of singular points of $V_{\mathbf{A}}$ and $V_{\mathbf{B}}$ must be the same. □

If $(\boldsymbol{t}, \boldsymbol{z})$ is a singular point of $\mathcal{D}_k^{\mathbf{A}}$, so is $(\boldsymbol{t}, \mathbf{0})$, and the singular points of $\mathcal{D}_k^{\mathbf{A}}$ with $\boldsymbol{z} = \mathbf{0}$ are precisely the points $(\boldsymbol{t}, \mathbf{0})$ such that $\operatorname{rank} \mathbf{A}(\boldsymbol{t}) < k$, (or simply $\boldsymbol{t} \in V_{\mathbf{A}}^{\mathrm{def}}$. Indeed, using Eq. 2 the gradient of $\mathfrak{d}_{\mathbf{A}}$ is

$$\left(\frac{\partial \mathfrak{d}_{\mathbf{A}}}{\partial t_1}, \ldots, \frac{\partial \mathfrak{d}_{\mathbf{A}}}{\partial t_d}, \mathfrak{d}_{\mathbf{A},1}, \ldots, \mathfrak{d}_{\mathbf{A},k+1} \right) \qquad \text{where} \qquad \frac{\partial \mathfrak{d}_{\mathbf{A}}}{\partial t_j}(\boldsymbol{t}, \boldsymbol{z}) = \sum_{i=1}^{k+1} \frac{\partial \mathfrak{d}_{\mathbf{A},i}}{\partial t_j}(\boldsymbol{t}) z_i$$

Then, the first d components of the gradient at a point $(\boldsymbol{t}, \mathbf{0})$ are necessarily zero, and $(\boldsymbol{t}, \mathbf{0})$ is singular if and only if $\mathfrak{d}_{\mathbf{A},i}(\boldsymbol{t}) = 0$ for $i = 1, \ldots, k+1$, since this implies that $\nabla \mathfrak{d}_{\mathbf{A}} = \mathbf{0}$ and it always holds that $\mathfrak{d}_{\mathbf{A}}(\boldsymbol{t}, \mathbf{0}) = 0$. This also shows that if $(\boldsymbol{t}, \boldsymbol{z})$ is singular, then so is $(\boldsymbol{t}, \mathbf{0})$. Moreover, the polynomials $\mathfrak{d}_{\mathbf{A},i}$ are by construction the k-minors of $\mathbf{A}$, and then the above means that $(\boldsymbol{t}, \mathbf{0})$ is singular if and only if $\operatorname{rank} \mathbf{A}(\boldsymbol{t}) < k$, or equivalently $\boldsymbol{t} \in V_{\mathbf{A}}^{\mathrm{def}}$. This allows us to prove the separation between the cascade and the linear MDDH problems.

Theorem 7. *There is no generic black-box reduction between the $\mathcal{C}_k$-MDDH and $\mathcal{L}_k$-MDDH problems (in either way), for any $k \geq 2$.*

Proof. According to Lemma 6, to prove the theorem it is enough showing that $V_{\mathcal{C}_k}$ has no singular points, while $V_{\mathcal{L}_k}$ has. Indeed, $V_{\mathcal{C}_k}^{\mathrm{def}} = \emptyset$, since $\operatorname{rank} \mathbf{A}(\boldsymbol{t}) = k$ for all $\boldsymbol{t} \in \mathbb{Z}_q^k$. Thus, $V_{\mathcal{C}_k}$ has no singular points. However, for $\mathcal{L}_k$, $\operatorname{rank} \mathbf{A}(\boldsymbol{t}) < k$ whenever two or more t_i are zero, which happens for all $k \geq 2$. □

The singular locus is a too coarse invariant, as there are many non-equivalent polynomial matrix distributions without singular points. Another interesting invariant is the group of "automorphisms" of the matrix distribution, that is the group $\mathrm{Aut}_{\mathbf{A}}$ of the bijective polynomial maps f such that $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{A}} \circ f$ for some nonzero constant λ. These maps actually correspond to the black-box generic self-reductions of the $\mathcal{D}_k^{\mathbf{A}}$-$\mathsf{MDDH}$ problem.

Lemma 7. *Given two hard polynomial matrix distributions $\mathcal{D}_k^{\mathbf{A}}$ and $\mathcal{D}_k^{\mathbf{B}}$ of degree 1 such that there exists a bijective polynomial map f and a nonzero constant λ such that $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$, then the groups $\mathrm{Aut}_{\mathbf{A}}$ and $\mathrm{Aut}_{\mathbf{B}}$ are isomorphic.*

Proof. As usually for this type of statement, we show that for any map $g_{\mathbf{A}} \in \mathrm{Aut}_{\mathbf{A}}$, the conjugate $g_{\mathbf{B}} = f \circ g_{\mathbf{A}} \circ f^{-1}$ is in $\mathrm{Aut}_{\mathbf{B}}$. Firstly, it is clear that $g_{\mathbf{B}}$ is a bijective polynomial map, because f and $g_{\mathbf{A}}$ are. In addition, using now $\mu\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{A}} \circ g_{\mathbf{A}}$ for certain nonzero constant μ, $\mathfrak{d}_{\mathbf{B}} \circ g_{\mathbf{B}} = \mathfrak{d}_{\mathbf{B}} \circ f \circ g_{\mathbf{A}} \circ f^{-1} = \lambda\mathfrak{d}_{\mathbf{A}} \circ g_{\mathbf{A}} \circ f^{-1} = \mu\lambda\mathfrak{d}_{\mathbf{A}} \circ f^{-1} = \mu\mathfrak{d}_{\mathbf{B}} \circ f \circ f^{-1} = \mu\mathfrak{d}_{\mathbf{B}}$ Similarly, f^{-1} transforms $g_{\mathbf{B}} \in \mathrm{Aut}_{\mathbf{B}}$ into $g_{\mathbf{A}} = f^{-1} \circ g_{\mathbf{B}} \circ f \in \mathrm{Aut}_{\mathbf{A}}$. □

Now we can use this invariant to separate MDDH problems with no singular points. Computing the whole group $\mathrm{Aut}_{\mathbf{A}}$ is in general a complex task, but for our purposes we only need to find a difference between $\mathrm{Aut}_{\mathbf{A}}$ and $\mathrm{Aut}_{\mathbf{B}}$ that prevents the isomorphism. For instance, two isomorphic groups have the same number of elements of order two, or they have to be either both abelian or both nonabelian, etcetera. Unfortunately, we could not find examples of matrix distributions such that showing that the automorphism groups are non isomorphic is easier than proving that the equation $\lambda\mathfrak{d}_{\mathbf{A}} = \mathfrak{d}_{\mathbf{B}} \circ f$ has no solutions.

Acknowledgments

The author is very thankful to Carla Ràfols, Gottfried Herold and Eike Kiltz, for the insightful discussions about the subject. In fact, the core of this paper were developed during a fruiful stage at HGI Bochum. He is also thankful to some of the anonymous referees for their valuable remarks.

References

1. M. Abdalla, F. Benhamouda, and D. Pointcheval. Disjunctions for hash proof systems: New constructions and applications. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 69–100, Sofia, Bulgaria, Apr. 26–30, 2015. Springer, Heidelberg, Germany.
2. N. Attrapadung. Dual system encryption framework in prime-order groups via computational pair encodings. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 591–623, Hanoi, Vietnam, Dec. 4–8, 2016. Springer, Heidelberg, Germany.
3. C. Bader, D. Hofheinz, T. Jager, E. Kiltz, and Y. Li. Tightly-secure authenticated key exchange. In Y. Dodis and J. B. Nielsen, editors, *TCC 2015, Part I*, volume 9014 of *LNCS*, pages 629–658, Warsaw, Poland, Mar. 23–25, 2015. Springer, Heidelberg, Germany.

4. G. Barthe, E. Fagerholm, D. Fiore, J. C. Mitchell, A. Scedrov, and B. Schmidt. Automated analysis of cryptographic assumptions in generic group models. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 95–112, Santa Barbara, CA, USA, Aug. 17–21, 2014. Springer, Heidelberg, Germany.
5. F. Benhamouda, G. Couteau, D. Pointcheval, and H. Wee. Implicit zero-knowledge arguments and applications to the malicious setting. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 107–129, Santa Barbara, CA, USA, Aug. 16–20, 2015. Springer, Heidelberg, Germany.
6. O. Blazy, S. A. Kakvi, E. Kiltz, and J. Pan. Tightly-secure signatures from chameleon hash functions. In J. Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 256–279, Gaithersburg, MD, USA, Mar. 30 – Apr. 1, 2015. Springer, Heidelberg, Germany.
7. O. Blazy, E. Kiltz, and J. Pan. (Hierarchical) identity-based encryption from affine message authentication. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 408–425, Santa Barbara, CA, USA, Aug. 17–21, 2014. Springer, Heidelberg, Germany.
8. J. Chen, R. Gay, and H. Wee. Improved dual system ABE in prime-order groups via predicate encodings. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 595–624, Sofia, Bulgaria, Apr. 26–30, 2015. Springer, Heidelberg, Germany.
9. 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, Heidelberg, Germany.
10. A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie-Hellman assumptions. Cryptology ePrint Archive, Report 2013/377, 2013. `http://eprint.iacr.org/2013/377` (full version of [9]).
11. G. Herold. Applications of classical algebraic geometry to cryptography. *PhD Thesis, Ruhr-Universität Bochum*, 2014.
12. G. Herold, J. Hesse, D. Hofheinz, C. Ràfols, and A. Rupp. Polynomial spaces: A new framework for composite-to-prime-order transformations. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 261–279, Santa Barbara, CA, USA, Aug. 17–21, 2014. Springer, Heidelberg, Germany.
13. E. Kiltz and H. Wee. Quasi-adaptive NIZK for linear subspaces revisited. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128, Sofia, Bulgaria, Apr. 26–30, 2015. Springer, Heidelberg, Germany.
14. U. Maurer. Abstract models of computation in cryptography. In N. Smart, editor, *Cryptography and Coding*, volume 3796 of *Lecture Notes in Computer Science*, pages 1–12. Springer Berlin Heidelberg, 2005.
15. P. Morillo, C. Ràfols, and J. L. Villar. Matrix computational assumptions in multilinear groups. Cryptology ePrint Archive, Report 2015/353, 2015. `http://eprint.iacr.org/2015/353`.
16. 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, Heidelberg, Germany.
17. J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.