An Algebraic Framework for Diffie-Hellman Assumptions

Alex Escala[1], Gottfried Herold[2], Eike Kiltz[⋆2], Carla Ràfols[2], and Jorge Villar[⋆⋆3]

[1] Universitat Autònoma de Barcelona, Spain
[2] Horst-Görtz Institute for IT Security and Faculty of Mathematics, Ruhr-Universität Bochum, Germany
[3] Universitat Politècnica de Catalunya, Spain

Abstract. We put forward a new algebraic framework to generalize and analyze Diffie-Hellman like Decisional Assumptions which allows us to argue about security and applications by considering only algebraic properties. Our $\mathcal{D}_{\ell,k}$-MDDH assumption states that it is hard to decide whether a vector in $\mathbb{G}^\ell$ is linearly dependent of the columns of some matrix in $\mathbb{G}^{\ell\times k}$ sampled according to distribution $\mathcal{D}_{\ell,k}$. It covers known assumptions such as DDH, 2-Lin (linear assumption), and k-Lin (the k-linear assumption). Using our algebraic viewpoint, we can relate the generic hardness of our assumptions in m-linear groups to the irreducibility of certain polynomials which describe the output of $\mathcal{D}_{\ell,k}$. We use the hardness results to find new distributions for which the $\mathcal{D}_{\ell,k}$-MDDH-Assumption holds generically in m-linear groups. In particular, our new assumptions 2-SCasc and 2-ILin are generically hard in bilinear groups and, compared to 2-Lin, have shorter description size, which is a relevant parameter for efficiency in many applications. These results support using our new assumptions as natural replacements for the 2-Lin Assumption which was already used in a large number of applications.

To illustrate the conceptual advantages of our algebraic framework, we construct several fundamental primitives based on any MDDH-Assumption. In particular, we can give many instantiations of a primitive in a compact way, including public-key encryption, hash-proof systems, pseudorandom functions, and Groth-Sahai NIZK and NIWI proofs. As an independent contribution we give more efficient NIZK and NIWI proofs for membership in a subgroup of $\mathbb{G}^\ell$, for validity of ciphertexts and for equality of plaintexts. The results imply very significant efficiency improvements for a large number of schemes, most notably Naor-Yung type of constructions.

Keywords: Diffie-Hellman Assumption, Groth-Sahai proofs, hash proof systems, public-key encryption.

[⋆] Funded by a Sofja Kovalevskaja Award of the Alexander von Humboldt Foundation and the German Federal Ministry for Education and Research.

[⋆⋆] Partially supported by the Spanish Government through projects MTM2009-07694 and Consolider Ingenio 2010 CDS2007-00004 ARES.

1 Introduction

Arguably, one of the most important cryptographic hardness assumptions is the Decisional Diffie-Hellman (DDH) Assumption. For a fixed additive group $\mathbb{G}$ of prime order q and a generator $\mathcal{P}$ of $\mathbb{G}$, we denote by $[a] := a\mathcal{P} \in \mathbb{G}$ the *implicit representation* of an element $a \in \mathbb{Z}_q$. The DDH Assumption states that $([a],[r],[ar]) \approx_c ([a],[r],[z]) \in \mathbb{G}^3$, where a, r, z are uniform elements in $\mathbb{Z}_q$ and $\approx_c$ denotes computationally indistinguishability of the two distributions. It has been used in numerous important applications such as secure encryption [8], key-exchange [16], hash-proof systems [9], pseudo-random functions [26], and many more.

Bilinear Groups and the Linear Assumption. Bilinear groups (i.e., groups $\mathbb{G}, \mathbb{G}_T$ of prime order q equipped with a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$) [20,3] revolutionized cryptography in recent years and and are the basis for a large number of cryptographic protocols. However, relative to a (symmetric) bilinear map, the DDH Assumption is no longer true in the group $\mathbb{G}$. (This is since $e([a],[r]) = e([1],[ar])$ and hence $[ar]$ is not longer pseudorandom given $[a]$ and $[r]$.) The need for an "alternative" decisional assumption in $\mathbb{G}$ was quickly addressed with the Linear Assumption (2-Lin) introduced by Boneh, Boyen, and Shacham [2]. It states that $([a_1],[a_2],[a_1r_1],[a_2r_2],[r_1+r_2]) \approx_c ([a_1],[a_2],[a_1r_1],[a_2r_2],[z]) \in \mathbb{G}^5$, where $a_1, a_2, r_1, r_2, z \leftarrow \mathbb{Z}_q$. 2-$\mathsf{Lin}$ holds in generic bilinear groups [2] and it has virtually become the standard decisional assumption in the group $\mathbb{G}$ in the bilinear setting. It has found applications to encryption [23], signatures [2], zero-knowledge proofs [17], pseudorandom functions [4] and many more. More recently, the 2-Lin Assumption was generalized to the $(k\text{-}\mathsf{Lin})_{k\in\mathbb{N}}$ Assumption family [19,29] (1-Lin = DDH), a family of increasingly (strictly) weaker Assumptions which are generically hard in k-linear maps.

Subgroup membership problems. Since the work of Cramer and Shoup [9] it has been recognized that it is useful to view the DDH Assumption as a hard subgroup membership problem in $\mathbb{G}^2$. In this formulation, the DDH Assumption states that it is hard to decide whether a given element $([r],[t]) \in \mathbb{G}^2$ is contained in the subgroup generated by $([1],[a])$. Similarly, in this language the 2-Lin Assumption says that it is hard to decide whether a given vector $([r],[s],[t]) \in \mathbb{G}^3$ is in the subgroup generated by the vectors $([a_1],[0],[1]),([0],[a_2],[1])$. The same holds for the $(k\text{-}\mathsf{Lin})_{k\in\mathbb{N}}$ Assumption family: for each k, the k-Lin assumption can be naturally written as a hard subgroup membership problem in $\mathbb{G}^{k+1}$. This alternative formulation has conceptual advantages for some applications, for instance, it allowed to provide more instantiations of the original DDH-based scheme of Cramer and Shoup and it is also the most natural point of view for translating schemes originally constructed in composite order groups into prime order groups [14].

Linear Algebra in Bilinear Groups. In its formulation as subgroup decision membership problem, the k-Lin assumption can be seen as the problem of deciding linear dependence "in the exponent." Recently, a number of works have illustrated the usefulness of a more algebraic point of view on decisional assumptions in bilinear groups, like the Dual Pairing Vector Spaces of Okamoto and Takashima [28] or the Subspace Assumption of Lewko [24]. Although these new decisional assumptions reduce to the 2-Lin Assumption, their flexibility and their algebraic description have proven to be crucial in many works to obtain complex primitives in strong security models previously unrealized in the literature, like Attribute-Based Encryption, Unbounded Inner Product Encryption and many more.

This work. Motivated by the success of this algebraic viewpoint of decisional assumptions, in this paper we explore new insights resulting from interpreting the k-Lin decisional assumption as a special case of what we call a Matrix Diffie-Hellman Assumption. The general problem states that it is hard to distinguish whether a given vector in $\mathbb{G}^\ell$ is contained in the space spanned by the columns of a certain matrix $[\mathbf{A}] \in \mathbb{G}^{\ell \times k}$, where $\mathbf{A}$ is sampled according to some distribution $\mathcal{D}_{\ell,k}$. We remark that even though all our results are stated in symmetric bilinear groups, they can be naturally extended to the asymmetric setting.

1.1 The Matrix Diffie-Hellman Assumption

A new framework for DDH-like Assumptions. For integers $\ell > k$ let $\mathcal{D}_{\ell,k}$ be an (efficiently samplable) distribution over $\mathbb{Z}_q^{\ell \times k}$. We define the $\mathcal{D}_{\ell,k}$-Matrix DH ($\mathcal{D}_{\ell,k}$-MDDH) Assumption as the following subgroup decision assumption:

$$\mathcal{D}_{\ell,k}\text{-}\mathsf{MDDH}: \quad [\mathbf{A}||\mathbf{A}\boldsymbol{r}] \approx_c [\mathbf{A}||\boldsymbol{u}] \in \mathbb{G}^{\ell \times (k+1)}, \tag{1}$$

where $\mathbf{A} \in \mathbb{Z}_q^{\ell \times k}$ is chosen from distribution $\mathcal{D}_{\ell,k}$, $\boldsymbol{r} \leftarrow \mathbb{Z}_q^k$, and $\boldsymbol{u} \leftarrow \mathbb{G}^\ell$. The $(k\text{-}\mathsf{Lin})_{k \in \mathbb{N}}$ family corresponds to this problem when $\ell = k+1$, and $\mathcal{D}_{\ell,k}$ is the specific distribution $\mathcal{L}_k$ (formally defined in Example 2).

Generic hardness. Due to its linearity properties, the $\mathcal{D}_{\ell,k}$-MDDH Assumption does not hold in $k+1$-linear groups. In Section 3.2 we give two different theorems which state sufficient conditions for the $\mathcal{D}_{\ell,k}$-MDDH Assumption to hold generically in m-linear groups. Theorem 1 is very similar to the Uber-Assumption [1,6] that characterizes hardness in bilinear groups (i.e., $m = 2$) in terms of linear independence of polynomials in the inputs. We generalize this to arbitrary m using a more algebraic language. This algebraic formulation has the advantage that one can use additional tools (e.g. Gröbner bases or resultants) to show that a distribution $\mathcal{D}_{\ell,k}$ meets the conditions of Theorem 1, which is specially important for large m. It also allows to prove a completely new result, namely Theorem 2, which states that a matrix assumption with $\ell = k+1$ is generically hard if a certain determinant polynomial is irreducible.

New Assumptions for bilinear groups. We propose other families of generically hard decisional assumptions that did not previously appear in the literature, e.g., those associated to $\mathcal{C}_k, \mathcal{SC}_k, \mathcal{IL}_k$ defined below. For the most important parameters $k = 2$ and $\ell = k+1 = 3$, we consider the following examples of distributions:

$$\mathcal{C}_2 : \mathbf{A} = \begin{pmatrix} a_1 & 0 \\ 1 & a_2 \\ 0 & 1 \end{pmatrix} \; \mathcal{SC}_2 : \mathbf{A} = \begin{pmatrix} a & 0 \\ 1 & a \\ 0 & 1 \end{pmatrix} \; \mathcal{L}_2 : \mathbf{A} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} \; \mathcal{IL}_2 : \mathbf{A} = \begin{pmatrix} a & 0 \\ 0 & a+1 \\ 1 & 1 \end{pmatrix},$$

for uniform $a, a_1, a_2 \in \mathbb{Z}_q$ as well as $\mathcal{U}_{3,2}$, the uniform distribution in $\mathbb{Z}_q^{3\times 2}$ (already considered in several previous works like [15]). All assumptions are hard in generic bilinear groups. It is easy to verify that $\mathcal{L}_2$-MDDH = 2-Lin. We define 2-Casc := $\mathcal{C}_2$-MDDH (Cascade Assumption), 2-SCasc := $\mathcal{SC}_2$-MDDH (Symmetric Cascade Assumption), and 2-ILin := $\mathcal{IL}_2$-MDDH (Incremental Linear Assumption). In the full version [12], we show that 2-SCasc $\Rightarrow$ 2-Casc, 2-ILin $\Rightarrow$ 2-Lin and that $\mathcal{U}_{3,2}$-MDDH is the weakest of these assumptions (which extends the results of [15,30,14] for 2-Lin), while 2-SCasc and 2-Casc seem incomparable to 2-Lin.

Efficiency improvements. As a measure of efficiency, we define the *representation size* $\mathsf{RE}_{\mathbb{G}}(\mathcal{D}_{\ell,k})$ of an $\mathcal{D}_{\ell,k}$-MDDH assumption as the minimal number of group elements needed to represent $[\mathbf{A}]$ for any $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$. This parameter is important since it affects the performance (typically the size of public/secret parameters) of schemes based on a Matrix Diffie-Hellman Assumption. 2-Lin and 2-Casc have representation size 2 (elements $([a_1],[a_2])$), while 2-ILin and 2-SCasc only 1 (element $[a]$). Hence our new assumptions directly translate into shorter parameters for a large number of applications (see the Applications in Section 4). Further, our result points out a tradeoff between efficiency and hardness which questions the role of 2-Lin as the "standard decisional assumption" over a bilinear group $\mathbb{G}$.

New Families of Weaker Assumptions. By defining appropriate distributions $\mathcal{C}_k$, $\mathcal{SC}_k$, $\mathcal{IL}_k$ over $\mathbb{Z}_q^{(k+1)\times k}$, one can generalize all three new assumptions naturally to $(k\text{-}\mathsf{Casc})_{k\in\mathbb{N}}$, $(k\text{-}\mathsf{SCasc})_{k\in\mathbb{N}}$, and $(k\text{-}\mathsf{ILin})_{k\in\mathbb{N}}$ with representation size k, 1, and 1, respectively. Using our results on generic hardness, it is easy to verify that all three assumptions are generically hard in k-linear groups. Since they are false in $k+1$-linear groups this gives us three new families of increasingly strictly weaker assumptions. In particular, the (k-SCasc) and (k-ILin) assumption families are of great interest due to their compact representation size of only 1 element.

Relations to Other Standard Assumptions. Surprisingly, the new assumption families can also be related to standard assumptions. The k-Casc Assumption is implied by the $(k+1)$-Party Diffie-Hellman Assumption ($(k+1)$-PDDH) [5] which states that $([a_1],\ldots,[a_{k+1}],[a_1\cdot\ldots\cdot a_{k+1}]) \approx_c ([a_1],\ldots,[a_{k+1}],[z]) \in \mathbb{G}^{k+2}$. Similarly, k-SCasc is implied by the $k+1$-Exponent Diffie-Hellman Assumption ($(k+1)$-EDDH) [22] which states that $([a],[a^{k+1}]) \approx_c ([a],[z]) \in \mathbb{G}^2$.

1.2 Basic Applications

We believe that all schemes based on 2-Lin can be shown to work for any Matrix Assumption. Consequently, a large class of known schemes can be instantiated more efficiently with the new more compact decisional assumptions, while offering the same generic security guarantees. To support this belief, in Section 4 we show how to construct some fundamental primitives based on any Matrix Assumption. All constructions are purely algebraic and therefore very easy to understand and prove.

- **Public-key Encryption.** We build a key-encapsulation mechanism with security against passive adversaries from any $\mathcal{D}_{\ell,k}$-MDDH Assumption. The public-key is $[\mathbf{A}]$, the ciphertext consists of the first k elements of $[z] = [\mathbf{A}\boldsymbol{r}]$, the symmetric key of the last $\ell - k$ elements of $[z]$. Passive security immediately follows from $\mathcal{D}_{\ell,k}$-MDDH.
- **Hash Proof Systems.** We build a smooth projective hash proof system (HPS) from any $\mathcal{D}_{\ell,k}$-MDDH Assumption. It is well-known that HPS imply chosen-ciphertext secure encryption [9], password-authenticated key-exchange, zero-knowledge proofs, and many other things.
- **Pseudo-Random Functions.** Generalizing the Naor-Reingold PRF [26,4], we build a pseudo-random function PRF from any $\mathcal{D}_{\ell,k}$-MDDH Assumption. The secret-key consists of *transformation matrices* $\mathbf{T}_1, \ldots, \mathbf{T}_n$ (derived from independent instances $\mathbf{A}_{i,j} \leftarrow \mathcal{D}_{\ell,k}$) plus a vector $\boldsymbol{h}$ of group elements. For $x \in \{0,1\}^n$ we define $\mathsf{PRF}_K(x) = \left[\prod_{i:x_i=1} \mathbf{T}_i \cdot \boldsymbol{h}\right]$. Using the random self-reducibility of the $\mathcal{D}_{\ell,k}$-MDDH Assumption, we give a tight security proof.
- **Groth-Sahai Non-Interactive Zero-Knowledge Proofs.** We show how to instantiatiate the Groth-Sahai proof system [17] based on any $\mathcal{D}_{\ell,k}$-MDDH Assumption. While the size of the proofs depends only on ℓ and k, the CRS and verification depends on the representation size of the Matrix Assumptions. Therefore our new instantiations offer improved efficiency over the 2-Lin-based construction from [17]. This application in particular highlights the usefulness of the Matrix Assumption to describe in a compact way many instantiations of a scheme: instead of having to specify the constructions for the DDH and the 2-Lin assumptions separately [17], we can recover them as a special case of a general construction.

More efficient proofs for CRS dependent languages. In Section 5 we provide more efficient NIZK and NIWI proofs for concrete natural languages which are dependent on the common reference string. More specifically, the common reference string of the $\mathcal{D}_{\ell,k}$-MDDH instantiation of Groth-Sahai proofs of Section 4.4 includes as part of the commitment keys the matrix $[\mathbf{A}]$, where $\mathbf{A} \in \mathbb{Z}_q^{\ell \times k} \leftarrow \mathcal{D}_{\ell,k}$. We give more efficient proofs for several languages related to $\mathbf{A}$. Although at first glance the languages considered may seem quite restricted, they naturally appear in many applications, where typically $\mathbf{A}$ is the public key of some encryption scheme and one wants to prove statements about ciphertexts. More specifically, we obtain improvements for several kinds of statements, namely:

- **Subgroup membership proofs**. We give more efficient proofs in the language $\mathcal{L}_{\mathbf{A},\mathbb{G},\mathcal{P}} := \{[\mathbf{A}\boldsymbol{r}], \boldsymbol{r} \in \mathbb{Z}_q^k\} \subset \mathbb{G}^\ell$. To quantify some concrete improvement, in the 2-Lin case, our proofs of membership are half of the size of a standard Groth-Sahai proof and they require only 6 groups elements. We stress that this improvement is obtained without introducing any new computational assumption. To see which kind of statements can be proved using our result, note that a ciphertext is a rerandomization of another one only if their difference is in $\mathcal{L}_{\mathbf{A},\mathbb{G},\mathcal{P}}$. The same holds for proving that two commitments with the same key hide the same value or for showing in a publicly verifiable manner that the ciphertext of our encryption scheme opens to some known message $[m]$. This improvement has a significant impact on recent results, like [25,13], and we think many more examples can be found.

- **Ciphertext validity**. The result is extended to prove membership in the language $\mathcal{L}_{\mathbf{A},\boldsymbol{z},\mathbb{G},\mathcal{P}} = \{[\boldsymbol{c}] : \boldsymbol{c} = \mathbf{A}\boldsymbol{r} + m\boldsymbol{z}\} \subset \mathbb{G}^\ell$, where $\boldsymbol{z} \in \mathbb{Z}_q^\ell$ is some public vector such that $\boldsymbol{z} \notin \mathrm{Im}(\mathbf{A})$, and the witness of the statement is $(\boldsymbol{r}, [m]) \in \mathbb{Z}_q^k \times \mathbb{G}$. The natural application of this result is to prove that a ciphertext is well-formed and the prover knows the message $[m]$, like for instance in [11].
- **Plaintext equality**. We consider Groth-Sahai proofs in a setting in which the variables of the proofs are committed with different commitment keys, defined by two matrices $\mathbf{A} \leftarrow \mathcal{D}_{\ell_1,k_1}, \mathbf{B} \leftarrow \mathcal{D}'_{\ell_2,k_2}$. We give more efficient proofs of membership in the language $\mathcal{L}_{\mathbf{A},\mathbf{B},\mathbb{G},\mathcal{P}} := \{([\boldsymbol{c}_A], [\boldsymbol{c}_B]) : [\boldsymbol{c}_A] = [\mathbf{A}\boldsymbol{r} + (0, \ldots, 0, m)^T], [\boldsymbol{c}_B] = [\mathbf{B}\boldsymbol{s} + (0, \ldots, 0, m)^T], \boldsymbol{r} \in \mathbb{Z}_q^{k_1}, \boldsymbol{s} \in \mathbb{Z}_q^{k_2}\} \subset \mathbb{G}^{\ell_1} \times \mathbb{G}^{\ell_2}$. To quantify our concrete improvements, the size of the proof is reduced by 4 group elements with respect to [21]. As in the previous case, this language appears most naturally when one wants to prove equality of two committed values or plaintexts encrypted under different keys, e.g., when using Naor-Yung techniques to obtain chosen-ciphertext security [27]. Concretely, our results apply also to the encryption schemes in [18,7,10].

2 Notation

For $n \in \mathbb{N}$, we write 1^n for the string of n ones. Moreover, $|x|$ denotes the length of a bitstring x, while $|S|$ denotes the size of a set S. Further, $s \leftarrow S$ denotes the process of sampling an element s from S uniformly at random. For an algorithm A, we write $z \leftarrow \mathsf{A}(x, y, \ldots)$ to indicate that A is a (probabilistic) algorithm that outputs z on input $(x, y, \ldots)$. If $\mathbf{A}$ is a matrix we denote by a_{ij} the entries and $\boldsymbol{a}_i$ the column vectors.

Let Gen be a probabilistic polynomial time (ppt) algorithm that on input 1^λ returns a description $\mathcal{G} = (\mathbb{G}, q, \mathcal{P})$ of a cyclic group $\mathbb{G}$ of order q for a λ-bit prime q and a generator $\mathcal{P}$ of $\mathbb{G}$. More generally, for any fixed $k \geq 1$, let MGen_k be a ppt algorithm that on input 1^λ returns a description $\mathcal{MG}_k = (\mathbb{G}, \mathbb{G}_{T_k}, q, e_k, \mathcal{P})$, where $\mathbb{G}$ and $\mathbb{G}_{T_k}$ are cyclic additive groups of prime-order q, $\mathcal{P}$ a generator of $\mathbb{G}$, and $e_k : \mathbb{G}^k \rightarrow \mathbb{G}_{T_k}$ is a (non-degenerated, efficiently computable) k-linear map. For $k = 2$ we define $\mathsf{PGen} := \mathsf{MGen}_2$ to be a generator of a bilinear group $\mathcal{PG} = (\mathbb{G}, \mathbb{G}_T, q, e, \mathcal{P})$.

For an element $a \in \mathbb{Z}_q$ we define $[a] = a\mathcal{P}$ as the implicit representation of a in $\mathbb{G}$. Similarly, $[a]_{T_k} = a\mathcal{P}_{T_k}$ is its implicit representation in $\mathbb{G}_{T_k}$, where $\mathcal{P}_{T_k} = e_k(\mathcal{P}, \ldots, \mathcal{P}) \in \mathbb{G}_{T_k}$. More generally, for a matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_q^{n \times m}$ we define $[\mathbf{A}]$ and $[\mathbf{A}]_{T_k}$ as the implicit representations of $\mathbf{A}$ computed elementwise.

When talking about elements in $\mathbb{G}$ and $\mathbb{G}_{T_k}$ we will always use this implicit notation, i.e., we let $[a] \in \mathbb{G}$ be an element in $\mathbb{G}$ or $[b]_{T_k}$ be an element in $\mathbb{G}_{T_k}$. Note that from $[a] \in \mathbb{G}$ it is generally hard to compute the value a (discrete logarithm problem in $\mathbb{G}$). Further, from $[b]_{T_k} \in \mathbb{G}_{T_k}$ it is hard to compute the value $b \in \mathbb{Z}_q$ (discrete logarithm problem in $\mathbb{G}_{T_k}$) or the value $[b] \in \mathbb{G}$ (pairing inversion problem). Obviously, given $[a] \in \mathbb{G}$, $[b]_{T_k} \in \mathbb{G}_{T_k}$, and a scalar $x \in \mathbb{Z}_q$, one can efficiently compute $[ax] \in \mathbb{G}$ and $[bx]_{T_k} \in \mathbb{G}_{T_k}$.

Also, all functions and operations acting on $\mathbb{G}$ and $\mathbb{G}_{T_k}$ will be defined implicitly. For example, when evaluating a bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ in $[a], [b] \in \mathbb{G}$ we will use again our implicit representation and write $[z]_T := e([a], [b])$. Note that $e([a], [b]) = [ab]_T$, for all $a, b \in \mathbb{Z}_q$.

3 Matrix DH Assumptions

3.1 Definition and Basic Properties

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

For simplicity we will also assume that, wlog, the first k rows of $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$ form an invertible matrix.

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

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

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

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

Definition 3. *Let $\mathcal{D}_{\ell,k}$ be a matrix distribution. Let $\mathbf{A}_0$ be the first k rows of $\mathbf{A}$ and $\mathbf{A}_1$ be the last $\ell - k$ rows of $\mathbf{A}$. The matrix $\mathbf{T} \in \mathbb{Z}_q^{(\ell-k)\times k}$ defined as $\mathbf{T} = \mathbf{A}_1\mathbf{A}_0^{-1}$ is called the transformation matrix of $\mathbf{A}$.*

We note that using the transformation matrix, one can alternatively define the advantage from Definition 2 as

$$\mathbf{Adv}_{\mathcal{D}_{\ell,k},\mathsf{Gen}}(\mathsf{D}) = \Pr[\mathsf{D}(\mathcal{G}, \begin{bmatrix} \mathbf{A}_0 \\ \mathbf{T}\mathbf{A}_0 \end{bmatrix}, \begin{bmatrix} \boldsymbol{h} \\ \mathbf{T}\boldsymbol{h} \end{bmatrix}) = 1] - \Pr[\mathsf{D}(\mathcal{G}, \begin{bmatrix} \mathbf{A}_0 \\ \mathbf{T}\mathbf{A}_0 \end{bmatrix}, [\boldsymbol{u}]) = 1],$$

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

We can generalize Definition 2 to the m-fold $\mathcal{D}_{\ell,k}$-MDDH Assumption as follows. Given $\mathbf{W} \leftarrow \mathbb{Z}_q^{k\times m}$ for some $m \geq 1$, we consider the problem of distinguishing the distributions $([\mathbf{A}], [\mathbf{AW}])$ and $([\mathbf{A}], [\mathbf{U}])$ where $\mathbf{U} \leftarrow \mathbb{Z}_q^{\ell\times m}$ is equivalent to m independent instances of the problem (with the same $\mathbf{A}$ but different $\boldsymbol{w}_i$). This can be proved through a hybrid argument with a loss of m in the reduction, or, with a tight reduction (independent of m) via random self-reducibility.

Lemma 1 (Random self reducibility). *For any matrix distribution $\mathcal{D}_{\ell,k}$, $\mathcal{D}_{\ell,k}$-MDDH is random self-reducible. Concretely, for any m,*

$$\mathbf{Adv}^{m}_{\mathcal{D}_{\ell,k},\mathsf{Gen}}(\mathsf{D}') \leq \begin{cases} m \cdot \mathbf{Adv}_{\mathcal{D}_{\ell,k},\mathsf{Gen}}(\mathsf{D}) & 1 \leq m \leq \ell - k \\ (\ell - k) \cdot \mathbf{Adv}_{\mathcal{D}_{\ell,k},\mathsf{Gen}}(\mathsf{D}) + \dfrac{1}{q-1} & m > \ell - k \end{cases},$$

where

$$\mathbf{Adv}^{m}_{\mathcal{D}_{\ell,k},\mathsf{Gen}}(\mathsf{D}') = \Pr[\mathsf{D}'(\mathcal{G}, [\mathbf{A}], [\mathbf{AW}]) = 1] - \Pr[\mathsf{D}'(\mathcal{G}, [\mathbf{A}], [\mathbf{U}]) = 1],$$

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

The proof is given in the full version [12].

We remark that, given $[\mathbf{A}], [\boldsymbol{z}]$ the above lemma can only be used to re-randomize the value $[\boldsymbol{z}]$. In order to re-randomize the matrix $[\mathbf{A}]$ we need that one can sample matrices $\mathbf{L}$ and $\mathbf{R}$ such that $\mathbf{A}' = \mathbf{LAR}$ looks like an independent instance $\mathbf{A}' \leftarrow \mathcal{D}_{\ell,k}$. In all of our example distributions we are able to do this.

Due to its linearity properties, the $\mathcal{D}_{\ell,k}$-MDDH assumption does not hold in $(k+1)$-linear groups.

Lemma 2. *Let $\mathcal{D}_{\ell,k}$ be any matrix distribution. Then the $\mathcal{D}_{\ell,k}$-Matrix Diffie-Hellman Assumption is false in $(k+1)$-linear groups.*

This is proven in the full version [12] by computing determinants in the target group.

3.2 Generic Hardness of Matrix DH

Let $\mathcal{D}_{\ell,k}$ be a matrix distribution as in Definition 1, which outputs matrices $\mathbf{A} \in \mathbb{Z}_q^{\ell\times k}$. We call $\mathcal{D}_{\ell,k}$ *polynomial-induced* if the distribution is defined by picking $\boldsymbol{t} \in \mathbb{Z}_q^d$ uniformly at random and setting $a_{i,j} := \mathfrak{p}_{i,j}(\boldsymbol{t})$ for some polynomials $\mathfrak{p}_{i,j} \in \mathbb{Z}_q[\boldsymbol{T}]$ whose degree does not depend on λ. E.g. for 2-Lin from Section 1.1, we have $a_{1,1} = t_1, a_{2,2} = t_2, a_{2,1} = a_{3,2} = 1$ and $a_{1,2} = a_{3,1} = 0$ with t_1, t_2 (called a_1, a_2 in Section 1.1) uniform.

We set $\mathfrak{f}_{i,j} = A_{i,j} - \mathfrak{p}_{i,j}$ and $\mathfrak{g}_i = Z_i - \sum_j \mathfrak{p}_{i,j} W_j$ in the ring $\mathcal{R} = \mathbb{Z}_q[A_{1,1}, \ldots, A_{\ell,k}, \boldsymbol{Z}, \boldsymbol{T}, \boldsymbol{W}]$. Consider the ideal $\mathcal{I}_0$ generated by all $\mathfrak{f}_{i,j}$'s and $\mathfrak{g}_i$'s and the ideal $\mathcal{I}_1$ generated only by the $\mathfrak{f}_{i,j}$'s in $\mathcal{R}$. Let $\mathcal{J}_b := \mathcal{I}_b \cap \mathbb{Z}_q[A_{1,1}, \ldots, A_{\ell,k}, \boldsymbol{Z}]$. Note that the equations $\mathfrak{f}_{i,j} = 0$ just encode the definition of the matrix entry $a_{i,j}$ by $\mathfrak{p}_{i,j}(\boldsymbol{t})$ and the equation $\mathfrak{g}_i = 0$ encodes the definition of z_i in the case $\boldsymbol{z} = \mathbf{A}\boldsymbol{\omega}$. So, informally, $\mathcal{I}_0$ encodes the relations between the $a_{i,j}$'s, z_i's, t_i's and w_i's in $([\mathbf{A}], [\boldsymbol{z}] = [\mathbf{A}\boldsymbol{\omega}])$ and $\mathcal{I}_1$ encodes the relations in $([\mathbf{A}], [\boldsymbol{z}] = [\boldsymbol{u}])$. For $b = 0$ ($\boldsymbol{z} = \mathbf{A}\boldsymbol{\omega}$) and $b = 1$ ($\boldsymbol{z}$ uniform), $\mathcal{J}_b$ encodes the relations visible by considering only the given data (i.e. the $A_{i,j}$'s and Z_j's).

Theorem 1. *Let $\mathcal{D}_{\ell,k}$ be a polynomial-induced matrix distribution with notation as above. Then the $\mathcal{D}_{\ell,k}$-MDDH assumption holds in generic m-linear groups if and only if $(\mathcal{J}_0)_{\leq m} = (\mathcal{J}_1)_{\leq m}$, where the $_{\leq m}$ means restriction to total degree at most m.*

Proof. Note that $\mathcal{J}_{\leq m}$ captures precisely what any adversary can generically compute with polynomially many group and m-linear pairing operations. Formally, this is proven by restating the Uber-Assumption Theorem of [1,6] and its proof more algebraically.

For a given matrix distribution, the condition $(\mathcal{J}_0)_{\leq m} = (\mathcal{J}_1)_{\leq m}$ can be verified by direct linear algebra or by elimination theory (using e.g. Gröbner bases). For the special case $\ell = k+1$, we can actually give a criterion that is simple to verify using determinants:

Theorem 2. *Let $\mathcal{D}_k$ be a polynomial-induced matrix distribution, which outputs matrices $a_{i,j} = \mathfrak{p}_{i,j}(\boldsymbol{t})$ for uniform $\boldsymbol{t} \in \mathbb{Z}_q^d$. Let $\mathfrak{d}$ be the determinant of $(\mathfrak{p}_{i,j}(\boldsymbol{T}) \| \boldsymbol{Z})$ as a polynomial in $\boldsymbol{Z}, \boldsymbol{T}$.*

1. *If the matrices output by $\mathcal{D}_k$ always have full rank (not just with overwhelming probability), even for t_i from the algebraic closure $\overline{\mathbb{Z}_q}$, then $\mathfrak{d}$ is irreducible over $\overline{\mathbb{Z}_q}$.*
2. *If all $\mathfrak{p}_{i,j}$ have degree at most one and $\mathfrak{d}$ is irreducible over $\overline{\mathbb{Z}_q}$ and the total degree of $\mathfrak{d}$ is $k+1$, then the $\mathcal{D}_k$-MDDH assumption holds in* generic *k-linear groups.*

This theorem and generalizations for non-linear $\mathfrak{p}_{i,j}$ and non-irreducible $\mathfrak{d}$ are proven in the full version [12] using tools from algebraic geometry.

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

Let $\mathcal{D}_{\ell,k}$ be a matrix distribution and $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$. Looking ahead to our applications, $[\mathbf{A}]$ will correspond to the public-key (or common reference string) and $[\mathbf{A}\boldsymbol{w}] \in \mathbb{G}^\ell$ will correspond to a ciphertext. We define the *representation size* $\mathsf{RE}_{\mathbb{G}}(\mathcal{D}_{\ell,k})$ of a given polynomial-induced matrix distribution $\mathcal{D}_{\ell,k}$ with linear $\mathfrak{p}_{i,j}$'s as the minimal number of group elements it takes to represent $[\mathbf{A}]$ for any $\mathbf{A} \in \mathcal{D}_{\ell,k}$. We will be interested in families of distributions $\mathcal{D}_{\ell,k}$ such that that Matrix Diffie-Hellman Assumption is hard in k-linear groups. By Lemma 2 we obtain a family of strictly weaker assumptions. Our goal is to obtain such a family of assumptions with small (possibly minimal) representation.

Example 1. Let $\mathcal{U}_{\ell,k}$ be the uniform distribution over $\mathbb{Z}_q^{\ell \times k}$.

The next lemma says that $\mathcal{U}_{\ell,k}$-MDDH is the weakest possible assumption among all $\mathcal{D}_{\ell,k}$-Matrix Diffie-Hellman Assumptions. However, $\mathcal{U}_{\ell,k}$ has poor representation, i.e., $\mathsf{RE}_{\mathbb{G}}(\mathcal{U}_{\ell,k}) = \ell k$.

Lemma 3. *Let $\mathcal{D}_{\ell,k}$ be any matrix distribution. Then $\mathcal{D}_{\ell,k}$-$\mathsf{MDDH} \Rightarrow \mathcal{U}_{\ell,k}$-$\mathsf{MDDH}$.*

Proof. Given an instance $([\mathbf{A}], [\mathbf{A}\boldsymbol{w}])$ of $\mathcal{D}_{\ell,k}$, if $\mathbf{L} \in \mathbb{Z}_q^{\ell\times\ell}$ and $\mathbf{R} \in \mathbb{Z}_q^{k\times k}$ are two random invertible matrices, it is possible to get a properly distributed instance of the $\mathcal{U}_{\ell,k}$-matrix DH problem as $([\mathbf{LAR}], [\mathbf{LA}\boldsymbol{w}])$. Indeed, $\mathbf{LAR}$ has a distribution statistically close to the uniform distributionin $\mathbb{Z}_q^{k\times\ell}$, while $\mathbf{LA}\boldsymbol{w} = \mathbf{LAR}\boldsymbol{v}$ for $\boldsymbol{v} = \mathbf{R}^{-1}\boldsymbol{w}$. Clearly, $\boldsymbol{v}$ has the uniform distribution in $\mathbb{Z}_q^k$.

*Example 2 (k-Linear Assumption/k-*Lin*).* We define the distribution $\mathcal{L}_k$ as follows

$$\mathbf{A} = \begin{pmatrix} a_1 & 0 & \ldots & 0 & 0 \\ 0 & a_2 & \ldots & 0 & 0 \\ 0 & 0 & & \ddots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \ldots & 0 & a_k \\ 1 & 1 & \ldots & 1 & 1 \end{pmatrix} \in \mathbb{Z}_q^{(k+1)\times k},$$

where $a_i \leftarrow \mathbb{Z}_q^*$. The transformation matrix $\mathbf{T} \in \mathbb{Z}_q^{1\times k}$ is given as $\mathbf{T} = (\frac{1}{a_1}, \ldots, \frac{1}{a_k})$. Note that the distribution $(\mathbf{A}, \mathbf{A}\boldsymbol{w})$ can be compactly written as $(a_1, \ldots, a_k, a_1w_1, \ldots, a_kw_k, w_1 + \ldots + w_k) = (a_1, \ldots, a_k, b_1, \ldots, b_k, \frac{b_1}{a_1} + \ldots + \frac{b_k}{a_k})$ with $a_i \leftarrow \mathbb{Z}_q^*$, $b_i, w_i \leftarrow \mathbb{Z}_q$. Hence the $\mathcal{L}_k$-Matrix Diffie-Hellman Assumption is an equivalent description of the k-linear Assumption [2,19,29] with $\mathsf{RE}_{\mathbb{G}}(\mathcal{L}_k) = k$.

It was shown in [29] that k-Lin holds in the generic k-linear group model and hence k-Lin forms a family of increasingly strictly weaker assumptions. Furthermore, in [5] it was shown that 2-Lin ⇒ BDDH.

*Example 3 (k-Cascade Assumption/k-*Casc*).* We define the distribution $\mathcal{C}_k$ as follows

$$\mathbf{A} = \begin{pmatrix} a_1 & 0 & \ldots & 0 & 0 \\ 1 & a_2 & \ldots & 0 & 0 \\ 0 & 1 & \ddots & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \ldots & 1 & a_k \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix},$$

where $a_i \leftarrow \mathbb{Z}_q^*$. The transformation matrix $\mathbf{T} \in \mathbb{Z}_q^{1\times k}$ is given as $\mathbf{T} = (\pm\frac{1}{a_1\cdot\ldots\cdot a_k}, \mp\frac{1}{a_2\cdot\ldots\cdot a_k} \ldots, \frac{1}{a_k})$. Note that $(\mathbf{A}, \mathbf{A}\boldsymbol{w})$ can be compactly written as $(a_1, \ldots, a_k, a_1w_1, w_1 + a_2w_2 \ldots, w_{k-1} + a_kw_k, w_k) = (a_1, \ldots, a_k, b_1, \ldots, b_k, \frac{b_k}{a_k} - \frac{b_{k-1}}{a_{k-1}a_k} + \frac{b_{k-2}}{a_{k-2}a_{k-1}a_k} - \ldots \pm \frac{b_1}{a_1\cdot\ldots\cdot a_k})$. We have $\mathsf{RE}_{\mathbb{G}}(\mathcal{C}_k) = k$.

Matrix $\mathbf{A}$ bears resemblance to a cascade which explains the assumption's name. Indeed, in order to compute the right lower entry w_k of matrix $(\mathbf{A}, \mathbf{A}\boldsymbol{w})$ from the remaining entries, one has to "descent" the cascade to compute all the other entries w_i $(1 \leq i \leq k-1)$ one after the other.

A more compact version of $\mathcal{C}_k$ is obtained by setting all $a_i := a$.

Example 4. (Symmetric k-Cascade Assumption) We define the distribution $\mathcal{SC}_k$ as $\mathcal{C}_k$ but now $a_i = a$, where $a \leftarrow \mathbb{Z}_q^*$. Then $(\mathbf{A}, \mathbf{A}\boldsymbol{w})$ can be compactly written as $(a, aw_1, w_1{+}aw_2, \ldots, w_{k-1}{+}aw_k, w_k) = (a, b_1, \ldots, b_k, \frac{b_k}{a} - \frac{b_{k-1}}{a^2} + \frac{b_{k-2}}{a^3} - \ldots \pm \frac{b_1}{a^k})$. We have $\mathsf{RE}_{\mathbb{G}}(\mathcal{C}_k) = 1$.

Observe that the same trick cannot be applied to the k-Linear assumption k-Lin, as the resulting Symmetric k-Linear assumption does not hold in k-linear groups. However, if we set $a_i := a + i - 1$, we obtain another matrix distribution with compact representation.

Example 5. (Incremental k-Linear Assumption) We define the distribution $\mathcal{IL}_k$ as $\mathcal{L}_k$ with $a_i = a + i - 1$, for $a \leftarrow \mathbb{Z}_q$. The transformation matrix $\mathbf{T} \in \mathbb{Z}_q^{1 \times k}$ is given as $\mathbf{T} = (\frac{1}{a}, \ldots, \frac{1}{a+k-1})$. $(\mathbf{A}, \mathbf{A}\boldsymbol{w})$ can be compactly written as $(a, aw_1, (a+1)w_2, \ldots, (a+k-1)w_k, w_1 + \ldots + w_k) = (a, b_1, \ldots, b_k, \frac{b_1}{a} + \frac{b_2}{a+1} + \ldots + \frac{b_k}{a+k-1})$. We also have $\mathsf{RE}_{\mathbb{G}}(\mathcal{IL}_k) = 1$.

The last three examples need some work to prove its generic hardness.

Theorem 3. *k-Casc, k-SCasc and k-ILin are hard in generic k-linear groups.*

Proof. We need to consider the (statistically close) variants with $a_i \in \mathbb{Z}_q$ rather that $\mathbb{Z}_q^*$. The determinant polynomial for $\mathcal{C}_k$ is $\mathfrak{d}(a_1, \ldots, a_k, z_1, \ldots, z_{k+1}) = a_1 \cdots a_k z_{k+1} - a_1 \cdots a_{k-1} z_k + \ldots + (-1)^k z_1$, which has total degree $k + 1$. As all matrices in $\mathcal{C}_k$ have rank k, because the determinant of the last k rows in $\mathbf{A}$ is always 1, by Theorem 2 we conclude that k-Casc is hard in k-linear groups. As $\mathcal{SC}_k$ is a particular case of $\mathcal{C}_k$, the determinant polynomial for $\mathcal{SC}_k$ is $\mathfrak{d}(a, z_1, \ldots, z_{k+1}) = a^k z_{k+1} - a^{k-1} z_k + \ldots + (-1)^k z_1$. As before, by Theorem 2, k-SCasc is hard in k-linear groups. Finally, in the case of $\mathcal{IL}$, $\mathfrak{d}(a, z_1, \ldots, z_{k+1}) = a(a+1) \cdots (a+k-1)\big(z_{k-1} - \frac{z_1}{a} - \frac{z_2}{a+1} - \ldots - \frac{z_k}{a+k-1}\big)$, which has total degree $k + 1$. It can be shown that all matrices in $\mathcal{IL}_k$ have rank k. Indeed, matrices in $\mathcal{L}_k$ can have lower rank only if at least two parameters a_i are zero, and this cannot happen to $\mathcal{IL}_k$ matrices. Therefore, as in the previous cases, k-ILin is hard in k-linear groups.

For relations among this new security assumptions we refer the reader to the full version [12].

4 Basic Applications

Basic cryptographic definitions (key-encapsulation, hash proof systems, and pseudo-random functions) are given in the full version [12].

4.1 Public-Key Encryption

Let Gen be a group generating algorithm and $\mathcal{D}_{\ell,k}$ be a matrix distribution that outputs a matrix over $\mathbb{Z}_q^{\ell \times k}$ such that the first k-rows form an invertible matrix with overwhelming probability. We define the following key-encapsulation mechanism $\mathsf{KEM}_{\mathsf{Gen},\mathcal{D}_{\ell,k}} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with key-space $\mathcal{K} = \mathbb{G}^{\ell-k}$.

- $\mathsf{Gen}(1^\lambda)$ runs $\mathcal{G} \leftarrow \mathsf{Gen}(1^\lambda)$ and $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$. Let $\mathbf{A}_0$ be the first k rows of $\mathbf{A}$ and $\mathbf{A}_1$ be the last $\ell-k$ rows of $\mathbf{A}$. Define $\mathbf{T} \in \mathbb{Z}_q^{(\ell-k)\times k}$ as the transformation matrix $\mathbf{T} = \mathbf{A}_1\mathbf{A}_0^{-1}$. The public/secret-key is
$$pk = (\mathcal{G}, [\mathbf{A}] \in \mathbb{G}^{\ell\times k}), \quad sk = (pk, \mathbf{T} \in \mathbb{Z}_q^{(\ell-k)\times k})$$
- Enc_{pk} picks $\boldsymbol{w} \leftarrow \mathbb{Z}_q^k$. The ciphertext/key pair is
$$[\boldsymbol{c}] = [\mathbf{A}_0\boldsymbol{w}] \in \mathbb{G}^k, \quad [K] = [\mathbf{A}_1\boldsymbol{w}] \in \mathbb{G}^{\ell-k}$$
- $\mathsf{Dec}_{sk}([\boldsymbol{c}] \in \mathbb{G}^k)$ recomputes the key as $[K] = [\mathbf{T}\boldsymbol{c}] \in \mathbb{G}^{\ell-k}$.

Correctness follows by the equation $\mathbf{T} \cdot \boldsymbol{c} = \mathbf{T} \cdot \mathbf{A}_0\boldsymbol{w} = \mathbf{A}_1\boldsymbol{w}$. The public key contains $\mathsf{RE}_{\mathbb{G}}(\mathcal{D}_{\ell,k})$ and the ciphertext k group elements.

Theorem 4. *Under the $\mathcal{D}_{\ell,k}$-MDDH Assumption $\mathsf{KEM}_{\mathsf{Gen},\mathcal{D}_{\ell,k}}$ is IND-CPA secure.*

Proof. By the $\mathcal{D}_{\ell,k}$ Matrix Diffie-Hellman Assumption, the distribution of $(pk, [\boldsymbol{c}]$ $, [K]) = ((\mathcal{G}, [\mathbf{A}]), [\mathbf{A}\boldsymbol{w}])$ is computationally indistinguishable from $((\mathcal{G}, [\mathbf{A}]), [\boldsymbol{u}])$, where $\boldsymbol{u} \leftarrow \mathbb{Z}_q^\ell$.

4.2 Hash Proof System

Let $\mathcal{D}_{\ell,k}$ be a matrix distribution. We build a universal$_1$ hash proof system $\mathsf{HPS} = (\mathsf{Param}, \mathsf{Pub}, \mathsf{Priv})$, whose hard subset membership problem is based on the $\mathcal{D}_{\ell,k}$ Matrix Diffie-Hellman Assumption.

- $\mathsf{Param}(1^\lambda)$ runs $\mathcal{G} \leftarrow \mathsf{Gen}(1^\lambda)$ and picks $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$. Define
$$\mathcal{C} = \mathbb{G}^\ell, \quad \mathcal{V} = \{[\boldsymbol{c}] = [\mathbf{A}\boldsymbol{w}] \in \mathbb{G}^\ell \ : \ \boldsymbol{w} \in \mathbb{Z}_q^k\}.$$
The value $\boldsymbol{w} \in \mathbb{Z}_q^k$ is a witness of $[\boldsymbol{c}] \in \mathcal{V}$. Let $\mathcal{SK} = \mathbb{Z}_q^\ell$, $\mathcal{PK} = \mathbb{G}^k$, and $\mathcal{K} = \mathbb{G}$. For $sk = \boldsymbol{x} \in \mathbb{Z}_q^\ell$, define the projection $\mu(sk) = [\boldsymbol{x}^\top\mathbf{A}] \in \mathbb{G}^k$. For $[\boldsymbol{c}] \in \mathcal{C}$ and $sk \in \mathcal{SK}$ we define
$$\Lambda_{sk}([\boldsymbol{c}]) := [\boldsymbol{x}^\top \cdot \boldsymbol{c}] \ . \tag{2}$$
The output of Param is $params = \big(\mathcal{S} = (\mathcal{G}, [\mathbf{A}]), \mathcal{K}, \mathcal{C}, \mathcal{V}, \mathcal{PK}, \mathcal{SK}, \Lambda_{(\cdot)}(\cdot), \mu(\cdot)\big)$.
- $\mathsf{Priv}(sk, [\boldsymbol{c}])$ computes $[K] = \Lambda_{sk}([\boldsymbol{c}])$.
- $\mathsf{Pub}(pk, [\boldsymbol{c}], \boldsymbol{w})$. Given $pk = \mu(sk) = [\boldsymbol{x}^\top\mathbf{A}]$, $[\boldsymbol{c}] \in \mathcal{V}$ and a witness $\boldsymbol{w} \in \mathbb{Z}_q^k$ such that $[\boldsymbol{c}] = [\mathbf{A} \cdot \boldsymbol{w}]$ the public evaluation algorithm $\mathsf{Pub}(pk, [\boldsymbol{c}], \boldsymbol{w})$ computes $[K] = \Lambda_{sk}([\boldsymbol{c}])$ as $[K] = [(\boldsymbol{x}^\top \cdot \mathbf{A}) \cdot \boldsymbol{w}]$.

Correctness follows by (2) and the definition of μ. Clearly, under the $\mathcal{D}_{\ell,k}$-Matrix Diffie-Hellman Assumption, the subset membership problem is hard in HPS.

We now show that Λ is a universal$_1$ projective hash function. Let $[\boldsymbol{c}] \in \mathcal{C} \setminus \mathcal{V}$. Then the matrix $(\mathbf{A}||\boldsymbol{c}) \in \mathbb{Z}_q^{\ell\times(k+1)}$ is of full rank and consequently $(\boldsymbol{x}^\top \cdot \mathbf{A}||\boldsymbol{x}^\top \cdot \boldsymbol{c}) \equiv (\boldsymbol{x}^\top\mathbf{A}||u)$ for $\boldsymbol{x} \leftarrow \mathbb{Z}_q^k$ and $u \leftarrow \mathbb{Z}_q$. Hence, $(pk, \Lambda_{sk}([\boldsymbol{c}]) = ([\boldsymbol{x}^\top\mathbf{A}], [\boldsymbol{x}^\top\boldsymbol{c}]) \equiv ([\boldsymbol{x}^\top\mathbf{A}], [u]) = ([\boldsymbol{x}^\top\mathbf{A}], [K])$.

4.3 Pseudo-Random Functions

Let Gen be a group generating algorithm and $\mathcal{D}_{\ell,k}$ be a matrix distribution that outputs a matrix over $\mathbb{Z}_q^{\ell\times k}$ such that the first k-rows form an invertible matrix with overwhelming probability. We define the following pseudo-random function $\mathsf{PRF}_{\mathsf{Gen},\mathcal{D}_{\ell,k}} = (\mathsf{Gen},\mathsf{F})$ with message space $\{0,1\}^n$. For simplicity we assume that $\ell - k$ divides k.

- $\mathsf{Gen}(1^\lambda)$ runs $\mathcal{G} \leftarrow \mathsf{Gen}(1^\lambda)$, $\boldsymbol{h} \in \mathbb{Z}_q^k$, and $\mathbf{A}_{i,j} \leftarrow \mathcal{D}_{\ell,k}$ for $i = 1,\dots,n$ and $j = 1,\dots,t := k/(\ell-k)$ and computes the transformation matrices $\mathbf{T}_{i,j} \in \mathbb{Z}_q^{(\ell-k)\times k}$ of $\mathbf{A}_{i,j} \in \mathbb{Z}_q^{\ell\times k}$ (cf. Definition 3). For $i = 1,\dots,n$ define the aggregated transformation matrices
$$\mathbf{T}_i = \begin{pmatrix}\mathbf{T}_{i,1}\\ \vdots \\ \mathbf{T}_{i,t}\end{pmatrix} \in \mathbb{Z}_q^{k\times k}$$
The key is defined as $K = (\mathcal{G}, \boldsymbol{h}, \mathbf{T}_1,\dots,\mathbf{T}_n)$.
- $\mathsf{F}_K(x)$ computes
$$\mathsf{F}_K(x) = \left[\prod_{i:x_i=1} \mathbf{T}_i \cdot \boldsymbol{h}\right] \in \mathbb{G}^k.$$

We prove the following theorem in the full version [12].

Theorem 5. *Under the $\mathcal{D}_{\ell,k}$-MDDH Assumption $\mathsf{PRF}_{\mathsf{Gen},\mathcal{D}_{\ell,k}}$ is a secure pseudo-random function.*

4.4 Groth-Sahai Non-interactive Zero-Knowledge Proofs

Groth and Sahai gave a method to construct non-interactive witness-indistinguishable (NIWI) and zero-knowledge (NIZK) proofs for satisfiability of a set of equations in a bilinear group $\mathcal{PG}$. (For formal definitions of NIWI and NIZK proofs we refer to [17].) The equations in the set can be of different types, but they can be written in a unified way as

$$\sum_{j=1}^{n} f(a_j, \mathsf{y}_j) + \sum_{i=1}^{m} f(\mathsf{x}_i, b_i) + \sum_{i=1}^{m}\sum_{j=1}^{n} f(\mathsf{x}_i, \gamma_{ij}\mathsf{y}_j) = t, \tag{3}$$

where A_1, A_2, A_T are $\mathbb{Z}_q$-modules, $\mathbf{x} \in A_1^m$, $\mathbf{y} \in A_2^n$ are the variables, $\boldsymbol{a} \in A_1^n$, $\boldsymbol{b} \in A_2^m$, $\boldsymbol{\Gamma} = (\gamma_{ij}) \in \mathbb{Z}_q^{m\times n}$, $t \in A_T$ are the constants and $f : A_1 \times A_2 \to A_T$ is a bilinear map. More specifically, equations are of either one these types i) Pairing product equations, with $A_1 = A_2 = \mathbb{G}$, $A_T = \mathbb{G}_T$, $f([\mathsf{x}],[\mathsf{y}]) = [\mathsf{xy}]_T \in \mathbb{G}_T$, ii) Multi-scalar multiplication equations, with $A_1 = \mathbb{Z}_q$, $A_2 = \mathbb{G}$, $A_T = \mathbb{G}$, $f(\mathsf{x},[\mathsf{y}]) = [\mathsf{xy}] \in \mathbb{G}$ or iii) Quadratic equations in $\mathbb{Z}_q$, with $A_1 = A_2 = A_T = \mathbb{Z}_q$, $f(\mathsf{x},\mathsf{y}) = \mathsf{xy} \in \mathbb{Z}_q$.

Overview. In the GS proof system the prover gives to the verifier a commitment to each element of the witness (i.e., values of the variables that satisfy the equations) and some additional information, the proof. Commitments and proof satisfy some related set of equations computable by the verifier because of their algebraic properties. To give new instantiations we need to specify the distribution of the common reference string, which includes the commitment keys and some maps whose purpose is roughly to give some algebraic structure to the commitment space. All details are postponed to the full version [12], here we only specify how to commit to scalars $\mathsf{x} \in \mathbb{Z}_q$ to give some intuition of the results in Sections 5.1, 5.2 and 5.3.

Commitments. The commitment key $[\mathbf{U}] = ([\boldsymbol{u}_1], \ldots, [\boldsymbol{u}_{k+1}]) \in \mathbb{G}^{\ell \times (k+1)}$ is either $[\mathbf{U}] = [\mathbf{A} || \mathbf{A}\boldsymbol{w}]$ in the soundness setting (binding key) or $[\mathbf{A} || \mathbf{A}\boldsymbol{w} - \boldsymbol{z}]$ in the WI setting (hiding key), where $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, $\boldsymbol{w} \leftarrow \mathbb{Z}_q^k$, and $\boldsymbol{z} \in \mathbb{Z}_q^\ell$, $\boldsymbol{z} \notin \mathrm{Span}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ is a fixed, public vector. Clearly, the two types of commitment keys are computationally indistinguishable under the $\mathcal{D}_{\ell,k}$-MDDH Assumption. To commit to a scalar $\mathsf{x} \in \mathbb{Z}_q$ using randomness $\boldsymbol{s} \leftarrow \mathbb{Z}_q^k$ we define the maps $\iota' : \mathbb{Z}_q \to \mathbb{Z}_q^\ell$ and $p' : \mathbb{G}^\ell \to \mathbb{Z}_q$ as

$$\iota'(\mathsf{x}) = \mathsf{x} \cdot (\boldsymbol{u}_{k+1} + \boldsymbol{z}), \;\; p'([\boldsymbol{c}]) = \boldsymbol{\xi}^\top \boldsymbol{c}, \;\; \text{defining } \mathsf{com}'_{[\mathbf{U}],\boldsymbol{z}}(\mathsf{x}; \boldsymbol{s}) := [\iota'(\mathsf{x}) + \mathbf{A}\boldsymbol{s}] \in \mathbb{G}^\ell,$$

where $\boldsymbol{\xi} \in \mathbb{Z}_q^\ell$ is an arbitrary vector such that $\boldsymbol{\xi}^\top \mathbf{A} = \mathbf{0}$ and $\boldsymbol{\xi}^\top \cdot \boldsymbol{z} = 1$. On a binding key (soundness setting) we have that $p' \circ [\iota']$ is the identity map on $\mathbb{Z}_q$ and $p'([\boldsymbol{u}_i]) = 0$ for all $i = 1 \ldots k$ so the commitment is perfectly binding. On a hiding key (WI setting), $\iota'(x) \in \mathrm{Span}(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k)$ for all $x \in \mathbb{Z}_q$, which implies that the commitment is perfectly hiding. Note that, given $[\mathbf{U}]$ and x, $\iota'(\mathsf{x})$ might not be efficiently computable but $[\iota'(\mathsf{x})]$ is, which is enough to be able to compute $\mathsf{com}'(\mathsf{x}; \boldsymbol{s})$.

Efficiency. We emphasize that for $\mathcal{D}_{\ell,k} = \mathcal{L}_2$ and $\boldsymbol{z} = (0,0,1)^\top$ and for $\mathcal{D}_{\ell,k} = \mathsf{DDH}$ and $\boldsymbol{z} = (0,1)^\top$ (in the natural extension to asymmetric bilinear groups), we recover the 2-Lin and the SXDH instantiations of [17]. While the size of the proofs depends only on ℓ and k, both the size of the CRS and the cost of verification increase with $\mathsf{RE}_{\mathbb{G}}(\mathcal{D}_{\ell,k})$. In particular, in terms of efficiency, the $\mathcal{SC}_2$ Assumption is preferable to the 2-Lin Assumption.

5 More Efficient Proofs for Some CRS Dependent Languages

5.1 More Efficient Subgroup Membership Proofs

Let $[\mathbf{U}]$ be the commitment key defined in last section as part of a $\mathcal{D}_{\ell,k}$-MDDH instantiation, for some $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$. In this section we show a new technique to obtain proofs of membership in the language $\mathcal{L}_{\mathbf{A},\mathcal{PG}} := \{[\mathbf{A}\boldsymbol{r}], \boldsymbol{r} \in \mathbb{Z}_q^k\} \subset \mathbb{G}^\ell$.

Intuition. Our idea is to exploit the special algebraic structure of commitments in GS proofs, namely the observation that if $[\boldsymbol{\Phi}] = [\mathbf{A}\boldsymbol{r}] \in \mathcal{L}_{\mathbf{A},\mathcal{PG}}$ then $[\boldsymbol{\Phi}] = \mathsf{com}_{[\mathbf{U}]}(0; \boldsymbol{r})$. Therefore, to prove that $[\boldsymbol{\Phi}] \in \mathcal{L}_{\mathbf{A},\mathcal{PG}}$, we proceed as if we were giving a GS proof of satisfability of the equation $\mathsf{x} = 0$ where the randomness used for the commitment to x is $\boldsymbol{r}$. In particular, no commitments have to be given in the proof, which results in shorter proofs. To prove zero-knowledge we rewrite the equation $\mathsf{x} = 0$ as $\mathsf{x} \cdot \delta = 0$. The real proof is just a standard GS proof with the commitment to $\delta = 1$ being $\iota'(1) = \mathsf{com}_{[\mathbf{U}]}(1; \mathbf{0})$, while in the simulated proof the trapdoor allows to open $\iota'(1)$ as a commitment of 0, so we can proceed as if the equation was the trivial one $\mathsf{x} \cdot 0 = 0$, for which it is easy to give a proof of satisfiability. For the 2-Lin Assumption, our proof consists of only 6 group elements, whereas without using our technique the proof consists of 12 elements. In the full version [12] we prove the following theorem.

Theorem 6. *Let $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, where $\mathcal{D}_{\ell,k}$ is a matrix distribution. There exists a Non-Interactive Zero-Knowledge Proof for the language $\mathcal{L}_{\mathbf{A},\mathcal{PG}}$, with perfect completeness, perfect soundness and composable zero-knowledge of $k\ell$ group elements based on the $\mathcal{D}_{\ell,k}$-MDDH Assumption.*

Applications. Think of $[\mathbf{A}]$ as part of the public parameters of the hash proof system of Section 4.2. Proving that a ciphertext is well-formed is proving membership in $\mathcal{L}_{\mathbf{A},\mathcal{PG}}$. For instance, in [25] Libert and Yung combine a proof of membership in 2-Lin with a one-time signature scheme to obtain publicly verifiable ciphertexts. With our result, we reduce the size of their ciphertexts from 15 to 9 group elements. We stress that in our construction the setup of the CRS can be built on top of the encryption key so that proofs can be simulated without the decryption key, which is essential in their case. Another application is to show that two ciphertexts encrypt the same message under the same public key, a common problem in electronic voting or anonymous credentials. There are many other settings in which subgroup membership problems appear, for instance when proving that a certain ciphertext is an encryption of $[m]$.

5.2 More Efficient Proofs of Validity of Ciphertexts

The techniques of the previous section can be extended to prove the validity of a ciphertext. More specifically, given $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, and some vector $\boldsymbol{z} \in \mathbb{Z}_q^{\ell}$, $\boldsymbol{z} \notin \mathrm{Im}(\mathbf{A})$, we show how to give a more efficient proof of membership in:

$$\mathcal{L}_{\mathbf{A},\boldsymbol{z},\mathcal{PG}} = \{[\boldsymbol{c}] : \boldsymbol{c} = \mathbf{A}\boldsymbol{r} + m\boldsymbol{z}\} \subset \mathbb{G}^{\ell},$$

where $(\boldsymbol{r}, [m]) \in \mathbb{Z}_q^k \times \mathbb{G}$ is the witness.

This is also a proof of membership in the subspace of $\mathbb{G}^{\ell}$ spanned by the columns of $[\mathbf{A}]$ and the vector $[\boldsymbol{z}]$, but the techniques given in Section 5.1 do not apply. The reason is that part of the witness, $[m]$, is in the group $\mathbb{G}$ and not in $\mathbb{Z}_q$, while to compute the subgroup membership proofs as described in Section 5.1 all of the witness has to be in $\mathbb{Z}_q$. In particular, since GS are non-interactive zero-knowledge proofs of knowledge when the witnesses are group elements, the proof guarantees both that the $\boldsymbol{c}$ is well-formed and that the prover knows $[m]$.

In a typical application, $[\boldsymbol{c}]$ will be the ciphertext of some encryption scheme, in which case $\boldsymbol{r}$ will be the ciphertext randomness and $[m]$ the message. Deciding membership in this space is trivial when $\mathrm{Im}(\mathbf{A})$ and $\boldsymbol{z}$ span all of $\mathbb{Z}_q^{\ell}$, so in particular our result is meaningful when $\ell > k + 1$. In the full version [12] we prove the following theorem:

Theorem 7. *Let $\mathcal{D}_{\ell,k}$ be a matrix distribution and let $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$. There exists a Non-Interactive Zero-Knowledge Proof for the language $\mathcal{L}_{\mathbf{A},\boldsymbol{z},\mathcal{PG}}$ of $(k+2)\ell$ group elements with perfect completeness, perfect soundness and composable zero-knowledge based on the $\mathcal{D}_{\ell,k}$-MDDH Assumption.*

5.3 More Efficient Proofs of Plaintext Equality

The encryption scheme derived from the KEM given in Section 4.1 corresponds to a commitment in GS proofs. That is, if $pk_A = (\mathcal{G}, [\mathbf{A}] \in \mathbb{G}^{\ell \times k})$, for some $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, given $\boldsymbol{r} \in \mathbb{Z}_q^k$,

$$\mathsf{Enc}_{pk_A}([m]; \boldsymbol{r}) = [\boldsymbol{c}] = [\mathbf{A}\boldsymbol{r} + (0, \ldots, 0, m)^\top] = [\mathbf{A}\boldsymbol{r} + m \cdot \boldsymbol{z}] = \mathsf{com}_{[\mathbf{A}||\mathbf{A}\boldsymbol{w}]}([m]; \boldsymbol{s}),$$

where $\boldsymbol{s}^\top := (\boldsymbol{r}^\top, 0)$ and $\boldsymbol{z} := (0, \ldots, 0, 1)^\top$. Therefore, given two (potentially distinct) matrix distributions $\mathcal{D}_{\ell_1,k_1}$, $\mathcal{D}'_{\ell_2,k_2}$ and $\mathbf{A} \leftarrow \mathcal{D}_{\ell_1,k_1}, \mathbf{B} \leftarrow \mathcal{D}'_{\ell_2,k_2}$, proving equality of plaintexts of two ciphertexts encrypted under pk_A, pk_B, corresponds to proving that two commitments under different keys open to the same value. Our proof will be more efficient because we do not give any commitments as part of the proof, since the ciphertexts themselves play this role. More specifically, given $[\boldsymbol{c}_A] = \mathsf{Enc}_{pk_A}([m])$ and $[\boldsymbol{c}_B] = \mathsf{Enc}_{pk_B}([m])$ we will treat $[\boldsymbol{c}_A]$ as a commitment to the variable $[\mathsf{x}] \in A_1 = \mathbb{G}$ and $[\boldsymbol{c}_B]$ as a commitment to the variable $[\mathsf{y}] \in A_2 = \mathbb{G}$ and prove that the quadratic equation $e([\mathsf{x}], [1]) \cdot e([-1], [\mathsf{y}]) = [0]_T$ is satisfied. The zero-knowledge simulator will open $\iota_1([1])$, $\iota_2([-1])$ as commitments to the $[0]$ variable and simulate a proof for the equation $e([\mathsf{x}], [0]) \cdot e([0], [\mathsf{y}]) = [0]_T$, which is trivially satisfiable and can be simulated. More formally, let $\boldsymbol{r} \in \mathbb{Z}_q^{k_1}, \boldsymbol{s} \in \mathbb{Z}_q^{k_2}, m \in \mathbb{Z}_q$, $\boldsymbol{z}_1 \in \mathbb{Z}_q^{\ell_1}$, and $\boldsymbol{z}_1 \notin \mathrm{Im}(\mathbf{A})$ and $\boldsymbol{z}_2 \in \mathbb{Z}_q^{\ell_2}$, $\boldsymbol{z}_2 \notin \mathrm{Im}(\mathbf{B})$. Define:

$$\mathcal{L}_{\mathbf{A},\mathbf{B},\boldsymbol{z}_1,\boldsymbol{z}_2,\mathcal{PG}} := \{([\boldsymbol{c}_A], [\boldsymbol{c}_B]) : \boldsymbol{c}_A = \mathbf{A}\boldsymbol{r} + m\boldsymbol{z}_1, \boldsymbol{c}_B = \mathbf{B}\boldsymbol{s} + \boldsymbol{z}_2\} \subset \mathbb{G}^{\ell_1} \times \mathbb{G}^{\ell_2}.$$

In the full version [12] we prove:

Theorem 8. *Let $\mathcal{D}_{\ell_1,k_1}$ and $\mathcal{D}'_{\ell_2,k_2}$ be two matrix distributions and let $\mathbf{A} \leftarrow \mathcal{D}_{\ell_1,k_1}, \mathbf{B} \leftarrow \mathcal{D}'_{\ell_2,k_2}$. There exists a Non-Interactive Zero-Knowledge Proof for the language $\mathcal{L}_{\mathbf{A},\mathbf{B},\boldsymbol{z}_1,\boldsymbol{z}_2,\mathcal{PG}}$ of $\ell_1(k_2+1) + \ell_2(k_1+1)$ group elements with perfect completeness, perfect soundness and composable zero-knowledge based on the $\mathcal{D}_{\ell_1,k_1}$-MDDH and the $\mathcal{D}_{\ell_2,k_2}$-MDDH Assumption.*

Applications. In [21], we reduce the size of the proof by 4 group elements from 18 to 22, while in [18] we save 9 elements although their proof is quite inefficient altogether. We note that even if both papers give a proof that two ciphertexts under two different 2-Lin public keys correspond to the same value, the proof in [18] is more inefficient because it must use GS proofs for pairing product equations instead of multi-scalar multiplication equations. Other examples include [7,10]. We note that our approach is easily generalizable to prove more general statements about plaintexts, for instance to prove membership in $\mathcal{L}'_{\mathbf{A},\mathbf{B},\boldsymbol{z}_1,\boldsymbol{z}_2,\mathcal{PG}} := \{([\boldsymbol{c}_A], [\boldsymbol{c}_B]) : \boldsymbol{c}_A = \mathbf{A}\boldsymbol{r} + (0, \ldots, 0, m)^\top, \boldsymbol{c}_B =$

$\mathbf{B}\boldsymbol{s} + (0, \ldots, 0, 2m)^\top, \boldsymbol{r} \in \mathbb{Z}_q^{k_1}, \boldsymbol{s} \in \mathbb{Z}_q^{k_2}\} \subset \mathbb{G}^{\ell_1} \times \mathbb{G}^{\ell_2}$ or in general to show that some linear relation between a set of plaintexts encrypted under two different public-keys holds.

References

1. D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456. Springer, May 2005. 3, 9
2. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55. Springer, Aug. 2004. 2, 10
3. D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, Aug. 2001. 2
4. D. Boneh, H. W. Montgomery, and A. Raghunathan. Algebraic pseudorandom functions with improved efficiency from the augmented cascade. In E. Al-Shaer, A. D. Keromytis, and V. Shmatikov, editors, *ACM CCS 10*, pages 131–140. ACM Press, Oct. 2010. 2, 5
5. D. Boneh, A. Sahai, and B. Waters. Fully collusion resistant traitor tracing with short ciphertexts and private keys. In S. Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 573–592. Springer, May / June 2006. 4, 10
6. X. Boyen. The uber-assumption family (invited talk). In S. D. Galbraith and K. G. Paterson, editors, *PAIRING 2008*, volume 5209 of *LNCS*, pages 39–56. Springer, Sept. 2008. 3, 9
7. J. Camenisch, N. Chandran, and V. Shoup. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In A. Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 351–368. Springer, Apr. 2009. 6, 16
8. R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In H. Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 13–25. Springer, Aug. 1998. 2
9. R. Cramer and V. Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In L. R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 45–64. Springer, Apr. / May 2002. 2, 5
10. Y. Dodis, K. Haralambiev, A. López-Alt, and D. Wichs. Cryptography against continuous memory attacks. In *51st FOCS*, pages 511–520. IEEE Computer Society Press, Oct. 2010. 6, 16
11. Y. Dodis, K. Haralambiev, A. López-Alt, and D. Wichs. Efficient public-key cryptography in the presence of key leakage. In M. Abe, editor, *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 613–631. Springer, Dec. 2010. 6
12. A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for diffie-hellman assumptions. Cryptology ePrint Archive, 2013. `http://eprint.iacr.org/`. 4, 8, 9, 11, 13, 14, 15, 16
13. M. Fischlin, B. Libert, and M. Manulis. Non-interactive and re-usable universally composable string commitments with adaptive security. In D. H. Lee and X. Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 468–485. Springer, Dec. 2011. 6

14. D. M. Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 44–61. Springer, May 2010. 2, 4
15. D. Galindo, J. Herranz, and J. L. Villar. Identity-based encryption with master key-dependent message security and leakage-resilience. In S. Foresti, M. Yung, and F. Martinelli, editors, *ESORICS 2012*, volume 7459 of *LNCS*, pages 627–642. Springer, Sept. 2012. 4
16. R. Gennaro and Y. Lindell. A framework for password-based authenticated key exchange. In E. Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 524–543. Springer, May 2003. `http://eprint.iacr.org/2003/032.ps.gz`. 2
17. J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, Apr. 2008. 2, 5, 13, 14
18. D. Hofheinz and T. Jager. Tightly secure signatures and public-key encryption. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 590–607. Springer, Aug. 2012. 6, 16
19. D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. In A. Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 553–571. Springer, Aug. 2007. 2, 10
20. A. Joux. A one round protocol for tripartite Diffie-Hellman. *Journal of Cryptology*, 17(4):263–276, Sept. 2004. 2
21. J. Katz and V. Vaikuntanathan. Round-optimal password-based authenticated key exchange. In Y. Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 293–310. Springer, Mar. 2011. 6, 16
22. E. Kiltz. A tool box of cryptographic functions related to the Diffie-Hellman function. In C. P. Rangan and C. Ding, editors, *INDOCRYPT 2001*, volume 2247 of *LNCS*, pages 339–350. Springer, Dec. 2001. 4
23. E. Kiltz. Chosen-ciphertext security from tag-based encryption. In S. Halevi and T. Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 581–600. Springer, Mar. 2006. 2
24. A. B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 318–335. Springer, Apr. 2012. 3
25. B. Libert and M. Yung. Non-interactive CCA-secure threshold cryptosystems with adaptive security: New framework and constructions. In R. Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 75–93. Springer, Mar. 2012. 6, 15
26. M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudorandom functions. In *38th FOCS*, pages 458–467. IEEE Computer Society Press, Oct. 1997. 2, 5
27. M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *22nd ACM STOC*. ACM Press, May 1990. 6
28. T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208. Springer, Aug. 2010. 3
29. H. Shacham. A cramer-shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive, Report 2007/074, 2007. `http://eprint.iacr.org/`. 2, 10
30. J. L. Villar. Optimal reductions of some decisional problems to the rank problem. In X. Wang and K. Sako, editors, *ASIACRYPT*, volume 7658 of *Lecture Notes in Computer Science*, pages 80–97. Springer, 2012. 4