Polynomial Spaces: A New Framework for Composite-to-Prime-Order Transformations

Gottfried Herold[1], Julia Hesse[2], Dennis Hofheinz[2],
Carla Ràfols[1], and Andy Rupp[2]

[1] Horst Görtz Institute for IT Security and Faculty of Mathematics,
Ruhr University Bochum, Germany
{gottfried.herold,carla.rafols}@rub.de
[2] Karlsruhe Institute of Technology, Germany
{julia.hesse,dennis.hofheinz,andy.rupp}@kit.edu

Abstract. At Eurocrypt 2010, Freeman presented a framework to convert cryptosystems based on composite-order groups into ones that use prime-order groups. Such a transformation is interesting not only from a conceptual point of view, but also since for relevant parameters, operations in prime-order groups are faster than composite-order operations by an order of magnitude. Since Freeman's work, several other works have shown improvements, but also lower bounds on the efficiency of such conversions.

In this work, we present a new framework for composite-to-prime-order conversions. Our framework is in the spirit of Freeman's work; however, we develop a different, "polynomial" view of his approach, and revisit several of his design decisions. This eventually leads to significant efficiency improvements, and enables us to circumvent previous lower bounds. Specifically, we show how to verify Groth-Sahai proofs in a prime-order environment (with a symmetric pairing) almost twice as efficiently as the state of the art.

We also show that our new conversions are optimal in a very broad sense. Besides, our conversions also apply in settings with a multilinear map, and can be instantiated from a variety of computational assumptions (including, e.g., the k-linear assumption).

Keywords: bilinear maps, composite-order groups, Groth-Sahai proofs.

1 Introduction

Motivation. Cyclic groups are a very popular platform for cryptographic constructions. Starting with Diffie and Hellman's seminal work [4], there are countless examples of cryptographic schemes that work in any finite, cyclic group G, and whose security can be reduced to a well-defined computational problem in G. In many cases, the order of the group G should be prime (or is even irrelevant). However, some constructions (e.g., [2, 10, 17, 13]) explicitly require a group G of *composite* order.

In particular in combination with a pairing (i.e., a bilinear map) e, groups of composite order exhibit several interesting properties. (For instance, $e(g_1, g_2) = 1$

for elements g_1, g_2 of coprime order. Or, somewhat more generally, the pairing operation operates on the different prime-order components of G independently.) This enables interesting technical applications (e.g., [17, 13]), but also comes at a price. Namely, to accommodate suitably hard computational problems, composite-order groups have to be chosen substantially larger than prime-order groups. Specifically, it should be hard to factor the group order. This leads to significantly slower operations in composite-order groups: [6] suggests that for realistic parameters, Tate pairings in composite-order groups are by a factor of about 50 less efficient than in prime-order groups.

Freeman's composite-order-to-prime-order transformation. It is thus interesting to try to find substitutes for the technical features offered by composite-order groups in prime-order settings. In fact, Freeman [6] has offered a framework and tools to semi-generically convert cryptographic constructions from a composite-order to a prime-order setting. Similar transformations have also been implicit in previous works [8, 17]. The premise of Freeman's approach is that composite-order group elements "behave as" vectors over a prime field. In this interpretation, subgroups correspond to linear subspaces.

Moreover, we can think of the vector components as exponents of prime-order group elements; we can then associate, e.g., a composite-order subgroup indistinguishability problem with the problem of distinguishing vectors (chosen either from a subspace or the whole space) "in the exponent." More specifically, Freeman showed that the composite-order subgroup indistinguishability assumption can be implemented in a prime-order group with the Decisional Diffie-Hellman (or with the k-linear) assumption. A pairing operation over the composite-order group then translates into a suitable "multiplication of vectors," which can mean different things, depending on the desired properties. For instance, Freeman considers both an inner product and a Kronecker product as "vector multiplication" operations (of course with different effects).

Limitations of Freeman's approach. Freeman's work has spawned a number of follow-up results that investigate more general or more efficient conversions of this type [13, 15, 14, 11, 12]. We note that all of these works follow Freeman's interpretation of vectors, and even his possible interpretations of a vector multiplication. Unfortunately, during these investigations, certain lower bounds for the efficiency of these transformations became apparent. For example, Seo [14] proves lower bounds both for the computational cost and the dimension of the resulting vector space of *arbitrary* transformations in Freeman's framework. More specifically, Seo reports a concrete bound on the number of required prime-order pairing operations necessary to simulate a composite-order pairing.

However, of course, these lower bounds crucially use the vector-space interpretation of Freeman's framework. Specifically, it is conceivable that a (perhaps completely different) more efficient composite-order-to-prime-order transformation exists outside of Freeman's framework. Such a more efficient transformation could also provide a way to implement, e.g., the widely used Groth-Sahai proof system [8] more efficiently.

Our contribution: a different view on composite-order-to-prime-order conversions. In this work, we take a step back and question several assumptions that are implicitly made in Freeman's framework. We exhibit a different composite-order-to-prime-order conversion outside of his model, and show that it circumvents previous lower bounds. In particular, our construction leads to more efficient verification of Groth-Sahai proofs in the symmetric setting (i.e., with a symmetric pairing). Moreover, our construction can be implemented from *any* matrix assumption [5] (including the k-linear assumption) and scales better to multilinear settings than previous approaches. In the following, we give more details on our construction and its properties.

A technical perspective: a polynomial interpretation of linear subspaces. To explain our approach, recall that Freeman identifies a composite-order group with a vector space over a prime field. Moreover, in his work, subgroups of the composite-order group always correspond to *uniformly chosen* subspaces of a certain dimension. Of course, such "unstructured" subspaces only allow for rather generic interpretations of composite-order pairings (as generic "vector multiplications" as above).

Instead, we interpret the composite-order group as a very structured vector space. More concretely, we interpret a composite-order group element as (the coefficient vector of) a polynomial $f(X)$ over a prime field. In this view, a composite-order subgroup corresponds to the set of all polynomials with a common zero s (for a fixed and hidden s). Composite-order group operation and pairing correspond to polynomial addition and multiplication. Moreover, the hidden common zero s can be used as a trapdoor to decide subgroup membership, and thus to implement a "projection" in the sense of Freeman.

Specifically, our "vector multiplication" is very structured and natural, and there are several ways to implement it efficiently. For instance, we can apply a convolution on the coefficient vectors, or, more efficiently, we can represent f as a vector of evaluations $f(i)$ at sufficiently many fixed values i, and multiply these evaluation vectors component-wise. In particular, we circumvent the mentioned lower bound of Seo [14] by our different interpretation of composite-order group elements as vectors.

Another interesting property of our construction is that it scales better to the multilinear setting than previous approaches. For instance, while it seems possible to generalize at least Freeman's construction of a "projecting pairing" to a setting with a k-linear map (instead of a pairing), the corresponding generic vector multiplication would lead to exponentially (in k) large vectors in the target group. In our case, a k-linear map corresponds to the multiplication of k polynomials, and only requires a quadratic number of group elements in the target group.[3]

In the description above, f is always a univariate polynomial. With this interpretation, we can show that the SCasc assumption from Escala et al. [5]

[3] We multiply k polynomials, and each polynomial should be of degree at least k, in order to allow for suitable subgroup indistinguishability problems that are plausible even in face of a k-linear map.

implies subgroup indistinguishability. However, we also provide a "multivariate" variant of our approach (with polynomials f in several variables) that can be implemented with *any* matrix assumption (such as the k-linear and even weaker assumptions). Furthermore, in the terminology of Freeman, we provide both a "projecting" and a "projecting and canceling" pairing construction (although the security of the "projecting and canceling" construction requires additional complexity assumptions).

Applications. The performance improvements of our approach are perhaps best demonstrated by the case of Groth-Sahai proofs. Compared to the most efficient previous implementations of Groth-Sahai proofs in prime-order groups with symmetric pairing [15, 5], we almost halve the number of required prime-order pairing operations (cf. Table 1). As a bonus, we also improve on the number of prime-order group elements in the target group, while retaining the small common reference string from [5]. Additionally, in the full version [9] of our paper, we show how to implement a variant of the Boneh-Goh-Nissim encryption scheme [2] in prime-order groups with a k-linear map. As already sketched, this is possible with Freeman's approach only for logarithmically small k.

Structural results. Of course, a natural question is whether *our* results are optimal, and if so, in what sense exactly. We can settle this question in the following sense: we show that the construction sketched above is optimal in our generalized framework. We also prove a similar result for our construction from general matrix assumptions.

Open problems. In this work, we focus on settings with a *symmetric* pairing (resp. multilinear map). It is an interesting open problem to extend our approach to asymmetric settings. Furthermore, the conversion that leads to a canceling *and* projecting map (in the terminology of Freeman) requires a nonstandard complexity assumption (that however holds generically, as we prove). It would be interesting to find constructions from more standard assumptions.

Outline. After recalling some preliminaries in Section 2, we describe our framework in Section 3. Our conversions follow in Section 4. We discuss the optimality of our conversions in Section 5, and compare them to previous conversions in Section 6. Finally, we discuss in Section 7 how our results imply more efficient Groth-Sahai proofs. We refer to the full version [9] for more detailed explanations and proofs.

2 Preliminaries

Notation. Throughout the paper we will use additive notation for all groups G. Nevertheless, we still talk about an exponentiation with exponent a considering a scalar multiplication $a\mathcal{P}$ for $\mathcal{P} \in G$ and $a \in \mathbb{Z}_{|G|}$. Let G be a cyclic group of order p generated by $\mathcal{P}$. Then by $[a] := a\mathcal{P}$ we denote the *implicit representation* of $a \in \mathbb{Z}_p$ in G. To distinguish between implicit representations in the domain G and the target group G_T of a multilinear map we use $[\cdot]$ and $[\cdot]_T$, respectively. More generally, we also define such representations for vectors $\vec{f} \in \mathbb{Z}_p^n$ by $[\vec{f}] :=$

$([f_i])_i \in G^n$, for matrices $\mathbf{A} = (a_{i,j})_{i,j} \in \mathbb{Z}_p^{n\times m}$ by $[\mathbf{A}] := ([a_{i,j}])_{i,j} \in G^{n\times m}$, and for sets $H \subset \mathbb{Z}_p^n$ by $[H] := \{[a] \mid a \in H\} \subset G^n$. We will often identify $\vec{f} \in \mathbb{Z}_p^n$ with the coefficients of a polynomial f in some space V with respect to a (fixed) basis $\mathfrak{q}_0, \ldots, \mathfrak{q}_{n-1}$ of V, i.e., $f = \sum_{i=0}^{n-1} f_i \mathfrak{q}_i$ (e.g., $V = \{f \mid f \in \mathbb{Z}_p[X], \deg(f) < n\}$ and $\mathfrak{q}_i = X^i$). In this case we may also write $[f] := [\vec{f}]$.

Symmetric prime-order k-linear group generators. We use the following formal definition of a k-linear prime-order group generator as the foundation for our constructions. In the scope of these constructions, we will refer to the output of such a generator as a *basic* (or, *prime-order*) k-linear map.

Definition 1 (symmetric prime-order k-linear group generator). *A* symmetric prime-order k-linear group generator *is a PPT algorithm $\mathcal{G}_k$ that on input of a security parameter 1^λ outputs a tuple of the form*

$$\mathcal{MG}_k := (k, G, G_T, e, p, \mathcal{P}, \mathcal{P}_T) \leftarrow \mathcal{G}_k(1^\lambda)$$

where G, G_T are descriptions of cyclic groups of prime order p, $\log p = \Theta(\lambda)$, $\mathcal{P}$ is a generator of G, and $e\colon G \times \ldots \times G \to G_T$ is a map which satisfies the following properties:

- ***k-linearity:*** *For all $Q_1, \ldots, Q_k \in G$, $\alpha \in \mathbb{Z}_p$, and $i \in \{1, \ldots, k\}$ we have $e(Q_1, \ldots, \alpha Q_i, \ldots, Q_k) = \alpha e(Q_1, \ldots, Q_k)$.*
- ***Non-Degeneracy:*** *$\mathcal{P}_T = e(\mathcal{P}, \ldots, \mathcal{P})$ generates G_T.*

In our paper, one should think of $\mathcal{G}_k$ as either a generator of a bilinear group setting (for $k = 2$) defined over some group of points of an elliptic curve and the multiplicative group of a finite field or, for $k > 2$, as generator of an abstract ideal multilinear map, approximated by the recent candidate constructions [7, 3].

Matrix assumptions. Our constructions are based on matrix assumptions as introduced in [5].

Definition 2 (Matrix Distributions and Assumptions [5]). *Let $n, \ell \in \mathbb{N}$, $n > \ell$. We call $\mathcal{D}_{n,\ell}$ a* matrix distribution *if it outputs (in probabilistic polynomial time, with overwhelming probability) matrices $\mathbf{A} \in \mathbb{Z}_p^{n\times \ell}$ of full rank ℓ. $\mathcal{D}_{n,\ell}$ is called* polynomially induced *if it is defined by picking $\vec{s} \in \mathbb{Z}_p^d$ uniformly at random and setting $a_{i,j} := \mathfrak{p}_{i,j}(\vec{s})$ for some polynomials $\mathfrak{p}_{i,j} \in \mathbb{Z}_p[X_1, \ldots, X_d]$ whose degrees do not depend on the security parameter. We define $\mathcal{D}_\ell := \mathcal{D}_{\ell+1,\ell}$. Furthermore, we say that the $\mathcal{D}_{n,\ell}$-*Matrix Diffie-Hellman assumption *or just* $\mathcal{D}_{n,\ell}$ assumption *for short holds relative to the k-linear group generator $\mathcal{G}_k$ if for all PPT adversaries D we have $\mathbf{Adv}_{\mathcal{D}_{n,\ell},\mathcal{G}_k}(\mathsf{D}) = \mathbf{Pr}[\mathsf{D}(\mathcal{MG}_k, [\mathbf{A}], [\mathbf{A}\vec{w}]) = 1] - \mathbf{Pr}[\mathsf{D}(\mathcal{MG}_k, [\mathbf{A}], [\vec{u}]) = 1] = \mathrm{negl}(\lambda)$, where the probability is taken over the output $\mathcal{MG}_k = (k, G, G_T, e, p, \mathcal{P}, \mathcal{P}_T) \leftarrow \mathcal{G}_k(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_{n,\ell}$, $\vec{w} \leftarrow \mathbb{Z}_p^\ell$, $\vec{u} \leftarrow \mathbb{Z}_p^n$ and the coin tosses of the adversary D.*

We note that all of the standard examples of matrix assumptions are polynomially induced and further, in all examples we consider in this paper, the degree of $\mathfrak{p}_{i,j}$ is 1. In particular, we will refer to the following examples of matrix distributions, all for $n = \ell + 1$:

$$\mathcal{SC}_\ell : \mathbf{A} = \begin{pmatrix} -s & 0 & \dots & 0 & 0 \\ 1 & -s & \dots & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & 0 & \dots & 1 & -s \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \mathcal{L}_\ell : \mathbf{A} = \begin{pmatrix} s_1 & 0 & 0 & \dots & 0 \\ 0 & s_2 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \dots & s_\ell \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix}, \mathcal{U}_\ell : \mathbf{A} \leftarrow \mathbb{Z}_p^{(\ell+1)\times\ell},$$

where $s, s_i \leftarrow \mathbb{Z}_p$. Up to sign, the $\mathcal{SC}_\ell$ assumption, introduced in [5], is the *ℓ-symmetric cascade assumption* (ℓ-SCasc). The $\mathcal{L}_\ell$ assumption is actually the well-known *ℓ-linear assumption* (ℓ-Lin, [1]) in matrix language (DDH equals 1-Lin), and the $\mathcal{U}_\ell$ assumption is the *ℓ-uniform assumption*. More generally, we can also define the $\mathcal{U}_{n,\ell}$ assumption for arbitrary $n > \ell$. Note that the $\mathcal{U}_{n,\ell}$ assumption is the weakest matrix assumption (with the worst representation size) and implied by any other $\mathcal{D}_{n,\ell}$ assumption [5]. In particular ℓ-Lin implies the ℓ-uniform assumption as shown by Freeman. Moreover, ℓ-SCasc, ℓ-Lin, and the ℓ-uniform assumption hold in the generic group model [16] relative to a k-linear group generator if $k \leq \ell$ [5].

Interpolating sets. Let $\vec{X} = (X_1, \dots, X_d)$ be a vector of variables. Let $W \subset \mathbb{Z}_p[\vec{X}]$ be a subspace of polynomials of finite dimension m. Given a set of polynomials $\{\mathfrak{r}_0, \dots, \mathfrak{r}_{m-1}\}$ which are a basis of W, we say that $\vec{x}_1, \dots, \vec{x}_m \in \mathbb{Z}_p^d$ is an *interpolating set* for W if the matrix whose (i, j)th entry is defined as $\mathfrak{r}_{j-1}(\vec{x}_i)$ has full rank. It can be easily seen that the property of being an interpolating set is independent of the basis. Further, when p is exponential (and m and the degrees of $\mathfrak{r}_i$ are polynomial) in the security parameter, any m random vectors $\vec{x}_1, \dots, \vec{x}_m$ form an interpolating set with overwhelming probability.

3 Our Framework

We now present our definitional framework for composite-to-prime-order transformations. Basically, the definitions in this section will enable us to describe how groups of prime order p with a multilinear map e can be converted into groups of order p^n for some $n \in \mathbb{N}$ with a multilinear map $\tilde{e}$. These converted groups will then "mimic" certain features of composite-order groups. Since $\tilde{e}$ is just a composition of several instances of e, we will refer to e as the *basic multilinear map*. We start with an overview of the framework of Freeman, since this is the established model for such transformations. Afterwards, we describe our framework in terms of differences to the model of Freeman.

Freeman's model. Freeman identifies some abstract properties of bilinear composite order groups which are essential to construct some cryptographic protocols, namely subgroup indistinguishability, the projecting property and the canceling property. For Freeman, a symmetric bilinear map generator takes a bilinear group of prime order p with a pairing e and outputs some groups $\mathbb{H} \subset \mathbb{G}, \mathbb{G}_T$ of order p^n for some $n \in \mathbb{N}$ and a symmetric bilinear map $\tilde{e}\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, computed via the basic pairing e. Useful instances of such generators satisfy the subgroup indistinguishability assumption, which means that it should be hard to decide membership in $\mathbb{H} \subset \mathbb{G}$. Further, the pairing is projecting if the bilinear map generator also outputs some maps π, π_T defined respectively on $\mathbb{G}, \mathbb{G}_T$ which commute with the pairing and such that $\ker \pi = \mathbb{H}$. The pairing is canceling if $\tilde{e}(\mathbb{H}, \mathbb{H}') = 0$ for some decomposition $\mathbb{G} = \mathbb{H} \oplus \mathbb{H}'$.

Instantiations. Further, Freeman gives several concrete instantiations in which the subgroups $\mathbb{H}$ output by the generator are sampled uniformly. More specifically, in the language of [5], the instantiations sample subgroups according to the $\mathcal{U}_{n,\ell}$ distribution. Although his model is not specifically restricted to this case, follow-up work seems to identify "Freeman's model" with this specific matrix distribution. For instance, the results of [13] on the impossibility of achieving the projecting and canceling property simultaneously or the impossibility result of Seo [14], who proves a lower bound on the size of the image of a projecting pairing, are also in this setting.

Our model. Essentially, we recover Freeman's original definitions for the symmetric setting, however with some additional precisions. First, we extend his model to multilinear maps and, like Seo [14], distinguish between basic multilinear map operations (e) and multilinear map operations ($\tilde{e}$), since an important efficiency measure is how many e-operations are required to compute $\tilde{e}$. The second and main block of differences is introduced with the goal of making the model compatible with several families of matrix assumptions, yielding a useful tool to prove optimality and impossibility results. For this, we extend Freeman's model to explicitly support different families of subgroup assumptions and state clearly what the dependency relations between the different outputs of the multilinear group generator are. In Section 6, we explicitly discuss the advantages of the refinement of the model.

Definition 3. *Let $k, \ell, n, r \in \mathbb{N}$ with $k > 1$ and $r \geq n > \ell$. A $(k, (r, n, \ell))$ symmetric multilinear map generator $\mathcal{G}_{k,(r,n,\ell)}$ takes as input a security parameter 1^λ and a basic k-linear map generator $\mathcal{G}_k$ and outputs in probabilistic polynomial time a tuple $(\mathcal{MG}_k, \mathbb{H}, \mathbb{G}, \mathbb{G}_T, \tilde{e})$, where*

- *$\mathcal{MG}_k := (k, G, G_T, e, p, \mathcal{P}, \mathcal{P}_T) \leftarrow \mathcal{G}_k(1^\lambda)$ is a description of a prime order symmetric k-linear group*
- *$\mathbb{G} \subset G^r$ is a subgroup of G^r with a minimal generating set of size n*
- *$\mathbb{H} \subset \mathbb{G}$ is a subgroup of $\mathbb{G}$ with a minimal generating set of size ℓ*
- *$\tilde{e} \colon \mathbb{G}^k \to \mathbb{G}_T$ is a non-degenerate k-linear map.*

We assume that elements in $\mathbb{H}, \mathbb{G}$ are represented as vectors in G^r. With this representation, it is natural to identify elements in these groups with vectors in $\mathbb{Z}_p^r$ in the usual way, via the canonical basis. Via this identification, any subgroup $\mathbb{H} \subset G^r$ spanned by $[\vec{b}_1], \ldots, [\vec{b}_\ell]$ corresponds to the subspace H of $\mathbb{Z}_p^r$ spanned by $\vec{b}_1, \ldots, \vec{b}_\ell$, and we write $\mathbb{H} = [H]$. Further, we may assume that $\mathbb{G}_T = G_T^m$ and elements of $\mathbb{G}_T$ are represented by m-tuples of G_T, for some fixed $m \in \mathbb{N}$, although we do not include m as a parameter of the multilinear generator.

In most constructions $n = r$, in which case we drop the index r from the definition, and we simply refer to such a generator as a $(k, (n, \ell))$ generator

$\mathcal{G}_{k,(n,\ell)}$. We always assume that membership in $\mathbb{G}$ is easy to decide.[4] In the case where $n = r$ and $\mathbb{G} = G^r$ this is obviously the case, but otherwise we assume that the description of $\mathbb{G}$ includes some auxiliary information which allows to test it (like in [15] or [12]).

Definition 4 (Properties of multilinear map generators). *Let $\mathcal{G}_{k,(r,n,\ell)}$ be a $(k,(r,n,\ell))$ symmetric multilinear map generator as in Definition 3 with output $(\mathcal{MG}_k, \mathbb{H}, \mathbb{G}, \mathbb{G}_T, \tilde{e})$. We define the following properties:*

- ***Subgroup indistinguishability.*** *We say that $\mathcal{G}_{k,(r,n,\ell)}$ satisfies the* subgroup indistinguishability property *if for all PPT adversaries* D*,*

$$\begin{aligned}\mathbf{Adv}_{\mathcal{G}_{k,(r,n,\ell)}}(\mathsf{D}) = &\ \mathbf{Pr}[\mathsf{D}(\mathcal{MG}_k, \mathbb{H}, \mathbb{G}, \mathbb{G}_T, \tilde{e}, x) = 1] \\ &- \mathbf{Pr}[\mathsf{D}(\mathcal{MG}_k, \mathbb{H}, \mathbb{G}, \mathbb{G}_T, \tilde{e}, u) = 1] = \mathrm{negl}(\lambda),\end{aligned}$$

  where the probability is taken over $(\mathcal{MG}_k, \mathbb{H}, \mathbb{G}, \mathbb{G}_T, \tilde{e}) \leftarrow \mathcal{G}_{k,(r,n,\ell)}(1^\lambda)$, $x \leftarrow \mathbb{H}, u \leftarrow \mathbb{G}$ and the coin tosses of the adversary D.
- ***Projecting.*** *We say that $(\mathcal{MG}_k, \mathbb{H}, \mathbb{G}, \mathbb{G}_T, \tilde{e})$ is* projecting *if there exist two non-zero homomorphisms $\pi\colon \mathbb{G} \to \mathbb{G}$, $\pi_T\colon \mathbb{G}_T \to \mathbb{G}_T$ such that $\ker \pi = \mathbb{H}$ and $\pi_T(\tilde{e}(x_1, \ldots, x_k)) = \tilde{e}(\pi(x_1), \ldots, \pi(x_k))$ for any $(x_1, \ldots, x_k) \in \mathbb{G}^k$. For the special case $r = n = \ell + 1$, $\mathbb{G} := G^n$, we can equivalently define the maps $\pi\colon G^n \to G$, $\pi_T\colon \mathbb{G}_T \to G_T$ such that $\ker \pi = \mathbb{H}$ and $\pi_T(\tilde{e}(x_1, \ldots, x_k)) = e(\pi(x_1), \ldots, \pi(x_k))$ (matching the original definition of [8]). We say that $\mathcal{G}_{k,(r,n,\ell)}$ is projecting if its output is projecting with overwhelming probability.*
- ***Canceling.*** *We say that $(\mathcal{MG}_k, \mathbb{H}_1, \mathbb{G}, \mathbb{G}_T, \tilde{e})$ is* canceling *if there exists a decomposition $\mathbb{G} = \mathbb{H}_1 \oplus \mathbb{H}_2$ such that for any $x_1 \in \mathbb{H}_{j_1}, \ldots, x_k \in \mathbb{H}_{j_k}$, $\tilde{e}(x_1, \ldots, x_k) = 0$ except for $j_1 = \ldots = j_k$. We call $\mathcal{G}_{k,(r,n,\ell)}$ canceling if its output is canceling with overwhelming probability.*

So far, the given definitions match those of Freeman (extended to the k-linear case) except that we explicitly define the basic k-linear group $\mathcal{MG}_k$ which is used in the construction. We will now introduce two aspects of our framework that are new compared to Freeman's model. First, we will define multilinear generators that sample subgroups according to a specific matrix assumptions. Then, we will define a property of the multilinear map $\tilde{e}$ that will be very useful to establish impossibility results and lower bounds.

Definition 5. *Let $k, \ell, n, r \in \mathbb{N}$ with $k > 1$, $r \geq n > \ell$ and $\mathcal{D}_{n,\ell}$ be a matrix distribution. A $(k,(r,n,\ell),\mathcal{D}_{n,\ell})$ multilinear map generator $\mathcal{G}_{k,(r,n,\ell),\mathcal{D}_{n,\ell}}$ is a $(k,(r,n,\ell))$ multilinear map generator which outputs $(\mathcal{MG}_k, \mathbb{H}, \mathbb{G}, \mathbb{G}_T, \tilde{e})$ such that the distribution of the subspaces H such that $\mathbb{H} = [H]$ equals $\mathcal{D}_{n,\ell}$ for any fixed choice of $\mathcal{MG}_k$.*

As usual, in the case where $r = n$, we just drop r and refer to a $(k, \mathcal{D}_{n,\ell})$ multilinear map generator $\mathcal{G}_{k,\mathcal{D}_{n,\ell}}$. We conclude our framework with a definition

[4] We note that with the recent approximate multilinear maps from [7, 3], not even group membership is efficiently recognizable. This will not affect our results, but of course hinders certain applications (such as Groth-Sahai proofs).

Table 1: Efficiency of different symmetric projecting k-linear maps. The size of the domain (n) and codomain (m) of $\tilde{e}$ is given as number of group elements of G and G_T, respectively. Costs are stated in terms of the number of applications of the basic map e, group operations (gop) including inversion in G/G_T, and ℓ-fold multi-exponentiations of the form $e_1[a_1] + \cdots + e_\ell[a_\ell]$ (ℓ-mexp) in G/G_T. Note that in this paper, for the computation of $\tilde{e}$, we use an evaluate-multiply-approach.

Construction	Ass.	Co-/Domain	Cost $\tilde{e}$	Cost π	Cost π_T
Freeman, $k = 2$ [6]	$\mathcal{U}_2$	9/3	9 e	3 3-mexp	9 9-mexp
Seo, $k = 2$ [14]	$\mathcal{U}_2$	6/3	9 e + 3 gop	3 3-mexp	6 6-mexp
This paper, $k = 2$	$\mathcal{SC}_2$	**5/3**	**5 e + 22 gop**	**1 2-mexp**	**1 5-mexp**
This paper, $k = 2$	$\mathcal{U}_2$	6/3	6 e + 12 3-mexp[1]	1 3-mexp	1 6-mexp
Freeman, $k > 2$	$\mathcal{U}_k$	$(k+1)^k/k+1$	$(k+1)^{k+1}$ e	$k+1$ $(k+1)$-mexp	$(k+1)^k$ $(k+1)^k$-mexp
This paper, $k > 2$	$\mathcal{U}_k$	$\binom{2k}{k}/k+1$	$\binom{2k}{k}$ e + $\binom{2k}{k}k$ $(k+1)$-mexp[1]	1 $(k+1)$-mexp	1 $\binom{2k}{k}$-mexp
This paper, $k > 2$	$\mathcal{SC}_k$	$k^2+1/k+1$	(k^2+1) e + (k^3+k) **k-mexp**[1]	**1 k-mexp**	**1 k^2+1-mexp**

[1] For the construction based on $\mathcal{SC}_k$, the involved exponents are relatively small, namely the biggest one is $(\lceil \frac{k^2+1}{2} \rceil)^k$. Also for $\mathcal{U}_k$, the involved exponents can usually be made small.

that enables us to distinguish generators where the multilinear map $\tilde{e}$ may or may not depend on the choice of the subgroups.

Definition 6. *We say that a $(k, (r, n, \ell), \mathcal{D}_{n,\ell})$ multilinear map generator with output $(\mathcal{MG}_k, \mathbb{H}, \mathbb{G}, \mathbb{G}_T, \tilde{e})$ as in Definition 5 defines a* fixed multilinear map *if the random variable H (s.t. $\mathbb{H} = [H]$) conditioned on $\mathcal{MG}_k$ and the random variable $(\mathbb{G}, \mathbb{G}_T, \tilde{e})$ conditioned on $\mathcal{MG}_k$ are independent.*

4 Our Constructions

All of our constructions arise from the following *polynomial point of view*: The key idea is to treat $\mathbb{G} = G^n$ as an implicit representation of some space of polynomials. Polynomial multiplication will then give us a natural multilinear map. For subspaces $\mathbb{H}^{(\vec{s})}$ that correspond to polynomials sharing a common root $\vec{s}$, this multilinear map will turn out to be projecting. We will first illustrate this idea by means of a simple concrete example where subgroup decision for $\mathbb{H}^{(\vec{s})}$ is equivalent to 2-SCasc (Section 4.1). Then we show that actually any polynomially induced matrix assumption gives rise to such a polynomial space and thus allows for the construction of a k-linear projecting map (Section 4.2). Finally, by considering $\mathbb{G}$ along with the multilinear map as an implicit representation of a polynomial ring modulo some reducible polynomial, we are able to construct a multilinear map which is both projecting and canceling (see Section 4.3 for a summary). See Table 1 for an overview of the characteristics of our projecting map constructions in comparison with previous work.

4.1 A Projecting Pairing based on the 2-SCasc Assumption

Let $(k = 2, G, G_T, e, p, \mathcal{P}, \mathcal{P}_T) \leftarrow \mathcal{G}_2(1^\lambda)$ be the output of a symmetric prime-order bilinear group generator. We set $\mathbb{G} := G^3$ and $\mathbb{G}_T := G_T^5$. For any $[\vec{f}] =$

$([f_0],[f_1],[f_2]) \in \mathbb{G} = G^3$, we identify $\vec{f}$ with the polynomial $f = f_0 + f_1 X + f_2 X^2 \in \mathbb{Z}_p[X]$ of degree at most 2. Similarly, any $[\vec{f}]_T \in \mathbb{G}_T$ corresponds to a polynomial of degree at most 4. Then the canonical group operation for $\mathbb{G}$ and $\mathbb{G}_T$ corresponds to polynomial addition (in the exponent), i.e., $[\vec{f}] + [\vec{g}] = [\vec{f}+\vec{g}] = [f+g]$ and $[\vec{f}]_T+[\vec{g}]_T = [f+g]_T$. Furthermore, polynomial multiplication (in the exponent) gives a map $\tilde{e}\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$,

$$\tilde{e}([\vec{f}],[\vec{g}]) := \Big(\Big[\sum_{i+j=0} f_i g_j \Big]_T, \ldots, \Big[\sum_{i+j=4} f_i g_j \Big]_T \Big) = [f \cdot g]_T$$

It is easy to see that $(\mathbb{G}, \mathbb{G}_T, \tilde{e})$ is again a bilinear group setting, where the group operations and the pairing $\tilde{e}$ can be efficiently computed.

A subgroup decision problem. For some fixed $s \in \mathbb{Z}_p$ let us consider the subgroup $\mathbb{H}^{(s)} \subset \mathbb{G}$ formed by all elements $[\vec{f}] \in \mathbb{G}$ such that $\vec{f}$ viewed as polynomial f has root s, i.e., $\mathbb{H}^{(s)} = \{[f] \in \mathbb{G} \mid f(s) = 0\}$. In other words, $\mathbb{H}^{(s)}$ consists of all $[f]$ with f of the form

$$(X - s)(f_1' X + f_0') \ , \tag{1}$$

where $f_1', f_0' \in \mathbb{Z}_p$. Thus, given $[f]$ and $[s]$, the subgroup decision problem for $\mathbb{H}^{(s)} \subset \mathbb{G}$ means to decide whether f is of this form or not. Viewing Eq. (1) as matrix-vector multiplication, we see that this is equivalent to deciding whether $\vec{f}$ belongs to the image of the 3×2 matrix

$$\mathbf{A}(s) := \begin{pmatrix} -s & 0 \\ 1 & -s \\ 0 & 1 \end{pmatrix} \tag{2}$$

Hence, our subgroup decision problem corresponds to the 2-SCasc problem (cf. Definition 2) which is hard in a generic bilinear group [5].

Projections. Given s, we can simply define projection maps $\pi\colon \mathbb{G} \to G$ and $\pi_T\colon \mathbb{G}_T \to G_T$ by polynomial evaluation at s (in the exponent), i.e., $[\vec{f}]$ is mapped to $[f(s)]$ and $[\vec{f}]_T$ to $[f(s)]_T$. Computing π, π_T requires group operations only. Obviously, it holds that $\ker(\pi) = \mathbb{H}^{(s)}$ and $e(\pi([\vec{f_1}]), \pi([\vec{f_2}])) = \pi_T(\tilde{e}([\vec{f_1}], [\vec{f_2}]))$.

Sampling from $\mathbb{H}^{(s)}$. Given $[(-s,1,0)], [(0,-s,1)] \in \mathbb{G}$, a uniform element from $\mathbb{H}^{(s)}$ can be sampled by picking $(f_0', f_1') \leftarrow \mathbb{Z}_p^2$ and, as with any matrix assumption, computing the matrix-vector product

$$\Big[\begin{pmatrix} -s & 0 \\ 1 & -s \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} f_0' \\ f_1' \end{pmatrix} \Big] = \Big[(-s f_0', f_0' - s f_1', f_1')^{\mathrm{T}} \Big] \tag{3}$$

Again, this can be done using the group operation only.

Efficiency. Computing $\tilde{e}$ in our construction corresponds to polynomial multiplication. Although this multiplication happens in the exponent (and we are "only" given implicit representations of the polynomials), we are not forced to stick to schoolbook multiplication. Instead, we propose to follow an evaluation-multiplication-interpolation approach (using small interpolation points) where the actual interpolation step is postponed to the computation of π_T.

More precisely, so far we used coefficient representation for polynomials over $\mathbb{G}$ and $\mathbb{G}_T$ with respect to the standard basis. However, other (s-independent) bases are also possible without affecting security. For efficiency, we propose to stick to this representation for $\mathbb{G}$ but to use point-value representation for polynomials over $\mathbb{G}_T$ with respect to the fixed interpolating set $M := \{-2, -1, 0, 1, 2\}$ (cf. Definition 2). This means we now identify a polynomial g in the target space with the vector $(g(-2), g(-1), g(0), g(1), g(2))$.

More concretely, to compute $\tilde{e}([f_1], [f_2]) = ([(f_1 f_2)(x)]_T)_{x \in M}$, we first evaluate f_1 and f_2 (in the exponent) with all $x \in M$, followed by a point-wise multiplication $([f_1(x)f_2(x)]_T)_{x \in M} = (e([f_1(x)], [f_2(x)]))_{x \in M}$. This way, $\tilde{e}$ can be computed more efficiently with only five pairings. Computing π is unchanged. To apply π_T, one first needs to obtain the coefficient representation by interpolation and then evaluate the polynomial at s. However, this can be done simultaneously and as the 1×5 matrix describing this operation can be precomputed (given s) it does not increase the computational cost much.

4.2 Projecting Multilinear Maps from any Matrix Assumption

In the following, we will first demonstrate that for any vector space of polynomials, the natural pairing given by polynomial multiplication is projecting for subspaces consisting of polynomials sharing a common root. We will then show that any (polynomially induced) matrix assumption can equivalently be considered as a subspace assumption in a vector space of polynomials of this type. This way, we obtain a natural projecting multilinear map for any polynomially induced matrix assumption.

A projecting multilinear map on spaces of polynomials. Let $\mathcal{MG}_k := (k, G, G_T, e, p, \mathcal{P}, \mathcal{P}_T) \leftarrow \mathcal{G}_k(1^\lambda)$ be the output of a prime-order k-linear group generator. Let $V \subset \mathbb{Z}_p[\vec{X}]$ be a vector space of polynomials of dimension n for which we fix a basis $\mathfrak{q}_0, \ldots, \mathfrak{q}_{n-1}$. Then for any $[\vec{f}] \in \mathbb{G} := G^n$ we can identify the vector $\vec{f} = (f_0, \ldots, f_{n-1})$ with a polynomial $f = \sum f_i \mathfrak{q}_i \in V$. In the 2-$\mathsf{SCasc}$ example above, V corresponds to univariate polynomials of degree at most 2 and the basis is given by $1, X, X^2$. On V, we have a natural k-linear map given by polynomial multiplication: $\mathrm{mult}_k\colon V^k \to \mathbb{Z}_p[\vec{X}], \mathrm{mult}_k(f_1, \ldots, f_k) = f_1 \cdots f_k$. Let $W \subset \mathbb{Z}_p[\vec{X}]$ be the span of the image of mult_k and m its dimension. Then we can again fix a basis $\mathfrak{r}_0, \ldots, \mathfrak{r}_{m-1}$ of W to identify polynomials with vectors. In the 2-SCasc example above, W consists of polynomials of degree at most 4 and we chose the basis $1, X, X^2, X^3, X^4$ of W for our initial presentation. From polynomial multiplication, we then obtain a non-degenerate k-linear map

$$\tilde{e}\colon \mathbb{G}^k \to G_T^m, \tilde{e}([\vec{f_1}], \ldots, [\vec{f_k}]) = [f_1 \cdots f_k]_T \ .$$

Now consider a subspace $\mathbb{H}^{(\vec{s})} \in \mathbb{G}$ of the form $\mathbb{H}^{(\vec{s})} = \{[f] \in \mathbb{G} \mid f(\vec{s}) = 0\}$. It is easy to see that $\tilde{e}$ is projecting for this subspace: A projection map $\pi\colon \mathbb{G} \to G$ with $\ker(\pi) = \mathbb{H}^{(\vec{s})}$ is given by evaluation at $\vec{s}$, i.e., $\pi([\vec{f}]) = [f(\vec{s})]$.

Similarly, $\pi_T\colon G_T^m \to G_T$ is defined by $\pi_T([\vec{g}]_T) = [g(\vec{s})]_T$ and by construction we have $e(\pi([\vec{f_1}]),\dots,\pi([\vec{f_k}])) = [f_1(\vec{s})\cdots f_k(\vec{s})]_T = [(f_1\cdots f_k)(\vec{s})]_T = \pi_T(\tilde{e}([\vec{f_1}],\dots,[\vec{f_k}]))$.

From a polynomially induced matrix distribution to a space of polynomials. Now, let $\mathcal{D}_{n-1}$ be any polynomially induced matrix distribution as defined in Definition 2 and let $\mathbf{A}(\vec{X}) \in (\mathbb{Z}_p[\vec{X}])^{n\times(n-1)}$ be the polynomial matrix describing this distribution. Then we set $\mathbb{G} := G^n$ and consider the subspace $[\mathsf{Im}\,\mathbf{A}(\vec{s})]$ for some $\vec{s}$. We now show that we can identify $\mathbb{G}$ with a vector space V of polynomials, such that the subspace $\mathsf{Im}\,\mathbf{A}(\vec{s})$ corresponds exactly to polynomials having a root at $\vec{s}$. To this end, consider the determinant of $(\mathbf{A}(\vec{X})||\vec{F})$ as a polynomial $\mathfrak{d}$ in indeterminates $\vec{X}$ and $\vec{F}$. Since we assume that $\mathbf{A}(\vec{s})$ has generically[5] full rank a given vector $\vec{f} \in \mathbb{Z}_p^n$ belongs to the image of $\mathbf{A}(\vec{s})$ iff the determinant of the extended matrix $(\mathbf{A}(\vec{s})||\vec{f})$ is zero, i.e., $\mathfrak{d}(\vec{s},\vec{f}) = 0$. To obtain the desired vector space V with basis $\mathfrak{q}_0,\dots,\mathfrak{q}_{n-1}$, we consider the Laplace expansion of this determinant to write $\mathfrak{d}$ as

$$\mathfrak{d}(\vec{X},\vec{F}) = \sum_{i=0}^{n-1} F_i \mathfrak{q}_i(\vec{X})\,. \tag{4}$$

for some polynomials $\mathfrak{q}_i(\vec{X})$ depending only on $\mathbf{A}$. For $\mathcal{SC}_2$, we have $\mathfrak{q}_i = X^i$. We note that in all cases of interest the $\mathfrak{q}_i$ are linearly independent (see [9]).

Thus, we may now identify $[\vec{f}] \in \mathbb{G}$ with the implicit representation of the polynomial $f = \mathfrak{d}(\vec{X},\vec{f}) = \sum_i f_i \mathfrak{q}_i$. As $f(\vec{s}) = \sum_i f_i \mathfrak{q}_i(\vec{s}) = 0$ iff $\vec{f} \in \mathsf{Im}\,\mathbf{A}(\vec{s})$, we have $\mathbb{H}^{(\vec{s})} = [\mathsf{Im}\,\mathbf{A}(\vec{s})] = \{[f] \in \mathbb{G} \mid f(s) = 0\}$. Hence, we may construct a projecting k-linear map from polynomial multiplication as described in the previous paragraph.

Working through the construction, one can obtain explicit coordinates as follows: let W be the span of $\{\mathfrak{q}_{i_1}\cdots\mathfrak{q}_{i_k} \mid 0 \le i_j < n\}$ and fix a basis $\mathfrak{r}_0,\dots,\mathfrak{r}_{m-1}$ of W. This determines coefficients $\lambda_t^{(i_1,\dots,i_k)}$ in $\mathfrak{q}_{i_1}\cdots\mathfrak{q}_{i_k} = \sum_{t=0}^{m-1}\lambda_t^{(i_1,\dots,i_k)}\mathfrak{r}_t$.

Recall that $\tilde{e}\colon (G^n)^k \to G_T^m$ is defined as $\tilde{e}([\vec{f_1}],\dots,[\vec{f_k}]) = [f_1\cdots f_k]_T$, expressed as an element of G_T^m via the basis $\vec{\mathfrak{r}}$. In coordinates this reads

$$\begin{aligned}\tilde{e}([\vec{f_1}],\dots,[\vec{f_k}]) = \Big(&\sum_{j_1\le\dots\le j_k}\lambda_0^{(j_1,\dots,j_k)}\cdot\sum_{\substack{(i_1,\dots,i_k)\in\\ \tau(j_1,\dots,j_k)}} e([f_{1,i_1}],\dots,[f_{k,i_k}]),\dots,\\ &\sum_{j_1\le\dots\le j_k}\lambda_{m-1}^{(j_1,\dots,j_k)}\cdot\sum_{\substack{(i_1,\dots,i_k)\in\\ \tau(j_1,\dots,j_k)}} e([f_{1,i_1}],\dots,[f_{k,i_k}])\Big)\end{aligned} \tag{5}$$

where $[f_{1,i_1}\cdots f_{k,i_k}]_T$ simply denotes $(f_{1,i_1}\cdots f_{k,i_k})\mathcal{P}_T$ and $\tau(j_1,\dots,j_k)$ denotes the set of permutations of $(j_1,\dots,j_k)$. The last optimization can be done

[5] This means that $\mathbf{A}(\vec{s})$ will be full rank with overwhelming probability and this is indeed equivalent to $\mathfrak{d} \neq 0$. To simplify the exposition, we may assume that the sampling algorithm is changed to exclude $\vec{s}$ where $\mathbf{A}(\vec{s})$ does not have full rank.

as $\mathfrak{q}_{i_1} \cdots \mathfrak{q}_{i_k} = \mathfrak{q}_{j_1} \cdots \mathfrak{q}_{j_k}$ for $(i_1, \dots, i_k) \in \tau(j_1, \dots, j_k)$. For the same reason, we have $m = \binom{n+k-1}{k}$ in the worst case. In this way, the target group in our constructions is always smaller than the target group in Freeman's construction (generalized to $k \geq 2$), which is of size n^k.

The following theorem summarizes our construction and its properties:

Theorem 1. *Let $k > 1$, $n \in \mathbb{N}$, and $\mathcal{D}_{n-1}$ be a polynomially induced matrix distribution. Let $\mathcal{G}_{k,\mathcal{D}_{n-1}}$ be an algorithm that on input of a security parameter 1^λ and a symmetric prime-order k-multilinear map generator $\mathcal{G}_k$ outputs $(\mathcal{MG}_k, \mathbb{H}^{(\vec{s})}, \mathbb{G}, \mathbb{G}_T, \tilde{e})$, where*

- $\mathcal{MG}_k := (k, G, G_T, e, p, \mathcal{P}, \mathcal{P}_T) \leftarrow \mathcal{G}_k(1^\lambda)$,
- $\mathbb{G} := G^n$, $\mathbb{H}^{(\vec{s})} := [\mathsf{Im}\, \mathbf{A}(\vec{s})]$, $\mathbf{A}(\vec{s}) \leftarrow \mathcal{D}_{n-1}$,
- $\mathbb{G}_T := G_T^m$, *where m equals the dimension of*

$$W := \left\{ \sum_{0 \leq i_1, \dots, i_k \leq n-1} \alpha_{i_1,\dots,i_k} \mathfrak{q}_{i_1} \cdots \mathfrak{q}_{i_k} \;\middle|\; \alpha_{i_1,\dots,i_k} \in \mathbb{Z}_p \right\}$$

(as vector space), and $\mathfrak{q}_0(\vec{X}), \dots, \mathfrak{q}_{n-1}(\vec{X}) \in \mathbb{Z}_p[\vec{X}]$ are polynomials s.t.

$$\det(\mathbf{A}(\vec{X}) || \vec{F}) = \sum_{i=0}^{n-1} F_i \mathfrak{q}_i(\vec{X})$$

for the matrix $\mathbf{A}(\vec{X})$ describing $\mathcal{D}_{n-1}$, and
- $\tilde{e} \colon \mathbb{G}^k \to \mathbb{G}_T$ *is the map defined by Eq. (5) for a basis $\mathfrak{r}_0, \dots, \mathfrak{r}_{m-1}$ of W.*

Then $\mathcal{G}_{k,\mathcal{D}_{n-1}}$ is a $(k, \mathcal{D}_{n-1})$ multilinear map generator. It is projecting, where the projection maps $\pi \colon \mathbb{G} \to G$ and $\pi_T \colon \mathbb{G}_T \to G_T$ defined by $\pi(\vec{f}) := \sum_{i=0}^{n-1} \mathfrak{q}_i(\vec{s})[f_i]$ and $\pi_T(\vec{g}) := \sum_{i=0}^{m-1} \mathfrak{r}_i(\vec{s})[g_i]_T$ are efficiently computable given the trapdoor $\vec{s}$. Furthermore, if the $\mathcal{D}_{n-1}$ assumption holds with respect to $\mathcal{G}_k$, then subgroup indistinguishability holds with respect to $\mathcal{G}_{k,\mathcal{D}_{n-1}}$.

Example 1. We can construct a projecting k-linear map generator satisfying subgroup indistinguishability under k-SCasc (which is hard in a k-linear generic group model). For $\mathcal{G}_{k,\mathcal{SC}_k}$, we would get $n = k+1$ and $\mathfrak{q}_i(X) = X^i$ if k is even and $\mathfrak{q}_i(X) = -X^i$ when k is odd, where $0 \leq i \leq k$. Using the basis $\mathfrak{r}_t(X) = X^t$ for W if k is even and $\mathfrak{r}_t(X) = -X^t$ if k is odd for $0 \leq t \leq k^2$, we obtain $\lambda_t^{(i_1,\dots,i_k)} = 1$ for $t = i_1 + \cdots + i_k$ and $\lambda_t^{(i_1,\dots,i_k)} = 0$ else. Note that we have $m = k^2 + 1$.

Example 2. We can also construct a k-linear map generator from k-Lin. For $\mathcal{G}_{k,\mathcal{L}_k}$, we would have $n = k+1$, and polynomials $\mathfrak{q}_k(X_0, \dots, X_{k-1}) = X_0 \cdots X_{k-1}$ and $\mathfrak{q}_i(X_0, \dots, X_{k-1}) = -\prod_{j \neq i} X_j$ for $0 \leq i \leq k-1$. As a basis for W we can simply take $\{\mathfrak{q}_{j_1} \cdots \mathfrak{q}_{j_k} \mid 0 \leq j_1 \leq \ldots \leq j_k \leq k\}$ yielding $m = \binom{n+k-1}{k}$.

Example 3. Like Freeman, we could also construct a k-linear map generator from the $\mathcal{U}_k$ assumption. Although the polynomials $\mathfrak{q}_i(X_{1,1}, \ldots, X_{k,k+1})$, $0 \leq i \leq k$, associated to $\mathcal{G}_{k,\mathcal{U}_k}$ have a much more complex description than in the k-Lin case, the image size of the resulting map is the same, namely $m = \binom{n+k-1}{k}$, because a basis of the image is also $\{\mathfrak{q}_{j_1} \cdots \mathfrak{q}_{j_k} \mid 0 \leq j_1 \leq \ldots \leq j_k \leq k\}$.

Efficiency. As in our setting any change of basis is efficiently computable, the security of our construction only depends on the vector space V (which in turn determines W), but not on the bases chosen. So we are free to choose bases that improve efficiency. We propose to follow the same approach as in Section 4.1: Select points $\vec{x}_0, \ldots, \vec{x}_{m-1}$ that form an interpolating set for W and represent $f \in W$ via the vector $f(\vec{x}_0), \ldots, f(\vec{x}_{m-1})$. This corresponds to choosing the basis of W consisting of polynomials $\mathfrak{r}_0, \ldots, \mathfrak{r}_{m-1} \in W$ such that $\mathfrak{r}_i(\vec{x}_j) = 1$ for $i = j$ and 0 otherwise. For the domain V, the choice is less significant and we might simply choose the $\mathfrak{q}_i$'s that the determinant polynomial gives us. Then we can compute $\tilde{e}([\vec{f_1}], \ldots, [\vec{f_k}])$ by an evaluate-multiply approach using only m applications of e. Note that the evaluation step can also be done pretty efficiently if the $\mathfrak{q}_i$'s have small coefficients (which usually is the case). For details see [9].

4.3 Canceling and Projecting k-Linear Maps From Polynomial Spaces

By considering polynomial multiplication modulo a polynomial h, which has a root at the secret s, we are able to construct a $(k, (n = \ell + 1, \ell))$ symmetric multilinear map generator with a *non-fixed* pairing that is both canceling and projecting. Our first construction relies on a $k' := k + 1$-linear prime-order map e. The one additional multiplication in the exponent is used to perform the reduction modulo h. Based on this construction, we propose another $(k, (r = 2\ell, n = \ell+1, \ell))$ symmetric multilinear map generator that requires only a $k' = k$-linear prime-order map. The security of our constructions is based on variants of the ℓ-SCasc assumption. We need to extend ℓ-SCasc by additional given group elements to allow for reduction in the exponent, e.g., in the simplest case hints of the form $[X^i \bmod h]$ are given. In the full version of this paper we give details, efficiency considerations, and show that our constructions are secure for $\ell \geq k'$ in generic k'-linear groups. We note that, to the best of our knowledge, this is the first construction of a projecting&canceling map that naturally generalizes to $k' > 2$.

5 Optimality and Impossibility Results

5.1 Optimality of Polynomial Multiplication

In this section we show that for any polynomially induced matrix assumption $\mathcal{D}_{\ell+1,\ell}$, the projecting multilinear map resulting from the polynomial viewpoint is optimal in terms of image size.

Theorem 2. *Let $k > 0$, and let $\mathcal{D}_{\ell+1,\ell}$ be a polynomially induced matrix assumption and let $\mathfrak{q}_0, \ldots, \mathfrak{q}_\ell$ be the polynomials associated to $\mathcal{D}_{\ell+1,\ell}$ as defined in Eq. (4) in Section 4.2 and let $W \subset \mathbb{Z}_p[\vec{X}]$ be the space of polynomials spanned by $\{\mathfrak{q}_{i_1} \ldots \mathfrak{q}_{i_k} \mid 0 \leq i_j \leq \ell\}$. Let $(\mathcal{MG}_k, \mathbb{H}, G^{\ell+1}, G_T^m, \tilde{e})$ be the output of any other fixed $(k, \mathcal{D}_{\ell+1,\ell})$ projecting multilinear map generator. Then, $\overline{m} := \dim W \leq m$.*

$$\begin{tikzcd}
\mathbb{G}^k \arrow[r, "\tilde{e}"] \arrow[d, "(\pi^{(\vec{s})})^k"] & G_T^m \arrow[d, "\pi_T^{(\vec{s})}"] \\
G^k \arrow[r, "e"] & G_T
\end{tikzcd}$$

$$\begin{tikzcd}
\mathbb{G}^k \times \ldots \times \mathbb{G}^k \arrow[r, "(\tilde{e}, \ldots, \tilde{e})"] \arrow[d, "\left((\pi^{(\vec{s}_1)})^k, \ldots, (\pi^{(\vec{s}_{\overline{m}})})^k\right)"] & G_T^m \times \ldots \times G_T^m \arrow[d, "\left(\pi_T^{(\vec{s}_1)}, \ldots, \pi_T^{(\vec{s}_{\overline{m}})}\right)"] \\
G^k \times \ldots \times G^k \arrow[r, "(e, \ldots, e)"] & G_T \times \ldots \times G_T
\end{tikzcd}$$

Figure 1: Left: Projecting property. Right: The diagram repeated $\overline{m}$ times for an interpolating set $\vec{s}_1, \ldots \vec{s}_{\overline{m}}$ for W.

Proof Intuition. An intuition of the proof is given by Figure 1. The first part of the proof shows that w.l.o.g. we can assume that $\pi_T^{(\vec{s})} \circ \tilde{e}$ is polynomial multiplication for all $\vec{s}$, that is, for any $[\vec{f_1}], \ldots, [\vec{f_k}] \in G^{\ell+1}$, $\pi_T(\tilde{e}([\vec{f_1}], \ldots, [\vec{f_k}])) = [(f_1 \ldots f_k)(\vec{s})]_T$. This follows from the commutative diagram on the left, i.e., the projecting property, together with the fact that, because $\mathbb{H}$ has codimension 1, the map $\pi^{(\vec{s})}$ must (up to scalar multiples) correspond to polynomial evaluation at $\vec{s}$. The intuition for the second part of the proof is given by the diagram on the right-hand side of Figure 1. Here we show that if $\vec{s}_1, \ldots \vec{s}_{\overline{m}}$ is an interpolating set for W, then the span of $\left\{\left(\pi_T^{(\vec{s}_1)}(\vec{x}), \ldots, \pi_T^{(\vec{s}_{\overline{m}})}(\vec{x})\right) | \vec{x} \in \tilde{e}(\mathbb{G}^k)\right\} \subset G_T^{\overline{m}}$ is of dimension $\overline{m}$. This dimension can be at most the dimension of the span of $\tilde{e}(\mathbb{G}^k)$, showing $\overline{m} \leq m$. A full proof is given in [9].

5.2 Optimality of our Projecting Multilinear Map from the SCasc-Assumption

As a result of our general viewpoint, we can actually show that the projecting multilinear map based on the SCasc-assumption is optimal among *all* polynomially induced matrix assumptions $\mathcal{D}_{n,\ell}$ that are not redundant. Non-redundancy rules out the case where some components of $\vec{z}$ are no help (even information-theoretically) in distinguishing $\vec{z} \in \mathbb{G}$ from $\vec{z} \in \mathbb{H}^{(s)}$. See [9] for a formal definition.

Theorem 3. *Let $n = \ell + 1$ and $\mathcal{D}_{n,\ell}$ be a polynomially induced matrix distribution which is not redundant. Let $(\mathcal{MG}_k, \mathbb{H}, G^n, G_T^m, \tilde{e})$ be the output of some projecting $(k, \mathcal{D}_{n,\ell})$ multilinear map generator with a fixed multilinear map. Then, $m \geq \ell k + 1$.*

Note that the projecting pairing based on the polynomial viewpoint of the ℓ-SCasc-assumption reaches this bound and is hence optimal.

Proof. We may identify G^n with some subspace $V \subset \mathbb{Z}_p[\vec{X}]$ of dimension n (see [9] for details). By Theorem 2 above, we may assume w.l.o.g. that $\tilde{e}$ is polynomial multiplication, as this only makes m smaller. Hence we can also identify G_T^m with some subspace $W \subset \mathbb{Z}_p[\vec{X}]$ of dimension m. Let $>$ be any monomial ordering on $\mathbb{Z}_p[\vec{X}]$. Let $\mathfrak{q}_0, \ldots, \mathfrak{q}_\ell$ be a basis of V in echelon form with respect to $>$. This implies that the leading monomials satisfy $\mathrm{LM}(\mathfrak{q}_0) > \ldots > \mathrm{LM}(\mathfrak{q}_\ell)$. Now consider the elements

$$\begin{array}{llcl}
\mathfrak{q}_0^k = \mathfrak{r}_0 = \mathfrak{q}_0 \cdots \mathfrak{q}_0 \mathfrak{q}_0 & & & \\
\mathfrak{r}_1 = \mathfrak{q}_0 \cdots \mathfrak{q}_1 \mathfrak{q}_0 & \mathfrak{r}_{\ell+1} = \mathfrak{q}_0 \cdots \mathfrak{q}_0 \mathfrak{q}_1 \mathfrak{q}_\ell & \cdots & \mathfrak{r}_{(k-1)\ell+1} = \mathfrak{q}_0 \mathfrak{q}_\ell \cdots \mathfrak{q}_\ell \\
\vdots & \vdots & & \vdots \\
\mathfrak{r}_\ell = \mathfrak{q}_0 \cdots \mathfrak{q}_0 \mathfrak{q}_\ell & \mathfrak{r}_{2\ell} = \mathfrak{q}_0 \cdots \mathfrak{q}_0 \mathfrak{q}_\ell \mathfrak{q}_\ell & \cdots & \mathfrak{r}_{\ell k} = \mathfrak{q}_\ell \mathfrak{q}_\ell \cdots \mathfrak{q}_\ell
\end{array}$$

(the definition of $\mathfrak{r}_{i+1}$ differs from that of $\mathfrak{r}_i$ in one single index being greater by one). It holds that all $\mathfrak{r}_i \in W$ by construction and $\mathrm{LM}(\mathfrak{r}_0) > \mathrm{LM}(\mathfrak{r}_1) > \ldots > \mathrm{LM}(\mathfrak{r}_{\ell k})$ by the properties of a monomial order. Hence, the $\mathfrak{r}_i$ are linearly independent, showing $m = \dim W \geq \ell k + 1$.

6 Review of Previous Results in our Framework

Let us consider some previous results using the language introduced in Section 3.

Projecting Pairings. Implicitly, in [8], Groth and Sahai were using the fact that the bilinear symmetric tensor product is a projecting map. Subsequently, Seo [14] constructed an improved symmetric projecting pairing which he claimed to be optimal in terms of image size and operations.

Theorem 4. *([14]) Let $\mathcal{G}_{2,\mathcal{U}_\ell}$ be any (symmetric) projecting $(2, \mathcal{U}_\ell)$ bilinear map generator with output $(\mathcal{MG}_2, \mathbb{H}, \mathbb{G}, G_T^m, \tilde{e})$. Then (a) we have $m \geq (\ell+1)(\ell+2)/2$, and (b) the map $\tilde{e}$ cannot be evaluated with less than $(\ell+1)^2$ prime-order pairing operations.*

Using the polynomial point of view, we prove in [9] that polynomial multiplication is optimal for *any* $\mathcal{D}_\ell$ assumption, and thus cover Theorem 4 (a) as a special case when $\mathcal{D}_\ell = \mathcal{U}_\ell$. On the other hand, the polynomial viewpoint immediately suggests a method to evaluate Seo's pairing with m (less than $(\ell+1)^2$) prime-order pairing operations, refuting Theorem 4 (b).[6] Further, our results also answer in the affirmative an open question raised by Seo about the existence of more efficient pairings outside of the model. Our construction of a k-linear map based on k-SCasc beats this lower bound and is much more efficient asymptotically in k.

[6] In [9] we discuss in more detail Seo's construction and the reason why Theorem 4 (b) is false.

Cancelling and Projecting Pairings. In his original paper [6], Freeman gives several constructions of bilinear pairings which are either projecting or canceling — but not both. Subsequently, Meiklejohn *et al.* [13] give evidence that it might be hard to obtain both features simultaneously:

Theorem 5. *([13]) Any symmetric* $(2,\mathcal{U}_\ell)$ *bilinear generator with a fixed pairing cannot be simultaneously projecting and canceling, except with negligible probability (over the output of the generator).*[7]

In [9] we show that this result can be extended to any $(2,\mathcal{L}_\ell)$ and any $(2,\mathcal{SC}_2)$ bilinear generator. It remains an open question if the impossibility results extend to $(2,\mathcal{SC}_\ell)$, for $\ell > 2$.

With these impossibility results, it is not surprising that all canceling and projecting constructions are for *non-fixed* pairings in the sense of Definition 6. Indeed, in [15] Cheon and Seo construct a pairing which is both canceling and projecting but not fixed since, implicitly, the group $\mathbb{G}$ depends on the hidden subgroup $\mathbb{H}$. In our language, the pairing of Seo and Cheon is a $(2,(r=\ell^2,n=\ell+1,\ell))$ pairing, i.e., $\mathbb{G} \subset G^{\ell^2}$ of dimension $n=\ell+1$. Recently, Lewko and Meiklejohn [12] simplified this construction, obtaining a $(2,(r=2\ell,n=\ell+1,\ell))$ bilinear map generator. In [9] we also construct a $(2,(r=2\ell,n=\ell+1,\ell))$ pairing achieving both properties (and which generalizes to any $(k,(r=2\ell,n=\ell+1,\ell))$ with $\ell \geq k$) , but using completely different techniques. A direct comparison of [15], [12] with our pairing is not straightforward, since in fact they use dual vector spaces techniques and their pairing is not really symmetric.

7 A Direct Application: More Efficient Groth-Sahai Proofs

Using our projecting pairing from Section 4.1, we can improve the performance of Groth-Sahai proofs by almost halving the number of required prime-order pairing operations for verification (cf. Table 1). Additionally, in [9], we show how to implement a k-linear variant of the Boneh-Goh-Nissim encryption scheme [2] using the projecting multilinear map generator $\mathcal{G}_{k,\mathcal{SC}_k}$.

Groth-Sahai proofs [8] are the most natural application of projecting bilinear maps. They admit various instantiations in the prime-order setting. It follows easily from the original formulation of Groth and Sahai that their proofs can be instantiated based on any $\mathcal{D}_{n,\ell}$ assumption and any fixed projecting map. Details are given in [5] but only for the projecting pairing corresponding to the symmetric bilinear tensor product. The generalization to any projecting pairing is straightforward.

The important parameters for efficiency of NIZK proofs are the size of the common reference string, the proof size and the verification cost. The proof size

[7] Their claim is that it is impossible to achieve both properties under what they call a "natural use" of the ℓ-Lin assumption, although, they are actually using the uniform assumption.

(for a given equation) depends only on the size of the matrix assumption, i.e., on n, ℓ, so it is omitted in our comparison. The size of the common reference string depends essentially on the size of the commitment key, which is $n + \mathrm{Re}_{\mathbb{G}}(\mathcal{D}_{n,\ell})$, where $\mathrm{Re}_{\mathbb{G}}(\mathcal{D}_{n,\ell})$ is the representation size of the matrix assumption $\mathcal{D}_{n,\ell}$, which is 1 for ℓ-SCasc, ℓ for ℓ-Lin and $(\ell+1)\ell$ for $\mathcal{U}_\ell$. Therefore, the ℓ-SCasc instantiation is the most advantageous from the point of view of the size of the common reference string (regardless of the pairing used), as pointed out in [5].

On the other hand, the choice of the pairing affects only the cost of verification[8]. Except for some restricted type of linear equations, verification involves several evaluations of $\tilde{e}$. In our most efficient construction, for each pairing evaluation $\tilde{e}$, we save, according to Table 1, at least 4 prime-order pairing evaluations. For instance, this leads to a saving of 12 pairing evaluations for proving that a committed value is a bit $b \in \{0, 1\}$.

Acknowledgements

We would like to thank the anonymous reviewers for very helpful and constructive comments. This work has been supported in part by DFG grant GZ HO 4534/4-1. Carla Ràfols was supported by a Sofja Kovalevskaja Award of the Alexander von Humboldt Foundation and the German Federal Ministry for Education and Research.

References

[1] Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer (Aug 2004)

[2] Boneh, D., Goh, E.J., Nissim, K.: Evaluating 2-DNF formulas on ciphertexts. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 325–341. Springer (Feb 2005)

[3] Coron, J.S., Lepoint, T., Tibouchi, M.: Practical multilinear maps over the integers. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 476–493. Springer (Aug 2013)

[4] Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory 22(6), 644–654 (1976)

[5] Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 129–147. Springer (Aug 2013)

[6] Freeman, D.M.: Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 44–61. Springer (May 2010)

[7] Garg, S., Gentry, C., Halevi, S.: Candidate multilinear maps from ideal lattices. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 1–17. Springer (May 2013)

[8] This is not exactly true, in fact, with the improved pairing for SCasc the prover needs to compute an additional 4 group operations, see the discussion in [9].

[8] Groth, J., Sahai, A.: Efficient noninteractive proof systems for bilinear groups. SIAM J. Comput. 41(5), 1193–1232 (2012)

[9] Herold, G., Hesse, J., Hofheinz, D., Ràfols, C., Rupp, A.: Polynomial spaces: A new framework for composite-to-prime-order transformations. Cryptology ePrint Archive (2014), http://eprint.iacr.org/

[10] Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer (Apr 2008)

[11] Lewko, A.B.: Tools for simulating features of composite order bilinear groups in the prime order setting. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 318–335. Springer (Apr 2012)

[12] Lewko, A.B., Meiklejohn, S.: A profitable sub-prime loan: Obtaining the advantages of composite-order in prime-order bilinear groups. IACR Cryptology ePrint Archive 2013, 300 (2013)

[13] Meiklejohn, S., Shacham, H., Freeman, D.M.: Limitations on transformations from composite-order to prime-order groups: The case of round-optimal blind signatures. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 519–538. Springer (Dec 2010)

[14] Seo, J.H.: On the (im)possibility of projecting property in prime-order setting. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 61–79. Springer (Dec 2012)

[15] Seo, J.H., Cheon, J.H.: Beyond the limitation of prime-order bilinear groups, and round optimal blind signatures. In: Cramer, R. (ed.) TCC 2012. LNCS, vol. 7194, pp. 133–150. Springer (Mar 2012)

[16] Shoup, V.: Lower bounds for discrete logarithms and related problems. In: Fumy, W. (ed.) EUROCRYPT'97. LNCS, vol. 1233, pp. 256–266. Springer (May 1997)

[17] Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer (Aug 2009)