# On the (Im)possibility of Projecting Property in Prime-Order Setting

Jae Hong Seo

National Institute of Information and Communications Technology,
4-2-1, Nukui-kitamachi, Koganei, Tokyo, 184-8795, Japan
jaehong@nict.go.jp

**Abstract.** Projecting bilinear pairings have frequently been used for designing cryptosystems since they were first derived from composite order bilinear groups. There have been only a few studies on the (im)possibility of projecting bilinear pairings. Groth and Sahai showed that projecting bilinear pairings can be achieved in the prime-order group setting. They constructed both projecting *asymmetric* bilinear pairings and projecting *symmetric* bilinear pairings, where a bilinear pairing $e$ is symmetric if it satisfies $e(g, h) = e(h, g)$ for any group elements $g$ and $h$; otherwise, it is asymmetric.

In this paper, we provide impossibility results on projecting bilinear pairings in a prime-order group setting. More precisely, we specify the lower bounds of

1. the image size of a projecting asymmetric bilinear pairing
2. the image size of a projecting symmetric bilinear pairing
3. the computational cost for a projecting asymmetric bilinear pairing
4. the computational cost for a projecting symmetric bilinear pairing

in a prime-order group setting naturally induced from the $k$-linear assumption, where the computational cost means the number of generic operations.

Our lower bounds regarding a projecting asymmetric bilinear pairing are tight, i.e., it is impossible to construct a more efficient projecting asymmetric bilinear pairing than the constructions of Groth-Sahai and Freeman. However, our lower bounds regarding a projecting symmetric bilinear pairing differ from Groth and Sahai's results regarding a symmetric bilinear pairing results; We fill these gaps by constructing projecting symmetric bilinear pairings.

In addition, on the basis of the proposed symmetric bilinear pairings, we construct more efficient instantiations of cryptosystems that essentially use the projecting symmetric bilinear pairings in a modular fashion. Example applications include new instantiations of the Boneh-Goh-Nissim cryptosystem, the Groth-Sahai non-interactive proof system, and Seo-Cheon round optimal blind signatures proven secure under the DLIN assumption. These new instantiations are more efficient than the previous ones, which are also provably secure under the DLIN assumption. These applications are of independent interest.

## 1 Introduction

A bilinear group is a tuple of abelian groups with a non-degenerate bilinear pairing. Projecting bilinear pairings, which are bilinear pairings with homomorphisms that satisfy a commutative property, have frequently been used for designing cryptosystems since they were first derived from composite order bilinear groups [10], though Freeman identified and named the projecting property recently [15]. Of special interest is the Groth-Sahai non-interactive proof system [22] and the Boneh-Goh-Nissim cryptosystem [10], both of which essentially use the projecting property and have numerous applications in various fields in cryptography. For example, the Groth-Sahai proofs were used to construct ring signatures [13], group signatures [19], round optimal blind signatures [25], verifiable shuffles [20], a universally composable adaptive oblivious transfer protocol [18], a group encryption scheme [12], anonymous credentials [7, 6], and malleable proof systems [14]. For its part, the Boneh-Goh-Nissim cryptosystem was used for designing private searching on streaming data [31], non-interactive zero-knowledge [21], shuffling [5], and privacy-preserving set operations [32].

**(Im)possibility of Projecting Bilinear Pairings:** Although the projecting bilinear pairings are often used for designing various cryptosystems, there have been only a few studies on the (im)possibility of projecting bilinear pairings. Groth and Sahai [22] demonstrated that projecting bilinear pairings can be achieved in the prime-order group setting. They provided two distinct constructions in prime-order group setting: projecting *asymmetric* bilinear pairings and projecting *symmetric* bilinear pairings, where a bilinear pairing $e$ is symmetric if it satisfies $e(g, h) = e(h, g)$ for any group elements $g$ and $h$; otherwise, it is asymmetric. On the basis of this idea of projecting bilinear pairings, they developed non-interactive proof systems for quadratic equations over modules that can be instantiated in composite-order bilinear groups, product groups of prime-order bilinear groups with asymmetric bilinear pairings, and product groups of prime-order groups with symmetric bilinear pairings. By extending Groth-Sahai's idea, Freeman [15] generalized Groth-Sahai's projecting asymmetric bilinear pairings.[1] Groth-Sahai and Freeman's constructions of projecting bilinear pairings allow for the simultaneous treatment of subgroup indistinguishability. To use projecting bilinear pairings for designing cryptographic protocols, we need to deal with cryptographic assumptions such as subgroup decision assumption at the same time. Meiklejohn, Shacham, and Freeman [25] have shown some impossibility results for projecting bilinear pairings, e.g., that projecting bilinear pairings cannot simultaneously have a cancelling property if the subgroup indistinguishability is naturally induced from the $k$-linear assumption [23, 36]. Recently, Seo and Cheon [35] proved that bilinear pairings can be simultaneously projecting and

[1] Freeman identified the other property of bilinear pairings in a composite-order group setting, called *cancelling*, and demonstrated how to achieve the cancelling bilinear pairings in the prime-order group setting.

cancelling when the subgroup decision assumption holds in the generic group model.[2]

**Contribution:** In this paper, our contribution is a two-fold. First, we aim to answer the fundamental question how efficient constructions for projecting bilinear pairing can be. Second, we propose a construction of projecting symmetric bilinear pairings that can achieve the efficiency of our lower bounds and then provide several constructions of cryptosystems based on the proposal in a modular fashion.

We focus on constructions only in the prime-order bilinear group setting since this type of group usually supports more efficient (group and bilinear pairing) operations than those in composite-order bilinear groups (see [15] for a detailed comparison of composite and prime-order groups). We present several impossibility results of the projecting bilinear pairings in a prime-order group setting. More precisely, we specify the lower bound of

1. the image size of a projecting asymmetric bilinear pairing
2. the image size of a projecting symmetric bilinear pairing
3. the computational cost for a projecting asymmetric bilinear pairing, and
4. the computational cost for a projecting symmetric bilinear pairing

in a prime-order group setting naturally induced from the decisional Diffie-Hellman (DDH) assumption, the decisional linear (DLIN) assumption, and the $k$-linear assumption, where the computational cost means the number of generic operations. In this paper, we restrict ourselves to a consideration of a framework in which the subgroup indistinguishability in the framework relies in a natural way on simple assumptions (i.e., the DDH, DLIN, and $k$-linear assumption). This framework covers all previous constructions by Groth-Sahai and Freeman, and this restriction on the framework has already been used in [25] to show another impossibility result on projecting bilinear pairings. As for the computational cost of projecting bilinear pairings, we consider a slightly restricted computational model since there are typically several ways to perform a given operation, which makes it very difficult to compare all possible (even unknown) ways. We have two basic assumption in our computational model. First, we only count the number of generic operations of the underlying elliptic curve group and the pairings − that is, we assume that one cannot utilize information about the representation of groups and bilinear pairing operations [37, 8]. Second, we assume that two inputs of a projecting bilinear pairing are uniformly and independently chosen. In special cases, an additional information about two inputs may lead to an efficient alternative way of computing a pairing operation. For example, when one computes $e(g_1, g_2)$ for the two given inputs $g_1$ and $g_2$, where $e : G \times G \to G_t$ is a pairing, if we knows $e(g, g)$, $a_1$ and $a_2$ such that $g_1 = g^{a_1}$ and $g_2 = g^{a_2}$ for a generator $g$ of $G$, then we can perform one field multiplication and one exponentiation in $G_t$ instead of performing $e$ for $e(g_1, g_2) = e(g, g)^{a_1 a_2}$. Since we want to

[2] Seo and Cheon's result does not contradict Meiklejohn et al.'s result. Rather, they showed that there is a more general class of bilinear groups than Meiklejohn et al. considered and that some of theses can be both cancelling and projecting.

consider the computational cost of $e$ in general, that is, without any additional information aside from the original two inputs, we assume that two inputs are uniformly and independently distributed in their respective domains: Hence, our computational model rules out special cases like the above example. Although our computational model does not perfectly correspond to the real world, we believe that its lower computational bounds can aid our understanding of the projecting property and enable us to locate efficient constructions for projecting bilinear pairings.

In this study, our lower bounds imply that Freeman's construction of projecting asymmetric bilinear pairings is optimal: that is, it is the most efficient construction for projecting asymmetric bilinear pairings [15]. In contrast, our lower bounds for the projecting symmetric bilinear pairing are different from those of Groth-Sahai [22]. We fill these gaps by constructing projecting symmetric bilinear pairings and demonstrating that our construction can achieve an efficiency coincident with the lower bounds.

The proposed projecting symmetric bilinear pairings can be used to create more efficient instantiations of cryptosystems, which essentially use projecting property and symmetric bilinear pairings, in a modular fashion. To show that the proposed projecting symmetric bilinear pairings can be adapted to various cryptosystems, we apply them to three distinct cryptosystems and create new efficient instantiations of the Groth-Sahai non-interactive proof system [22], the Boneh-Goh-Nissim cryptosystem [10], and Seo-Cheon round optimal blind signatures [35] that are provably secure under the DLIN assumption.[3] The proposed instantiation of the non-interactive proof system has a faster verification than Groth-Sahai's instantiation based on the DLIN assumption, and the proposed instantiation of the Boneh-Goh-Nissim cryptosystem has a smaller ciphertext size and a faster decryption algorithm than Freeman's instantiation based on the DLIN assumption. We can also reduce the verification costs of the Seo-Cheon round optimal blind signatures. These applications are of independent interest. Our new instantiation is based on the DLIN assumption so that we can improve the efficiency of all subsequent protocols using Groth-Sahai's instantiation 3 (based on the DLIN assumption).

We should note here that symmetric bilinear pairings require the use of supersingular elliptic curves and thus the associated bilinear groups are larger than those with asymmetric bilinear pairings using ordinary curves (please see [16] for a detailed comparison). However, some constructions of pairing-based cryptosystems essentially use the symmetric property of bilinear pairings (e.g., Groth-Ostrovsky-Sahai zero-knowledge proofs [21]). Therefore, the proposed projecting symmetric bilinear pairings can be used for designing such cryptosystems.

[3] The Seo-Cheon round optimal blind signature scheme can be considered a prime order group version of the Meiklejohn-Shacham-Freeman round optimal blind signature scheme in composite order groups [25]. Since we only consider prime order group settings in this paper, we provide a new instantiation of the Seo-Cheon scheme instead of the Meiklejohn-Shacham-Freeman scheme.

**Modular Approach in Cryptography:** Generally speaking, a modular approach for cryptosystems leads to a simple design but inefficient constructions in comparison to an ad hoc approach. Recently, we have found a few exceptions for structure preserving cryptography [1, 2, 11] and mathematical structures [26, 27]. Structure preserving schemes enable one to construct modular protocols while preserving conceptual simplicity and yielding reasonable efficiency at the same time. Structure-preserving signatures, commitments [1], and encryptions [11] restrict all components in schemes to group elements, so schemes can easily be combined with Groth-Sahai proofs [22]. In a modular fashion, round optimal blind signatures, group signatures, and anonymous proxy signatures can be derived from structure preserving signatures, and oblivious trusted third parties can be achieved due to the structure preserving encryptions. There has been some impossibility results for structure preserving cryptography [2–4]. These save our efforts in terms of impossible goals and widen our understanding regarding modular constructions.

Okamoto and Takashima [26] introduced a mathematical structure called "dual pairing vector spaces" that can be instantiated using a product of bilinear groups or a Jacobian variety of a supersingular curve of genus $\geq 1$. On the basis of these dual pairing vector spaces, a homomorphic encryption scheme [26], functional encryption scheme [27, 28, 30], attribute-based signature scheme [29], and (hierarchical) identity-based encryption scheme [24] have been proposed.

**Open Problem:** It would be interesting to extend the (im)possibility of the projecting property into a wider framework than ours. Furthermore, finding other applications of projecting pairings is also interesting.

**Road Map:** In Section 2, we give definitions for bilinear groups, projecting property, and cryptographic assumptions. In Section 3, we explain our impossibility results of projecting bilinear pairings. In Section 4, we show the optimality of Groth-Sahai and Freeman's projecting asymmetric bilinear pairings and give our construction for optimal projecting symmetric bilinear pairings. In Section 5, we apply the proposed projecting symmetric bilinear pairings to three distinct cryptosystems, the Groth-Sahai non-interactive proof system, the Boneh-Goh-Nissim cryptosystem, and the Seo-Cheon round optimal blind signatures.

## 2 Definition

We use notation $x \xleftarrow{\$} A$ to mean that, if $A$ is a finite group $\mathbb{G}$, an element $x$ is uniformly chosen from $\mathbb{G}$, and, if $A$ is an algorithm, $A$ outputs $x$ by using its own random coins. We use $[i, j]$ to denote a set of integers $\{i, \ldots, j\}$, $\langle g_1, \ldots, g_n \rangle$ to denote a group generated by $g_1, \ldots, g_n$, and $\mathbb{F}_p$ to denote a finite field of prime order $p$. For a map $\tau : T_D \rightarrow T_R$, and any subset $S_D$ of $T_D$, $\tau(S_D) := \{\tau(s) | s \in S_D\}$. All values in our paper are outputs of some functions taking the security parameter $\lambda$ and $\approx$ denotes the difference between both sides is a negligible function in $\lambda$.

We use two commonly used mathematical notations *internal direct sum*, denoted by $\oplus$, and *tensor product (Kronecker product)*, denoted by $\otimes$. For an abelian group $G$, if $G_1$ and $G_2$ are subgroups of $G$ such that $G = G_1 + G_2 = \{g_1 \cdot g_2 | g_1 \in G_1, g_2 \in G_2\}$ and $G_1 \cap G_2 = \{1_G\}$ for the identity $1_G$ of $G$, then we write $G = G_1 \oplus G_2$. If $A = (a_{i,j})$ is a $m_1 \times m_2$ matrix and $B = (b_{i,j})$ is an $\ell_1 \times \ell_2$ matrix, the *tensor product* $A \otimes B$ is the $m_1\ell_1 \times m_2\ell_2$ matrix whose $(i,j)$-th block is $a_{i,j}B$, where we consider $A \otimes B$ as $m_1 \times m_2$ blocks. That is,

$$A \otimes B = \begin{bmatrix} a_{1,1}B & \dots & a_{1,m_2}B \\ \vdots & \ddots & \vdots \\ a_{m_1,1}B & \dots & a_{m_1,m_2}B \end{bmatrix} \in Mat_{m_1\ell_1 \times m_2\ell_2}(\mathbb{F}_p).$$

We use several properties of the internal direct sum and tensor product. Every element $g$ in $G$ has a unique representation if $G = G_1 \oplus G_2$. That is, $g \in G$ can be uniquely written as $g = g_1 g_2$ for some $g_1 \in G_1$ and $g_2 \in G_2$. If two matrices $A$ and $B$ are invertible, then $A \otimes B$ is also invertible and the inverse is given by $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$. The transposition operation is distributive over the tensor product. That is, $(A \otimes B)^t = A^t \otimes B^t$. We sometimes consider a vector over $\mathbb{F}_p$ as a matrix with one row.

### 2.1 Bilinear Groups and Projecting Bilinear Pairings

**Definition 1** *Let $\mathcal{G}$ be an algorithm that takes as input the security parameter $\lambda$. We say that $\mathcal{G}$ is a* bilinear group generator *if $\mathcal{G}$ outputs a description of five finite abelian groups $(G, G_1, H, H_1,$ and $G_t)$ and a map $e$ such that $G_1 \subset G$, $H_1 \subset H$, and $e : G \times H \to G_t$ is a non-degenerate bilinear pairing; that is, it satisfies*

- *Bilinearity: $e(g_1g_2, h_1h_2) = e(g_1,h_1)e(g_1,h_2)e(g_2,h_1)e(g_2,h_2)$ for $g_1, g_2 \in G$ and $h_1, h_2 \in H$,*
- *Non-degeneracy: for $g \in G$, if $e(g,h) = 1\ \forall h \in H$, then $g = 1$. Similarly, for $h \in H$, if $e(g,h) = 1\ \forall g \in G$, then $h = 1$.*

*In addition, we assume that group operations in each group ($G$, $H$, and $G_t$), bilinear pairing computations, random samplings from each group, and membership-check in each group are efficiently computable (i.e., polynomial time in $\lambda$).*
*If the order of output groups of $\mathcal{G}$ is prime $p$, we call $\mathcal{G}$ a* bilinear group generator of prime order *and say $\mathcal{G}_1 \xrightarrow{\$} (p, \mathbb{G}, \mathbb{H}, \mathbb{G}_t, \hat{e})$; that is, $\mathbb{G}$, $\mathbb{H}$ and $\mathbb{G}_t$ are finite abelian groups of prime order $p$.*
*If $G = H$, $G_1 = H_1$, and $e(g,h) = e(h,g)$ for all $g, h \in G$, we say that $\mathcal{G}$ is symmetric. Otherwise, we say that $\mathcal{G}$ is asymmetric.*

We define the projecting property of a bilinear pairings.

**Definition 2** *Let $\mathcal{G}$ be a bilinear group generator, and $\mathcal{G} \xrightarrow{\$} (G, G_1, H, H_1, G_t, e)$. We say that $\mathcal{G}$ is projecting if there exist a subgroup $G_t' \subset G_t$ and three homomorphisms $\pi : G \to G$, $\bar{\pi} : H \to H$, and $\pi_t : G_t \to G_t$ such that*

1. $\pi(G) \neq \{1_G\}$, $\bar{\pi}(H) \neq \{1_H\}$, *and* $\pi_t(e(G,H)) \neq \{1_t\}$, *where* $1_G$, $1_H$, *and* $1_t$ *are identities of* $G$, $H$, $G_t$, *respectively.*
2. $G_1 \subset \ker(\pi)$, $H_1 \subset \ker(\bar{\pi})$, *and* $G_t' \subset \ker(\pi_t)$.
3. $\pi_t(e(g,h)) = e(\pi(g), \bar{\pi}(h))$ *for all* $g \in G$ *and* $h \in H$.

*If* $\mathcal{G}$ *is symmetric, set* $\pi = \bar{\pi}$.

Note that in Definition 2 we slightly revised Freeman's original projecting definition to fit our purpose. First, we added a requirement for homomorphisms to be non-trivial (first condition of Definition 2). If we allowed trivial homomorphisms, they would satisfy the projecting property. Since trivial homomorphisms may not be helpful in designing cryptographic protocols, our modification is quite reasonable. Second, our definition requires only the existence of $G_t'$ and homomorphisms while Freeman required them to be output [15]. Since our definition is weaker than Freeman's (if we ignore our first modification), our main results (the lower bounds and optimal construction) are meaningful. Several other researchers [25, 24] have used an existence definition like ours instead of Freeman's definition for the projecting property.

### 2.2 Subgroup Decision Assumption and $k$-Linear Assumption

Here we define *subgroup decision problem* and *subgroup decision assumption* in the bilinear group setting, which were introduced by Freeman [15].

**Definition 3** *Let* $\mathcal{G}$ *be a bilinear group generator. We define the advantage of an algorithm* $\mathcal{A}$ *in solving the* subgroup decision problem on the left*, denoted by* $Adv^{SDP_L}_{\mathcal{A},\mathcal{G}}(\lambda)$*, as*

$$\Big| \Pr\left[\mathcal{A}(G, G_1, H, H_1, G_t, e, g) \to 1 \,|\, (G, G_1, H, H_1, G_t, e) \xleftarrow{\$} \mathcal{G}(\lambda), g \xleftarrow{\$} G\right] - \Pr\left[\mathcal{A}(G, G_1, H, H_1, G_t, e, g_1) \to 1 \,|\, (G, G_1, H, H_1, G_t, e) \xleftarrow{\$} \mathcal{G}(\lambda), g_1 \xleftarrow{\$} G_1\right] \Big|.$$

*We say that* $\mathcal{G}$ *satisfies the subgroup decision assumption on the left if, for any PPT algorithm* $\mathcal{A}$*, its* $Adv^{SDP_L}_{\mathcal{A},\mathcal{G}}(\lambda)$ *is a negligible function of the security parameter* $\lambda$.

We analogously define the *subgroup decision problem on the right*, the advantage $Adv^{SDP_R}_{\mathcal{A},\mathcal{G}}$ of $\mathcal{A}$, and the *subgroup decision assumption on the right* by using $H$ and $H_1$ instead of $G$ and $G_1$.

**Definition 4** *We say that a bilinear group generator* $\mathcal{G}$ *satisfies the subgroup decision assumption if* $\mathcal{G}$ *satisfies both the subgroup decision assumptions on the left and subgroup decision assumptions on the right.*

For a subgroup decision assumption in the prime-order group setting, we use the widely-known k-linear assumption which is introduced by Hofheinz and Kiltz and Shacham [23, 36], in the bilinear group setting. We give the formal definition of $k$-linear assumption below.

**Definition 5** *Let $\mathcal{G}_1$ be a bilinear group generator of prime order and $k \geq 1$. We define the advantage of an algorithm $\mathcal{A}$ in solving the k-linear problem in $\mathbb{G}$, denoted by $Adv^{k\text{-}Lin_{\mathbb{G}}}_{\mathcal{A},\mathcal{G}_1}(\lambda)$, to be*

$$\Big| \Pr\Big[\mathcal{A}(\mathbb{G},\mathbb{H},\mathbb{G}_t,e,\mathfrak{g},\mathfrak{u}_i,\mathfrak{u}_i^{a_i},\mathfrak{g}^b,\mathfrak{h} \text{ for } i\in[1,k]) \to 1 | \\ (\mathbb{G},\mathbb{H},\mathbb{G}_t,e) \xleftarrow{\$} \mathcal{G}_1(\lambda), \mathfrak{g},\mathfrak{u}_i \xleftarrow{\$} \mathbb{G}, \mathfrak{h} \xleftarrow{\$} \mathbb{H}, a_i \xleftarrow{\$} \mathbb{F}_p \text{ for } i\in[1,k], b \xleftarrow{\$} \mathbb{F}_p\Big] \\ - \Pr\Big[\mathcal{A}(\mathbb{G},\mathbb{H},\mathbb{G}_t,e,\mathfrak{g},\mathfrak{u}_i,\mathfrak{u}_i^{a_i},\mathfrak{g}^b,\mathfrak{h} \text{ for } i\in[1,k]) \to 1| \\ (\mathbb{G},\mathbb{H},\mathbb{G}_t,e) \xleftarrow{\$} \mathcal{G}_1(\lambda), \mathfrak{g},\mathfrak{u}_i \xleftarrow{\$} \mathbb{G}, \mathfrak{h} \xleftarrow{\$} \mathbb{H}, a_i \xleftarrow{\$} \mathbb{F}_p \text{ for } i\in[1,k], b = \textstyle\sum_{i\in[1,k]} a_i\Big]\Big|.$$

*Then, we say that $\mathcal{G}_1$ satisfies the k-linear assumption in $\mathbb{G}$ if for any PPT algorithm $\mathcal{A}$, $Adv^{k\text{-}Lin_{\mathbb{G}}}_{\mathcal{A},\mathcal{G}_1}(\lambda)$ is a negligible function of the security parameter.*

We can analogously define the k-linear assumption in $\mathbb{H}$. The 1-linear assumption in $\mathbb{G}$ is the DDH assumption in $\mathbb{G}$ and the 2-linear assumption in $\mathbb{G}$ is the decisional linear assumption in $\mathbb{G}$ [9].

## 3 Impossibility Results of Projecting Bilinear Pairings

In this section, we first formally define natural product groups of prime-order bilinear groups. Next, we derive conditions for projecting bilinear groups, and then provide our impossibility results of projecting bilinear pairings. We begin by defining some notations that will help us to simplify explanations. For group elements $\mathfrak{g},\mathfrak{g}_1,\ldots,\mathfrak{g}_{k+1} \in \mathbb{G}$, a vector $\overrightarrow{\alpha} = (a_1,\ldots,a_{k+1}) \in \mathbb{F}_p^{k+1}$, and a matrix $M = (m_{i,j}) \in Mat_{(k+1)\times(k+1)}(\mathbb{F}_p)$, we use the notation

$$\mathfrak{g}^{\overrightarrow{\alpha}} := (\mathfrak{g}^{a_1},\ldots,\mathfrak{g}^{a_{k+1}}) \in \mathbb{G}^{k+1}$$

and

$$(\mathfrak{g}_1,\ldots,\mathfrak{g}_{k+1})^M := (\prod_{i\in[1,k+1]} \mathfrak{g}_i^{m_{i,1}},\ldots,\prod_{i\in[1,k+1]} \mathfrak{g}_i^{m_{i,k+1}}).$$

From this notation, we can easily obtain $(\mathfrak{g}^{\overrightarrow{\alpha}})^M = \mathfrak{g}^{(\overrightarrow{\alpha}M)}$.

### 3.1 Bilinear Groups Naturally Induced from *k*-linear Assumption

In Figure 1, we provide a generator $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ for $A_\ell \in Mat_{(k+1)\times(k+1)}(\mathbb{F}_p)$ and $\ell \in [1,m]$. When we refer to the natural construction of product groups of prime-order bilinear groups such that the subgroup decision assumption "naturally" follows from the $k$-linear assumption, we mean $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$.[4] When we

[4] Meiklejohn et al. [25] also used the word "natural" to refer to $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$. They used $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ to show the limitation result of both projecting and cancelling: They showed that for any $A_\ell$ matrices used in $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$, $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ cannot be both projecting and cancelling with overwhelming probability, where the probability goes over the randomness used in $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$.

1. $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ takes the security parameter $\lambda$ as input.
2. Run $\mathcal{G}_1(\lambda) \to (p, \mathbb{G}, \mathbb{H}, \mathbb{G}_t, \hat{e})$.
3. Define $G = \mathbb{G}^{k+1}$, $H = \mathbb{H}^{k+1}$, and $G_t = \mathbb{G}_t^m$.
4. Randomly choose $\overrightarrow{x}_1, \ldots, \overrightarrow{x}_k, \overrightarrow{y}_1, \ldots, \overrightarrow{y}_k \in \mathbb{F}_p^{k+1}$ such that the set $\{\overrightarrow{x}_i\}_{i\in[1,k]}$ and $\{\overrightarrow{y}_i\}_{i\in[1,k]}$ are each linearly independent.
5. Randomly choose generators $\mathfrak{g} \in \mathbb{G}$ and $\mathfrak{h} \in \mathbb{H}$, and let $G_1 = \langle \mathfrak{g}^{\overrightarrow{x}_1}, \ldots, \mathfrak{g}^{\overrightarrow{x}_k} \rangle$ and $H_1 = \langle \mathfrak{h}^{\overrightarrow{y}_1}, \ldots, \mathfrak{h}^{\overrightarrow{y}_k} \rangle$.
6. Define a map $e : G \times H \to G_t$ as an $m$-tuple of maps $e(\cdot,\cdot)_\ell$ for $\ell \in [1, m]$ as follows:
$$e((\mathfrak{g}_1, \ldots, \mathfrak{g}_{k+1}), (\mathfrak{h}_1, \ldots, \mathfrak{h}_{k+1}))_\ell := \prod_{i,j\in[1,k+1]} \hat{e}(\mathfrak{g}_i, \mathfrak{h}_j)^{a_{i,j}^{(\ell)}},$$
where $A_\ell = (a_{ij}^{(\ell)}) \in Mat_{(k+1)\times(k+1)}(\mathbb{F}_p)$ for $\ell \in [1, m]$.
7. Output description of $(p, G, G_1, H, H_1, G_t, e)$; each group description has its generators only. (e.g., $G_1$'s description has $\mathfrak{g}^{\overrightarrow{x}_1}, \ldots, \mathfrak{g}^{\overrightarrow{x}_k}$, but $\overrightarrow{x}_i$ is not contained in the description of $G_1$.)

**Fig. 1.** Description of $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$

consider the subgroup decision assumption, which is induced from the $k$-linear assumption, to mean that, given $g$, it is hard to determine if $g \xleftarrow{\$} G_1$ or $g \xleftarrow{\$} G$, $G$ is a rank-$(k+1)$ $\mathbb{F}_p$-module, and $G_1$ is a randomly chosen rank-$k$ submodule of $G$. For any matrices $A_1, \ldots, A_m$ in $Mat_{(k+1)\times(k+1)}(\mathbb{F}_p)$, a group generator $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ satisfies the subgroup decision assumption if the underlying prime-order bilinear group generator $\mathcal{G}_1$ satisfies the $k$-linear assumption.

**Theorem 1** *[15, Theorem 2.5] If $\mathcal{G}_1$ satisfies the $k$-linear assumption in $\mathbb{G}$ and $\mathbb{H}$, $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ satisfies the subgroup decision assumption regardless the choice of $\{A_\ell\}_{\ell\in[1,m]}$.*

Note that $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ contains Groth-Sahai's constructions based on the DDH assumption ($k = 1$) and the DLIN assumption ($k = 2$).

### 3.2 Conditions for Symmetric Property

A bilinear pairing $e$ of $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ in Figure 1 can be rewritten, using matrix notation, as
$$e(\mathfrak{g}^{\overrightarrow{x}}, \mathfrak{h}^{\overrightarrow{y}})_\ell = \hat{e}(\mathfrak{g}, \mathfrak{h})^{\overrightarrow{x} A_\ell \overrightarrow{y}^t}$$
where $\overrightarrow{x}$ is considered to be a $1 \times (k+1)$ matrix, and $\overrightarrow{y}^t$ is considered to be a $(k+1) \times 1$ matrix.

If $\mathcal{G}_1$ is a symmetric bilinear group generator of prime-order, then one may think that $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ is also a symmetric bilinear group generator. However,

not all bilinear groups with underlying symmetric bilinear pairings $\hat{e}$ do satisfy symmetric property. The following theorem shows the necessary and sufficient condition of $\{A_\ell\}_{\ell\in[1,m]}$ for $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ to be symmetric, that is, $e(g,h)=e(h,g)$ for any group elements $g$ and $h$.

**Theorem 2** *$\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ is symmetric if and only if $\mathbb{G}=\mathbb{H}$, $\mathfrak{g}=\mathfrak{h}$, $\overrightarrow{x}_i=\overrightarrow{y}_i$ for all $i\in[1,k]$, and $A_\ell$ is symmetric for all $\ell\in[1,m]$, where $\mathbb{G},\mathbb{H},\mathfrak{g},\mathfrak{h},\overrightarrow{x}_i$ and $\overrightarrow{y}_i$ are defined in the description of $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$.*

Because of space constraints, we give the proof of Theorem 2 in the full version of this paper.

### 3.3 Necessary Condition for Projection Property

Using a tensor product $\otimes$, we can further simplify $e$ computation as follows: Let $B$ be a $(k+1)^2\times m$ matrix such that $B$'s $((i-1)(k+1)+j,\ell)$ entry is $a_{i,j}^{(\ell)}$, where $A_\ell=(a_{i,j}^{(\ell)})$. Then,

$$\begin{aligned} e(\mathfrak{g}^{\overrightarrow{x}},\mathfrak{h}^{\overrightarrow{y}}) &= (e(\mathfrak{g}^{\overrightarrow{x}},\mathfrak{h}^{\overrightarrow{y}})_1,\ldots,e(\mathfrak{g}^{\overrightarrow{x}},\mathfrak{h}^{\overrightarrow{y}})_m)\\ &= (\hat{e}(\mathfrak{g},\mathfrak{h})^{\overrightarrow{x}A_1\overrightarrow{y}^t},\ldots,\hat{e}(\mathfrak{g},\mathfrak{h})^{\overrightarrow{x}A_m\overrightarrow{y}^t}) = \hat{e}(\mathfrak{g},\mathfrak{h})^{(\overrightarrow{x}\otimes\overrightarrow{y})B}. \end{aligned}$$

From now, we use a notation $\mathcal{G}_k^B$ as well as $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ to denote a bilinear group generator naturally induced from the $k$-linear assumption, where $B$ is defined by $\{A_\ell\}_{\ell\in[1,m]}$ as above. This notation is well-defined since there are one-to-one correspondence between $B$ and $\{A_\ell\}_{\ell\in[1,m]}$.

We give a necessary condition of $B$ for $\mathcal{G}_k^B$ to be projecting in Lemma 1. This lemma says that if $G=G_1\oplus G_2$ and $H=H_1\oplus H_2$, then $e(G_2,H_2)$ should have at least an element not contained in the subgroup generated by other parts of images.

**Lemma 1** *1. If $\mathcal{G}_k^B$ is asymmetric (that is, $\mathcal{G}_k^B\xrightarrow{\$}(p,G,G_1,H,H_1,G_t,e)$) and projecting, for decompositions $G=G_1\oplus G_2$ and $H=H_1\oplus H_2$ it satisfies that $e(G_2,H_2)\not\subset\mathbb{D}$, where $\mathbb{D}$ is the smallest group containing $e(G_1,H)$ and $e(G,H_1)$.*

*2. If $\mathcal{G}_k^B$ is symmetric (that is, $\mathcal{G}_k^B\xrightarrow{\$}(p,G,G_1,G_t,e)$) and projecting, for any decomposition $G=G_1\oplus G_2$ it satisfies that $e(G_2,G_2)\not\subset\mathbb{D}$, where $\mathbb{D}$ is the smallest group containing $e(G,G_1)$.*

*Proof.* (1) Suppose that $\mathcal{G}_k^B$ is projecting. Then, there exist three homomorphisms $\pi$, $\bar{\pi}$, and $\pi_t$. Since $\pi$ and $\bar{\pi}$ are non-trivial homomorphisms, $G_1$ and $H_1$ are proper subgroups of $G$ and $H$, respectively. Since $G_1$ and $H_1$ are proper subgroups, for any decompositions $G=G_1\oplus G_2$ and $H=H_1\oplus H_2$, $\{1_G\}\neq G_2\subset G$ and $\{1_H\}\neq H_2\subset H$. We show that $G_1,G_2,H_1$, and $H_2$ satisfy the condition in the theorem. By definition of $\mathbb{D}$, $\mathbb{D}$ is a group generated by all elements in $e(G_1,H)$ and $e(G,H_1)$ so that every element in $\mathbb{D}$ can be written as a product of

elements in $e(G_1, H)$ and $e(G, H_1)$ (though it is not uniquely written). For any $g_1 \in G_1$, $h_1 \in H_1$, $g \in G$, and $h \in H$, $\pi_t(e(g_1, h)e(g, h_1))$ is equal to $1_t$ since

$$\pi_t(e(g_1, h))\pi_t(e(g, h_1)) = e(\pi(g_1), \bar{\pi}(h))e(\pi(g), \bar{\pi}(h_1)) = e(1_G, \bar{\pi}(h))e(\pi(g), 1_H).$$

We can see that by homomorphic property of $\pi_t$, $\pi_t(\mathbb{D}) = 1_t$. If $e(G_2, H_2) \subset \mathbb{D}$, then $e(G, H) \subset \mathbb{D} \subset \ker(\pi_t)$. That is a contradiction of $\pi_t$'s non-trivial condition.

(2) We can prove similarly as (1). Essential proof idea is same to (1). Thus, we omit it. □

For our impossibility results regarding the image size and computational cost, we will focus on the $(k+1)^2 \times m$ matrix $B$ of $\mathcal{G}_k^B$. All non-zero entries in $B$ imply $\hat{e}$-computations (bilinear pairing $\hat{e}$ of underlying bilinear group generator $\mathcal{G}_1$) and the lower bound of $m$ implies the lower bound of the image size of bilinear pairings. We compute the lower bound of the rank of $B$ of $\mathcal{G}_k^B$, where $\mathcal{G}_k^B$ is asymmetric and projecting, by using the necessary condition of projecting property in Lemma 1. For projecting symmetric bilinear pairings, the overall strategy is similar to those of projecting asymmetric bilinear pairings except that symmetric bilinear pairings have the special form of $B$ as mentioned in Theorem 2. We give the formal statement below.

**Lemma 2** *The following statements about $\mathcal{G}_k^B$ are true with overwhelming probability, where the probability goes over the randomness used in the $\mathcal{G}_k^B$.*

1. *If $\mathcal{G}_k^B$ is asymmetric and projecting, then $B$ has $(k+1)^2$ linearly independent rows.*
2. *If $\mathcal{G}_k^B$ is symmetric and projecting, then $B$ has $\frac{(k+1)(k+2)}{2}$ linearly independent rows.*

*Proof.* (1) Let $\mathcal{G}_k^B$ be a projecting asymmetric bilinear group generator. Let $(G, G_1, H, H_1, G_t, e)$ be the output of $\mathcal{G}_k^B$ and $G$ and $H$ be decomposed by $G = G_1 \oplus G_2$ and $H = H_1 \oplus H_2$, respectively for some subgroups $G_2$ and $H_2$. Then, $G_1 = \langle \mathfrak{g}^{\overrightarrow{x}_1}, \ldots, \mathfrak{g}^{\overrightarrow{x}_k} \rangle$, $H_1 = \langle \mathfrak{h}^{\overrightarrow{y}_1}, \ldots, \mathfrak{h}^{\overrightarrow{y}_k} \rangle$, $G_2 = \langle \mathfrak{g}^{\overrightarrow{x}_{k+1}} \rangle$, and $H_2 = \langle \mathfrak{h}^{\overrightarrow{y}_{k+1}} \rangle$ for some sets of linearly independent vectors $\{\overrightarrow{x}_i\}_{i \in [1,k+1]}$ and $\{\overrightarrow{y}_i\}_{i \in [1,k+1]}$. Let $X$ be a $(k+1) \times (k+1)$ matrix over $\mathbb{F}_p$ with $\overrightarrow{x}_i$ as its $i$-th row, and $Y$ be a $(k+1) \times (k+1)$ matrix over $\mathbb{F}_p$ with $\overrightarrow{y}_i$ as its $i$-th row. Note that $X$ and $Y$ are invertible. Since $B$ is a $(k+1)^2 \times m$ matrix for some $m$, $B$ can have at most $(k+1)^2$ linear independent rows.

Suppose that $B$ has less than $(k+1)^2$ linearly independent rows. We observe that

$$e(G_2, H_2) = \langle e(\mathfrak{g}^{\overrightarrow{x}_{k+1}}, \mathfrak{h}^{\overrightarrow{y}_{k+1}}) \rangle = \langle \hat{e}(\mathfrak{g}, \mathfrak{h})^{(\overrightarrow{x}_{k+1} \otimes \overrightarrow{y}_{k+1})B} \rangle = \langle \hat{e}(\mathfrak{g}, \mathfrak{h})^{\overrightarrow{e}_{(k+1)^2}(X \otimes Y)B} \rangle,$$

and similarly

$$\mathbb{D} = \langle \hat{e}(\mathfrak{g}, \mathfrak{h})^{\overrightarrow{e}_1(X \otimes Y)B}, \ldots, \hat{e}(\mathfrak{g}, \mathfrak{h})^{\overrightarrow{e}_{(k+1)^2-1}(X \otimes Y)B} \rangle,$$

where $\overrightarrow{e}_i$ is the $i$-th canonical vector of $\mathbb{F}_p^{(k+1)^2}$. Now, we show that there exists a non-zero vector $\overrightarrow{c} \in \mathbb{F}_p^{(k+1)^2}$ with a non-zero in the $(k+1)^2$-th entry such that $\overrightarrow{c} \cdot (X \otimes Y)B = \overrightarrow{0} \in \mathbb{F}_p^m$. The existence of such a vector $\overrightarrow{c}$ implies that the $(k+1)^2$-th row of $(X \otimes Y)B$ can be represented by the linear combination of upper rows of $(X \otimes Y)B$ so that $e(G_2, H_2) \subset \mathbb{D}$. Then, it would be a contradiction with Lemma 1.

By hypothesis ($rank(B) < (k+1)^2$), there exists a non-zero vector $\overrightarrow{r} \in \mathbb{F}_p^{(k+1)^2}$ such that $\overrightarrow{r}B = \overrightarrow{0} \in \mathbb{F}_p^m$. For such an $\overrightarrow{r}$, we show that $\overrightarrow{r}(X^{-1} \otimes Y^{-1})$ satisfies conditions for it to be $\overrightarrow{c}$ aforementioned. First, we obtain $\overrightarrow{r}(X^{-1} \otimes Y^{-1}) \cdot (X \otimes Y)B = \overrightarrow{r}B = \overrightarrow{0}$. Next, we argue that $\overrightarrow{r}(X^{-1} \otimes Y^{-1})$'s $(k+1)^2$-th entry is non-zero with overwhelming probability, where the probability goes over the randomness used in $\mathcal{G}_k^B$ (to choose $\overrightarrow{x}_1, \ldots, \overrightarrow{x}_k, \overrightarrow{y}_1, \ldots, \overrightarrow{y}_k$). We consider the $(k+1)$-th column vector $\hat{x}^t$ of $X^{-1}$ such that $\hat{x}$ is orthogonal to all upper $k$ rows of $X$. Denote the orthogonal complement of $\langle \overrightarrow{x}_1, \ldots, \overrightarrow{x}_k \rangle$ by $\langle \overrightarrow{w} \rangle$. Then, $\hat{x}^t$ is a non-zero vector in $\langle \overrightarrow{w} \rangle$. By definition of $\mathcal{G}_k^B$, $\overrightarrow{x}_1, \ldots, \overrightarrow{x}_k$ are randomly chosen so that $\overrightarrow{w}$ is also uniformly distributed in $\mathbb{F}_p^{k+1}$. Similarly, the $(k+1)$-th column vector $\hat{y}^t$ of $Y^{-1}$ is a non-zero vector in $\langle \overrightarrow{y}_1, \ldots, \overrightarrow{y}_k \rangle^\perp := \langle \overrightarrow{z} \rangle$, and $\overrightarrow{z}$ is uniformly distributed in $\mathbb{F}_p^{k+1}$. The $(k+1)^2$-th entry of $\overrightarrow{r}(X^{-1} \otimes Y^{-1})$ is $\overrightarrow{r}(\hat{x}^t \otimes \hat{y}^t)$, and it is a non-zero constant multiple of $\overrightarrow{r}(\overrightarrow{w} \otimes \overrightarrow{z})^t$. By the first statement of Lemma 3, which is given below, $\overrightarrow{r}(\overrightarrow{w} \otimes \overrightarrow{z})^t$ is non-zero with overwhelming probability. Therefore, we complete the proof of the first statement of theorem.

(2) We can prove the second statement of theorem by using the second statements of Lemma 1 and Lemma 3. The overall strategy is same to the proof of the first statement of theorem. The key observation of the proof of the second statement is that $B$ has a special form due to Theorem 2. We leave the detail of the proof of the second statement in the full version. □

**Lemma 3** *Let $V$ be a subspace of $\mathbb{F}_p^{(k+1)^2}$ generated by $\{\overrightarrow{a}_{i,j}\}_{1 \le i \le j \le k+1}$, where $\overrightarrow{a}_{i,j}$ is a vector with 1 in the $(i-1)(k+1)+j$-th entry, $-1$ in the $(j-1)(k+1)+i$-th entry, and zeros elsewhere.*

1. *For any non-zero vector $\overrightarrow{r} \in \mathbb{F}_p^{(k+1)^2}$, $\Pr[\overrightarrow{r} \cdot (\overrightarrow{w} \otimes \overrightarrow{z})^t = 0] \le \frac{2}{p}$, where the probability goes over the choice of vectors $\overrightarrow{w}$, $\overrightarrow{z} \in \mathbb{F}_p^{k+1}$.*
2. *For any vector $\overrightarrow{r} \in \mathbb{F}_p^{(k+1)^2} \setminus V$, $\Pr[\overrightarrow{r} \cdot (\overrightarrow{w} \otimes \overrightarrow{w})^t = 0] \le \frac{2}{p}$, where the probability goes over the choice of a vector $\overrightarrow{w} \in \mathbb{F}_p^{k+1}$.*

We can prove Lemma 3 by using the Schwartz-Zippel lemma [33] and leave a detailed proof in the full version.

### 3.4 Impossibility of Projecting Property

Basing on Lemma 2, we derive our main theorem on the impossibility results of projecting bilinear pairings. We begin with explaining our computational model

for the lower bounds of computational cost of projecting bilinear pairings. In our computational model, we assume two things: First, one who computes projecting bilinear pairings $e$ can not utilize the representation of the underlying bilinear pairing $\hat{e}$ and groups $\mathbb{G}, \mathbb{H}$, and $\mathbb{G}_t$ over which $\hat{e}$ is defined. Note that we rule out techniques for multi-pairings [34, 17] in our computational model. This assumption is same to that of the generic group model [37], in particular, generic bilinear group [8]. In [37, 8], the generic (bilinear) group model is used to show the computational lower bounds of attacker solving number theoretic problems such as the discrete logarithm problem and $q$-strong Diffie-Hellman problem. Second, two inputs are uniformly and independently chosen so that any relations with two inputs are unknown. In special cases such that a relation with two inputs are known, there are several alternative way to compute bilinear pairings. For example, one knowing $g_1$, $h_1$, $e(g, h)$, and a relation $g_1 = g^2$ and $h_1 = h^3$ can compute $e(g_1, h_1)$ by performing $e(g, h)^6$ instead of performing a bilinear pairing. Since we want to consider the computational cost of $e$ without using any additional information of two inputs, we assume that two inputs are uniformly and independently distributed in their respective domains. We provide our main theorem below.

**Theorem 3** *(Lower Bounds) The following statements about $\mathcal{G}_k^B$ are true with overwhelming probability, where the probability goes over the randomness used in the $\mathcal{G}_k^B$.*

1. *The image size of a projecting asymmetric bilinear pairing is at least $(k+1)^2$ elements in $\mathbb{G}_t$.*
2. *The image size of a projecting symmetric bilinear pairing is at least $\frac{(k+1)(k+2)}{2}$ elements in $\mathbb{G}_t$.*
3. *Any construction for a projecting (asymmetric or symmetric) bilinear pairing should perform at least $(k+1)^2$ computations of $\hat{e}$ in our computational model.*

*Proof.* (1) Suppose that $\mathcal{G}_k^B$ is asymmetric and projecting. Since a $(k+1)^2 \times m$ matrix $B$ has at least $(k+1)^2$ linearly independent rows by Lemma 2, $m \geq (k+1)^2$. This implies that $G_t = \mathbb{G}_t^m$ consists of $m$ ($\geq (k+1)^2$) elements in $\mathbb{G}_t$.

(2) If $\mathcal{G}_k^B$ is symmetric and projecting, then $(k+1)^2 \times m$ matrix $B$ has at least $\frac{(k+1)(k+2)}{2}$ linear independent rows by Lemma 2. Thus, $m \geq \frac{(k+1)(k+2)}{2}$; hence, an element in $G_t = \mathbb{G}_t^m$ is $m$ ($\geq \frac{(k+1)(k+2)}{2}$) elements in $\mathbb{G}_t$.

(3) First, we show that for two inputs $g = (\mathfrak{g}_1, \ldots, \mathfrak{g}_{k+1}) \in G$ and $h = (\mathfrak{h}_1, \ldots, \mathfrak{h}_{k+1}) \in H$, projecting (asymmetric or symmetric) pairings require computing all $\hat{e}(\mathfrak{g}_i, \mathfrak{h}_j)$ for all $i, j \in [1, k+1]$. To this end, it is sufficient to show that every row in the matrix $B$ is non-zero. (Recall that $e(\mathfrak{g}^{\overrightarrow{w}}, \mathfrak{h}^{\overrightarrow{z}}) = \hat{e}(\mathfrak{g}, \mathfrak{h})^{(\overrightarrow{w} \otimes \overrightarrow{z})B}$ and if every row in $B$ is non-zero, then $\hat{e}(\mathfrak{g}^{w_i}, \mathfrak{h}^{z_j})$ should be computed at least one time.) If a group generator $\mathcal{G}_k^B$ is projecting and asymmetric, then the rank of $B$ is $(k+1)^2$ by Lemma 1. Since $B$ has $(k+1)^2$ rows, there is no zero rows. If a group generator $\mathcal{G}_k^B$ is projecting and symmetric, then the rank of $B$ is $\frac{(k+1)(k+2)}{2}$

by Lemma 1. We know that the matrix $B$ of symmetric bilinear group generators has the special form by Theorem 2. From Theorem 2, some $\frac{k(k+1)}{2}$ rows in $B$ have respective same rows in $B$. Since $B$ has $(k+1)^2$ rows and $(k+1)^2 - \frac{k(k+1)}{2}$ is equal to the rank of $B$, every row in $B$ has at least one non-zero entry.

Next, we show that computing $\hat{e}(\mathfrak{g}_i, \mathfrak{h}_j)$ cannot be generally substitute by a product of other $\hat{e}(\mathfrak{g}_{i'}, \mathfrak{h}_{j'})$ for $i' \in [1, k+1] \setminus \{i\}$ and $j' \in [1, k+1] \setminus \{j\}$ in our computational model. To this end, it is sufficient to show that for any non-zero vector $\overrightarrow{r} = (r_1, \ldots, r_{(k+1)^2}) \in \mathbb{F}_p^{(k+1)^2}$,

$$\Pr_{g \xleftarrow{\$} G, h \xleftarrow{\$} H} \Big[ \prod_{i,j \in [1,k+1]} \hat{e}(\mathfrak{g}_i, \mathfrak{h}_j)^{r_{(i-1)(k+1)+j}} = 1_{\mathbb{G}_t} \Big] \approx 0.$$

For two random inputs $\mathfrak{g}^{\overrightarrow{w}}$ and $\mathfrak{h}^{\overrightarrow{z}}$,

$$\prod_{i,j \in [1,k+1]} \hat{e}(\mathfrak{g}^{w_i}, \mathfrak{h}^{z_j})^{r_{(i-1)(k+1)+j}} = \hat{e}(\mathfrak{g}, \mathfrak{h})^{(\overrightarrow{w} \otimes \overrightarrow{z})\overrightarrow{r}^t},$$

where $\overrightarrow{w} = (w_1, \ldots, w_{k+1}) \in \mathbb{F}_p^{k+1}$ and $\overrightarrow{z} = (z_1, \ldots, z_{k+1}) \in \mathbb{F}_p^{k+1}$. Since $\overrightarrow{r}^t$ is a non-zero vector in $\mathbb{F}_p^{(k+1)^2}$, $(\overrightarrow{w} \otimes \overrightarrow{z})\overrightarrow{r}^t \neq 0$ with overwhelming probability by Lemma 3, and hence we obtain the desired result such that

$$\prod_{i,j \in [1,k+1]} \hat{e}(\mathfrak{g}^{w_i}, \mathfrak{h}^{z_j})^{r_{(i-1)(k+1)+j}} \neq 1_{\mathbb{G}_t}$$

with overwhelming probability.

Therefore, all projecting bilinear pairings require at least $(k+1)^2$ $\hat{e}$-computations. □

## 4 Optimal Projecting Bilinear Pairings

In this section, we show that our lower bounds are tight; for projecting asymmetric bilinear pairing, we show that Groth-Sahai and Freeman's constructions are optimal (in our computational model), and for projecting symmetric bilinear pairing, we propose a new construction achieving optimal efficiency (in our computational model).

**Definition 6** *Let $\mathcal{G}_k^B$ be a projecting asymmetric (symmetric, resp.) bilinear group generator. If the bilinear pairing $e$ consists of $(k+1)^2$ $\hat{e}$-computation in our computational model and $G_t = \mathbb{G}_t^{(k+1)^2}$ ($G_t = \mathbb{G}_t^{\frac{(k+1)(k+2)}{2}}$, resp.), we say that $\mathcal{G}_k^B$ is* optimal.

We can define $\mathcal{G}_k^B$ by defining a $(k+1)^2 \times m$ matrix $B$, or equivalently a set of $(k+1) \times (k+1)$ matrices $\{A_\ell\}_{\ell \in [1,m]}$. For a projecting asymmetric bilinear group generator, we define $B$ as $I_{(k+1)^2}$, where $I_{(k+1)^2}$ is the identity matrix in $GL_{(k+1)^2}(\mathbb{F}_p)$. Note that $\mathcal{G}_k^{I_{(k+1)^2}}$ is exactly equal to Freeman's projecting

asymmetric bilinear group generator [15] (We can easily check that $\mathcal{G}_k^{I_{(k+1)^2}}$ does not satisfy the symmetric property due to Theorem 2). Theorem 3 implies that $\mathcal{G}_k^{I_{(k+1)^2}}$ is optimal. Therefore, we obtain the following theorem.

**Theorem 4** *$\mathcal{G}_k^{I_{(k+1)^2}}$ is an optimal projecting asymmetric bilinear group generator.*

$\mathcal{G}_k^{I_{(k+1)^2}}$ covers one of the most interesting cases $k = 1$: $\mathcal{G}_1^{I_4}$ is optimal.[5]

### 4.1 Optimal Projecting Symmetric Bilinear Pairings

We propose an optimal projecting symmetric bilinear group generator $\mathcal{G}_k^B$ by defining $B$ (equivalently $A_1, \ldots, A_m$). Let a set $S$ be $\{(i,j) \in [1, k+1] \times [1, k+1] | 1 \leq j \leq i \leq k+1\}$. We consider a map $\tau : S \to [1, \frac{(k+1)(k+2)}{2}]$ defined by $(i,j) \mapsto \frac{i(i-1)}{2} + j$.

**Lemma 4** *$\tau$ is a bijective map.*

We give the proof of Lemma 4 in the full version.

**Description of $A_\ell$ (equivalently $B$) for optimal projecting symmetric bilinear pairings:** Let $\tau^{-1}(\ell) = (i,j)$. For each $\ell \in [1, \frac{(k+1)(k+2)}{2}]$, $A_\ell = (a_{s,t}^{(\ell)})$ is defined as a $(k+1) \times (k+1)$ matrix with

$$\begin{cases} 1 \text{ in the entry } (i,j) \text{ and zeros elsewhere} & \text{if } i = j, \\ 1 \text{ in the entries } (i,j) \text{ and } (j,i), \text{ and zeros elsewhere} & \text{otherwise .} \end{cases}$$

We give an example to easily explain the proposal.

*Example 1.* For $k = 2$, define

$$A_1 = \begin{pmatrix} 1\,0\,0 \\ 0\,0\,0 \\ 0\,0\,0 \end{pmatrix}, A_2 = \begin{pmatrix} 0\,1\,0 \\ 1\,0\,0 \\ 0\,0\,0 \end{pmatrix}, A_3 = \begin{pmatrix} 0\,0\,0 \\ 0\,1\,0 \\ 0\,0\,0 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 0\,0\,1 \\ 0\,0\,0 \\ 1\,0\,0 \end{pmatrix}, A_5 = \begin{pmatrix} 0\,0\,0 \\ 0\,0\,1 \\ 0\,1\,0 \end{pmatrix}, A_6 = \begin{pmatrix} 0\,0\,0 \\ 0\,0\,0 \\ 0\,0\,1 \end{pmatrix}.$$

□

Define $B$ as a $(k+1)^2 \times \frac{(k+1)(k+2)}{2}$ matrix such that $B$'s $((s-1)n + t, \ell)$ entry is $a_{s,t}^{(\ell)}$ for $s, t \in [1, k+1]$ and $\ell \in [1, \frac{(k+1)(k+2)}{2}]$. (Then, we implicitly define $G_t = \mathbb{G}_t^{\frac{(k+1)(k+2)}{2}}$.) By using the matrix $B$, we can construct a bilinear group generator $\mathcal{G}_k^B$.

Next, we show that a group generator $\mathcal{G}_k^B$, where $B$ is defined as above, is an optimal projecting symmetric bilinear group generator. The following Theorem 5 provides the desired result.

[5] Freeman used the notation $\mathcal{G}_P$, which is equivalent to our notation $\mathcal{G}_1^{I_4}$.

**Theorem 5** *Let $\mathcal{G}_k^B$ be a bilinear group generator with restrictions such that $\mathbb{G} = \mathbb{H}$, $\mathfrak{g} = \mathfrak{h}$, $\overrightarrow{x}_i = \overrightarrow{y}_i$ for all $i \in [1,k]$, and $B$ is a $(k+1)^2 \times \frac{(k+1)(k+2)}{2}$ matrix defined as above. Then, $\mathcal{G}_k^B$ is an optimal projecting symmetric bilinear group generator with overwhelming probability, where the probability goes over the randomness used in $\mathcal{G}_k^B$.*

We leave the proof of Theorem 5 in the full version.

Our definition of projecting requires only the existence of homomorphisms satisfying some conditions. However, some applications (ex: Boneh-Goh-Nissim cryptosystem [10, 15]) require that such homomorphisms are efficiently computable. We provide the way how to construct efficiently computable homomorphisms (precisely, natural projections) satisfying projecting property in the full version.

*Example 2.* For $k = 2$, we can construct an optimal projecting symmetric bilinear group generator by using the matrices in example 1. We denote such a bilinear group generator by $\mathcal{G}_2^{B^*}$, where $B^*$ is a $9 \times 6$ matrix defined by the $A_1, \ldots, A_6$ matrices in example 1.

$$B^* = \begin{pmatrix} \boxed{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & \boxed{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \boxed{1} & 0 & 0 \\ 0 & \boxed{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & \boxed{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} & 0 \\ 0 & 0 & 0 & \boxed{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{1} \end{pmatrix} \quad \text{for } \mathcal{G}_2^{B^*}$$

By Theorem 5, $\mathcal{G}_2^{B^*}$ is optimal projecting symmetric: Since $B^*$ is a $9 \times 6$ matrix, the target group $G_t$ is equal to $\mathbb{G}_t^6$. Moreover, $B^*$ has nine 1's in the entries and zeros elsewhere so that bilinear pairing $e$ requires 9 $\hat{e}$-computations (without any exponentiations).

## 5 Application

On the basis of our optimal projecting symmetric bilinear pairings, we derive new instantiations of three distinct cryptosystems with improved efficiency. In particular, we apply the projecting symmetric bilinear group generator $\mathcal{G}_2^{B^*}$ in the example 2 for the Groth-Sahai non-interactive proof system, the Boneh-Goh-Nissim Cryptosystem, and the Seo-Cheon round optimal Blind signature scheme. Because of space constraints, we leave details in the full version.

**Acknowledgements** We gratefully acknowledge the detailed and helpful comments of anonymous reviewers of ASIACRYPT 2012. We also thank Jung Hee Cheon and Daisuke Moriyama for constructive feedback on an early draft of the paper.

## References


1. M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-preserving signatures and commitments to group elements. In *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236. Springer, 2010.
2. M. Abe, J. Groth, K. Haralambiev, and M. Ohkubo. Optimal structure-preserving signature in asymmetric bilinear groups. In *CRYPTO 2011*, volume 6841 of *LNCS*, pages 649–666. Springer, 2011.
3. M. Abe, J. Groth, and M. Ohkubo. Separating short structure-preserving signatures from non-interactive assumptions. In *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 628–646. Springer, 2011.
4. M. Abe, K. Haralambiev, and M. Ohkubo. Group to group commitments do not shrink. In *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 301–317. Springer, 2012.
5. B. Adida and D. Wikström. How to shuffle in public. In *TCC 2007*, volume 4392 of *LNCS*, pages 555–574. Springer, 2007.
6. M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham. Randomizable proofs and delegatable anonymous credentials. In *CRYPTO 2009*, volume 5677 of *LNCS*, pages 108–125. Springer, 2009.
7. M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya. P-signature and non-interactive anonymous credentials. In *TCC 2008*, volume 4984 of *LNCS*, pages 356–374. Springer, 2008.
8. D. Boneh and X. Boyen. Short signatures without random oracles. In *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 382–400. Springer, 2004.
9. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55. Springer, 2004.
10. D. Boneh, E. Goh, and K. Nissim. Evaluating 2-DNF formulas on ciphertexts. In *TCC 2005*, volume 3378 of *LNCS*. Springer-Verlag, 2005.
11. J. Camenisch, K. Haralambiev, M. Kohlweiss, J. Lapon, and V. Naessens. Structure preserving CCA secure encryption and applications. In *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 89–106. Springer, 2011.
12. J. Cathalo, B. Libert, and M. Yung. Group encryption: Non-interactive realization in the standard model. In *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 179–196. Springer, 2009.
13. N. Chandran, J. Groth, and A. Sahai. Ring signatures of sub-linear size without random oracles. In *ICALP 2007*, volume 4596 of *LNCS*, pages 423–434. Springer, 2007.
14. M. Chase, M. Kohlweiss, A. Lysyanskaya, and S. Meiklejohn. Malleable proof systems and applications. In *EUROCRYPT 2012*, LNCS. Springer, 2012.
15. D. M. Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 44–61. Springer, (full version is available from http://eprint.iacr.org/2009/540) (full version is available from http://eprint.iacr.org/2009/540), 2010.
16. S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. In *Discrete Applied Mathematics*, volume 156, pages 3113–3121, 2008.
17. R. Granger and N. Smart. On computing products of pairings. In *Cryptology ePrint Archive, Report 2006/172*, 2006.
18. M. Green and S. Hohenberger. Universally composable adaptive oblivious transfer. In *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 179–197. Springer, 2008.

19. J. Groth. Fully anonymous group signatures without random oracles. In *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 164–180. Springer, 2007.
20. J. Groth and S. Lu. A non-interactive shuffle with pairing based verifiability. In *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 51–67. Springer, 2007.
21. J. Groth, R. Ostrovsky, and A. Sahai. Perfect non-interactive zero-knolwedge for NP. In *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 339–358. Springer, 2006.
22. J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, 2008.
23. D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. In *CRYPTO 2007*, volume 4622 of *LNCS*, pages 553–571. Springer, 2007.
24. A. B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In *EUROCRYPT 2012*, LNCS. Springer, 2012.
25. S. Meiklejohn, H. Shacham, and D. M. Freeman. Limitations on transformations from composite-order to prime-order groups: The case of round-optimal blind signatures. In *ASIACRYPT 2010*, volume 6477 of *LNCS*, pages 519–538. Springer, 2010.
26. T. Okamoto and K. Takashima. Homomorphic encryption and signature from vector decomposition. In *Pairing 2008*, volume 5209 of *LNCS*, pages 57–74. Springer, 2008.
27. T. Okamoto and K. Takashima. Hierarchical predicate encryption for inner-products. In *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 214–231. Springer, 2009.
28. T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208. Springer, 2010.
29. T. Okamoto and K. Takashima. Efficient attribute-based signatures for non-monotone predicates in the standard model. In *PKC 2011*, volume 6571 of *LNCS*, pages 35–52. Springer, 2011.
30. T. Okamoto and K. Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In *EUROCRYPT 2012*, LNCS. Springer, 2012.
31. R. Ostrovsky and W. Skeith. Private searching on streaming data. In *Journal of Cryptology*, volume 20, pages 397–430. Springer, 2007.
32. Y. Sang and H. Shen. Efficient and secure protocols for privacy-preserving set operations. In *ACM Transactions on Information and Systems Security*, volume 13, 2009.
33. J. Schwartz. Fast probabilistic algorithms for verification of polynomials identities. In *Journal of the ACM*, volume 27, pages 701–717, 1980.
34. M. Scott. Computing the Tate pairing. In *CT-RSA 2005*, volume 3376 of *LNCS*, pages 239–304. Springer, 2005.
35. J. H. Seo and J. H. Cheon. Beyond the limitation of prime-order groups, and round optimal blind signatures. In *TCC 2012*, volume 7194 of *LNCS*, pages 133–150. Springer, 2012.
36. H. Shacham. A cramer-shoup encryption scheme from the linear assumption and from progressively weaker linear variants. In *Cryptology ePrimt Archive, Report 2007/074*. http://eprint.iacr.org/2007/074, 2007.
37. V. Shoup. Lower bounds for discrete logarithms and related problems. In *EUROCRYPT 1997*, pages 256–266. Springer, 1997.