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

Jae Hong Seo

Department of Mathematics, Myongji University,
Yongin, Republic of Korea
jaehongseo@mju.ac.kr

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 (EUROCRYPT 2008) showed that projecting bilinear pairings can be achieved in a 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. Subsequently, Freeman (EUROCRYPT 2010) generalized Groth-Sahai's projecting asymmetric bilinear pairings.

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; 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 a prime-order group setting. They provided two distinct constructions in the 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 in the prime-order group setting.[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 in the prime-order group setting, 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 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 pairings 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 assumptions 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

[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.

[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.

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 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 [15]: that is, it is the most efficient construction for projecting asymmetric bilinear pairings in our framework and computational model. In contrast, our lower bounds for a 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 the 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 the 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 the 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 the 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.

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.

[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.

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 ≥ 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 $\tau : T_D \to T_R$, 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 λ and $\approx$ denotes the difference between both sides is a negligible function in λ.

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,

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

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 λ. 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 λ).

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 λ.

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 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 ($k=2$).

[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_ℓ 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 λ as input.
2. Run $\mathcal{G}_1(\lambda) \xrightarrow{\$} (p, \mathbb{G}, \mathbb{H}, \mathbb{G}_t, \hat{e})$.
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 $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$

3.2 Conditions for Bilinearity and Non-degeneracy

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.

Theorem 2 *Let e be a map generated by $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$. Then, e is always bilinear regardless of $\{A_\ell\}_{\ell\in[1,m]}$.*

Proof. The bilinearity of e comes directly from the bilinearity of $\hat{e}$ and the definition of e. □

Theorem 3 *Let e be a map generated by $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$. Let V_c and V_r be vector spaces over $\mathbb{F}_p$ spanned by all column vectors and all row vectors of $\{A_\ell\}_{\ell\in[1,m]}$, respectively. Then, e is non-degenerate if and only if both dimensions of V_c and V_r are equal to $(k+1)$.*

Proof. ($\Rightarrow$) We show that if $\dim(V_c) < k+1$ or $\dim(V_r) < k+1$, then e is degenerate. Suppose that $\dim(V_c) < k+1$. Then, there exists a non-zero vector $\overrightarrow{x} \in V_c^\perp \subset \mathbb{F}_p^{k+1}$, where $V_c^\perp$ is an orthogonal complement of V_c in the $(k+1)$-dimensional vector space $\mathbb{F}_p^{k+1}$; That is, for $\forall \overrightarrow{z} \in V_c$, $\overrightarrow{x} \cdot \overrightarrow{z}^t = 0$. It implies that $\overrightarrow{x} A_\ell = 0$ for $\forall \ell \in [1, m]$ so that for $\forall \overrightarrow{y} \in \mathbb{F}_p^{k+1}$,

$$e(\mathfrak{g}^{\overrightarrow{x}}, \mathfrak{h}^{\overrightarrow{y}}) = (\hat{e}(\mathfrak{g}, \mathfrak{h})^{\overrightarrow{x} A_1 \overrightarrow{y}^t}, \ldots, \hat{e}(\mathfrak{g}, \mathfrak{h})^{\overrightarrow{x} A_m \overrightarrow{y}^t}) = 1_t,$$

where 1_t is the identity of G_t. Therefore, e is degenerate. Similarly, if $\dim(V_r) < k+1$, then there exists a non-zero vector $\overrightarrow{y} \in V_r^\perp \subset \mathbb{F}_p^{k+1}$ such that for $\forall \overrightarrow{x} \in \mathbb{F}_p^{k+1}$, $e(\mathfrak{g}^{\overrightarrow{x}}, \mathfrak{h}^{\overrightarrow{y}}) = 1_t$ so that e is degenerate.

($\Leftarrow$) Suppose that e is degenerate. Then, there exists a non-zero vector $\overrightarrow{x} \in \mathbb{F}_p^{k+1}$ such that for $\forall \overrightarrow{z} \in \mathbb{F}_p^{k+1}$, $e(\mathfrak{g}^{\overrightarrow{x}}, \mathfrak{h}^{\overrightarrow{z}}) = 1_t$, or there exists a non-zero vector $\overrightarrow{y} \in \mathbb{F}_p^{k+1}$ such that for $\forall \overrightarrow{w} \in \mathbb{F}_p^n$, $e(\mathfrak{g}^{\overrightarrow{w}}, \mathfrak{h}^{\overrightarrow{y}}) = 1_t$. We show that if such a vector $\overrightarrow{x}$ exists, then $\dim(V_c) < k+1$, and if such a vector $\overrightarrow{y}$ exists, then $\dim(V_r) < k+1$. Suppose that there exists a non-zero vector $\overrightarrow{x} \in \mathbb{F}_p^{k+1}$ such that for $\forall \overrightarrow{z} \in \mathbb{F}_p^{k+1}$, $e(\mathfrak{g}^{\overrightarrow{x}}, \mathfrak{h}^{\overrightarrow{z}}) = (\hat{e}(\mathfrak{g}, \mathfrak{h})^{\overrightarrow{x} A_1 \overrightarrow{z}^t}, \ldots, \hat{e}(\mathfrak{g}, \mathfrak{h})^{\overrightarrow{x} A_m \overrightarrow{z}^t}) = 1_t$. Since $\hat{e}$ is non-degenerate, $\overrightarrow{x} A_\ell \overrightarrow{z}^t = 0$ for $\forall \ell \in [1, m]$ and $\forall \overrightarrow{z} \in \mathbb{F}_p^{k+1}$. This implies that $\overrightarrow{x} A_\ell = (0, \ldots, 0) \in \mathbb{F}_p^{k+1}$ for $\forall \ell \in [1, m]$ so $\overrightarrow{x} \in V_c^\perp$. Since $\overrightarrow{x}$ is a non-zero vector, $V_c^\perp \neq \{0\}$ so that $\dim(V_c) < k+1$. Similarly, if that there exists a non-zero vector $\overrightarrow{y} \in \mathbb{F}_p^{k+1}$ such that for $\forall \overrightarrow{w} \in \mathbb{F}_p^{k+1}$, $e(\mathfrak{g}^{\overrightarrow{w}}, \mathfrak{h}^{\overrightarrow{y}}) = 1_t$, then $\overrightarrow{y} \in V_r^\perp$ is a non-trivial subspace so that $\dim(V_r) < k+1$. □

3.3 Conditions for Symmetric Property

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 4 *$\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$ 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_ℓ 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 $\mathcal{G}_k^{\{A_\ell\}_{\ell\in[1,m]}}$.*

Proof. ($\Rightarrow$) Suppose that $\mathcal{G}_k^B$ is symmetric. Then, $\mathbb{G}=\mathbb{H}$, $\mathfrak{g}=\mathfrak{h}$, $\overrightarrow{x}_i=\overrightarrow{y}_i$ for all $i\in[1,k]$, and $e(\mathfrak{g}^{\overrightarrow{x}},\mathfrak{g}^{\overrightarrow{y}})=e(\mathfrak{g}^{\overrightarrow{y}},\mathfrak{g}^{\overrightarrow{x}})$. Thus,

$$(\hat{e}(\mathfrak{g},\mathfrak{g})^{\overrightarrow{x}A_1\overrightarrow{y}^t},\ldots,\hat{e}(\mathfrak{g},\mathfrak{g})^{\overrightarrow{x}A_m\overrightarrow{y}^t})=(\hat{e}(\mathfrak{g},\mathfrak{g})^{\overrightarrow{y}A_1\overrightarrow{x}^t},\ldots,\hat{e}(\mathfrak{g},\mathfrak{g})^{\overrightarrow{y}A_m\overrightarrow{x}^t}).$$

Since $\overrightarrow{x}A_\ell\overrightarrow{y}^t\in\mathbb{F}_p$, $\overrightarrow{x}A_\ell\overrightarrow{y}^t=(\overrightarrow{x}A_\ell\overrightarrow{y}^t)^t=\overrightarrow{y}A_\ell^t\overrightarrow{x}^t$; Hence, for all $\ell\in[1,k+1]$ $\overrightarrow{y}A_\ell^t\overrightarrow{x}^t=\overrightarrow{y}A_\ell\overrightarrow{x}^t$. Since $\overrightarrow{x}$ and $\overrightarrow{y}$ are arbitrary, $A_\ell=A_\ell^t$.

($\Leftarrow$) Suppose that $\mathbb{G}=\mathbb{H}$, $\mathfrak{g}=\mathfrak{h}$ and $\overrightarrow{x}_i=\overrightarrow{y}_i$ for all $i\in[1,k]$. These imply that $G=H$ and $G_1=H_1$. Suppose that A_ℓ is symmetric; That is $A_\ell^t=A_\ell$. Since $\overrightarrow{x}A_\ell\overrightarrow{y}^t\in\mathbb{F}_p$, $\overrightarrow{x}A_\ell\overrightarrow{y}^t=(\overrightarrow{x}A_\ell\overrightarrow{y}^t)^t=\overrightarrow{y}A_\ell^t\overrightarrow{x}^t=\overrightarrow{y}A_\ell\overrightarrow{x}^t$. This implies that $e(\mathfrak{g}^{\overrightarrow{x}},\mathfrak{g}^{\overrightarrow{y}})=e(\mathfrak{g}^{\overrightarrow{y}},\mathfrak{g}^{\overrightarrow{x}})$. □

3.4 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 π, $\bar{\pi}$, and π_t. Since π 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 π_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 π_t's non-trivial condition.

(2) We can prove similarly as (1). Essential proof idea is same as (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 4. 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 as 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 4.

Let $\mathcal{G}_k^B$ be a projecting symmetric bilinear group generator, (G, G_1, G_t, e) be its output, and G be decomposed by $G = G_1 \oplus G_2$ for some subgroup G_2. Then, $G_1 = \langle \mathfrak{g}^{\overrightarrow{x}_1}, \ldots, \mathfrak{g}^{\overrightarrow{x}_k} \rangle$ and $G_2 = \langle \mathfrak{g}^{\overrightarrow{x}_{k+1}} \rangle$ for some linearly independent vectors $\overrightarrow{x}_1, \ldots, \overrightarrow{x}_{k+1}$. Let X be a $n \times n$ matrix over $\mathbb{F}_p$ with $\overrightarrow{x}_i$ as its i-th row. Note that X is invertible.

We know that B has a some special form by Theorem 4 so that B has at most $\frac{(k+1)(k+2)}{2}$ linearly independent rows: 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. We know that $\overrightarrow{v}B = \overrightarrow{0}$ for any vector $\overrightarrow{v} \in V$. Since the dimension of V is $\frac{k(k+1)}{2}$, B has at most $\frac{(k+1)(k+2)}{2}$ linear independent rows. (Recall B has $(k+1)^2$ rows and $(k+1)^2 = \frac{(k+1)(k+2)}{2} + \frac{k(k+1)}{2}$.)

Suppose that B has linear independent rows less than $\frac{(k+1)(k+2)}{2}$. We observe that

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

and similarly,

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

where $\overrightarrow{e}_i$ is the i-th canonical vector of $\mathbb{F}_p^{(k+1)^2}$. 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 $\overrightarrow{c} \cdot (X \otimes X)B = \overrightarrow{0} \in \mathbb{F}_p^m$. The existence of such a vector $\overrightarrow{c}$ implies that $e(G_2, G_2) \subset \mathbb{D}$. Then, it would be a contradiction with Lemma 1.

By hypothesis ($rank(B) < \frac{(k+1)(k+2)}{2}$), there exists a non-zero vector $\overrightarrow{r} \in \mathbb{F}_p^{(k+1)^2} \backslash V$ such that $\overrightarrow{r}B = \overrightarrow{0}$. For such an $\overrightarrow{r}$, we show that $\overrightarrow{r}(X^{-1} \otimes X^{-1})$ satisfies conditions for it to be $\overrightarrow{c}$ aforementioned. $\overrightarrow{r}(X^{-1} \otimes X^{-1}) \cdot (X \otimes X)B = \overrightarrow{r}B = \overrightarrow{0}$, so $\overrightarrow{r}(X^{-1} \otimes X^{-1})$ satisfies the first condition. Next, we argue that $\overrightarrow{r}(X^{-1} \otimes X^{-1})$'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 $\overrightarrow{x}_1, \ldots, \overrightarrow{x}_k$). 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. The $(k+1)^2$-th entry of $\overrightarrow{r}(X^{-1} \otimes X^{-1})$ is $\overrightarrow{r}(\hat{x}^t \otimes \hat{x}^t)$, and it is a non-zero constant multiple of $\overrightarrow{r}(\overrightarrow{w} \otimes \overrightarrow{w})^t$. By the second statement of Lemma 3, $\overrightarrow{r}(\overrightarrow{w} \otimes \overrightarrow{w})^t$ is non-zero with overwhelming probability. Therefore, we complete the proof of the second statement of theorem. □

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 $\overrightarrow{w} \in \mathbb{F}_p^{k+1}$.*

Proof. (1) Let $\overrightarrow{r} = (r_{1,1}, \ldots, r_{1,k+1}, r_{2,1}, \ldots, r_{2,k+1}, \ldots, r_{k+1,k+1})$, $\overrightarrow{w} = (w_1, \ldots, w_{k+1})$, and $\overrightarrow{z} = (z_1, \ldots, z_{k+1})$. Then, $\overrightarrow{r} \cdot (\overrightarrow{t} \otimes \overrightarrow{s})^t = \sum_{i,j \in [1,k+1]} r_{i,j} w_i z_j$. Since $\overrightarrow{r}$ is a non-zero vector, $\sum_{i,j \in [1,k+1]} r_{i,j} w_i z_j$ is a non-zero polynomial of degree at most 2 over $\mathbb{F}_p$ if we consider $w_1, \ldots, w_{k+1}, z_1, \ldots, z_{k+1}$ as variables. By Schwartz-Zippel lemma, we obtain $\Pr[\overrightarrow{r} \cdot (\overrightarrow{w} \otimes \overrightarrow{z})^t = 0] \le \frac{2}{p}$.

(2) Let $\overrightarrow{r} = (r_{1,1}, \ldots, r_{1,k+1}, r_{2,1}, \ldots, r_{2,k+1}, \ldots, r_{k+1,k+1})$, and $\overrightarrow{w} = (w_1, \ldots, w_{k+1})$. Then, $\overrightarrow{r} \cdot (\overrightarrow{w} \otimes \overrightarrow{w})^t = \sum_{1 \le i \le j \le k+1} (r_{i,j} + r_{j,i}) w_i w_j$. Since $\overrightarrow{r} \notin V$, there exists a (i,j) such that $(r_{i,j} + r_{j,i}) \neq 0$. Thus, $\sum_{1 \le i \le j \le k+1} (r_{i,j} + r_{j,i}) w_i w_j$ is a non-zero polynomial of degree at most 2 over $\mathbb{F}_p$ if we consider $w_1, \ldots, w_{k+1}$ as variables. By Schwartz-Zippel lemma, we obtain $\Pr[\overrightarrow{r} \cdot (\overrightarrow{w} \otimes \overrightarrow{w})^t = 0] \le \frac{2}{p}$. □

Lemma 4 *(Schwartz-Zippel) [33] Let $P \in \mathbb{F}_p[x_1, \ldots, x_{k+1}]$ be a non-zero polynomial of degree $d \ge 0$ over $\mathbb{F}_p$. Then,*

$$\Pr[P(t_1, t_2, \ldots, t_{k+1}) = 0] \le \frac{d}{p},$$

where the probability goes over the randomness for uniformly choosing $t_1, \ldots, t_{k+1}$.

3.5 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 as 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 an exponentiation $e(g,h)^6$ instead of performing a bilinear pairing. Since we want to consider the computational cost of e in general 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 5 *(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 4. From Theorem 4, 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 4). Theorem 5 implies that $\mathcal{G}_k^{I_{(k+1)^2}}$ is optimal. Therefore, we obtain the following theorem.

Theorem 6 *$\mathcal{G}_k^{I_{(k+1)^2}}$ 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 5 *τ is a bijective map.*

Proof. If $\frac{i(i-1)}{2} + j = \frac{i'(i'-1)}{2} + j'$ for some $1 \leq j' \leq i' \leq k+1$, then

$$(i - i')\frac{i' + i - 1}{2} = (j' - j).$$

If $i = i'$, then $j' = j$. Otherwise, without loss of generality we assume that $i' < i$. Then, the left-hand side is larger than or equal to i', but the right-hand side is less than i'. Therefore, $i' = i$ and $j' = j$, so that τ is injective. Since τ is injective and the size of the domain of τ and the size of the range of τ are equal, τ is surjective, too. □

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

Description of A_ℓ (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 7 provides the desired result.

Theorem 7 *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 $\mathcal{G}_k^B$.*

Proof. We can denote A_ℓ by $A_{i,j}$ for $\tau^{-1}(\ell) = (i, j)$ since τ is bijective. By definition, $A_{i,i}$ has 1 in only entry (i, i) and zeros elsewhere. All column vectors of $\{A_{i,i}\}_{i \in [1,k+1]}$ span $\mathbb{F}_p^{k+1}$ and all row vectors of $\{A_{i,i}\}_{i \in [1,k+1]}$ span $\mathbb{F}_p^{k+1}$. Therefore, e is non-degenerate by Theorem 3. Since each A_ℓ is symmetric, $\mathcal{G}_k^B$ is symmetric by Theorem 4.

Next, we show that $\mathcal{G}_k^B$ is projecting. $G_1 = \langle \mathfrak{g}^{\overrightarrow{x}_1}, \ldots, \mathfrak{g}^{\overrightarrow{x}_k} \rangle$ for some set of linearly independent vectors $\{\overrightarrow{x}\}_{i \in [1,k]}$. Choose a vector $\overrightarrow{x}_{k+1}$ $\mathbb{F}_p^{k+1}$ such that $\overrightarrow{x}_1, \ldots, \overrightarrow{x}_{k+1}$ are linearly independent. Let $G_2 = \langle \mathfrak{g}^{\overrightarrow{x}_{k+1}} \rangle$. Let X be a $(k+1) \times (k+1)$ matrix such that the i-th row of X is $\overrightarrow{x}_i$. To show that $\mathcal{G}_k^B$ is projecting, we show that $e(G_2, G_2) \neq \{1_t\}$ and $e(G_2, G_2) \cap \mathbb{D} = \{1_t\}$, where $\mathbb{D}$ is a group generated by by all elements in $e(G_1, G)$. Then, it is easy to check natural projections $\pi : G \to G_2$, $\pi_t : G_t \to e(G_2, G_2)$ and $G_t' := \mathbb{D}$ satisfy conditions for being projecting; (1) $\pi(G) = G_2 \neq \{1_G\}$, $\pi_t(e(G, G)) = e(G_2, G_2) \neq \{1_t\}$, (2) $G_1 \subset \ker(\pi)$, $G_t' = \mathbb{D} \subset \ker(\pi_t)$, and (3) $\pi_t(e(g_1 g_2, h_1 h_2)) = \pi_t(e(g_1, h_1) e(g_2, h_1) e(g_1, h_2)\ e(g_2, h_2)) = e(g_2, h_2) = e(\pi(g_1 g_2), \pi(h_1 h_2))$ for any $g_1, h_1 \in G_1$ and $g_2, h_2 \in G_2$. We know that

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

and

$$\mathbb{D} = \langle \hat{e}(\mathfrak{g}, \mathfrak{g})^{(\overrightarrow{x}_i \otimes \overrightarrow{x}_j) B} : i \in [1, k] \text{ or } j \in [1, k] \rangle.$$

Let Z be a $\frac{(k+1)(k+2)}{2} \times (k+1)^2$ matrix such that its ℓ-th row is $\overrightarrow{x}_i \otimes \overrightarrow{x}_j$ for $\ell = \frac{(k+2-i)(k+1-i)}{2} + k + 2 - j$ and $1 \leq i \leq j \leq k+1$ and let $D = ZB$. Then, by definition of D,

$$e(G_2, G_2) = \langle \hat{e}(\mathfrak{g}, \mathfrak{g})^{\overrightarrow{e}_1 D} \rangle$$

and

$$\mathbb{D} = \langle \hat{e}(\mathfrak{g}, \mathfrak{g})^{\overrightarrow{e}_2 D}, \ldots, \hat{e}(\mathfrak{g}, \mathfrak{g})^{\overrightarrow{e}_{\frac{(k+1)(k+2)}{2}} D} \rangle,$$

where $\overrightarrow{e}_i$ is the i-th canonical vector in $\mathbb{F}_p^{\frac{(k+1)(k+2)}{2}}$. By Lemma 6, D is invertible so that we obtain the desired result that $e(G_2, G_2) \neq \{1_t\}$ and $e(G_2, G_2) \cap \mathbb{D} = \{1_t\}$.

Since for $i = j$, $A_{i,j}$ has only one non-zero entry, and for $i \neq j$ $A_{i,j}$ has two non-zero entries, there are $(k+1)^2$ non-zero entries in all $\{A_{i,j}\}$. Since all non-zero entires are 1, e requires only $(k+1)^2$ $\hat{e}$-computations (without additional exponentiations). Therefore, the proposed $\mathcal{G}_k^B$ is optimal: that is, e requires $(k+1)^2$ $\hat{e}$-computations, and $G_t = \mathbb{G}_t^{\frac{(k+1)(k+2)}{2}}$. □

Lemma 6 *Let B be a $(k+1)^2 \times \frac{(k+1)(k+2)}{2}$ matrix defined as above. Let $\{\overrightarrow{x}_i\}_{i\in[1,k+1]}$ be a set of linearly independent vectors in $\mathbb{F}_p^{k+1}$. Let Z be a $\frac{(k+1)(k+2)}{2} \times (k+1)^2$ matrix such that its ℓ-th row is $\overrightarrow{x}_i \otimes \overrightarrow{x}_j$ for $\ell = \frac{(k+2-i)(k+1-i)}{2} + k + 2 - j$ and $1 \leq i \leq j \leq k+1$. Then, Z is well-defined and $D = ZB$ is an invertible $\frac{(k+1)(k+2)}{2} \times \frac{(k+1)(k+2)}{2}$ matrix.*

Proof. Let $I = k + 2 - i$ and $J = k + 2 - j$. Then, I and J satisfy $\ell = \frac{I(I-1)}{2} + J$ and $1 \leq J \leq I \leq n$. By Lemma 5, there is one-to-one correspondence between so ℓ and (I, J) such that I and J satisfy $\ell = \frac{I(I-1)}{2} + J$ and $1 \leq J \leq I \leq n$. Therefore, Z is well-defined.

We show that D's rank is $\frac{(k+1)(k+2)}{2}$. By the definition of Z, Z is a part of $X \otimes X$ (in the sense that each row of Z is also row of $X \otimes X$). Let $\bar{Z}$ be a $\frac{k(k+1)}{2} \times (k+1)$ matrix, which is a disjoint part of $X \otimes X$ from Z. By the definition of B, a rank of $(X \otimes X)B$ is equal to that of D. (By definition of B, for each row $\overrightarrow{x}_j \otimes \overrightarrow{x}_i \in \bar{Z}$, there exists a $\overrightarrow{x}_i \otimes \overrightarrow{x}_j \in Z$ such that $(\overrightarrow{x}_j \otimes \overrightarrow{x}_i)B = (\overrightarrow{x}_i \otimes \overrightarrow{x}_j)B$.) B's rank is $\frac{(k+1)(k+2)}{2}$ (by the definition of B) and $X \otimes X$'s rank is $(k+1)^2$ (by the property of the *tensor product*). Therefore, $(X \otimes X)B$'s rank is $\frac{(k+1)(k+2)}{2}$ so that the rank of D is also $\frac{(k+1)(k+2)}{2}$; Hence, D is invertible. □

Our definition of projecting requires only the existence of homomorphisms satisfying some conditions. However, some applications (e.g., 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. Let $G_1 = \langle \mathfrak{g}^{\overrightarrow{x}_1}, \ldots, \mathfrak{g}^{\overrightarrow{x}_k} \rangle$ and $G_2 = \langle \mathfrak{g}^{\overrightarrow{x}_{k+1}} \rangle$ such that $\overrightarrow{x}_1, \ldots, \overrightarrow{x}_{k+1}$ are linearly independent vectors in $\mathbb{F}_p^{k+1}$. We construct two projections $\pi : G \to G_2$ and $\pi_t : G_t \to e(G_2, G_2)$. Let U be a $(k+1) \times (k+1)$ diagonal matrix with 1 in the entry $(k+1, k+1)$ and zeros elsewhere, and V be a $\frac{(k+1)(k+2)}{2} \times \frac{(k+1)(k+2)}{2}$ diagonal matrix with 1 in the entry $(1, 1)$ and zeros elsewhere. Let Z and B be defined in Lemma 6. Then, D is invertible. Define π and π_t by

$$\pi(g) := g^{X^{-1}UX} \quad \text{and} \quad \pi_t(g_t) := g_t^{D^{-1}VD}.$$

Now, we show that π and π_t are projections. Every element $g \in G$ can be written as $\mathfrak{g}^{\sum_{i\in[1,k+1]} a_i \overrightarrow{e}_i X}$ for some $a_i \in \mathbb{F}_p$.

$$\pi(g) = \pi(\mathfrak{g}^{\sum_{i\in[1,k+1]} a_i \overrightarrow{e}_i X}) = (\mathfrak{g}^{\sum_{i\in[1,k+1]} a_i \overrightarrow{e}_i X})^{X^{-1}UX} = \mathfrak{g}^{a_{k+1}\overrightarrow{e}_{k+1}X}.$$

Therefore, π is a projection to G_2. Similarly, element $g_t \in G_t$ can be written as $e(\mathfrak{g}, \mathfrak{g})^{\sum_{i\in[1,\frac{(k+1)(k+2)}{2}]} a_i \overrightarrow{e}_i D}$ for some $a_i \in \mathbb{F}_p$.

$$\pi_t(g_t) = \pi(e(\mathfrak{g}, \mathfrak{g})^{\sum_{i\in[1,\frac{(k+1)(k+2)}{2}]} a_i \overrightarrow{e}_i D}) = (e(\mathfrak{g}, \mathfrak{g})^{\sum_{i\in[1,\frac{(k+1)(k+2))}{2}]} a_i \overrightarrow{e}_i D})^{D^{-1}VD} = e(\mathfrak{g}, \mathfrak{g})^{a_1 \overrightarrow{e}_1 D}.$$

Therefore, π_t is a projection to $e(G_2, G_2)$. From the relation $G = G_1 \oplus G_2$, we know that elements g', g'' in G can be uniquely written as $g' = g_1' g_2'$ and $g'' = g_1'' g_2''$, where $g_1', g_1'' \in G_1$ and $g_2', g_2'' \in G_2$. Then,

$$\pi_t(e(g', g'')) = \pi_t(e(g_1', g_1'')e(g_1', g_2'')e(g_2', g_1'')e(g_2', g_2'')) = e(g_2', g_2'') = e(\pi(g'), \pi(g'')),$$

so π, π_t, and $G_t' := \mathbb{D}$, where $\mathbb{D}$ is the smallest subgroup containing $e(G, G_1)$, satisfy the projecting property. The first equality follows from the bilinearity of e, the second follows from the definition of π_t, and the third follows from the definition of π.

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 9×6 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 7, $\mathcal{G}_2^{B^*}$ is optimal projecting symmetric: Since B^* is a 9×6 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.

5.1 Groth-Sahai Non-Interactive Proof System under DLIN Assumption

We create a new instantiation of the Groth-Sahai non-interactive proof system for several types of quadratic equations [22]. The proposed instantiation uses $\mathcal{G}_2^{B^*}$ in example 2, which is symmetric and projecting. Since $\mathcal{G}_2^{B^*}$ is optimal (in the sense of Definition 6), our instantiation provides efficient verification algorithms. (In Groth-Sahai non-interactive proof system, the bilinear pairing operations and the exponentiations in G_t are used to verify the proofs.)

First we review the formal definition of non-interactive proof system for the Groth-Sahai proofs. Let R be a ternary relation consists of the setup gk, the statement x and the witness w. In our instantiation, gk is a bilinear group description. We let L be the language consisting of statements x with a witness w in R for a given some gk. The Groth-Sahai non-interactive proof system consists of four algorithms: a setup algorithm Setup, a common reference string (CRS) generation algorithm K, a prover P, and a verifier V. The setup algorithm takes the security parameter λ as input and outputs a setup (gk, sk). In our instantiation, sk is empty string.[6] The CRS generation algorithm K takes (gk, sk) as input and outputs a CRS σ. The prover P takes (gk, σ, x, w) as input and outputs a proof Θ. The verifier V takes (gk, σ, x, Θ) and outputs 1 if the proof Θ is acceptable and 0 otherwise. We say these four algorithms (Setup, K, P, V) are a non-interactive proof system for the relation R with setup algorithm Setup if it satisfies the following definitions of the completeness and soundness properties.

Definition 7 *We say that (Setup, K, P, V) is perfectly complete if for all adversaries $\mathcal{A}$,*

$$\Pr\left[\mathsf{V}(gk, \sigma, x, \Theta) = 1 \text{ if } (gk, x, w) \in R \middle| \begin{array}{l} (gk, sk) \xleftarrow{\$} \mathsf{Setup} \;\; ; \sigma \xleftarrow{\$} \mathsf{K}(gk, sk); \\ (x, w) \xleftarrow{\$} \mathcal{A}(gk, \sigma) \; ; \Theta \xleftarrow{\$} \mathsf{P}(gk, \sigma, x, w) \end{array}\right] = 1.$$

[6] The Groth-Sahai's instantiation in composite-order group requires sk to be factorization information of the group order.

Definition 8 *We say that (Setup, K, P, V) is perfectly sound if for all adversaries $\mathcal{A}$,*

$$\Pr\left[\mathsf{V}(gk,\sigma,x,\Theta)=1 \text{ if } x\notin L \middle| \begin{array}{l}(gk,sk)\xleftarrow{\$}\mathsf{Setup} \quad ;\sigma\xleftarrow{\$}\mathsf{K}(gk,sk);\\ (x,\Theta)\xleftarrow{\$}\mathcal{A}(gk,\sigma)\end{array}\right]=0.$$

We give the definition of non-interactive proof system with composable witness-indistinguishability.

Definition 9 *We say that (Setup, K, P, V) is composable witness-indistinguishable if there exists a probability polynomial time simulator $\mathcal{S}$, such that for all non-uniform polynomial time adversaries $\mathcal{A}$,*

$$\left|\Pr\left[\mathcal{A}(gk,\sigma)=1\middle|\begin{array}{l}(gk,sk)\xleftarrow{\$}\mathsf{Setup};\\ \sigma\xleftarrow{\$}\mathsf{K}(gk,sk)\end{array}\right]-\Pr\left[\mathcal{A}(gk,\sigma)=1\middle|\begin{array}{l}(gk,sk)\xleftarrow{\$}\mathsf{Setup};\\ \sigma\xleftarrow{\$}\mathcal{S}(gk,sk)\end{array}\right]\right|$$

is negligible in the security parameter, and for all adversaries $\mathcal{A}$

$$\begin{aligned}&\Pr\left[\mathcal{A}(\Theta)=1\middle|\begin{array}{ll}(gk,sk)\xleftarrow{\$}\mathsf{Setup} & ;\sigma\xleftarrow{\$}\mathcal{S}(gk,sk);\\ (x,w_0,w_1)\xleftarrow{\$}\mathcal{A}(gk,\sigma) \text{ such that } (gk,x,w_0),(gk,x,w_1)\in R & ;\Theta\xleftarrow{\$}\mathsf{P}(gk,\sigma,x,w_0)\end{array}\right]\\ =&\Pr\left[\mathcal{A}(\Theta)=1\middle|\begin{array}{ll}(gk,sk)\xleftarrow{\$}\mathsf{Setup} & ;\sigma\xleftarrow{\$}\mathcal{S}(gk,sk);\\ (x,w_0,w_1)\xleftarrow{\$}\mathcal{A}(gk,\sigma) \text{ such that } (gk,x,w_0),(gk,x,w_1)\in R & ;\Theta\xleftarrow{\$}\mathsf{P}(gk,\sigma,x,w_1)\end{array}\right].\end{aligned}$$

The common reference string generated by K contains *soundness string* and the description of imbedding functions and the commitment schemes. The simulated common reference string generated by $\mathcal{S}$ consists of *witness-indistinguishability (WI) string* and the description of imbedding functions and the commitment schemes. We describe Setup, soundness string, WI string, imbedding functions and commitment schemes below.

$\mathsf{Setup}(\lambda)$	$\mathcal{G}_2^{B^*}(\lambda)\xrightarrow{\$}(p,G,G_1,G_t,e)$. Set $g_2=(1_{\mathbb{G}},1_{\mathbb{G}},\mathfrak{g})\in G$, where $\mathfrak{g}$ is a generator of $\mathbb{G}$ and $G=\mathbb{G}^3$. and set $gk=(p,G,G_1,G_t,e,g_2)$.
Soundness string	On input gk, set $\sigma=(p,G,G_1,G_t,e,u_1,u_2,u_3)$, where $u_1,u_2,u_3\xleftarrow{\$}G_1$.
WI string	On input gk, set $\sigma=(p,G,G_1,G_t,e,u_1,u_2,u_3)$, where $u_1,u_2,u_2'\xleftarrow{\$}G_1, u_3=u_3'g_2^{-1}$.
Imbedding Functions	Let $G_2=\langle g_2\rangle$, and $G_2'=\langle u_3g_2\rangle$. $\iota_{G_2}: \mathbb{G}\to G_2;\ \mathcal{X}\mapsto(1_{\mathbb{G}},1_{\mathbb{G}},\mathcal{X})$, $\iota_{G_2'}: \mathbb{F}_p\to G_2';\ x\mapsto(u_3g_2)^x$, $\iota_{e(G_2,G_2)}: \mathbb{G}_t\to e(G_2,G_2);\ \mathcal{Z}_t\mapsto(1_{\mathbb{G}_t},1_{\mathbb{G}_t},1_{\mathbb{G}_t},1_{\mathbb{G}_t},1_{\mathbb{G}_t},\mathcal{Z}_t)$, $\iota_{e(G_2,G_2')}: \mathbb{G}\to e(G_2,G_2');\ \mathcal{Z}\mapsto e(\iota_{G_2}(\mathcal{Z}),\iota_{G_2'}(1))$, $\iota_{e(G_2',G_2')}: \mathbb{F}_p\to e(G_2',G_2');\ z\mapsto e(\iota_{G_2'}(z),\iota_{G_2'}(1))$, where $\mathfrak{g}_t=\hat{e}(\mathfrak{g},\mathfrak{g})$.
Commitment Schemes	$\mathsf{C}_{G_2}(\mathcal{X})=\iota_{G_2}(\mathcal{X})u_1^{r_1}u_2^{r_2}u_3^{r_3}$ for $r_1,r_2,r_3\xleftarrow{\$}\mathbb{F}_p$, $\mathsf{C}_{G_2'}(x)=\iota_{G_2'}(x)u_1^{r_1}u_2^{r_2}$ for $r_1,r_2\xleftarrow{\$}\mathbb{F}_p$

Note that $G_2\cap G_1=\{1_G\}$ (with overwhelming probability), and in the soundness setting $G_2'\cap G_1=\{1_G\}$ (with overwhelming probability). Imbedding functions $\iota_{G_2},\iota_{G_2'},\iota_{e(G_2,G_2)}$, $\iota_{e(G_2,G_2')}$ and $\iota_{e(G_2',G_2')}$ are group homomorphisms, where we consider $\mathbb{G}$, $\mathbb{G}_t$, G, G_t as multiplicative groups, and $\mathbb{F}_p$ as an additive group.

Lemma 7 *If the soundness string is given, the commitment schemes C_{G_2} and $\mathsf{C}_{G_2'}$ are perfectly binding, and if the witness-indistinguishability string is given, C_{G_2} and $\mathsf{C}_{G_2'}$ are perfectly hiding.*

Proof. In the soundness setting, suppose that for some $\mathcal{X}, \mathcal{Y} \in \mathbb{G}$, $\mathsf{C}_{G_2}(\mathcal{X}) = \iota_{G_2}(\mathcal{X}) u_1^{r_1} u_2^{r_2} u_3^{r_3}$ is equal to $\mathsf{C}_{G_2}(\mathcal{Y}) = \iota_{G_2}(\mathcal{Y}) u_1^{s_1} u_2^{s_2} u_3^{s_3}$. Then $\iota_{G_2}(\mathcal{X}) \cdot \iota_{G_2}(\mathcal{Y})^{-1} = u_1^{s_1 - r_1} u_2^{s_2 - r_2} u_3^{s_3 - r_3} \in \langle u_1, u_2, u_3 \rangle = G_1$. By definition of ι_{G_2}, $\iota_{G_2}(\mathcal{X}) \cdot \iota_{G_2}(\mathcal{Y})^{-1} = (1_{\mathbb{G}}, 1_{\mathbb{G}}, \mathcal{X} \cdot \mathcal{Y}^{-1}) \in G_2$. Since $G_1 \cap G_2 = \{1_G\}$, we obtain $\mathcal{X} = \mathcal{Y}$. Therefore, C_{G_2} is perfectly binding.

In the soundness setting, suppose that for some $x, y \in \mathbb{F}_p$, $\mathsf{C}_{G_2'}(x) = \iota_{G_2'}(x) u_1^{r_1} u_2^{r_2}$ is equal to $\mathsf{C}_{G_2'}(y) = \iota_{G_2'}(y) u_1^{s_1} u_2^{s_2}$. Then $\iota_{G_2'}(x) \cdot \iota_{G_2'}(y)^{-1} = u_1^{s_1 - r_1} u_2^{s_2 - r_2} \in \langle u_1, u_2 \rangle = G_1$. By definition of $\iota_{G_2'}$, $\iota_{G_2'}(x) \cdot \iota_{G_2'}(y)^{-1} = (u_3 g_2)^{x-y}$. Since $u_3 g_2 \notin G_1$, we obtain $x = y$. Therefore, $\mathsf{C}_{G_2'}$ is perfectly binding.

In the witness-indistinguishability setting, $\mathsf{C}_{G_2}(\mathcal{X})$ is uniformly distributed in G regardless of $\mathcal{X}$ since u_1, u_2, and u_3 span G. In the witness-indistinguishability setting, $\mathsf{C}_{G_2'}(x)$ is uniformly distributed in G_1 regardless of x since u_1 and u_2 span G_1, and $\iota_{G_2'}(x) = u_3^{lx} \in G_1$. Therefore, C_{G_2} and $\mathsf{C}_{G_2'}$ are perfectly hiding. □

We give a non-interactive proof system for the following equation

$$\prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{A_j}), \iota_{S_2}(\mathsf{Y_j})) \prod_{i=1}^{\mu} e(\iota_{S_1}(\mathsf{X_i}), \iota_{S_2}(\mathsf{B_i})) \prod_{i=1}^{\mu} \prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{X_i}), \iota_{S_2}(\mathsf{Y_j}))^{\gamma_{ij}} = \iota_{e(S_1,S_2)}(\mathsf{Z}), \tag{1}$$

where $\mathsf{A_j} \in S_1$, $\mathsf{B_i} \in S_2$, $\mathsf{Z} \in Dom(\iota_{e(S_1,S_2)})$ are constants, $\mathsf{X_i} \in S_1$, $\mathsf{Y_j} \in S_2$ are variables, $S_1, S_2 \in \{G_2, G_2'\}$, and commitments $\mathsf{C}_{S_1}(\mathsf{X_i})$ and $\mathsf{C}_{S_2}(\mathsf{Y_j})$ are given. This equation covers all equations considered in [22]. In the next subsection, we show that this equation implies a pairing product equation, a multi-scalar multiplication equation in $\mathbb{G}$, and a quadratic equation in $\mathbb{F}_p$.

Proof: The prover takes the common reference string (imbedding functions, commitment schemes, and σ) and witness $\{\mathsf{X_i}\}_{i \in [1,\mu]}$, $\{\mathsf{Y_j}\}_{j \in [1,\nu]}$ as inputs. Then, the prover does as follows.

1. Commit to $\mathsf{X_i} \in S_1$ and $\mathsf{Y_j} \in S_2$ as

$$\mathsf{C}_{S_1}(\mathsf{X_i}) := \iota_{S_1}(\mathsf{X_i}) u_1^{r_{i1}} u_2^{r_{i2}} u_3^{r_{i3}}, \quad \mathsf{C}_{S_2}(\mathsf{Y_j}) := \iota_{S_2}(\mathsf{Y_j}) u_1^{r'_{j1}} u_2^{r'_{j2}} u_3^{r'_{j3}},$$

$$\text{where } \begin{cases} r_{i1}, r_{i2}, r_{i3} \xleftarrow{\$} \mathbb{F}_p & \text{if } S_1 = G_2 \\ r_{i1}, r_{i2} \xleftarrow{\$} \mathbb{F}_p \text{ and } r_{i3} = 0 & \text{if } S_1 = G_2' \end{cases}, \text{ and } \begin{cases} r'_{j1}, r'_{j2}, r'_{j3} \xleftarrow{\$} \mathbb{F}_p & \text{if } S_2 = G_2 \\ r'_{j1}, r'_{j2} \xleftarrow{\$} \mathbb{F}_p \text{ and } r'_{j3} = 0 & \text{if } S_2 = G_2' \end{cases}.$$

2. Choose $\zeta_1, \zeta_2, \eta \xleftarrow{\$} \mathbb{F}_p$ and make a proof $(\Theta_1, \Theta_2, \Theta_3)$ as follows.

$$\Theta_1 = \prod_{j=1}^{\nu} \iota_{S_1}(\mathsf{A_j})^{r'_{j1}} \prod_{i=1}^{\mu} \iota_{S_2}(\mathsf{B_i})^{r_{i1}} \prod_{i=1}^{\mu} \prod_{j=1}^{\nu} \iota_{S_1}(X_i)^{r'_{j1}\gamma_{ij}} \mathsf{C}_{S_2}(\mathsf{Y}_j)^{r_{i1}\gamma_{ij}} \cdot (u_2^{\zeta_1} u_3^{\zeta_2}),$$

$$\Theta_2 = \prod_{j=1}^{\nu} \iota_{S_1}(\mathsf{A_j})^{r'_{j2}} \prod_{i=1}^{\mu} \iota_{S_2}(\mathsf{B_i})^{r_{i2}} \prod_{i=1}^{\mu} \prod_{j=1}^{\nu} \iota_{S_1}(X_i)^{r'_{j2}\gamma_{ij}} \mathsf{C}_{S_2}(\mathsf{Y}_j)^{r_{i2}\gamma_{ij}} \cdot (u_1^{-\zeta_1} u_3^{\eta}),$$

$$\Theta_3 = \prod_{j=1}^{\nu} \iota_{S_1}(\mathsf{A_j})^{r'_{j3}} \prod_{i=1}^{\mu} \iota_{S_2}(\mathsf{B_i})^{r_{i3}} \prod_{i=1}^{\mu} \prod_{j=1}^{\nu} \iota_{S_1}(X_i)^{r'_{j3}\gamma_{ij}} \mathsf{C}_{S_2}(\mathsf{Y}_j)^{r_{i3}\gamma_{ij}} \cdot (u_1^{-\zeta_2} u_2^{-\eta}).$$

For notational convenience, let $\overrightarrow{\Theta} := (\Theta_1, \Theta_2, \Theta_3)$. Return a proof $\overrightarrow{\Theta}$ for the satisfiability of the equation (1).

Verification: Given committed values $\{\mathsf{C}_{S_1}(\mathsf{X_i})\}_{i\in[1,\mu]}$, $\{\mathsf{C}_{S_2}(\mathsf{Y_j})\}_{j\in[1,\nu]}$ and a proof $\overrightarrow{\Theta}$, check

$$\prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{A_j}),\mathsf{C}_{S_2}(\mathsf{Y_j}))\prod_{i=1}^{\mu} e(\mathsf{C}_{S_1}(\mathsf{X_i}),\iota_{S_2}(\mathsf{B_i}))\prod_{i=1}^{\mu}\prod_{j=1}^{\nu} e(\mathsf{C}_{S_1}(\mathsf{X_i}),\mathsf{C}_{S_2}(\mathsf{Y_j}))^{\gamma_{ij}} \stackrel{?}{=} \iota_{e(S_1,S_2)}(\mathsf{Z})\prod_{i=1}^{3} e(u_i,\Theta_i),$$

and accept the proof if and only if it holds. We call the above equation by the verification equation.

We show that the above non-interactive proof system satisfies perfect completeness (no matter σ is the soundness string or the witness-indistinguishability string), perfect soundness (where σ is the soundness string), and composable witness-indistinguishability.

Theorem 8 *The above protocol satisfies perfect completeness.*

Proof. We show that an honestly generated proof $\overrightarrow{\Theta}$ will be accepted. On substituting $\mathsf{C}_{S_1}(\mathsf{X_i})$ and $\mathsf{C}_{S_2}(\mathsf{Y_j})$ in the left-hand side of the verification equation with

$$\mathsf{C}_{S_1}(\mathsf{X_i}) = \iota_{S_1}(\mathsf{X_i})u_1^{r_{i1}}u_2^{r_{i2}}u_3^{r_{i3}} \text{ and } \mathsf{C}_{S_2}(\mathsf{Y_j}) = \iota_{S_2}(\mathsf{Y_j})u_1^{r'_{j1}}u_2^{r'_{j2}}u_3^{r'_{j3}},$$

we obtain

$$\begin{aligned}
&\textstyle\prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{A_j}),\iota_{S_2}(\mathsf{Y_j})u_1^{r'_{j1}}u_2^{r'_{j2}}u_3^{r'_{j3}})\prod_{i=1}^{\mu} e(\iota_{S_1}(\mathsf{X_i})u_1^{r_{i1}}u_2^{r_{i2}}u_3^{r_{i3}},\iota_{S_2}(\mathsf{B_i}))\\
&\qquad\cdot\textstyle\prod_{i=1}^{\mu}\prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{X_i})u_1^{r_{i1}}u_2^{r_{i2}}u_3^{r_{i3}},\iota_{S_2}(\mathsf{Y_j})u_1^{r'_{j1}}u_2^{r'_{j2}}u_3^{r'_{j3}})^{\gamma_{ij}}\\
=\ &\iota_{e(S_1,S_2)}(\mathsf{Z})\textstyle\prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{A_j}),u_1^{r'_{j1}}u_2^{r'_{j2}}u_3^{r'_{j3}})\prod_{i=1}^{\mu} e(u_1^{r_{i1}}u_2^{r_{i2}}u_3^{r_{i3}},\iota_{S_2}(\mathsf{B_i}))\\
&\qquad\cdot\textstyle\prod_{i=1}^{\mu}\prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{X_i}),u_1^{r'_{j1}}u_2^{r'_{j2}}u_3^{r'_{j3}})^{\gamma_{ij}} e(u_1^{r_{i1}}u_2^{r_{i2}}u_3^{r_{i3}},\iota_{S_2}(\mathsf{Y_j})u_1^{r'_{j1}}u_2^{r'_{j2}}u_3^{r'_{j3}})^{\gamma_{ij}}\\
=\ &\iota_{e(S_1,S_2)}(\mathsf{Z})e(u_1,\textstyle\prod_{j=1}^{\nu}\iota_{S_1}(\mathsf{A_j})^{r'_{j1}}\prod_{i=1}^{\mu}\iota_{S_2}(\mathsf{B_i})^{r_{i1}}\prod_{i=1}^{\mu}\prod_{j=1}^{\nu}\iota_{S_1}(\mathsf{X_i})^{r'_{j1}\gamma_{ij}}\mathsf{C}_{S_2}(\mathsf{Y_j})^{r_{i1}\gamma_{ij}})\\
&\qquad\cdot e(u_2,\textstyle\prod_{j=1}^{\nu}\iota_{S_1}(\mathsf{A_j})^{r'_{j2}}\prod_{i=1}^{\mu}\iota_{S_2}(\mathsf{B_i})^{r_{i2}}\prod_{i=1}^{\mu}\prod_{j=1}^{\nu}\iota_{S_1}(\mathsf{X_i})^{r'_{j2}\gamma_{ij}}\mathsf{C}_{S_2}(\mathsf{Y_j})^{r_{i2}\gamma_{ij}})\\
&\qquad\cdot e(u_3,\textstyle\prod_{j=1}^{\nu}\iota_{S_1}(\mathsf{A_j})^{r'_{j3}}\prod_{i=1}^{\mu}\iota_{S_2}(\mathsf{B_i})^{r_{i3}}\prod_{i=1}^{\mu}\prod_{j=1}^{\nu}\iota_{S_1}(\mathsf{X_i})^{r'_{j3}\gamma_{ij}}\mathsf{C}_{S_2}(\mathsf{Y_j})^{r_{i3}\gamma_{ij}})\\
=\ &\iota_{e(S_1,S_2)}(\mathsf{Z})e(u_1,\Theta_1)e(u_2,\Theta_2)e(u_3,\Theta_3).
\end{aligned}$$

The first equality due to the statement equation (1). □

Note that $(u_2^{\zeta_1}u_3^{\zeta_2})$ in Θ_1, $(u_1^{-\zeta_1}u_3^{\eta})$ in Θ_2 and $(u_1^{-\zeta_2}u_2^{-\eta})$ in Θ_3 are used to blind other factors. On defining $\Theta'_1,\Theta'_2,\Theta'_3$ by removing these blinding factors from $\Theta_1,\Theta_2,\Theta_3$, we can check that $\Theta'_1,\Theta'_2,\Theta'_3$ will also satisfy perfect completeness.

Theorem 9 *The above protocol satisfies perfect soundness.*

Proof. When σ is the soundness string, u_1,u_2,u_3 are chosen from G_1 so that $G_1\cap S_1=\{1_G\}$ and $G_1\cap S_2=\{1_G\}$. (Recall that $S_1,S_2\in\{G_2,G'_2\}$, $G_2=\langle g_2\rangle$ and $G'_2=\langle u_3g_2\rangle$.) First, we argue that $G_t=e(S_1,S_2)\oplus\mathbb{D}$, where $\mathbb{D}$ is the smallest group containing $e(G_1,G)$. Since $\mathcal{G}_2^{B^*}$ is projecting, we obtain that $e(G_2,G_2)\not\subset\mathbb{D}$ by Lemma 1. This implies that $e(S_1,S_2)\not\subset\mathbb{D}$ no matter whether $S_1,S_2\in\{G_2,G'_2\}$. Since $e(S_1,S_2)$ is a cyclic group of order p, we obtain $G_t=e(S_1,S_2)\oplus\mathbb{D}$.

Since $G_t=e(S_1,S_2)\oplus\mathbb{D}$, we can define a natural projection $\pi_{e(S_1,S_2)}$ from G_t to $e(S_1,S_2)$ by $g'_tg''_t\mapsto g'_t$, where $g'_t\in e(S_1,S_2)$ and $g''_t\in\mathbb{D}$. (Since $G_t=e(S_1,S_2)\oplus\mathbb{D}$, every element in G_t can be uniquely written as $g'_tg''_t$ for some $g'_t\in e(S_1,S_2)$ and $g''_t\in\mathbb{D}$.)

Suppose that the verification equation holds. By applying $\pi_{e(S_1,S_2)}$ in the left-hand side of the verification equation, we obtain that

$$\begin{aligned}
&\pi_{e(S_1,S_2)}(\textstyle\prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{A_j}),\mathsf{C}_{S_2}(\mathsf{Y_j}))\prod_{i=1}^{\mu} e(\mathsf{C}_{S_1}(\mathsf{X_i}),\iota_{S_2}(\mathsf{B_i}))\prod_{i=1}^{\mu}\prod_{j=1}^{\nu} e(\mathsf{C}_{S_1}(\mathsf{X_i}),\mathsf{C}_{S_2}(\mathsf{Y_j}))^{\gamma_{ij}})\\
=\ &\textstyle\prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{A_j}),\iota_{S_2}(\mathsf{Y_j}))\prod_{i=1}^{\mu} e(\iota_{S_1}(\mathsf{X_i}),\iota_{S_2}(\mathsf{B_i}))\prod_{i=1}^{\mu}\prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{X_i}),\iota_{S_2}(\mathsf{Y_j}))^{\gamma_{ij}}.
\end{aligned}$$

The equality follows from the fact that $G_t = e(S_1, S_2) \oplus \mathbb{D}$. (Note that $\mathsf{C}_{S_\ell}(\cdot)$ consists of a product of an element in S_ℓ and an element in G_1, and for all $g_1, g_1' \in G_1$, $e(\iota_{S_1}(\cdot), g_1), e(g_1, \iota_{S_2}(\cdot)), e(g_1, g_1') \in \mathbb{D} \subset \ker(\pi_{e(S_1,S_2)})$.)

Applying $\pi_{e(S_1,S_2)}$ in the right-hand side of the verification equation, we get

$$\begin{aligned} &\pi_{e(S_1,S_2)}(\iota_{e(S_1,S_2)}(\mathsf{Z}) \textstyle\prod_{i=1}^{3} e(u_i, \Theta_i)) \\ &= \iota_{e(S_1,S_2)}(\mathsf{Z}). \end{aligned}$$

The equality also follows from the fact that $G_t = e(S_1, S_2) \oplus \mathbb{D}$ and $\pi_{e(S_1,S_2)}$ is a projection to $e(S_1, S_2)$. We applied $\pi_{e(S_1,S_2)}$ in the both sides of the verification equation. The result equation implies that the desired statement equation (1). □

Lemma 8 *If $\mathcal{G}_2^{B^*}$ satisfies the* subgroup decision assumption*, then the common reference string in the soundness setting is computationally indistinguishable from the common reference string in the witness-indistinguishability setting.*

Proof. We can prove by using the standard hybrid argument. Define $Game_1$, $Game_2$, and $Game_3$ as follows. In $Game_1$ $u_3 \xleftarrow{\$} G_1$, in $Game_2$ $u_3 \xleftarrow{\$} G$, and in $Game_3$ $u_3 = u_3' g_2^{-1}$ for $u_3' \xleftarrow{\$} G_1$. In all games $u_1, u_2 \xleftarrow{\$} G_1$. The subgroup decision assumption gives us the indistinguishability between $Game_1$ and $Game_2$, and the indistinguishability between $Game_2$ and $Game_3$. By the hybrid argument, $Game_1$ and $Game_3$ are indistinguishable by the subgroup decision assumption. Since $Game_1$ is identical to the soundness setting and $Game_3$ is identical to the witness-indistinguishability setting, we conclude the desired result. □

Lemma 9 *Let $(\Theta_1', \Theta_2', \Theta_3')$ be a special solution of an equation $\prod_{i=1}^{3} e(u_i, \mathcal{X}_i) = g_t$ for some $g_t \in G_t$, where (u_1, u_2, u_3) is CRS in the witness-indistinguishability setting, and $\mathcal{X}_1, \mathcal{X}_2$ and $\mathcal{X}_3$ are variables. For $\zeta_1, \zeta_2, \eta \xleftarrow{\$} \mathbb{F}_p$,*

$$(\Theta_1 := \Theta_1'(u_2^{\zeta_1} u_3^{\zeta_2}), \quad \Theta_2 := \Theta_2'(u_1^{-\zeta_1} u_3^{\eta}), \quad \Theta_3 := \Theta_3'(u_1^{-\zeta_2} u_2^{-\eta}))$$

is uniformly distributed in a solution set $\{(\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3) | \prod_{i=1}^{3} e(u_i, \mathcal{X}_i) = g_t\}$.

Proof. In the witness-indistinguishability setting, $G = \langle u_1, u_2, u_3 \rangle$ and $\{e(u_i, u_j)\}_{1 \le i \le j \le 3}$ is basis of $\mathbb{F}_p$-module G_t. (Recall that G_t's rank is 6.) Therefore, g_t can be uniquely written as $g_t = \prod_{1 \le i \le j \le 3} e(u_i, u_j)^{\alpha_{ij}}$ for some $\alpha_{ij} \in \mathbb{F}_p$. Re-define a variable $\mathcal{X}_i := u_1^{(i)} u_2^{(i)} u_3^{(i)}$ by using variables $u_j^{(i)} \in \langle u_j \rangle$. Since $g_t = \prod_{i=1}^{3} e(u_i, \mathcal{X}_i) = \prod_{i=1}^{3} \prod_{j=1}^{3} e(u_i, u_j^{(i)})$, we obtain

$$e(u_1, u_1^{(1)}) = e(u_1, u_1)^{\alpha_{11}}, \quad e(u_1, u_2^{(1)}) e(u_2, u_1^{(2)}) = e(u_1, u_2)^{\alpha_{12}}, \quad e(u_1, u_3^{(1)}) e(u_3, u_1^{(3)}) = e(u_1, u_3)^{\alpha_{13}},$$

$$e(u_2, u_2^{(2)}) = e(u_2, u_2)^{\alpha_{22}}, \quad e(u_2, u_3^{(2)}) e(u_3, u_2^{(3)}) = e(u_2 u_3)^{\alpha_{23}}, \quad e(u_3, u_3^{(3)}) = e(u_3, u_3)^{\alpha_{33}}.$$

Therefore, $u_1^{(1)}, u_2^{(2)}, u_3^{(3)}$ are fixed and there are p^3 solutions in the solution set. We can easily check that for each different tuple $(\zeta_1, \zeta_2, \eta) \in \mathbb{F}_p^3$,

$$(\Theta_1'(u_2^{\zeta_1} u_3^{\zeta_2}), \quad \Theta_2'(u_1^{-\zeta_1} u_3^{\eta}), \quad \Theta_3'(u_1^{-\zeta_2} u_2^{-\eta}))$$

is a different solution by the fact that (u_1, u_2, u_3) is a basis of $\mathbb{F}_p$-module G. Since there are p^3 number of (ζ_1, ζ_2, η)-tuples, $(\Theta_1 := \Theta_1'(u_2^{\zeta_1} u_3^{\zeta_2}))$, $\Theta_2 := \Theta_2'(u_1^{-\zeta_1} u_3^{\eta})$, $\Theta_3 := \Theta_3'(u_1^{-\zeta_2} u_2^{-\eta}))$ is uniformly distributed in the solution set. □

Theorem 10 *The above protocol satisfies composable witness-indistinguishability.*

Proof. Under the decisional linear assumption, $\mathcal{G}_2^{B^*}$ satisfies *subgroup decision assumption* by Theorem 1. By Lemma 8 the soundness string is computationally indistinguishable from the WI string. When the simulated common reference string generated by $\mathcal{S}$ is given, C_{S_i} is perfectly hiding. By Lemma 9, a proof $\overrightarrow{\Theta}$ is uniformly distributed in a solution set of the verification equation. Therefore, the committed values and the proof always have identical distribution regardless of the witness. □

Size-reduced non-interactive proof system when $S_1 = S_2 = G'_2$: If $S_1 = S_2 = G'_2$, then we can reduce the size of a proof by removing Θ_3 and slightly changing blinding factors in Θ_1 and Θ_2. Suppose that $S_1 = S_2 = G'_2$. Define

$$\overrightarrow{\Theta} = (\Theta_1, \Theta_2) := (\Theta'_1(u_2^{\zeta_1}),\ \Theta'_2(u_1^{-\zeta_1})),$$

and modify a verification equation to contain only Θ_1 and Θ_2 as follows.

$$\prod_{j=1}^{\nu} e(\iota_{G'_2}(\mathsf{A_j}), \mathsf{C}_{G'_2}(\mathsf{Y_j})) \prod_{i=1}^{\mu} e(\mathsf{C}_{G'_2}(\mathsf{X_i}), \iota_{G'_2}(\mathsf{B_i})) \prod_{i=1}^{\mu}\prod_{j=1}^{\nu} e(\mathsf{C}_{G'_2}(\mathsf{X_i}), \mathsf{C}_{G'_2}(\mathsf{Y_j}))^{\gamma_{ij}} \stackrel{?}{=} \iota_{e(G'_2,G'_2)}(\mathsf{Z}) \prod_{i=1}^{2} e(u_i, \Theta_i)$$

Then, similar arguments show that this protocol is also a non-interactive proof system with composable witness-indistinguishability for satisfiability of a quadratic equation over bilinear groups where the decisional linear assumption holds. Key observation of this size-reduced non-interactive proof system when $S_1 = S_2 = G'_2$ is that (1) Θ_3 contains only blinding factors ($r_{i3} = r'_{j3} = 0$), and (2) the images of $\iota_{G'_2}$ and $\mathsf{C}_{G'_2}$ are contained in G_1 in the witness-indistinguishability setting. Therefore, we can (independently) blind Θ_1 and Θ_2 by using only u_1 and u_2 instead of u_1, u_2 and u_3.

Note that by applying similar method of extending from the original Groth-Sahai non-interactive proof system with composable witness-indistinguishability for a quadratic equation to the one for a set of quadratic equations, ours for a quadratic equation can be extend to the one for a set of quadratic equations. Furthermore, we can also obtain a non-interactive zero-knowledge proof system for a set of quadratic equations by similar method as Groth-Sahai's.

Verification Complexity: For verification, $\mu\nu$ exponentiations in G_t, $\mu\nu + \mu + \nu + 3$ e-computations are required (if we ignore costs for multiplications in G_t and evaluations of imbedding functions). For each exponentiation in G_t and each e-computation, they cost 6 exponentiations in $\mathbb{G}_t$ and 9 $\hat{e}$-computations, respectively. Therefore, in total $6\mu\nu$ exponentiations in $\mathbb{G}_t$ and $9(\mu\nu + \mu + \nu + 3)$ pairing computations are required for verifying a quadratic equation.

Comparison with Instantiation of Groth-Sahai non-interactive proof system under DLIN: The proposed instantiation is similar to the Groth-Sahai's instantiation 3 (based on the DLIN assumption) since both follow the module-based abstraction of the Groth-Sahai proof system. The biggest differences are bilinear pairing e and the target group G_t. Groth and Sahai implicitly used a bilinear group generator that differs from ours.[7] They define a symmetric bilinear pairing e by using an asymmetric bilinear pairing $\bar{e}$ as follows: $e(g,h) = (\bar{e}(g,h))^{1/2}(\bar{e}(h,g))^{1/2} \in G_t = \mathbb{G}_t^9$, where $\bar{e}$ is defined by using a 9×9 identity matrix (i.e., $\bar{e}$ is the output of Freeman's asymmetric projecting bilinear group $\mathcal{G}_2^{I_9}$). They implicitly used a matrix B to define the bilinear group generator:

$$B = \begin{pmatrix}
\boxed{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \boxed{1/2} & 0 & \boxed{1/2} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \boxed{1/2} & 0 & 0 & 0 & \boxed{1/2} & 0 & 0 \\
0 & \boxed{1/2} & 0 & \boxed{1/2} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \boxed{1} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \boxed{1/2} & 0 & \boxed{1/2} & 0 \\
0 & 0 & \boxed{1/2} & 0 & 0 & 0 & \boxed{1/2} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \boxed{1/2} & 0 & \boxed{1/2} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \boxed{1}
\end{pmatrix}.$$

[7] In [22], they used notation F and B_T to denote a bilinear pairing and its target module, respectively; they are equivalent to our e and G_t, respectively.

However, we can improve the efficiency of the Groth-Sahai's symmetric bilinear pairing, though they do not mention how to improve efficiency of their construction. Since the second column and fourth column are equal, the third column and seventh column are equal, and the sixth column and eighth column are equal, we can remove the fourth, seventh, and eighth columns from B. Then, the resulting matrix has 6 columns and nine non-zero entries. Since the number of non-zero entries corresponds to the number of $\hat{e}$-computations, the resulting bilinear map costs 9 $\hat{e}$-computations. The 1/2 entries represent exponentiation, so that the resulting bilinear map requires 6 additional exponentiations in $\mathbb{G}_t$. (A map e in $\mathcal{G}_2^{B^*}$, which is used in our protocol, costs only 9 $\hat{e}$-computations and has no exponentiations in $\mathbb{G}_t$.) Therefore, the verification of the proposed protocol is slightly faster than that of the Groth-Sahai's DLIN instantiation. All components in a proof are elements in $\mathbb{G}$. Therefore, the size of the proof and the computational cost of the prover of the proposed protocol are the same as those of the Groth-Sahai's protocol.

5.2 Additional Details for Groth-Sahai Proofs

We show that the following equation implies a pairing product equation, a multi-scalar multiplication equation in $\mathbb{G}$, and a quadratic equation in $\mathbb{F}_p$.

$$\prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{A_j}), \iota_{S_2}(\mathsf{Y_j})) \prod_{i=1}^{\mu} e(\iota_{S_1}(\mathsf{X_i}), \iota_{S_2}(\mathsf{B_i})) \prod_{i=1}^{\mu}\prod_{j=1}^{\nu} e(\iota_{S_1}(\mathsf{X_i}), \iota_{S_2}(\mathsf{Y_j}))^{\gamma_{ij}} = \iota_{e(S_1,S_2)}(\mathsf{Z}), \tag{2}$$

Pairing product equation. Set $S_1 = S_2 = G_2$. The image of $e(\cdot,\cdot)$ consists of 6 elements in $\mathbb{G}_t$. The equation (2) implies entry-wise equations in G_t, that is, 6 equations in $\mathbb{G}_t$. We only focus on the last 6-th entry of the equation (2). By definition of e, we know that $e((1_\mathbb{G}, 1_\mathbb{G}, S), (1_\mathbb{G}, 1_\mathbb{G}, T)) = (1_t, \ldots, 1_t, \hat{e}(S,T)) \in G_t = \mathbb{G}_t^6$. Therefore, by definition of ι_{G_2} and $\iota_{e(G_2,G_2)}$, we obtain from the 6-th entry of the equation (2) the desired pairing product equation

$$\prod_{j=1}^{\nu} \hat{e}(\mathsf{A_j}, \mathsf{Y_j}) \prod_{i=1}^{\mu} \hat{e}(\mathsf{X_i}, \mathsf{B_i}) \prod_{i=1}^{\mu}\prod_{j=1}^{\nu} \hat{e}(\mathsf{X_i}, \mathsf{Y_j})^{\gamma_{ij}} = \mathsf{Z},$$

where $\mathsf{A_j}, \mathsf{B_i} \in \mathbb{G}$, $\mathsf{Z} \in \mathbb{G}_t$, $\gamma_{ij} \in \mathbb{F}_p$ are constants and $\mathsf{X_i}, \mathsf{Y_j} \in \mathbb{G}$ are variables.[8]

Multi-scalar multiplication equation in $\mathbb{G}$. Set $S_1 = G_2$ and $S_2 = G_2'$. We know that every element in the equation (2) is contained in $e(G_2, G_2')$, which is a cyclic group of order p, by definitions of ι_{G_2}, $\iota_{G_2'}$, and $\iota_{e(G_2,G_2')}$. Thus, we can take discrete logarithms of both sides of the equation (2) based on $e(g_2, u_3 g_2) \in e(G_2, G_2')$.

For $\mathsf{A_j}, \mathsf{X_i}, \mathsf{Z} \in \mathbb{G}$, these group elements uniquely determine field elements $\mathsf{a_j}, \mathsf{x_i}, \mathsf{z} \in \mathbb{F}_p$ such that $\mathsf{A_j} = \mathfrak{g}^{\mathsf{a_j}}$, $\mathsf{X_i} = \mathfrak{g}^{\mathsf{x_i}}$, and $\mathsf{Z} = \mathfrak{g}^{\mathsf{z}}$. Since $g_2 = (1_\mathbb{G}, 1_\mathbb{G}, \mathfrak{g})$, $\iota_{G_2}(\mathsf{A_j}) = (1_\mathbb{G}, 1_\mathbb{G}, \mathsf{A_j}) = g_2^{\mathsf{a_j}}$ and $\iota_{G_2}(\mathsf{X_i}) = (1_\mathbb{G}, 1_\mathbb{G}, \mathsf{X_i}) = g_2^{\mathsf{x_i}}$ and $\iota_{G_2}(\mathsf{Z}) = (1_\mathbb{G}, 1_\mathbb{G}, \mathsf{Z}) = g_2^{\mathsf{z}}$. If we compute the discrete logarithm of the equation (2) based on $e(g_2, u_3 g_2)$, then we obtain

$$\sum_{j=1}^{\nu} \mathsf{a_j}\mathsf{Y_j} + \sum_{i=1}^{\mu} \mathsf{x_i}\mathsf{B_i} + \sum_{i=1}^{\mu}\sum_{j=1}^{\nu} \gamma_{\mathsf{ij}}\mathsf{x_i}\mathsf{Y_j} = \mathsf{z} \pmod p.$$

This equation implies a multi-scalar multiplication equation in a cyclic group $\mathbb{G}$ of order p.

$$\prod_{j=1}^{\nu} \mathsf{A_j}^{\mathsf{Y_j}} \prod_{i=1}^{\mu} \mathsf{X_i}^{\mathsf{B_i}} \prod_{i=1}^{\mu}\prod_{j=1}^{\nu} (\mathsf{X_i}^{\mathsf{Y_j}})^{\gamma_{ij}} = \mathsf{Z},$$

where $\mathsf{A_j}, \mathsf{Z} \in \mathbb{G}$, $\mathsf{B_i}, \gamma_{ij} \in \mathbb{F}_p$ are constants and $\mathsf{X_i} \in \mathbb{G}$, $\mathsf{Y_j} \in \mathbb{F}_p$ are variables.

[8] If we set $\mathsf{B_i} = 1_G$, $m = n$, and $\mathsf{X_i} = \mathsf{Y_i}$ for all i, we can more simplify. The resulting simplified equation is equivalent the form of a pairing product equation in [22].

Quadratic equation in $\mathbb{F}_p$. Set $S_1 = S_2 = G'_2$. We know that both sides of the equation (2) is contained in $e(G'_2, G'_2)$, which is a cyclic group of order p. Thus, we can take discrete logarithms based on $e(u_3g_2, u_3g_2)$. If we compute the discrete logarithm of the equation (2) based on $e(g_2, g_2)$, then we obtain a quadratic equation in $\mathbb{F}_p$

$$\sum_{j=1}^{\nu} \mathsf{A_j}\mathsf{Y_j} + \sum_{i=1}^{\mu} \mathsf{X_i}\mathsf{B_i} + \sum_{i=1}^{\mu}\sum_{j=1}^{\nu} \gamma_{\mathsf{ij}}\mathsf{X_i}\mathsf{Y_j} = \mathsf{Z} \quad (\mod p),$$

where $\mathsf{A_j}, \mathsf{B_i}, \mathsf{Z}, \gamma_{ij} \in \mathbb{F}_p$ are constants and $\mathsf{X_i}, \mathsf{Y_j} \in \mathbb{F}_p$ are variables.[9]

5.3 Boneh-Goh-Nissim Cryptosystem under DLIN Assumption

Our second application of the optimal projecting symmetric bilinear pairings is the partially doubly homomorphic encryption scheme (BGN encryption scheme) of Boneh, Goh, and Nissim [10]. Given two ciphertexts, anyone can create a new ciphertext that encrypts the sum of two corresponding plaintexts. That is, the BGN encryption scheme is additive homomorphic. In addition, the BGN encryption scheme supports *one* multiplication (followed by arbitrary additions) of encrypted values. Since the BGN encryption scheme allows only *one* multiplication, we call it "partially doubly homomorphic" encryption scheme.

We give our instantiation of the BGN encryption scheme, which is proven secure under the DLIN assumption, in Figure 2. Our instantiation uses the projecting symmetric bilinear group generator $\mathcal{G}_2^{B^*}$ in the example 2. Note that $\mathcal{G}_2^{B^*}$ supports random samplings from G and G_1; The description of G (G_1, resp.) contains a basis of G (G_1, resp.), and linear combinations of basis with random coefficients are random elements in G (G_1, resp.). Furthermore, one can randomly samples from $\mathbb{D}$; For example, $\mathbb{D} = \langle e(u_1,u_1), e(u_1,u_2), e(u_1,g), e(u_2,u_2), e(u_2,g)\rangle$, where $G_1 = \langle u_1, u_2\rangle$ and $G = G_1 \oplus \langle g\rangle$. Thus, linear combinations of $e(u_1,u_1), e(u_1,u_2), e(u_1,g), e(u_2,u_2)$, and $e(u_2,g)$ with random coefficients are random elements in $\mathbb{D}$. Note that $G = G_1 \oplus G_2$ and $G_t = e(G_2, G_2) \oplus \mathbb{D}$, and π and π_t satisfy the projecting property with $G'_t = \mathbb{D}$.

For a ciphertext CT, if $CT \in G$, information about the corresponding plaintext M is contained in the exponent of $\pi(g)$. If $CT \in G_t$, then the corresponding plaintext information is contained in the exponent of $e(\pi(g), \pi(g)) = \pi_t(e(g,g))$. For ciphertexts CT_1 and CT_2, we can see that the output of Add contains the addition of messages of CT_1 and CT_2 either in the exponent of $\pi(g)$ (if both ciphertexts are in G) or in the exponent of $\pi_t(e(g,g))$ (if both ciphertexts are in G_t). Further, we can see that the output of $\mathsf{Multiply}$ contains the multiplication of two input ciphertexts in the exponent of $\pi_t(e(g,g))$. The correctness of decryption algorithm directly follows from the fact that CT contains the corresponding plaintext information either in the exponent of $\pi(g)$ (if $CT \in G$) or in the exponent of $\pi_t(e(g,g))$ (if $CT \in G_t$).

The semantic security of our instantiation of BGN cryptosystem follows from the subgroup decision assumption in G. In a ciphertext $CT \in G$, a blinding factor $g' \in G_1$ is indistinguishable from the element randomly chosen from G; Thus, CT is indistinguishable from an uniform element in G so that it leaks no information about the corresponding plaintext. The semantic security of ciphertexts in G_t follows from the semantic security of two input ciphertexts in G.

Theorem 11 *If $\mathcal{G}_1$ satisfies the DLIN assumption and $\mathcal{G}_2^{B^*}$ is constructed from $\mathcal{G}_1$ (as in the example 2), then the BGN cryptosystem instantiated with $\mathcal{G}_2^{B^*}$ is semantically secure.*

Ciphertext Size: A ciphertext of our instantiation of the BGN cryptosystem consists of an element in either G or G_t. By definition of $\mathcal{G}_2^{B^*}$, $G = \mathbb{G}^3$ and $G_t = \mathbb{G}_t^6$ so that a ciphertext consists of either 3 elements in G or 6 elements in G_t.

[9] If we set $\mathsf{A_j} = 0$, $n = m$, and $\mathsf{Y_j} = \mathsf{X_j}$ for all j, then we obtain a simplified equation that is equivalent to the form of a quadratic equation in [22].

$\mathsf{KeyGen}(\lambda)$

$\mathcal{G}_2^{B^*}(\lambda) \xrightarrow{\$} (p, G, G_1, G_t, e)$, where $G = \mathbb{G}^3$.
$\mathfrak{g} \xleftarrow{\$} \mathbb{G}$. Let $g_2 = (1_{\mathbb{G}}, 1_{\mathbb{G}}, \mathfrak{g}) \in G$ and $G_2 = \langle g_2 \rangle$.
Let $\mathbb{D}$ be the smallest group containing $e(G, G_1)$.
Define $\pi : G \to G_2$ and $\pi_t : G_t \to e(G_2, G_2)$ by
$g_1 g_2' \mapsto g_2'$ and $g_t g_t' \mapsto g_t'$,
where $g_1 \in G_1, g_2' \in G_2, g_t \in \mathbb{D}$, and $g_t' \in e(G_2, G_2)$.
Choose $g \xleftarrow{\$} G$.
Output $PK = \{p, G, G_1, G_t, e, g\}$ and $SK = \{\pi, \pi_t\}$.

$\mathsf{Encrypt}(PK, M)$

Choose $g_1 \xleftarrow{\$} G_1$.
Output the ciphertext $CT = (g^M \cdot g_1) \in G$.

$\mathsf{Multiply}(PK, CT_1, CT_2)$

Choose $g_t' \xleftarrow{\$} \mathbb{D}$.
Output the ciphertext $CT = e(CT_1, CT_2) \cdot g_t' \in G_t$

$\mathsf{Add}(PK, CT_1, CT_2)$

If $CT_1, CT_2 \in G$, then choose $g_1 \xleftarrow{\$} G_1$, and
output the ciphertext $CT_1 \cdot CT_2 \cdot g_1 \in G$.
If $CT_1, CT_2 \in G_t$, then choose $g_t' \xleftarrow{\$} \mathbb{D}$, and
output the ciphertext $CT_1 \cdot CT_2 \cdot g_t' \in G_t$.

$\mathsf{Decrypt}(SK, CT)$

If $CT \in G$, then output the ciphertext $\log_{\pi(g)}(\pi(CT))$.
If $CT \in G_t$, then output the ciphertext $\log_{\pi_t(e(g,g))}(\pi_t(CT))$.

Fig. 2. BGN encryption scheme under DLIN assumption

Comparison with Freeman's Instantiation of the BGN cryptosystem under DLIN: Freeman proposed an instantiation of the BGN cryptosystem under k-linear assumption. In his construction, he used the projecting asymmetric bilinear pairing e defined over $G \times H$ so that the size of $G_t = \mathbb{G}_t^{n^2}$. Although Freeman used the asymmetric bilinear group generator, the underlying group generator $\mathcal{G}_1$ can be symmetric; That is, a map $\hat{e}$ generated by $\mathcal{G}_1$ is a symmetric pairing. If $\mathcal{G}_1$ is symmetric, for a bilinear pairing e used in Freeman's construction of projecting asymmetric bilinear pairings one can compute both $e(g, h)$ and $e(h, g)$ but $e(g, h) \neq e(h, g)$. Thus, we call e is asymmetric. The original BGN cryptosystem in composite-order bilinear groups uses a symmetric bilinear pairing, and in some applications the symmetric property of a (underlying) bilinear pairing would be useful to design protocols.

When Freeman's instantiation of the BGN cryptosystem uses a symmetric pairing $\hat{e}$ in the underlying *prime-order* group generator $\mathcal{G}_1$, each ciphertext consists of 1 element in either G or G_t. That is, a ciphertext consists of either 3 elements in $\mathbb{G}$ or 9 elements in $\mathbb{G}_t$. Therefore, our instantiation of the BGN cryptosystem under DLIN assumption has smaller ciphertexts size than that of Freeman's. In addition, the better efficiency of our Apply algorithm and Decrypt algorithm follow from the fact that our protocol's ciphertext size is shorter than Freeman's.

5.4 Seo-Cheon Round Optimal Blind Signatures under DLIN Assumption

The proposed projecting symmetric bilinear pairings can be used for efficient instantiation of the Seo-Cheon round optimal blind signature scheme under DLIN assumption [35]. Seo-Cheon's scheme uses Groth-Sahai's projecting symmetric bilinear pairings. Furthermore, they define a new property, called *translating*, and

showed that the Groth-Sahai's symmetric construction satisfies translating property. In the proof of their scheme, both projecting and translating properties are essentially used. Our construction for projecting symmetric bilinear pairings also satisfies the translating property.

Definition 10 *(translating) $\mathcal{G}$ is a bilinear group generator. We say that $\mathcal{G}$ is (i,j)-translating if there exists efficiently computable maps $\mathcal{T}_{i,j} : G_i'^2 \times G_j' \to G_j'$ defined by $(g_i, g_i^a, g_j) \mapsto g_j^a$ for an integer $a \in \mathbb{Z}$, where $G = \oplus_{i\in[1,k+1]} G_i'$.*

When we compare the proposed symmetric bilinear pairing with that of Groth-Sahai, both constructions for projecting symmetric bilinear pairings have the same domain and range (if we slightly modify the range of the Groth-Sahai's construction for efficiency improvement as aforementioned). Only bilinear pairing computation is different between ours and the Groth-Sahai's construction for projecting symmetric bilinear pairings. The definition of translating is only associated with G. Therefore, we can similarly show that our construction also satisfies translating property as the proof given in [35].

When we use $\mathcal{G}_2^{B^*}(\lambda)$ instead of $\mathcal{G}_{SP}(\lambda, 3)$, which is given in [35], we can improve efficiency of interactions and the resulting signatures. During each interaction between a user and a signer, the signer verifies GS proofs by using bilinear pairings. The resulting signatures are Waters signatures [38] so that the verification algorithm uses bilinear pairings. Since $\mathcal{G}_2^{B^*}(\lambda)$ generates more efficient bilinear pairings than $\mathcal{G}_{SP}(\lambda, 3)$, we can improve efficiency in the both cases using bilinear pairings.

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.
38. B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127. Springer-Verlag, 2005.