Beyond the Limitation of Prime-Order Bilinear Groups, and Round Optimal Blind Signatures

Jae Hong Seo[1] and Jung Hee Cheon[2]

[1] National Institute of Information and Communications Technology, Tokyo, Japan
jaehong@nict.go.jp
[2] ISaC & Dep. of Mathematical Sciences, Seoul National University, Seoul, Korea
jhcheon@snu.ac.kr

Abstract. At Eurocrypt 2010, Freeman proposed a transformation from pairing-based schemes in composite-order bilinear groups to equivalent ones in prime-order bilinear groups. His transformation can be applied to pairing-based cryptosystems exploiting only one of two properties of composite-order bilinear groups: cancelling and projecting. At Asiacrypt 2010, Meiklejohn, Shacham, and Freeman showed that prime-order bilinear groups according to Freeman's construction cannot have two properties simultaneously except negligible probability and, as an instance of implausible conversion, proposed a (partially) blind signature scheme whose security proof exploits both the cancelling and projecting properties of composite-order bilinear groups.

In this paper, we invalidate their evidence by presenting a security proof of the prime-order version of their blind signature scheme. Our security proof follows a different strategy and exploits only the projecting property. Instead of the cancelling property, a new property, that we call *translating*, on prime-order bilinear groups plays an important role in the security proof, whose existence was not known in composite-order bilinear groups. With this proof, we obtain a 2-move (i.e., round optimal) (partially) blind signature scheme (without random oracle) based on the decisional linear assumption in the common reference string model, which is of independent interest.

As the second contribution of this paper, we construct prime-order bilinear groups that possess both the cancelling and projecting properties at the same time by considering more general base groups. That is, we take a rank n $\mathbb{Z}_p$-submodule of $\mathbb{Z}_p^{n^2}$, instead of $\mathbb{Z}_p^n$, to be a base group G, and consider the projections into its rank 1 submodules. We show that the subgroup decision assumption on this base group G holds in the generic bilinear group model for $n = 2$, and provide an efficient membership-checking algorithm to G, which was trivial in the previous setting. Consequently, it is still open whether there exists a cryptosystem on composite-order bilinear groups that cannot be constructed on prime-order bilinear groups.

1 Introduction

Since Boneh, Goh, and Nissim [10] introduced composite-order bilinear groups in 2005, they have been used to solve many challenging problems in cryptography. Cryptographic systems using composite-order bilinear groups mostly utilize one of two properties, called *cancelling* and *projecting*, which Freeman [17] identified. (Though Freeman named two properties recently, these properties were already used before.) The security of almost all crypto systems using composite-order bilinear groups is based on the subgroup decision assumption, introduced by Boneh, Goh, and Nissim [10], or its variants.

Recently, some literature has aimed at constructing mathematical structures using prime-order bilinear groups with properties similar to (or richer than) composite-order bilinear groups [32, 24, 17, 19]. In particular, Freeman [17] proposed two product groups of prime-order bilinear groups with separately defined bilinear maps. He showed that two proposed product groups satisfy the subgroup decision assumption (in the sense that given g, it is infeasible to determine whether g is in a subgroup or the whole product group), and each product group with a bilinear map satisfies *cancelling* and *projecting*, respectively. One direct benefit of this approach is efficiency improvements of group operations and pairing computations. Loosely speaking, in bilinear groups of composite order, the group order N must be infeasible to factor so that group operations and pairing computations are less efficient than those of bilinear groups of prime order for the same security level. See [17, 19] for detailed efficiency comparison between composite-order groups and prime-order groups.

On the other hand, Meiklejohn, Shacham, and Freeman [30] gave a negative result, that is, an evidence of the limitation of constructing in some class of bilinear groups with both the *cancelling* and *projecting* properties, which is constructed on prime-order bilinear groups. To impart meaning to their result, they also proposed a round optimal blind signature scheme in composite-order bilinear groups whose security proof exploits both the *cancelling* and *projecting* properties of the composite-order bilinear group.[1] Their round optimal blind signature scheme is of independent interest since it is the first practical scheme of this type based on static assumptions (not based on q-type assumptions) in the common reference string model. They left two open questions: (1) whether the instantiation in prime-order groups of their round optimal blind signature scheme is provably secure or insecure, and (2) whether their limitation result can be applied to a wider class of bilinear groups constructed from prime-order groups.

In this paper, we answer both questions. We propose a (partially) blind signature scheme in a prime-order bilinear group setting. The proposed scheme can be considered as an adapted version of the scheme in [30] to the prime-order group setting. However, we prove the one-more unforgeability of the proposed

[1] The scheme in [30] itself does not use *cancelling* and *projecting*. Only the proof of security uses both *cancelling* and *projecting* properties. Thus, the authors do not rule out the existence of different proof strategy.

scheme by using a completely different strategy from [30]. Our proof does not require the *cancelling* property, and instead we use another property, that we call *translating*, on prime order groups. Informally, the *translating* property is that given $g_1, g_1^a \in G_1, g_2 \in G_2$, where G_1 and G_2 are distinct subgroups of G, there exists a map $\mathcal{T}$ outputting g_2^a. The *translating* property is used, in an essential way, to prove the one-more unforgeability of the proposed scheme. With this proof, we obtain a round optimal (partially) blind signature scheme (without relying on the random oracle heuristic) based on the decisional linear assumption in the common reference string model, which is of independent interest. Our blind signature scheme is more efficient than [30]. For example, our scheme has a shorter signature size (six elements in the prime-order group vs. two elements in the composite-order group). Moreover, the security of our blind signature scheme does not rely on the factoring assumption. (The blindness of the signature scheme in [30] based on the subgroup hiding assumption, which requires that the factorization of group order N is infeasible.)

As the second contribution, we show that there exists a more general class of bilinear groups than Meiklejohn, Shacham, and Freeman considered, and some of theses can be both *cancelling* and *projecting*. That is, we take a rank n $\mathbb{Z}_p$-submodule of $\mathbb{Z}_p^{n^2}$, instead of $\mathbb{Z}_p^n$, to be a base group G, and consider the projections into its rank 1 submodules. In this case, we should carefully consider group membership tests of a subgroup. We provide an efficient membership-checking algorithm to G, which was trivial in the previous setting, and we show that the subgroup decision assumption on this base group G holds in the generic bilinear group model for $n = 2$. Consequently, it is still open as to whether there exists a cryptosystem on composite-order bilinear groups that cannot be constructed on prime-order bilinear groups.

We note that although we construct a structure satisfying both *cancelling* and *projecting*, our construction can not be applied directly to the scheme in [30] to transform it to prime-order setting. The proof of [30] uses a property of composite-order group such that two subgroups' order are relatively prime, and our construction does not support such property so that we could not apply our construction to the round optimal blind signature scheme in [30].

Related Work: Blind Signatures. Since Chaum [11, 12] introduced the concept of blind signatures in 1982, it has been studied extensively [6, 1, 7, 8, 16, 28, 31, 25, 5, 18, 4, 2, 21, 30, 3, 20] because of its numerous applications, such as electronic voting [13] and electronic cash [14]. Blind signatures are interactive protocols between a user and a signer. In blind signatures, informally, the user can obtain a signature (signed by the signer) on a message (chosen by the user) without revealing the message to the signer that is signed during the protocol; that is, the signer learns nothing about the message after finishing the protocol.

In particular, round optimal (i.e., 2-move) blind signature schemes have received attention since the round complexity is an important measurement of efficiency in the computer network, and round optimal blind signature schemes directly imply that they are concurrently secure. In the random oracle model, there are elegant round optimal blind signatures by Chaum [12] and Boldyreva [8].

Without relying on the random oracle heuristic, there is an approach using general NIZKs for NP, and its security depends on the assumption that a common reference string exists [16, 5]. Very recently, Garg et al. proposed the first round optimal blind signature in the standard model (without random oracle and a setup assumption such as a common reference string) [20]. These approaches without random oracle, however, are not as efficient as an approach, in which we are interested, using a bilinear map [9, 10].

In recent years several efficient round optimal blind signatures [18, 4, 2, 30, 3] have been proposed in the common reference string model, using a bilinear map, by combining signature schemes with efficient NIWI proofs [23, 22, 24]. These approaches using a bilinear map either rely on q-type dynamic assumptions [18, 4, 2, 3] or working on the composite-order group [30]. Though there is an analysis of a family of q-type dynamic assumptions by Cheon [15], the security of q-type assumptions still remains obscure. (q-type assumptions used in the above schemes hold in the generic group model [35] and these can be strong evidence for believing such assumptions. However, we believe that as the next step, constructing schemes without relying on such strong assumptions is an encouraging research approach.) In [30], a round optimal blind signature scheme based on static assumptions (not on q-type assumptions) using composite-order groups is proposed.

2 Notations and Definitions

Throughout this paper, we use notation $\oplus$ for the internal direct product: for an abelian group G, we write $G = G_1 \oplus G_2$ when G_1 and G_2 are subgroups of G and $G_1 \cap G_2 = \{1_G\}$ for the identity 1_G of G. In this case, every element g in G can be uniquely written by $g = g_1 \cdot g_2$ for some $g_1 \in G_1$ and $g_2 \in G_2$, where $\cdot$ is a group operation in G, and will be omitted sometimes. We use notation $x \xleftarrow{\$} A$. If A is a group $\mathbb{G}$, then it means that an element x is randomly chosen from $\mathbb{G}$, and if A is an algorithm, then it means that A outputs x. $[i, j]$ denotes a set of integers $\{i, \cdots, j\}$. We denote an abelian group generated by $g_1, \cdots, g_n$ by $\langle g_1, \cdots, g_n \rangle$.

We give formal definitions of bilinear group generators, and properties and cryptographic assumptions defined on the bilinear group.

Definition 1 *We say that $\mathcal{G}(\cdot, \cdot)$ is a* bilinear group generator *if it takes as input a security parameter λ and a positive integer $n \geq 1$, and it outputs a tuple $(G, G_i, H, H_i, G_t, e, \sigma | \, i \in [1, n]) \xleftarrow{\$} \mathcal{G}(\lambda, n)$, where G, H, G_t are finite abelian groups, G_i and H_i are cyclic subgroups of G and H of same order, respectively, such that $G = \oplus_{i \in [1,n]} G_i$ and $H = \oplus_{i \in [1,n]} H_i$, and $e : G \times H \to G_t$ is a non-degenerate bilinear map, that is, it satisfies*

Bilinearity: $e(g_1 g_2, h_1 h_2) = e(g_1, h_1) e(g_1, h_2) e(g_2, h_1) e(g_2, h_2)$ *for $g_1, g_2 \in G$ and $h_1, h_2 \in H$,*

Non-degeneracy: for $g \in G$, if $e(g, h) = 1$ for any $h \in H$, then $g = 1$, for $h \in H$, if $e(g, h) = 1$ for any $g \in G$, then $h = 1$,

and σ is additional information for group membership-check. Moreover, we assume that group operations, random samplings, and membership-checks in each group, and computation of e can be efficiently performed (i.e. polynomial-time in λ).

We do not exclude the case that $G = H$. When $G = H$, we say that $\mathcal{G}$ is a symmetric bilinear group generator.

Definition 2 *We say that an algorithm $\mathcal{G}_1$ is a bilinear group generator of* prime order *if $\mathcal{G}_1(\lambda) = \mathcal{G}(\lambda, 1)$, and $\mathcal{G}_1$ outputs groups G, G_1, H, H_1, G_t of prime order p and a map e. Then, $G = G_1$, $H = H_1$. We denote the three distinct groups G, H, G_t by $\mathbb{G}, \mathbb{H}, \mathbb{G}_t$, respectively, and a bilinear map e by $\hat{e}$.*

Now, we provide definitions of two properties, called *cancelling* and *projecting*, which are introduced by Freeman [17].

Definition 3 *A bilinear group generator $\mathcal{G}$ is* cancelling *if $e(g_i, h_j) = 1_t$ whenever $g_i \in G_i$, $h_j \in H_j$, and $i \neq j$, where 1_t is the identity of G_t.*

Definition 4 *A bilinear group generator $\mathcal{G}$ is* projecting *if there exist subgroups $G' \subset G$, $H' \subset H$, and $G'_t \subset G_t$, and non-trivial[2] homomorphisms $\pi : G \to G$, $\bar{\pi} : H \to H$, and $\pi_t : G_t \to G_t$ such that*

1. *$G' \subset \ker(\pi)$, $H' \subset \ker(\bar{\pi})$, and $G'_t \subset \ker(\pi_t)$.*
2. *$\pi_t(e(g, h)) = e(\pi(g), \bar{\pi}(h))$ for $\forall g \in G$ and $\forall h \in H$.*

If $\mathcal{G}$ is a symmetric bilinear group generator, that is, $G = H$, then set $G' = H'$ and $\pi = \bar{\pi}$.

To prove the security of the proposed blind signature scheme, we need two widely-known assumptions, the Computational Diffie-Hellman assumption, and k-Linear assumption which is introduced by Hofheinz and Kiltz and Shacham [26, 34], in the bilinear group setting.

Definition 5 *Let $\mathcal{G}_1$ be a bilinear group generator of prime order. We define the advantage of an algorithm $\mathcal{A}$ in solving Computational Diffie-Hellman (CDH) problem in G, denoted by $Adv^{CDHP_G}_{\mathcal{A},\mathcal{G}_1}$, is to be*

$$\Pr\left[\mathcal{A}(G, H, G_t, e, g, g^a, g^b) \to g^{ab} : (G, H, G_t, e) \xleftarrow{\$} \mathcal{G}_1, g \xleftarrow{\$} G, a, b, \xleftarrow{\$} \mathbb{Z}_p\right].$$

We say that $\mathcal{G}$ satisfies Computational Diffie-Hellman (CDH) assumption in G if for any PPT algorithm $\mathcal{A}$, $Adv^{CDHP_G}_{\mathcal{A},\mathcal{G}_1}$ is a negligible function of λ.

[2] The non-triviality does not appear in the original definition [17]. Without this, however, every bilinear group can be *projecting* by using the trivial homomorphisms.

Definition 6 *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 G, denoted by $Adv^{k\text{-}Lin_G}_{\mathcal{A},\mathcal{G}_1}$, is to be*

$$\Big| \Pr\Big[\mathcal{A}(G, H, G_t, e, g, u_i, u_i^{a_i}, g^b, h \text{ for } i \in [1,k]) \to 1 : (G, H, G_t, e) \xleftarrow{\$} \mathcal{G}_1, g, u_i \xleftarrow{\$} G, h \xleftarrow{\$} H, a_i \xleftarrow{\$} \mathbb{Z}_p \text{ for } i \in [1,k], b \xleftarrow{\$} \mathbb{Z}_p\Big] - \Pr\Big[\mathcal{A}(G, H, G_t, e, g, u_i, u_i^{a_i}, g^b, h \text{ for } i \in [1,k]) \to 1 : (G, H, G_t, e) \xleftarrow{\$} \mathcal{G}_1, g, u_i \xleftarrow{\$} G, h \xleftarrow{\$} H, a_i \xleftarrow{\$} \mathbb{Z}_p \text{ for } i \in [1,k], b = \textstyle\sum_{i\in[1,k]} a_i\Big]\Big|.$$

Then, we say that $\mathcal{G}$ satisfies the k-Linear assumption in G if for any PPT algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ $Adv^{k\text{-}Lin_G}_{\mathcal{A},\mathcal{G}_1}$ is a negligible function of λ.

We can analogously define the CDH assumption and the k-Linear assumption in H. The *1-Linear assumption* in G is the *DDH assumption* in G and the *2-Linear assumption* in G is the *decisional linear assumption* in G.

Next, we provide the definition of the *subgroup decision assumption*, adapted from [17] to fit our purpose.

Definition 7 *Let $\mathcal{G}$ be a bilinear group generator. We define the advantage of an algorithm $\mathcal{A}$ in solving the* (n,k)-subgroup decision problem on the left*, denoted by $Adv^{SDA_L}_{\mathcal{A},\mathcal{G}}$, is to be*

$$\Big| \Pr\Big[\mathcal{A}(G, G', H, H', G_t, e, \sigma, g) \to 1 : (G, G_i, H, H_i, G_t, e, \sigma) \xleftarrow{\$} \mathcal{G}(\lambda, n), G' := \oplus_{i\in[1,k]} G_i, H' := \oplus_{i\in[1,k]} H_i, g \xleftarrow{\$} G\Big] - \Pr\Big[\mathcal{A}(G, G', H, H', G_t, e, \sigma, g') \to 1 : (G, G_i, H, H_i, G_t, e, \sigma) \xleftarrow{\$} \mathcal{G}(\lambda, n), G' := \oplus_{i\in[1,k]} G_i, H' := \oplus_{i\in[1,k]}, g' \xleftarrow{\$} G'\Big]\Big|.$$

We say that $\mathcal{G}$ satisfies the (n,k)-subgroup decision assumption on the left *if for any PPT algorithm $\mathcal{A}$, its advantage $Adv^{SDA_L}_{\mathcal{A},\mathcal{G}}$ is a negligible function in λ.*

We analogously define the (n,k)*-subgroup decision assumption on the right.*

Definition 8 *We say that a bilinear group generator $\mathcal{G}(\cdot,\cdot)$ satisfies the* (n,k)-subgroup decision assumption *if $\mathcal{G}(\cdot, n)$ satisfies both the* (n,k)-subgroup decision assumptions on the left *and* on the right*.*

We will often omit (n,k) term, if it is clear in the context.

3 Round-Optimal Blind Signature in Prime-Order group

3.1 Symmetric Bilinear Group with Projecting Pairing

We construct a symmetric bilinear group generator with the *projecting* property. (The symmetric bilinear groups mean that $G = H$, and $G_i = H_i$ in our definition

of bilinear groups.) We borrow some notations from Freeman's paper [17]. Let $\mathbb{G}$ be a group, $\mathfrak{g}, \mathfrak{g}_1, \cdots, \mathfrak{g}_n$ be elements in $\mathbb{G}$, $\overrightarrow{\alpha} = (a_1, \cdots, a_n)$ be a vector in $\mathbb{Z}_p^n$, and $M = (m_{ij})$ be an $n \times n$ matrix. We denote $\mathfrak{g}^{\overrightarrow{\alpha}} := (\mathfrak{g}^{a_1}, \cdots, \mathfrak{g}^{a_n}) \in \mathbb{G}^n$ and $(\mathfrak{g}_1, \cdots, \mathfrak{g}_n)^M := (\prod_{i\in[1,n]} \mathfrak{g}_i^{m_{i1}}, \cdots, \prod_{i\in[1,n]} \mathfrak{g}_i^{m_{in}})$. We can see that $(\mathfrak{g}^{\overrightarrow{\alpha}})^M = \mathfrak{g}^{(\overrightarrow{\alpha}M)}$. We newly define some notations useful to explain product groups. Let $G = \oplus_{i\in[1,n]} G_i$ and $H = \oplus_{j\in[1,n]} H_j$, where G_i and H_j are cyclic groups of same order. Let $e(G_i, H_j)$ be a set $\{e(g_i, h_j) | g_i \in G_i, h_j \in H_j\}$; hence $e(G_i, H_j)$ is a cyclic group since G_i and H_j are cyclic groups. In particular, when G_i and H_j have prime order p, $e(G_i, H_j)$ is a cyclic group of order p or 1.

Now, we construct a symmetric bilinear group generator $\mathcal{G}_{SP}(\lambda, 3)$, which is a generalization of Groth and Sahai's instantiation based on the decisional linear assumption [24], and is also a symmetric version of Freeman's asymmetric bilinear group generator with the *projecting* property [17].

1. $\mathcal{G}_1(\lambda) \xrightarrow{\$} (p, \mathbb{G}, \mathbb{G}_t, \hat{e})$.
2. Set $G = \mathbb{G}^3, G_t = \mathbb{G}_t^9$.
3. Choose linearly independent vectors $\overrightarrow{x}_1, \overrightarrow{x}_2, \overrightarrow{x}_3 \in \mathbb{Z}_p^3$, and set $G_1 = \langle \mathfrak{g}^{\overrightarrow{x}_1} \rangle$, $G_2 = \langle \mathfrak{g}^{\overrightarrow{x}_2} \rangle$ and $G_3 = \langle \mathfrak{g}^{\overrightarrow{x}_3} \rangle$. Then, $G = G_1 \oplus G_2 \oplus G_3$.
4. Define a map $e : G \times G \to G_t$ by

$$= e((\mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3), (\mathfrak{h}_1, \mathfrak{h}_2, \mathfrak{h}_3))$$

$$\Big(\hat{e}(\mathfrak{g}_1, \mathfrak{h}_1)^{1/2}, \hat{e}(\mathfrak{g}_1, \mathfrak{h}_2)^{1/2}, \hat{e}(\mathfrak{g}_1, \mathfrak{h}_3)^{1/2}, \hat{e}(\mathfrak{g}_2, \mathfrak{h}_1)^{1/2}, \hat{e}(\mathfrak{g}_2, \mathfrak{h}_2)^{1/2}, \hat{e}(\mathfrak{g}_2, \mathfrak{h}_3)^{1/2},$$
$$\hat{e}(\mathfrak{g}_3, \mathfrak{h}_1)^{1/2}, \hat{e}(\mathfrak{g}_3, \mathfrak{h}_2)^{1/2}, \hat{e}(\mathfrak{g}_3, \mathfrak{h}_3)^{1/2}\Big)$$
$$\cdot\Big(\hat{e}(\mathfrak{g}_1, \mathfrak{h}_1)^{1/2}, \hat{e}(\mathfrak{g}_2, \mathfrak{h}_1)^{1/2}, \hat{e}(\mathfrak{g}_3, \mathfrak{h}_1)^{1/2}, \hat{e}(\mathfrak{g}_1, \mathfrak{h}_2)^{1/2}, \hat{e}(\mathfrak{g}_2, \mathfrak{h}_2)^{1/2}, \hat{e}(\mathfrak{g}_3, \mathfrak{h}_2)^{1/2},$$
$$\hat{e}(\mathfrak{g}_1, \mathfrak{h}_3)^{1/2}, \hat{e}(\mathfrak{g}_2, \mathfrak{h}_3)^{1/2}, \hat{e}(\mathfrak{g}_3, \mathfrak{h}_3)^{1/2}\Big).$$

   Then, $e(\mathfrak{g}^{\overrightarrow{x}}, \mathfrak{g}^{\overrightarrow{y}}) = \hat{e}(\mathfrak{g}, \mathfrak{g})^{1/2(\overrightarrow{x}\otimes\overrightarrow{y})+1/2(\overrightarrow{y}\otimes\overrightarrow{x})}$, where $\otimes$ is a tensor product (Kronecker product) of two 3-dimensions vectors.
5. For $i \in [1, 3]$, define maps $\pi_i : G \to G$ and $\pi_{t,i} : G_t \to G_t$ by

$$\pi_i(g) = g^{M^{-1}U_iM} \text{ and } \pi_{t,i}(g_t) = g_t^{(M^{-1}U_iM)\otimes(M^{-1}U_iM)}, \text{ respectively,}$$

   where M is a 3×3 matrix having $\overrightarrow{x}_i$ as its i-th row, U_i is a 3×3 matrix with 1 in the (i, i) entry and zeroes elsewhere, and $\otimes$ is a tensor product of matrices: For $\ell_1 \times \ell_2$ matrix $A = (a_{i,j})$ and $\ell_3 \times \ell_4$ matrix $B = (b_{i,j})$, $A \otimes B$ is a $\ell_1\ell_3 \times \ell_2\ell_4$ matrix whose (i, j)-th block is equal to $a_{i,j}B$, where we consider $A \otimes B$ as $\ell_1 \times \ell_2$ blocks. Then, π_i is a projection such that for $g_1 \in G_1, g_2 \in G_2, g_3 \in G_3$, $\pi_i(g_1g_2g_3)$ is equal to g_i.
6. Output $(p, G, G_1, G_2, G_3, G_t, e, \pi_1, \pi_2, \pi_3, \pi_{t,1}, \pi_{t,2}, \pi_{t,3})$.

We provide a useful lemma to understand the structure of the image of e.

Lemma 1 *The image of e generated by $\mathcal{G}_{SP}$ is equal to $\oplus_{1\le i\le j\le 3} e(G_i, G_j)$, and each $e(G_i, G_j)$'s order is p.*

We provide the proof of Lemma 1 in the full version of this paper. Non-degeneracy of e is directly coming from the lemma 1. (That is, $e(g,h) \neq 1_t$ for any non-identity elements $g, h \in G$. If not, the image is not equal to $\oplus_{1\leq i\leq j\leq 3} e(G_i, G_j)$.) The bilinear property of e can be easily checked from the bilinear property of the tensor product. Further, $\mathcal{G}_{SP}$ satisfies the *projecting* property: Let $G' = G_2 \oplus G_3$, $G'_t = \oplus_{2\leq i\leq j\leq 3} e(G_i, G_j)$, $\pi = \pi_1$, and $\pi_t = \pi_{t,1}$, where G', G'_t, π, and π_t are defined in the definition 4. Then, $G' \subset \ker(\pi)$ and $G'_t \subset \ker(\pi_t)$, and e, π, π_t satisfy the following commutative property.

$$\pi_t(e(\mathfrak{g}^{\overrightarrow{x}}, \mathfrak{g}^{\overrightarrow{y}})) = e(\pi(\mathfrak{g}^{\overrightarrow{x}}), \pi(\mathfrak{g}^{\overrightarrow{y}})).$$

We can check this commutative property as follows:

$$\begin{aligned}
&\pi_t(e(\mathfrak{g}^{\overrightarrow{x}}, \mathfrak{g}^{\overrightarrow{y}})) \\
&= \pi_{t,1}(e(\mathfrak{g}^{\overrightarrow{x}}, \mathfrak{g}^{\overrightarrow{y}})) \\
&= \pi_{t,1}(\hat{e}(\mathfrak{g},\mathfrak{g})^{1/2(\overrightarrow{x}\otimes\overrightarrow{y})+1/2(\overrightarrow{y}\otimes\overrightarrow{x})}) \\
&= (\hat{e}(\mathfrak{g},\mathfrak{g})^{1/2(\overrightarrow{x}\otimes\overrightarrow{y})+1/2(\overrightarrow{y}\otimes\overrightarrow{x})})^{(M^{-1}U_iM)\otimes(M^{-1}U_iM)} \\
&= \hat{e}(\mathfrak{g},\mathfrak{g})^{1/2(\overrightarrow{x}\otimes\overrightarrow{y})((M^{-1}U_iM)\otimes(M^{-1}U_iM))+1/2(\overrightarrow{y}\otimes\overrightarrow{x})((M^{-1}U_iM)\otimes(M^{-1}U_iM))} \\
&= \hat{e}(\mathfrak{g},\mathfrak{g})^{1/2(\overrightarrow{x}M^{-1}U_iM)\otimes(\overrightarrow{y}M^{-1}U_iM)+1/2(\overrightarrow{y}M^{-1}U_iM)\otimes(\overrightarrow{x}M^{-1}U_iM)} \\
&= e(\mathfrak{g}^{(\overrightarrow{x}M^{-1}U_iM)}, \mathfrak{g}^{(\overrightarrow{y}M^{-1}U_iM)}) \\
&= e((\mathfrak{g}^{\overrightarrow{x}})^{M^{-1}U_iM}, (\mathfrak{g}^{\overrightarrow{y}})^{M^{-1}U_iM}) \\
&= e(\pi_1(\mathfrak{g}^{\overrightarrow{x}}), \pi_1(\mathfrak{g}^{\overrightarrow{y}})) = e(\pi(\mathfrak{g}^{\overrightarrow{x}}), \pi(\mathfrak{g}^{\overrightarrow{y}})).
\end{aligned}$$

The fifth equality comes from the property of the tensor product such as $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$, where A and B are matrices having ℓ columns and C and D are matrices having ℓ rows for some ℓ. (We can consider a vector as a matrix having one row.)

In contrast to the composite order bilinear group, our product group of prime order group has an additional property, we name *translating* and define as follow.

Definition 9 *A bilinear group generator $\mathcal{G}$ is* (i,j)-translating *if there exists efficiently computable (that is, polynomial time in λ) maps $\mathcal{T}_{i,j} : G_i^2 \times G_j \to G_j$ defined by $(g_i, g_i^a, g_j) \mapsto g_j^a$ and $\bar{\mathcal{T}}_{i,j} : H_i^2 \times H_j \to H_j$ defined by $(h_i, h_i^a, h_j) \mapsto h_j^a$ for an integer $a \in \mathbb{Z}$. If $\mathcal{G}$ is a symmetric bilinear group generator, then set $\bar{\mathcal{T}}_{i,j} = \mathcal{T}_{i,j}$.*

We show that the above $\mathcal{G}_{SP}$ construction satisfies *translating* property.

Theorem 1 *$\mathcal{G}_{SP}(\lambda, 3)$ satisfies* translating *property for all $i, j \in [1,3]$.*

Proof. We first construct $\mathcal{T}_{3,1}$. Given g_3^a and a 3×3 matrix M defined as in the description of $\mathcal{G}_{SP}$, we can compute g_1^a without knowing a as follows:

$$(g_3^a)^{M^{-1}} = ((\mathfrak{g}^{\overrightarrow{x}_3})^a)^{M^{-1}} = (\mathfrak{g}^{a\overrightarrow{e}_3 M})^{M^{-1}} = \mathfrak{g}^{a\overrightarrow{e}_3} = (1, 1, \mathfrak{g}^a),$$

$$(\mathfrak{g}^a, 1, 1)^M = (\mathfrak{g}^{a\overrightarrow{e}_1})^M = \mathfrak{g}^{a\overrightarrow{x}_1} = g_1^a,$$

where $\overrightarrow{e}_i$ is the canonical i-th vector in $\mathbb{Z}_p^3$, for example, $\overrightarrow{e}_1 = (1,0,0)$. We can construct other $\mathcal{T}_{i,j}$ analogously. □

Moreover, $\mathcal{G}_{SP}$ satisfies $(3,2)$-subgroup decision assumption when the underlying group generator $\mathcal{G}_1$ satisfies the decisional linear assumption.

Lemma 2 *If $\mathcal{G}_1$ satisfies the decisional linear assumption, then $\mathcal{G}_{SP}$ satisfies the $(3,2)$-subgroup decision assumption.*

We relegate the proof of Lemma 2 in the full version of this paper.

Remark 1. Note that $\mathcal{G}_{SP}$ does not satisfy the *cancelling* property since $e(G_i, G_j)$ is not equal to $\{1_t\}$ for $i \neq j$ (Lemma 1).

3.2 Construction

The abstract of our scheme looks very similar to the Meiklejohn et al.'s construction in the composite order bilinear group [30]. We slightly changed the Meiklejohn et al.'s construction to adapt in the prime order bilinear group setting.

(Partially) blind signature schemes in the common reference model consist of five (interactive) algorithms: Setup, KeyGen, User, Signer, and Verify. We provide the formal definition of (partially) blind signature schemes, and concurrently security, in the full version of this paper. We follow the security definition of [30], which is slightly stronger than [6], by allowing the adversary to choose the public key in the *blindness* definition. As a definition of the blind signature, [30] is modified from [27]; (1) it strengthens the *blindness* game to allow the adversary to generate the public key, and (2) it weakens the *one-more unforgeability* game to require that the messages (instead of pairs of message and signature) must all be distinct.[3]

The proposed partially blind signature scheme for a message space $\mathcal{M} = \{0,1\}^m$ is as follows.[4]:

- $\mathsf{Setup}(\lambda)$: $\mathcal{G}_{SP}(\lambda, 3) \xrightarrow{\$} (p, G, G_1, G_2, G_3, G_t, e, \pi_i, \pi_{t,i})$. Choose $g, u', u_1, \cdots, u_m$, $v_1 \cdots, v_m \xleftarrow{\$} G$, $h_1 \xleftarrow{\$} G_1$ and $h_2 \xleftarrow{\$} G_2$. Define

$$CRS = (p, G, G_t, e, g, u', u_1, \cdots, u_m, v_1, \cdots, v_m, h_1, h_2).$$

- $\mathsf{KeyGen}(CRS)$: Choose $g' \xleftarrow{\$} G$. Set $A = e(g, g')$. The public key is $PK = \{A\}$, and the secret key is $SK = \{g'\}$.
- $\mathsf{User}(CRS, PK, info, Msg)$: Let $info$ be an m_0 bits string and Msg be an $m - m_0$ bit string. We write $info$ bitwise as $b_0 \cdots b_{m_0}$ and Msg as $b_{m_0+1} \cdots b_m$. For $i \in [m_0 + 1, m]$, pick random integers $t_{i,1}, t_{i,2}, s_{i,1}, s_{i,2}, r_i, r'_i \xleftarrow{\$} \mathbb{Z}_p$, and

[3] This weakened definition is necessary if the output signature can be re-randomized. [30]'s partially blind signature and ours are in the case.

[4] For large message spaces, we can use a collision resistance hash function first.

compute

$c_i = (u_i)^{b_i} h_1^{t_{i,1}} h_2^{t_{i,2}}$, $d_i = (v_i)^{b_i} h_1^{s_{i,1}} h_2^{s_{i,2}}$,
$\theta_{i,1} = u_i^{b_i s_{i,1}} (v_i^{b_i - 1} h_1^{s_{i,1}} h_2^{s_{i,2}})^{t_{i,1}} h_2^{r_i}$, $\theta_{i,2} = u_i^{b_i s_{i,2}} (v_i^{b_i - 1} h_1^{s_{i,1}} h_2^{s_{i,2}})^{t_{i,2}} h_1^{-r_i}$,
$\theta_{i,3} = u_i^{(b_i - 1) s_{i,1}} (v_i^{b_i} h_1^{s_{i,1}} h_2^{s_{i,2}})^{t_{i,1}} h_2^{r'_i}$, $\theta_{i,4} = u_i^{(b_i - 1) s_{i,2}} (v_i^{b_i} h_1^{s_{i,1}} h_2^{s_{i,2}})^{t_{i,2}} h_1^{-r'_i}$.

Let $\overrightarrow{\theta}_i = (\theta_{i,1}, \cdots, \theta_{i,4})$, and send $req = \{(c_i, d_i, \overrightarrow{\theta}_i)\}_{i \in [m_0+1, m]}$ to the signer and save $state = \{(t_{i,1}, t_{i,2})\}_{i \in [m_0+1, m]}$.

- $\mathsf{Signer}(CRS, SK, info, req)$: Write $req = \{(c_i, d_i, \overrightarrow{\theta}_i)\}_{i \in [m_0+1, m]}$ and $info = b_1 \cdots b_{m_0}$. For each $i \in [m_0 + 1, m]$, verify c_i is a commitment of 0 or 1 by checking that

$$e(c_i, d_i v_i^{-1}) \stackrel{?}{=} e(h_1, \theta_{i,1}) e(h_2, \theta_{i,2}) \text{ and } e(c_i u_i^{-1}, d_i) \stackrel{?}{=} e(h_1, \theta_{i,3}) e(h_2, \theta_{i,4}).$$

If for some i the above equation does not hold, abort the protocol and output $\perp$. Otherwise, compute

$$c = \left(u' \prod_{i \in [1, m_0]} u_i^{b_i} \right) \left(\prod_{i \in [m_0+1, m]} c_i \right),$$

choose a random integer $r \stackrel{\$}{\leftarrow} \mathbb{Z}_p$, compute

$$K_1 = g' c^r, \quad K_2 = g^{-r}, \quad K_{3,1} = h_1^{-r}, \quad K_{3,2} = h_2^{-r},$$

send $(K_1, K_2, K_{3,1}, K_{3,2})$ to the user, and output *success* and $info$.

- $\mathsf{User}(state, (K_1, K_2, K_{3,1}, K_{3,2}))$: Write $state = \{(t_{i,1}, t_{i,2})\}_{i \in [m_0+1, m]}$. Check that

$$e(K_{3,1}, g) \stackrel{?}{=} e(K_2, h_1) \text{ and } e(K_{3,2}, g) \stackrel{?}{=} e(K_2, h_2).$$

If one of two above equations is fail to hold, then abort the protocol and output $\perp$. Otherwise, unblind the signature by computing

$$S_1 = K_1 \cdot \left(\prod_{i \in [m_0+1, m]} K_{3,1}^{t_{i,1}} K_{3,2}^{t_{i,2}} \right) \text{ and } S_2 = K_2.$$

Check the validity of the signature (S_1, S_2) by running Verify. If it outputs *accept*, then go to the next step. Otherwise, abort the protocol and output $\perp$. Finally re-randomize the signature by picking a random $s \stackrel{\$}{\leftarrow} \mathbb{Z}_p$ and computing

$$S'_1 = S_1 \cdot (u' \prod_{i \in [1, m]} u_i^{b_i})^s \text{ and } S'_2 = S_2 \cdot g^{-s}.$$

Output the signature $sig = (S'_1, S'_2), info$, and *success*.

- $\mathsf{Verify}(CRS, PK, info, Msg, sig)$: Write $PK = \{A\}$, $info = b_1 \cdots b_{m_0}$, $Msg = b_{m_0} \cdots b_m$, and $sig = (S_1, S_2)$. Check that

$$e(S_1, g) \cdot e(S_2, u' \prod_{i \in [1, m]} u_i^{b_i}) \stackrel{?}{=} A.$$

If the above equality holds, then output *accept*. Otherwise, output $fail$.

In the first procedure of the user, c_i and d_i are GS-commitment to b_i, and $\overrightarrow{\theta}_i$ is GS-proof that b_i satisfies the equation $b_i(b_i - 1) = 0$ so that $b_i = 0$ or $b_i = 1$. More precisely, when b_i and b'_i are openings of c_i and d_i, respectively, $\overrightarrow{\theta}_i$ is a proof that $b_i(b'_i - 1) = 0$ and $(b'_i - 1)b_i = 0$. Then, $(b_i = 0$ or $b'_i = 1) \bigwedge (b_i = 1$ or $b'_i = 0)$ so that $b_i = b'_i = 0$ or $b_i = b'_i = 1$. We provide three theorems to prove the security of the proposed (partially) blind signature scheme.

Theorem 2 *The above blind signature is correct.*

Theorem 3 *If $\mathcal{G}_1$ satisfies the decisional linear assumption, then the above blind signature satisfies blindness.*

The proof of Theorem 2 and 3 are similar to the previous ones [30]. We provide the proof in the full version of this paper.

Theorem 4 *If $\mathcal{G}_1$ satisfies the the CDH assumption, then the above blind signature is one-more unforgeable.*

Due to space constraints, we leave the proof of Theorem 4 to the full version of this paper. Instead, we briefly explain our idea to prove the one-more unforgeability, and the reason why we cannot apply the Meiklejohn et al. proof strategy to the proposed scheme. At the end of the interaction, the user obtains a Waters-signature, which is existentially unforgeable based on the CDH assumption. If the user obtains only a Waters signature, then the proposed scheme is, loosely speaking, also one-more unforgeable. However, the user obtains not only a Waters signature (of the form $g'(u \prod_{i\in[1,m]} u_i^{b_i})^r$ and g^{-r} for message $b_1 \cdots b_m$), but also some additional information, that is, it eventually gets

$$g'(u \prod_{i\in[1,m]} u_i^{b_i})^r (\prod_{i\in[m_0+1,m]} h_1^{t_{i,1}} h_2^{t_{i,2}})^r, \quad g^{-r}, \quad h_1^{-r}, \text{ and } h_2^{-r}$$

for some (unknown and uniformly distributed) $r \in \mathbb{Z}_p$, and $t_{i,1}$, $t_{i,2}$, and b_i chosen by itself. Therefore, we should show that h_1^{-r}, h_2^{-r}, and $(\prod_{i\in[m_0,m]} h_1^{t_{i,1}} h_2^{t_{i,2}})^r$ will not be helpful for the user to break the one-more unforgeability. In [30], a pairing e satisfies the *cancelling* property, and orders of subgroups are relatively prime so that each part contained in each subgroup in a signature scheme is independent. [30] essentially utilized this independence. If, in our scheme, the $G_1 \oplus G_2$ part and G_3 part were independent, the user could not obtain any additional information about the part in G_3 from the above information. (Since all information other than a Waters signature, which the user gets at the end of the protocol, is related to h_1 and h_2, which are elements in $G_1 \oplus G_2$, this information will not be helpful for forging the Waters signature in the G_3 part.) Hence, the one-more unforgeability of the scheme can be reduced to the existential unforgeability of the Waters signature (in G_3 in the case of our scheme). However, we cannot apply this Meiklejohn et al. proof strategy to our scheme since our bilinear map e does not have the *cancelling* property and each subgroup has the same order p. Instead, we prove the one-more unforgeability using a completely different strategy. Our simulation basically follows the simulation for the existential

unforgeability of the Waters signature, and at the same time simulates directly additional information h_1^{-r}, h_2^{-r}, and $(\prod_{i\in[m_0+1,m]} h_1^{t_{i,1}} h_2^{t_{i,2}})^r$. It seems hard to simulate $(\prod_{i\in[m_0+1,m]} h_1^{t_{i,1}} h_2^{t_{i,2}})^r$ since $t_{i,1}$ and $t_{i,2}$ are chosen by the user and r is usually not known to the simulator during the simulation. (r is usually of the form $Ra + S$ for some unknown a and constants R and S, where a is given by the form $\mathfrak{g}^a$.) We circumvent this obstacle by using the *projecting* property and the *translating* property mentioned in section 3.1. To simulate this additional information, the simulator first extracts the message, that is, recovers $b_1 \cdots b_m$ by computing $log_{\pi_1(u_i)}\pi_1(c_i) = b_i$, and second computes $\pi_j(c_i/u_i^{b_i}) = h_j^{t_{i,j}}$ and

$$\text{if } b_i = 0, \begin{cases} \pi_3(\theta_{i,1}^{-1}) = \pi_3(v_i)^{t_{i,1}} \\ \pi_3(\theta_{i,2}^{-1}) = \pi_3(v_i)^{t_{i,2}}, \end{cases} \qquad \text{if } b_i = 1, \begin{cases} \pi_3(\theta_{i,3}) = \pi_3(v_i)^{t_{i,1}} \\ \pi_3(\theta_{i,4}) = \pi_3(v_i)^{t_{i,2}}. \end{cases}$$

Though $\pi_3(v_i)^{t_{i,j}}$ is contained in G_3, we can change it to be of the form $h_j^{at_{i,j}}$ for some unknown a by using the *translating* property mentioned in section 3.1 when v_i contains a in the exponent. The simulator can generate $(\prod_{i\in[m_0+1,m]} h_1^{t_{i,1}} h_2^{t_{i,2}})^r$ by using $h_j^{t_{i,j}}$ and $h_j^{at_{i,j}}$.

Remark 2. The decisional linear assumption implies the CDH assumption. (The decisional linear assumption implies the computational linear assumption, and the computational linear assumption implies the CDH assumption. Reductions are quite straightforward.)

Remark 3. In the user's first procedure, the GS-commitment and proof appear to have redundant parts. It would be more natural to change them to

$$c_i = (u_i)^{b_i} h_1^{t_{i,1}} h_2^{t_{i,2}}, \theta_{i,1} = (u_i^{2b_i-1} h_1^{t_{i,1}} h_2^{t_{i,2}})^{t_{i,1}} h_2^{r_i}, \theta_{i,2} = (u_i^{2b_i-1} h_1^{t_{i,1}} h_2^{t_{i,2}})^{t_{i,2}} h_1^{-r_i},$$

and it can be verified by $e(c_i, c_i u_i^{-1}) \stackrel{?}{=} e(h_1, \theta_{i,1}) e(h_2, \theta_{i,2})$. This commitment and proof is GS commitment and proof for $b_i \in \{0, 1\}$. However, we note that in this case, we could not prove the one-more unforgeability based on the CDH assumption. We only proved the one-more unforgeability based on the decisional linear assumption and augmented CDH assumption. (Augmented CDH assumption roughly says that given $\mathfrak{g}, \mathfrak{g}^a, \mathfrak{g}^b, \mathfrak{g}^{a^2}$, it is infeasible to compute $\mathfrak{g}^{ab}$.) To avoid requiring $\mathfrak{g}^{a^2}$, in the simulation, that is, to prove the one-more unforgeability based on the CDH assumption, we modified the commitment and the proof to the current form.

4 Bilinear Group: Both Cancelling and Projecting

4.1 Interpreting Limitation Result in [30]

In [30], the authors consider the cases that the bilinear group generator $\mathcal{G}(\lambda, n)$ is defined as follows:

1. $(p, \mathbb{G}, \mathbb{H}, \mathbb{G}_t, \hat{e}) \stackrel{\$}{\leftarrow} \mathcal{G}_1(\lambda)$

2. $G = \mathbb{G}^n$, $H = \mathbb{G}^n$, and $G_t = \mathbb{G}_t^m$ for some positive integer m.
3. a bilinear map $e : G \times G \to G_t$ is defined by

$$\begin{aligned} e((\mathfrak{g}_1, \cdots, \mathfrak{g}_n), (\mathfrak{h}_1, \cdots, \mathfrak{h}_n)) &= (\cdots, e((\mathfrak{g}_1, \cdots, \mathfrak{g}_n), (\mathfrak{h}_1, \cdots, \mathfrak{h}_n))^{(\ell)}, \cdots) \\ &= (\cdots, \textstyle\prod_{i,j \in [1,n]} \hat{e}(\mathfrak{g}_i, \mathfrak{h}_j)^{e_{ij}^{(\ell)}}, \cdots), \end{aligned}$$

where $e_{ij}^{(\ell)} \in \mathbb{Z}_p$ for all $i, j \in [1, n]$ and $\ell \in [1, m]$.

The authors showed that e can be both the *cancelling* and *projecting* only with negligible probability when e is defined as the above. In the above $\mathcal{G}$ construction, to generate a rank n $\mathbb{Z}_p$-module, G is defined as $\mathbb{G}^n$. In the proof for the limitation result ([30, Proposition 6.4 and Theorem 6.5]), the authors used, in an essential way, the fact that a rank n $\mathbb{Z}_p$-module is of the form $\mathbb{G}^n$.

We can, however, also define, in a different way, a rank n $\mathbb{Z}_p$-module G. First generate a rank $n' (> n)$ $\mathbb{Z}_p$-module $\tilde{G}$, and then define G as a rank n $\mathbb{Z}_p$-submodule of $\tilde{G}$. For example, define $\tilde{G} = \mathbb{G}^4$ and

$$G = \langle (\mathfrak{g}^{a_1}, \mathfrak{g}^{b_1}, \mathfrak{g}^{c_1}, \mathfrak{g}^{d_1}), (\mathfrak{g}^{a_2}, \mathfrak{g}^{b_2}, \mathfrak{g}^{c_2}, \mathfrak{g}^{d_2}), (\mathfrak{g}^{a_3}, \mathfrak{g}^{b_3}, \mathfrak{g}^{c_3}, \mathfrak{g}^{d_3}) \rangle,$$

where $\{(a_i, b_i, c_i, d_i)\}_{i \in [1,3]}$ is a set of linearly independent vectors in $\mathbb{Z}_p^4$. Then, G is a rank 3 $\mathbb{Z}_p$-submodule of a rank 4 $\mathbb{Z}_p$-module $\tilde{G}$. This example is not included in the case of the above $\mathcal{G}$ construction. In this example, we should argue about the membership check of G since any group should be easy to check for its membership to be used for cryptographic applications. If there is no additional information, the membership check of G is infeasible since it is equivalent to the decisional 3-linear problem. However, we should not rule out this case when some additional information for membership check is given. Our construction is exactly such a case.

4.2 Our Construction

First, we give an instructive intuition of our construction. To construct a bilinear group generator with *projecting*, we should consider the order of image of a bilinear map, which should be larger than prime p.[5] We start from a bilinear group generator with the *cancelling* property [17]. We consider n different bilinear group generators (of rank n) with *cancelling* property. Let $G^{(i)} = \oplus_{j \in [1,n]} G_{ij}$ (rank n $\mathbb{Z}_p$-module), $H^{(i)} = \oplus_{j \in [1,n]} H_{ij}$ (rank n $\mathbb{Z}_p$-module) and $\bar{e}_i$ (bilinear map) be the output of i-th bilinear group generator. Let $G_{ij} = \langle g_{ij} \rangle$ that is a rank 1 $\mathbb{Z}_p$-submodule of a rank n $\mathbb{Z}_p$-module. Let G_j be $\langle (g_{1j}, \cdots, g_{nj}) \rangle$, which is a rank 1 $\mathbb{Z}_p$-submodule of a rank n^2 $\mathbb{Z}_p$-module (n direct product of n $\mathbb{Z}_p$-modules). Define H_j similarly, and define $G = \oplus_{j \in [1,n]} G_j$ and $H = \oplus_{j \in [1,n]} H_j$. We define a map e by using bilinear maps $\bar{e}_i$ defined over each $G^{(i)} \times H^{(i)}$ as follows:

$$e((g_1, \cdots, g_n),\ (h_1, \cdots, h_n)) \ = \ (\bar{e}_1(g_1, h_1), \cdots, \bar{e}_n(g_n, h_n)),$$

[5] If the image of a bilinear map is prime p, it cannot satisfy *projecting* property [30].

where $g_i \in G^{(i)}$ and $h_i \in H^{(i)}$. This construction also satisfies the *cancelling* property. If we can control the basis of the image of e so that the order of image is not prime p, then we may obtain the *projecting* property.

For vectors $\Gamma = (\overrightarrow{\alpha}_1, \cdots, \overrightarrow{\alpha}_n) = (\alpha_{11}, \cdots, \alpha_{nn})$ and $\Lambda = (\overrightarrow{\beta}_1, \cdots, \overrightarrow{\beta}_n) = (\beta_{11}, \cdots, \beta_{nn}) \in \mathbb{Z}_p^{n^2}$, and a group element $\mathfrak{g} \in \mathbb{G}$, we define a notation $\Gamma \circ \Lambda := (\overrightarrow{\alpha}_1 \cdot \overrightarrow{\beta}_1, \cdots, \overrightarrow{\alpha}_n \cdot \overrightarrow{\beta}_n) \in \mathbb{Z}_p^n$, where $\overrightarrow{\alpha}_j$'s and $\overrightarrow{\beta}_j$'s are vectors in $\mathbb{Z}_p^n$, and $\overrightarrow{\alpha}_j \cdot \overrightarrow{\beta}_j = \sum_{\ell \in [1,n]} \alpha_{j\ell}\beta_{j\ell}$. Now, we describe our construction $\mathcal{G}_{CP}$.

1. Take a security parameter and a positive integer n as inputs, run $\mathcal{G}_1$, and obtain $(p, \mathbb{G}, \mathbb{H}, \mathbb{G}_t, \hat{e})$.
2. Choose generators $\mathfrak{g}$ and $\mathfrak{h}$ at random from $\mathbb{G}$ and $\mathbb{H}$, respectively.
3. Choose $X_1, \cdots, X_n$ and D from $GL_n(\mathbb{Z}_p)$ at random. Define $D_i \in Mat_n(\mathbb{Z}_p)$ be a diagonal matrix having D's i-th column vector as its diagonal. Define Y_i by $D_i(X_i^{-1})^t$.
4. Let $\overrightarrow{\psi}_{ij}$ be the i-th row of X_j and $\overrightarrow{\phi}_{ij}$ be the i-th row of Y_j. Let $\Psi_i = (\overrightarrow{\psi}_{i1}, \cdots, \overrightarrow{\psi}_{in})$ and $\Phi_i = (\overrightarrow{\phi}_{i1}, \cdots, \overrightarrow{\phi}_{in})$. Then, define G_i by a cyclic subgroup in $\mathbb{G}^{n^2}$ generated by $\langle \mathfrak{g}^{\Psi_i} \rangle$, and define H_i by a cyclic group in $\mathbb{H}^{n^2}$ generated by $\langle \mathfrak{h}^{\Phi_i} \rangle$.
5. Define G and H by the internal direct product of G_i's and H_i's, respectively. That is, $G = \oplus_{i \in [1,n]} G_i \subset \mathbb{G}^{n^2}$, and $H = \oplus_{i \in [1,n]} H_i \subset \mathbb{H}^{n^2}$. Define G_t by $\mathbb{G}_t^n$.
6. Define a map $e : G \times H \to G_t$ as follows:

$$e(\mathfrak{g}^{\Gamma}, \mathfrak{h}^{\Lambda}) := (\prod_{\ell \in [1,n]} \hat{e}(\mathfrak{g}^{\alpha_{1\ell}}, \mathfrak{h}^{\beta_{1\ell}}), \cdots, \prod_{\ell \in [1,n]} \hat{e}(\mathfrak{g}^{\alpha_{n\ell}}, \mathfrak{h}^{\beta_{n\ell}})) \quad = \quad \hat{e}(\mathfrak{g}, \mathfrak{h})^{\Gamma \circ \Lambda},$$

   for any $\Gamma = (\alpha_{11}, \cdots, \alpha_{nn})$ and $\Lambda = (\beta_{11}, \cdots, \beta_{nn})$.
7. Take a basis of $\langle \Psi_1, \cdots, \Psi_n \rangle^{\perp}$ at random, say $\{\hat{\Psi}_1, \cdots, \hat{\Psi}_{n^2-n}\}$, and take a basis of $\langle \Phi_1, \cdots, \Phi_n \rangle^{\perp}$ at random, say $\{\hat{\Phi}_1, \cdots, \hat{\Phi}_{n^2-n}\}$, where the notation $\langle \Gamma_1, \cdots, \Gamma_n \rangle^{\perp}$ means a set of all orthogonal vectors to $\langle \Gamma_1, \cdots, \Gamma_n \rangle$. Define

$$\sigma := (\hat{e}, \{\mathfrak{h}^{\hat{\Psi}_1}, \cdots, \mathfrak{h}^{\hat{\Psi}_{n^2-n}}\}, \{\mathfrak{g}^{\hat{\Phi}_1}, \cdots, \mathfrak{g}^{\hat{\Phi}_{n^2-n}}\}).$$

8. Output $(G, G_1, \cdots, G_n, H, H_1, \cdots, H_n, G_t, e, \sigma)$.

In the description of $\mathcal{G}_{CP}$ each G_i and H_i is defined to be rank 1, as $\mathbb{Z}_p$-submodules of $\mathbb{G}^{n^2}$, and for $i \neq j$, $G_i \cap G_j = H_i \cap H_j = \{1_{\mathbb{G}^{n^2}}\}$, where $1_{\mathbb{G}^{n^2}}$ is the identity of $\mathbb{G}^{n^2}$. Therefore, in the step 5, $G = \oplus_{i \in [1,n]} G_i$ and $H = \oplus_{i \in [1,n]} H_i$ are well-defined and rank n $\mathbb{Z}_p$-submodules of $\mathbb{G}^{n^2}$.

4.3 Cancelling, Projecting, and Translating

It is straightforward to check that e is a non-degenerate bilinear map. We show that e satisfies *cancelling*, *projecting* and *translating*.

Theorem 5 *Let* $(G = \oplus_{i\in[1,n]}G_i, G_i, H = \oplus_{i\in[1,n]}H_i, H_i, G_t, e, \sigma)$ *be the output of the above* $\mathcal{G}_{CP}$*. Then,* e *is both* cancelling *and* projecting*.*

Proof. Let $X_1, \cdots, X_n, Y_1, \cdots, Y_n$ and D be generated in the step 3 of Section 4.2. These satisfy the following three conditions.

(1) X_ℓ and Y_ℓ are in $GL_n(\mathbb{Z}_p)$ for $\ell \in [1, n]$.
(2) For $\ell \in [1, n]$ each $X_\ell \cdot Y_\ell^\top$ is a diagonal matrix with a diagonal $\mathbf{d}_\ell$.
(3) $D = (\mathbf{d}_1 \cdots \mathbf{d}_n)$, that is, the i-th column vector of D is $\mathbf{d}_i$.

From the condition (1) we can see that Ψ_i's are linearly independent and Φ_i's are linearly independent and so $G = \oplus_{i\in[1,n]}G_i$ and $H = \oplus_{i\in[1,n]}H_i$ are well-defined. The condition (2) guarantees that e is a *cancelling* bilinear map: For $i \neq j$, $\Psi_i \circ \Phi_j := (\overrightarrow{\psi}_{i1} \cdot \overrightarrow{\phi}_{j1}, \cdots, \overrightarrow{\psi}_{in} \cdot \overrightarrow{\phi}_{jn}) = 0$ and so $e(\mathfrak{g}^{\Psi_i}, \mathfrak{h}^{\Phi_j}) = e(\mathfrak{g}, \mathfrak{h})^{\Psi_i \circ \Phi_j} = (1_{\mathbb{G}_t}, \cdots, 1_{\mathbb{G}_t})$ is equal to the identity of the product group $(\mathbb{G}_t)^n$. The third condition (3) implies that $\{\Psi_i \circ \Phi_i\}_{i\in[1,n]}$ is a set of linearly independent vectors in $\mathbb{Z}_p^n$; hence, any pair of groups $e(G_i, H_i) = \langle e(\mathfrak{g}, \mathfrak{h})^{\Psi_i \circ \Phi_i} \rangle = \langle (\mathfrak{g}, \mathfrak{h})^{(d_{i1}, \cdots, d_{in})} \rangle$ has no common element except the identity so that $Im(e) = \oplus_{i\in[1,n]} e(G_i, H_i) = G_t$. We can consider natural projections $\pi_i : G \to G_i$, $\bar{\pi}_i : H \to H_i$, and $\pi_{t,i} : G_t \to e(G_i, H_i)$. We can construct these projections, in a similar way as the construction of the projections in the subsection 3.1. We leave the details to the full version of this paper. Let $G' = \oplus_{[2,n]}G_i$, $H' = \oplus_{[2,n]}H_j$, $G'_t = e(G', H')$, $\pi = \pi_i$, $\bar{\pi} = \bar{\pi}_i$, and $\pi_t = \pi_{t,i}$. Then, e satisfies the definition 4. □

Theorem 6 $\mathcal{G}_{CP}(\lambda, n)$ *satisfies* translating *property for all* $i, j \in [1, n]$*.*

Proof. We will construct $\mathcal{T}_{3,1}$. We can construct other $\mathcal{T}_{i,j}$ and $\bar{\mathcal{T}}_{i,j}$ similarly. Given g_3, g_3^a and $n \times n$ matrices X_i defined as in the description of $\mathcal{G}_{CP}$, we can compute g_1^a without knowing a as follows:

$$\text{Parse } g_3^a \text{ as } (\mathfrak{g}^{\Psi_3})^a = ((\mathfrak{g}^{\overrightarrow{\psi}_{31}})^a, \cdots, (\mathfrak{g}^{\overrightarrow{\psi}_{3n}})^a), \text{ and compute}$$

$$\text{for } j \in [1, n],\ ((\mathfrak{g}^{\overrightarrow{\psi}_{3j}})^a)^{X_j^{-1}} = (\mathfrak{g}^{a\overrightarrow{e}_3 X_j})^{X_j^{-1}} = \mathfrak{g}^{a\overrightarrow{e}_3} = (1, 1, \mathfrak{g}^a, \cdots, 1),$$

$$(\mathfrak{g}^a, 1, \cdots, 1)^{X_j} = (\mathfrak{g}^{a\overrightarrow{e}_1})^{X_j} = \mathfrak{g}^{a\overrightarrow{\psi}_{1j}},$$

$$\text{then } (\mathfrak{g}^{a\overrightarrow{\psi}_{11}}, \cdots, \mathfrak{g}^{a\overrightarrow{\psi}_{1n}}) = (\mathfrak{g}^{\Psi_1})^a = g_1^a.$$

where $\overrightarrow{e}_i$ is the canonical i-th vector in $\mathbb{Z}_p^n$, for example, $\overrightarrow{e}_1 = (1, 0, 0, \cdots, 0)$. □

We show that anyone knowing σ can test membership of elements in G and H (membership test for G_t is trivial) in the full version. Finally, we should show that $\mathcal{G}$ satisfies the subgroup decision assumption, but it is not easy to prove that $\mathcal{G}$ satisfies the subgroup decision for any n. Instead, in the full version we give a proof that, for $n = 2$, $\mathcal{G}$ satisfies the $(2, 1)$-subgroup decision assumption in the generic bilinear group model [35] (that is, we assume that the adversary should access the oracles for group operations of $\mathbb{G}$, $\mathbb{H}$, $\mathbb{G}_t$ and pairing computations for $\hat{e}$, where $\mathcal{G}_1 \to (p, \mathbb{G}, \mathbb{H}, \mathbb{G}_t, \hat{e})$). Though we give a proof for the case $n = 2$,

we are positive that $\mathcal{G}_{CP}$ satisfies the subgroup decision assumption for $n > 2$. For $n > 2$, there are several variables, particularly in σ, we should consider for the subgroup decision assumption, so these make it hard to prove for the case $n > 2$, even in the generic bilinear group model.[6]

5 Conclusions and Further Work

In this paper, we answered two open questions left by Meiklejohn, Shacham, and Freeman. First, we showed that the security of the Meiklejohn et al.'s (partial) blind signature can be proved in the prime-order bilinear group setting.[7] Second, we showed that there exist bilinear group generators that are both *cancelling* and *projecting* in the prime-order bilinear group setting.

The proof of the Meiklejohn-Shacham-Freeman blind signature scheme, and the Lewko-Waters identity-based encryption scheme [29] essentially use the fact that orders of subgroups are relatively prime as well as the projecting and/or cancelling properties. For each scheme, the adapted version in prime-order bilinear groups is proposed, with a different security proof strategy, in this paper and [29], respectively. It would be interesting to find a general procedure to transform such schemes using relatively prime orders in composite-order groups to schemes in prime-order groups.

We proposed a new mathematical framework with both *cancelling* and *projecting* in a prime-order bilinear group setting, and gave the proof that the $(2, 1)$ subgroup decision assumption holds in the generic bilinear group model when $n = 2$. This research leaves many interesting open problems. We ask if the subgroup decision assumption holds when $n > 2$, and if the subgroup decision assumption can be reduced to the simple assumption such as the (decisional) k-linear assumption. We did not find good cryptographic applications of this framework. It would be interesting to design cryptographic schemes based on the proposed framework. We expect that this research will provide other directions for our primitive question: whether there exists a cryptosystem on composite-order bilinear groups that cannot be constructed on prime-order bilinear groups.

Acknowledgements The first author is grateful to MinJae Seo for his useful comments on an early draft of this paper. We are grateful to anonymous reviewers in TCC 2012 for their valuable comments. The second author was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 20110018345)

[6] All variables in σ is public, so to show that $\mathcal{G}_{CP}$ satisfies the subgroup decision assumption, the simulator should simulate σ in the proof.

[7] We modified their scheme slightly to prove its security under the CDH assumption. We remark that, however, the security of the direct instantiation of their scheme in the prime-order bilinear group can also be proven secure under the decisional linear assumption and the augmented CDH assumption, which is stronger than the CDH assumption.

References

1. M. Abe. A secure three-move blind signature scheme for polynomially many signatures. In *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 136–151. Springer, 2001.
2. 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.
3. 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.
4. M. Abe, K. Haralambiev, and M. Ohkubo. Signing on elements in bilinear groups for modular protocol design. In *Cryptology ePrint Archive, Report 2010/133*. http://eprint.iacr.org/2010/133, 2010.
5. M. Abe and M. Ohkubo. A framework for universally composable non-committing blind signatures. In *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 435–450. Springer, 2009.
6. M. Abe and T. Okamoto. Provably secure partially blind signatures. In *CRYPTO 2000*, volume 1880 of *LNCS*, pages 271–286. Springer, 2000.
7. M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko. The one-more-rsa-inversion problems and the security of chaum's blind signature scheme. In *Journal of Cryptology*, volume 16, pages 185–215, 2003.
8. A. Boldyreva. Trheshold signature, multisignature and blind signature schemes based on the gap-diffie-hellman-group signature scheme. In *PKC 2003*, volume 2567 of *LNCS*, pages 31–46. Springer, 2003.
9. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO 2001*, volume 2139 of *LNCS*, pages 19–23. Springer-Verlag, 2001.
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. D. Chaum. Blind signatures for untraceable payments. In *CRYPTO*, pages 199–203, 1982.
12. D. Chaum. Blind signature system. In *CRYPTO 1983*, 1983.
13. D. Chaum. Elections with unconditionally-secret ballots and disruption equivalent to breaking rsa. In *EUROCRYPT*, volume 330 of *LNCS*, pages 177–182. Springer, 1988.
14. D. Chaum, A. Fiat, and M. Naor. Untraceable electoronic cash. In *CRYPTO*, volume 403 of *LNCS*, pages 319–327. Springer, 1988.
15. J. H. Cheon. Discrete logarithm problems with auxiliary inputs. In *Journal of Cryptology*, volume 23, pages 457–476, 2010.
16. M. Fischlin. Round-optimal composable blind signatures in the common reference string model. In *CRYPTO 2006*, volume 4117 of *LNCS*, pages 60–77. Springer, 2006.
17. D. M. Freeman. Converting pairing-based cryptosystems from composite-orde groups to prime-order groups. In *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 44–61. Springer, 2010.
18. G. Fuchsbauer. Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. In *Cryptology ePrint Archive, Report 2009/320*. http://eprint.iacr.org/2009/320, 2009.
19. S. Garg, A. Kumarasubramanian, A. Sahai, and B. Waters. Building efficient fully collusion-resilient traitor tracing and revocation schemes. In *ACM Conference on Computer and Communications Security*, pages 121–130. ACM, 2010.

20. S. Garg, V. Rao, A. Sahai, D. Schröder, and D. Unruh. Round optimal blind signature. In *CRYPTO 2011*, volume 6841 of *LNCS*, pages 630–648. Springer, 2011.
21. E. Ghadafi and N. Smart. Efficient two-move blind signatures in the common reference string model. In *Cryptology ePrimt Archive, Report 2010/568*. http://eprint.iacr.org/2010/568, 2010.
22. J. Groth, R. Ostrovsky, and A. Sahai. Non-interactive zaps and new techniques for nizk. In *CRYPTO 2006*, volume 4117 of *LNCS*, pages 97–111. Springer, 2006.
23. J. Groth, R. Ostrovsky, and A. Sahai. Perfect non-interactive zero-knolwedge for np. In *EUROCRYPT*, volume 4004 of *LNCS*, pages 339–358. Springer, 2006.
24. 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.
25. C. Hazay, J. Katz, C.-Y. Koo, and Y. Lindell. Concurrently-secure blind signatures without random oracles or setup assumptions. In *TCC 2007*, volume 4392 of *LNCS*, pages 323–341. Springer, 2007.
26. D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. In *CRYPTO*, volume 4622 of *LNCS*, pages 553–571. Springer, 2007.
27. A. Juels, M. Luby, and R. Ostrovsky. Security of blind digital signatures. In *CRYPTO 1997*, volume 1294 of *LNCS*, pages 150–164. Springer, 1997.
28. A. Kiayias and H.-S. Zhou. Concurrently-secure blind signatures without random oracles. In *SCN 2006*, volume 4116 of *LNCS*, pages 49–62. Springer, 2006.
29. A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure hibe with short ciphertexts. In *TCC 2010*, volume 5978 of *LNCS*, pages 455–479. Springer, 2010.
30. 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.
31. T. Okamoto. Efficient blind and partially blind signatures without random oracles. In *TCC 2006*, volume 3876 of *LNCS*, pages 80–99. Springer, 2006.
32. T. Okamoto and K. Takashima. Homomorphic encryption and signature from vector decomposition. In *Pairing*, volume 5209 of *LNCS*, pages 57–74. Springer, 2008.
33. T. Okamoto and K. Takashima. Hierarchical predicate encryption for inner-products. In *ASIACRYPT*, volume 5912 of *LNCS*, pages 214–231. Springer, 2009.
34. 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.
35. V. Shoup. Lower bounds for discrete logarithms and related problems. In *EUROCRYPT*, pages 256–266. Springer, 1997.