Limitations on Transformations from Composite-Order to Prime-Order Groups: The Case of Round-Optimal Blind Signatures

Sarah Meiklejohn[1], Hovav Shacham[1], and David Mandell Freeman[2]

[1] University of California, San Diego
La Jolla, CA 92037, USA
{smeiklej,hovav}@cs.ucsd.edu
[2] Stanford University
Stanford, CA 94305, USA
dfreeman@cs.stanford.edu

Abstract. Beginning with the work of Groth and Sahai, there has been much interest in transforming pairing-based schemes in composite-order groups to equivalent ones in prime-order groups. A method for achieving such transformations has recently been proposed by Freeman, who identified two properties of pairings using composite-order groups — "cancelling" and "projecting" — on which many schemes rely, and showed how either of these properties can be obtained using prime-order groups.

In this paper, we give evidence for the existence of limits to such transformations. Specifically, we show that a pairing generated in a natural way from the Decision Linear assumption in prime-order groups can be simultaneously cancelling and projecting only with negligible probability.

As evidence that these properties can be helpful together as well as individually, we present a cryptosystem whose proof of security makes use of a pairing that is both cancelling and projecting. Our example cryptosystem is a simple round-optimal blind signature scheme that is secure in the common reference string model, without random oracles, and based on mild assumptions; it is of independent interest.

1 Introduction

Composite-order groups were introduced for pairing-based cryptography in 2005 by Boneh, Goh, and Nissim [12] and have since been used to realize a large number of cryptographic systems (see, e.g., the schemes surveyed by Freeman [24]). At the same time, the limited number of elliptic curve families on which composite-order groups can be instantiated and the larger parameter sizes associated with composite-order groups (cf. [23, 13]) has motivated research on translating these schemes to or obtaining similar ones in the prime-order setting.

In one of the first papers to unify the composite- and prime-order settings, Groth and Sahai [31] developed non-interactive zero-knowledge schemes that not only can be instantiated either in composite- or prime-order groups, but are

in fact described identically in either instantiation. What facilitates this flexibility is a new abstraction for pairing-based cryptography in terms of modules over finite commutative rings with an associated bilinear map; this abstraction allows for the simultaneous treatment of three different cryptographic assumptions: the Subgroup Hiding (SGH) assumption of Boneh, Goh, and Nissim [12] in composite-order groups; the Decision Linear (DLIN) assumption of Boneh, Boyen, and Shacham [11], and its k-Linear family of generalizations [45, 33],[3] in prime-order groups; and the so-called Symmetric External Diffie-Hellman assumption [7], also in prime-order groups.

More recently, Freeman [24] and Garg, Sahai, and Waters [27] have proposed methods for transforming schemes secure in the composite-order setting into ones secure (under different but analogous assumptions) in the prime-order setting. Freeman, in particular, identifies two properties of pairings on composite-order groups, *projecting* and *cancelling*, and shows how either can be obtained in prime-order groups. He then demonstrates how to transform several known cryptosystems that rely on one of these properties from composite- to prime-order groups.

Our contribution: limits on transformations from composite to prime order. In this paper, we show limits to the feasibility of composite-to-prime transformations such as those mentioned above, suggesting that some schemes cannot be transformed mechanically from one setting to the other. In our main theorem, Theorem 6.5, we show that no pairing over prime-order groups can — except in a negligible fraction of cases — be both projecting and cancelling when subgroup indistinguishability relies in a natural way on k-Linear, where "natural" simply means that we follow the definition of the assumption as closely as possible.

If no cryptosystem required a pairing that is both projecting and cancelling, however, our Theorem 6.5 would not be particularly interesting. As such, we present a new cryptosystem — a natural pairing-based blind signature scheme that is of independent interest, and discussed below — whose proof of security calls for a pairing that is both projecting and cancelling.[4]

Blind signatures were introduced by Chaum in 1982 [17]. In a blind signature scheme, a user interacts in a protocol with a signer to obtain a signature on a message of the user's choice. When the protocol execution ends, the user obtains the signature but the signer learns nothing about the message that was signed. Blind signatures have been used as a building block in a variety of applications, including electronic cash [20] and electronic voting [19].

One useful feature of a blind signature scheme is *concurrency*. For example, if a blind signature used to build an electronic cash system does not retain its security even when the signer engages in multiple protocol executions concurrently, it leaves the issuing bank susceptible to denial-of-service attacks. Concurrency

[3] A family of progressively strictly weaker decisional assumptions, where 1-Linear is DDH and 2-Linear is DLIN.

[4] We emphasize that it is the security proof, not the statement of the scheme, that uses the two pairing properties. We thus do not rule out the possibility that a *different* proof strategy will show our scheme secure in prime-order groups.

turns out to be as difficult to achieve for blind signatures as it is for other cryptographic protocols. While many blind signature schemes have proofs of security only for sequential executions of the protocol, the problem is not merely with proofs. In one example, Martinet, Poupard, and Sola [38] show that signatures in a partially blind signature scheme of Cao, Lin and Xue [16] are forgeable if the signer interacts with two users concurrently.

Our contribution: a round-optimal blind signature scheme. As mentioned above, we present a new pairing-based blind signature scheme. Our blind signing protocol is round-optimal: it consists of only two moves (a request and a response), which implies that it is secure even in the presence of concurrent signing protocol executions. Our scheme is practical, has a proof of security (without random oracles) in the common reference string model, and relies for its security on falsifiable and non-interactive assumptions: computational Diffie-Hellman and Subgroup Hiding. These assumptions are milder than those used in any previous practical concurrently secure blind signature, including those in the random oracle model. ("Practical" in this sense means not relying on general NIZKs for NP as a building block.) Our scheme extends in a natural way to give a partially blind signature scheme [3] with the same properties.

Our blind signatures combine the Waters signature scheme [46] with non-interactive witness-indistinguishable proofs developed in a line of papers by Groth, Ostrovsky, and Sahai [30, 29, 31]. In this structure our scheme is related to the group signature scheme of Boyen and Waters [15]. The primary disadvantage of our scheme, as with the Boyen-Waters group signature, is its bit-at-a-time nature, which makes the user's blind signing request large: some 40 kilobytes at the 1024-bit security level. The signer's response and the resulting signatures, however, are short.

Related work. The blind signature literature is extensive and varied. Below, we briefly survey the most closely related schemes with concurrent security; see [5, 4] for more complete recent treatments.

In the random oracle model, there exist elegant round-optimal blind signatures, due to Chaum [18] and Boldyreva [10], that feature short public keys, short signatures, and an efficient blind signing protocol. Unfortunately the security proofs for these schemes rely on strong interactive assumptions: the RSA known-target inversion assumption [9] and the chosen-target CDH assumption (by contrast, the underlying ordinary signatures can be shown secure using RSA and CDH, respectively).

In the common reference string model, several practical concurrently secure blind signature schemes have been proposed. Unlike our scheme, these schemes rely on assumptions that are interactive or whose statement size grows with the number of queries in the reduction (i.e., "q-type"). Kiayias and Zhou [35] give four-move blind and partially-blind signature schemes secure under the (interactive) LRSW assumption [37], the Paillier assumption [42], and DLIN. Okamoto [40] gives four-move blind and partially blind signature schemes based on the (q-type) Two-Variable Strong Diffie-Hellman assumption and Paillier.

Fuchsbauer [25] gives two-move blind signature schemes based on the (q-type) Asymmetric Double Hidden Strong Diffie-Hellman assumption, the Asymmetric Weak Flexible CDH assumption, and DLIN. Finally, Abe, Haralambiev, and Ohkubo [4] give two-move blind signature schemes based on the (q-type) Simultaneous Flexible Pairing assumption and DLIN. (The last two papers appeared together as [2].)

Also in the common reference string model, blind signatures that use general NIZKs for NP (and are therefore not practical) were given by Juels, Luby, and Ostrovsky [34], Fischlin [22], and Abe and Ohkubo [5]. The Fischlin and Abe-Ohkubo schemes are round-optimal.

Okamoto [40] first observed that the Waters signature can be combined with witness-indistinguishable proofs for a simple NP language to yield blind and partially blind signatures. Our scheme could be viewed as an instantiation of Okamoto's framework (though we blind the message differently) where we take advantage of Groth-Ostrovsky-Sahai proofs to eliminate a round of interaction.

Until recently, no concurrently secure blind signature schemes were known in the plain public-key model. The first such scheme was given by Hazay et al. [32]; it relies on general NIZKs, and its round complexity is poly-logarithmic in the number of concurrent executions for which security must be guaranteed.

Applications and extensions. Finally, as an application of our techniques, we show (in the full version of our paper [39]) how our blind signatures may be used within the Waters IBE system [46] to yield a blind IBE scheme, as introduced by Green and Hohenberger [28]. Compared to Green and Hohenberger's blind extraction protocol, our protocol achieves concurrent security but adds a common reference string and a reliance on the SGH assumption.[5] Furthermore, the Waters signature naturally extends into a hierarchical identity-based signature (cf. [43]); applying our construction at level 2 of the resulting signature gives an identity-based blind signature [47] concurrently secure in the common reference string model.[6] Alternatively, using the Boyen-Waters group signature [15] at level 1 of the hierarchy and our blind signature at level 2 gives a group blind signature [36] concurrently secure in the common reference string model.

2 Mathematical Background

In this paper, we work with *bilinear groups*, which are cyclic groups G of some finite order that admit a nondegenerate bilinear map $e\colon G\times G \to G_T$. Because we generalize the concept of a group and work with modules, we are able to describe

[5] The efficient range proofs due to Boudot [14] rely on the Strong RSA assumption (due to Baric and Pfitzmann [8]) and require a common reference string. If the scheme of Green and Hohenberger is instantiated with these range proofs then its assumptions and setup model are comparable to those of our scheme, but without providing concurrent security.

[6] One could also obtain an identity-based blind signature through generic composition of our blind signature and an ordinary signature [26].

our scheme without relying on any particular properties of the underlying group (with the caveat, as mentioned above, that the scheme is provably secure only for composite-order groups).

2.1 Modules

We first recall the definition of a module; this serves as the foundation for our blind signature scheme, and more specifically for the Groth-Sahai commitments used in our scheme. (See [21, Ch. 10] for further background on modules.)

Definition 2.1. Let $(\mathcal{R}, +, \cdot, 0, 1)$ be a finite commutative ring. An *$\mathcal{R}$-module* A is an abelian group $(A, +, 0)$ such that there exists an operator (namely, scalar multiplication) $\mathcal{R} \times A \to A$, denoted by $(r, x) \mapsto rx$, satisfying the following four properties for all $r, s \in \mathcal{R}$ and $x, y \in A$:

- $(r + s)x = rx + sx$.
- $r(x + y) = rx + ry$.
- $r(sx) = (rs)x$.
- $1x = x$.

When A is written multiplicatively our operator becomes exponentiation and the requirements are written as $x^{r+s} = x^r \cdot x^s$, $(x \cdot y)^r = x^r \cdot y^r$, $(x^r)^s = x^{rs}$, and $x^1 = x$ for all $r, s \in \mathcal{R}$ and $x, y \in A$.

The concept of a module generalizes that of a vector space: when $\mathcal{R}$ is a field, the definitions of an $\mathcal{R}$-module and an $\mathcal{R}$-vector space coincide. The concept of a module also generalizes the concept of an abelian group, as any abelian group can be viewed as a $\mathbb{Z}$-module. If A is isomorphic to $\mathcal{R}^r$ as abelian groups, then r is the *rank* of A. When $\mathcal{R}$ is a field, module rank is the same as vector space dimension. In cryptography, we are most used to working with $\mathbb{Z}/n\mathbb{Z}$- and $\mathbb{F}_p$-modules; for example, any finite group of exponent p can be viewed as a $\mathbb{F}_p$-module.

2.2 Groth-Sahai commitments

Groth and Sahai [31] devise two types of commitments: commitments to elements in an $\mathcal{R}$-module A, and commitments to elements in the ring $\mathcal{R}$. For our purposes, we will need only commitments to bits; we can simplify things even further by always setting $A = G$ for our bilinear group G.

To form commitments to module elements, Groth and Sahai define an $\mathcal{R}$-module B and two homomorphisms $\tau : A \to B$ and $\rho : B \to A$.[7] These maps are defined such that, for some elements $h_1, \ldots, h_m$ in B, $\rho(h_i) = 1$ for all i and ρ is non-trivial for all x that are not contained in $B_1 := \langle h_1, \ldots, h_m \rangle$. A commitment to $x \in A$ is then defined as $c(x) = \tau(x) \prod_{i=1}^{m} h_i^{r_i}$ for random values $r_1, \ldots, r_m \leftarrow \mathcal{R}$. This means that the h_i elements act as keys for the commitment scheme, and that the common reference string is $(\mathcal{R}, A, B, \tau, \rho, h_1, \ldots, h_m)$. There are two cases:

[7] Our notation differs from that of Groth and Sahai, but the ideas are the same.

– Hiding keys: in this case, the h_i elements generate the whole module B; in other words, $B_1 = \langle h_1, \ldots, h_m \rangle = B$. This implies that $\tau(A) \subseteq B_1$, which means that $c(x)$ will be perfectly hiding (as each commitment will be a random element of B).
– Binding keys: in this case, $B_1 \neq B$ and $\rho(c) = \rho(\tau(x)h^r) = \rho \circ \tau(x)$ for some restricted space of inputs x. To determine what this restricted space is, we see that c will generally reveal the coset of B_1 where $\tau(x)$ lives. Thus in order for the commitment to be perfectly binding we must restrict the space of inputs x to be the inverse image of $B_2 \simeq B/B_1$; because we know that $B_1 \neq B$, both B_2 and $\tau^{-1}(B_2)$ are non-trivial and so this domain restriction is actually meaningful. (Since B is an abelian group, the quotient module is always well-defined.)

It is clear from these definitions that a set of keys cannot be both hiding and binding, as the settings require very different properties of the commitment keys $h_1, \ldots, h_m$. To get any meaningful blindness properties, however, we need these two settings to be indistinguishable. We therefore require an assumption that implies this indistinguishability; the choice of assumption depends on the instantiation being used.

3 Security Notions for Blind Signatures

We define a blind or partially blind signature scheme in the common reference string (CRS) model to be a collection of four protocols: a $\mathsf{Setup}(1^k)$ algorithm that outputs the CRS σ_{CRS}, a $\mathsf{KeyGen}(\sigma_{CRS})$ algorithm that outputs the signing key pair (pk, sk), a $\mathsf{BlindSign}$ protocol, which consists of an interaction of the form $\mathsf{User}(\sigma_{CRS}, pk, M) \leftrightarrow \mathsf{Signer}(\sigma_{CRS}, sk)$ (in which the signer outputs $\mathsf{success}$ if the protocol is successful, and the user outputs $\mathsf{success}$ and the unblinded signature σ), and finally a $\mathsf{Verify}(\sigma_{CRS}, pk, M, \sigma)$ algorithm that outputs accept if the signature is valid and fail if not.

In general, there are two properties that blind and partially blind signatures must satisfy: blindness and one-more unforgeability. Informally, the blindess requirement says that in the process of signing a user's message, the signer does not learn anything abut the message he is signing. The one-more unforgeability requirement says that if the user interacts with the signer ℓ times, then he should be able to produce ℓ signatures and no more (so in particular, he cannot produce $\ell + 1$). We now describe these properties more formally.

3.1 Blind signatures

Formal definitions of blind signatures were introduced by Juels, Luby, and Ostrovsky [34], although both properties were considered informally in Chaum's original paper on the subject [17], and one-more unforgeability was considered formally in Pointcheval and Stern's work on security arguments for signatures [44].

In the Juels-Luby-Ostrovsky formalization, the blindness property is defined as follows: the adversary is given a public-private key pair and outputs two messages M_0 and M_1. He then engages in two signing protocols with honest users: the first user requests a signature on message M_b and the second on message M_{1-b}, where b is a random bit unknown to the adversary. The adversary is then given the resulting signatures σ_0 and σ_1, but only if both interactions are successful, and his goal is to guess the bit b (given the messages, the corresponding signatures, and the signing protocol transcripts).

In this paper, we use a stronger version of the blindness property which allows the adversary to generate the signing key pair himself, possibly in a malicious manner. This strengthening was proposed independently in several recent papers [1, 41, 35].

The one-more unforgeability property can be defined as follows: the adversary is given a public key and engages in multiple executions of the blind signing protocol with a signer; the adversary is able to choose how to interleave the executions. At the end, the adversary is considered successful if he is able to output $\ell + 1$ distinct message-signature pairs $(M_1, \sigma_1), \ldots, (M_{\ell+1}, \sigma_{\ell+1})$, where ℓ is the number of executions in which the signer outputs success.

In this definition, two message-signature pairs (M_i, σ_i) and (M_j, σ_j) are considered distinct even if $M_i = M_j$ (so if σ_i and σ_j are just two different signatures on the same message) for $i \neq j$. Unfortunately, this means that any signature scheme in which signatures can be re-randomized (like our signature scheme, as we will see in Section 4) will automatically be unable to satisfy one-more unforgeability. We therefore weaken the property by requiring that the adversary be unable to output $\ell + 1$ message-signature pairs in which the *messages* are all distinct.[8] This modified definition was also considered recently by Okamoto [41].

We put all this information together and give a formal definition of security for blind signature schemes in the full version of this paper [39].

3.2 Partially blind signatures

The security properties of blind signatures can also be extended to partially blind signatures; these formalizations are due to Abe and Okamoto [6]. For partially blind signatures, the adversary outputs two info strings $info^{(0)}$ and $info^{(1)}$ in addition to its messages M_0 and M_1. It then interacts with two separate users in the same manner as before, except this time the first user requests a signature on M_b using $info^{(0)}$ and the second requests a signature on M_{1-b} with info $info^{(1)}$. The adversary is given the resulting signatures σ_0 and σ_1 if both interactions were successful and if $info^{(0)} = info^{(1)}$. As before, his goal is to guess the bit b.

The one-more unforgeability property is also quite similar to the property for blind signatures; here, the adversary is allowed to choose the info string for each interaction with the signer. The goal is then for the adversary to output an info string $info^*$ as well as $\ell + 1$ message-signature pairs $(M_1, \sigma_1), \ldots, (M_{\ell+1}, \sigma_{\ell+1})$,

[8] We observe that blind signatures satisfying this weakened unforgeability property are still sufficient for e-cash and other standard applications of blind signatures.

where ℓ represents the number of interactions in which the signer output success while using the info string $info^*$.

4 Underlying Signature Scheme

As our underlying signature scheme we use a slightly modified version of the Waters signature scheme [46]. Essentially, we just need to generalize the Waters signature scheme by bringing it into the language of modules so that we can use it in combination with Groth-Sahai commitments to create our blind signature scheme.

4.1 CRS setup

For the Waters signature, the required elements for the common reference string are a bilinear group G, the target group G_T and the bilinear map $e\colon G \times G \to G_T$, as well as generators $g, u', u_1, \ldots, u_k$ for G, where k denotes the length of the messages to be signed. We now add in the elements discussed in Section 2.2: we start with a ring $\mathcal{R}$ such that G can be interpreted as an $\mathcal{R}$-module. We then add in an $\mathcal{R}$-module B, a map $\tau\colon G \to B$, a map $\rho\colon B \to G$, and a bilinear map $E\colon B \times B \to B_T$, which also requires us to specify a target module B_T and the resulting τ_T and ρ_T maps. This means that the CRS will be $\sigma_{sig} = (\mathcal{R}, G, G_T, B, B_T, e, E, \tau, \tau_T, \rho, \rho_T, g, u', u_1, \ldots, u_k)$. The relations between all these maps are summarized in the following figure:

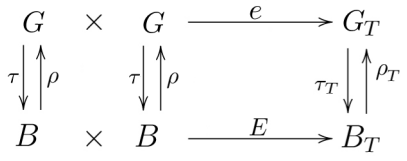

Fig. 1. Commutative diagram for our modules.

4.2 Signing protocol

In our generalized Waters signature, the size of the message space will be $\{0,1\}^k$ for some value k (for example, to use hash-and-sign with SHA-1 as the hash function we would set $k = 160$). As noted above, the CRS, which is shared between the user and the signer, will contain $k + 1$ random generators of G.

- $\mathsf{Setup}(1^k)$: Output a tuple σ_{sig} that has been computed as described in the previous section.
- $\mathsf{KeyGen}(\sigma_{sig})$: Pick a random value $\alpha \leftarrow \mathcal{R}$ and set $A = E(\tau(g), \tau(g))^\alpha$. The public key will be $pk = A$ and the secret key will be $sk = \alpha$ (actually, $\tau(g)^\alpha$ will suffice).

– $\mathsf{Sign}(\sigma_{sig}, sk, M)$: Write the message out bitwise as $M = b_1 \dots b_k$, and write $sk = \tau(g)^\alpha$. Pick a random $r \leftarrow \mathcal{R}$ and compute

$$S_1 = \tau(g)^\alpha \Big(\tau(u') \prod_{i=1}^{k} \tau(u_i)^{b_i}\Big)^r \quad \text{and} \quad S_2 = \tau(g)^{-r}.$$

Output the signature $\sigma = (S_1, S_2)$.

– $\mathsf{Verify}(\sigma_{sig}, pk, M, \sigma)$: Again, write the message out bitwise as $M = b_1 \dots b_k$; also write the signature as $\sigma = (S_1, S_2)$ and the public key as $pk = A$. Check that these values satisfy the following equation:

$$E(S_1, \tau(g)) \cdot E\Big(S_2, \tau(u') \prod_{i=1}^{k} \tau(u_i)^{b_i}\Big) = A. \tag{1}$$

If they do, output accept; else, output fail.

One nice property of the Waters signature (and our extended Waters signature) is that anyone can re-randomize a signature by choosing $s \leftarrow \mathcal{R}$ and computing $S_1' = S_1 \cdot \big(\tau(u') \prod_i \tau(u_i)^{b_i}\big)^s$ and $S_2' = S_2 \cdot \tau(g)^{-s}$. Since this results in $S_1' = \tau(g)^\alpha \big(\tau(u') \prod_i \tau(u_i)^{b_i}\big)^{r+s}$ and $S_2' = \tau(g)^{-(r+s)}$, the re-randomization process really does give us a valid signature. In particular, the randomness in the resulting signature (S_1', S_2') will be information-theoretically independent from the randomness r chosen by the signer in the signature (S_1, S_2).

We recall the computational Diffie-Hellman (CDH) assumption used for the Waters signature:

Assumption 4.1. *Let $\mathcal{G}$ be an algorithm that outputs a tuple (q, G, g), where G is a group of order q (not necessarily prime) and g is a generator of g. We say that G satisfies the computational Diffie-Hellman assumption if it is computationally infeasible to compute the value g^{ab} given the tuple (g, g^a, g^b). More formally, for all PPT adversaries $\mathcal{A}$ there exists a negligible function $\nu(\cdot)$ and a security parameter k_0 such that the following holds for all $k > k_0$:*

$$\Pr\big[(q, G, g) \leftarrow \mathcal{G}(1^k);\ a, b \leftarrow \mathbb{Z}_q\ :\ \mathcal{A}(g, g^a, g^b) = g^{ab}\big] = \nu(k).$$

The Waters signature scheme is existentially unforgeable if G satisfies the CDH assumption. In our extended version, the signature scheme will be existentially unforgeable if B satisfies the CDH assumption. As the proof is a trivial extension of Waters' proof, we will not include it here.

5 Our Blind Signature Scheme

In this section we describe our blind signature scheme. Although we describe only the partially blind setting, our description also encapsulates the fully blind setting, which corresponds to the case $k_0 = 0$.

5.1 CRS setup

In our CRS we must include all the necessary elements for Groth-Sahai commitments as well as values in the tuple σ_{sig} of Section 4.1. This means our CRS will be $\sigma_{CRS} = (\sigma_{sig}, h_1, \ldots, h_m)$, where the h_i elements are binding keys for Groth-Sahai commitments. Specifically, the elements h_i generate a proper submodule B_1 of the module B used in the Waters signature scheme.

5.2 The partially blind protocol

In the following protocol, the user and signer both have access to an info string *info*. At the end of the protocol, the user obtains a signature on $info||M$ for a message M, while the signer learns nothing beyond the fact that the message M followed the guidelines laid out in *info*. In addition, the user and the signer will have agreed upon the length of the *info* string; call it k_0 for $0 \leq k_0 \leq k$. Setting $k_0 = 0$ corresponds to a fully blind signature, while setting $k_0 = k$ corresponds to an ordinary run of the (generalized) Waters signature scheme.

- $\mathsf{Setup}(1^k)$: Output σ_{CRS} as described in the previous section (Section 5.1).
- $\mathsf{KeyGen}(\sigma_{CRS})$: Same as KeyGen from Section 4.2.
- $\mathsf{User}(\sigma_{CRS}, pk, info, M)$: First write the info string out bitwise, as $info = b_1 \ldots b_{k_0}$, and similarly write the message as $M = b_{k_0+1} \ldots b_k$. Now, for each i such that $k_0 < i \leq k$, pick random values $t_{i1}, \ldots, t_{im} \leftarrow \mathcal{R}$ and compute

$$c_i = \tau(u_i)^{b_i} \cdot \prod_{j=1}^{m} h_j^{t_{ij}} \quad \text{and} \quad \pi_{ij} = \Big(\tau(u_i)^{2b_i - 1} \cdot \prod_{j=1}^{m} h_j^{t_{ij}}\Big)^{t_{ij}},$$

  where c_i acts as a GS commitment to the bit b_i and $\vec{\pi}_i = \{\pi_{ij}\}_{j=1}^m$ acts as a proof that the value contained in c_i is in fact a 0 or a 1. Send the tuple $req = (c_{k_0+1}, \vec{\pi}_{k_0+1}, \ldots, c_k, \vec{\pi}_k)$ as a request to the issuer (and save some state information *state*).
- $\mathsf{Signer}(\sigma_{CRS}, sk, info, req)$: First, write $info = b_1 \ldots b_{k_0}$ and $sk = \tau(g)^\alpha$. Upon receiving the request, check that each c_i is indeed a commitment to a 0 or 1 by checking that

$$E\big(c_i, \tau(u_i)^{-1} c_i\big) = \textstyle\prod_{j=1}^{m} E(h_j, \pi_{ij}) \tag{2}$$

  for each $k_0 < i \leq k$. If this equation fails to hold for any value of i, abort the protocol and output $\perp$. Otherwise, compute the value

$$c = \tau(u')\Big(\prod_{i=1}^{k_0} \tau(u_i)^{b_i}\Big)\Big(\prod_{i=k_0+1}^{k} c_i\Big).$$

  Finally, pick a random value $r \leftarrow \mathcal{R}$ and compute

$$K_1 = \tau(g)^\alpha \cdot c^r, \quad K_2 = \tau(g)^{-r}, \quad \text{and} \quad K_{3j} = h_j^{-r} \quad \text{for } 1 \leq j \leq m.$$

  Set $\vec{K}_3 = \{K_{3j}\}_{j=1}^m$, send the tuple $(K_1, K_2, \vec{K}_3)$ back to the user, and output $\mathsf{success}$ and *info*.

– $\mathsf{User}(state, (K_1, K_2, \vec{K}_3))$: First, check that K_2 and $\vec{K}_3$ were formed properly by checking satisfiability of

$$E\big(K_{3j}, \tau(g)\big) = E(K_2, h_j) \tag{3}$$

for each $1 \leq j \leq m$. If this equation does not verify for some j, abort and output $\perp$. Otherwise, unblind the signature by computing

$$S_1 = K_1 \prod_{i=k_0+1}^{k} \prod_{j=1}^{m} K_{3j}^{\,t_{ij}} \quad \text{and} \quad S_2 = K_2. \tag{4}$$

Next verify that this is a valid signature on $info||M$ by running $\mathsf{Verify}(\sigma_{CRS}, pk, info||M, (S_1, S_2))$. If this step outputs fail, abort the protocol and output $\perp$. If it outputs accept, however, re-randomize the signature by choosing a random value $s \leftarrow \mathcal{R}$ and computing

$$S_1' = S_1\Big(\tau(u') \prod_{i=1}^{k} \tau(u_i)^{b_i}\Big)^s \quad \text{and} \quad S_2' = S_2 \cdot \tau(g)^{-s}.$$

The final signature is $\sigma = (S_1', S_2')$; output σ as well as *info* and $\mathsf{success}$.

– $\mathsf{Verify}(\sigma_{CRS}, pk, M, \sigma)$: Same as Verify from Section 4.2.

Theorem 5.1. *The blind signature scheme outlined above is correct and partially blind, under the assumption that the h_i values in the hiding and binding settings are indistinguishable.*

The proof of Theorem 5.1 appears in the full version of this paper [39]. The theorem demonstrates correctness and (partial) blindness, but it does not show one-more unforgeability. In order to prove this last property, we need to define two properties of pairings, adapted from Freeman [24, §3] for our purposes:

Definition 5.2. A pairing $E\colon B \times B \to B_T$ is *cancelling* if there exists a decomposition $B = B_1 \times B_2$ such that $E(b_1, b_2) = 1$ for all $b_1 \in B_1$, $b_2 \in B_2$.

Definition 5.3. A pairing $E\colon B \times B \to B_T$ is *projecting* if there exists a decomposition $B = B_1 \times B_2$, a submodule $B_T' \subset B_T$, and homomorphisms $\pi\colon B \to B$ and $\pi_T\colon B_T \to B_T$, such that $B_1 \subseteq \ker(\pi)$, $\pi(x) = x$ for $x \in B_2$, $B_T' \subseteq \ker(\pi_T)$, and $\pi_T(E(x, y)) = E(\pi(x), \pi(y))$ for all $x, y \in B$.

As we will see below, the pairing E has both of these properties (with respect to the same decomposition $B = B_1 \times B_2$) when instantiated using composite-order groups under the Subgroup Hiding (SGH) assumption. Because SGH also provides the necessary indistinguishability properties, we obtain the following theorem, a proof of which can be found in the full version of this paper [39]:

Theorem 5.4. *The blind signature scheme outlined above is one-more unforgeable under the SGH assumption and the assumption that the modified Waters signature scheme in Section 4 is existentially unforgeable on the submodule $B_2 \subseteq B$.*

5.3 Instantiation under the SGH assumption

We first recall the Subgroup Hiding (SGH) assumption:

Assumption 5.5 ([12]). *Let $\mathcal{G}$ be an algorithm that outputs a tuple (p, q, G, G_T, e) such that G and G_T are both groups of order $n = pq$ and $e\colon G \times G \to G_T$ is a nondegenerate bilinear map. We say that G satisfies the Subgroup Hiding assumption if it is computationally infeasible to distinguish between an element of G and an element of G_q. More formally, for all PPT adversaries $\mathcal{A}$ there exists a negligible function $\nu(\cdot)$ and a security parameter k_0 such that the following holds for all $k > k_0$:*

$$\Big|\Pr\big[(p,q,G,G_T,e) \leftarrow \mathcal{G}(1^k); n = pq; x \leftarrow G : \mathcal{A}(n, G, G_T, e, x) = 0\big] - \Pr\big[(p,q,G,G_T,e) \leftarrow \mathcal{G}(1^k); n = pq; x \leftarrow G : \mathcal{A}(n, G, G_T, e, x^p) = 0\big]\Big| < \nu(k).$$

To instantiate our blind signature scheme under this assumption, we use a group G of order $n = pq$ with p, q prime. We define $B = G$ and τ to be the identity map; this means that we can use $E = e$. We need only one h_i element, namely an h_1 such that h_1 generates G_q in the binding setting and h_1 generates the whole group G in the hiding setting. The SGH assumption tells us that these choices of h_1 are indistinguishable. We can also describe our ρ map as $\rho(c_i) = c_i^q = (u_i^q)^{b_i}$ since h_1 has order q. Because the u_i are all generators for G and therefore $u_i^q \neq 1$, we see that the ρ map will indeed reveal the bit b_i.

Because h_1 will generate either G or G_q, we have $B = G_p \times G_q$, which means (looking back at the statement of Theorem 5.4) that we assume for the security of our blind signature that CDH is hard in G_p. To see that the pairing e is cancelling, note that every element of G_p can be written as $a = g^{\alpha q}$ for some $\alpha \in \mathbb{F}_p$ and every element of G_q can be written as as $b = g^{\beta p}$ for some $\beta \in \mathbb{F}_q$. Then $e(a, b) = e(g^{\alpha q}, g^{\beta p}) = e(g^{\alpha\beta pq}, g) = e\big((g^n)^{\alpha\beta}, g\big) = 1$ because G has order n. To see that e is projecting, note that there exists a $\lambda \in \mathbb{Z}_n$ such that $\lambda \equiv 1 \bmod p$ and $\lambda \equiv 0 \bmod q$, and that furthermore this value is efficiently computable (given the factorization of n) using the Chinese Remainder Theorem. Thus exponentiating by λ cancels out the G_q component of a group element while leaving the G_p component unchanged. This allows us to define $\pi(z) = z^\lambda$ for $z \in G$ and $\pi_T(z_T) = (z_T)^\lambda$ for $z_T \in G_T$. These maps are easily seen to satisfy the projecting properties.

Finally, to compute the value h_1 we can set $h_1 = g$ in the hiding setting and $h_1 = g^p$ in the binding setting. This means that, as with the map ρ, the factorization of n will be required as a trapdoor to compute h_1.

The obvious downside of using our scheme under the SGH assumption is the use of a composite-order group, which necessitates a common reference string generated by a trusted third party.[9] The upside, on the other hand, is that the

[9] It is an open problem to replace the trusted third party with an efficient secure multiparty computation protocol for computing the CRS.

scheme is as efficient as possible under this assumption, as each part of the signature involves only one group element.[10]

6 Converting to a Prime-Order Setting

In this section we argue that our scheme cannot be instantiated securely under a natural usage of the k-Linear family of assumptions in prime-order groups. The k-Linear family generalizes the Decision Diffie-Hellman and Decision Linear [11] assumptions (which can be recovered by setting $k = 1$ or 2, respectively) and is defined as follows:

Assumption 6.1 ([45, 33]). *Let $\mathcal{G}$ be a generation algorithm that outputs a tuple (p, G, g) such that p is prime, G is a group of order p, and g is a generator of G. We say that G satisfies the k-Linear assumption if it is computationally infeasible to distinguish between tuples of the form $(g^{\alpha_1}, \ldots, g^{\alpha_{k+1}}, g^{\alpha_1 r_1}, \ldots, g^{\alpha_k r_k}, g^{\alpha_{k+1} \sum_{i=1}^{k} r_i})$ and tuples of the form $(g^{\alpha_1}, \ldots, g^{\alpha_{k+1}}, g^{\alpha_1 r_1}, \ldots, g^{\alpha_{k+1} r_{k+1}})$ for random $\alpha_i, r_i \leftarrow \mathbb{F}_p$. More formally, for all PPT adversaries $\mathcal{A}$ there exists a negligible function $\nu(\cdot)$ and a security parameter k_0 such that the following holds for all $k > k_0$:*

$$\left| \Pr\left[\begin{array}{l} (p,G,g) \leftarrow \mathcal{G}(1^k) \\ \alpha_1,\ldots,\alpha_{k+1} \xleftarrow{R} \mathbb{F}_p \\ r_1,\ldots,r_k \xleftarrow{R} \mathbb{F}_p \end{array} : \mathcal{A}(g^{\alpha_1}, \ldots, g^{\alpha_{k+1}}, g^{\alpha_1 r_1}, \ldots, g^{\alpha_{k+1} \sum_{i=1}^{k} r_i}) = 0 \right] \right.$$
$$\left. - \Pr\left[\begin{array}{l} (p,G,g) \leftarrow \mathcal{G}(1^k) \\ \alpha_1,\ldots,\alpha_{k+1} \xleftarrow{R} \mathbb{F}_p \\ r_1,\ldots,r_{k+1} \xleftarrow{R} \mathbb{F}_p \end{array} : \mathcal{A}(g^{\alpha_1}, \ldots, g^{\alpha_{k+1}}, g^{\alpha_1 r_1}, \ldots, g^{\alpha_{k+1} r_{k+1}}) = 0 \right] \right| < \nu(k),$$

Let G be a bilinear group of prime order p with a pairing $e\colon G \times G \to G_T$. When we refer to a "natural" use of the k-Linear assumption, we mean that we define the module B to be G^{k+1} and the module B_1 to be generated by k elements of B that span a rank-k submodule. Indeed, one way to interpret the k-Linear assumption is that a random element in the submodule B_1 of G^{k+1} generated by elements of the form $(1, \ldots, 1, g^{\alpha_i}, 1, \ldots, 1, g)$ for $i = 1, \ldots, k$ is indistinguishable from a random element of G^{k+1}. Our use of the assumption generalizes this interpretation only slightly, by randomizing the generators of B_1. Note that in our setup the quotient module $B_2 = B/B_1$ has $\mathbb{F}_p$-rank 1.

Following Freeman [24, §2], we define a (symmetric) pairing on B by setting $B_T = (G_T)^m$ for some integer m and choosing $(k+1) \times (k+1)$ (symmetric) matrices $E^{(\ell)}$ over $\mathbb{F}_p$ for $\ell = 1, \ldots, m$. We then set the ℓth component of the pairing to be

$$E\Big((g_1, \ldots, g_{k+1}), (h_1, \ldots, h_{k+1})\Big)^{(\ell)} := \prod_{i,j=1}^{k+1} e(g_i, h_j)^{e_{ij}^{(\ell)}}, \tag{5}$$

[10] Of course, the number of bits taken to represent the composite-order group element, approximately 1024, is much larger than it would be for a prime-order group element, which can be as small as 160 bits (at the 80-bit security level).

where $e_{ij}^{(\ell)}$ denotes the (i,j)-th entry of $E^{(\ell)}$. The connection between this setup and the k-Linear assumption is given by the following theorem:

Theorem 6.2 ([24, Theorem 2.5]). *Let G, B, B_1, B_T be as described above, with B_1 a uniformly random rank-k submodule of B. If G satisfies the k-Linear assumption, then a random element of B_1 is computationally indistinguishable from a random element in B.*

While any scheme based on Groth-Sahai proofs requires the projecting property of Definition 5.3 and the indistinguishability of elements in B_1 and B (i.e., the indistinguishability of hiding and binding commitment keys), our scheme also requires the cancelling property of Definition 5.2. In the remainder of this section, we show that for any k, the three properties (projecting, cancelling, and key indistinguishability) cannot simultaneously be obtained in prime-order groups using the k-Linear assumption as described above, except with negligible probability (over the choice of the module B_1).

We start by showing that the image of a symmetric pairing on a group G of prime order p must also have order p. In what follows, we denote by $E(B,B)$ the submodule of B_T generated by all elements of the form $E(x,y)$ for $x, y \in B$.

Lemma 6.3. *If G is a group of prime order p and $e\colon G \times G \to G_T$ is a nondegenerate symmetric bilinear map, then the order of $e(G,G)$ is p.*

Proof. We first observe that $e(G,G)$ has exponent p; to see this, note that since G has order p, we have $e(x,y)^p = e(x^p, y) = e(1,y) = 1$ for any $x, y \in G$. Since $e(G,G)$ has exponent p, any element is of the form $z = \prod_i e(x_i, y_i)^{c_i}$ for $x_i, y_i \in G$ and $c_i \in \mathbb{F}_p$. Since G is cyclic, we can write $x_i = g^{a_i}$ and $y_i = g^{b_i}$ for a generator g and unique $a_i, b_i \in \mathbb{F}_p$. By bilinearity, we can write $z = e(g,g)^{\sum_i a_i b_i c_i}$, and therefore $e(G,G)$ is a cyclic group generated by $e(g,g)$; the nondegeneracy of e implies that $e(g,g)$ has order p. □

Lemma 6.3 shows that by replacing G_T with $e(G,G)$, we may assume without loss of generality that G_T has order p. We make this assumption in the remainder of the section. We will also assume that the values used to define the pairing E on the module B are independent of the submodules B_1 and B_2; if they are not independent, then the fact that they are related to the (publicly known) generators of B_1 gives an adversary information about B_1 that could be used to break the indistinguishability assumption. Similarly, if the pairing depends on B_2, then the adversary may be able to use this information to compute an element $y \in B_2$; then given an element x in either B_1 or B, he could compute $E(x,y)$ and conclude that $x \in B_1$ if and only if the resulting value is 1.

We can now show that in the prime-order setting our indistinguishability restrictions on B and its submodules will, with high probability, yield a pairing E that can be either projecting or cancelling, but not both at the same time. Our approach is to construct a cancelling pairing and then show that it implies that the image of the pairing E is of order p. We will then show that this implies that the pairing cannot satisfy the projecting property.

In general, there are two methods in the literature for cancelling paired group elements. As seen in Section 5.3, the cancelling in the composite setting is fairly straightforward: it follows from the fact that the orders of the G_p and G_q subgroups are relatively prime. In a prime-order setting this is not an option, as every component (i.e., G, G_T, B, B_1, B_2, B_T) has exponent p. We therefore need to use linear combinations of exponents in order to successfully cancel elements. Our next result can be interpreted as showing that forming these linear combinations requires us to combine elements in the pairing and thus shrink the size of the pairing's image. To simplify notation, we state the proposition relative to the $(k-1)$-Linear assumption.

Proposition 6.4. *Let G be a bilinear group of prime order p with pairing $e\colon G \times G \to G_T$. Let B be the rank-k G-module G^k, let $B_T = (G_T)^m$ for some positive integer m, and let $E\colon B \times B \to B_T$ be a nondegenerate pairing defined as in* (5)*. If B_1 is a uniformly random rank-$(k-1)$ submodule of B and E is a cancelling pairing that is independent of the decomposition $B = B_1 \times B_2$, then $e(B, B)$ has order p with overwhelming probability.*

Proof. To start, we write elements in B as either $\mathbf{a} = (a_1, \ldots, a_k)$ or $\mathbf{b} = (b_1, \ldots, b_k)$ with $a_i, b_i \in G$. Equivalently, we can fix a generator g of G and write $\mathbf{a} = (g^{\alpha_1}, \ldots, g^{\alpha_k})$ and $\mathbf{b} = (g^{\beta_1}, \ldots, g^{\beta_k})$ for exponents $\alpha_i, \beta_i \in \mathbb{F}_p$. As we saw in (5) above, the element $E(\mathbf{a}, \mathbf{b}) \in B_T$ is a tuple of elements of G_T, in which each entry is of the form $T = \prod_{i,j} e(a_i, b_j)^{e_{ij}}$. By assumption, the coefficients $e_{ij} \in \mathbb{F}_p$ are independent of the α_i and β_i values.

Suppose that $\mathbf{a} \in B_1$ and $\mathbf{b} \in B_2$; let us see what we require in order to have $T = 1$. Let $\mathbf{a}_1, \ldots, \mathbf{a}_{k-1}$ be a set of generators of B_1, and write $\mathbf{a}_u = (g^{\alpha_{u1}}, \ldots, g^{\alpha_{u,k-1}})$ for $u = 1, \ldots, k-1$. Then a general element of B_1 is given by $\mathbf{a} = \mathbf{a}^{r_1} \cdots \mathbf{a}^{r_{k-1}}$ for arbitrary $r_1, \ldots, r_{k-1} \in \mathbb{F}_p$. Since B_1 has rank $k-1$, the submodule B_2 has rank 1 and a general element of B_2 is given by $\mathbf{b} = (g^{\beta_1 t}, \ldots, g^{\beta_k t})$ for some fixed $\beta_1, \ldots, \beta_k \in \mathbb{F}_p$ and arbitrary $t \in \mathbb{F}_p$. Looking back at how our element T is computed in (5), we can see that the condition $T = 1$ is equivalent to

$$\sum_u r_u \left(\sum_i \alpha_{ui} \left(\sum_j e_{ij} \beta_j t \right) \right) = 0$$

In matrix notation, this is $\vec{r} \cdot A \cdot E \cdot \vec{b} \cdot t = 0$, where $\vec{r}$ is the row vector $(r_1, \ldots, r_{k-1})$, $E = [e_{ij}]$ is the $k \times k$ matrix specifying the pairing coefficients (denoted $E^{(\ell)}$ in (5)), $A = [\alpha_{ui}]$ is the $(k-1) \times k$ matrix whose rows are the vectors corresponding to the generators of B_1, and $\vec{b}$ is the column vector $(\beta_1, \ldots, \beta_k)$. Because this requirement must hold for all values of $\vec{r}$ and t, we can further reduce the equation to $A \cdot E \cdot \vec{b} = 0$. We now consider two different cases: when E is invertible and when E is singular.

We first consider the case where E is singular. The cancelling property requires that $A \cdot E \cdot \vec{b} = 0$. If $E \cdot \vec{b} = 0$, then the pairing is degenerate in this component, as *any* element paired with $\vec{b}$ will be 1. Therefore, this cannot be

the only type of element in the pairing tuple, or else the entire pairing would be degenerate. On the other hand, if $E \cdot \vec{b} \neq 0$, then since $A \cdot E \cdot \vec{b} = 0$, we see that $E \cdot \vec{b}$ is a nonzero vector in both the image of E and the kernel of A.

Next we consider the case where E is invertible, and consider not only the element T but also another element T' in the target tuple. The element T' will have its own associated coefficient matrix E', with the requirement that $A \cdot E' \cdot \vec{b} = 0$. Then we have $A \cdot E \cdot \vec{b} = A \cdot E' \cdot \vec{b} = 0$, which implies that $\vec{b}$ is contained in both the kernel of $A \cdot E$ and the kernel of $A \cdot E'$. Since A has rank $k-1$ and we are assuming E to be invertible, we know that the dimension of $\ker(A \cdot E)$ is 1. Furthermore, since E is invertible we can write

$$A \cdot E' \cdot \vec{b} = A \cdot (E \cdot E^{-1}) \cdot E' \cdot \vec{b} = A \cdot E \cdot (E^{-1} \cdot E' \cdot \vec{b}) = 0,$$

which implies that $E^{-1}E' \cdot \vec{b}$ is also contained in the kernel of $A \cdot E$. Since this kernel is one-dimensional, $E^{-1}E' \cdot \vec{b}$ must be a constant multiple of $\vec{b}$; i.e., $E^{-1}E' \cdot \vec{b} = \lambda \cdot \vec{b}$ for some $\lambda \in \mathbb{F}_p$ and $\vec{b}$ is an eigenvector of $E^{-1}E'$.

We now observe that because A has rank $k-1$, its kernel has rank one; furthermore, choosing a rank-$(k-1)$ submodule B_1 is equivalent to choosing the one-dimensional subspace $\ker(A)$. Since E is invertible and independent of B_1, this is equivalent to choosing the one-dimensional subspace $\ker(A \cdot E)$. Let $\vec{u}$ be any vector in $\ker(A \cdot E)$. Then $\vec{u} = \gamma \cdot \vec{b}$ for some $\gamma \in \mathbb{F}_p$, and our analysis above shows that $\vec{u}$ is an eigenvector of $E^{-1}E$. Since $\ker(A \cdot E)$ can contain *any* nonzero vector $\vec{u}$, this implies that *every* vector is an eigenvector of $E^{-1}E$. Therefore $E^{-1}E'$ must be a diagonal matrix with the same value in each diagonal entry; in other words, we have $E^{-1}E' = cI$ for some constant $c \in \mathbb{F}_p$. Thus we have $E' = cI \cdot E = c \cdot E$, and so $T' = T^c$.

It remains only to put everything together. Let $E^{(\ell)}$ be the coefficient matrix from (5) used to compute the ℓth component of the pairing. Our argument above shows that if *one* of the matrices $E^{(\ell)}$ is invertible, then *all* matrices $E^{(\ell')}$ are constant multiples of $E^{(\ell)}$, and therefore the order of $e(B, B)$ is the same as the order of $e(G, G) = G_T$, which is p. Thus if the pairing E is cancelling and the order of $e(B, B)$ is greater than p, then *none* of the matrices $E^{(\ell)}$ can be invertible.

Now suppose all of the $E^{(\ell)}$ are singular. Our consideration of this case above shows that if the pairing E is cancelling, then there must be *some* matrix $E^{(\ell)}$ with $\ker(A) \cap \mathrm{im}(E^{(\ell)}) \neq \{0\}$. As noted above, choosing the module B_1 is equivalent to choosing the one-dimensional subspace $\ker A$. Since $E^{(\ell)}$ is not invertible, we have $\dim(\mathrm{im}(E^{(\ell)})) \leq k-1$. Thus the number of one-dimensional subspaces in $\mathrm{im}(E^{(\ell)})$ is at most $(p^{k-1}-1)/(p-1)$, while the number of one-dimensional subspaces in $\mathbb{F}_p^k$ is $(p^k-1)/(p-1)$. We conclude that the probability (taken over a uniformly random choice of $\ker(A)$ and thus also of A) that $\ker(A)$ has nontrivial intersection with the image of $E^{(\ell)}$ is at most $(p^{k-1}-1)/(p^k-1) < 2/p$. Taking a union bound, we conclude that the probability that $\ker(A) \cap \mathrm{im}(E^{(\ell)}) \neq 0$ for *some* ℓ is at most $2m/p$, which is negligible. □

Putting all this together, we can prove our main theorem:

Theorem 6.5. *Let G be a bilinear group of prime order p with pairing $e\colon G \times G \to G_T$. Let B be the rank-k G-module G^k, let $B_T = (G_T)^m$ for some positive integer m, and let $E\colon B \times B \to B_T$ be a nondegenerate pairing defined as in (5). If B_1 is a uniformly random rank-$(k-1)$ submodule of B and E is a cancelling pairing that is independent of the decomposition $B = B_1 \times B_2$, then with overwhelming probability the pairing E cannot be projecting (with respect to the same decomposition $B = B_1 \times B_2$).*

Proof. By Proposition 6.4, we know that if E is cancelling, then $E(B, B)$ has order p with overwhelming probability. This means that $E(B, B)$ is cyclic and any nonzero element is a generator.

Suppose E is projecting and choose some $x \in B_1$. Since E is nondegenerate, there is some $y \in B$ such that $E(x, y) \neq 1$. Now the projecting property implies that $\pi_T(E(x, y)) = E(\pi(x), \pi(y)) = E(1, \pi(y)) = 1$. Since $E(x, y)$ generates $E(B, B)$, we conclude that $\pi_T(E(B, B)) = \{1\}$.

On the other hand, now choose some $x' \in B_2$. Then there is some $y' \in B$ such that $E(x', y') \neq 1$. Furthermore, the cancelling property implies that without loss of generality we can assume $y' \in B_2$. The projecting property now implies that $\pi_T(E(x', y')) = E(\pi(x'), \pi(y')) = E(x', y') \neq 1$, so we conclude that $\pi_T(E(B, B)) = E(B, B)$, contradicting our conclusion above. □

7 Conclusions and Open Problems

In this paper we have shown that there are limitations on transformations of pairing-based cryptosystems from composite- to prime-order groups. In particular, we have given evidence that two properties of composite-order pairings identified by Freeman — cancelling and projecting — cannot be simultaneously obtained in prime-order groups.

Specifically, we have shown that a pairing defined in a natural way with subgroup hiding provided by the Decision Linear assumption can be both cancelling and projecting with only negligible probability. As evidence that both properties are sometimes called for simultaneously, we have presented a natural cryptographic scheme whose proof of security calls for a pairing that is both cancelling and projecting. This scheme is a practical round-optimal blind (and partially blind) signature secure in the common reference string model, under mild assumptions and without random oracles.

Many open questions remain. First, we would like either to generalize our result so it applies to a wider class of pairings constructed from prime order groups (possibly including asymmetric pairings), or instead to show that no such generalization is possible by exhibiting a pairing in prime-order groups that is simultaneously projecting and cancelling. Second, we have given evidence that our specific proof strategy for our blind signature scheme is unlikely to generalize to prime-order groups, but have not settled the question of whether our scheme when instantiated in prime-order groups is in fact provably secure (by means of a different, ad-hoc proof) or insecure (i.e., actually susceptible to attack). Finally, it is interesting to consider whether a more general procedure (not relying on

Freeman's properties) can be used to transform every composite-order scheme to a prime-order one, or whether some schemes provably cannot be so transformed.

Acknowledgements. We are grateful to Melissa Chase for helpful discussions about this work and to our anonymous reviewers for their helpful comments. The first author is supported in part by a MURI grant administered by the Air Force Office of Scientific Research and in part by a graduate fellowship from the Charles Lee Powell Foundation. The third author is supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship.

References

1. M. Abdalla, C. Namprempre, and G. Neven. On the (im)possibility of blind message authentication codes. In D. Pointcheval, editor, *Proceedings of CT-RSA 2006*, volume 3860 of *LNCS*, pages 262–79. Springer-Verlag, Feb. 2006.
2. M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-preserving signatures and commitments to group elements. In T. Rabin, editor, *Proceedings of Crypto 2010*, volume 6223 of *LNCS*, pages 209–36. Springer, 2010.
3. M. Abe and E. Fujisaki. How to date blind signatures. In K. Kim and T. Matsumoto, editors, *Proceedings of Asiacrypt 1996*, volume 1163 of *LNCS*, pages 244–51. Springer-Verlag, Nov. 1996.
4. M. Abe, K. Haralambiev, and M. Ohkubo. Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133, 2010. `http://eprint.iacr.org/`.
5. M. Abe and M. Ohkubo. A framework for universally composable non-committing blind signatures. In M. Matsui, editor, *Proceedings of Asiacrypt 2009*, volume 5912 of *LNCS*, pages 435–50. Springer-Verlag, Dec. 2009.
6. M. Abe and T. Okamoto. Provably secure partially blind signatures. In M. Bellare, editor, *Proceedings of Crypto 2000*, volume 1880 of *LNCS*, pages 271–86. Springer-Verlag, Aug. 2000.
7. L. Ballard, M. Green, B. de Medeiros, and F. Monrose. Correlation-resistant storage via keyword-searchable encryption. Cryptology ePrint Archive, Report 2005/417, 2005. `http://eprint.iacr.org/`.
8. N. Baric and B. Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. In W. Fumy, editor, *Proceedings of Eurocrypt 1997*, volume 1233 of *LNCS*, pages 480–494. Springer-Verlag, May 1997.
9. M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko. The power of RSA inversion oracles and the security of Chaum's RSA-based blind signature scheme. In P. Syverson, editor, *Proceedings of Financial Cryptography 2001*, volume 2339 of *LNCS*, pages 319–38. Springer-Verlag, 2002.
10. A. Boldyreva. Threshold signature, multisignature and blind signature schemes based on the gap-Diffie-Hellman-group signature scheme. In Y. Desmedt, editor, *Proceedings of PKC 2003*, volume 2567 of *LNCS*, pages 31–46. Springer-Verlag, Jan. 2003.
11. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. Franklin, editor, *Proceedings of Crypto 2004*, volume 3152 of *LNCS*, pages 41–55. Springer-Verlag, Aug. 2004.
12. D. Boneh, E.-J. Goh, and K. Nissim. Evaluating 2-DNF formulas on ciphertexts. In J. Kilian, editor, *Proceedings of TCC 2005*, number 3378 in LNCS, pages 325–41. Springer-Verlag, Feb. 2005.

13. D. Boneh, K. Rubin, and A. Silverberg. Finding composite order ordinary elliptic curves using the Cocks-Pinch method. Cryptology ePrint Archive, Report 2009/533, 2009. http://eprint.iacr.org/2009/533.
14. F. Boudot. Efficient proofs that a committed number lies in an interval. In B. Preneel, editor, *Proceedings of Eurocrypt 2000*, volume 1807 of *LNCS*, pages 431–44. Springer-Verlag, May 2000.
15. X. Boyen and B. Waters. Compact group signatures without random oracles. In S. Vaudenay, editor, *Proceedings of Eurocrypt 2006*, volume 4004 of *LNCS*, pages 427–44. Springer-Verlag, May 2006.
16. T. Cao, D. Lin, and R. Xue. A randomized RSA-based partially blind signature scheme for electronic cash. *Computers and Security*, 24(1):44–49, Feb. 2005.
17. D. Chaum. Blind signatures for untraceable payments. In D. Chaum, R. Rivest, and A. Sherman, editors, *Proceedings of Crypto 1982*, pages 199–204. Plenum Press, 1983.
18. D. Chaum. Blind signature system (abstract). In D. Chaum, editor, *Proceedings of Crypto 1983*, page 153. Plenum Press, 1984.
19. D. Chaum. Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA. In C. Günther, editor, *Proceedings of Eurocrypt 1988*, volume 330 of *LNCS*, pages 177–82. Springer-Verlag, May 1988.
20. D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In S. Goldwasser, editor, *Proceedings of Crypto 1988*, volume 403 of *LNCS*, pages 319–27. Springer-Verlag, 1990.
21. D. Dummit and R. Foote. *Abstract Algebra*. Prentice-Hall, Upper Saddle River, NJ, 2nd edition, 1999.
22. M. Fischlin. Round-optimal composable blind signatures in the common reference string model. In C. Dwork, editor, *Proceedings of Crypto 2006*, volume 4117 of *LNCS*, pages 60–77. Springer-Verlag, Aug. 2006.
23. D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. *J. Cryptology*, 23(2):224–80, Apr. 2010.
24. D. M. Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In H. Gilbert, editor, *Proceedings of Eurocrypt 2010*, LNCS, pages 44–61. Springer-Verlag, May 2010.
25. G. Fuchsbauer. Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. Cryptology ePrint Archive, Report 2009/320, 2009. http://eprint.iacr.org/.
26. D. Galindo, J. Herranz, and E. Kiltz. On the generic construction of identity-based signatures with additional properties. In X. Lai and K. Chen, editors, *Proceedings of Asiacrypt 2006*, volume 4284 of *LNCS*, pages 178–93. Springer-Verlag, Dec. 2006.
27. S. Garg, A. Sahai, and B. Waters. Efficient fully collusion-resilient traitor tracing scheme. Cryptology ePrint Archive, Report 2009/532, 2009. http://eprint.iacr.org/2009/532.
28. M. Green and S. Hohenberger. Blind identity-based encryption and simulatable oblivious transfer. In *Proceedings of Asiacrypt 2007*, volume 4833 of *LNCS*, pages 265–282. Springer-Verlag, 2007.
29. J. Groth, R. Ostrovsky, and A. Sahai. Non-interactive zaps and new techniques for NIZK. In C. Dwork, editor, *Proceedings of Crypto 2006*, volume 4117 of *LNCS*, pages 97–111. Springer-Verlag, Aug. 2006.
30. J. Groth, R. Ostrovsky, and A. Sahai. Perfect non-interactive zero knowledge for NP. In S. Vaudenay, editor, *Proceedings of Eurocrypt 2006*, volume 4004 of *LNCS*, pages 339–58. Springer-Verlag, May 2006.

31. J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In *Proceedings of Eurocrypt 2008*, volume 4965 of *LNCS*, pages 415–432. Springer-Verlag, 2008.
32. C. Hazay, J. Katz, C.-Y. Koo, and Y. Lindell. Concurrently-secure blind signatures without random oracles or setup assumptions. In S. Vadhan, editor, *Proceedings of TCC 2007*, volume 4392 of *LNCS*, pages 323–341. Springer-Verlag, 2007.
33. D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. In A. Menezes, editor, *Proceedings of Crypto 2007*, volume 4622 of *LNCS*, pages 553–71. Springer-Verlag, Aug. 2007.
34. A. Juels, M. Luby, and R. Ostrovsky. Security of blind digital signatures. In B. Kaliski, Jr., editor, *Proceedings of Crypto 1997*, volume 1294 of *LNCS*, pages 150–64. Springer-Verlag, Aug. 1997.
35. A. Kiayias and H.-S. Zhou. Concurrent blind signatures without random oracles. In M. Yung, editor, *Proceedings of SCN 2006*, volume 4116 of *LNCS*, pages 49–62. Springer-Verlag, Sept. 2006.
36. A. Lysyanskaya and Z. Ramzan. Group blind digital signatures: A scalable solution to electronic cash. In R. Hirschfeld, editor, *Proceedings of Financial Cryptography 1998*, volume 1465 of *LNCS*, pages 184–97. Springer-Verlag, Feb. 1998.
37. A. Lysyanskaya, R. Rivest, A. Sahai, and S. Wolf. Pseudonym systems. In H. Heys and C. Adams, editors, *Proceedings of SAC 1999*, volume 1758 of *LNCS*, pages 184–99. Springer-Verlag, Aug. 1999.
38. G. Martinet, G. Poupard, and P. Sola. Cryptanalysis of a partially blind signature scheme, or How to make $100 bills with $1 and $2 ones. In G. D. Crescenzo and A. Rubin, editors, *Proceedings of Financial Cryptography 2006*, volume 4107 of *LNCS*, pages 171–76. Springer-Verlag, 2006.
39. 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. Cryptology ePrint Archive, Report 2010/474, 2010. `http://eprint.iacr.org/2010/474`.
40. T. Okamoto. Efficient blind and partially blind signatures without random oracles. Cryptology ePrint Archive, Report 2006/102, 2006. `http://eprint.iacr.org/`.
41. T. Okamoto. Efficient blind and partially blind signatures without random oracles. In S. Halevi and T. Rabin, editors, *Proceedings of TCC 2006*, volume 3876 of *LNCS*, pages 80–99. Springer-Verlag, Mar. 2006.
42. P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In J. Stern, editor, *Proceedings of Eurocrypt 1999*, volume 1592 of *LNCS*, pages 223–38. Springer-Verlag, May 1999.
43. K. Paterson and J. Schuldt. Efficient identity-based signatures secure in the standard model. In L. Batten and R. Safavi-Naini, editors, *Proceedings of ACISP 2006*, volume 4058 of *LNCS*, pages 207–22. Springer-Verlag, July 2006.
44. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *J. Cryptology*, 13(3):361–96, 2000.
45. H. Shacham. A Cramer-Shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive, Report 2007/074, 2007. `http://eprint.iacr.org/`.
46. B. Waters. Efficient identity-based encryption without random oracles. In R. Cramer, editor, *Proceedings of Eurocrypt 2005*, volume 3494 of *LNCS*, pages 114–27. Springer-Verlag, May 2005.
47. F. Zhang and K. Kim. ID-based blind signature and ring signature from pairings. In Y. Zheng, editor, *Proceedings of Asiacrypt 2002*, volume 2501 of *LNCS*, pages 533–47. Springer-Verlag, Dec. 2002.