# Extending Parameter Hiding in Prime Order Groups

Zaira Pindado*
Universitat Pompeu Fabra, Barcelona, Spain

## ABSTRACT

Many cryptographic protocols are designed in bilinear groups of order $N$, a large integer hard to factor. These groups have a lot of structure which can be exploited to prove security but they are not efficient. Thus, several works explore how to simulate the properties of composite order bilinear groups in the prime order setting. Wee (TCC, 2016) leaves as an open question to decide if a complex form of a property called parameter hiding is satisfied in the prime order setting. In this work, we give an algebraic characterization of this property and we discuss its implications.

**ACM Reference format:**
Zaira Pindado[1]. 2017. Extending Parameter Hiding in Prime Order Groups. In *Proceedings of womENcourage conference, UPC, Barcelona, September 2017,* 1 pages.
DOI: -

## 1 INTRODUCTION

A *bilinear group* is a tuple $(N, \mathbb{G}, g, \mathbb{G}_T, e)$ where $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order $N$ (written mutiplicatively), $g$ is a generator of $\mathbb{G}$, $e$ is a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, usually referred to as pairing operation and $e(g, g)$ is a generator of $\mathbb{G}_T$. From a cryptographic perspective, bilinear groups are interesting when the discrete logarithm problem is hard in $\mathbb{G}$ and $\mathbb{G}_T$. That is, given $(g, g^a)$ it is assumed that finding $a$ is a hard problem (when the group $\mathbb{G}$ is large enough).

Bilinear groups are extremely useful to design cryptographic protocols, specially if $N$ is a large integer which is hard to factor. In this case the group $\mathbb{G}$ has a richer structure which is hidden from an adversary not knowing the factorization of $N$. For instance, when $N$ is the product of two primes $N = p_1p_2$, there is a non-trivial subgroup $\mathbb{G}_i$ of order $p_i$ for $i = 1, 2$. It is not known how to distinguish if an element $t \in \mathbb{G}$ is in a subgroup $\mathbb{G}_i$ in polynomial time without the factors of $N$. This property is called *subgroup hiding*. Further, the two subgroups are "orthogonal" in the sense that if $g_i \in \mathbb{G}_i$, $i = 1, 2$, then $e(g_1, g_2) = 1_{\mathbb{G}_T}$.

Unfortunately, in practice operations in composite order bilinear groups are too inefficient. Thus, several papers have shown how to simulate this richer, useful structure when $N$ is a prime. For instance, in bilinear groups there is the well known Diffie-Hellman Assumption, which can be used to have a subgroup hiding assumption in $\mathbb{G} \times \mathbb{G}$.

However, it is still not known how to simulate all the interesting properties or how to systematically translate one protocol from composite to prime order bilinear groups. In this work we focus on a property called parameter hiding.

*Definition 1.1.* For a bilinear group $(N, \mathbb{G}, g, \mathbb{G}_T, e)$, $N = p_1p_2$, $p_i$ prime, let $\mathbb{G}_i$ be the subgroup of $\mathbb{G}$ of order $p_i$ and $g_i$ be its generator. Define $\mathcal{F} := \{f_w : \mathbb{Z}_N \to \mathbb{Z}_N, f_w(x) = \frac{1}{w+x}\}$. *Parameter hiding* holds with respect to $\mathcal{F}$ if when $w, v \leftarrow \mathbb{Z}_N$, $g_1^{f_w(x)}g_2^{f_w(x)}$ and $g_1^{f_w(x)}g_2^{f_v(x)}$ are identically distributed for all $x \in \mathbb{Z}_N$.

This property holds because, by the Chinese Remainder Theorem (CRT), $w \pmod{p_2}$ is independent of $w \pmod{p_1}$. In prime order groups we cannot apply the CRT.

## 2 RESULTS

The name parameter hiding (introduced by Lewko [2]) reflects the fact that $g_1^{\frac{1}{\alpha+x}}$ hides all information about the projection of this function in the other subgroup of $\mathbb{G}$, i.e. $g_2^{\frac{1}{\alpha+x}}$ and $g_1^{\frac{1}{\alpha+x}}$ are statistically independent. Wee uses this result in his security proof of a very efficient identity-based encryption (IBE) in composite order groups and he also proposes a translation of his IBE scheme in a prime order group but without security proof ([3]). Finding a proof would be extremely interesting (by a result of [1], it would imply the first efficient IBE scheme with tight security reduction with constant-size parameters under standard assumptions).

In prime order groups, the analogue of subgroup hiding says that given $(g^{\mathbf{B}}, g^{\vec{t}})$, it is hard to decide if $\vec{t} = \mathbf{B}\vec{r}$ or $\vec{t}$ is random in $\mathbb{G}^{k+1}$, for $\mathbf{B} \in \mathbb{Z}_p^{(k+1)\times(k+1)}$, $\vec{r} \in \mathbb{Z}_p^{k+1}$ and some $k$ depending on the security parameter[2]. Wee defines this natural analogue of parameter hiding and leaves open the question to see if it holds.

*Definition 2.1.* Let $p$ be a prime and $(p, \mathbb{G}, g, \mathbb{G}_T, e)$ a bilinear group. Define $\mathcal{F} := \{f_{\mathbf{W}} : \mathbb{Z}_p^{(k+1)\times(k+1)} \to \mathbb{Z}_p^{(k+1)\times(k+1)}, f_{\mathbf{W}}(x) = (\mathbf{W} + x\mathbf{I})^{-1}\}$. *Parameter hiding* holds with respect to $\mathcal{F}$ if, when $\mathbf{W}, \mathbf{V} \leftarrow \mathbb{Z}_p^{(k+1)\times(k+1)}$, the distribution $f_{\mathbf{W}}(x)\vec{t}_1 + f_{\mathbf{W}}(x)\vec{t}_2$ is identical to $f_{\mathbf{W}}(x)\vec{t}_1 + f_{\mathbf{V}}(x)\vec{t}_2$ for all $x \in \mathbb{Z}_p$, where $\mathbf{I}$ is the identity matrix, $\vec{t}_1 = \mathbf{B}\vec{r}$ and $\vec{t}_2 \leftarrow \mathbb{Z}_q^{k+1}$ (independent of $\mathbf{B}$).

We prove that this depends on the relative position of $\vec{t}_1$ with the eigenvectors of $\mathbf{W}$.

Theorem 2.2. *Let $t_1 \in \mathbb{Z}_p^{k+1}$. Let $\vec{d}_1, \ldots, \vec{d}_{k+1}$ the eigenvectors of a matrix $\mathbf{W} \in \mathbb{Z}_p^{(k+1)\times(k+1)}$ and let $\vec{r}$ the unique vector in $\mathbb{Z}_p^{k+1}$ such that $\vec{t}_1 = \sum_{i=1}^{k+1} r_i\vec{d}_i$. If $r_i \neq 0$ for all $i$, then $\{f_{\mathbf{W}}(x)\vec{t}_2 : x \in \mathbb{Z}_p\}$ can be uniquely determined from $\{f_{\mathbf{W}}(x)\vec{t}_1 : x \in \mathbb{Z}_p\}$ for all $\vec{t}_2 \in \mathbb{Z}_p^{k+1}$.*

Thus, we cannot obtain a straigthforward analogue of Def. 1.1 in prime order groups. The security proof of the IBE of Wee cannot be constructed using the same techniques as in the composite case.

## REFERENCES

[1] Jie Chen. 2016. Tightly Secure IBE under Constant-size Master Public Key. Cryptology ePrint Archive, Report 2016/891. (2016). http://eprint.iacr.org/2016/891.
[2] Allison B. Lewko. 2012. Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting. 318–335.
[3] Hoeteck Wee. 2016. Déjà Q: Encore! Un Petit IBE. 237–258. DOI: http://dx.doi.org/10.1007/978-3-662-49099-0_9

[1] Working jointly with Vanesa Daza, Carla Ràfols and Javier Silva of Universitat Pompeu Fabra, Barcelona, Spain.

[2] Exponentiation for vectors and matrices is defined componentwise.