# Oh Non! Quel Malheur! Standard Techniques Fail for the Prime-Order Petit IBE

No Author Given

No Institute Given

## 1 Introduction

Many cryptographic protocols are designed in bilinear groups of composite order $N$. The parameters are chosen such that $N$ is hard to factor. These groups have a lot of structure that can be exploited to prove security but arithmetic is not efficient. Thus, several works explore how to simulate the properties of composite-order bilinear groups in the prime-order setting. Wee (TCC, 2016) constructed an IBE scheme (the Petit IBE) in composite-order groups with very attractive features, namely: constant size public and secret keys, concrete efficiency (including short ciphertexts) and reduction to a constant-size assumption.

Wee proposed a candidate with the same features in prime-order groups, but he did not give a security proof. The main open question was, more concretely, to decide if a complex form of some property called parameter hiding is satisfied in the prime-order setting.

We give an overview of the known techniques for converting to prime-order groups in the specific case of Wee's Petit IBE, and answer the question of Wee by giving an algebraic characterization of when parameter hiding works. We finally dicuss why this indicates that constructing a proof of Wee's Petit IBE in prime-order groups requires substantially new ideas.

**Proof Techniques in Composite Order.** Security of Wee's Petit IBE is proven using the dual system technique of Waters [8] in composite order groups [6]. In such a technique, ciphertexts and keys can be either normal or semifunctional. A semifunctional ciphertext has an additional randomized component which is invisible when decryption is done with a normal key, but which prevents decryption with a semifunctional key. The dual system technique starts from a real game where all components are honestly generated, switches the challenge ciphertext to semifunctional and then, in a sequence of games, it progressively changes all the secret keys requested by the adversary to semifunctional. In the final game, both challenge ciphertext and keys are semifunctional and it is typically simple to argue security.

In Wee's Petit IBE, keys are turned to semifunctional in $q$ steps. Each of these is divided into a computational and an information-theoretic step. This technique is at the core of the Déjà Q framework of Chase and Meiklejohn [1] to reduce $q$-type assumptions to standard assumptions.

More in detail, Wee's Petit IBE is defined in a bilinear group of composite order $N = p_1p_2p_3$, the product of three primes. Let $(G, G_T, e, N)$,$e : \mathbb{G} \times G \to \mathbb{G}_T$ be a bilinear group of order $N$. Given $d|N$, let $\mathbb{G}_d$ be the subgroup of $\mathbb{G}$ of order $d$. For $i = 1, 2, 3$, let $g_i$ be a generator of $\mathbb{G}_{p_i}$. At a glance, Wee's Petit IBE is as follows[1]:

$$\begin{array}{ll} \mathsf{mpk} := g_1, g_1^{\alpha}, e(g_1, u), \mathsf{H} & u \leftarrow \mathbb{G}_{p_1}, \alpha \leftarrow \mathbb{Z}_N \\ \mathsf{sk}_{\mathsf{id}} := u^{\frac{1}{\alpha+\mathsf{id}}} R_3 & R_3 \leftarrow \mathbb{G}_{p_3} \\ \mathsf{ct}_{\mathsf{id}} := g_1^{(\alpha+\mathsf{id})s}, \kappa := \mathsf{H}(e(\mathsf{ct}, \mathsf{sk}_{\mathsf{id}})) & s \leftarrow \mathbb{Z}_p, \end{array}$$

where $\mathsf{H}$ is a hash function. Note that public parameters, secret keys and ciphertexts are all defined in $\mathbb{G}_{p_1}$, which is usually called the *functional space.* The group of order $p_3$, $\mathbb{G}_{p_3}$, serves to randomize the secret keys and $\mathbb{G}_{p_2}$ appears only in the security proof and is usually called the *semifunctional space.*

Given some values $r_1, \ldots, r_q$, we define the following function for $j = 1, \ldots, q$,

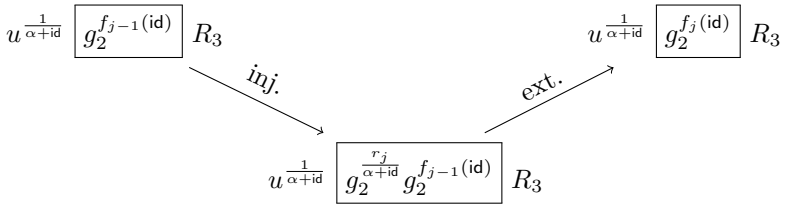
$$f_j(x) := \sum_{i=1}^{j} \frac{r_j}{\alpha_j + x} \mod p_2,$$

and $f_0(x) = 1$. Changing keys to semifunctional is done in $q$ steps, and at the $j$th step, $j = 0, \ldots, q$, secret keys have the following form:

$$\mathsf{sk}_{\mathsf{id}} := u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{f_j(\mathsf{id})} R_3$$

In the $q$th step, since $f_q(\mathsf{id})$ is a $q$-wise independent function, one can easily argue that the ciphertext is fully random even given the secret keys. To jump from $j$th to the $(j+1)$-step, one applies first a computational argument and then an information-theoretic argument, which, in terms of [3], are, respectively the entropy-injection and entropy-extraction part:

[1] We are following the exposition of Wee's proof in the composite order case as given by Chen *et al.* [3]




For the entropy injection step, one uses the subgroup decision assumption. Roughly speaking, given an element $T$ that is either $u \in \mathbb{G}_{p_1}$ or some $ug_2^{r_j} \in \mathbb{G}_{p_1p_2}$, one can define the secret keys as $T^{\frac{1}{\alpha+\mathsf{id}}} g_2^{f_{j-1}(\mathsf{id})} R_3$.

For the entropy-extraction part, the point is that, because of the Chinese remainder theorem, the only term in the secret keys which has information about $\alpha \mod p_2$ is $g_2^{\frac{r_j}{\alpha+\mathsf{id}}}$. Further, this term is completely independent of $u^{\frac{1}{\alpha+\mathsf{id}}}$, which depends only on $\alpha \mod p_1$, because $u \in \mathbb{G}_{p_1}$. Thus we can replace $\alpha$ by some independently chosen $\alpha_j$ such that $\alpha \equiv \alpha_j \mod p_2$ in $g_2^{\frac{r_j}{\alpha+\mathsf{id}}+f_{j-1}(\mathsf{id})}$, which results in $g_2^{\frac{r_j}{\alpha_j+\mathsf{id}}+f_{j-1}(\mathsf{id})} = g_2^{f_j(\mathsf{id})}$.

**A Candidate Prime Order IBE.** Wee [9] proposes the following translation to prime order groups of his Petit IBE. In the following, $[a]_\sigma$, $\sigma \in \{1, 2, T\}$ denotes $a\mathcal{P}_\sigma$, where for $\sigma = \{1, 2\}$, $\mathcal{P}_\sigma$ is a generator of $\mathbb{G}_\sigma$, $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a bilinear map and $\mathcal{P}_T = e(\mathcal{P}_1, \mathcal{P}_2)$.

$$\begin{array}{ll} \mathsf{mpk} := [\mathbf{A}]_1, [\mathbf{A}^\top \mathbf{W}]_1, [\mathbf{A}^\top \mathbf{B}]_T & \mathbf{A}, \mathbf{B} \leftarrow \mathcal{D}_k, \boldsymbol{u} \leftarrow \mathbb{Z}_p^k \\ \mathsf{sk}_{\mathsf{id}} := [(\mathbf{W} + \mathsf{id}\mathbf{I})^{-1} \mathbf{B}\boldsymbol{u}]_2 & \\ \mathsf{ct}_{\mathsf{id}} := [s^\top \mathbf{A}^\top (\mathbf{W} + \mathsf{id}\mathbf{I})]_1, \kappa := [\boldsymbol{s}^\top \mathbf{A}^\top \mathbf{B}\boldsymbol{u}] & s \leftarrow \mathbb{Z}_p, \end{array}$$

Here, the columns of $\mathbf{A}, \mathbf{B} \in \mathbb{Z}_p^{(k+1)\times k}$ are sampled from some distrbution $\mathcal{D}_k$ such that it is hard to decide membership in their image. In other words, this holds under the $\mathcal{D}_k$-Matrix Diffie Hellman assumption [4] in $\mathbb{G}_1$ and $\mathbb{G}_2$, which is a generalization of the $k$-Linear family [5,7]. The functional space, in this case, is the image of $\mathbf{A}$, $\mathbf{Im}(\mathbf{A}) \subset \mathbb{G}_1^{k+1}$ and $\mathbf{Im}(\mathbf{B}) \subset \mathbb{G}_2^{k+1}$. The semifunctional space, following an idea of [2], can be defined as $\boldsymbol{a}^\perp$ in $\mathbb{G}_2^{k+1}$ and as $\boldsymbol{b}^\perp$ in $\mathbb{G}_1^{k+1}$ (the orthogonal to $\mathbf{A}$ and $\mathbf{B}$, respectively). With this definition of semifunctional space, it is clear that honest ciphertexts decrypt correctly with semifunctional keys and viceversa.

Now, if one tries to prove security with the inject-extract idea of the Déjà Q, the "entropy-injection" part goes smoothly under the assumption that deciding membership in the image of $\mathbf{A}$ or $\mathbf{B}$ is hard (which is the natural analogue of subgroup hiding in prime order). Define $\mathbf{M}_{\mathsf{id}} := (\mathbf{W} + \mathsf{id}\mathbf{I})^{-1}$. More specifically, given a vector $[\boldsymbol{z}]_2 = [\mathbf{B}\boldsymbol{u} + v\boldsymbol{a}^\perp]_2$ in $\mathbb{G}_2^{k+1}$ which is either in the image of $\mathbf{B}$ ($v = 0$) or uniform in $\mathbb{G}_2^{k+1}$ ($v \leftarrow \mathbb{Z}_p$) , one defines the secret keys as:

$$(\mathbf{W} + x\mathbf{I})^{-1}[\boldsymbol{z}]_2 = [\mathbf{M}_{\mathsf{id}}\boldsymbol{z}]_2 = [\mathbf{M}_{\mathsf{id}}\mathbf{B}\boldsymbol{u} + v\mathbf{M}_{\mathsf{id}}\boldsymbol{a}^\perp]_2. \tag{1}$$

Now, for the entropy extraction part, following the parallel with the composite order case, the hope would be that $\mathbf{M}_{\mathsf{id}}\mathbf{B}\boldsymbol{u}$ and $\mathbf{M}_{\mathsf{id}}\boldsymbol{a}^\perp$ are somewhat independent, in terms of the information about $\mathbf{W}$ they leak. The ultimate goal would be to argue that Eq. 1 is identically distributed to:

$$(\mathbf{W} + x\mathbf{I})^{-1}\boldsymbol{z} = \mathbf{M}_{\mathsf{id}}\mathbf{B}\boldsymbol{u} + v\mathbf{M}'_{\mathsf{id}}\boldsymbol{a}^\perp.$$

where $\mathbf{M}'_{\mathsf{id}} := (\mathbf{W}' + \mathsf{id}\mathbf{I})^{-1}$, for some matrix $\mathbf{W}'$ in some specific relation with $\mathbf{W}$, whose definition would depend on the information leaked about $\mathbf{W}$ by $\mathbf{M}_{\mathsf{id}}\mathbf{B}\boldsymbol{u}$. The analogy with the composite order case is that there we argue that we can replace $\alpha$ by $\alpha'$ such that $\alpha \equiv \alpha' \mod p_2$ because only $\alpha \mod p_1$ is leaked by the functional part of the scheme. Here, we would replace $\mathbf{W}$ by some matrix $\mathbf{W}'$ which does not affect the functional part of the scheme. Wee [9] says that analyzing the information that the values $\mathbf{M}_{\mathsf{id}}\mathbf{B}\boldsymbol{u}$ leak is the main problem in finding a proof for his candidate prime order construction and observes that any diagonal matrix $\mathbf{W}$ is completely leaked, i.e. there is no natural analog of parameter hiding in prime-order groups for these matrices.

**An Algebraic Characterization of Parameter Hiding for Inverses.** To find a prime-order analog of the entropy-extraction part, our first step is to prove a series of algebraic properties of eigenspaces. We note that given a matrix $\mathbf{W} \in \mathbb{Z}_p^{n\times n}$ which is diagonalizable and with paiwise distinct eigenvalues $\alpha_1, \ldots, \alpha_n$, there exists a basis of eigenvalues of $\mathbf{W}$, $\mathbf{F}$, and a basis of eigenvalues of $\mathbf{W}^\top$, $\mathbf{D}$, such that $\mathbf{D}^\top\mathbf{F} = \mathbf{I}$. One can derive formulae[2] which express the ciphertexts and the secret keys of the candidate prime order scheme of Wee in terms of the eigenvalues and eigenvectors of $\mathbf{W}$. More specifically, for any vector $\boldsymbol{v} \in \mathbb{Z}_p^n$, if $\boldsymbol{r}, \boldsymbol{s}$ are such that $\boldsymbol{v} = \mathbf{D}\boldsymbol{s}$, $\boldsymbol{v} = \mathbf{F}\boldsymbol{r}$ then we prove:

$$\boldsymbol{v}^\top(\mathbf{W} + x\mathbf{I}) = \sum_{i=1}^{n}(\alpha_i + x\mathbf{I})s_i\boldsymbol{d}_i \qquad (\mathbf{W} + x\mathbf{I})^{-1}\boldsymbol{v} = \sum_{i=1}^{n}\frac{r_i}{\alpha_i + x}\boldsymbol{f}_i. \tag{2}$$

[2] Upon reviewer's request, we can provide more details and the proof of these claims.

With these formulae at hand, one can easily see that, if $\mathbf{B}$ and $\mathbf{W}$ are in general position, then the secret keys reveal $\mathbf{W}$ in an information-theoretic sense. In the candidate prime order construction, e.g. $\mathbf{B} \leftarrow \mathcal{D}_k$ and $\mathbf{W}$ is a uniform matrix. Indeed, because of the right-hand formula in (2), the secret keys are of the form:

$$\mathsf{sk}_{\mathsf{id}} := (\mathbf{W} + \mathsf{id}\mathbf{I})^{-1}\mathbf{B}\boldsymbol{u} = \sum_{i=1}^{k+1} \frac{r_i}{\alpha_j + \mathsf{id}} \boldsymbol{f}_i, \tag{3}$$

where $\boldsymbol{r} \in \mathbb{Z}_p^{k+1}$ is (the unique) vector such that $\mathbf{B}\boldsymbol{u} = \mathbf{F}\boldsymbol{r}$. If $\mathbf{B}$ and $\mathbf{W}$ are defined as in [9], i.e. they are chosen independently, with all but negligible probability $r_i \neq 0$ for all $i$, in which case, all of $\mathbf{W}$ can be recovered from $q$ secret keys $\mathsf{sk}_{\mathsf{id}}$ for different identities. On the other hand, it is obvious that if some $r_i = 0$, the secret keys hide the projection of $\boldsymbol{f}_i$. Thus, the right-hand side of (2) characterizes parameter hiding for the secret keys, while the left-hand side identifies how the information about $\mathbf{W}$ is leaked by the public parameters.

**Conclusion: Revisiting the Functional and Semifunctional Spaces.** This characterization of parameter hiding suggests a slightly different translation of the composite-order Petit IBE in the prime-order setting. In particular, it seems natural to define the functional subspace, which is $\mathbb{G}_{p_1}$ in the composite-order scheme, as a subspace of eigenvectors of $\mathbf{W}$. More in detail, as we mentioned, the natural candidates to the functional space in the respective side of the pairing are $\mathbf{Im}(\mathbf{A})$ on the left, and $\mathbf{Im}(\mathbf{B})$ on the right, which are $k$-dimensional spaces. In view of Equation (2), it would make sense to define:

$$\mathbf{Im}(\mathbf{A}) = \langle \boldsymbol{d}_1, \ldots, \boldsymbol{d}_k \rangle \qquad \mathbf{Im}(\mathbf{B}) = \langle \boldsymbol{f}_1, \ldots, \boldsymbol{f}_k \rangle,$$

where $\boldsymbol{d}_i$ (resp. $\boldsymbol{f}_i$) denote the first $k$ columns of $\mathbf{D}$ (resp. $\mathbf{F}$) and $\langle \cdot \rangle$ denotes the space spanned by some set of vectors. With this definition, $\mathbf{A}^\top$ is invariant with respect to multiplication on the right by $\mathbf{W}$. In particular, $\mathbf{A}^\top\mathbf{W}$ as included in the public parameters hides the eigenvalue $\alpha_{k+1}$. Since $\mathbf{Im}(\mathbf{B}) = \langle f_1, \ldots, f_k \rangle$, if $\mathbf{B} = \mathbf{F}\boldsymbol{r}$, $r_{k+1} = 0$ and the secret key also hides all information about the eigenvalue $\alpha_{k+1}$. Thus, in this case the semifunctional space can be defined as $\boldsymbol{d}_{k+1}$ on the left side of the pairing and $\boldsymbol{f}_{k+1}$ in the other. One would hope that the candidate prime-order IBE could be proven secure with this change in the joint distrribution of $\mathbf{A}, \mathbf{B}, \mathbf{W}$.

However, when proving the security of this adaptation of the prime-order Petit IBE, we run into a fundamental difficulty. Namely, in the reduction, if we know the matrix $\mathbf{W}$ we know its decomposition in eigenvectors and thus we do not know how to combine this with decisional assumptions in $\mathbf{A}, \mathbf{B}$. This is a fundamental difference with the composite-order case, where we have hard problems (difficulty of factoring) also "in the exponent". More specifically, if the reduction controls $\mathbf{W}$ in the field $\mathbb{Z}_p$, it can always tell if a vector is in the space generated by $\mathbf{B}$, because it can always distinguish vectors which are in the space generated by only $k$ eigenvectors or by $k+1$ eigenvectors. For instance, if $[\boldsymbol{z}]_2$ is a vector in $\mathbb{G}_2^{k+2}$, the reduction can compute some basis of eigenvectors $\tilde{\mathbf{F}}$ and compute $\tilde{\mathbf{F}}^{-1}[\boldsymbol{z}]_2$. The result is a vector $[\boldsymbol{r}]_2$ such that $\tilde{\mathbf{F}}\boldsymbol{r} = \boldsymbol{z}$ and the reduction just needs to see if some coordinate of $[\boldsymbol{r}]_2$ is $[\mathbf{0}]_2$.

On the other hand, it is also far from clear how to build a reduction without letting the challenger choose $\mathbf{W}$. The problem in this case is to answer secret key queries (in fact, this is precisely the point why, before the Déjà Q framework, one had to resort to $q$-type assumptions).

In summary, our opinion is that fundamentally new ideas are necessary to prove the Petit IBE of Wee in prime-order groups.

## References


1. M. Chase and S. Meiklejohn. Déjà Q: Using dual systems to revisit q-type assumptions. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 622–639, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany. 1
2. J. Chen, R. Gay, and H. Wee. Improved dual system ABE in prime-order groups via predicate encodings. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 595–624, Sofia, Bulgaria, Apr. 26–30, 2015. Springer, Heidelberg, Germany. 2
3. J. Chen, J. Gong, and J. Weng. Tightly secure IBE under constant-size master public key. LNCS, pages 207–231, Amsterdam, The Netherlands, Mar. 28–31, 2017. Springer, Heidelberg, Germany. 1
4. A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie-Hellman assumptions. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147, Santa Barbara, CA, USA, Aug. 18–22, 2013. Springer, Heidelberg, Germany. 2
5. D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. In A. Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 553–571, Santa Barbara, CA, USA, Aug. 19–23, 2007. Springer, Heidelberg, Germany. 2
6. A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In D. Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 455–479, Zurich, Switzerland, Feb. 9–11, 2010. Springer, Heidelberg, Germany. 1
7. 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/2007/074`. 2
8. B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In S. Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636, Santa Barbara, CA, USA, Aug. 16–20, 2009. Springer, Heidelberg, Germany. 1
9. H. Wee. Déjà Q: Encore! Un petit IBE. In E. Kushilevitz and T. Malkin, editors, *TCC 2016-A, Part II*, volume 9563 of *LNCS*, pages 237–258, Tel Aviv, Israel, Jan. 10–13, 2016. Springer, Heidelberg, Germany. 2, 3