Composite Order Bilinear Pairing on Elliptic Curve for Dual System Encryption

Fatin Nabila Abd Latiff\textsuperscript{a} and Wan Ainun Mior Othman\textsuperscript{b}

\textit{a} Institute of Mathematical Sciences, Faculty of Science University of Malaya, 50603 Kuala Lumpur, Malaysia
\texttt{fatin_nabilaa@yahoo.com}

\textit{b} Institute of Mathematical Sciences, Faculty of Science University of Malaya, 50603 Kuala Lumpur, Malaysia
\texttt{wanainun@um.edu.my}

Abstract. In this paper, we explore the pairing-based cryptography on elliptic curve. The security of protocols using composite order bilinear pairing on elliptic curve depends on the difficulty of factoring the number $N$. Here, we show how to construct composite ordinary pairing-friendly elliptic curve having the subgroup of composite order $N$ by using Cocks-Pinch Method. We also introduce dual system encryption to transform Identity-Based Encryption (IBE) scheme built over prime-order bilinear, to composite order bilinear groups. The new Identity-Based Encryption (IBE) is secured since it uses the Dual System Encryption methodology which guaranteed full security of the new IBE system.

Keywords: Composite order; bilinear pairing; Cocks-Pinch method; dual system encryption; identity-based encryption.

PACS: 03.67.Dd

INTRODUCTION

Pairing-based cryptography is the operation of a pairing between the elements of two cryptographic groups to a third group to construct cryptographic systems. If the same group is used for the first two groups, the pairing is called symmetric and is a mapping from two elements of one group to an element from a second group. Like this, pairings can be used to reduce an unbreakable problem in one group to a different, generally easier problem in another group. For example, in groups with a bilinear mapping such as the Weil pairing or Tate pairing, generalizations of the computational Diffie–Hellman problem are supposed to be infeasible while the easier decisional Diffie–Hellman problem can be easily solved using the pairing function.

Recently, Boneh [1] introduced a new idea in pairing-based cryptography, which is to use composite order groups instead of prime order ones. It has been used in most of important applications including non-interactive zero-knowledge proofs, group and ring signatures, searching encrypted data, and fully collusion-resistant tracing.

If we want to construct pairing-based schemes with composite order groups, we can either apply the pairing using supersingular curves as in the original construction in [1] or use ordinary curves as proposed in [2]. These are particularly recommended if the security relies on the Decisional Diffie-Hellman (DDH) assumption. Recent results show that the discrete logarithm problem on supersingular curves is weak. The reason for constructing pairing-friendly ordinary curve is because recent announcements [3] show that pairings of supersingular curves as defined in [4] are no longer safe.

In this paper we show the construction of composite ordinary pairing-friendly elliptic curve using ordinary curve and use it as a method to transform Identity Based Encryption (IBE) to composite order bilinear groups. The dual system encryption methodology introduced by Waters [5] is a tool for proving full security of Identity-Based Encryption (IBE) and related encryption systems. We apply Dual System Encryption methodology to prove the security of our newly transformed IBE system.

COMPOSITE ORDER BILINEAR GROUP

In this section we discuss the construction of composite ordinary pairing friendly elliptic curve.
Background

Composite order bilinear groups were first introduced in [1]. We define them by using a group generator $G$, an algorithm which takes a security parameter $\lambda$ as input and outputs a description of a bilinear group $G$. We let $G_1, G_2$ and $G_T$ be finite cyclic groups. The order of these three groups is composite integer $N$ with some large prime factors $p_1, p_2, \ldots, p_n$. In our case, $G$ outputs $(N = p_1 p_2 p_3, G, G_T, e)$ where $p_1, p_2, p_3$ are distinct primes, $G$ and $G_T$ are cyclic groups of order $N = p_1 p_2 p_3$, and $e: G^2 \to G_T$ is a map such that:

1. (Bilinear) $\forall g, h \in G; a, b \in \mathbb{Z}_N, e(g^a, h^b) = e(g, h)^{ab}$
2. (Non-degenerate) $\exists g \in G$ such that $e(g, g)$ has order $N$ in $G_T$

We further require that the group operations in $G$ and $G_T$ as well as the bilinear map $e$ are computable in polynomial time with respect to $\lambda$. Also, we assume the group descriptions of $G$ and $G_T$ include generators of the respective cyclic groups. We let $G_{p_1}, G_{p_2}$, and $G_{p_3}$ denote the subgroups of order $p_1, p_2$, and $p_3$ in $G$ respectively.

We note that when $h_i \in G_{p_1}$ and $h_j \in G_{p_j}$ for $i \neq j$, $e(h_i, h_j)$ is the identity element in $G_T$. To see this, suppose $h_1 \in G_{p_1}$ and $h_2 \in G_{p_2}$. We let $g$ denote a generator of $G$. Then, $g^{p_1}p_2$ generates $G_{p_3}$, $g^{p_1}p_3$ generates $G_{p_2}$, and $g^{p_2}p_3$ generates $G_{p_1}$. Hence, for some $\alpha_1, \alpha_2, h_1 = (g^{p_1}p_1)^{\alpha_1}$ and $h_2 = (g^{p_1}p_3)^{\alpha_2}$. We note:

$$e(h_1, h_2) = e(g^{p_1}p_1^{\alpha_1}, g^{p_1}p_3^{\alpha_2}) = e(g^{\alpha_1}, g^{p_1}p_3^{\alpha_2})^{p_1p_3} = 1$$

(1)

This orthogonality property of $G_{p_1}, G_{p_2}, G_{p_3}$ will be a principal tool in our constructions.

Cocks-Pinch Method

We use the Cocks-Pinch algorithm for finding pairing-friendly elliptic curves [6] and the Complex Multiplication (CM) method of curve construction [8].

**Input:**
- A positive integer $k$;
- $k$ will be the embedding degree,
- A prime $p$ congruent to 1 modulo $k$.

**Output:**
- A prime $q$;
- An elliptic curve $E$ over $\mathbb{F}_q$ of embedding degree $k$ with respect to $p$.

Step 1: Choose an integer $X$ that has order $k$ in $(\mathbb{Z}/p\mathbb{Z})^\times$

Step 2: Choose a positive integer $D$ (the CM discriminant) so that $-D$ is a square modulo $p$.

Step 3: Fix $s \pmod{p}$ such that $s^2 \equiv -D \pmod{p}$.

Step 4: Take an integer $Y$ congruent to $\pm (X - 1)s^{-1} \pmod{p}$.

Step 5: Let $q = ((X + 1)^2 + DY^2)/4$.

Step 6: If $q$ is a prime number, use the CM method to obtain an elliptic curve $E$ over $\mathbb{F}_q$ with trace $t = X + 1$.

So

$$|E(\mathbb{F}_q)| = q + 1 - t = q - X$$

(2)

Since $q \equiv X \pmod{p}$, the group order $|E(\mathbb{F}_q)|$ is divisible by $p$, and $k$ is the embedding degree for $E$ over $\mathbb{F}_q$ with respect to $p$.

If $q$ is not a prime number, start again with a different $X$ and/or $Y$.  

020027-2
Recall that for the CM method [7], the input is a prime \( q \) of the form \( 422 D_{ba} \), and the output is an elliptic curve \( E \) over \( \mathbb{F}_q \) with \( |E(F_q)| = q + 1 - a \).

They also construct composite order groups with embedding degree 1 [8], and from the construction no information about \( N \)'s factorization is leaked, since knowledge of \( N \)'s factors was not used.

We generalize the Cocks-Pinch method to the case where \( p \) is replaced by a composite \( N \). In this version the restrictions are on the input \( k \) and on \( D \) (in Step 2).

**Input:**
- A positive integer \( k \) such that either \( 4|k \) or \( k \) has a prime divisor that is congruent to 3 modulo 4,
- Distinct primes \( p_1, \ldots, p_r \) congruent to 1 modulo \( k \), and
- Positive integers \( \alpha_1, \ldots, \alpha_r \).
- Let \( N = \prod_{i=1}^r p_i^{\alpha_i} \)

**Output:**
- A prime \( q \);
- An elliptic curve \( E \) over \( \mathbb{F}_q \) of embedding degree \( k \) with respect to \( N \).

**Step 1:** Choose an integer \( X \) that has order \( k \) in \( \left( \mathbb{Z} / p_i^{\alpha_i} \mathbb{Z} \right)^* \) for all \( i \).

**Step 2:** Choose a positive square-free divisor \( D \) of \( k \) such that if \( k \) is a multiple of 4 then \( D \) divides \( k / 4 \), while if \( k \) is not a multiple of 4 then \( D \equiv 3 \pmod{4} \).

**Step 3:** With \( \left( \frac{-D}{a} \right) \) denoting the Jacobi symbol, let

\[
S = \sum_{a=1}^{2D-1} \left( \frac{-D}{a} \right)^{ak \pmod{N}} \frac{q}{D^{a \pmod{N}}} \Rightarrow X \pmod{4}
\]

\[
S = \begin{cases} 
\frac{1}{2} \sum_{a=1}^{4D-1} \left( \frac{-D}{a} \right)^{ak \pmod{N}} \text{if } D \equiv 3 \pmod{4} \\
\sum_{a=1}^{2D-1} \left( \frac{-D}{a} \right)^{ak \pmod{N}} \text{otherwise}
\end{cases}
\]

**Step 4:** Take an integer \( Y \) congruent to \( \pm (X-1)^r \pmod{N} \).

**Step 5:** Let \( q = ((X+1)^2 + DY^2) / 4 \in \mathbb{Q} \).

**Step 6:** If \( q \) is a prime number, use the CM method to obtain an elliptic curve \( E \) over \( \mathbb{F}_q \) with trace \( t = X + 1 \),

\[
|E(F_q)| = q + 1 - t = q - X
\]

If \( q \) is not a prime number, start again with a different \( X \) and/or \( Y \).

In version 1, \( p \) is replaced by a composite \( N \) and \( N \) is a product of primes that are 1 (mod \( k \)) is leaked in this construction. The square root \( s \) of \( -D \pmod{N} \) is revealed from \( q \), \( N \), and \( E \). While in version 2, the difference are only in steps 2 and 3. The method of computing a square root \( s \) of \( -D \pmod{N} \) in this version does not leak additional information about the factorization of \( N \) that was not already leaked by knowledge of \( X \). Therefore we use the second version of the algorithm, rather than the first.

**IDENTITY BASED ENCRYPTION**

In this section, we transform Identity Based Encryption (IBE) to composite order bilinear groups. Then we apply Dual System Encryption methodology to prove security of our newly transformed IBE system.
Background

The concept of Identity-Based Encryption (IBE) was first proposed by Shamir [9] and later constructed by Boneh and Franklin [2] and Cocks [10]. In an identity-based encryption scheme, users are associated with identities and obtain secret keys from a master authority. Encryption to any identity can be done knowing only the identity and some global public parameters. Both of the initial constructions of IBE were proven secure in the random oracle model.

An Identity-Based Encryption (IBE) scheme consists of four algorithms: Setup, Encrypt, KeyGen, and Decrypt.

- **Setup.** The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters and a master secret key MSK.

- **Key Generation (MSK, I).** The key generation algorithm takes as input the master secret key MSK and an identity I. It outputs a private key SK.

- **Encrypt (PK, M, I).** The encryption algorithm takes as input the public parameters PK, a message M, and an identity I. The algorithm outputs a ciphertext CT.

- **Decrypt (PK, CT, SK).** The decryption algorithm takes as input the public parameters PK, a ciphertext CT, and a secret key. If the ciphertext was an encryption to I and the secret key was the output of a key generation for the same identity then the algorithm will output the encrypted message M.

IBE Construction

We use the ordinary composite order group version II in this IBE system. The construction will use composite order groups of order \( p_1p_2p_3 \) and identities in \( \mathbb{Z}_N \).

- **Setup.** The setup algorithm chooses a bilinear group \( G \) of order \( N = p_1p_2p_3 \) (where \( p_1, p_2, \) and \( p_3 \) are distinct primes). We let \( G_{p_i} \) denote the subgroup of order \( p_i \) in \( G \). It then chooses \( u, g, h \in G_{p_3} \) and \( \alpha \in \mathbb{Z}_N \). The public parameters are published as:

\[
PK = \{N, u, g, h, e(g, g)^\theta\}
\]

The secret parameters are \( \alpha \) and a generator of \( G_{p_3} \).

- **KeyGen. (ID, MSK)** The key generation algorithm chooses \( r \in \mathbb{Z}_N \) and \( R_3, R'_3 \in G_{p_3} \) randomly. (Random elements of \( G_{p_3} \) can be obtained by taking a generator of \( G_{p_3} \) and raising it to random exponents modulo \( N \).) The key is formed as:

\[
K_1 = g^rR_3, \quad K_2 = g^\alpha(u^{ID}h)^rR'_3
\]

Then secret key is computed as

\[
SK_{ID} = (K_1, K_2) = (g^rR_3, g^\alpha(u^{ID}h)^rR'_3)
\]

- **Encrypt. (M, ID)** The encryption algorithm chooses \( s \in \mathbb{Z}_N \) randomly and creates the ciphertext as:

\[
C_0 = M_p(g; g)^{as}, \quad C_1 = (u^{ID}h)^s, \quad C_2 = g_s
\]

The ciphertext is then generated as

\[
CT = (C_0, C_1, C_2) = (M_p(g; g)^{as}, (u^{ID}h)^s, g_s)
\]

- **Decryption.** If the ID's of the ciphertext and key are equal, the decryption algorithm computes the plaintext as:
The security of our newly transformed Identity-Based Encryption (IBE) is proved to be secured since it is applicable to the Dual System Encryption that was introduced by Waters [6].

CONCLUSION

We constructed composite order bilinear group in elliptic curve and used the method to transform our IBE system to composite order bilinear group. Our newly transformed IBE system has a convenient setting for Dual System Encryption methodology that guaranteed its full security. For future work, we would like to improve on the construction of composite order pairing and to study the security and efficiency of Identity-Based Encryption (IBE) as a result of the new improved construction.

ACKNOWLEDGMENTS

The authors would like to thank the referee for careful reading and useful comments. This paper is supported by UMRG 270-13AFR.

REFERENCES


