Copyright © 2005 IEEE

Reprinted from:

2005 3rd IEEE International Conference on Industrial Informatics (INDIN) Perth, Australia 10-12 August 2005

IEEE Catalog Number ISBN 05EX1057
ISBN 0-7803-9094-6

This material is posted here with permission of the IEEE. Such permission of the IEEE does not in any way imply IEEE endorsement of any of Curtin University of Technology's products or services. Internal or personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution must be obtained from the IEEE by writing to pubs-permissions@ieee.org.

By choosing to view this document, you agree to all provisions of the copyright laws protecting it.

A New Encryption Algorithm over Elliptic Curve

S. Han
School of Information Systems
Curtin University of Technology

E. Chang
School of Information Systems
Curtin University of Technology

W. Liu
Department of Computing
Curtin University of Technology

J. Wang
National Natural Foundation of China
Beijing, China

V. Potdar
School of Information Systems
Curtin University of Technology

Abstract— **Various public key encryption systems have been proposed in modern information techology. Some of them have also been used in various applications, such as E-commerce and mobile database. This paper proposes two secure receiptor-oriented encryption systems. The decryptioner's private keys could be changed with the different time periods. This case would be very useful in some practical scenarios, for instance, in a mobile database environment. Besides the semantic security, the proposed schemes have the backward-and-future security, a new security requirement for semantically secure encryption schemes. In terms of construction, the two schemes are based on the pairings over elliptic curves. Also, this paper provides a heuristic security analysis for the underlying system.**

I. Introduction

Various public key encryption systems have been proposed in modern information techology. Some of them have also been used in various applications, such as E-commerce and mobile database. Semantic security is one of the security requirements for a secure cryptosystem. Generally speaking, semantic security means that: the view of the ciphertext gives no additional information about the plaintext. Galindo et al proposed these two schemes [1], [2] in 2003, which are based on elliptic curves. Both of them present semantic security. And they only use the single coordinate of any point over elliptic curves. In contrast to the two schemes, our new schemes use the whole point on the elliptic curves and bilinear pairings to take part in calculations. In addition, our semantically secure encryption scheme is a new type of cryptosystems, since it provides a new security requirement, i.e. backward-and-future security.

Bilinear pairings modified from Weil or Tate pairings [3] are becoming one of new active research topics in information security. Especially, the supersingular curves are the main object used by the bilinear pairings. However, prior to [2], [4], [9], the supersingular curves were undesirable in cryptographic settings since Weil pairing can reduce the discrete logarithm problems in supersingular curves to that in an extension of the underlying finite field. Thanks to Joux [4] and Boneh et al [2], the pairings have become desirable and applied to various cryptographic primitives: public key encryption [2], digital signature [5], key agreement [4]; and signcryptions [6]. In our paper, we propose several new public key encryption schemes different from [2]. And the new constructions are motivated by some techniques from [7], [1], [9].

The main contributions of our paper are:

- A new type of semantically secure public key encryption schemes are proposed in this paper. That is, it combines the encryptioner's both public key and private keys with the decryptioner's public keys in encryption algorithms.
- The backward-and-future security is introduced into the semantic secure cyrptosytems. Since in some cases, one part of private keys may be compromised by some attackers, so backward-and-future security will solve these circumstances.
- Various semantically secure encryption schemes are proposed over elliptic curves, which are based on Pairings. And this will provide more choices in public key cryptosystems.

The organization of the rest of our paper is as follows: Section 2 introduces the definition of receiptor-oriented encryption scheme and the corresponding requirements on the receiptor-oriented encryption schemes. Section 3 presents some preliminaries for the new proposed schemes. The constructions on the new cryptosystems are presented in section 4. The security analysis and the efficiency analysis stay in section 5 and section 6, respectively. And section 7 concludes this paper.

II. Definitions of Receiptor-Oriented Encryptions

In this section, the model of the receiptor-oriented encryption scheme is presented as follows.

Definition 1 (Receiptor-Oriented Encryptions) A *receiptor-oriented encryption* (abbr. *ROE*) scheme is a public key cryptosystem comprised of the following three procedures, and in which two entities (encryptioner and decryptioner) are involved:

(1) ***Key Generation:*** On input a security parameter ℓ, this probabilistic algorithm returns the long-term public keys and private keys for the encriptioner (pk_2, sk_2) and the decriptioner (pk_1, sk_1), respectively. Simultaneously, this algorithm also outputs a pair of specified time-stage(t_i) public key pk_{t_i} and private key sk_{t_i} for the oriented receiptor, i.e. the decryptioner. The initialized time-stage is t_0. Therefore, the initial time-stage public key and private key for the

0-7803-9094-6/05/$20.00 ©2005 IEEE

decryptioner are pk_{t_0} and sk_{t_0}, respectively.

(2) ***Encryption:*** This is a probabilistic algorithm carried by the encryptioner. Given a plaintext m, the encryptioner will encrypt m by use of its own long-term public key pk_2 and private key sk_2. During the encrypting, the encryptioner will also use the oriented receiptor's (i.e. decryptioner's) specified time-stage public key pk_{t_i} and long-term public key pk_1. In addition, some random elements chosen by the encryptioner will be involved. In the end, the encryptioner publishes the ciphertext C (of plaintext m) on its homepage. Furthermore, its homepage will be renewed in time.

(4) ***Decryption:*** This is an algorithm done by the decryptioner. The algorithm inputs the ciphertext C, the decryptioner's long-term public key pk_1 and private key sk_1, its specified time-stage public key pk_{t_i} and private key sk_{t_i}, as well as the encryptioner's public key pk_2. In the end, the plaintext m will be returned.

Definition 2 (Requirements of a Secure ROE Scheme) A *secure receiptor oriented public key encryption* scheme must satisfy at least the following three requirements.

(1) **Soundness**: For any plaintext $m \in M$ (M is the plaintext space), and for any given time stage t_i, there always holds that:

$$D_{pk_1,pk_2,sk_1,sk_{t_i},pk_{t_i}}(E_{pk_1,pk_2,sk_2,pk_{t_i}}(m,r)) = m \qquad (1)$$

where E and D are the encryption and the decryption algorithms respectively; r is a random element chosen by the encryptioner; pk_1, pk_{t_i}, and sk_1, sk_{t_i} are the decryptioner's public keys and private keys respectively; pk_2 and sk_2 are the encryptioner's public and private keys.

(2) **Semantic Security**: For any $m \in M$(M is the plaintext space), for any polynomial time attacker **A**, who can input the public keys of the encryptioner and decryptioner, cannot distinguish the ciphertext c(of plaintext m) from a random element $\phi \in_R C$ (C is the ciphertext space) in polynomial time.

(3) **Backward-and-future Security**: This property is with respect to the oriented receiptor while its specified time-stage private sk_{t_i} is compromised by an attcker **A**. Backward-and-future security means that even though attacker **A** obtains the time-stage private sk_{t_i} for the time stage t_i, **A** is still not able to do the followings:

- figure out the plaintext of any ciphertext c encrypted during time-stage t_i.
- derive the former time-stage t_{i-1}'s private key $sk_{t_{i-1}}$ from sk_{t_i}.
- calculate the latter time-stage t_{i+1}'s private key $sk_{t_{i+1}}$ from sk_{t_i}.

III. Preliminaries

In this paper, we choose ℓ as the security parameter for all the proposed receiptor-oriented encryption schemes. Let q be a large prime, and Z_q^* be $Z_q \backslash \{0\}$. F_q denotes a finite field with q elements. $\bigoplus$ denotes the bit-wise *XOR* calculation. Let n be a positive integer with $n = \bigcirc(\ell)$. Let H_1 and H_2 be two cryptographic hash functions: $H_1 : G_2 \to \{0,1\}^n$, and $H_2 : G_1 \times G_1 \to Z_q^*$; where H_1 is a universal one-way hash function [8]. G_1 and G_2 will be given later.

Definition 3 Let $p > 3$ be a prime. An elliptic curve over the the finite field F_p, denoted by $E_p(a,b)$ or $E(a,b)/F_p$, where $a, b \in F_p$, and $gcd(4a^3 + 27b^2) = 1$, is the set of points $P_{(x,y)}$ such that $y^2 = (x^3 + ax + b)$mod p, together with a point Ô, called the point at infinity.

In our paper, we choose elliptic curves $E(a,b)/F_p$ with $y^2 = (x^3 + ax + b)$mod p such that:

- $a = 0$; b is some random integer with gcd$(27b^2, p) = 1$. For simplicity, b may be equal 1.
- $p \equiv 2$mod 3. In this case, the order of $E(0,b)/F_p$(the number of it) is $|E(0,b)/F_p| = p + 1$, and thus avoiding the difficulty of computing $|E(a,b)/F_p|$.
- the bit length of p is ℓ; and ℓ may be equal to or larger than 160 for security reason.

IV. Receiptor-Oriented Encryption Schemes

In this section, we will propose two receiptor-oriented encryption schemes. Both of these schemes are constructed over elliptic curves described in section 3.1. And we develop the constructions motivated by some techniques from [9], [1], [7]. In detail, we will propose two non-identity receiptor-oriented encryption schemes. That is, we will only use the elliptic curve settings to construct the ROE schemes. This kind of ROE schemes does not involve the fully contracted obsession, i.e. there needs no key generation centre.

A. non-Identity based ROE Scheme 1

By the definition of the ROE scheme, the non-identity based receiptor-oriented encryption scheme 1 has still three algorithms:

(1) **Key Generation** This is a polynomially probabilistic algorithm, which first obtains an elliptic curve $E((o,1)/F_p$ constructed as in section 3. All other system parameters are the same as what are in section 3, including p, q, G_1, G_2, $e(*,*)$, and a generator $P \in G_1$. At the end of this algorithm, it returns two pairs of long-term public keys and private keys respectively for the encryptioner and the decryptioner. The encryptioner's long-term public key is $uP \in G_1$, and private key is $u \in Z_q^*$. And the decryptioner's long-term public key is $sP \in G_1$, and private key is $s \in Z_q^*$. In addition, the decryptioner will have a pair of specified time-stage public key $vP \in G_1$ and private key $v \in Z_q^*$ according to the definition of ROE scheme.

(2) **Encryption** This is a polynomially probabilistic algorithm, which inputs a plaintext $m \in M$ and outputs its corresponding ciphertext.

- the encryptioner chooses uniformly and randomly an element $r \in Z_q^*$, and computes $f_1 = rP$.
- the encryptioner then computes

  $$f_2 = e(vP + H_2(vP, sP)sP, c_1 + H_2(c_1, uP)uP)^{u+H_2(vP,c_1)r} \text{mod}$$

  and $f_3 = H_1(f_2)$, respectively.
- At the last step, he computes $f_4 = f_3 \oplus m$.

Then, he publishes the ciphertext $\{f_1, f_4\}$.

(3) **Decryption** This is a deterministic algorithm, apart from ciphertexts, which inputs the decryptioner's public key and private key, as well as her specified time-stage public and private key. In addition, the encryptioner's public key will also be inputted.

- the decryptioner first calculates

$$d_1 = e(c_1+H_2(c_1, uP)uP, uP+H_2(vP, c_1)c_1)^{v+H_2(vP,sP)s} \mathrm{mod}\ q$$

- she calculates $d_2 = H_1(d_1)$.
- she recovers the corresponding plaintext m by $m = d_2 \oplus f_4$. If the ciphertext $\{f_1, f_4\}$ is invalid, then she will output nothing $\sqcup$.

In the above scheme, there are one pairing evaluation and an modular exponentiation in both encryption and decryption algorithms.

B. Non-ID-based ROE Scheme 2

The non-identity based ROE scheme 2 has the following three algorithms: Key generation, Encryption, and Decryption algorithms.

(1) **Key Generation** This is a polynomiallly probabilistic algorithm, which returns the domain parameters: a security parameter ℓ ; two groups G_1 and G_2 with the same order q, and the former is an additive group, and the latter is a multiplicative group; a bilinear pairing $e(*,*) : G_1 \times G_1 \to G_2$; a generator $P \in G_1$, and therefore $e(P, P) \in G_2$ is a generator of G_2; a universal collision-free one-way hash function $H_1(\cdot) : G_2 \to \{0,1\}^n$, where $n = \bigcirc(\ell)$. At the end of this algorithm, the encryptioner obtains his long-term public key $\beta P \in G_1$ and private key $\beta \in Z_q^*$; Besides obtaining her long-term public key $\alpha P \in G_1$ and private key $\alpha \in Z_q^*$, the decryptioner also obtains a pair of specified time-stage public key $\rho P \in G_1$ and private key $\rho \in Z_q^*$, respectively.

(2) **Encryption** This algorithm is dealt with by the encryptioner in probabilistic polynomial time. For any plaintext $m \in M = \{0,1\}^n$, the following procedures will be done:

- the encryptioner first chooses uniformly and randomly an elelment $r \in Z_q^*$, and calculates $f_1 = rP \in G_1$.
- he then calculates by use of pairing $e(*,*)$ $f_2 = e(\alpha P, f_1)^\beta e(\beta P, \rho P)^r$, and as well $f_3 = H_1(f_2)$.
- In the end, he returns the corresponding ciphertext $\langle f_1, f_4\rangle$ by $f_4 = m \oplus f_3$.

(3) **Decryption** This is a deterministic algorithm carried out by the decryptioner (i.e. the oriented receiptor). Given a ciphtext $\langle f_1, f_4\rangle$, she will do.

- the decryptioner first calculates an elelment $d_1 = e(f_1, \beta P)^\alpha e(\beta P, f_1)^\rho \in G_2$, and $d_2 = H_1(d_1) \in \{0,1\}^n$.
- she recovers the corresponding plaintext m by $m = d_2 \oplus f_4$.

Remark: In the above two non-identity based receiptor-oriented encryption schemes, the encryptioner and the decryptoiner may make use of some key distribution technique [9], and commitment technique [?], [?], and Schnnor authentication scheme to manage their own public key and private key, respectively.

V. Security Analysis

In this section, we will deal with some security analyses on these ROE schemes by the definition of receiptor-oriented encryption scheme. We will prove that the two non-identity based schemes both have the soundness, semantic security, and backward-and-future security.

A. Soundness

The soundness of the receiptor-oriented encryption schemes is that: if the encryptioner correctly calculates the ciphertexts according to the descriptions of encryption algorithm, and if the decryptioner correctly carries on the decryption algorithm, then the latter will surely recover the corresponding plaintexts.

Theorem 1 The two non-identity based receiptor-oriented encryption schemes in section 4 both have the soundness. In other words, if $\{f_1, f_4\}$ is a legal ciphertext returned by the encryptioner on plaintext $m \in \{0,1\}^n$, then the decryptioner will surely recover the plaintext $m \in \{0,1\}^n$ such that

$$D_{uP,u,sP,vP,P}(E_{uP,sP,s,sP,P}(m, r)) = m \qquad (2)$$

where E and D are the encryption and the decryption algorithms respectively; r is a random element chosen by the encryptioner; and other data are the same to what in the two non-identity based ROE schemes in section 4.

Proof. Because of the similar proofs on the two ROE schemes, we only present the theorem proof for the non-identity based ROE scheme 1.

By the encryption algorithm of the identity-based ROE scheme 1, we can write

$f_1 = rP$;

$f_2 = e(vP + H_2(vP, sP)sP, f_1 + H_2(f_1, uP)uP)^{u+H_2(vP,f_1)r} \mathrm{mod}\ q$;

$f_3 = H(f_2)$;

$f_4 = f_3 \oplus m$.

where $r \in Z_q^*$ is a random element.

Since $d_1 = e(c_1 + H_2(f_1, uP)uP, uP + H_2(vP, f_1)f_1)^{v+H_2(vP,sP)s} \mathrm{mod}\ q$, and by the key generation algorithm, therefore

$$\begin{aligned} d_1 &= e(f_1 + H_2(f_1, uP)uP, uP)^{v+H_2(vP,sP)s} \times e(f_1 + H_2(f_1, uP)uP, H_2(vP, f_1)f_1)^{v+H_2(vP,sP)s} \mathrm{mod}\ q \\ &= e(f_1 + H_2(f_1, uP)uP, uP)^v \times e(f_1 + H_2(f_1, uP)uP, uP)^{H_2(vP,sP)s} \times e(f_1 + H_2(f_1, uP)uP, H_2(vP, f_1)f_1)^{v+H_2(vP,sP)s} \mathrm{mod}\ q \\ &= e(f_1 + H_2(f_1, uP)uP, vP + H_2(vP, sP)sP)^{u+H_2(vP,f_1)r} \times e(f_1 + H_2(f_1, uP)uP, H_2(vP, f_1)f_1)^{v+H_2(vP,sP)s} \mathrm{mod}\ q \\ &= e(f_1 + H_2(f_1, uP)uP, vP + H_2(vP, sP)sP)^{u+H_2(vP,f_1)r} \times e(f_1 + H_2(f_1, uP)uP, H_2(vP, f_1)f_1)^v \times e(f_1 + H_2(f_1, uP)uP, H_2(vP, f_1)f_1)^{H_2(vP,sP)s} \mathrm{mod}\ q \\ &= e(f_1 + H_2(f_1, uP)uP, vP + H_2(vP, sP)sP)^{u+H_2(vP,f_1)r} \times e(f_1 + H_2(f_1, uP)uP, vP)^{rH_2(vP,f_1)} \times e(f_1 + H_2(f_1, uP)uP, H_2(vP, sP)sP)^{rH_2(vP,f_1)} \mathrm{mod}\ q \end{aligned}$$

$= e(f_1 + H_2(f_1, uP)uP, vP + H_2(vP, sP)sP)^u \times e(vP + H_2(vP, sP)sP, f_1 + H_2(f_1, uP)uP)^{rH_2(vP,f_1)} \text{mod } q$
$= e(vP + H_2(vP, sP)sP, f_1 + H_2(f_1, uP)uP)^{u+H_2(vP,f_1)r} \text{mod } q$
$= f_2 \text{ mod } q.$
Hence,

$$d_2 = H_1(d_1) = f_3.$$

Thus, the recovered plaintext is

$$d_2 \oplus f_4 = f_3 \oplus f_4 = m.$$

Therefore, the soundness is satisfied in this scheme.

B. Semantic Security

The semantic security of the receiptor-oriented encryption schemes is that: if for any plaintext $m_0 \in \{0,1\}^n$ (the plaintext space), for any polynomial time attacker **A**, who can input the public keys of the encryptioner and decryptioner, cannot distinguish the ciphertext c (of plaintext m_0) from a random element $\phi \in_R C$ (C is the ciphertext space) in polynomial time.

Theorem 2 The two non-identity based receiptor-oriented encryption schemes in section 4 both have the semantic security. That is to say, if $\{f_1, f_4\}$ is any legal ciphertext returned by the encryptioner on plaintext $m \in \{0,1\}^n$, then any probabilistic polynomial time attacker $\boldsymbol{A}$ will distinguish between $\{f_1, f_4\}$ and $\{X, Y\}$ with negligible probability; where X and Y are two random elements belonging to G_1 and G_2, respectively.

Proof. Notice that, By the descriptions on encryption algorithms of the identity-based receiptor-oriented encryption scheme 1 in section 4, and without loss of generality, we may let

$f_1 = \zeta P$
$f_2 = e(\zeta Q_1, P_{KGC})e(S_2, pk_{t_i}) (\text{mod } q)$
$f_3 = H_1(f_2)$
$f_4 = f_3 \oplus m.$

where $\zeta \in Z_q^*$ is an unknown (with respect to A) random element; pk_{t_i} and Q_1 are the decryptioner's specified time-stage public key and long-term public key, respectively. m is any plaintext in $\{0,1\}^n$. P_{KGC} is the domain public parameter.

Since ζ is a random element in Z_q^*, $f_1 = \zeta P$ is a random element in G_1. In addition, c_2 is also random in G_2 since $e(*, *)$ is a bilinear map from $G_1 \times G_1$ to G_2. Therefore, by the definition of universal collision-free one-way hash function [8], we know that $f_4 = f_3 \oplus m$ is a random element in G_2. What's more, the attacker A does not know the value of $\zeta \in Z_q^*$ and $S_2 \in G_1$. Hence, from the point of view of the attacker $\boldsymbol{A}$, $\{f_1, f_4\}$ is a random pair in $G_1 \times G_2$. Therefore, the probability of attacker A tells $\{f_1, f_4\}$ from $\{X, Y\}$ is approximately $1/q^2$.

According to the above analysis, any probabilistic polynomial time attacker $\boldsymbol{A}$ will distinguish between $\{f_1, f_4\}$ and $\{X, Y\}$ only with negligible probability.

C. Backward-and-future Security

The backward-and-future security is formalized with respect to the oriented receiptor while its specified time-stage private sk_{t_i} is compromised by a probabilistic polynomial time attcker **A**. Backward-and-future security means that even though attacker **A** obtains the time-stage private sk_{t_i} for the time stage t_i, **A** is still not able to: (1) figure out the corresponding plaintext of any ciphertext c encrypted during time-stage t_i; (2) derive the former time-stage t_{i-1}'s private key $sk_{t_{i-1}}$ from sk_{t_i}; (3) calculate the latter time-stage t_{i+1}'s private key $sk_{t_{i+1}}$ based on sk_{t_i}.

Theorem 3 The two non-identity based receiptor-oriented encryption schemes in section 4 both have the backward-and-future security defined in section 2.

Proof. Due to the similar construction of the two non-identity based ROE schemes, the authors will prove this theorem with non-identity based ROE scheme 1.

Without loss of generality, we may assume there is a probabilistic polynomial time attacker **A**, who already (because of some special reason) compromised the time-stage private key sk_{t_i} of the decryptioner during the course of t_i. In addition, suppose $\{f_1, f_4\}$ is any legal ciphertext on an arbitrary plaintext m enciphered by the encryptioner. To complete the proof, we may by the encryption algorithm assume

$f_1 = \eta P;$
$f_2 = e(vP + H_2(vP, sP)sP, f_1 + H_2(f_1, uP)uP)^{u+\eta H_2(vP,f_1)} (\text{mod } q);$
$f_3 = H_1(f_2);$
$f_4 = f_3 \oplus m.$

where η is a random element; and the compromised private key by attacker **A** is $sk_{t_i} = v$.

Now we will prove the probabilistic polynomial time attacker **A** will not be able to:

(1) figure out the corresponding plaintext m of $\{f_1, f_4\}$;

(2) derive the former time-stage private key $sk_{t_{i-1}}$ (of the decrytioner) from $sk_{t_i} = vP$;

(3) calculate the latter time-stage private key $sk_{t_{i+1}}$ (of the decryptioner) based on $sk_{t_i} = vP$.

Notice that η, s, and u are all hidden i.e. unknown by the attacker **A** from the information theoretical view. Therefore,

(1) By the assumption of ECDL, **A** is not able to inverse η from $f_1 = \eta P$. At the same time,

$$f_2 = e(vP+H_2(vP, sP)sP, f_1+H_2(f_1, uP)uP)^{u+\eta H_2(vP,f_1)}$$

$$= e(uP + H_2(vP, f_1)f_1, f_1 + H_2(f_1, uP)uP)^{v+sH_2(vP,sP)}$$

$$= e(uP+H_2(vP, f_1)f_1, vP+H_2(vP, sP)sP)^{\eta+uH_2(f_1,uP)} (\text{mod } q).$$

By the BDH assumption and IWP assumption, **A** is not able to compute d_2 , as well as d_3. Therefore, she is not able to figure out the plaintext $m = d_3 = d_2 \oplus f_4$.

(2) By the construction of the non-identity based ROE scheme 1, both the decryptioner's time-stage private key sk_{t_i} and $sk_{t_{i-1}}$ are randomly and uniformly chosen by the decrypitoner from Z_q^*. Therefore, from the point of view of

attacker A, sk_{t_i} and $sk_{t_{i-1}}$ have no relationship useful to attacker A. Thus, she will be not able to derive the former time-stage private key $sk_{t_{i-1}}$ from sk_{t_i}.

(3) Due to the similar reason as above (2), attacker A is not able to calculate the latter time-stage private key $sk_{t_{i+1}}$ (of the decryptioner) based on $sk_{t_i} = vP$.

VI. Efficiency Analysis

We first investigate the *expansion factor* of our new schemes. Recall what is the *expansion factor* of encryption schemes, it is the ratio between the lengths of the cipher text and the plaintext. The expansion factor of the proposed new schemes is the same as that of [2]. By this definition, we can use some compression technique applying to the cipher text $\{f_1, f_4\}$ (of message m) to get its length equal to f_4 [8]. Therefore, the expansion factor of all our new schemes is 1, and at most 2.

In terms of encryption algorithms, the dominated computation is the bilinear pairing evaluation. The encryption for non-identity based ROE scheme 2 need two bilinear pairing evaluations, and one of them can be precomputed. While non-identity based ROE scheme 1 only need one pairing evaluation. Because of the symmetric construction of the encryption and decryption algorithms, so they have the same computation workloads.

VII. Conclusion

This paper proposed two non-identity based receiptor-oriented encryption schemes respectively. In contrast to previous encryption schemes with semantic security, the new schemes make use of both the public and private key of encrytioner and the public keys of decryptioner. This case may be very useful in some practical scenarios. Besides the semantics security the proposed schemes have the backward-and-future security, a new security requirement for semantically secure encryption schemes. As a research topic, it is interesting to analyze the security against chosen cipher-text attack on the proposed schemes.

Acknowledgment

The authors would like to thank the anonymous reviewers.

The first author thanks the support of Research Felllowship and ARC Funding at the Centre CEEBI and School of Information Systems, Curtin Business School, Curtin University of Technology.

References

[1] D.Galindo, S.Martin, P.Morillo & L.Villar, *An efficient semantically secure elliptic curve cryptosystem based on KMOV scheme,* International Workshop on Coding and Cryptography WCC 2003. Versailles, France, 2003.

[2] D.Galindo, S.Martin, P.Morillo & L.Villar, *An IND-CPA cryptosystem from Demytko's primitive,* 2003 IEEE Information Theory Workshop. La Sorbonne, Paris, France, 2003.

[3] D.Boneh & M.Franklin, *Identity-based encryption from the Weil pairing,* Proceedings of CRYPTO 2001, Springer-verlag, LNCS 2139, 213-229, 2001.

[4] A.Joux, *A one-round protocol for tripartite Diffie-Hellman,* Algorithm Number Theory Symposium - ANTS-IV, Springer-Verlag, LNCS 1838, 385-394, 2000.

[5] F.Hess, *Efficient identity based signature schemes based on pairings,* K. Nyberg and H. Heys(Eds.), Selected Areas in Cryptography, SAC 2002, Springer-Verlag, 310-324, 2003.

[6] B. Libert & Jean-Jacques Quisquater, *New identity based signcryption schemes from pairings,* Proceedings of IEEE Information Theory Workshop 2003, 2003.

[7] D.Catalano, R.Gennaro, N.Howgrave-Graham & P.Nguyen, *Paillier's cryptosystem revisited,* ACM Conference on Computer and Communication Security, USA, 2002.

[8] A.Menezes, P.C.van Oorschot & S.A.Vanstone, *Handbook of applied cryptography,* CRC Press, Boca Raton, 1997.

[9] R.Sakai, K.Ohgishi & M.Kasahara, *Cryptogsystems based on pairings,* Proceedings of SCIS 2000, Oiso, Janpan.