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

J. Wang
National Natural Foundation of China
Beijing, China

W. Liu
Department of Computing
Curtin University of Technology

V. Potdar
School of Information Systems
Curtin University of Technology

Abstract—Various public key encryption systems have been proposed in modern information technology. 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 decryptionor’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 technology. 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 signcryption [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 encryptionor’s both public key and private keys with the decryptionor’s public keys in encryption algorithms.
• The backward-and-future security is introduced into the semantic secure cryptosystems. 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 receptor-oriented encryption scheme and the corresponding requirements on the receptor-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 receptor-oriented encryption scheme is presented as follows.

Definition 1 (Receptor-Oriented Encryption) A receptor-oriented encryption (abbr. ROE) scheme is a public key cryptosystem comprised of the following three procedures, and in which two entities (encryptionor and decryptionor) are involved:

1) Key Generation: On input a security parameter $\ell$, this probabilistic algorithm returns the long-term public keys and private keys for the encryptionor ($pk_1$, $sk_1$) and the decryptionor ($pk_2$, $sk_2$), 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 receptor, i.e. the decryptionor. The initialized time-stage is $t_0$. Therefore, the initial time-stage public key and private key for the
decrepancy are \( pk_t \) and \( sk_t \), 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 receptor’s (i.e. decryptioner’s) specified time-stage public key \( pk_t \) 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 \( pk_t \) and private key \( sk_t \), 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 receptor 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:

\[
D_{pk_1, pk_2, sk_1, sk_2, pk_t, sk_t}(Ep_{pk_1, pk_2, sk_2, pk_t}(m, r)) = m
\]

where \( E \) and \( D \) are the encryption and the decryption algorithms respectively; \( r \) is a random element chosen by the encryptioner; \( pk_1, pk_2, sk_1, sk_2 \) 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 receptor while its specified time-stage private \( sk_t \), is compromised by an attacker \( A \). Backward-and-future security means that even though attacker \( A \) obtains the time-stage private \( sk_t \) 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 \( sk_t \).
- calculate the latter time-stage \( t_{i+1} \)’s private key \( sk_{t_{i+1}} \) from \( sk_t \).

**III. Preliminaries**

In this paper, we choose \( \ell \) as the security parameter for all the proposed receptor-oriented encryption schemes. Let \( q \) be a large prime, and \( \mathbb{Z}_q^* \) be \( \mathbb{Z}_q \setminus \{0\} \). \( F_q \) 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: \( H_1 : G_2 \rightarrow \{0,1\}^n \), and \( H_2 : G_1 \times G_1 \rightarrow \mathbb{Z}_q^* \); 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 \( \mathcal{O} \), 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 \( \ell \); and \( \ell \) may be equal to or larger than 160 for security reason.

**IV. Receiver-oriented Encryption Schemes**

In this section, we will propose two receptor-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 receptor-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 receptor-oriented encryption scheme 1 has still three algorithms:

(1) **Key Generation** This is a polynomially probabilistic algorithm, which first obtains an elliptic curve \( E((1, 0))/F_p \) 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 \( u \in \mathbb{Z}_q^* \) and the decryptioner’s long-term public key is \( sP \in G_1 \), and private key is \( s \in \mathbb{Z}_q^* \). In addition, the decryptioner will have a pair of specified time-stage public key \( vP \in G_1 \) and private key \( v \in \mathbb{Z}_q^* \) 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 \( r \in \mathbb{Z}_q^* \), and computes \( f_1 = rP \).
- the encryptioner then computes

\[
f_2 = e(vP + H_2(vP, sP)sP, c_1 + H_2(c_1, uP)uP)u + H_2(vP, c_1) \mod q
\]

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
  \[
  d_1 = e(c_1 + H_2(c_1, uP) uP, uP + H_2(vP, c_1) c_1) v + H_2(vP, sP) a
  \]
- 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 \( \bot \).

In the above scheme, there are one pairing evaluation and a 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 polynomially probabilistic algorithm, which returns the domain parameters: a security parameter \( \ell \); two groups \( G_1 \) and \( G_2 \) with the same order \( q \) and the former is an additive group; a bilinear pairing \( e(*) : G_1 \times G_1 \rightarrow G_2 \); 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 \( H_1(\cdot) : G_2 \rightarrow \{0,1\}^n \), where \( n = \lceil \ell \rceil \). 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 element \( r \in Z_q^* \), and calculates \( f_1 = rP \in G_1 \).
- he then calculates by use of pairing \( e(*)^\beta \)
  \[
  f_2 = e(\alpha P, f_1)^\beta e(\beta P, P)^r, \text{ and as well } f_3 = H_1(f_2).
  \]
- 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 receptor). Given a ciphertext \( \{f_1, f_4\} \), she will do:

- the decryptioner first calculates an element \( d_1 = e(f_1, \beta P)^\alpha e(\beta P, f_1)^\rho \in G_2 \), 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 receptor-oriented encryption schemes, the encryptioner and the decryptioner may make use of some key distribution technique [9], and commitment technique [7], [7], and Schnorr 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 receptor-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 receptor-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 receptor-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

\[
D_{uP, uS, P, vP, P, (E_{uP, sP, sP, P, P}(m, r))} = m
\]

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

\[
\begin{align*}
    f_1 &= rP; \\
    f_2 &= e(vP, H_2(vP, sP) sP, f_1) + H_2(f_1, uP) uP P + e(vP, H_2(vP, sP) sP, f_1) e(vP, H_2(vP, sP) sP, f_1) \mod q; \\
    f_3 &= H_2(f_2); \\
    f_4 &= f_5 \oplus m.
\end{align*}
\]

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

Since \( d_1 = e(c_1 + H_2(f_1, uP) uP P, uP P) H_2(vP, sP) sP \mod q \), and by the key generation algorithm, therefore

\[
\begin{align*}
    d_1 &= e(f_1 + H_2(f_1, uP) uP P, uP P) H_2(vP, sP) sP \mod q \\
    &= e(f_1 + H_2(f_1, uP) uP P, uP P) H_2(vP, sP) sP \mod q \\
    &= e(f_1 + H_2(f_1, uP) uP P, uP P) H_2(vP, sP) sP \mod q \\
    &= e(f_1 + H_2(f_1, uP) uP P, uP P) H_2(vP, sP) sP \mod q \\
    &= e(f_1 + H_2(f_1, uP) uP P, uP P) H_2(vP, sP) sP \mod q \\
    &= e(f_1 + H_2(f_1, uP) uP P, uP P) H_2(vP, sP) sP \mod q \\
    &= e(f_1 + H_2(f_1, uP) uP P, uP P) H_2(vP, sP) sP \mod q.
\end{align*}
\]

767
\[ e(f_1 + H_2(f_1, uP)uP, vP + H_2(vP, sP)sP)^n \times e(vP + H_2(vP, sP)sP, f_1 + H_2(f_1, uP)uP)^{nH2(vP, f_1)} \mod q = e(vP + H_2(vP, sP)sP, f_1 + H_2(f_1, uP)uP)^{nH2(vP, f_1)} \mod q = f_2 \mod q. \]

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 receptor-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 encryption and decryptioner, cannot distinguish the ciphertext \( c \) (of plaintext \( m_0 \)) from a random element \( \phi \in _R C \) (where \( C \) is the ciphertext space) in polynomial time.

**Theorem 2** The two non-identity based receptor-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 \( A \) 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 receptor-oriented encryption scheme I in section 4, and without loss of generality, we may let
\[ f_1 = \zeta P \]
\[ f_2 = e(\zeta Q_1, PKGC) e(S_2, p k_{t_1})(\mod q) \]
\[ f_3 = H_1(f_2) \]
\[ f_4 = f_3 \oplus m, \]

where \( \zeta \in Z_q^* \) is an unknown (with respect to \( A \)) random element; \( p k_{t_1} \) 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 \( \zeta \) 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 \( e(\cdot, \cdot) \) 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 \( G_2 \). Thus, 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 \( A \), \( \{f_1, f_4\} \) 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 \( 1/2 \).

According to the above analysis, any probabilistic polynomial time attacker \( A \) 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 receiver while its specified time-stage private key \( s_{k_{t_1}} \) is compromised by a probabilistic polynomial time attacker \( A \). Backward-and-future security means that even though attacker \( A \) obtains the time-stage private key \( s_{k_{t_1}} \) for the time stage \( t_1 \), \( A \) is still not able to: (1) figure out the corresponding plaintext of any ciphertext \( c \) encrypted during time-stage \( t_1 \); (2) derive the former time-stage \( t_{i-1} \)’s private key \( s_{k_{t_{i-1}}} \) from \( s_{k_{t_1}} \); (3) calculate the latter time-stage \( t_{i+1} \)’s private key \( s_{k_{t_{i+1}}} \) based on \( s_{k_{t_1}} \).

**Theorem 3** The two non-identity based receptor-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 \( s_{k_{t_1}} \) of the decryptioner during the course of \( t_1 \). In addition, suppose \( \{f_1, f_4\} \) is any legal ciphertext on an arbitrary plaintext \( m \) encrypted by the encryptioner. To complete the proof, we may by the encryption algorithm assume
\[ f_1 = \eta P; \]
\[ f_2 = e(vP + H_2(vP, sP)sP, f_1 + H_2(f_1, uP)uP)^{nH2(vP, f_1)} \mod q; \]
\[ f_3 = H_1(f_2); \]
\[ f_4 = f_3 \oplus m, \]

where \( \eta \) is a random element; and the compromised private key by attacker \( A \) is \( s_{k_{t_1}} = v \).

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 \( s_{k_{t_{i-1}}} \) (of the decryptioner) from \( s_{k_{t_1}} = vP; \)
3. calculate the latter time-stage private key \( s_{k_{t_{i+1}}} \) (of the decryptioner) based on \( s_{k_{t_1}} = vP. \)

Notice that \( \eta, s, \) 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 \( \eta \) from \( f_1 = \eta P \). At the same time,
\[ f_2 = e(vP + H_2(vP, sP)sP, f_1 + H_2(f_1, uP)uP)^{nH2(vP, f_1)} = e(uP + H_2(vP, f_1)uP, f_1 + H_2(f_1, uP)uP)^{nH2(vP, f_1)} = e(uP + H_2(vP, f_1)f_1, vP + H_2(vP, sP)sP)^{nH2(f_1, uP)} \mod q. \]

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 \( m = d_3 = d_3 \oplus d_4 \).

2. By the construction of the non-identity based ROE scheme 1, both the decryptioner’s time-stage private key \( s_{k_{t_1}} \) and \( s_{k_{t_{i-1}}} \) are randomly and uniformly chosen by the decryptor from \( Z_q^* \). Therefore, from the point of view of
attacker $A$, $sk_{t_1}$ 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 $sk_{t_1}$.

(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 decryption) based on $sk_{t_1} = vP$.

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 ciphertext 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 \( \{ f_1, f_2 \} \) (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 receptor-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 encryptor and the public keys of decryptor. 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 Fellowship and ARC Funding at the Centre CEEBI and School of Information Systems, Curtin Business School, Curtin University of Technology.

REFERENCES


