Pairing-based Public-key Encryption Schemes with Backward-and-Forward Security

Song Han\textsuperscript{1}, Elizabeth Chang\textsuperscript{1}, and Tharam Dillon\textsuperscript{2}

\textsuperscript{1} School of Information Systems, CBS, Curtin University of Technology, GPO Box U1987, WA 6845, Australia
\textsuperscript{2} Faculty of Information Technology, University of Technology Sydney, PO Box 123 Broadway NSW 2007 Australia

\textbf{Abstract.} Identity-based cryptosystems utilize some arbitrary strings as the participants' public key in the underlying system. The encryptor will not need to obtain the decryptor's certificate. That will simplify the certificate management. Therefore, it is still interesting to propose some new identity-based encryption schemes. In this paper, we will propose two new different constructions, i.e. \textit{receiver-oriented encryption schemes}. They are both identity-based encryption schemes and also based on pairings. The proposed encryption schemes have a new advantage, i.e. backward-and-forward security. In addition, we provide the security analysis for the proposed schemes.


1 Introduction

Public key cryptography has been widely involved in today's digital life, such as network communication, wireless communication, smart cards, etc. [10, 11]. Public key encryption technique plays an important role in its utilization of public key cryptography. Very recently, some new semantically secure encryption schemes are attracting attention. Galindo et al proposed two schemes [5, 6]. However, most of the previous encryption schemes have not provided several properties; One of these properties is backward-and-forward security, i.e. some partial keys of participants can be changed with ongoing time. This property is necessary, since an attacker may gain all the time catch up with a targeted communication channel and try to break the underlying private key. Therefore, it is potentially important to construct new semantically secure public key encryption schemes which have the above backward-and-forward security property. In this paper, we will propose two such schemes.

Identity-based cryptosystems and cryptographic protocols have also been paid more attention over the years since Shamir proposed the first identity-based encryptions and signatures [13]. The benefits of identity-based cryptosystems and cryptographic protocols are that they use some arbitrary strings as the participant’s public key in the underlying schemes. Thus it will not need the
encryptioner to obtain the decryptioner's certificate. Therefore, that will simplify certificate management [11]. Some identity-based signatures, encryptions, key agreement, and signcryption were proposed in references [7, 2, 9]. In our paper, we propose two identity-based semantically secure encryption schemes.

Recently, the bilinear pairings modified from Weil or Tate pairings [8, 12] are becoming one of the new active research topics in information security. Especially, the supersingular curves are the main object used by the bilinear pairings. However, prior to [2, 8], 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 [8] and Boneh et al [2], the pairings have become desirable and applied to various cryptographic primitives: public key encryption [2], digital signature [7], key agreement [8]; and signcryption [9]. In our paper, we propose two new public key encryption schemes different from [2, 14]. And the new constructions are motivated by some techniques from references [3, 5, 6, 8, 11, 14].

The organization of the rest of our paper is as follows: The definition of receptor-oriented encryption scheme is presented in section 2. Section 3 provides the new cryptosystems. The security and efficiency analysis is given in section 4 and section 5, respectively. The conclusion is in section 6.

## 2 Definitions of Receiver-Oriented Encryptions

In this section, the definition of the receptor-oriented encryption system is presented as follows. This follows [14].

**Definition 1 (Receiver-Oriented Encryptions)** A receiver-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 $\ell$, this probabilistic algorithm returns the long-term public keys and private keys for the encryptioner $(pk_2, sk_2)$ and the decryptioner $(pk_1, sk_1)$ respectively. Simultaneously, this algorithm also outputs a pair of specified time-stage($t_0$) public key $pk_{t_0}$ and private key $sk_{t_0}$, for the oriented receiver, i.e. the decryptioner. The initialized time-stage is $t_0$. Therefore, the initial time-stage public key and private key for the decryptioner are $pk_{t_0}$ and $sk_{t_0}$, respectively. The relationship of the three main keypairs $(pk_1, sk_1)$, $(pk_2, sk_2)$ and $(pk_{t_0}, sk_{t_0})$ are as follows: $(pk_1, sk_1)$ and $(pk_2, sk_2)$ are long-term keys, while $(pk_{t_0}, sk_{t_0})$ are short-term (i.e. specified-time-stage) keys; Suppose a message $m$ is encrypted in time-stage $t_i$; for encryption, the keys including $pk_1$, $(pk_2, sk_2)$ and $pk_{t_0}$ will be involved in the generation of a ciphertext $c_t$ of $m$; for decryption, the keys $(pk_1, sk_1)$, $pk_2$ and $(pk_{t_0}, sk_{t_0})$ will be involved in the generation of the plaintext (i.e. $m$) from $c_t$.

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 receiver'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 encryptor will be involved. In the end, the encryptor publishes the ciphertext \( C \) (of plaintext \( m \)) on its homepage. Furthermore, its homepage will be renewed in time.

(3) **Decryption:** This is an algorithm done by the decryptor. The algorithm inputs the ciphertext \( C \), the decryptor’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 encryptor’s public key \( pk_2 \). In the end, the plaintext \( m \) will be returned.

**Definition 2 (Requirements of a Secure ROE System)** A secure receiver oriented public key encryption system 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:

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

where \( E \) and \( D \) are the encryption and the decryption algorithms respectively; \( r \) is a random element chosen by the encryptor; \( pk_1 \), \( pk_t \), and \( sk_1 \), \( sk_t \) are the decryptor’s public keys and private keys respectively; \( pk_2 \) and \( sk_2 \) are the encryptor’s public and private keys, respectively.

2. **Semantic Security:** For any \( m_0 \in M \) (M is the plaintext space), for any polynomial time attacker \( A \), who can input the public keys of the encryptor and decryptor, 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-Forward 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-forward security means that even though an 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 \( sk_t \).

## 3 ID-based Encryption Schemes

In this section we will propose two identity-based receptor-oriented encryption schemes (ID-based ROE schemes). We develop the constructions motivated by some techniques from \([3, 5, 6, 8, 11]\). The proposed identity-based encryption schemes are based on pairings over elliptic curves. We will first review some mathematical tools, that will be used in the proposed schemes.

### 3.1 Notations

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 \( Z_q^* \) be \( Z_q \setminus \{0\} \). \( F_q \)
denotes a finite field with \( q \) elements. \( \oplus \) denotes the bit-wise XOR calculation. Let \( n \) be a positive integer with \( n = \bigcirc (\ell) \). Let \( H \) and \( H_1 \) be two cryptographic hash functions: \( H : \{0,1\}^* \rightarrow G_1 \), and \( H_1 : G_2 \rightarrow \{0,1\}^n \); where \( H_1 \) is a universal one-way hash function [11, 16]. \( G_1 \) and \( G_2 \) will be given later.

**Definition 3** Let \( p > 3 \) be a prime. An elliptic curve over the finite field \( \mathbb{F}_p \), denoted by \( E_p(a, b) \) or \( E(a, b)/\mathbb{F}_p \), where \( a, b \in \mathbb{F}_p \), 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 \( \mathbb{O} \) [15], called the point at infinity.

In our paper, we choose elliptic curves \( E(a, b)/\mathbb{F}_p \) 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 \( E(0, b)/\mathbb{F}_p \) (the number of it) is \( |E(0, b)/\mathbb{F}_p| = p + 1 \), and thus avoiding the difficulty of computing \( |E(a, b)/\mathbb{F}_p| \).
- the bit length of \( p \) is \( \ell \); and \( \ell \) may be 160 or larger than it for security reason.

### 3.2 Pairings over Elliptic Curves

Let \( p \) be a sufficiently large prime that satisfies: (a) \( p \equiv 2 \mod 3 \); (b) \( p = 6q - 1 \), where \( q \) is also a large prime. Consider the elliptic curves \( E/\mathbb{F}_p \) defined by the equation:

\[
y^2 = x^3 + 1.
\]

(2)

Let \( G_1 \) be an additive group of points of prime order \( q \) on the elliptic curve \( E/\mathbb{F}_p \), and let \( G_2 \) be a multiplicative group of same order \( q \) of some finite field \( \mathbb{F}_{p^2} \). We are able to derive a bilinear pairing from the Weil pairing or Tate pairing [1, 4]:

\[
e : G_1 \times G_1 \rightarrow G_2
\]

(3)

with respect to which the Elliptic Curve Discrete Logarithm (ECDL) problems are difficult in \( G_1 \) and the Computational Diffi-Hellman (CDH) problems and the Inversion of Weil pairing (IWP) problem are difficult in \( G_2 \).

The pairing \( e : G_1 \times G_1 \rightarrow G_2 \) has the following properties:

1. Bilinearity: \( e(aP, bQ) = e(P, Q)^{ab} \) for every pair \( P, Q \in G_1 \) and for any \( a, b \in \mathbb{Z}_p \).

2. Non-degenerate: there exists at least one point \( P \in G_1 \) such that \( e(P, P) \neq 1 \).

3. Efficient Computability: there are efficient algorithms to compute the bilinear pairings \( e \).

### 3.3 ID-based ROE Scheme 1

By the definition of ROE system in section 2, the ROE system 1 has three algorithms:

1. **Key Generation** The KGC first chooses an elliptic curve \( E/\mathbb{F}_p \), as in section 3. And then it chooses \( G_1, G_2, P, e(\ast, \ast) \) as above in the same section.
It then chooses \( s \in Z_q \) and computes domain public key \( P_{KGC} = sP \). The
encryption and the receptor-oriented decryption's respective identities \( id_2 \)
and \( id_1 \) as their prime public keys. Then, the decryption's long-term public key
and private key are respectively \( S_1 = sQ_1 \) and \( Q_1 \); the encryption's long-term
public key and private key are respectively \( S_2 = sQ_2 \) and \( Q_2 \); where \( Q_1 = H(id_1) \)
and \( Q_2 = H(id_2) \). Since the decryption is a receptor-oriented entity, so by the
definition she will have a pair of specified time-stage private key \( sk_{t_0} \) and public
key \( pk_{t_0} \). The initialized time-stage is \( t_0 \). Therefore, the initial time-stage public
key and private key for the decryption may take \( pk_{t_0} = vP \) and \( sk_{t_0} = v \),
respectively. In addition, the plaintext space is \( M = \{0, 1\}^m \).

(2) **Encryption** This is a probabilistic algorithm done by the encoder.
For any plaintext \( m \in M \),

- the encoder chooses uniformly and randomly an element \( r \in Z_q^* \), and
  computes \( c_1 = rP \).
- the encoder then computes \( c_2 = e(rQ_1, P_{KGC})e(S_2, vP) \), and \( c_3 = 
  H_1(c_2) \), respectively.
- At the last step, he computes \( c_4 = c_3 \oplus m \).

Then, he publishes the ciphertext \( \{c_1, c_4\} \).

(3) **Decryption** This is a deterministic algorithm done by the receptor-oriented
decryption. Given the ciphertext \( \{c_1, c_4\} \),

- she first calculates \( d_1 = e(vQ_2, P_{KGC}) \cdot e(S_1, c_1) \).
- she then calculates \( d_2 = H_1(d_1) \).
- she recovers the plaintext by \( m = d_2 \oplus c_4 \). If the ciphertext is invalid one,
  then she recovers nothing \( \perp \).

In the above encryption algorithm, the computation of ciphertext of plaintext
\( m \) combines the encoder's public and private keys with the decryptor's
public key and the specified time-stage public key. In addition, some random
elements and a universal collision-free one-way hash function are also involved.

### 3.4 ID-based ROE Scheme 2

By the definition of ROE system in section 2, the ROE system 2 has three
algorithms:

(1) **Key Generation** The KGC first chooses an elliptic curve \( E/F_p \) as in
section 3. And then it chooses \( G_1, G_2, P, e(\cdot, \cdot) \) as above in the same section.
It then chooses \( s \in Z_q \) and computes domain public key \( P_{KGC} = sP \). The
encoder and the receptor-oriented decryptor's respective identities \( id_2 \)
and \( id_1 \) as their prime public keys. Then, the decryption's long-term public key
and private key are respectively \( S_1 = sQ_1 \) and \( Q_1 \); the encoder's long-term
public key and private key are respectively \( S_2 = sQ_2 \) and \( Q_2 \); where \( Q_1 = H(id_1) \)
and \( Q_2 = H(id_2) \). Since the decryptor is a receptor-oriented entity, so by the
definition she will have a pair of specified time-stage private key \( sk_{t_0} \) and public
key \( pk_{t_0} \). The initialized time-stage is \( t_0 \). Therefore, the initial time-stage public
key and private key for the decryptor may (without loss of generality) take
\(pk_{\alpha} = \alpha Q_1\) and \(sk_{\alpha} = \alpha\), respectively.

(2) Encryption
This is a polynomially probabilistic algorithm done by the encryptor. For any plaintext \(m \in M\),

- the encryptor chooses uniformly and randomly an element \(r \in \mathbb{Z}_q^*\), and
  computes \(c_1 = rQ_2\).
- the encryptor then computes \(c_2 = e(\alpha Q_1 + rQ_1, S_2)\), and \(c_3 = H_1(c_2)\),
  respectively.
- At the last step, he computes \(c_4 = c_3 \oplus m\).

Then, he publishes the ciphertext \(\{c_1, c_4\}\).

(3) Decryption
This is a deterministic algorithm done by the receptor-oriented decryptor. Given the ciphertext \(\{c_1, c_4\}\),

- she first calculates \(d_1 = e(c_1 + \alpha Q_2, S_1)\).
- she then calculates \(d_2 = H_1(d_1)\).
- she recovers the plaintext \(m = d_2 \oplus c_4\). If the ciphertext is invalid one,
  then she recovers nothing \(\square\).

It is easy to see the difference between the above two ROE schemes is that the former has two pairing evaluations on both encryption and decryption; and the latter has only one such evaluation. Probably, the second one is more efficient than the first. Fortunately, in identity-based ROE system 1, one of the two pairing evaluations could be preprocessed.

4 Security Analysis

In this section, we will prove that both of the two identity-based ROE schemes have the soundness, semantic security, and backward-and-forward security.

4.1 Soundness

The soundness of the receptor-oriented encryption schemes is that: if the encryptor correctly calculates the ciphertexts according to the descriptions of encryption algorithm, and if the decryptor correctly carries on the decryption algorithm, then the latter will surely recovers the corresponding plaintexts.

**Theorem 1** The two identity-based receptor-oriented encryption schemes in section 4 both have the soundness. In other words, if \(\{c_1, c_4\}\) is a legal ciphertext returned by the encryptor on plaintext \(m \in \{0, 1\}^n\), then the decryptor will surely recovers the plaintext \(m \in \{0, 1\}^n\) such that
\[
D_{Q_1, Q_2, S_1, s_{h_{1_0}}, pk_{\alpha}}(E_{Q_2, Q_1, S_2, p_{h_{1_0}}}(m, r)) = m
\]
where \(E\) and \(D\) are the encryption and the decryption algorithms, respectively; \(r\) is a random element chosen by the encryptor; and other data are the same to what are in the two identity-based ROE schemes in section 4.
Proof. Because of the similar proofs on the two ROE schemes, the authors only present the theorem proof for the identity-based ROE system 1.

By the encryption algorithm of the identity-based ROE system 1, we can write
\[
\begin{align*}
    c_1 &= rP; \\
    c_2 &= e(rQ_1, P_{KGC})e(S_2, vP)(\mod q); \\
    c_3 &= H(c_2); \\
    c_4 &= c_3 \oplus m.
\end{align*}
\]
where \( r \in \mathbb{Z}_q^* \) is a random element.

Since \( d_1 = e(vQ_2, P_{KGC}) \cdot e(S_1, c_1) \), and by the key generation algorithm, therefore
\[
\begin{align*}
    d_1 &= e(vQ_2, P_{KGC}) \cdot e(S_1, c_1) \\
    &= e(vQ_2, sP)e(sQ_1, c_1) \\
    &= e(Q_2, P)^{sr}e(Q_1, P)^{sr} (\mod q) \\
    &= e(sQ_2, vP) \cdot e(rQ_1, sP) \\
    &= e(S_2, vP) \cdot e(rQ_1, P_{KGC}) \\
    &= c_2 (\mod q)
\end{align*}
\]
Hence,
\[
d_2 = c_3.
\]
Thus, the recovered plaintext is
\[
m = c_3 \oplus c_4 = d_2 \oplus c_4.
\]
Therefore, the soundness is satisfied in this system.

4.2 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 encryptor and decryptor, cannot distinguish the ciphertext \( c \) (of plaintext \( m \)) from a random element \( \phi \in \mathbb{R} \) \( C \) (the ciphertext space) in polynomial time.

**Theorem 2** The two identity-based receptor-oriented encryption schemes in section 4 both have the semantic security. In other words, if \( \{c_1, c_4\} \) is any legal ciphertext returned by the encryptor on plaintext \( m \in \{0,1\}^n \), then any probabilistic polynomial time attacker \( A \) will distinguish between \( \{c_1, c_4\} \) and \( \{\phi, \psi\} \) with negligible probability; where \( \phi \) and \( \psi \) 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 system 1 in section 4, and without of generality, we may let
\[
\begin{align*}
    c_1 &= \zeta P \\
    c_2 &= e(\zeta Q_1, P_{KGC})e(S_2, pk_t)(\mod q) \\
    c_3 &= H_1(c_2) \\
    c_4 &= c_3 \oplus m.
\end{align*}
\]
where \( \zeta \in \mathbb{Z}_q^* \) is an unknown (with respect to \( A \)) random element; \( pk_t \), and \( Q_1 \).
are the decryptor’s specified time-stage public key and long-term public key, respectively. \( m \) is any plaintext in \( \{0,1\}^n \). \( \mathsf{PKGC} \) is the domain public parameter.

Since \( \zeta \) is a random element in \( \mathbb{Z}_q^* \), \( c_1 = \zeta P \) 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 [11], we know that \( c_4 = c_3 \oplus m \) is a random element in \( G_2 \). What’s more, the attacker \( A \) does not know the value of \( \zeta \in \mathbb{Z}_q^* \) and \( S_2 \in G_1 \). Hence, from the point of view of the attacker \( A \), \( \{c_1, c_4\} \) is a random pair in \( G_1 \times G_2 \). Therefore, the probability of attacker \( A \) tells \( \{c_1, c_4\} \) from \( \{\Phi, \Psi\} \) is approximately \( 1/q^2 \).

According to the above analysis, any probabilistic polynomial time attacker \( A \) will distinguish between \( \{c_1, c_4\} \) and \( \{\Phi, \Psi\} \) only with negligible probability.

4.3 Backward-and-Forward Security

The backward-and-forward security is formalized with respect to the oriented receptor while its specified time-stage private \( sk_{t_i} \) is compromised by a probabilistic polynomial time attacker \( A \). 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 \( sk_{t_i} \).

\textbf{Theorem 3} The two identity based receptor-oriented encryption schemes in section 4 both have the backward-and-forward security defined in section 2.

\textit{Proof.} Due to the similar construction of the two identity based ROE schemes, we will prove this theorem with identity based ROE system 1.

Without 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 decryptor during the course of \( t_i \). In addition, suppose \( \{c_1, c_4\} \) is any legal ciphertext on an arbitrary plaintext \( m \) enciphered by the encryptor. To complete the proof, we may by the encryption algorithm assume that

\[
\begin{align*}
    c_1 &= \eta P; \\
    c_2 &= e(\eta Q_1, sP) e(sQ_2, vP); \\
    c_3 &= H_1(c_2); \\
    c_4 &= c_3 \oplus m.
\end{align*}
\]

where \( \eta \) 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 \( \{c_1, c_4\} \);
2. derive the former time-stage private key \( sk_{t_{i-1}} \) (of the decryptor) from \( sk_{t_i} = vP \);
(3) calculate the latter time-stage private key $sk_{t_{i+1}}$ (of the decryptioner) based on $sk_t = vP$.

Notice that $\eta$ and $s$ are both 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 $c_1 = \eta P$. At the same time,

$$c_2 = e(\eta Q_1, sP)e(sQ_2, vP) = e(\eta Q_1, P)^s e(sQ_2, P)^v = e(s\eta Q_1, P)e(vsQ_2, P) = e(s\eta Q_1 + vsQ_2, P)$$

By the IWP assumption, $A$ is not able to compute $d_1$. Consequently, $A$ is not able to figure $d_2 = H_1(d_1)$. Therefore, she is not able to figure out the plaintext $m = d_3 = d_2 \oplus d_4$.

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

5 Performance Comparison

When all the new proposed semantically secure encryption schemes are implemented, the performance of them is dominated by the encryption algorithm and the decryption algorithm respectively.

We first investigate the expansion factor, i.e. 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 $\{c_1, c_4\}$ (of message $m$) to get its length equal to $c_4$ [11]. 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 identity-based ROE system 1 needs two bilinear pairing evaluations, and one of them can be precomputed. While id-based ROE system 2 only needs one pairing evaluation. Because of the symmetric construction of the encryption and decryption algorithms, so they have the same computation workloads. On the other hand, our schemes are identity-based encryption schemes, while those in [5, 6, 14] are not identity-based ones. Therefore, our encryption schemes are better than those of [5, 6, 14], from the certificate management point of view [11]. In addition, the scheme in [14] involves two pairing evaluations, while the proposed scheme only needs one evaluation.
The following table presents the complexity comparison of the encryption algorithm between the Scheme in [2] and the new ROE scheme 2 in our paper. Please refer to the appendix.

Table 1: Comparison between Encryption algorithm in reference [2] and the ROE scheme 2

<table>
<thead>
<tr>
<th>Complexity comparison</th>
<th>ROE scheme 2</th>
<th>Scheme in reference [2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pairing evaluation</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Map-to-point has operation in $G_1$</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Scalar multiplication in $G_1$</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Group exponent in $G_2$</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>XOR operation</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Hash operation in $G_2$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Backward-and-forward security</td>
<td>available</td>
<td>not available</td>
</tr>
</tbody>
</table>

6 Conclusion

This paper proposed two identity-based receptor-oriented encryption schemes: id-based ROE scheme 1 and id-based ROE scheme 2. Both of the proposed encryption schemes have a new security characteristic, namely backward-and-forward security. This means that if an attacker were able to obtain the private key for a particular time stage, be it not able to obtain the former and later time stage private keys not is it able to figure out the plaintext corresponding to ciphertext encrypted at that time stage. In addition, We proved that both of the new schemes possess soundness, semantic security, and backward-and-forward security. A complexity comparison was presented. From the complexity comparison, the id-based ROE scheme 2 is more efficient and reliable in terms of backward-and-forward security.

Acknowledgements

The authors thank the anonymous referees for helpful comments. The first author also thanks Polly Poon for her help in preparing the final version.

References


