An Anonymous Multireceiver with Online/Offline Identity-Based Encryption

Qihua Wang, Fagen Li, and Huaqun Wang

1 School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
2 School of Medical Information Engineering, Jining Medical University, Rizhao 272067, China
3 School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

Correspondence should be addressed to Fagen Li; fagenli@uestc.edu.cn

Received 2 March 2018; Revised 21 May 2018; Accepted 13 June 2018; Published 12 August 2018

Abstract

Anonymous multireceiver encryption scheme can not only protect the privacy of the receiver but also ensure the security of message. However, the computational cost of this scheme is very large. It is not suitable for the sender which has limited resources, such as mobile devices and sensor nodes. In this work, an anonymous multireceiver online/offline identity-based encryption is proposed based on offline/online and identity-based encryption (IBE). In identity-based encryption scheme, the sender can encrypt the message using the unique information of the user (such as identity number or e-mail address) as its public key. The receiver obtains the private key from a central authority. For mobile device with limited resource, the online/offline encryption scheme can reduce the computational cost. Compared to the previous anonymous multireceiver schemes, the proposed scheme can efficiently encrypt message with online/offline method and ensure the anonymity of receivers. The analysis results also show that our scheme is efficient in terms of computational cost by comparing to the previous works.

1. Introduction

Multireceiver communication [1] is a crucial way to send and receive message. It can effectively solve the problem of key management and data sending. Multireceiver encryption also is converted to broadcast encryption [2] in certain extent. In multireceiver encryption strategy, the sender/encryptor can select any receiver. In broadcast encryption scheme, the sender/encryptor sends message to a group of users; only the legal users can decrypt the ciphertext. This scheme is widely used in pay-TV applications, the distribution of copyright materials, etc.

In [3], the authors use the idea of identity-based encryption (IBE for short) for reference. The identity information of the receiver is converted to a public key. The receiver’s private key which is distributed by a Key Generator Center (KGC) is connected with the identity information. The receiver can use the private key to decrypt the ciphertext. In [4], Lu and Hu addressed a pairing based multireceiver encryption scheme which can broadcast sensitive information in a complex environment, but it did not protect the privacy of the users. That is to say, this scheme cannot reach the anonymity of the users. A secure and efficient anonymous multireceiver IBE scheme was proposed in [5]. Based on [5], an anonymous multireceiver IBE scheme was improved by Wang et al. [6]. The proposed method cannot truly attain the anonymity of the receiver’s information, and the receiver’s privacy was not protected. In [5, 6], a legal receiver can easily verify whether a specific user is one of the legal receiver or not using only two bilinear pairing computational costs. Li et al. [7] analyzed the security vulnerabilities that exist in [6], but they did not give specific solutions. In order to deal with the privacy of the legal receivers, a really anonymous multireceiver IBE scheme was proposed in [8]. In the proposed scheme, all users can receive the broadcast ciphertext of the sender/encryptor, but only the receiver which was selected by the sender/encryptor can decrypt the ciphertext information. No one except the sender knows who the receiver is. The key issue of this scheme is how to design encryption scheme by using Lagrange interpolation function.
Chien [9] proposed an improved scheme which can achieve the receiver’s anonymity and enhance the security of the message. However, in encryption phase, this scheme requires a number of bilinear pairing operations which is proportional to the number of receivers. He et al. [10] addressed an efficient certificateless anonymous multireceiver encryption scheme according to elliptic curve cryptography for devices with limited resources. The anonymous multirecipient IBE scheme can be used in pay-per-view TV channel and sensitive program order. The receiver does not want any other receivers to know his or her identity information.

In IBE, the computational cost of multiplication and exponentiation operations in groups is larger. It takes much more time and battery power to execute exponential operations for the receiver with limited energy such as mobile phones or mobile devices. In IBE, data encryption needs bilinear pairing operation which can increase the runtime of encryption because the computational cost of bilinear pairing operation is very large. It is difficult to complete the encryption task in a short time for lightweight devices such as wireless sensor nodes or smart cards. Moreover, the anonymous multireceiver IBE takes more time compared to standard IBE.

One challenge in the anonymous multireceiver IBE is that the added functionality may increase the computation cost compared to standard public key cryptography. Online/offline technology can effectively reduce encryption time. The first online/offline IBE scheme was proposed by Guo et al. [11]. The scheme divided the encryption process into two stages: online stage and offline stage. In offline stage, the complex operation is preprocessed. In online encryption stage, the sender performs simple operations and generates the ciphertext. The online phase would be very fast. Moreover, it requires little computational cost in this phase. The online/offline encryption strategy is more suitable for lightweight equipment such as wireless sensor nodes or smart cards [12, 13]. Online/offline identity-based encryption scheme has attracted extensive attention, and series of research results have emerged [14–16]. Recently online/offline technology is also used in attribute-based encryption [17,18]. However, previous literatures did not apply the online/offline scheme to the anonymous multireceiver IBE.

In this article, we concentrate on multireceiver IBE scheme that takes into consideration online/offline encryption. The offline information cannot be reused in previous work. In our proposed scheme, a few operations can be done in offline phase. The offline ciphertext which is computed in offline phase can be reused for the same receiver sets. This method can reduce the computation cost for the senders when they encrypt the message to the same receive sets.

Our motivating application for the work in this way is mobile device with limited resources. The preparation computation can be done while the mobile device is plugged into a power supply, and then when it is on the move without plugging, it performs the encryption operations with little computational cost.

The structure of this work is organized as follows. Section 2 reviews the cryptographic backgrounds and Section 3 describes an anonymous multireceiver online/offline identity-based encryption. The security proof and performance analysis are given in Section 4. Finally, Section 5 is the conclusions of this work.

2. Preliminary
Some fundamental backgrounds related to this work are given in this section.

2.1. Lagrange Interpolation Theorem. Fitting the curve through these points \((x_1, y_1), (x_2, y_2), \ldots, (x_t, y_t)\) can be expressed as follows [6]:

\[
f(x) = \sum_{i=1}^{t} F_i(x) = \sum_{i=0}^{t} a_i x^i \tag{1}
\]

where for each \(i\)

\[
F_i(x) = y_i \prod_{1 \leq j \neq i \leq t} \frac{x - x_j}{x_i - x_j} = \begin{cases} y_i & x = x_i \\ 0 & x \in \{x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_t\} \end{cases} \tag{2}
\]

\(x_i\) is mapped by identity information \(id_i\) of the receiver.

2.2. Bilinear Maps. Let \(G_1\) and \(G_2\) be two multiplicative cyclic groups with the same prime order \(p\). Let \(P\) be a generator of \(G_1\). Let \(e : G_1 \times G_1 \rightarrow G_2\) be a bilinear map which has the following properties [19]:

1. Bilinearity: \(\forall Q, R \in G_1\) and \(a, b \in \mathbb{Z}_p\), \(e(Q, R) = e(aP, bP) = e(P, P)^{ab}\).
2. Nondegeneracy: \(\exists Q, R \in G_1\), such that \(e(R, Q) \neq 1\). \(1\) denotes the identity element of \(G_2\).
3. Computability: \(\forall Q, R \in G_1\); there is an efficient polynomial algorithm to calculate \(e(Q, R)\).

According to the bilinearity, the bilinear mapping \(e\) has the following specific property:

\[
e(aP, bP) = e(P, P)^{ab} = e(bP, aP) \tag{3}
\]

2.3. Hard Problems. The following security assumptions are used in many encryption schemes. We will use them to deal with some problems in our scheme. In our paper, \(P\) denotes the generator of \(G_1\).

1. Computational Diffie-Hellman problem: given \((P, aP, bP)\) for any \(a, b \in \mathbb{Z}_p^*\), compute \(P^{ab}\).
2. Bilinear Diffie-Hellman (BDH) problem: given \((P, aP, Pb, cP)\) for some \(a, b, c \in \mathbb{Z}_q^*\) compute \(e(g, g)^{abc}\).
3. Coincident Diffie-Hellman (Co-BDH) problem [6]: given \((P, aP, bP, Q)\) for any \(a, b \in \mathbb{Z}_q^*\) and \(Q \in G_1\), compute \(e(P, Q)^{ab}\).
(4) Codecision bilinear Diffie-Hellman (Co-DBDH) problem [6]: given \((P, aP, bP, Q, Z)\) for any \(a, b \in \mathbb{Z}_p\), \(Q \in G_1\) and \(Z \in G_2\), decide whether \(Z = e(P, Q)^{ab}\).

(5) Codecision bilinear Diffie-Hellman (Co-DBDH) assumption [5]: an algorithm \(B\) with an output \(\beta \in \{0, 1\}\) has advantage \(\varepsilon\) in solving the Co-DBDH problem if
\[
\left| \Pr \left[ B(P, aP, bP, Q, e(P, Q)^{ab}) = 1 \right] - \Pr \left[ B(P, aP, bP, Q, Z) = 1 \right] \right| \geq \varepsilon
\]

(6) Given two groups \(G_1\) and \(G_2\) of the same prime order \(q\), \((P, aP, \alpha P, \ldots, \alpha^k P), \alpha \in \mathbb{Z}_p^*, \) a generator \(P\) of \(G_1\), and a bilinear map \(e: G_1 \times G_1 = G_2, q\)-bilinear Diffie-Hellman inversion \((q\text{-BDHI})\) problem is to compute \(e(P, P)^{1/\alpha}\).

(7) Given two groups \(G_1\) and \(G_2\) of the same prime order \(q\), \((P, aP, y), \alpha \in \mathbb{Z}_p^*, y \in \mathbb{Z}_p^*, \) a generator \(P\) of \(G_1\), and a bilinear map \(e: G_1 \times G_1 = G_2\), the modified bilinear inverse Diffie-Hellman (mBIDH) problem is to compute \(e(P, P)^{1/(\alpha+\gamma)}\).

2.4. Security Definition. According to the works [3, 5, 6], a general model and security formalization problem is given. Security formalization problem is indistinguishability encryptions of chosen ciphertext attacks, under selective multi-ID (IND-CCA-sMID for short) [5, 6]. The notion of IND-CCA-sMID is given as follows.

Definition 1 (IND-CCA-sMID) [5, 6]. Let \(A\) be a polynomial-time algorithm attacker. Symbol \(\|\) denotes a general multireceiver IBE scheme. Attacker \(A\) interacts with the challenger in the following steps.

Setup. The challenger executes the setup algorithm. Attacker \(A\) attains the resulting public parameters from challenger. The attacker does not know any information about private key. The challenger keeps the master key secret.

Phase 1. \(A\) outputs multiple targets identities \((id_1, \ldots, id_t)\) where \(t\) denotes a positive integer.

Phase 2. \(A\) publishes private key extraction queries. When a private key extraction query with identity \(id_i\) is received, the challenger obtains private key \(\delta_j = \text{Extract}(\text{params}, s, id_i)\) by running the private key extraction algorithm. The only constraint is that \(id_i \neq id_j\) for \(i = 1, \ldots, t\).

Phase 3. \(A\) publishes decryption queries for target identity information. When a decryption query denoted by \((C^*, id_t)\) for some \(t \in \{1, 2, \ldots, t\}\) is received, the challenger creates a private key which is denoted by \(d\), associated with identity information \(id_i\). The challenger returns the information \(D = \text{Decrypt}(\text{params}, C^*, id_t, d)\) to \(A\).

Challenge. \(A\) outputs a target plaintext message pair \((M_0, M_1)\); the challenger randomly selects \(\beta \in \{0, 1\}\) and creates a target ciphertext information \(C = \text{Encrypt}(\text{params}, id_1, \ldots, id_t, M_\beta)\). Ciphertext \(C\) is given to \(A\) by the challenger.

Phase 4. \(A\) publishes the private key extraction queries and decryption queries for target identities, and query methods are the same as in phase 2 and phase 3, respectively. Restrictive condition is that \(C^* \neq C\).

Guess. To the end, \(A\) outputs the result of conjecture \(\beta\) \(\in\{0, 1\}\). We can say that \(A\) wins the game if \(\beta = \beta\). \(A\)’s conjecture advantage is defined as follows:
\[
\text{Adv}_{1}^{\text{IND-CCA-sMID}}(A) = \left| \Pr \left( \beta = \beta^* \right) - \frac{1}{2} \right|.
\]

Our scheme \(\|\) is said to be \((\tau, e)\)-IND-CCA-sMID secure if the conjecture advantage \(\text{Adv}_{1}^{\text{IND-CCA-sMID}}(A)\) of any attacker \(A\) with polynomial running time \(\tau\) is less than \(e\).

A breaks IND-CCA-sMID of \(\|\) with \((\tau, q_1, q_2, e)\) if and only if the conjecture advantage of the attack \(A\) is not less than \(e\) with the running time \(\tau, q_1, q_2\) denote the number of private key extraction queries and decryption queries, respectively. Scheme \(\|\) is said to be \((\tau, q_1, q_2, e)\)-IND-CCA-sMID secure if there is no polynomial-time algorithm attacker \(A\) with \((\tau, q_1, q_2, e)\) that can break IND-CCA-sMID of scheme \(\|\).

3. The Proposed Encryption Scheme

In this section, we introduce a novel anonymous multireceiver IBE on the basis of offline/online encryption. Our scheme ensures both the confidentiality of the information and the anonymity of the receiver. The process of our encryption scheme is given in Figure 1. As shown in Figure 1, the system framework comprises three types of participants: Sender, Receiver, and KGC.

Sender. The sender encrypts the information and sends the ciphertext message to the designed receivers.

Receiver. The receiver can decrypt the ciphertext message according to the private key.

KGC. It is responsible for the generation of receivers’ private keys.

In this section, an anonymous multireceiver online/offline IBE is proposed according to literature [6, 20]. Our encryption scheme usually consists of six algorithms as follows: Setup, Key extract, Offline encryption, Online encryption, and Decryption. In the following, we will describe the processes of our encryption scheme in detail.

Setup Phase. The algorithm works in setup phase as follows:

1. Pick a random value \(s \in \mathbb{Z}_q^*\), and \(P_1 \in G_1\).
2. Compute \(P_{pub} = sP\).
3. Select six one-way hash functions.
\[
H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*, H_2 : \{0, 1\}^* \rightarrow G_1^*, H_3 : G_2 \rightarrow \{0, 1\}^w, H_4 : \{0, 1\}^w \rightarrow \{0, 1\}^w, H_5 : G_2 \parallel \{0, 1\}^w \parallel G_2 \times G_2 \times \cdots \times G_2, z < w, H_6 : G_2 \rightarrow \{0, 1\}^l, l < w, l + z = w.
\]

The symbols \(w, z, l\), and \(l\) are some positive integers. They denote the length of binary data.
Offline Encryption Phase. In this phase, the sender computes the following steps:

(1) Compute \( Q_i = H_i(id_i) \).
(2) Compute the secret key \( d_i \) for the identity \( id_i \) of the receiver as
\[
d_i = (d_{i1}, d_{i2}) = \left( s(Q_i + P_i), \frac{1}{H(id_i) + s} \right)
\] (6)

Online Encryption Phase

(1) According to the identity information, compute each potential receiver’s \( x_i \) and \( Q_i \).
(2) For \( i = 1 \) to \( t \), compute \( x_i = H(id_i) \) and \( Q_i = H_i(id_i) \).
(3) For \( i = 1 \) to \( t \), compute
\[
f_i(x) = \prod_{1 \leq j \leq t, j \neq i} x_i - x_j = a_{i1} + a_{i2}x + \cdots + a_{it}x^{t-1} \] (9)

Inputting message \( M \) and selecting \( t \) identities of the receivers, the sender performs the following steps.

(1) Compute \( V = H_4(K) \parallel H_5(K \parallel M \parallel K_1 \parallel \cdots \parallel K_t) \oplus H_6(e(P_{pub}, P_i)^y) \) and separate \( H_5(K \parallel M \parallel K_1 \parallel \cdots \parallel K_t) \) to obtain \( H_5(K \parallel M \parallel K_1 \parallel \cdots \parallel K_t) \) or not. Decrypted message \( M' \) is message \( M \) if equality holds.

4. Security and Performance Analysis

In Section 4, we first give the correctness analysis of our scheme, and then we compare security and computational cost with the previous literatures [5, 6, 8, 9].

4.1. Security Analysis. In Section 4.1, the correctness and security of our encryption scheme are analyzed.
4.1.1. Correctness. For each authorized receiver, it can decrypt the ciphertext by the following way. First, it can compute $K'$ and then recover the message $M'$ in the following way:

$$K' = e(C_i + (C_i P), d_{i2}) = e\left((x P_{pub}) + (xy_i P) + (x (H (id_i) - y_{i1}) P), \frac{1}{H (id_i) + s} P\right)$$

$$= e\left((xsP + xH (id_i) P), \frac{1}{H (id_i) + s} P\right) = e\left((sx + xH (id_i) P), \frac{1}{H (id_i) + s} P\right) = e(P, P)^x = K$$

For each authorized receiver $i (i \in [1, t])$ with identity $id_i$, the receiver $i$ can compute $x_i = H(id_i)$ and structure function $\lambda(x)$. It can obtain $\lambda_i$ using Lagrange interpolating polynomial theorem.

$$\lambda_i = R_1 + x_1 R_2 + \cdots + x_i^{-1} R_i + \cdots + x_t^{-1} R_t$$

$$= (a_{i1} + a_{i2} x_i + \cdots + a_{it} x_i^{-1}) y_i Q_i + \cdots + (a_{t1} + a_{t2} x_t + \cdots + a_{tt} x_t^{-1}) y_t Q_t = y_i Q_i$$

(12)

The receiver can obtain

$$\frac{e(U, d_{i1})}{e(K_i, \lambda_i)} = \frac{e(rP, s(Q_i + P_i))}{e(\alpha P_{pub}, y_i Q_i)} = e(rP, sQ_i) \cdot e(rP, sP_i) = e(P_{pub} Q_i, \alpha P_i)$$

$$= e(sP, Q_i)^T \cdot e(sP, P_i)^T = e(P_{pub}, Q_i)^T = e(P_{pub}, P_i)^T$$

(13)

Thus, the authorized receiver can perform the following steps:

1. $H_2(K) \parallel H_2(K || M || K_1 || \cdots || K_t) = V$ \hspace{1em} $H_2(e(P_{pub}, P_i)^T)$.

2. Separate $H_2(K) \parallel H_2(K || M || K_1 || \cdots || K_t)$ to obtain $H_2(K || M || K_1 || \cdots || K_t)$.

3. Finally, the authorized receiver decrypts the ciphertext $M' = D_{H_2(\{id_{i1}, \{i\}\})}(W)$.

4.1.2. The Confidentiality of Message. In order to decrypt the ciphertext information, the decryptor should know the symmetric secret key $H_2(e(P_{pub}, P_i)^T)$. If decryptor is not an authorized receiver, he/she would deal with the Co-BDH problem to compute $e(P, P)^x$ in order to make our paper rigorous and complete. Theorem 2 is given in detail according to the proving process of papers [5, 6].

**Theorem 2.** Our proposed scheme is $\mathbf{\{\tau, q_{H}, q_{H}, q_{H}, q_{H}, q_{H}, q_{H}, q_{H}, q_{H}, q_{H}, \epsilon\}}$-IND-CCA-sMID secure under the $(\tau', \epsilon')$-co-decision bilinear Diffie-Hellman assumption, where $\epsilon' \geq \epsilon$ and $\tau' = \tau + \epsilon + \epsilon'$. 

**Proof.** Assume that $A$ is a $(\tau, q_{H}, q_{H}, q_{H}, q_{H}, q_{H}, q_{H}, q_{H}, q_{H}, q_{H}, \epsilon)$ attacker that can break our scheme $[\mathbb{1}]$. The challenger $B$ can resolve the Co-BDBDH problem with advantage $\epsilon$ in runtime $\tau'$ by using $A$. According to the Co-BDBDH assumption, the confidentiality of the proposed scheme can be guaranteed.

Assume that $B$ is given the tuple $(q, G_1, G_2, e, n, P, aP, bP, Q, Z)$ as an instance of the Co-BDBDH problem. $B$ simulates the challenging environment in IND-CCA-sMID game for $A$ as follows.

**Phase 1.** Assume that $A$ output is the target identity information $(id_{i1}, id_{i2}, \ldots, id_{it})$ where $t$ is a positive integer.

**Setup.** $B$ sets $P_1 = Q$ and $P_{pub} = bP$. $B$ gives the public parameters $N$ to the attacker $A$ where $N = (q, G_1, G_2, e, n, P, aP, bP, H_1, H_2, H_3, H_4, H_5, H_6)$ and $n$ is a positive integer and denotes the number of all users. Let $T, T_1, T_2, T_3, T_4, T_5, T_6$ store the results of querying hash functions $H_1, H_2, H_3, H_4, H_5, H_6$, respectively.

**H-Query.** Input identity information $id_{i1}$ to $H$. $B$ checks $T$. If there exists $(id_{i1}, x_i)$ in $T$ return $x_i$. Otherwise, do the following steps:

1. (Pick a randomly integer $x_i \in Z_q^*$).
2. (Put $(id_{i1}, x_i)$ to $T$).
3. (Return $x_i$).

**H_1-Query.** Input identity information $id_{i1}$ to $H_1$. $B$ checks the $T_1$. If there exists $(id_{i1}, l_j, Q_j)$ in $T_1$ return $Q_j$. Otherwise, do the following steps:

1. (Pick a randomly integer $l_j \in Z_q^*$).
2. (If $i \in [1, 2, \ldots, t]$ compute $Q_j = l_j P$ else compute $Q_j = l_j P - P_1$).
3. (Put $(id_{i1}, l_j, Q_j)$ to $T_1$).
4. (Return $Q_j$).

**H_2-Query.** Input $Z_j \in G_2$ to $H_2$. $B$ checks the $T_2$. If there exists $(Z_j, \delta_j)$ in $T_2$, return $\delta_j$. Otherwise, do the following steps:

1. (Pick a randomly string $\delta_j \in [0, 1]^w$).
2. (Put $(Z_j, \delta_j)$ to $T_2$ and return $\delta_j$).
$H_6$. Query. Input $Z'_j \in G_2$ to $H_6$. B checks $T_6$. If there exists $(Z'_j, \delta'_j)$ in $T_6$, return $\delta'_j$. Otherwise, do the following steps:

1. Pick a randomly string $\delta'_j \in \{0, 1\}^t$.
2. Put $(Z'_j, \delta'_j)$ to $T_6$ and return $\delta'_j$.

$H_5$. Query. Input $(K'_j, R_j, M_j)$ to $H_5$. B checks $T_5$. If there exists $(K'_j, R_j, M_j, \rho_j, \Gamma_j)$ in $T_5$ where $K'_j, \Gamma_j \in G_2$, $\rho_j \in Z^*_q$, $N_j \in G_2 \times G_2 \times \cdots \times G_2$ return $\rho_j$. Otherwise, do the following steps:

1. Pick a randomly string $\rho_j \in Z^*_q$ and compute $\Gamma_j = \rho_j P$.
2. Put $(Q'_j, N_j, M_j, \rho_j, \Gamma_j)$ to $T_5$ and return $\rho_j$.

$H_4$. Query. Input $\sigma_j \in \{0, 1\}^w$ to $H_4$. B checks $T_4$. If there exists $(\sigma_j, \eta_j)$ in $T_4$, return $\eta_j$. Otherwise, do the following steps:

1. Pick a randomly string $\eta_j \in \{0, 1\}^w$.
2. Put $(\sigma_j, \eta_j)$ to $T_4$ and return $\eta_j$.

Phase 2. A issues private key extraction queries for $id_j$ where $j \in \{1, 2, \ldots, t\}$. B does the following steps:

1. If there exists $(id_j, l_j, Q_j)$ in $T_1$, then compute $d_{j_1} = l_j P_{pub}$; otherwise, pick a randomly integer $l_j \in Z^*_q$ and compute $d_{j_1} = l_j P_{pub}, Q_j = l_j P - P_{1}$.
2. Put $(id_j, l_j, Q_j)$ to $T_1$ and return $d_{j_1}$ to $A$.

Phase 3. A issues decryption query $(C^*, id_i)$ for identity information $id_i$ where $i \in \{1, 2, \ldots, t\}$ and $C^* = (U, K_1, \ldots, K_t, V, W, C_{11}, C_{12}, \ldots, C_{1b})$. B does the following steps:

1. Search $T_2$ to obtain $(K'_i, N_i, M_i, \rho_i, \Gamma_i)$ when $\Gamma'_i = K'_i$.
2. If not found, return “reject” to $A$.
3. Compute $x_i = H(id_i)$.
4. Compute $\lambda_i = R_1 + x_i R_2 + \cdots + x_i^{t-1} R_t$.
5. Compute $\gamma' = V \oplus H_2 \left( e \left( P_{pub}, \rho_i P_i \right) e \left( U, l_i P_{pub} \right) / e \left( K'_i, \lambda_i \right) \right)$ (14).

where

$$e \left( P_{pub}, \rho_i P_i \right) e \left( U, l_i P_{pub} \right) = e \left( sP, \rho_i P_i \right) e \left( U, l_i sP \right) = e \left( \rho_i P, sP_i \right) e \left( U, l_i sP \right) = e \left( U, sP_i \right) e \left( U, l_i sP \right) = e \left( U, s \left( P_i + Q_i \right) \right) = e \left( U, d_{i1} \right)$$ (15).

6. Set $K = K'_i$ and separate $\eta' = H_5(K || M_j || K_1 || \cdots || K_t)$ from $\alpha'$. (5).
7. Test whether $M_j = D_{H_5(\alpha')}(W)$ or not. If not, return “reject” to $A$; else return $M_j$ to $A$.

Challenge. A outputs a plaintext information pair $(M_0, M_1)$. When receiving $(M_0, M_1)$, B does the following steps:

1. Randomly pick $\beta \in \{0, 1\}$.
2. For $i = 1, 2, \ldots, t$ search $T_4$ to obtain $l_i$ according to $id_i$.
3. Set $U = aP = rP$ and $I = Z$.
4. For $i = 1, 2, \ldots, t$ compute

$$f_i(x) = \prod_{1 \leq j \leq t} x - x_j = a_1 + a_2 x + \cdots + a_g x^{t-1}$$ (16)

where $a_j \in Z_q, j \in \{1, 2, \ldots, t\}$.

5. Pick a randomly integer $a_j \in Z_q$. For $i = 1, 2, \ldots, t$ compute

$$R_i = \sum_{j=1}^{t} a_j \gamma_j^{-1} l_j U = \sum_{j=1}^{t} a_j \gamma_j^{-1} r l_j P = \sum_{j=1}^{t} a_j y_j Q_j = \sum_{j=1}^{t} b_j Q_j$$ (17)

6. Compute $K = e(C_{11} + (C_{12} P), d_{12})$.
7. Set $\xi = H_5(K || M_{1b} || K_1 || \cdots || K_t)$, where $\xi \in \{0, 1\}^2$ and create a target ciphertext information $C$, where $C = (U, K_1, K_2, \ldots, K_t, H_4(K) || \xi \oplus H_7(I), E_{H_7(I)}(M_{1b}))$.
8. Return $C$ to attacker $A$.

Phase 4. A publishes private key extraction and decryption queries, and they are the same as phases 2 and 3. The constraint condition of decryption queries is that $C^* \neq C$.

Guess. To the end, A outputs the guessing result $\beta' \in \{0, 1\}$. If $\beta' = \beta$ then B outputs 1; else it outputs 0. If $I = e(P, Q)^{\beta}$ then

$$H(K) || \xi \oplus H_7(I) = H_6(K) || \xi \oplus H_7(K) (e(bP, Q)^{\beta}) = H_6(K) || \xi \oplus H_7 \left( e \left( P_{pub}, P_i \right) \right)$$ (18)

That is to say, $C$ is a valid ciphertext message. Otherwise, $K$ is a randomized element of $G_2$ and $C$ is invalid. According to the above constructions, B simulates the random oracle hash function $[H, H_1, H_2, H_4, H_5, H_6]$, the private key extraction, and the decryption queries in phases 2, 3, and 4 successfully. So, we have

$$\Pr \left[ B \left( P, aP, bP, Q, e(P, Q)^{\beta} \right) = 1 \right] = \Pr \left[ \beta' = \beta \right]$$ (19)

where $\Pr[\beta' = \beta] - 1/2 \geq \epsilon$, and $Pr[B(P, aP, bP, Q, Z) = 1] = 1/2, Z$ is a random element in $G_2$. Hence, we obtain
Theorem 3. Our scheme satisfies the anonymity of receiver if the Co-DBDH problem is hard.

In this work, we do not give the proofs of Theorem 3. We can refer to literature [9] and literature [8] for details.

Theorem 4. In the random oracle model, our scheme is IND-CCA2 secure under the q-BDHI and mBIDH assumptions.

This proof is similar to the proof of literature [21, 22]. Please refer to literature [21, 22] for details.

4.2. Performance Analysis. In this section, the computational consumption of our scheme is given. In order to analyze the computational performance, some notations of the symbols are summarized in Table 1.

The implementation environment is on a mobile phone (Samsung Galaxy S5 with a Quad-core 2.45G processor, 2G bytes memory, and the Google Android 4.4.2 operating system) [10]. The implementation runtime results of main operations are listed in Table 2 [10, 23]. The efficiency comparison is summarized in Tables 3 and 4. The computational cost in our scheme is compared to literature [5, 6, 8, 9]. In addition, the mentioned five schemes contain encryption and decryption computational cost. From Table 5, we can see that our scheme is nearly identical to the ciphertext length of other schemes in [5, 6, 8, 9]. As shown from Table 6, our offline/online encryption scheme is the same as literature [8, 9], and encryption schemes of them are anonymous. However, literature [8] and literature [9] do not use the offline/online encryption scheme.

From Tables 3 and 4, we can see that our scheme needs one bilinear pairing operation and three bilinear pairing operations in encryption phase and decryption phase. The number of bilinear pairing operation increases linearly with the number of recipients in encryption and decryption phase.

<table>
<thead>
<tr>
<th>Symbols</th>
<th>Meanings of the symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>The number of all users</td>
</tr>
<tr>
<td>t</td>
<td>The number of authorized receivers, ( t \in [1, n] )</td>
</tr>
<tr>
<td>( C_P )</td>
<td>The computational cost of one bilinear pairing operation</td>
</tr>
<tr>
<td>( C_{Enc} )</td>
<td>The cost of symmetric encryption or decryption one message</td>
</tr>
<tr>
<td>( C_{Sim} )</td>
<td>The computational cost of one scalar multiplication in ( G_1 )</td>
</tr>
<tr>
<td>( C_{Ex-z} )</td>
<td>The computational cost of exponentiation computation in ( Z_q^* )</td>
</tr>
<tr>
<td>( C_{Ma-z} )</td>
<td>The computational cost of multiplication in ( Z_q^* )</td>
</tr>
<tr>
<td>( C_{Ma} )</td>
<td>The computational cost of addition in ( Z_q^* )</td>
</tr>
<tr>
<td>( C_{Add-z} )</td>
<td>The computational cost of addition in ( G_1 )</td>
</tr>
<tr>
<td>( C_{Add} )</td>
<td>The computational cost of one general hash operation</td>
</tr>
<tr>
<td>( C_H )</td>
<td>The computational cost of one hash value</td>
</tr>
<tr>
<td>( C_{H-p} )</td>
<td>The computational cost of one bilinear pairing operation</td>
</tr>
<tr>
<td>( L_{Ecp} )</td>
<td>The length of hash value</td>
</tr>
<tr>
<td>( L_H )</td>
<td>The bit length of a plaintext messages</td>
</tr>
</tbody>
</table>

\[
\left| Pr \left[ B(P, aP, bP, Q, e(P, Q)^{ab}) = 1 \right] - Pr \left[ B(P, aP, bP, Q, Z) = 1 \right] \right| \geq \left| \left( \frac{1}{2} \pm \epsilon \right) - \frac{1}{2} \right| \quad (20)
\]

Thus, \( \epsilon \geq \epsilon \) and \( r' = \tau + (qH_1 + qH_2 + q_3)O(\tau_1) + q_3O(\tau_1 + \tau_2) + qH_1O(1) + qH_2O(1) + qH_1O(1) + qH_2O(1), q_{H_1}, q_{H_2}, q_{H_3}, q_{H_4}, q_{H_5}, q_{H_6} \) denote the number of queries to hash function, \( H_1, H_2, H_3, H_4, H_5 \), and \( H_6 \).

4.1.3. The Anonymity of Receivers. Fan et al’s encryption strategy [5] cannot satisfy the anonymity of multireciever. Every legal receiver can easily verify whether anyone is a legal receiver or not. A legal receiver with identity \( id_l \) can compute \( f(H(id_k)) \), where \( id_k \) denotes the identity information of the receiver. If equation \( e(Q_i, f(H(x_k))) = e(Q_k, f(H(x_k))) \) holds, the receiver with identity \( id_k \) is an authorized receiver. In order to achieve multireceiver anonymity, Wang et al. [6] improved the multireceiver anonymous encryption scheme. For a ciphertext, \( Q_i, P_{pub}, r \) are fixed 9 in their scheme. The authorized receiver with identity information \( id_l \) can obtain value \( r \) from decryption process, although the numerical value of symbol \( r \) is randomly generated in encryption stage. If the equation \( e(\lambda(H(id_l)), \nu(H(id_l))) = e(H_1(id_l), P_{pub})^r \) holds, the receiver with identity \( id_l \) also is an authorized receiver. Random number \( r \) can be recovered by symmetric key and message \( M \). Unfortunately, our scheme cannot protect the privacy of the receiver. That is to say, it did not satisfy the anonymity of the receiver.

In our proposed scheme, the above problems are solved. Only the authorized receiver can decrypt ciphertext information. Each receiver does not know whether others are authorized receivers or not. Thus, the privacy of the user can be protected.

Table 1: The notations of the symbols.
Table 2: Computational cost of main operations.

<table>
<thead>
<tr>
<th>Operations</th>
<th>Computational cost (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_P$</td>
<td>32.713</td>
</tr>
<tr>
<td>$C_{H-p}$</td>
<td>33.582</td>
</tr>
<tr>
<td>$C_{Sm}$</td>
<td>13.401</td>
</tr>
<tr>
<td>$C_{\text{Add}}$</td>
<td>0.056</td>
</tr>
<tr>
<td>$C_{\text{Ex-z}}$</td>
<td>0.002</td>
</tr>
<tr>
<td>$C_{\text{Ex}}$</td>
<td>2.249</td>
</tr>
<tr>
<td>$C_{H}$</td>
<td>0.006</td>
</tr>
<tr>
<td>$C_{\text{Enc}}$</td>
<td>0.001</td>
</tr>
<tr>
<td>$C_{\text{Add-z}}$</td>
<td>0.001</td>
</tr>
<tr>
<td>$C_{\text{Mu-z}}$</td>
<td>0.001</td>
</tr>
<tr>
<td>$C_{\text{Mu}}$</td>
<td>0.008</td>
</tr>
</tbody>
</table>

in literature [9]. Bilinear pairing operation requires a lot of calculation consumption. It is not suitable for mobile devices with limited energy. From Table 6, we know that only our scheme uses offline/online encryption.

In order to give an intuitive knowledge, Figures 2 and 3 also describe the computational cost in encryption and decryption schemes, respectively. Symbol $t$ denotes the number of authorized receivers in Figures 2 and 3. According to Tables 2 and 3, we can easily compute the runtime of encryption and decryption scheme at different literatures [5, 6, 8, 9]. The computational cost on encryption and decryption is summarized in Figures 2 and 3, respectively. From Figure 2, we can see that the computational cost in [9] is the least, and our proposed scheme consumes little computation time in encryption. Literature [9] does not use offline/online encryption, and computational cost in our proposed scheme contains runtime of offline encryption and online encryption. When receivers decrypt the ciphertext, our scheme consumes the minimum computation time. As legal receiver $t$ increases, the computational cost increases gradually in Figures 2 and 3.

5. Conclusion

Finally, conclusion and future work are summarized. An anonymous multireceiver online/offline identity-based encryption was proposed in our work. We developed an efficient offline/online encryption scheme which can ensure the anonymity of the receiver. Our scheme divided encryption into two phases: offline and online. A sender can do a lot of preparatory calculations on offline phases, and a receiver can encrypt the message with little computational cost on online phases. The computational cost of the receivers was improved in the proposed scheme. The analysis results demonstrated that our scheme is secure and efficient, and it is suitable for mobile devices. The preparation computation can be done while mobile device is plugged into a power supply. When it is on the move without plugging, it performs the encryption operations with little computational cost.

An interesting future work is that we will pay more attention to anonymous attribute-based encryption using offline/online scheme for mobile devices.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of Interest.

Acknowledgments

The work is supported by the Supporting Fund for Teachers’ Research of Jining Medical University (no. JY2017KJ053), Qing Lan Project of Jiangsu Province, 1311 Talent Plan Foundation of Nanjing University of Posts and Telecommunications, and Doctoral Research Fund of Jining Medical University.
Table 3: The comparisons of computation cost in different encryption schemes.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>The cost of encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Literature [5]</td>
<td>((t + 3)C_H + tC_{HE-p} + \left((t^2 + 1 + (t^2 + 2t - 2)(t - 1)^2)C_{Mu-z} + (t^2 + t + 2)C_{Sm} + C_{Ex} + C_{Ex-z} + \right.)</td>
</tr>
<tr>
<td>Literature [6]</td>
<td>((t + 3)C_H + tC_{HE-p} + \left((t^2 + 1 + (t^2 + 2t - 2)(t - 1)^2)C_{Mu-z} + (2t^2 + t + 1)C_{Sm} + C_{Ex} + tC_{Ex-z} + \right.)</td>
</tr>
<tr>
<td>Literature [8]</td>
<td>((t + 4)C_H + tC_{HE-p} + \left((t^2 + t + (t^2 + 2t - 2)(t - 1)^2)C_{Mu-z} + (t + 1)C_{Sm} + C_{Ex} + tC_{Ex-z} + \right.)</td>
</tr>
<tr>
<td>Literature [9]</td>
<td>((t + 2)C_H + (t + 2)C_{Sm} + tC_p)</td>
</tr>
<tr>
<td>Proposed scheme</td>
<td>(tC_{HE} + tC_{HE-p} + (t - 1)C_{Mu-z} + (t - 1)C_{Sm} + (t - 1)C_{Ex-z} + C_p)</td>
</tr>
</tbody>
</table>

Table 4: The comparisons of computation cost in different decryption schemes.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>The cost of decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Literature [5]</td>
<td>(3C_H + tC_{Sm} + (t - 1)C_{Ex-z} + (t - 1)C_{Add} + 2C_p)</td>
</tr>
<tr>
<td>Literature [6]</td>
<td>(3C_H + (2t - 1)C_{Sm} + 2t - 1)C_{Ex-z} + 2t - 1)C_{Add} + 2C_p)</td>
</tr>
<tr>
<td>Literature [8]</td>
<td>(6C_H + (t - 1)C_{Sm} + (t - 2)C_{Ex-z} + (t - 1)C_{Add} + 2C_p)</td>
</tr>
<tr>
<td>Literature [9]</td>
<td>((t + 2)C_H + (t + 2)C_{Sm} + tC_p)</td>
</tr>
<tr>
<td>Proposed scheme</td>
<td>(6C_H + tC_{Add} + (t - 2)C_{Ex-z} + 3C_p + C_{Ex})</td>
</tr>
</tbody>
</table>

Table 5: The comparisons of ciphertext length in different schemes.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>The length of ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>Literature [5]</td>
<td>((t + 2)L_{EP} + L_{HE} + L_{Enc})</td>
</tr>
<tr>
<td>Literature [6]</td>
<td>((2t + 2)L_{EP} + L_{HE} + L_{Enc})</td>
</tr>
<tr>
<td>Literature [8]</td>
<td>((2t + 1)L_{EP} + L_{HE} + L_{Enc})</td>
</tr>
<tr>
<td>Literature [9]</td>
<td>((t + 2)L_{EP} + L_{HE} + L_{Enc})</td>
</tr>
<tr>
<td>Proposed scheme</td>
<td>((3t + 1)L_{EP} + L_{HE} + L_{Enc})</td>
</tr>
</tbody>
</table>

Table 6: Comparison of different schemes.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Offline/online encryption</th>
<th>Anonymity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Literature [5]</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Literature [6]</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Literature [8]</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Literature [9]</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Proposed scheme</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

References


