Future Generation Computer Systems 99 (2019) 177–185

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Secure and flexible economic data sharing protocol based on ID-based dynamic exclusive broadcast encryption in economic system

Xiaofen Wang [a,b,*], Hong-Ning Dai [c], Ke Zhang [d]

[a] Center for Cyber Security, University of Electronic Science and Technology of China, Chengdu 611731, China
[b] State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China
[c] Department of Information Technology, Macau University of Science and Technology, Macau 0000, China
[d] Department of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

HIGHLIGHTS

- A novel cryptographic terminology, ID-based Dynamic Exclusive Broadcast Encryption (IBDEBE) is proposed.
- The first IBDEBE scheme with constant size private key and ciphertext is constructed.
- Based on the IBDEBE scheme, a secure and efficient economic data sharing protocol is proposed.

ARTICLE INFO

Article history:
Received 7 July 2018
Received in revised form 25 October 2018
Accepted 11 November 2018
Available online 22 February 2019

Keywords:
Broadcast encryption
Data sharing
Identity-based
Economic data
Anonymity

ABSTRACT

Sharing economic data is paramount for improving quality and developing more efficient ways to produce statistics, and making better economic decisions. The economic data is of great importance to the corporations and governments, and they must be protected against the outsiders. Unfortunately, in an economic administration system, a few users may be malicious, or they are at high risk to leak information to the outsiders. Therefore, the economic data must also be protected against these users. The traditional broadcast encryption can provide protected data sharing among honest users. However, it is not efficient when most of the users are honest, and only a small amount of users are malicious. The traditional method is not cost effective, and does not fit to the situation where the set of malicious users dynamically changes either. Meanwhile, in traditional broadcast encryption, the authorized users' identities need to be sent with the ciphertext. The valid users' anonymity is not provided. To solve these problems, in this work, we present a novel cryptographic primitive, i.e. ID-based Dynamic Exclusive Broadcast Encryption (IBDEBE), and based on a hybrid framework (the combination of the exponent-inversion framework and the commutative-blinding framework) we propose an IBDEBE scheme with constant-size private keys and ciphertexts. The IBDEBE scheme is proved to be semi-adaptively semantically secure in the random oracle model. By applying the IBDEBE scheme, a secure economic data sharing protocol is devised, which is efficient and flexible in dynamic honest user groups, and it provides good security properties, i.e. source authenticity, data integrity protection, data access control, resistance to collusion attack and anonymity. We evaluate the performance of our solution with experiments and the results show good computation efficiency.

1. Introduction

Sharing economic data is paramount for improving quality and developing more efficient ways to produce statistics, and making better economic decisions [1]. Some government departments already take a lead in supporting economic data-sharing amongst their reporting organizations. This is helpful as realizing the potential benefits from increased economic data sharing requires such support, particularly to overcome technology issues which disproportionately affect smaller, data-poor organizations, and to regulate more sensible policies. Economic data sharing is also very important among different sections of a corporation, which helps to realize better cooperation and optimized decision.

Economic data is sensitive, and its leakage may lead to deadly problems. For a government, the leakage of economic data may jeopardize national security and cause social instability. For a corporation, the economic data leakage will lead to a drop in the stock price of the company and the loss of users, which will have a direct impact on the economic interests of the company.

* Corresponding author at: Center for Cyber Security, University of Electronic Science and Technology of China, Chengdu 611731, China.
E-mail address: wangxuedou@sina.com (X. Wang).

https://doi.org/10.1016/j.future.2018.11.013
0167-739X/

Therefore, when the economic data is shared, it must be protected against the outsiders [2].

Data access control mechanisms can be implemented in economic data sharing to provide data protection. In the practical applications, two types of access control mechanisms are applied, i.e. the *positive access control mechanism* and the *exclusive access control mechanism*. In the positive access control mechanism, the authorized users of the economic data are set, and these authorized users can access the data; in the exclusive access control mechanism, the unauthorized users are set, and the users who are not in this unauthorized user set can access the data, while those in the set cannot.

To implement the positive access control, traditional public key broadcast encryption [3–6] or identity-based broadcast encryption [7–10] can be used. In the traditional public key broadcast encryption schemes, an encrypter can create an encryption for a set of authorized users using their public keys. Broadcast encryption was extended to identity-based broadcast encryption in [7–10], where ciphertexts are created using the users' identities. These schemes have constant-size private keys and ciphertexts, and the size of the public system parameters is linearly proportional to the number of total users. The broadcast encryption scheme [6], where the public parameters and the users' private keys are of constant size, can be easily extended to identity-based broadcast encryption. The length of the ciphertexts generated from these broadcast encryption schemes is linearly proportional to the number of the authorized users. Thus, the ciphertext will be very long when the authorized user set is very large. This mechanism is not practical in controlled economic data access and sharing when the most of the users are honest and authorized, and only a small amount of users are malicious.

In the exclusive access control mechanism, the unauthorized users are set, and the users not in the unauthorized user set can access the data. To implement exclusive access control, in this paper, we put forward a new cryptographic terminology, exclusive broadcast encryption, which is a complementary to the traditional broadcast encryption. In the exclusive broadcast encryption scheme, the encrypter can create an encryption of the data using the unauthorized users' public keys, and the users not in the unauthorized user set can decrypt and recover the data. The idea of exclusive broadcast encryption is similar to the idea of revocation system proposed by Lewko, Sahai and Waters [11], where the ciphertext is computed by using the revoked users' public keys. They also proposed ID-based revocation systems with constant-size public parameters and user private keys, but their ciphertext is linear with the number of revoked users. Therefore, their schemes are not efficient when the number of revoked users is large. The ID-based revocation schemes proposed by Attrapadung and Libert [12] and by Attrapadung, Libert and Panafieu [13] have constant ciphertext, but both suffer from linear extending private keys in the maximum number of revoked users. Another problem is that these schemes [11–13] are not dynamic, i.e. they do not provide any simple and efficient mechanism to update the ciphertexts when revoked users are changed. The only way is to recompute the ciphertext of each data thoroughly. Therefore, in the economic system, these schemes do not fit to the situation where the malicious users are dynamically changed.

1.1. Our contribution

To meet the requirements in implementing the exclusive access control in economic system where the unauthorized users are dynamically changed, we propose a novel cryptographic terminology, ID-based Dynamic Exclusive Broadcast Encryption (IBDEBE), where the unauthorized users are dynamically set and their identities are used as the public keys in computing the ciphertexts. We propose the first IBDEBE scheme with constant size private keys and ciphertexts over bilinear group. The ciphertext is composed of three group elements, and the private key is composed of only two group elements. The scheme is efficiently constructed by using a new hybrid framework, i.e. an exponent-inversion framework (such as $g^{\frac{1}{\alpha+H(ID)}}$) and a commutative-binding framework (such as $(g^{\alpha}H(ID)^{r}, g^{r})$). Our construction is still efficient even when the users are changed. When new honest users are authorized , the original ciphertext does not need to be changed. When new malicious users are revoked, only one exponentiation computation is needed to update the ciphertext. To show the advantages of our proposal, a detailed comparison of the sizes of the public parameters, the private keys and the ciphertexts of our scheme and the traditional revocation schemes [11–13] is made. Based on our IBDEBE scheme, a secure economic data sharing protocol is constructed, which provides source authenticity, data integrity protection, data access control, resistance to collusion attack and anonymity. To show the performance of our protocol, the computation efficiency of our protocol is evaluated.

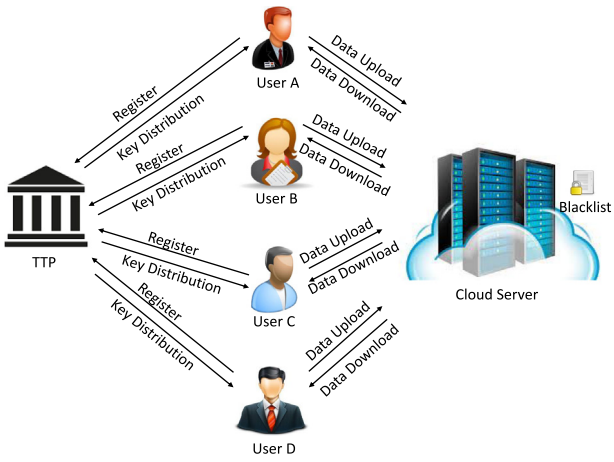


Fig. 1. Private-preserving economic data sharing system.

The paper is organized as follows: in Section 2, we introduce the system framework and the system objectives. In Section 3, the notion of IBDEBE and its security model are formalized, and the preliminaries including bilinear pairing and the security assumptions are introduced. The IBDEBE scheme, its formal security proof and the comparison of this scheme and the traditional revocation schemes are proposed in Section 4. A privacy-preserving economic data sharing protocol is presented in Section 5, followed by its security analysis and performance evaluation in Section 6. We conclude the paper in Section 7.

2. Problem statement

2.1. System framework

We consider the system where a group of users share economic data privately and securely in an economic system as illustrated in Fig. 1. It involves three types of entities in the system: trusted authority (TA), data users, and cloud server.

- *TA. TA* is a fully trusted third party in the system, which provides register service, issues the private keys for the data users and helps to update the ciphertexts in the economic system.
- *Cloud Server.* The cloud server provides data storage service for the economic data users. It evaluates the behavior of

the users and maintains a blacklist which lists all the malicious users and is updated when the list of malicious users change.

- *Data User.* The data user in the economic system can upload the encrypted and signed economic data to the cloud server. The data users can download the data ciphertext and signature from the cloud server, and any honest authorized data user can decrypt the ciphertext and verify the signature.

2.2. Security objectives

To enable authorized data sharing in the economic system, our system should guarantee the following security properties.

Source authenticity. The cloud server can authenticate the sender of the economic data.

Data integrity. The data users can check if there is any modification in the data transmitted. If there is, the data will not be accepted.

Access control. Only the authorized data users can obtain the shared data. None of the outsiders, the malicious users and the cloud server can obtain any information of the outsourced economic data in the system.

Resistance to collusion attack. Even when the malicious users collude, or the malicious users collude with the cloud server, they cannot recover the economic data from the ciphertext.

Anonymity. The malicious data users, the cloud server or the outsiders cannot learn the identities of the authorized users.

3. Definitions and preliminaries

3.1. Definition of ID-based dynamic exclusive broadcast encryption

We first define the syntax of an ID-based Dynamic Exclusive Broadcast Encryption (IBDEBE) and its security notion.

Definition 1. An ID-based Dynamic Exclusive Broadcast Encryption (IBDEBE) consists of the following five algorithms:

$\mathsf{Setup}(1^\lambda, N)$. Taking as input the security parameter 1^λ and the maximum number of malicious users' identities N, it outputs the public parameters *Params* and the master secret key *MSK*. The master key is kept secret.

$\mathsf{KeyGen}(Params, MSK, ID)$. Taking as input the public parameters *Params*, the master secret key *MSK*, and a user identity *ID*, it outputs the private key SK_{ID} for the user.

$\mathsf{Encrypt}(Params, M, S)$. Taking as input the public parameters *Params*, a message M from the message space $\mathcal{M}$, and a set of malicious users' identities $S = [ID_1, ID_2, \ldots, ID_n]$ with $n \leq N$, it outputs a ciphertext CT.

$\mathsf{Update}(Params, MSK, CT, ID')$. Taking as input the public parameters *Params*, the master secret key *MSK*, a ciphertext CT, the original set of malicious users' identities $S = [ID_1, ID_2, \ldots, ID_n]$ and a new set of malicious users' identities $S' = [ID'_1, ID'_2, \ldots, ID'_l]$, it outputs an updated ciphertext CT'.

$\mathsf{Decrypt}(Params, S, CT, ID, SK_{ID})$. Taking as input the public parameters *Params*, a malicious user identity set S, the corresponding ciphertext CT, an identity *ID* and his private key SK_{ID}, it outputs M if $ID \notin S$ or $\perp$ otherwise.

Security notion. The security of an IBDEBE indicates that any user whose identity is in the malicious user identity set cannot retrieve the plaintext message. We formalize the security notion of semi-adaptive indistinguishability against chosen plaintext attack for IBDEBE, which is defined as a security game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

Definition 2. The IBDEBE scheme is (t, q_e, ε)-semi-adaptively indistinguishable against chosen plaintext attack if for any adversary $\mathcal{A}$ who runs in polynomial time t, plays the following game with a challenger $\mathcal{C}$, and makes q_e private key queries has an advantage ε at most in breaking the scheme, where ε is a negligible function of λ.

Setup. $\mathcal{C}$ runs the $\mathsf{Setup}(1^\lambda, N)$ algorithm to generate the system public parameters *Params* and the master secret key *MSK*. Then it sends *Params* to $\mathcal{A}$.

Initiate. $\mathcal{A}$ outputs a malicious user identity set S^* with $|S^*| = n$ and sends it to $\mathcal{C}$.

Phase 1. $\mathcal{A}$ issues private key queries for *ID* with restriction that $ID \in S^*$. $\mathcal{C}$ runs $\mathsf{KeyGen}(Params, MSK, ID)$ to generate the private key SK_{ID} and sends SK_{ID} to $\mathcal{A}$.

Challenge. Once $\mathcal{A}$ decides phase 1 is over, it outputs two distinct messages M_0, M_1 from the same message space $\mathcal{M}$. $\mathcal{C}$ randomly chooses a bit $\sigma \in \{0, 1\}$ and generates the challenge ciphertext CT^* of the message M_σ using the malicious users' identities in S^* for $\mathcal{A}$.

Phase 2. $\mathcal{A}$ issues a number of private key queries as in Phase 1.

Guess. Finally, $\mathcal{A}$ outputs its guess of σ as $\sigma' \in \{0, 1\}$, and wins the game if $\sigma = \sigma'$.

$\mathcal{A}$'s advantage in winning the above game is defined as

$$Adv_{IBDEBE}(\lambda, N) = \left| Prob[\sigma' = \sigma] - \frac{1}{2} \right| .$$

3.2. Bilinear pairing

Let two multiplicative cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ be of the same prime order p, and g, h are generators of $\mathbb{G}$. A bilinear pairing e is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ with properties of bilinearity $e(g^a, h^b) = e(g, h)^{ab}$ for all $g, h \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p^*$, and non-degeneracy $e(g, g) \neq 1$. Let the bilinear group parameters be $\mathbb{BG} = \{p, e, \mathbb{G}, \mathbb{G}_T\}$ and g be the generator.

3.3. Security assumption

The security of the IBDEBE scheme is based on a specific general Decisional Diffie–Hellman (GDDHE) problem introduced by Boneh, Boyen and Goh, i.e. f-GDDHE problem [14]. In the following, we will explain the problem and its intractability.

f-GDDHE problem. Let $(\mathbb{G}, \mathbb{G}_T, e, p)$ be a bilinear group and g be the generator of $\mathbb{G}$. Let n, N be integers satisfying $n \leq N$. An n-degree polynomial f is defined as

$$f(X) = (X + x_1^*)(X + x_2^*) \cdots (X + x_n^*)$$

The following group elements are given.

$$\begin{array}{cccccccc}
g, & g^a, & g^{a^2}, & \ldots, & g^{a^{n-2}}, & \ldots, & g^{a^N}, \\
g^b, & g^{ab}, & g^{a^2 b}, & \ldots, & g^{a^{n-2} b}, & & \\
g^{bc}, & g^{abc}, & g^{a^2 bc}, & \ldots, & g^{a^{n-2} bc}, & \ldots, & g^{a^N bc}, \\
g^{f(a)b}, & g^{f(a)ab}, & g^{f(a)a^2 b}, & \ldots, & g^{f(a)a^{n-2} b}, & \ldots, & g^{f(a)a^N b}, \\
 & & & g^c, g^{cr}, g^{f(a)bcr}, & & & \\
\end{array}$$

where a, b, c are unknown random exponents in $\mathbb{Z}_p$, r is a random element in $\mathbb{Z}_p$, and Z is a group element chosen in $\mathbb{G}_T$. The problem is to decide whether $Z = Z_T = e(g, g)^{a^{n-1} bcr}$ or not. It

outputs "True", if $Z = Z_T$; it outputs "False", if $Z = Z_R$, where Z_R is a random element in $\mathbb{G}_T$ and different from Z_T.

Given the above instance I, the advantage $Adv_{\mathcal{D}}^{GDDHE}(I)$ for an algorithm $\mathcal{D}$ in solving the f-GDDHE problem is defined as

$$Adv_{\mathcal{D}}^{GDDHE}(I) = |Prob[\mathcal{D}(I) = True|Z = Z_T] - Prob[\mathcal{D}(I) = False|Z = Z_R]|,$$

where the probability is over the random choice of generator g in $\mathbb{G}$, the random choice of a, b, c, r in $\mathbb{Z}_p$, and the random choice of Z in $\mathbb{G}_T$.

Theorem 1. *The f-GDDHE problem is a case of the GDDHE hard problem fulfilling the hardness conditions in BBG [14].*

Proof. For simplicity, the f-GDDHE problem is reformulated as

$$D = \begin{pmatrix} 1, & a, & a^2, & \cdots, & a^{n-2}, & \cdots, & a^N, \\ b, & ab, & a^2b, & \cdots, & a^{n-2}b, & & \\ bc, & abd, & a^2bc, & \cdots, & a^{n-2}bc, & \cdots, & a^Nbc, \\ f(a)b, & f(a)ab, & f(a)a^2b, & \cdots, & f(a)a^{n-2}b, & \cdots, & f(a)a^Nb, \\ & & & c, cr, f(a)bcr, & & & \end{pmatrix}$$

$$E = 1,$$

$$P = a^{n-1}bcr.$$

In the following, it will be shown that P is independent of D, E, i.e. no not-all-zero coefficients $\{x_{i,j}\}$ and y exist such that

$$P = a^{n-1}bcr = \sum x_{i,j}d_id_j + y,$$

where $d_i, d_j \in D$.

The above problem can be evaluated in two cases.

In the first case, if $y \neq 0$, the equation $P = a^{n-1}bcr = \sum x_{i,j}d_id_j + y$ will not hold, as y is a constant value in $\mathbb{Z}_p$, while $P = a^{n-1}bcr$ contains no constant value.

In the second case, when $y = 0$, we will show no not-all-zero coefficients $\{x_i, x_j\}$ exist such that $P = a^{n-1}bcr = \sum x_{i,j}d_id_j$. As P contains a fraction of bcr, all possible multiplications of any two elements from D must contain bcr to satisfy the equation. We find only cr and $f(a)bcr$ contain the unknown element r. Therefore, one of d_i and d_j must be chosen from cr and $f(a)bcr$. By listing all possible multiplications in P', where

$$P' = \begin{pmatrix} b \cdot cr, & ab \cdot cr, & \cdots, & a^{n-2}b \cdot cr, & \\ f(a)bcr, & f(a)abcr, & \cdots, & f(a)a^{n-2}bcr, & \cdots, & f(a)a^Nbcr, \end{pmatrix}$$

it is found that no linear combination among the elements from the list P' leads to $P = a^{n-1}bcr$.

Any such linear combination associated with bcr can be written as

$$P = a^{n-1}bcr = F(a)b \cdot cr + G(a) \cdot f(a)bcr,$$

where $F(a)$ and $G(a)$ are polynomials such that $deg(F(a)) \leq n-2$ and $deg(G(a)) \leq N$. We can simplify the above equation as

$$a^{n-1} - F(a) = G(a)f(a).$$

Then we evaluate the following two cases:

Case 1: Suppose $G(a) = 0$. We need to have $a^{n-1} - F(a) = 0$, i.e. $F(a) = a^{n-1}$. It contradicts $deg(F(a)) \leq n-2$.

Case 2: Suppose $G(a) \neq 0$. As $deg(F(a)) \leq n-2$, we have $deg(G(a)f(a)) = deg(a^{n-1} - F(a)) = n-1$. As $deg(f(a)) = n$, we have $deg(G(a)f(a)) \geq n$, which contradicts $deg(G(a)f(a)) = n-1$.

Therefore, there exists no coefficients $\{x_{i,j}\}$ and y such that $P = a^{n-1}bcr = \sum x_{i,j}d_id_j + y$ holds. □

4. Building block: The proposed IBDEBE scheme

In this section, we propose an IBDEBE scheme and formally prove its security.

4.1. Construction of IBDEBE scheme

An ID-based Dynamic Exclusive Broadcast Encryption (IBDEBE) scheme consists of the following five algorithms:

Setup($1^\lambda, N$). Taking as input the security parameter 1^λ and an integer N, the algorithm generates the bilinear group parameters $\mathbb{BG} = \{p, e, \mathbb{G}, \mathbb{G}_T\}$ and a generator $g \in \mathbb{G}$, and chooses a collision resistant hash function $H : \{0,1\} \to \mathbb{Z}_p$. It chooses random exponents $\alpha, \beta, \gamma_1, \gamma_2, \tau_1, \tau_2 \in \mathbb{Z}_p$, such that $\gamma_1\tau_1 = \gamma_2\tau_2$. For $i = 0, 1, \ldots, N$, the algorithm computes $u_i = g^{\gamma_1\beta^i}$. For $i = 0, 1, \ldots, N-1$, the algorithm computes $v_i = g^{\tau_2\beta^i}$. The algorithm computes $w = g^{\gamma_2}$ and $T = e(g,g)^{\alpha\gamma_2}$. The system public parameters *Params* are published as:

$$Params = \left(\mathbb{BG}, g, H, \{u_i\}_{i=0,1,\ldots,N}, \{v_i\}_{i=0,1,\ldots,N-1}, w, T\right).$$

The master secret key $MSK = \{\alpha, \beta, \gamma_1, \gamma_2, \tau_1, \tau_2\}$ is kept secret.

KeyGen(*Params*, *MSK*, *ID*). Taking as input the public parameters *Params*, the master secret key *MSK*, and a user identity $ID \in \{0,1\}^*$, it outputs the private key SK_{ID} as:

$$SK_{ID} = (d_1, d_2) = (g^{\frac{\tau_1}{\beta + H(ID)}}, g^{\alpha + \frac{\tau_2}{\beta + H(ID)}}).$$

Encrypt(*Params*, M, S). Taking as input the public parameters *Params*, a message $M \in \mathbb{G}_T$, and a malicious identity set $S = \{ID_1, ID_2, \ldots, ID_n\}$ with $n \leq N$, the algorithm picks a random $s \in \mathbb{Z}_p$, and computes the ciphertext CT as:

$$CT = (C_1, C_2, C_3) = \left(g^{s \cdot \gamma_1(\beta + H(ID_1))(\beta + H(ID_2))\cdots(\beta + H(ID_n))}, g^{\gamma_2 \cdot s}, M \cdot T^s\right)$$

Update(*Params*, *MSK*, *CT*, *ID*′). Assume the malicious user list is updated. The original malicious user set is $S = \{ID_1, ID_2, \ldots, ID_n\}$, and the new malicious user set is $S' = \{ID'_1, ID'_2, \ldots, ID'_l\}$. Taking as input the public parameters *Params*, the master secret key *MSK*, a ciphertext $CT = (C_1, C_2, C_3)$, and the old and new malicious user sets S and S', it chooses a random element $s' \in \mathbb{Z}_p$, and outputs an updated ciphertext CT' as:

$$CT' = (C'_1, C'_2, C'_3) = \left(C_1^{\frac{s' \cdot (\beta + H(ID'_1))\cdots(\beta + H(ID'_l))}{(\beta + H(ID_1))\cdots(\beta + H(ID_n))}}, \quad C_2^{s'}, \quad C_3^{s'}\right).$$

Decrypt(*Params*, S, *CT*, *ID*, SK_{ID}). Taking as input the public parameters *Params*, a malicious user set S, the corresponding ciphertext *CT*, an identity *ID* and his private key SK_{ID}, it outputs $\perp$ if $ID \in S$. Otherwise, it decrypts the ciphertext as follows.

Firstly it computes a polynomial of x as:

$$f(x) = \prod_{i=1}^{n}(x + H(ID_i)).$$

As $ID \notin S$, we have

$$\frac{f(x)}{x + H(ID)} = \frac{(x+H(ID_1))(x+H(ID_2))\cdots(x+H(ID_n))}{x+H(ID)} = h_{n-1}x^{n-1} + h_{n-2}x^{n-2} + \cdots + h_1x + h_0 + \frac{z}{x+H(ID)},$$

where $z = f(-H(ID)) \neq 0$ and $h_0, h_1, \ldots, h_{n-1}$ are coefficients that can be computed. The plaintext message M can be retrieved as follows.

$$M = C_3 \cdot \left(\frac{e(d_1, C_1)}{e(\prod_{i=0}^{n-1} v_i^{h_i}, C_2)}\right)^{\frac{1}{z}} \cdot \frac{1}{e(d_2, C_2)}.$$

Correctness. In the following, we will show the correctness of decryption in the proposed IBDEBE scheme. Assume that $\gamma_1\tau_1 = \gamma_2\tau_2 = \theta$.

Firstly, we have

$$\begin{aligned}
&\left(\frac{e(d_1, C_1)}{e(\prod_{i=0}^{n-1} v_i^{h_i}, C_2)}\right)^{\frac{1}{z}} \\
=\ &\left(\frac{e(g^{\frac{\tau_1}{\beta+H(ID)}}, g^{s\gamma_1(\beta+H(ID_1))(\beta+H(ID_2))\cdots(\beta+H(ID_n))})}{e(\prod_{i=0}^{n-1} g^{h_i\tau_2\beta^i}, g^{s\gamma_2})}\right)^{\frac{1}{z}} \\
=\ &\left(\frac{e(g,g)^{s\gamma_1\tau_1\cdot\frac{f(\beta)}{\beta+H(ID)}}}{e(g,g)^{s\gamma_2\tau_2(\Sigma_{i=0}^{n-1}h_i\beta^i)}}\right)^{\frac{1}{z}} \\
=\ &\left(e(g,g)^{s\theta(\frac{f(\beta)}{\beta+H(ID)}-\Sigma_{i=0}^{n-1}h_i\beta^i)}\right)^{\frac{1}{z}} \\
=\ &e(g,g)^{s\theta\cdot\frac{z}{\beta+H(ID)}\cdot\frac{1}{z}} \\
=\ &e(g,g)^{\frac{s\theta}{\beta+H(ID)}}.
\end{aligned}$$

and

$$\begin{aligned}
&e(d_2, C_2) \\
=\ &e(g^{\alpha+\frac{\tau_2}{\beta+H(ID)}}, g^{s\gamma_2}) \\
=\ &e(g,g)^{s\alpha\gamma_2}\cdot e(g,g)^{\frac{s\gamma_2\tau_2}{\beta+H(ID)}} \\
=\ &T^s\cdot e(g,g)^{\frac{s\theta}{\beta+H(ID)}}.
\end{aligned}$$

Then we have

$$\begin{aligned}
&C_3\cdot\left(\frac{e(d_1, C_1)}{e(\prod_{i=0}^{n-1} v_i^{h_i}, C_2)}\right)^{\frac{1}{z}}\cdot\frac{1}{e(d_2, C_2)} \\
=\ &M\cdot T^s\cdot e(g,g)^{\frac{s\theta}{\beta+H(ID)}}\cdot\frac{1}{T^s\cdot e(g,g)^{\frac{s\theta}{\beta+H(ID)}}} \\
=\ &M.
\end{aligned}$$

Therefore, by following the decryption algorithm, the plaintext message M can be correctly retrieved.

4.2. Security proof of the IBDEBE scheme

In this section, we prove the security of the proposed IBDEBE scheme.

Theorem 2. *The proposed IBDEBE scheme is semi-adaptively IND-CPA secure if f-GDDHE Problem is intractable for any probabilistic polynomial-time adversary.*

Proof. Suppose there exists a probabilistic polynomial-time adversary $\mathcal{A}$ who can attack our scheme with advantage ϵ in polynomial time τ after making q_e private key queries. We build a simulator $\mathcal{B}$, who simulates the challenger and has advantage Adv^{GDDHE} in solving the *f-GDDHE Problem*.

The simulator $\mathcal{B}$ is given as input the bilinear group parameters $\mathbb{BG} = \{p, e, \mathbb{G}, \mathbb{G}_T\}$, the group generator g and the f-GDDHE instance as:

$$f(X) = (X + x_1^*)(X + x_2^*)\cdots(X + x_n^*),$$

and the group elements

$$g,\quad g^a,\quad g^{a^2},\quad \cdots,\quad g^{a^{n-2}},\quad \cdots,\quad g^{a^N}, \tag{1}$$

$$g^b,\quad g^{ab},\quad g^{a^2b},\quad \cdots,\quad g^{a^{n-2}b}, \tag{2}$$

$$g^{bc},\quad g^{abc},\quad g^{a^2bc},\quad \cdots,\quad g^{a^{n-2}bc},\quad \cdots,\quad g^{a^Nbc}, \tag{3}$$

$$g^{f(a)b},\quad g^{f(a)ab},\quad g^{f(a)a^2b},\quad \cdots,\quad g^{f(a)a^{n-2}b},\quad \cdots,\quad g^{f(a)a^Nb}, \tag{4}$$

$$g^c, g^{cr}, g^{f(a)bcr},\quad Z, \tag{5}$$

We define the polynomials for $i = 1, \ldots, n$ as

$$f_i(X) = \frac{f(X)}{X + x_i^*} = h_{n-1}^i X^{n-1} + h_{n-2}^i X^{n-2} + \cdots + h_1^i X + h_0^i.$$

Without knowing the knowledge of a, we can compute $g^{f_i(a)}$ from the elements in line (1) of the above instance as:

$$g^{f_i(a)} = g^{h_{n-1}^i a^{n-1} + h_{n-2}^i a^{n-2} + \cdots + h_1^i a + h_0^i} = \prod_{j=0}^{n-1}(g^{a^j})^{h_j^i}.$$

$\mathcal{B}$ interacts with $\mathcal{A}$ in the following game:

Setup. $\mathcal{B}$ randomly chooses $x, y \in \mathbb{Z}_p$ and implicitly sets the master private key $MSK = \{\alpha, \beta, \gamma_1, \gamma_2, \tau_1, \tau_2\}$ as

$$\begin{aligned}
&\alpha = x - ya^{n-1}b,\ \beta = a,\quad \gamma_1 = bc,\\
&\gamma_2 = c,\quad \tau_1 = yf(a),\ \tau_2 = yf(a)b.
\end{aligned}$$

It is found that $\gamma_1\tau_1 = \gamma_2\tau_2 = yf(a)bc$. The system public parameters $\{u_i\}_{i=0,1,\ldots,N}$, $\{v_i\}_{i=0,1,\ldots,N-1}$, w, T can be computed as follows:

$$\begin{aligned}
u_i &= g^{\gamma_1\beta^i} = g^{a^ibc},\quad i \in [1, N],\\
v_i &= g^{\tau_2\beta^i} = g^{yf(a)a^ib},\quad i \in [1, N-1],\\
w &= g^{\gamma_2} = g^c,\\
T &= e(g,g)^{\gamma_2\alpha} = e(g^{xc}\cdot g^{-ya^{n-1}bc}, g) = e(g,g)^{(x-ya^{n-1}b)c}.
\end{aligned}$$

We find that the public parameters $\{u_i\}_{i=1,\ldots,N}$, $\{v_i\}_{i=0,1,\ldots,N-1}$ and w come directly from the elements in line (3)–(5) of the above instance, respectively. From g^c in line (5) and $g^{a^{n-1}bc}$ in line (3), we can compute $T = e((g^c)^x\cdot(g^{a^{n-1}bc})^{-y}, g)$. Then $\mathcal{B}$ gives to $\mathcal{A}$ the system public parameters:

$$Params = \left(\mathbb{BG}, g, \{u_i\}_{i=0,1,\ldots,N}, \{v_i\}_{i=0,1,\ldots,N-1}, w, T, H\right),$$

where H is set as a random oracle controlled by $\mathcal{B}$.

Init. The adversary initially sets a malicious user identity set

$$S^* = \{ID_1^*, ID_2^*, \ldots, ID_n^*\}$$

as the challenge target set, where $n(n \le N)$ is the size of the set.

Phase 1. The adversary $\mathcal{A}$ can adaptively issues hash queries and private key queries as follows.

Hash Queries. At any time, $\mathcal{A}$ can make hash query on any identity. To respond the hash query, $\mathcal{B}$ maintains a list $\mathcal{L}_H$ of tuples (ID_i, x_i). The list is initially empty. Upon receiving ID_i, $\mathcal{B}$ firstly looks for it in $\mathcal{L}_H$. If ID_i is already in the list, the corresponding x_i is returned to $\mathcal{A}$. Otherwise, $\mathcal{B}$ responds as follows:

- If $ID_i \notin S^*$, $\mathcal{B}$ randomly picks $x_i \in \mathbb{Z}_p$ as the value of $H(ID_i)$, sends x_i to $\mathcal{A}$ and adds (ID_i, x_i) to $\mathcal{L}_H$;
- If $ID_i \in S^*$, $\mathcal{B}$ sets $H(ID_i) = x_i^*$, where x_i^* is from the polynomial $f(X)$ in the instance of the f-GDDHE problem, and sends x_i^* to $\mathcal{A}$ and adds the new tuple (ID_i, x_i^*) to the list.

Private Key Queries. $\mathcal{A}$ adaptively issues private key queries on any $ID_i \in S^*$. $\mathcal{B}$ responds with the corresponding private key $SK_i = (d_{1_i}, d_{2_i})$ as follows:

$$d_{1_i} = g^{\frac{\tau_1}{\beta+H(ID_i)}} = g^{\frac{yf(a)}{a+x_i^*}} = g^{yf_i(a)} = \prod_{j=0}^{n-1}(g^{h_j^ia^j})^y,$$

$$d_{2_i} = g^{\alpha+\frac{\tau_2}{\beta+H(ID_i)}} = g^{x-ya^{n-1}b+\frac{yf(a)b}{a+x_i^*}} = g^x\cdot\prod_{j=0}^{n-2}(g^{h_j^ia^jb})^y.$$

The private key $SK_i = (d_{1_i}, d_{2_i})$ can be directly computed from the elements in line (1) and (2) of the instance, and it is a valid private key of ID_i.

Challenge. Once $\mathcal{A}$ decides **Phase 1** is over, it outputs two plaintext messages M_0 and M_1 from the same message space. $\mathcal{B}$ picks a random bit $\sigma \in \{0, 1\}$ and computes the challenge ciphertext

Table 1
Comparison of identity-based broadcast encryption schemes.

Schemes	*Params*	Private Key	Ciphertext	Dynamics
LSF [11]	$4\mathbb{G}+\mathbb{G}_T$	$3\mathbb{G}$	$(2n+1)\mathbb{G}+\mathbb{G}_T$	No
AL [12]	$(2N+1)\mathbb{G}+\mathbb{G}_T$	$(N+2)\mathbb{G}$	$3\mathbb{G}+\mathbb{G}_T$	No
ALP [13]	$(N+1)\mathbb{G}+\mathbb{G}_T$	$(N+1)\mathbb{G}$	$2\mathbb{G}+\mathbb{G}_T$	No
Ours	$(2N+3)\mathbb{G}+\mathbb{G}_T$	$2\mathbb{G}$	$2\mathbb{G}+\mathbb{G}_T$	Yes

of M_σ as

$$CT^* = (C_1^*, C_2^*, C_3^*) = \left(g^{f(a)bcr}, g^{cr}, e(g^x, g^{cr}) \cdot Z^{-y} \cdot M_\sigma\right).$$

The challenge ciphertext CT^* is computed from the elements in line (5) of the instance.

Let r be the random value for the encryption. If $Z = e(g,g)^{a^{n-1}bcr}$, we have

$$\begin{aligned} C_1^* &= g^{f(a)bcr} = g^{r\cdot bc(a+x_1^*)(a+x_2^*)\cdots(a+x_n^*)} \\ &= g^{r\cdot\gamma_1(\beta+H(ID_1^*))(\beta+H(ID_2^*))\cdots(\beta+H(ID_n^*))}, \\ C_2^* &= g^{cr} = (g^{\gamma_2})^r, \\ C_3^* &= e(g^x, g^{cr}) \cdot Z^{-y} \cdot M_\sigma = e(g^x, g^{cr}) \cdot e(g,g)^{-ya^{n-1}bcr} \cdot M_\sigma \\ &= e(g,g)^{(x-ya^{n-1}b)cr} \cdot M_\sigma = T^r \cdot M_\sigma. \end{aligned}$$

Therefore, if $Z = e(g,g)^{a^{n-1}bcr}$, the ciphertext is an encryption of the message M_σ under the system public parameters *Params* for S^*.

Phase 2. $\mathcal{A}$ continues to issue hash queries and private key queries, and $\mathcal{B}$ responds as in **Phase 1**.

Guess. Finally, $\mathcal{A}$ outputs its guess $\sigma' \in \{0,1\}$. $\mathcal{B}$ outputs 1, if $\sigma = \sigma'$; otherwise, it outputs 0.

This completes the simulation of the attack, and it is not hard to verify that the simulation is indistinguishable from the real attack.

If $Z = e(g,g)^{a^{n-1}bcr}$, according to the assumption, we have

$$Prob[\sigma = \sigma' | Z = e(g,g)^{a^{n-1}bcr}] = \varepsilon + \frac{1}{2}.$$

On the other hand, if Z is a random element of $\mathbb{G}_T$, but not equal to $e(g,g)^{a^{n-1}bcr}$, we have

$$Prob[\sigma = \sigma' | Z \in_R \mathbb{G}_T] = \frac{1}{2}.$$

Therefore, the advantage for $\mathcal{B}$ to solve the f-GDDHE problem is

$$\begin{aligned} Adv^{GDDHE} &= \Pr[\sigma = \sigma' | Z = e(g,g)^{a^{n-1}bcr}] - \Pr[\sigma = \sigma' | Z \in_R \mathbb{G}_T] \\ &= \epsilon. \end{aligned}$$

The time cost mainly comes from the point multiplications in $\mathbb{G}$ in the q_e private key queries. Note that there is no abortion during the simulation. Thus $\mathcal{B}$ can solve the f-GDDHE problem in running time which is approximately $\tau + \mathcal{O}(q_e \cdot n)$.

This completes the proof. □

4.3. Comparison of identity-based broadcast encryption schemes

In Table 1, we compare our ID-based dynamic exclusive broadcast encryption scheme with some identity-based encryption with revocation schemes [11–13] in terms of the sizes of the system public parameters *Params*, the sizes of the user private keys, the sizes of the ciphertexts, and the dynamic property. In Table 1, N is the maximal number of malicious unauthorized identities and n is the number of the malicious unauthorized identities in the ciphertext creation.

From Table 1, we find that in our ID-based dynamic exclusive broadcast encryption scheme, the size of the system public parameters is linear in the maximal number of malicious unauthorized identities (denoted by N in this paper). The user's private key and the ciphertext created in our proposed scheme are the shortest and are of constant sizes, and only our scheme provides dynamic property.

5. The privacy-preserving data sharing protocol in the economic system

In this section, we propose a privacy-preserving data sharing protocol in the economic system, where an authorized user in the system can access the shared economic data while its privacy is protected against the outsiders, the malicious users and the cloud server. As explained in Section 2, three types of participants take part in the protocol: the trusted authority (TA), a set of data users and the cloud server. *TA* generates and issues the private keys for the economic data users in the system, and updates the ciphertexts. The cloud server evaluates the data users' behavior, and maintains a blacklist which keeps a record of the current malicious users. The protocol consists of five phases: system initiation, user register, data upload, data access and data update. The notations used in the protocol are listed in Table 2.

5.1. System initiation

In this phase, the system parameters of the economic data sharing system are set up by *TA*. *TA* manages the whole system running and maintenance. *TA* first generates its master secret key *MSK* and the system public parameters *Params* by running the Setup algorithm. Then *TA* chooses a signature scheme [15]. *TA* keeps the master secret key *MSK* private and publicizes the system parameters *Params* and the signature scheme.

5.2. User register

Assume N data users will register in the system, where N is an integer. For $t \in [1, N]$, the tth data user U_t with identity ID_t submits a register request and ID_t to *TA*. Upon receiving the register request, *TA* checks the ownership and correctness of the identity ID_t and runs the KeyGen algorithm to generate the private key SK_t. Then *TA* distributes SK_t to U_t through a secure channel.

5.3. User evaluation

In each time period, according to the data users' historic behavior, the cloud server evaluates their honesty and records the malicious data users' identities in a black list. Assume at time period T, the malicious users' identities in the blacklist L_T are $\{ID_1^T, ID_2^T, \ldots, ID_n^T\}$, where $n < N$.

5.4. Data upload

In time period T, the data user U_i of identity ID_i ($i \in [1, n]$) uploads the economic data m_i to the cloud server as follows.

1. The user U_i looks up the blacklist L_T from the cloud server to find the malicious user set $S = \{ID_1^T, ID_2^T, \ldots, ID_n^T\}$.
2. The user U_i runs the Encrypt algorithm to generate the ciphertext CT_i of the economic data m_i by using the malicious users' identities $ID_1^T, ID_2^T, \ldots, ID_n^T$.
3. The user U_i generates a signature of the ciphertext CT_i as $S_{i,T} = \mathsf{Sign}_{SK_i}(CT_i)$ with his private key SK_i.

Table 2
Notations used in the proposed protocol.

Notations	Descriptions
TA	The trust authority.
L_T	The blacklist at time T.
$Params$	The system public parameters.
MSK	TA's master secret key
ID_t	The user U_t's identity.
SK_t	The user U_t's private key.
Sign	The signature algorithm in BLS signature scheme [15].
Verify	The verification algorithm in BLS signature scheme [15].
Setup	The setup algorithm in our proposed broadcast encryption scheme.
KeyGen	The private key generation algorithm in our proposed broadcast encryption scheme.
Encrypt	The encryption algorithm in our proposed broadcast encryption scheme.
Decrypt	The decryption algorithm in our proposed broadcast encryption scheme.
Update	The update algorithm in our proposed broadcast encryption scheme.
m_i	The user U_i's economic data.
CT_i	The ciphertext of m_i.
$S_{i,T}$	The signature of CT_i at time period T.

4. The user U_i transmits $M_{i,T} = CT_i \| S_{i,T} \| ID_i$ to the cloud server. Upon receiving $M_{i,T}$, the cloud server verifies the signature $S_{i,T}$ with U_i's identity ID_i. If it is failed, the cloud server rejects the data; otherwise, it stores the data $M_{i,T}$ in its storage.

5.5. Data access

In time period T, assume the economic data $CT_1 \| S_{1,T} \| ID_1, \ldots, CT_N \| S_{N,T} \| ID_N$ is stored in the cloud server. The data user U_j of identity ID_j ($j \in [1, N]$) acquires the economic data as follows.

1. The data user U_j submits the data request of economic data from the user ID_i as $REQ_i \parallel ID_j$ to the cloud server.
2. The cloud server returns the encrypted data $CT_i \| S_{i,T} \| ID_i$ to the data user U_j.
3. The data user U_j firstly verifies the integrity of the data by running Verify algorithm of the signature scheme [15]. If the output is "False", he rejects the data. Otherwise, if $ID_j \notin [ID_1^T, ID_2^T, \ldots, ID_n^T]$, the user U_j decrypts the ciphertext CT_i with his secret key SK_j by running Decrypt algorithm and recovers the plaintext of the economic data m_i.

5.6. Data update

Assume in time period T', the malicious users are changed in the system. The newly updated identities listed in the blacklist L_T' are $\{ID_1^{T'}, ID_2^{T'}, \ldots, ID_v^{T'}\}$. Then TA needs to update the economic data as follows.

1. TA looks up the old blacklist L_T and the new blacklist L_T' from the cloud server to find the old malicious user set $S = \{ID_1^T, ID_2^T, \ldots, ID_l^T\}$ and the new malicious user set $S' = \{ID_1^{T'}, ID_2^{T'}, \ldots, ID_l^{T'}\}$.
2. TA runs the Update algorithm to generate the new ciphertext CT_i' ($i \in [1, N]$) of the economic data m_i by using the old and new malicious users' identities $\{ID_1^T, ID_2^T, \ldots, ID_l^T\}$ and $\{ID_1^{T'}, ID_2^{T'}, \ldots, ID_l^{T'}\}$, and the original ciphertext CT_i, and then sends the ciphertext CT_i' to the user U_i ($i \in [1, N]$).
3. The user U_i ($i \in [1, N]$) generates a signature of the ciphertext CT_i' as $S_{i,T'} = \mathsf{Sign}_{SK_i}(CT_i')$ with his private key SK_i.
4. The user U_i ($i \in [1, N]$) transmits $M_{i,T'} = CT_i' \| S_{i,T'} \| ID_i$ to the cloud server. Upon receiving $M_{i,T'}$, the cloud server verifies the signature $S_{i,T'}$ with U_i's identity ID_i by running the Verify algorithm. If it is failed, the cloud server rejects the data; otherwise, it stores the data $CT_i' \| S_{i,T'} \| ID_i$ in its storage.

6. Analysis and discussion

6.1. Protocol analysis

In this subsection, we analyze that our privacy-preserving economic data sharing protocol achieves the objectives we mentioned in Section 2.

Source authentication. In our protocol, when the data user uploads data to the cloud server, the data is signed with his private key. According to the *Existential Unforgeability* of the signature scheme [15], without the data user's private key, no other user can forge his valid signature. Therefore, the identity of the data sender can be authenticated.

Data integrity. As the ciphertext of the data is signed with the sender's private key, if there is any modification of the message sent, the signature will not be approved. Therefore, the data integrity is maintained in our protocol.

Access control. As our proposed exclusive broadcast encryption satisfies semi-adaptive IND-CPA security, without any private key of the authorized users, the outsiders, the malicious users, and the cloud server cannot decrypt the ciphertexts of the economic data. Only authorized users with valid private keys can access the economic data. Thus, the data access control is provided in our data sharing protocol.

Resistance to collusion attack. In our proposed exclusive broadcast encryption scheme, the users' private keys are generated by the honest party TA. Even when the malicious users collude, or they collude with the cloud server, they cannot obtain the private key of any authorized user. From the semi-adaptive semantic security of the proposed exclusive broadcast encryption scheme, without the private key of an authorized user, any colluding users or the cloud server cannot access the economic data.

Anonymity. In our protocol, only the malicious data users are listed by the cloud server. The data user who has got a valid private key from TA and is not in the blacklist can decrypt the ciphertext. The outsiders or the malicious users do not know the identities of the users who are sharing the economic data. Therefore, anonymity is achieved.

6.2. Performance evaluation

The experiments are conducted on computers to evaluate the performance of our privacy-preserving data sharing protocol. The computers of the following configurations: Intel Core™ i7-4790 CPU @ 3.60 GHz, 12 GB RAM with Windows 7 64-bit operation system are utilized to simulate the protocol. In the experiments, Stanford Pairing Based Cryptography (PBC) Library [16] is leveraged.

In the experiment, we use the Tate pairing defined over a supersingular elliptic curve $E/\mho_p : y^2 = x^3+x$ with an embedding degree of two. The group $\mathbb{G}$ generated over the elliptic curve $E/\mho_p : y^2 = x^3 + x$ is of order p, where $|\ \mathbb{G}\ | = 160$ bit, $|\ \mathbb{G}_T\ | = 1024$ bit and $|\ \mathbb{Z}_p\ | = 160$ bit.

In the experiment we find that even if the number of malicious users in the protocol increases, the ciphertexts are of constant size. For each piece economic data of 128 bytes, the length of its ciphertext is only 168 bytes, which is very short. From the data sharing protocol, we find that in the data upload phase, the computation cost for the data user is about 16.74 ms; in the data update phase, *TA* only needs 6.423 ms to compute the new ciphertext for each piece of the economic data; in the data access phase, the computation cost for the user to recover the economic data and verify its integrity is about 63.095 ms. If we use a real cloud server in the experiment, the computation cost will be greatly reduced. Therefore, the protocol is very efficient.

7. Conclusion

In this paper, we formalize the definition of ID-based Dynamic Exclusive Broadcast Encryption (IBDEBE) and its security model which captures semi-adaptive IND-CPA security. Based on a hybrid framework (the combination of the exponent-inversion framework and the commutative-blinding framework), we propose a provable semi-adaptively semantic secure IBDEBE scheme, which allows the data sender encrypts the data using the excluded malicious users' public keys, while the authorized honest users can decrypt the ciphertext. When there is any change of the malicious users, *TA* can update the ciphertext with very low cost. Utilizing this IBDEBE scheme as a construction block, we propose a privacy-preserving economic data sharing protocol, where the source authenticity, data integrity, access control, resistance to malicious attack, and anonymity are achieved. Because of the constant size ciphertext, and light weight computation in the data upload, data access and data update phases, our protocol is applicable in practical economic system.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grants U1833122, the foundation from the State Key Laboratory of Integrated Services Networks, Xidian University (No. ISN18-09), and the 6th Innovation and Entrepreneurship Leading Talents Project of Dongguan.

References

[1] G. Bellala, B.A. Huberman, Securing private data sharing in multi-party analytics, First Monday 21 (9) (2016).

[2] C. Zuo, J. Shao, J.K. Liu, G. Wei, Y. Ling, Fine-grained two-factor protection mechanism for data sharing in cloud storage, IEEE Trans. Inf. Forensics Secur. 13 (1) (2018) 186–196.

[3] A. Fiat, M. Naor, Broadcast encryption, in: Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22–26, 1993, Proceedings, 1993, pp. 480–491.

[4] D. Boneh, C. Gentry, B. Waters, Collusion resistant broadcast encryption with short ciphertexts and private keys, in: Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14–18, 2005, Proceedings, 2005, pp. 258–275.

[5] C. Gentry, B. Waters, Adaptive security in broadcast encryption systems (with short ciphertexts), in: Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26–30, 2009. Proceedings, 2009, pp. 171–188.

[6] D. Boneh, B. Waters, M. Zhandry, Low overhead broadcast encryption from multilinear maps, in: Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17–21, 2014, Proceedings, Part I, 2014, pp. 206–223.

[7] C. Delerablée, Identity-based broadcast encryption with constant size ciphertexts and private keys, in: Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2–6, 2007, Proceedings, 2007, pp. 200–215.

[8] J. Kim, W. Susilo, M.H. Au, J. Seberry, Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext, IEEE Trans. Inf. Forensics Secur. 10 (3) (2015) 679–693.

[9] K. He, J. Weng, J. Liu, J.K. Liu, W. Liu, R.H. Deng, Anonymous identity-based broadcast encryption with chosen-ciphertext security, in: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2016, Xi'an, China, May 30–June 3, 2016, 2016, pp. 247–255.

[10] J. Lai, Y. Mu, F. Guo, R. Chen, Fully privacy-preserving ID-based broadcast encryption with authorization, Comput. J. 60 (12) (2017) 1809–1821.

[11] A.B. Lewko, A. Sahai, B. Waters, Revocation systems with very small private keys, in: 31st IEEE Symposium on Security and Privacy, S&P 2010, 16–19 May 2010, Berleley/Oakland, California, USA, 2010, pp. 273–285.

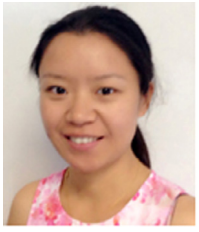
[12] N. Attrapadung, B. Libert, Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation, in: Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26–28, 2010. Proceedings, 2010, pp. 384–402.

[13] N. Attrapadung, B. Libert, E. de Panafieu, Expressive key-policy attribute-based encryption with constant-size ciphertexts, in: Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6–9, 2011. Proceedings, 2011, pp. 90–108.

[14] D. Boneh, X. Boyen, E. Goh, Hierarchical identity based encryption with constant size ciphertext, in: Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22–26, 2005, Proceedings, 2005, pp. 440–456.

[15] D. Boneh, B. Lynn, H. Shacham, Short signatures from the weil pairing, J. Cryptology 17 (4) (2004) 297–319.

[16] B. Lynn, Pairing-Based Cryptography, 2000, https://crypto.stanford.edu/pbc/.



Xiaofen Wang received her Ph.D. and M.S. degrees from Xidian University, Xi'an, China, in 2009 and 2006, respectively. Dr. Wang is currently an associate professor at School of Computer Science and Engineering and Center for cyber security, University of Electronic Science and Technology of China, Chengdu, China. She was also currently a visiting research fellow in Centre for Computer and Information Security, University of Wollongong. Her research interests are public key cryptography and cyber security.

Hong-Ning Dai is an associate professor in Faculty of Information Technology at Macau University of Science and Technology. He obtained the Ph.D. degree in Computer Science and Engineering from Department of Computer Science and Engineering at the Chinese University of Hong Kong. He also received the B.Eng. and M.Eng. degrees in Computer Science and Engineering from South China University of Technology. He also worked in Department of Information Engineering at the Chinese University of Hong Kong and the Hong Kong Applied Science and Technology Research Institute after his Ph.D. study. His research interests include cyber–physical systems,

wireless networks, and distributed systems. He has served as a guest editor of IEEE Transactions on Industrial Informatics and an editor of International Journal of Wireless and Mobile Communication for Industrial Systems. He also served as conference staff members of a number of conferences, including IEEE ICCS, IEEE ANT, ACM MobiHoc, IEEE SCC, IEEE GCC and CIAPR etc. He is a professional member of the Association for Computing Machinery (ACM), a senior member of the Institute of Electrical and Electronics Engineers (IEEE) and a member of IEEE Communications Society.

Ke Zhang received his Ph.D, M.S. and M.Eng. degrees in Computer Science and Engineering from degrees from University of Electronic Science and Technology of China, Chengdu, China., in 2009, 2006 and 2003, respectively. Dr. Zhang is currently an associate professor at School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. He is a member of the Association for Computing Machinery (ACM), and a member of IEEE Communications Society. His research interests are cyber security, big data analysis and Internet of thing.