This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

Conditional Identity-based Broadcast Proxy Re-Encryption and Its Application to Cloud Email

Peng Xu, *Member, IEEE*, Tengfei Jiao, Qianhong Wu, *Member, IEEE*, Wei Wang, *Member, IEEE*,Hai Jin, *Senior Member, IEEE*

Abstract—Recently, a number of extended Proxy Re-Encryptions (PRE), *e.g.* Conditional (CPRE), Identity-Based PRE (IPRE) and Broadcast PRE (BPRE), have been proposed for flexible applications. By incorporating CPRE, IPRE and BPRE, this paper proposes a verstatile primitive referred to as Conditional Identity-based Broadcast PRE (CIBPRE) and formalizes its semantic security. CIBPRE allows a sender to encrypt a message to multiple receivers by specifying these receivers' identities, and the sender can delegate a re-encryption key to a proxy so that he can convert the initial ciphertext into a new one to a new set of intended receivers. Moreover, the re-encryption key can be associated with a condition such that only the matching ciphertexts can be re-encrypted, which allows the original sender to enforce access control over his remote ciphertexts in a fine-grained manner. We propose an efficient CIBPRE scheme with provable security. In the instantiated scheme, the initial ciphertext, the re-encrypted ciphertext and the re-encryption key are all in constant size, and the parameters to generate a re-encryption key is independent of the original receivers of any initial ciphertext. Finally, we show an application of our CIBPRE to secure cloud email system advantageous over existing secure email systems based on Pretty Good Privacy protocol or Identity-Based Encryption.

Index Terms—Proxy Re-Encryption, Cloud Storage, Identity-based Encryption, Broadcast Encryption, Secure Cloud Email

1 Introduction

Proxy Re-Encryption (PRE) [1] provides a secure and flexible method for a sender to store and share data. A user may encrypt his file with his own public key and then store the ciphertext in an honest-but-curious server. When the receiver is decided, the sender can delegate a re-encryption key associated with the receiver to the server as a proxy. Then the proxy re-encrypts the initial ciphertext to the intended receiver. Finally, the receiver can decrypt the resulting ciphertext with her private key. The security of PRE usually assures that (1) neither the server/proxy nor non-intended receivers can learn any useful information about the (re-)encrypted file, and (2) before receiving the re-encryption key, the proxy can not re-encrypt the initial ciphertext in a meaningful way.

Efforts have been made to equip PRE with versatile capabilities. The early PRE was proposed in the traditional public-key infrastructure setting which incurs complicated certificate management [2]. To relieve from this problem, several Identity-based PRE (IPRE) schemes [3], [4], [5], [6], [7], [8] were proposed so that the receivers' recognizable identities can serve as public keys. Instead of fetching and verifying the receivers' certificates, the sender and the proxy just need to know the receivers' identities, which is more convenient in practice.

PRE and IPRE allows a single receiver. If there are more receivers, the system needs to invoke PRE or IPRE multiple times. To address this issue, the concept of Broadcast PRE (BPRE) has been proposed [9]. BPRE works in a similar way as PRE and IPRE but more versatile. In contrast, BPRE allows a sender to generate an initial ciphertext to a receiver set, instead of a single receiver. Further, the sender can delegate a re-encryption key associated with another receiver set so that the proxy can re-encrypt to.

The above PRE schemes only allows the re-encryption procedure is executed in an all-or-nothing manner. The proxy can either re-encrypt all the initial ciphertexts or none of them. This coarse-gained control over ciphertexts to be re-encrypted may limit the application of PRE systems. To fill this gap, a refined concept referred to as Conditional PRE (CPRE) has been proposed. In CPRE schemes [6], [7], [8], [9], [10], [11], [12], [13], a sender can enforce fine-grained re-encryption control over his initial ciphertexts. The sender achieves this goal by associating a condition with a re-encryption key. Only the ciphertexts meeting the specified condition can be re-encrypted by the proxy holding the corresponding re-encryption key.

A recent conditional proxy broadcast re-encryption scheme [14] allows the senders to control the time to re-encrypt their initial ciphertexts. When a sender generates a re-encryption key to re-encrypt an initial ciphertext, the

- *P. Xu, T. Jiao and H. Jin are with Services Computing Technology and System Lab, Cluster and Grid Computing Lab, School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, 430074, China. P. Xu is also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China. E-Mail: {xupeng, M201272784, hjin}@mail.hust.edu.cn.*
- *Q. Wu is with the School of Electronics and Information Engineering, Beihang Univerisity, Beijing, 100191, China and the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China. E-mail: qhwu@xidian.edu.cn.*
- *W. Wang is with Embedded and Pervasive Computing Lab, School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, 430074, China. E-Mail: viviawangww@gmail.com.*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

sender needs to take the original receivers' identities of the initial ciphertext as input. In practice, it means that the sender must locally remember the receivers' identities of all initial ciphertexts. This requirement makes this scheme constrained for the memory-limited or mobile senders and efficient only for special applications.

1.1 Our Contribution

In this paper, we refine PRE by incorporating the advantages of IPRE, CPRE and BPRE for more flexible applications and propose a new concept of Conditional Identity-based Broadcast PRE (CIBPRE). In a CIBPRE system, a trusted Key Generation Center (KGC) initializes the system parameters of CIBPRE, and generates private keys for users. To securely share files to multiple receivers, a sender can encrypt the files with the receivers' identities and file-sharing conditions. If later the sender would also like to share some files associated with the same condition with other receivers, the sender can delegate a re-encryption key labeled with the condition to the proxy, and the parameters to generate the re-encryption key is independent of the original receivers of these files. Then the proxy can re-encrypt the initial ciphertexts matching the condition to the resulting receiver set. With CIBPRE, in addition to the initial authorized receivers who can access the file by decrypting the initial ciphertext with their private keys, the newly authorized receivers can also access the file by decrypting the re-encrypted ciphertext with their private keys. Note that the initial ciphertexts may be stored remotely while keeping secret. The sender does not need to download and re-encrypt repetitively, but delegates a single key matching condition to the proxy. These features make CIBPRE a versatile tool to secure remotely stored files, especially when there are different receivers to share the files as time passes.

We define a practical security notion for CIBPRE systems. Intuitively, without the corresponding private keys, one can learn nothing about the plaintext hidden in the initial or re-encrypted CIBPRE ciphertext; an initial ciphertext can not be correctly re-encrypted by a re-encryption key if the ciphertext and the key are associated with different conditions. We formally define these security requirements via the standard indistinguishability under selective-ID and Chosen Plaintext Attack (IND-sID-CPA). We model the adversarial deployment environment via a game between a challenger and an attacker trying to break a CIBPRE scheme. Both the challenger and the attacker are modeled as Probabilistically Polynomial Time (PPT) algorithms. If the attacker has only negligible advantage to win in this game, then the CIBPRE scheme is IND-sID-CPA secure.

We propose an efficient CIBPRE that is provably secure in the above adversary model. We prove that the IND-sID-CPA security of the proposed CIBPRE scheme if the underlying identity-based broadcast encryption (IBBE) scheme is secure and the Decisional Bilinear Diffie-Hellman (DBDH) assumption holds. Our proposed CIBPRE scheme enjoys constant-size initial and re-encrypted ciphertexts, and eliminates the constraints of the recent work in [14].

1.2 Cloud Email System: A Promising Application

Cloud email system allows an enterprise to rent the cloud SaaS service to build an email system. It is much cheaper and scalable than traditional on-premises solution. In 2014, the Radicati Group [17] showed the worldwide revenue forecast for Cloud Business Email, from 2014 to 2018. Fig. 1 shows that the Cloud Business Email market is expected to generate nearly 17 billion by 2018.

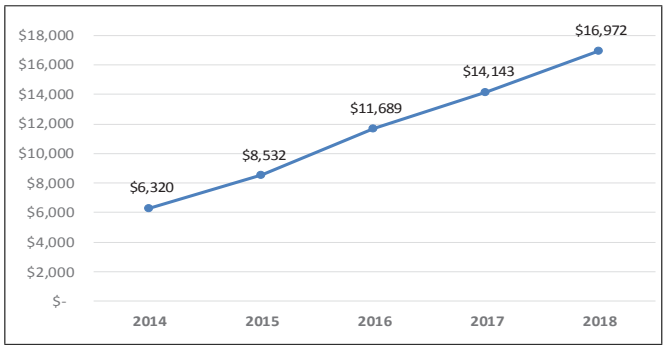


Fig. 1. The worldwide revenue forecast for Cloud Business Email (unit: Million) [17].

In 2012, the Proofpoint Group [18] used an economic model that estimates opportunities for quantifiable cost savings of cloud email system compared with traditional on-premises email system. The Proofpoint model calculates expenses for both systems at the time of acquisition as well as over a four-year period, such as software licensing costs, hardware and storage costs, service expenses, operational expenses. Table 1 summarizes savings using the economic model. Note that NAS (Network Attached Storage) and CAS (Content-addressable storage) in this table are two different technologies which are usually applied in many storage systems.

TABLE 1
Cloud-based archiving vs. on-premises archiving [18].

Number of Users	Storage Technology	On-Premises Costs, Including Labor	SaaS Costs, Including Labor	Total Cost Savings Through Proofpoint SaaS
5,000	NAS	$2,108,300	$1,097,488	48%
10,000	CAS	$23,259,600	$1,986,232	92%
20,000	CAS	$45,829,200	$3,634,976	93%
30,000	CAS	$69,357,200	$5,454,975	93%

Cloud email system is a promising and important application due to its advantageous features. We build an encrypted cloud email system with CIBPRE. It allows a user to send an encrypted email to multiple receivers, store his encrypted emails in an email server, review his history encrypted emails, forward his history encrypted emails of the expected subject to multiple new

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

receivers. Moreover, the cost of an extra email header to achieve this goal is the constant. Compared with existing approaches such as Privacy Good Privacy (PGP) protocol [15] and Identity-Based Encryption (IBE) [16], our CIBPRE-based system is implementation-friendly and more efficient in communication.

In PGP, a sender first verifies a receiver's certificate and encrypts an email by the receiver's public key; then the receiver decrypts the received email with his private key. IBE avoids the certificate verification of PGP. Using IBE, a sender directly encrypts an email using a receiver's email address. Though both PGP and IBE keep the security of cloud email, their performances are less than CIBPRE. When a sender wants to send an encrypted email to multiple receivers, the size of the ciphertext generated by CIBPRE is constant. In contrast, both PGP and IBE cause the size linear with the number of receivers. When a sender wants to forward a historically encrypted email to multiple receivers, CIBPRE only requires the sender to generate a re-encryption key (with constant size) and send the key to cloud, and then the cloud re-encrypts the email and generates a constant size ciphertext for these receivers. In contrast, with PGP or IBE, the sender must fetch the historically encrypted email from the cloud and decrypt it, and then re-encrypt it again to these receivers one by one. Therefore, CIBPRE is very suitable for building encrypted cloud email systems and our proposed CIBPRE scheme is more convenient than PGP and IBE to keep the security of cloud email system.

1.3 Related Work

The first PRE scheme was proposed by Blaze, Bleumer and Strauss in [1]. Following this seminal work, a number of PRE schemes [19], [20], [21], [22], [23], [24], [25] have been proposed in the traditional public key setting. These PRE schemes need certificates to prove the validity of public keys. A user has to verify the certificates before encrypting a plaintext.

In order to avoid the overhead to verify public keys' certificates, several IPRE schemes [3], [4], [5] have been presented by incorporating the idea of identity-based encryption [16]. The scheme in [3] is proven secure in the random oracle (RO) model in which a hash function is assumed fully random. In contrast, the scheme in [4] is proven secure in the standard model. The scheme in [5] is proven secure in a stronger security sense, i.e., indistinguishability against chosen-ciphertext attack in the standard model.

The above PRE schemes only allow data sharing in a coarse-grained manner. That is, if the user delegates a re-encryption key to the proxy, all ciphertexts can be re-encrypted and then be accessible to the intended users; else none of the ciphertexts can be re-encrypted or accessed by others. This issue is addressed in the recent CPRE schemes [6], [8], [9], [10], [11], [12], [13] allowing fine-grained data sharing. The schemes in [8], [12], [13] are proven secure against chosen-ciphertext attack. The conditional identity-based PRE (CIPRE) schemes in [6], [7], [8] combines the underlying ideas of CPRE and IPRE. Similarly, the two conditional broadcast PRE (CBPRE) schemes in [9] combines the notions of CPRE and broadcast encryption, and are secure against chosen-plaintext attacks and chosen-ciphertext attacks, respectively. In addition to fine-grained data sharing, an extra advantage of these CBPRE schemes is that it allows one to share data with multiple users in a more efficient way.

Several other optional properties have been achieved in recent PRE schemes. The PRE schemes in [13], [24], [25] are equipped with an extra property that the receiver of a ciphertext is anonymous. The schemes in [26], [27] achieve multi-use bidirectional re-encryption. A ciphertext can be re-encrypted multiple times. Moreover, a re-encryption key realizes the bidirectional share between two users. Specifically, if Alice delegates a re-encryption key to a proxy for re-encrypting her ciphertexts to Bob. The re-encryption key can also enable to re-encrypt Bob's ciphertexts to Alice. These two PRE schemes are provably secure under the chosen-ciphertext attack respectively in the random oracle and standard models. In contrast, the PRE scheme in [21] is multi-use unidirectional PRE schemes in which bidirectional re-encryption is forbidden. The work in [28] defines a general notion for PRE, which is called deterministic finite automata-based functional PRE (DFA-based FPRE), and proposes a concrete DFA-based FPRE system. The recent work in [29] proposes cloud-based revocable identity-based proxy re-encryption that supports user revocation and delegation of decryption rights.

1.4 Organization

Section 2 reviews the IBBE scheme in [30] and its provable security. Section 3 defines the concept of CIBPRE and its semantic security. Based on the IBBE scheme in Section 2, an instance of CIBPRE is proposed in Section 4. Its semantic security is proved in Section 5. Section 6 compares the performance of existing PRE schemes. Section 7 shows the CIBPRE-based cloud email system and its advantages. Section 8 concludes this paper.

2 Reviewing An IBBE Scheme

Our CIBPRE scheme exploits a known IBBE scheme, referred to as the D07 scheme, proposed by Delerablée in [30]. The the D07 scheme is proven secure and has the short private keys and ciphertexts.

2.1 Bilinear Map

Our constructions are built from bilinear maps reviewed below. Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative groups with prime order p, and let g be a generator of $\mathbb{G}$. A bilinear map is a function $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ with following properties:

- Bilinearity: for any $(u, v) \in \mathbb{G}^2$ and $(a, b) \in \mathbb{Z}_p^{*\,2}$, $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$ holds.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

- Non-degeneracy: $\hat{e}(g,g)$ is a generator of $\mathbb{G}_T$.
- Computability: for any $(u,v) \in \mathbb{G}^2$, $\hat{e}(u,v)$ can be efficiently computed.

2.2 D07 Scheme

The D07 scheme consists of algorithms $\mathbf{Setup}_{\text{IBBE}}$, $\mathbf{Extract}_{\text{IBBE}}$, $\mathbf{Enc}_{\text{IBBE}}$ and $\mathbf{Dec}_{\text{IBBE}}$. Let $N \in \mathbb{N}$ be the maximal size of receiver set for one IBBE encryption. These algorithms work as follows:

- $\mathbf{Setup}_{\text{IBBE}}(\lambda, N)$: Given a security parameter $\lambda \in \mathbb{N}$ and N, this algorithm probabilistically constructs a bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, where $\mathbb{G}$ and $\mathbb{G}_T$ are two multiplicative group with prime order p and $|p| = \lambda$, randomly chooses two generators $(g,h) \in \mathbb{G}^2$ and a value $\gamma \in \mathbb{Z}_p^*$, chooses a cryptographic hash function $\mathcal{H} : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$, finally outputs a master public key $\mathbf{PK}_{\text{IBBE}} = (p, \mathbb{G}, \mathbb{G}_T, \hat{e}, w, v, h, h^{\gamma}, \ldots, h^{\gamma^N}, \mathcal{H})$ and a master secret key $\mathbf{MK}_{\text{IBBE}} = (g, \gamma)$, where $w = g^{\gamma}$ and $v = \hat{e}(g,h)$.
- $\mathbf{Extract}_{\text{IBBE}}(\mathbf{MK}_{\text{IBBE}}, ID)$: Given $\mathbf{MK}_{\text{IBBE}}$ and an identity ID, this algorithm outputs the private key $SK_{\text{IBBE}}^{ID} = g^{\frac{1}{\gamma + \mathcal{H}(ID)}}$.
- $\mathbf{Enc}_{\text{IBBE}}(\mathbf{PK}_{\text{IBBE}}, \mathcal{S}, m)$: Given $\mathbf{PK}_{\text{IBBE}}$, a set $\mathcal{S}$ of some identities (where $|\mathcal{S}| \leq N$) and a plaintext $m \in \mathbb{G}_T$, this algorithm randomly picks $k \in \mathbb{Z}_p^*$, and outputs an IBBE ciphertext $C = (c_1, c_2, c_3)$, where $c_1 = w^{-k}$, $c_2 = h^{k \cdot \prod_{ID_i \in \mathcal{S}} (\gamma + \mathcal{H}(ID_i))}$ and $c_3 = v^k \cdot m$.
- $\mathbf{Dec}_{\text{IBBE}}(\mathbf{PK}_{\text{IBBE}}, ID, SK_{\text{IBBE}}^{ID}, C, \mathcal{S})$: given $\mathbf{PK}_{\text{IBBE}}$, an identity ID and its private key SK_{IBBE}^{ID}, an IBBE ciphertext $C = (c_1, c_2, c_3)$, and a set $\mathcal{S}$ of some identities (where $|\mathcal{S}| \leq N$), this algorithm computes

$$K = (\hat{e}(c_1, h^{\Delta_\gamma(ID,\mathcal{S})}) \cdot \hat{e}(SK_{\text{IBBE}}^{ID}, c_2))^{\frac{1}{\prod_{ID_i \in \mathcal{S} \wedge ID_i \neq ID} \mathcal{H}(ID_i)}}$$

with

$$\Delta_\gamma(ID,\mathcal{S}) = \gamma^{-1} \cdot (\prod_{ID_i \in \mathcal{S} \wedge ID_i \neq ID} (\gamma + \mathcal{H}(ID_i)) - \prod_{ID_i \in \mathcal{S} \wedge ID_i \neq ID} \mathcal{H}(ID_i))$$

and finally outputs a plaintext $m = \frac{c_3}{K}$.

In a typical implementation scenario of the D07 scheme, there are a sender, a KGC and some receivers. The KGC runs algorithm $\mathbf{Setup}_{\text{IBBE}}$ to generate a master public key $\mathbf{PK}_{\text{IBBE}}$ and a master secret key $\mathbf{MK}_{\text{IBBE}}$, and then runs algorithm $\mathbf{Extract}_{\text{IBBE}}$ for each receiver to generate their private keys. To securely broadcast a plaintext to these receivers, the sender runs algorithm $\mathbf{Enc}_{\text{IBBE}}$ to generate an IBBE ciphertext and sends it to these receivers. The consistency of the D07 scheme guarantees that these receivers can decrypt out the plaintext by running algorithm $\mathbf{Dec}_{\text{IBBE}}$. In addition, the provable security of the D07 scheme, which will be introduced in the next subsection, guarantees that except for the sender, the KGA and these receivers, no one can learn something about the plaintext in practice. In the aspect of performance, since the generated IBBE ciphertext has the constant size, D07 scheme obtains the high efficiency in communication cost.

2.3 The D07 scheme Security

[30] shown that the D07 scheme has ciphertexts indistinguishability against the selective identity and chosen plaintext attack (IND-sID-CPA). The IND-sID-CPA security means that no PPT adversary can know which one of two plaintexts is linked with an IBBE ciphertext, if the adversary does not know the private keys of the ciphertext's receivers. The IND-sID-CPA security are formally defined as follows.

Definition 1 (IND-sID-CPA Security of IBBE): An IBBE scheme is IND-sID-CPA secure, if any PPT adversary $\mathcal{B}$ has a negligible advantage $Adv_{IBBE,\ \mathcal{B}}^{\text{IND-sID-CPA}}$ to win in the following game:

- **Initialization Phase**: Adversary $\mathcal{B}$ chooses a set $\mathcal{S}^*$ of challenge identities (with $|\mathcal{S}^*| \leq N$) that he wants to attack, and sends $\mathcal{S}^*$ to challenger $\mathcal{C}$.
- **Setup Phase**: Challenger $\mathcal{C}$ runs algorithm $\mathbf{Setup}_{\text{IBBE}}$ to generate a master public key $\mathbf{PK}_{\text{IBBE}}$ and a master secret key $\mathbf{MK}_{\text{IBBE}}$, and sends $\mathbf{PK}_{\text{IBBE}}$ to adversary $\mathcal{B}$.
- **Query Phase 1**: Adversary $\mathcal{B}$ adaptively issues the following query multi-times.
  - Private Key Query $\mathcal{Q}_{\text{IBBE}}^{SK}(ID)$: With the constraint $ID \notin S^*$, challenger $\mathcal{C}$ runs algorithm $\mathbf{Extract}_{\text{IBBE}}(\mathbf{MK}_{\text{IBBE}}, ID)$ to generate the private key SK_{IBBE}^{ID}, and sends SK_{IBBE}^{ID} to adversary $\mathcal{B}$.
- **Challenge Phase**: Adversary $\mathcal{B}$ gives two challenge plaintexts (m_0, m_1) to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ generates a challenge IBBE ciphertext $C^* \leftarrow \mathbf{Enc}_{\text{IBBE}}(\mathbf{PK}_{\text{IBBE}}, \mathcal{S}^*, m_b)$ (where b is randomly chosen in $\{0,1\}$), and sends C^* to adversary $\mathcal{B}$.
- **Query Phase 2**: Adversary $\mathcal{B}$ continuously issues queries as in Query Phase 1.
- **Guess Phase**: Adversary $\mathcal{B}$ outputs a guess $b' \in \{0,1\}$. We say that adversary $\mathcal{B}$ wins if $b' = b$. And let $Adv_{IBBE,\ \mathcal{B}}^{\text{IND-sID-CPA}} = |Pr[b' = b] - \frac{1}{2}|$ be the advantage to win this game.

Based on the General Decisional Diffie- Hellman Exponent (GDDHE) assumption [30], the D07 scheme is proven IND-sID-CPA secure in the RO model, as stated in the following lemma.

Lemma 1: Suppose the $GDDHE$ assumption holds. The D07 scheme is IND-sID-CPA secure in the RO model.

3 Defining CIBPRE and Its Security

A CIBPRE system consists of algorithms $\mathbf{Setup}_{\text{PRE}}$, $\mathbf{Extract}_{\text{PRE}}$, $\mathbf{Enc}_{\text{PRE}}$, $\mathbf{RKExtract}_{\text{PRE}}$, $\mathbf{ReEnc}_{\text{PRE}}$, $\mathbf{Dec\text{-}1}_{\text{PRE}}$ and $\mathbf{Dec\text{-}2}_{\text{PRE}}$. In a typical implementation scenario of a CIBPRE system, a KGA runs algorithms $\mathbf{Setup}_{\text{PRE}}$ and $\mathbf{Extract}_{\text{PRE}}$ respectively to set up a CIBPRE scheme and generate users' private keys according to their identities. A sender runs algorithm $\mathbf{Enc}_{\text{PRE}}$ to encrypt a plaintext, and generate an initial CIBPRE ciphertext which can be decrypted by some intended receivers, and uploads the ciphertext to a server. Let $\mathcal{S}$ be the set of these intended receivers. When a receiver in set $\mathcal{S}$ is online,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

he retrieves the initial CIBPRE ciphertext from the server and runs algorithm $\mathbf{Dec\text{-}1}_{\text{PRE}}$ to decrypt out the plaintext. when a receiver in set $\mathcal{S}$ wants to share the plaintext to several new receivers (who are not in set $\mathcal{S}$), he runs algorithm $\mathbf{RKExtract}_{\text{PRE}}$ to generate a re-encryption key and delegate this key to a proxy. Let $\mathcal{S}'$ be the set of these new receivers. The proxy runs algorithm $\mathbf{ReEnc}_{\text{PRE}}$ to re-encrypt the initial CIBPRE ciphertext and generate a re-encrypted CIBPRE ciphertext. When a receiver in set $\mathcal{S}'$ is online, he retrieves the re-encrypted CIBPRE ciphertext from the proxy and runs algorithm $\mathbf{Dec\text{-}2}_{\text{PRE}}$ to decrypt out the plaintext. The formal definition of CIBPRE is as follows.

Definition 2 (CIBPRE): Let $N \in \mathbb{N}$ be the maximal size of receiver set for one CIBPRE encryption or re-encryption. A CIBPRE scheme consists of following algorithms:

- $\mathbf{Setup}_{\text{PRE}}(\lambda, N)$: Given a security parameter $\lambda \in \mathbb{N}$ and value N, this algorithm outputs a master public key $\mathbf{PK}_{\text{PRE}}$ and a master secret key $\mathbf{MK}_{\text{PRE}}$.
- $\mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID)$: Given $\mathbf{MK}_{\text{PRE}}$ and an identity ID, this algorithm outputs the private key SK_{PRE}^{ID}.
- $\mathbf{Enc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, \mathcal{S}, m, \alpha)$: Given $\mathbf{PK}_{\text{PRE}}$, a set $\mathcal{S}$ of some identities (where $|\mathcal{S}| \leq N$), a plaintext m and a condition α, this algorithm outputs an initial CIBPRE ciphertext C.
- $\mathbf{RKExtract}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK_{\text{PRE}}^{ID}, \mathcal{S}', \alpha)$: Given $\mathbf{PK}_{\text{PRE}}$, an identity ID and its private key SK_{PRE}^{ID}, a set $\mathcal{S}'$ of some identities (where $|\mathcal{S}'| \leq N$) and a condition α, this algorithm outputs a re-encryption key $d_{ID \to \mathcal{S}'|\alpha}$.
- $\mathbf{ReEnc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, d_{ID \to \mathcal{S}'|\alpha}, C, \mathcal{S})$: Given $\mathbf{PK}_{\text{PRE}}$, a re-encryption key $d_{ID \to \mathcal{S}'|\alpha}$, an initial CIBPRE ciphertext C and a set $\mathcal{S}$ of some identities (where $|\mathcal{S}| \leq N$), this algorithm outputs a re-encrypted CIBPRE ciphertext $\tilde{C}$.
- $\mathbf{Dec\text{-}1}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK_{\text{PRE}}^{ID}, C, \mathcal{S})$: Given $\mathbf{PK}_{\text{PRE}}$, an identity ID and its private key SK_{PRE}^{ID}, an initial CIBPRE ciphertext C, and a set $\mathcal{S}$ of some identities (where $|\mathcal{S}| \leq N$), this algorithm outputs a plaintext.
- $\mathbf{Dec\text{-}2}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK_{\text{PRE}}^{ID}, \tilde{C}, \mathcal{S}')$: Given $\mathbf{PK}_{\text{PRE}}$, an identity ID and its private key SK_{PRE}^{ID}, a re-encrypted CIBPRE ciphertext $\tilde{C}$ and a set $\mathcal{S}'$ of some identities (where $|\mathcal{S}'| \leq N$), this algorithm outputs a plaintext.

As usual, a CIBPRE scheme must satisfy the following consistencies:

- For any initial CIBPRE ciphertext $C \leftarrow \mathbf{Enc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, \mathcal{S}, m, \alpha)$ and any private key $SK_{\text{PRE}}^{ID} \leftarrow \mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID)$, if $ID \in \mathcal{S}$, then algorithm $\mathbf{Dec\text{-}1}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK_{\text{PRE}}^{ID}, C, \mathcal{S})$ always outputs the plaintext m.
- For any re-encrypted CIBPRE ciphertext $\tilde{C} \leftarrow \mathbf{ReEnc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, d_{ID \to \mathcal{S}'|\alpha'}, C, \mathcal{S})$ and any private key $SK_{\text{PRE}}^{ID'} \leftarrow \mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID')$, where $d_{ID \to \mathcal{S}'|\alpha'} \leftarrow \mathbf{RKExtract}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, SK_{\text{PRE}}^{ID}, \mathcal{S}', \alpha')$, $C \leftarrow \mathbf{Enc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, \mathcal{S}, m, \alpha)$ and $SK_{\text{PRE}}^{ID} \leftarrow \mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID)$, if $ID \in \mathcal{S} \bigwedge \alpha = \alpha' \bigwedge ID' \in \mathcal{S}'$, then algorithm $\mathbf{Dec\text{-}2}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID', SK_{\text{PRE}}^{ID'}, \tilde{C}, \mathcal{S}')$ always outputs the plaintext m.

The first consistency is straightforward. It means that any initial CIBPRE ciphertext can be correctly decrypted by its intended receivers. The second consistency is a somewhat sophisticated. Its main idea is to define that any correctly re-encrypted CIBPRE ciphertext can be correctly decrypted by its intended receivers. Therefore, to define the second consistency, we must define what is a correctly re-encrypted CIBPRE ciphertext, and define who can correctly decrypt the ciphertext.

For any re-encrypted CIBPRE ciphertext of an initial CIBPRE ciphertext by a re-encryption key, the second consistency defines that the re-encrypted CIBPRE ciphertext is correct, if the generator of the re-encryption key is an intended receiver of the initial CIBPRE ciphertext, and the initial CIBPRE ciphertext and the re-encryption key has the same condition. Also it defines that the correctly re-encrypted CIBPRE ciphertext can be correctly decrypted by the receivers who are defined by the re-encryption key.

We next define the IND-sID-CPA security of CIBPRE. Roughly speaking, the security means that no PPT adversary can decide which one of two plaintexts is encrypted by an initial CIBPRE ciphertext, if he does not know the private keys of the intended receivers both of the initial CIBPRE ciphertext and its re-encrypted CIBPRE ciphertexts. In other words, without the corresponding private keys, an initial CIBPRE ciphertext and its re-encrypted CIBPRE ciphertexts leak nothing about their encrypted plaintext.

The IND-sID-CPA security of CIBPRE defines an attack game between a PPT adversary and a challenger. The attack game consists of several phases. In the initialization phase, the adversary commits a set $\mathcal{S}^*$ of challenge identities and a challenge condition α^* that he wants to attack. In the setup phase, the challenger sets up a CIBPRE scheme. In the challenge phase, the adversary chooses two challenge plaintexts; the challenger randomly chooses one of these two plaintexts, encrypts the chosen plaintext by the committed $\mathcal{S}^*$ and α^* to generate an initial CIBPRE ciphertext (it also is a challenge ciphertext in the attack game), and asks the adversary to decide which one of these two plaintexts is encrypted. Before and after the challenge phase, the adversary is allowed to query some identities' private keys and re-encryption keys. It means that the adversary can collude with some users in practice. But the adversary can not query the private keys of the challenge identities in set $\mathcal{S}^*$ and the private keys which can decrypt the re-encrypted CIBPRE ciphertext of the challenge ciphertext. If the adversary has no advantage to make a correct decision, then we say that the CIBPRE scheme is IND-sID-CPA secure. The details are as follows:

Definition 3 (IND-sID-CPA Security of CIBPRE): We say that a CIBPRE scheme is IND-sID-CPA secure,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

if any PPT adversary $\mathcal{A}$ has a negligible advantage $Adv^{\text{IND-sID-CPA}}_{CIBPRE,\ \mathcal{A}}$ to win in the following game:

- **Initialization Phase**: Adversary $\mathcal{A}$ chooses a set $\mathcal{S}^*$ of challenge identities (where $|\mathcal{S}^*| \leq N$) and a challenge condition α^* that he wants to attack, and sends $\mathcal{S}^*$ and α^* to challenger $\mathcal{C}$.
- **Setup Phase**: Challenger $\mathcal{C}$ runs algorithm $\mathbf{Setup}_{\text{PRE}}(\lambda, N)$ to generate a master public key $\mathbf{PK}_{\text{PRE}}$ and a master secret key $\mathbf{MK}_{\text{PRE}}$, and sends $\mathbf{PK}_{\text{PRE}}$ to adversary $\mathcal{A}$.
- **Query Phase 1**: Adversary $\mathcal{A}$ can adaptively issue the following two kinds of queries multi-times.
  - Private Key Query $\mathcal{Q}^{SK}_{\text{PRE}}(ID)$: With the constraint $ID \notin \mathcal{S}^*$, challenger $\mathcal{C}$ runs algorithm $\mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID)$ to generate the private key SK^{ID}_{PRE}, and sends SK^{ID}_{PRE} to adversary $\mathcal{A}$.
  - Re-Encryption Key Query $\mathcal{Q}^{RK}_{\text{PRE}}(ID, \mathcal{S}', \alpha)$: With the constraint that adversary $\mathcal{A}$ can not query both $\mathcal{Q}^{RK}_{\text{PRE}}(ID, \mathcal{S}', \alpha^*)$ and $\mathcal{Q}^{SK}_{\text{PRE}}(ID')$ for any $\mathcal{S}'$, $ID \in \mathcal{S}^*$ and $ID' \in \mathcal{S}'$, challenger $\mathcal{C}$ runs algorithm $\mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID)$ to generate identity ID's private key SK^{ID}_{PRE}, and then runs algorithm $\mathbf{RKExtract}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK^{ID}_{\text{PRE}}, \mathcal{S}', \alpha)$ to generate a re-encryption key $d_{ID \to \mathcal{S}'|\alpha}$, finally sends $d_{ID \to \mathcal{S}'|\alpha}$ to adversary $\mathcal{A}$.
- **Challenge Phase**: Adversary $\mathcal{A}$ gives two challenge plaintexts (m_0, m_1) to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ generates a challenge ciphertext $C^* \leftarrow \mathbf{Enc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, \mathcal{S}^*, m_b, \alpha^*)$ (where b is randomly chosen in $\{0, 1\}$), and send C^* to adversary $\mathcal{A}$.
- **Query Phase 2**: Adversary $\mathcal{A}$ continuously issues queries as in Query Phase 1.
- **Guess Phase**: Adversary $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$. We say that adversary $\mathcal{A}$ wins if $b' = b$. And let $Adv^{\text{IND-sID-CPA}}_{CIBPRE,\ \mathcal{A}} = |Pr[b' = b] - \frac{1}{2}|$ be the advantage to win this game.

From above definitions, it is easy to see how the capabilities "Identity-based" and "Broadcast" were defined in the concept of CIBPRE. The capability "Conditional" definition is sophisticated. We explain it with more details. Note that both algorithms $\mathbf{Enc}_{\text{PRE}}$ and $\mathbf{RKExtract}_{\text{PRE}}$ take a parameter of condition as one of inputs respectively to generate an initial CIBPRE ciphertext and a re-encryption key. And one can arbitrarily choose a specified condition in each running of these two algorithms. Suppose an initial CIBPRE ciphertext has the specified condition α, and a re-encryption key has the specified condition α'. The second consistency defines that $\alpha = \alpha'$ is one of sufficient conditions to correctly re-encrypt the initial CIBPRE ciphertext by the re-encryption key. In addition, the IND-sID-CPA security defined that if $\alpha \neq \alpha'$, the re-encryption key can not be used to break the initial CIBPRE ciphertext. In other words, if $\alpha \neq \alpha'$, the re-encryption key can not be used to correctly re-encrypt the initial CIBPRE ciphertext.

4 The Proposed CIBPRE Scheme

Referring to the concept of CIBPRE, roughly speaking, both the initial CIBPRE ciphertext and the re-encrypted CIBPRE ciphertext are the IBBE ciphertexts. But it is different with an IBBE scheme that CIBPRE provides algorithms to transform an IBBE ciphertext (corresponding to an initial CIBPRE ciphertext) into another IBBE ciphertext (corresponding to an re-encrypted CIBPRE ciphertext). Moreover, the transformation is correct if it satisfies the consistencies defined by CIBPRE. Therefore, in order to construct a CIBPRE scheme, we refers to the D07 scheme which was reviewed in Section 2. Compared with the D07 scheme, the proposed CIBPRE scheme associates a D07 IBBE ciphertext with a new part to generate an initial CIBPRE ciphertext. This new part will be used to realize the capability "Conditional" of CIBPRE. In addition, it provides some new algorithms, which are respectively to generate a re-encryption key, re-encrypt an initial CIBPRE ciphertext and decrypt a re-encrypted CIBPRE ciphertext. The decryption of an initial CIBPRE ciphertext is the same with the D07 scheme.

The proposed CIBPRE scheme is as follows:

- $\mathbf{Setup}_{\text{PRE}}(\lambda, N)$: Given a security parameter $\lambda \in \mathbb{N}$ and value N (the maximum number of receivers in each encryption), this algorithm probabilistically constructs a bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, where $\mathbb{G}$ and $\mathbb{G}_T$ are two multiplicative group with prime order p ($|p| = \lambda$), randomly chooses $(g, h, u, t) \in \mathbb{G}^4$ and $\gamma \in \mathbb{Z}^*_p$, chooses two cryptographic hash functions $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}^*_p$ and $\mathcal{H}' : \mathbb{G}_T \to \mathbb{G}$, finally outputs a master public key $\mathbf{PK}_{\text{PRE}} = (p, \mathbb{G}, \mathbb{G}_T, \hat{e}, w, v, h, h^{\gamma}, \ldots, h^{\gamma^N}, u, u^{\gamma}, \ldots, u^{\gamma^N}, t, t^{\gamma}, \ldots, t^{\gamma^N}, \mathcal{H}, \mathcal{H}')$ and a master secret key $\mathbf{MK}_{\text{PRE}} = (g, \gamma)$, where $w = g^{\gamma}$ and $v = \hat{e}(g, h)$.
- $\mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID)$: Given $\mathbf{MK}_{\text{PRE}}$ and an identity ID, this algorithm outputs the private key $SK^{ID}_{\text{PRE}} = g^{\frac{1}{\gamma + \mathcal{H}(ID)}}$.
- $\mathbf{Enc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, \mathcal{S}, m, \alpha)$: Given $\mathbf{PK}_{\text{PRE}}$, a set $\mathcal{S}$ of some identities (where $|\mathcal{S}| \leq N$), a plaintext $m \in \mathbb{G}_T$ and a condition $\alpha \in \mathbb{Z}^*_p$, this algorithm randomly picks $k \in \mathbb{Z}^*_p$, and outputs an initial CIBPRE ciphertext $C = (c_1, c_2, c_3, c_4)$, where

$$c_1 = w^{-k},\ c_2 = h^{k \cdot \prod_{ID_i \in \mathcal{S}} (\gamma + \mathcal{H}(ID_i))},$$
$$c_3 = v^k \cdot m,\ c_4 = (u \cdot t^{\alpha})^{k \cdot \prod_{ID_i \in \mathcal{S}} (\frac{\gamma + \mathcal{H}(ID_i)}{\mathcal{H}(ID_i)})}$$

- $\mathbf{RKExtract}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK^{ID}_{\text{PRE}}, \mathcal{S}', \alpha)$: Given $\mathbf{PK}_{\text{PRE}}$, an identity ID and its private key SK^{ID}_{PRE}, a set $\mathcal{S}'$ of some identities (where $|\mathcal{S}'| \leq N$) and a condition $\alpha \in \mathbb{Z}^*_p$, this algorithm randomly picks $(k', s) \in \mathbb{Z}^{*\ 2}_p$, and outputs a re-encryption key $d_{ID \to \mathcal{S}'|\alpha} = (d_1, d_2, d_3, d_4)$, where

$$d_1 = w^{-k'},\ d_2 = h^{k' \cdot \prod_{ID_i \in \mathcal{S}'} (\gamma + \mathcal{H}(ID_i))},$$
$$d_3 = \mathcal{H}'(v^{k'}) \cdot h^s,\ d_4 = SK^{ID}_{\text{PRE}} \cdot (u \cdot t^{\alpha})^{\frac{s}{\mathcal{H}(ID)}}$$

- $\mathbf{ReEnc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, d_{ID \to \mathcal{S}'|\alpha}, C, \mathcal{S})$: Given $\mathbf{PK}_{\text{PRE}}$, a re-encryption key $d_{ID \to \mathcal{S}'|\alpha} = (d_1, d_2, d_3, d_4)$, an ini-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

tial CIBPRE ciphertext $C = (c_1, c_2, c_3, c_4)$, and a set $\mathcal{S}$ of some identities (where $|\mathcal{S}| \leq N$), this algorithm outputs a re-encrypted CIBPRE ciphertext $\tilde{C} = (\tilde{c}_1, \tilde{c}_2, \tilde{c}_3, \tilde{c}_4, \tilde{c}_5)$, where $\tilde{c}_1 = d_1$, $\tilde{c}_2 = d_2$, $\tilde{c}_3 = d_3$, $\tilde{c}_4 = c_4$ and

$$\tilde{c}_5 = c_3 \cdot (\hat{e}(c_1, h^{\Delta_\gamma(ID,\mathcal{S})}) \cdot \hat{e}(d_4, c_2))^{\frac{-1}{\prod_{ID_i \in \mathcal{S} \bigwedge ID_i \neq ID} \mathcal{H}(ID_i)}}$$

with

$$\Delta_\gamma(ID, \mathcal{S}) = \gamma^{-1} \cdot (\prod_{ID_i \in \mathcal{S} \bigwedge ID_i \neq ID}(\gamma + \mathcal{H}(ID_i)) - \prod_{ID_i \in \mathcal{S} \bigwedge ID_i \neq ID} \mathcal{H}(ID_i)).$$

- **Dec-1**$_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK^{ID}_{\text{PRE}}, C, \mathcal{S})$: Given $\mathbf{PK}_{\text{PRE}}$, an identity ID and its private key SK^{ID}_{PRE}, an initial CIBPRE ciphertext $C = (c_1, c_2, c_3, c_4)$, and a set $\mathcal{S}$ of some identities (where $|\mathcal{S}| \leq N$), this algorithm computes

$$K = (\hat{e}(c_1, h^{\Delta_\gamma(ID,\mathcal{S})}) \cdot \hat{e}(SK^{ID}_{\text{PRE}}, c_2))^{\frac{1}{\prod_{ID_i \in \mathcal{S} \bigwedge ID_i \neq ID} \mathcal{H}(ID_i)}}$$

with

$$\Delta_\gamma(ID, \mathcal{S}) = \gamma^{-1} \cdot (\prod_{ID_i \in \mathcal{S} \bigwedge ID_i \neq ID}(\gamma + \mathcal{H}(ID_i)) - \prod_{ID_i \in \mathcal{S} \bigwedge ID_i \neq ID} \mathcal{H}(ID_i))$$

and finally outputs plaintext $m = \frac{c_3}{K}$.

- **Dec-2**$_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID', SK^{ID'}_{\text{PRE}}, \tilde{C}, \mathcal{S}')$: Given $\mathbf{PK}_{\text{PRE}}$, an identity ID' and its private key $SK^{ID'}_{\text{PRE}}$, a re-encrypted CIBPRE ciphertext $\tilde{C} = (\tilde{c}_1, \tilde{c}_2, \tilde{c}_3, \tilde{c}_4, \tilde{c}_5)$, and a set $\mathcal{S}'$ of some identities (where $|\mathcal{S}'| \leq N$), this algorithm computes

$$K = (\hat{e}(\tilde{c}_1, h^{\Delta_\gamma(ID',\mathcal{S}')}) \cdot \hat{e}(SK^{ID'}_{\text{PRE}}, \tilde{c}_2))^{\frac{1}{\prod_{ID_i \in \mathcal{S}' \bigwedge ID_i \neq ID'} \mathcal{H}(ID_i)}}$$

with

$$\Delta_\gamma(ID', \mathcal{S}') = \gamma^{-1} \cdot (\prod_{ID_i \in \mathcal{S}' \bigwedge ID_i \neq ID'}(\gamma + \mathcal{H}(ID_i)) - \prod_{ID_i \in \mathcal{S}' \bigwedge ID_i \neq ID'} \mathcal{H}(ID_i)),$$

computes $K' = \frac{\tilde{c}_3}{\mathcal{H}'(K)}$, and finally outputs plaintext $m = \tilde{c}_5 \cdot \hat{e}(K', \tilde{c}_4)$.

The consistency of the proposed CIBPRE scheme is guaranteed by the following Theorems 1 and 2, which are respectively proved in Fig. 1 and 2.

Theorem 1: For any initial CIBPRE ciphertext $C \leftarrow \mathbf{Enc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, \mathcal{S}, m, \alpha)$ and any private key $SK^{ID}_{\text{PRE}} \leftarrow \mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID)$, if $ID \in \mathcal{S}$, then algorithm $\mathbf{Dec\text{-}1}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK^{ID}_{\text{PRE}}, C, \mathcal{S})$ always outputs the plaintext m.

Theorem 2: For any re-encrypted CIBPRE ciphertext $\tilde{C} \leftarrow \mathbf{ReEnc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, d_{ID \to \mathcal{S}'|\alpha'}, C, \mathcal{S})$ and any private key $SK^{ID'}_{\text{PRE}} \leftarrow \mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID')$, where $d_{ID \to \mathcal{S}'|\alpha'} \leftarrow \mathbf{RKExtract}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK^{ID}_{\text{PRE}}, \mathcal{S}', \alpha')$, $C \leftarrow \mathbf{Enc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, \mathcal{S}, m, \alpha)$ and $SK^{ID}_{\text{PRE}} \leftarrow \mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID)$, if $ID \in \mathcal{S} \bigwedge \alpha = \alpha' \bigwedge ID' \in \mathcal{S}'$, then algorithm $\mathbf{Dec\text{-}2}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID', SK^{ID'}_{\text{PRE}}, \tilde{C}, \mathcal{S}')$ always outputs the plaintext m.

5 Security Proof

Before the security proof of the proposed CIBPRE scheme, we first review the DBDH assumption. This assumption is very popular in the security proof of cryptographic schemes. It has been used in many famous cryptographic schemes, e.g., [31], [32]. This assumption also will be used in our security proof. It is defined as follows.

Definition 4 (The DBDH Assumption): Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative groups with prime order p, and let g be a generator of $\mathbb{G}$. The DBDH problem on the bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is defined as the advantage of any adversary $\mathcal{A}$ to distinguish the following two tuples $(g^a, g^b, g^c, \hat{e}(g, g)^{abc})$ and $(g^a, g^b, g^c, \hat{e}(g, g)^r)$, where a, b, c and r are randomly chosen in $\mathbb{Z}^*_q$. Let $Adv^{IND}_{DBDH,\ \mathcal{A}}$ be the advantage. We say that the DBDH assumption holds, if for any PPT adversary $\mathcal{A}$ the advantage $Adv^{IND}_{DBDH,\ \mathcal{A}}$ is negligible.

In addition to the DBDH assumption, the security of our proposed CIBPRE scheme also relies on the IND-sID-CPA security of the D07 scheme. In other words, the IND-sID-CPA security of the proposed CIBPRE scheme will be reduced to the DBDH assumption and the IND-sID-CPA security of the D07 scheme. Let $\perp$ denote to abort an algorithm. The proof is as follows.

Theorem 3: Suppose that the DBDH assumption holds. Since the D07 scheme is IND-sID-CPA secure in the RO model, the proposed CIBPRE scheme is IND-sID-CPA secure in the RO model.

Proof. Suppose that there is an adversary $\mathcal{A}$ having advantage $Adv^{\text{IND-sID-CPA}}_{CIBPRE,\ \mathcal{A}}$ to break the IND-sID-CPA security of the proposed CIBPRE scheme. To prove this theorem, we will construct an adversary $\mathcal{B}$, who leverages adversary $\mathcal{A}$ to break the IND-sID-CPA security of the D07 scheme with advantage $Adv^{\text{IND-sID-CPA}}_{D07,\ \mathcal{B}}$. Moreover, we will prove that $Adv^{\text{IND-sID-CPA}}_{D07,\ \mathcal{B}} = Adv^{\text{IND-sID-CPA}}_{CIBPRE,\ \mathcal{A}}(1 - T \cdot Adv^{IND}_{DBDH,\ \mathcal{A}} - T \cdot Adv^{\text{IND-sID-CPA}}_{D07,\ \mathcal{A}})$ holds, where value T will be defined latterly.

Let $\mathcal{C}$ be the challenger defined in D07's IND-sID-CPA security. Next, we will describe a game among adversary $\mathcal{A}$, adversary $\mathcal{B}$ and challenger $\mathcal{C}$. In this game, challenger $\mathcal{C}$ tests adversary $\mathcal{B}$'s ability in breaking D07's IND-sID-CPA security; adversary $\mathcal{B}$ also serves as a challenger to test adversary $\mathcal{A}$'s ability in breaking the IND-sID-CPA security of the proposed CIBPRE scheme. So in this game, adversary $\mathcal{B}$ aims to utilize adversary $\mathcal{A}$'s ability to break the IND-sID-CPA security of D07. The details of this game are as follows:

- **Initialization Phase**: Adversary $\mathcal{A}$ chooses a set $\mathcal{S}^*$ of challenge identities (where $|\mathcal{S}^*| \leq N$) and a challenge condition α^* that he wants to attack, and sends $\mathcal{S}^*$and α^* to adversary $\mathcal{B}$, then adversary $\mathcal{B}$ forwards set $\mathcal{S}^*$ to challenger $\mathcal{C}$. In addition, adversary $\mathcal{B}$ prepares the following two tables:
  - $\mathcal{L}_{SK}$ to store the identities which's private keys have been queried by adversary $\mathcal{A}$.
  - $\mathcal{L}_{RK}$ with columns $(Identity, ReceiverSet, Re\text{-}EncryptionKey, Condition)$ to store the related information of the re-encryption keys queried by adversary $\mathcal{A}$.
- **Setup Phase**: This phase consists of two parts: firstly challenger $\mathcal{C}$ generates D07's master public and secret keys for adversary $\mathcal{B}$; secondly adversary $\mathcal{B}$ generates the proposed CIBPRE scheme's master public key for adversary $\mathcal{A}$. In this two parts, three hash functions are modeled as random oracles respectively by challenger $\mathcal{C}$ and adversary $\mathcal{B}$. So above master public keys do not contain any hash function in this proof. The details are as follows:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

For any initial CIBPRE ciphertext $C \leftarrow \mathbf{Enc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, \mathcal{S}, m, \alpha)$ and any private key $SK_{\text{PRE}}^{ID} \leftarrow \mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID)$, we have $C = (c_1, c_2, c_3, c_4)$ and $SK_{\text{PRE}}^{ID} = g^{\frac{1}{\gamma+\mathcal{H}(ID)}}$ without loss of generality, where $c_1 = w^{-k}$, $c_2 = h^{k\cdot\prod_{ID_i\in\mathcal{S}}(\gamma+\mathcal{H}(ID_i))}$, $c_3 = v^k \cdot m$ and $c_4 = u^{k\cdot\prod_{ID_i\in\mathcal{S}}(\frac{\gamma+\mathcal{H}(ID_i)}{\mathcal{H}(ID_i)})}$.
We next prove $\mathbf{Dec\text{-}1}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK_{\text{PRE}}^{ID}, C, \mathcal{S}) = m$ if $ID \in \mathcal{S}$. When $ID \in \mathcal{S}$, we have

$$\begin{aligned}
&(\hat{e}(c_1, h^{\Delta_\gamma(ID,\mathcal{S})}) \cdot \hat{e}(SK_{\text{PRE}}^{ID}, c_2))^{\frac{1}{\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}\mathcal{H}(ID_i)}}\\
&= (\hat{e}(g^{-k\cdot\gamma}, h^{\Delta_\gamma(ID,\mathcal{S})}) \cdot \hat{e}(g^{\frac{1}{\gamma+\mathcal{H}(ID)}}, h^{k\cdot\prod_{ID_i\in\mathcal{S}}(\gamma+\mathcal{H}(ID_i))}))^{\frac{1}{\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}\mathcal{H}(ID_i)}}\\
&= (\hat{e}(g^{-k\cdot\gamma}, h^{\Delta_\gamma(ID,\mathcal{S})}) \cdot \hat{e}(g,h)^{k\cdot\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}(\gamma+\mathcal{H}(ID_i))})^{\frac{1}{\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}\mathcal{H}(ID_i)}}\\
&= (\hat{e}(g,h)^{k\cdot\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}\mathcal{H}(ID_i)})^{\frac{1}{\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}\mathcal{H}(ID_i)}} = v^k
\end{aligned}$$

with

$$\Delta_\gamma(ID,\mathcal{S}) = \gamma^{-1}\cdot(\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}(\gamma+\mathcal{H}(ID_i)) - \prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}\mathcal{H}(ID_i))$$

Since $m = \frac{c_3}{v^k}$, we proved that $\mathbf{Dec\text{-}1}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK_{\text{PRE}}^{ID}, C) = m$ if $ID \in \mathcal{S}$.

Fig. 2. The proof of Theorem 1.

For $d_{ID\to\mathcal{S}'|\alpha'} \leftarrow \mathbf{RKExtract}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID, SK_{\text{PRE}}^{ID}, \mathcal{S}', \alpha')$, let $d_{ID\to\mathcal{S}'|\alpha'} = (d_1, d_2, d_3, d_4)$ without loss of generality, where $d_1 = w^{-k'}$, $d_2 = h^{k'\cdot\prod_{ID_i\in\mathcal{S}'}(\gamma+\mathcal{H}(ID_i))}$, $d_3 = \mathcal{H}'(v^{k'})\cdot h^s$ and $d_4 = SK_{\text{PRE}}^{ID}\cdot(u\cdot t^{\alpha'})^{\frac{s}{\mathcal{H}(ID)}}$. For $C \leftarrow \mathbf{Enc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, \mathcal{S}, m, \alpha)$, let $C = (c_1, c_2, c_3, c_4)$ without loss of generality, where $c_1 = w^{-k}$, $c_2 = h^{k\cdot\prod_{ID_i\in\mathcal{S}}(\gamma+\mathcal{H}(ID_i))}$, $c_3 = v^k\cdot m$ and $c_4 = (u\cdot t^\alpha)^{k\cdot\prod_{ID_i\in\mathcal{S}}(\frac{\gamma+\mathcal{H}(ID_i)}{\mathcal{H}(ID_i)})}$. For $\tilde{C} \leftarrow \mathbf{ReEnc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, d_{ID\to\mathcal{S}'|\alpha'}, C, \mathcal{S})$, we have $\tilde{C} = (\tilde{c}_1, \tilde{c}_2, \tilde{c}_3, \tilde{c}_4, \tilde{c}_5)$, where $\tilde{c}_1 = d_1$, $\tilde{c}_2 = d_2$, $\tilde{c}_3 = d_3$, $\tilde{c}_4 = c_4$, $\tilde{c}_5 = c_3\cdot(\hat{e}(c_1, h^{\Delta_\gamma(ID,\mathcal{S})})\cdot\hat{e}(d_4, c_2))^{\frac{-1}{\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}\mathcal{H}(ID_i)}}$ with

$$\Delta_\gamma(ID,\mathcal{S}) = \gamma^{-1}\cdot(\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}(\gamma+\mathcal{H}(ID_i)) - \prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}\mathcal{H}(ID_i))$$

We next prove $\mathbf{Dec\text{-}2}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID', SK_{\text{PRE}}^{ID'}, \tilde{C}, \mathcal{S}') = m$ if $ID \in \mathcal{S}\bigwedge\alpha = \alpha'\bigwedge ID' \in \mathcal{S}'$. If $ID' \in \mathcal{S}'$, we have

$$K' = (\hat{e}(\tilde{c}_1, h^{\Delta_\gamma(ID',\mathcal{S}')})\cdot\hat{e}(SK_{\text{PRE}}^{ID'}, \tilde{c}_2))^{\frac{1}{\prod_{ID_i\in\mathcal{S}'\bigwedge ID_i\neq ID'}\mathcal{H}(ID_i)}} = v^{k'}$$

with

$$\Delta_\gamma(ID',\mathcal{S}') = \gamma^{-1}\cdot(\prod_{ID_i\in\mathcal{S}'\bigwedge ID_i\neq ID'}(\gamma+\mathcal{H}(ID_i)) - \prod_{ID_i\in\mathcal{S}'\bigwedge ID_i\neq ID'}\mathcal{H}(ID_i))$$

If $ID \in \mathcal{S}\bigwedge\alpha = \alpha'$, we have

$$\begin{aligned}
\tilde{c_5} &= c_3\cdot(\hat{e}(c_1, h^{\Delta_\gamma(ID,\mathcal{S})})\cdot\hat{e}(d_1, c_2))^{\frac{-1}{\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}\mathcal{H}(ID_i)}}\\
&= c_3\cdot(\hat{e}(c_1, h^{\Delta_\gamma(ID,\mathcal{S})})\cdot\hat{e}(SK_{\text{PRE}}^{ID}, c_2)\cdot\hat{e}((u\cdot t^\alpha)^{\frac{s}{\mathcal{H}(ID)}}, c_2))^{\frac{-1}{\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}\mathcal{H}(ID_i)}}\\
&= c_3\cdot v^{-k}\cdot\hat{e}((u\cdot t^\alpha)^{\frac{s}{\mathcal{H}(ID)}}, h^{k\cdot\prod_{ID_i\in\mathcal{S}}(\gamma+\mathcal{H}(ID_i))})^{\frac{-1}{\prod_{ID_i\in\mathcal{S}\bigwedge ID_i\neq ID}\mathcal{H}(ID_i)}} = m\cdot\hat{e}((u\cdot t^\alpha), h)^{-s\cdot k\cdot\prod_{ID_i\in\mathcal{S}}(\frac{\gamma+\mathcal{H}(ID_i)}{\mathcal{H}(ID_i)})}
\end{aligned}$$

Since $\tilde{c}_3 = d_3 = \mathcal{H}'(v^{k'})\cdot h^s$, we have $h^s = \frac{\tilde{c}_3}{\mathcal{H}'(K')}$. Furthermore, we have

$$\tilde{c}_5\cdot\hat{e}(K', \tilde{c}_4) = m\cdot\hat{e}((u\cdot t^\alpha), h)^{-s\cdot k\cdot\prod_{ID_i\in\mathcal{S}}(\frac{\gamma+\mathcal{H}(ID_i)}{\mathcal{H}(ID_i)})}\cdot\hat{e}(h^s, (u\cdot t^\alpha)^{k\cdot\prod_{ID_i\in\mathcal{S}}(\frac{\gamma+\mathcal{H}(ID_i)}{\mathcal{H}(ID_i)})}) = m.$$

Consequently, we proved that $\mathbf{Dec\text{-}2}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID', SK_{\text{PRE}}^{ID'}, \tilde{C}, \mathcal{S}') = m$ if $ID \in \mathcal{S}\bigwedge\alpha = \alpha'\bigwedge ID' \in \mathcal{S}'$.

Fig. 3. The proof of Theorem 2.

- Challenger $\mathcal{C}$ runs D07's algorithm $\mathbf{Setup}_{\text{IBBE}}(\lambda, N)$ to generate a master public key $\mathbf{PK}_{\text{IBBE}}$ and a master secret key $\mathbf{MK}_{\text{IBBE}}$, where $\mathbf{PK}_{\text{IBBE}} = (p, \mathbb{G}, \mathbb{G}_T, \hat{e}, w = g^\gamma, v = \hat{e}(g,h), h, h^\gamma, \ldots, h^{\gamma^N}, \mathcal{H})$ and $\mathbf{MK}_{\text{IBBE}} = (g, \gamma)$. Since the hash function $\mathcal{H}$ is modeled as a random oracle in this proof, challenger $\mathcal{C}$ sends the reduced master public key $\mathbf{PK}_{\text{IBBE}} = (p, \mathbb{G}, \mathbb{G}_T, \hat{e}, w = g^\gamma, v = \hat{e}(g,h), h, h^\gamma, \ldots, h^{\gamma^N})$ to adversary $\mathcal{B}$. And challenger $\mathcal{C}$ provides hash query service $\mathcal{Q}_{\text{IBBE}}^{\mathcal{H}}(ID)$ for adversary $\mathcal{B}$ and models the hash function $\mathcal{H}$ as a random oracle. He prepares a table $\mathcal{L}_H$ for $\mathcal{Q}_{\text{IBBE}}^{\mathcal{H}}(ID)$ with columns $(Identity, HashValue)$ to store the queried identities and their responses.
- Adversary $\mathcal{B}$ randomly picks $(x, y) \in \mathbb{Z}_p^{*\,2}$, and generates the proposed CIBPRE scheme's master public key $\mathbf{PK}_{\text{PRE}} = (\mathbf{PK}_{\text{IBBE}}, u, u^\gamma, \ldots, u^{\gamma^N}, t, t^\gamma, \ldots, t^{\gamma^N}, \mathcal{H}, \mathcal{H}')$, where $u^{\gamma^i} = h^{\gamma^i\cdot x}$ and $t^{\gamma^i} = h^{\gamma^i\cdot y}$ for $i \in [0, N]$. Since the hash functions $\mathcal{H}$ and $\mathcal{H}'$ also are modeled as two random oracles in this proof, adversary $\mathcal{B}$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

sends the reduced master public key $\mathbf{PK}_{\text{PRE}} = (\mathbf{PK}_{\text{IBBE}}, u, u^{\gamma}, \ldots, u^{\gamma^N}, t, t^{\gamma}, \ldots, t^{\gamma^N})$ to adversary $\mathcal{A}$. And adversary $\mathcal{B}$ provides the hash query services $\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)$ and $\mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}(Y)$ (where $Y \in \mathbb{G}_T$) for adversary $\mathcal{A}$ and models the hash functions $\mathcal{H}$ and $\mathcal{H}'$ as two random oracles. Indeed, $\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)$ is a copy of $\mathcal{Q}^{\mathcal{H}}_{\text{IBBE}}(ID)$. Any query of adversary $\mathcal{A}$ to $\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)$ will be forwarded by adversary $\mathcal{B}$ to challenger $\mathcal{C}$, and any response from challenger $\mathcal{C}$ also will be forwarded by adversary $\mathcal{B}$ to adversary $\mathcal{A}$. In addition, adversary $\mathcal{B}$ prepares a table $\mathcal{L}_{H'}$ for $\mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}$ with columns $(GroupElement, HashValue)$ to store the queried group elements and their responses.

- **Query Phase 1**: Adversary $\mathcal{B}$ can issue hash query $\mathcal{Q}^{\mathcal{H}}_{\text{IBBE}}(ID)$ and private key query $\mathcal{Q}^{SK}_{\text{IBBE}}(ID)$ to challenger $\mathcal{C}$. Adversary $\mathcal{A}$ can issue hash queries $\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)$ and $\mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}(Y)$, private key query $\mathcal{Q}^{SK}_{\text{PRE}}(ID)$, and re-encryption key query $\mathcal{Q}^{RK}_{\text{PRE}}(ID, \mathcal{S}', a)$ to adversary $\mathcal{B}$. These queries work as follows:
  - Hash Query $\mathcal{Q}^{\mathcal{H}}_{\text{IBBE}}(ID)$: To answer the query "$ID$", if there is a tuple $(ID, X \in \mathbb{Z}^*_p) \in \mathcal{L}_H$, challenger $\mathcal{C}$ responds X; otherwise challenger $\mathcal{C}$ randomly chooses a value $X \in \mathbb{Z}^*_p$, adds tuple (ID, X) into table $\mathcal{L}_H$ and responds X.
  - Private Key Query $\mathcal{Q}^{SK}_{\text{IBBE}}(ID)$: To answer the query "$ID$", if $ID \in \mathcal{S}^*$, challenger $\mathcal{C}$ responds $\perp$; otherwise, challenger $\mathcal{C}$ responds $SK^{ID}_{\text{IBBE}} = g^{\frac{1}{\gamma + \mathcal{Q}^{\mathcal{H}}_{\text{IBBE}}(ID)}}$.
  - Hash Query $\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)$: To answer the query "$ID$", adversary $\mathcal{B}$ forwards the query to $\mathcal{Q}^{\mathcal{H}}_{\text{IBBE}}(ID)$, and returns the response of $\mathcal{Q}^{\mathcal{H}}_{\text{IBBE}}(ID)$.
  - Hash Query $\mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}(Y \in \mathbb{G}_T)$: To answer the query "$Y$", if there is a tuple $(Y, Z \in \mathbb{G}) \in \mathcal{L}_{H'}$, adversary $\mathcal{B}$ responds Z; otherwise adversary $\mathcal{B}$ randomly chooses a value $Z \in \mathbb{G}$, adds tuple (Y, Z) into table $\mathcal{L}_{H'}$ and responds Z.
  - Private Key Query $\mathcal{Q}^{SK}_{\text{PRE}}(ID)$: To answer the query "$ID$", if $ID \in \mathcal{S}^*$, adversary $\mathcal{B}$ responds $\perp$; if there is a tuple $(ID', \mathcal{S}', *, \alpha^*)$ in table $\mathcal{L}_{RK}$ has $ID' \in \mathcal{S}^*$ and $ID \in \mathcal{S}'$, adversary $\mathcal{B}$ responds $\perp$; otherwise, adversary $\mathcal{B}$ forwards the query to $\mathcal{Q}^{SK}_{\text{IBBE}}(ID)$ and obtains SK^{ID}_{IBBE}, returns $SK^{ID}_{\text{PRE}} = SK^{ID}_{\text{IBBE}}$ and adds ID into table $\mathcal{L}_{SK}$.
  - Re-Encryption Key Query $\mathcal{Q}^{RK}_{\text{PRE}}(ID, \mathcal{S}', \alpha)$: Adversary $\mathcal{A}$ queries the re-encryption key from the identity ID to the identity set $\mathcal{S}'$ with the condition α. To answer this query, if there is a tuple $(ID, \mathcal{S}', d_{ID \to \mathcal{S}'|\alpha}, \alpha)$ in table $\mathcal{L}_{RK}$, adversary $\mathcal{B}$ responds $d_{ID \to \mathcal{S}'|a}$ to adversary $\mathcal{A}$; otherwise, we have the following cases:
    1) $ID \notin \mathcal{S}^*$: Adversary $\mathcal{B}$ queries $\mathcal{Q}^{SK}_{\text{IBBE}}(ID)$ to get the private key SK^{ID}_{IBBE}, randomly chooses $(k', s) \in \mathbb{Z}^{*\,2}_p$, computes the re-encryption key $d_{ID \to \mathcal{S}'|\alpha} = (w^{-k'}, h^{k' \cdot \prod_{ID_i \in \mathcal{S}'} (\gamma + \mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID_i))}, \mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}(v^{k'}) \cdot h^s, SK^{ID}_{\text{IBBE}} \cdot (u \cdot t^{\alpha})^{\frac{s}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}})$, responds $d_{ID \to \mathcal{S}'|\alpha}$ to adversary $\mathcal{A}$, and adds tuple $(ID, \mathcal{S}', d_{ID \to \mathcal{S}'|\alpha}, \alpha)$ into table $\mathcal{L}_{RK}$.
    2) $ID \in \mathcal{S}^*$, $\alpha = \alpha^*$ and $\mathcal{S}' \bigcap \mathcal{L}_{SK} \neq \emptyset$: Adversary $\mathcal{B}$ responds $\perp$.
    3) In the following three cases: a) $ID \in \mathcal{S}^*$, $\alpha \neq \alpha^*$ and $\mathcal{S}' \bigcap \mathcal{L}_{SK} \neq \emptyset$; b) $ID \in \mathcal{S}^*$, $\alpha \neq \alpha^*$ and $\mathcal{S}' \bigcap \mathcal{L}_{SK} = \emptyset$; c) $ID \in \mathcal{S}^*$, $\alpha = \alpha^*$ and $\mathcal{S}' \bigcap \mathcal{L}_{SK} = \emptyset$. Adversary $\mathcal{B}$ randomly chooses $d_4 \in \mathbb{G}$ and $(k', s) \in \mathbb{Z}^{*\,2}_p$, responds the re-encryption key $d_{ID \to \mathcal{S}'|\alpha} = (w^{-k'}, h^{k' \cdot \prod_{ID_i \in \mathcal{S}'} (\gamma + \mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID_i))}, \mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}(v^{k'}) \cdot h^s, d_4)$ to adversary $\mathcal{A}$, and adds tuple $(ID, \mathcal{S}', d_{ID \to \mathcal{S}'|\alpha}, \alpha)$ into table $\mathcal{L}_{RK}$.
- **Challenge Phase**: When adversary $\mathcal{A}$ decides that Query Phase 1 is over, he sends two challenge messages (m_0, m_1) to adversary $\mathcal{B}$. Adversary $\mathcal{B}$ forwards (m_0, m_1) to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ generates the challenge ciphertext $C^*_{\text{IBBE}} \leftarrow \mathbf{Enc}_{\text{IBBE}}(\mathbf{PK}_{\text{IBBE}}, \mathcal{S}^*, m_b)$ (where b is randomly chosen in $\{0, 1\}$), and sends C^*_{IBBE} to adversary $\mathcal{B}$. According to the structure of the ciphertext C^*_{IBBE}, let $C^*_{\text{IBBE}} = (c_1, c_2, c_3)$. And without loss of generality, let $c_1 = w^{-k}$, $c_2 = h^{k \cdot \prod_{ID_i \in \mathcal{S}^*} (\gamma + \mathcal{Q}^{\mathcal{H}}_{\text{IBBE}}(ID_i))}$ and $c_3 = v^k \cdot m_b$. Recall that in Setup Phase, adversary $\mathcal{B}$ randomly chose $(x, y) \in \mathbb{Z}^{*\,2}_p$ and set $u = h^x$ and $t = h^y$. Adversary $\mathcal{B}$ can extend the ciphertext C^*_{IBBE} to a valid initial CIBPRE ciphertext by computing $c_4 = (c_2^x \cdot c_2^{y \cdot \alpha})^{\prod_{ID_i \in \mathcal{S}^*} \frac{1}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID_i)}}$. And let $C^*_{\text{PRE}} = (C^*_{\text{IBBE}}, c_4)$. The ciphertext C^*_{PRE} is a valid challenge ciphertext which was defined in the IND-sID-CPA security of CIBPRE, since we have $\mathcal{Q}^{\mathcal{H}}_{\text{IBBE}} = \mathcal{Q}^{\mathcal{H}}_{\text{PRE}}$ and $c_4 = (c_2^x \cdot c_2^{y \cdot \alpha})^{\prod_{ID_i \in \mathcal{S}^*} \frac{1}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID_i)}} = (u \cdot t^{\alpha})^{k \cdot \prod_{ID_i \in \mathcal{S}^*} (\frac{\gamma + \mathcal{Q}^{\mathcal{H}}_{\text{IBBE}}(ID_i)}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID_i)})}$. Finally adversary $\mathcal{B}$ sends the challenge ciphertext C^*_{PRE} to adversary $\mathcal{A}$.
- **Query phase 2**: This phase is the same with Query Phase 1.
- **Guess Phase**: When adversary $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$, adversary $\mathcal{B}$ forwards b' to challenger $\mathcal{C}$.

We can find that adversary $\mathcal{B}$ successfully and efficiently simulates $\mathcal{A}$'s view in attacking the IND-sID-CPA security of the proposed CIBPRE scheme, except the re-encryption key query $\mathcal{Q}^{RK}_{\text{PRE}}(ID, \mathcal{S}', \alpha)$ in the following three cases:

- *Case 1:* $ID \in \mathcal{S}^*$, $\alpha \neq \alpha^*$ and $\mathcal{S}' \bigcap \mathcal{L}_{SK} \neq \emptyset$;
- *Case 2:* $ID \in \mathcal{S}^*$, $\alpha \neq \alpha^*$ and $\mathcal{S}' \bigcap \mathcal{L}_{SK} = \emptyset$;
- *Case 3:* $ID \in \mathcal{S}^*$, $\alpha = \alpha^*$ and $\mathcal{S}' \bigcap \mathcal{L}_{SK} = \emptyset$.

In other words, suppose the exception in above three cases never be found by adversary $\mathcal{A}$. Then adversary $\mathcal{B}$ successfully breaks the IND-sID-CPA security of D07 scheme, if adversary $\mathcal{A}$ successfully breaks the IND-sID-CPA security of the proposed CIBPRE scheme. Next, we compute the probability of adversary $\mathcal{A}$ to find the exception.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

In the exception, adversary $\mathcal{B}$ forges a re-encryption key $d_{ID\rightarrow\mathcal{S}'|\alpha} = (w^{-k'}, h^{k'\cdot\prod_{ID_i\in\mathcal{S}'}(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID_i))}, \mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}(v^{k'})\cdot h^s, d_4)$ by randomly choosing $d_4 \in \mathbb{G}$ and $(k', s) \in \mathbb{Z}_p^*$ [2]. Suppose adversary $\mathcal{A}$ totally queries $\mathcal{Q}^{RK}_{\text{PRE}}$ T times. We next prove that the probability of adversary $\mathcal{A}$ to find the exception is no more than $T\cdot(Adv^{IND}_{DBDH,\ \mathcal{A}} + Adv^{\text{IND-sID-CPA}}_{D07,\ \mathcal{A}})$ by following the following two lemmas. Let $\mathcal{A}_{Dis}(A, B)$ denote the event that adversary $\mathcal{A}$ can distinguish event A and event B.

Lemma 2: In Case 1, the probability of adversary $\mathcal{A}$ to find the exception of $d_{ID\rightarrow\mathcal{S}'|\alpha}$ is no more than $Adv^{IND}_{DBDH,\ \mathcal{A}}$.

Proof. Suppose adversary $\mathcal{A}$ can find the exception of $d_{ID\rightarrow\mathcal{S}'|\alpha}$ in this case. In *Case 1*, since $\mathcal{S}'\bigcap\mathcal{L}_{SK} \neq \emptyset$, adversary $\mathcal{A}$ can decrypt out h^s, we have that $\mathcal{A}_{Dis}(d_4, SK^{ID}_{\text{IBBE}}\cdot(u\cdot t^{\alpha})^{\frac{s}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}})$ holds. Since adversary $\mathcal{A}$ can computes $h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))}$, we have

$\mathcal{A}_{Dis}(d_4, SK^{ID}_{\text{IBBE}}\cdot(u\cdot t^{\alpha})^{\frac{s}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}})$ holds

$\Rightarrow \mathcal{A}_{Dis}(\hat{e}(d_4, h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))}), \hat{e}(SK^{ID}_{\text{IBBE}}\cdot(u\cdot t^{\alpha})^{\frac{s}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}}, h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))}))$ holds

Since $\hat{e}(g, h)$ is a public value, we have

$\mathcal{A}_{Dis}(\hat{e}(d_4, h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))}), \hat{e}(SK^{ID}_{\text{IBBE}}\cdot(u\cdot t^{\alpha})^{\frac{s}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}}, h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))})$ holds

$\Rightarrow \mathcal{A}_{Dis}(\hat{e}(d_4, h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))})\cdot\hat{e}(g,h)^{-1}, \hat{e}((u\cdot t^{\alpha})^{\frac{s}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}}, h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))}))$ holds

Since d_4 was randomly chosen in $\mathbb{G}$, there is a value $r \in \mathbb{Z}_p^*$ having $\hat{e}(d_4, h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))})\cdot\hat{e}(g,h)^{-1} = \hat{e}(h,h)^r$. And since $u = h^x$ and $t = h^y$, we have

$\mathcal{A}_{Dis}(\hat{e}(d_4, h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))})\cdot\hat{e}(g,h)^{-1}, \hat{e}((u\cdot t^{\alpha})^{\frac{s}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}}, h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))})$ holds

$\Rightarrow \mathcal{A}_{Dis}(\hat{e}(h,h)^r, \hat{e}(h,h)^{(x+y\alpha)\cdot s\cdot(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))\cdot\frac{1}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}})$ holds

In addition, it is clear that adversary $\mathcal{A}$ knows $h^{x+y\alpha}$, h^s and $h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))\cdot\frac{1}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}}$. Now we compute the probability of the event that $\mathcal{A}_{Dis}(\hat{e}(h,h)^r, \hat{e}(h,h)^{(x+y\alpha)\cdot s\cdot(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))\cdot\frac{1}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}})$ holds.

When $\mathcal{A}_{Dis}(\hat{e}(h,h)^r, \hat{e}(h,h)^{(x+y\alpha)\cdot s\cdot(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))\cdot\frac{1}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}})$ holds, it means that taking $h^{x+y\alpha}$, h^s and $h^{(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))\cdot\frac{1}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}}$ as input, adversary $\mathcal{A}$ can solve an instance of the DBDH problem by distinguishing $\hat{e}(h,h)^r$ and $\hat{e}(h,h)^{(x+y\alpha)\cdot s\cdot(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))\cdot\frac{1}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}}$. According to the definition of the DBDH problem, we have that $\mathcal{A}_{Dis}(\hat{e}(h,h)^r, \hat{e}(h,h)^{(x+y\alpha)\cdot s\cdot(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID))\cdot\frac{1}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}})$ holds with the probability no more than $Adv^{IND}_{DBDH,\ \mathcal{A}}$. Therefore, adversary $\mathcal{A}$ has the probability no more than $Adv^{IND}_{DBDH,\ \mathcal{A}}$ to find the exception of $d_{ID\rightarrow\mathcal{S}'|\alpha}$ in *Case 1*. □

Lemma 3: In Cases 2 and 3, the probability of adversary $\mathcal{A}$ to find the exception of $d_{ID\rightarrow\mathcal{S}'|\alpha}$ is no more than $Adv^{\text{IND-sID-CPA}}_{D07,\ \mathcal{A}}$.

Proof. Since d_4 is randomly chosen in $\mathbb{G}$, it is clear that there is a value $s' \in \mathbb{Z}_p^*$ having $d_4 = SK^{ID}_{IBBE}\cdot(u\cdot t^{\alpha})^{\frac{s'}{\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID)}}$. If adversary $\mathcal{A}$ can find the exception in *cases 2* and *3*, it means that adversary $\mathcal{A}$ can find that $s' \neq s$. Recall that in $d_{ID\rightarrow\mathcal{S}'|\alpha}$, the part $(w^{-k'}, h^{k'\cdot\prod_{ID_i\in\mathcal{S}'}(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID_i))}, \mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}(v^{k'})\cdot h^s)$ indeed is an encryption of h^s. If adversary $\mathcal{A}$ can find that $s' \neq s$, we have that $\mathcal{A}_{Dis}(\mathbf{A}, \mathbf{B})$ holds, where $\mathbf{A} = (w^{-k'}, h^{k'\cdot\prod_{ID_i\in\mathcal{S}'}(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID_i))}, \mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}(v^{k'})\cdot h^s)$, $\mathbf{B} = (w^{-k''}, h^{k''\cdot\prod_{ID_i\in\mathcal{S}'}(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID_i))}, \mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}(v^{k''})\cdot h^{s'})$ and k'' is randomly chosen in $\mathbb{Z}_p^*$. Next, we prove that $\mathcal{A}_{Dis}(\mathbf{A}, \mathbf{B})$ holds only when adversary $\mathcal{A}$ can break the IND-sID-CPA security of the D07 scheme.

Since $\mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}$ is a random oracle, there is a value $R \in \mathbb{G}_T$ having $\mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}(v^{k''})\cdot h^{s'} = \mathcal{Q}^{\mathcal{H}'}_{\text{PRE}}(v^{k''}\cdot R)\cdot h^s$. So when $\mathcal{A}_{Dis}(\mathbf{A}, \mathbf{B})$ holds, we have that $\mathcal{A}_{Dis}(\mathbf{A}', \mathbf{B}')$ holds, where $\mathbf{A}' = (w^{-k'}, h^{k'\cdot\prod_{ID_i\in\mathcal{S}'}(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID_i))}, v^{k'})$, $\mathbf{B}' = (w^{-k''}, h^{k''\cdot\prod_{ID_i\in\mathcal{S}'}(\gamma+\mathcal{Q}^{\mathcal{H}}_{\text{PRE}}(ID_i))}, v^{k''}\cdot R)$. It is clear that $\mathbf{A}'$ and $\mathbf{B}'$ are two ciphertexts generated by the D07 scheme. Furthermore, since we have $\mathcal{S}'\bigcap\mathcal{L}_{SK} = \emptyset$ both in *Cases 2* and *3*, it means that when adversary $\mathcal{A}$ takes $\mathcal{S}'$ as the set of challenge identities and takes $1 \in \mathbb{G}_T$ and R as two challenge messages, he can break the IND-sID-CPA security of the D07 scheme without knowing the private key SK^{ID}_{IBBE} of any $ID \in \mathcal{S}'$. According to the definition of D07's IND-sID-CPA security, the probability of adversary $\mathcal{A}$ to find the exception is no more than $Adv^{\text{IND-sID-CPA}}_{D07,\ \mathcal{A}}$ in *Cases 2* and *3*. □

According to above two lemmas, we clearly have the following result.

Lemma 4: When adversary $\mathcal{A}$ totally queries $\mathcal{Q}^{RK}_{\text{PRE}}$ T times, adversary $\mathcal{B}$ successfully simulates adversary $\mathcal{A}$'s view in attacking the IND-sID-CPA security of our proposed CIBPRE scheme, except the probability no more than $T\cdot(Adv^{IND}_{DBDH,\ \mathcal{A}} + Adv^{\text{IND-sID-CPA}}_{D07,\ \mathcal{A}})$.

Since we suppose that adversary $\mathcal{A}$ has the advantage $Adv^{\text{IND-sID-CPA}}_{CIBPRE,\ \mathcal{A}}$ to break our CIBPRE scheme, we have that adversary $\mathcal{B}$ has the advantage $Adv^{\text{IND-sID-CPA}}_{D07,\ \mathcal{B}} = Adv^{\text{IND-sID-CPA}}_{CIBPRE,\ \mathcal{A}}(1 - T\cdot Adv^{IND}_{DBDH,\ \mathcal{A}} - T\cdot Adv^{\text{IND-sID-CPA}}_{D07,\ \mathcal{A}})$ to break the IND-sID-CPA security of the D07 scheme.

Since the D07 scheme is IND-sID-CPA secure in the RO model, both $Adv^{\text{IND-sID-CPA}}_{D07,\ \mathcal{B}}$ and $Adv^{\text{IND-sID-CPA}}_{D07,\ \mathcal{A}}$ are negligible. In addition, since the DBDH assumption holds, $Adv^{IND}_{DBDH,\ \mathcal{A}}$ also is negligible. So it demonstrates that $Adv^{\text{IND-sID-CPA}}_{CIBPRE,\ \mathcal{A}}$ must be negligible. In other words, the proposed CIBPRE scheme is IND-sID-CPA secure in the RO model. □

6 Performance

In this section, we compare our proposed CIBPRE scheme with the related up-to-dated TR-CPBRE scheme [14]. To compare the performances, Table 2 summarizes

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

TABLE 2
The complexity of algortihms $\mathbf{Enc}_{\text{PRE}}$, $\mathbf{Dec\text{-}1}_{\text{PRE}}$, $\mathbf{RKExtract}_{\text{PRE}}$, $\mathbf{ReEnc}_{\text{PRE}}$ and $\mathbf{Dec\text{-}2}_{\text{PRE}}$.

	$\mathbf{Enc}_{\text{PRE}}$			$\mathbf{Dec\text{-}1}_{\text{PRE}}$			$\mathbf{RKExtract}_{\text{PRE}}$			$\mathbf{ReEnc}_{\text{PRE}}$			$\mathbf{Dec\text{-}2}_{\text{PRE}}$		
	BM	ME	MI	BM	ME	MI	BM	ME	MI	BM	ME	MI	BM	ME	MI
TR-CPBRE	1	$S+7$	1	2	$S-1$	2	0	$2S+7$	1	8	S	2	4	3S+2	4
CIBPRE	0	$3S+4$	1	2	S	2	0	$S+6$	1	2	S	1	3	S	2
Symbols BM, ME and MI respectively denote bilinear map, modular exponentiation and modular inversion. Symbols S denotes the number of receivers.															

TABLE 3
The size of initial ciphertext, re-encryption key and re-encrypted ciphertext; and whether the original receivers' identities is needed in running algorithms $\mathbf{RKExtract}_{\text{PRE}}$ and $\mathbf{Dec\text{-}2}_{\text{PRE}}$.

	Size of Initial Ciphertext	Size of Re-Encryption Key	Size of Re-Encrypted Ciphertext	Take $\mathcal{S}$ as Input ?	
				$\mathbf{RKExtract}_{\text{PRE}}$	$\mathbf{Dec\text{-}2}_{\text{PRE}}$
TR-CPBRE	$7.5\|\mathbb{G}\|$	$6\|\mathbb{G}\|$	$9.5\|\mathbb{G}\|+\|\mathbb{G}_T\|$	Yes	Yes
CIBPRE	$3\|\mathbb{G}\|+\|\mathbb{G}_T\|$	$4\|\mathbb{G}\|$	$4\|\mathbb{G}\|+\|\mathbb{G}_T\|$	No	No
Symbol $\mathcal{S}$ denotes the original receivers' identities of an initial ciphertext. Symbols $\|\mathbb{G}\|$ and $\|\mathbb{G}_T\|$ respectively denote the binary size of groups $\mathbb{G}$ and $\mathbb{G}_T$.					

the number of expensive algebraic operations in algorithms $\mathbf{Enc}_{\text{PRE}}$, $\mathbf{Dec\text{-}1}_{\text{PRE}}$, $\mathbf{RKExtract}_{\text{PRE}}$, $\mathbf{ReEnc}_{\text{PRE}}$ and $\mathbf{Dec\text{-}2}_{\text{PRE}}$. It shows that our CIBPRE is slightly more efficient than the TR-CPBRE, with both CIBPRE and TR-CPBRE having the constant-size initial ciphertext, re-encryption key and re-encrypted ciphertext.

One may note that CIBPRE is more convenient than TR-CPBRE in practice, since the CIBPRE does not take extra burden on storage and communication as TR-CPBRE does (showed in Table 3). TR-CPBRE takes the original receivers' identities (denoted by $\mathcal{S}$) of an initial ciphertext as input to run algorithms $\mathbf{RKExtract}_{\text{PRE}}$ and $\mathbf{Dec\text{-}2}_{\text{PRE}}$. Hence it requires extra storage for each sender with the original receivers' identities of all generated initial ciphertexts, and increased communication overhead for the proxy to send the corresponding $\mathcal{S}$ to all new receivers of a re-encrypted ciphertext. Conclusively, CIBPRE avoids these constraints and makes the application more practical.

TABLE 4
Configuration of System Parameters.

Hardware	Intel Core 2 Duo CPU E5300 @ 2.60GHz
OS and Compiler	Windows XP, Microsoft Visual C++ 6.0
Program Library	MIRACL version 5.4.1
Parameters of bilinear map	
Elliptic Curve	$y^2 = x^3 + A \cdot x + B \cdot x$
Pentanomial Basis	$t^m + t^a + t^b + t^c + 1$
Base Field: 2^m	$m = 379$
A	1
B	1
Group Order: q	$2^m + 2^{(m+1)/2} + 1$
a	315
b	301
c	287
The default unit is decimal.	

Finally, we coded our CIBPRE scheme and tested the time cost of algorithms $\mathbf{Enc}_{\text{PRE}}$, $\mathbf{Dec\text{-}1}_{\text{PRE}}$, $\mathbf{RKExtract}_{\text{PRE}}$, $\mathbf{ReEnc}_{\text{PRE}}$ and $\mathbf{Dec\text{-}2}_{\text{PRE}}$ for different number of receivers. Table 4 shows the system parameters including hardware, software and the chosen elliptic curve. Table 5 shows the experiment results.

7 CIBPRE-BASED CLOUD EMAIL SYSTEM

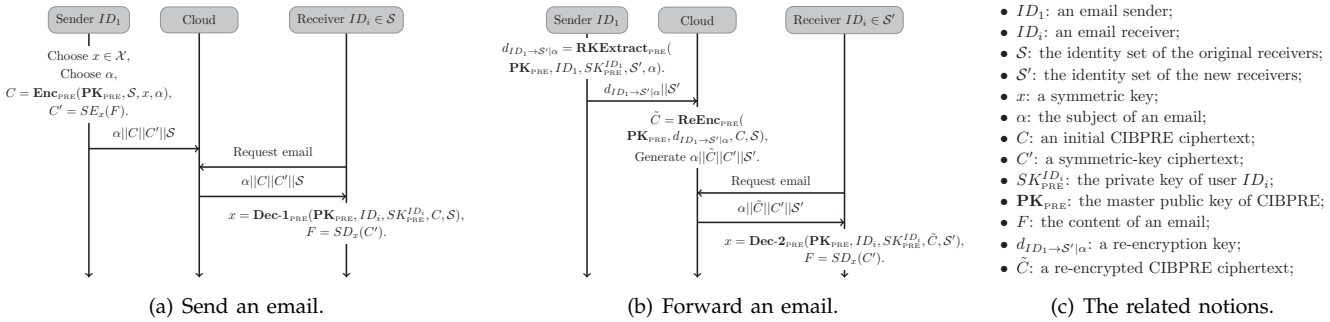
Recall that CIBPRE consists of algorithms $\mathbf{Setup}_{\text{PRE}}$, $\mathbf{Extract}_{\text{PRE}}$, $\mathbf{Enc}_{\text{PRE}}$, $\mathbf{RKExtract}_{\text{PRE}}$, $\mathbf{ReEnc}_{\text{PRE}}$, $\mathbf{Dec\text{-}1}_{\text{PRE}}$ and $\mathbf{Dec\text{-}2}_{\text{PRE}}$. The CIBPRE-based cloud email system consists of a trusted KGC (built by an enterprise administrator), a cloud server and users. The CIBPRE-based cloud email system works as follows:

- **Initialization**: In this phase, the KGC generates the system parameters to initialize the CIBPRE-based cloud email system. It chooses a security parameter $\lambda \in \mathbb{N}$ and a value $N \in \mathbb{N}$ (the maximal number of receivers of an email), and runs algorithm $\mathbf{Setup}_{\text{PRE}}(\lambda, N)$ to generate a pair of master public and secret keys $\mathbf{PK}_{\text{PRE}}$ and $\mathbf{MK}_{\text{PRE}}$. It chooses a secure symmetric key encryption scheme, i.e. AES (the popular choice in practice). Without loss of generality, let the chosen symmetric key encryption scheme be $(\mathcal{X}, SE_x, SD_x)$, where $\mathcal{X} \subseteq \mathbb{G}_T \in \mathbf{PK}_{\text{PRE}}$ is the symmetric key space, SE_x and SD_x respectively denotes the encryption and decryption algorithms both with a symmetric key $x \in \mathcal{X}$. Finally, it publishes $(\mathbf{PK}_{\text{PRE}}, \mathcal{X}, SE_x, SD_x)$.
  In the email system, we take users' email addresses as their identities. When running algorithm $\mathbf{Enc}_{\text{PRE}}$ to encrypt an email, we take the subject of the email as the inputted condition. Though an inputted condition must belong to $\mathbb{Z}_p^* \in \mathbf{PK}_{\text{PRE}}$, it is easy to map the subject of an email into $\mathbb{Z}_p^*$. So it is convenient for us to suppose that all emails' subjects belong to $\mathbb{Z}_p^*$. In addition, we suppose that all emails of a user have the different subjects.
- **Key Management**: In this phase, when a new user joins this system, the KGC generates a private key for him. Without loss of generality, let ID denote the email address of the new user. The KGC runs algorithm $\mathbf{Extract}_{\text{PRE}}(\mathbf{MK}_{\text{PRE}}, ID)$ to generate the private key SK_{PRE}^{ID}, and sends it to the user in a secure channel which is established by the SSL/TLS protocol.
- **Send An Encrypted Cloud Email**: In this phase, a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

TABLE 5
Time Cost of algorithms $\mathbf{Enc}_{\text{PRE}}$, $\mathbf{Dec\text{-}1}_{\text{PRE}}$, $\mathbf{RKExtract}_{\text{PRE}}$, $\mathbf{ReEnc}_{\text{PRE}}$ and $\mathbf{Dec\text{-}2}_{\text{PRE}}$.

Number of Receivers	Time Cost (Unit: CPU cycle)				
	$\mathbf{Enc}_{\text{PRE}}$	$\mathbf{Dec\text{-}1}_{\text{PRE}}$	$\mathbf{RKExtract}_{\text{PRE}}$	$\mathbf{ReEnc}_{\text{PRE}}$	$\mathbf{Dec\text{-}2}_{\text{PRE}}$
4	34397064 (13.230ms)	79089153 (30.419ms)	36721919 (14.124ms)	78398268 (30.153ms)	123970236 (47.681ms)
8	54009982 (20.773ms)	88327408 (33.972ms)	41353858 (15.905ms)	86587345 (33.303ms)	128471538 (49.412ms)
12	74940619 (28.823ms)	96779670 (37.223ms)	49816676 (19.160ms)	93755987 (36.060ms)	136606496 (52.541ms)



(a) Send an email. (b) Forward an email. (c) The related notions.

Fig. 4. Two main processes of CIBPRE-based cloud email system and their related notions.

user can send an encrypted email to other users. And this email will be stored in the cloud server. If the user wants to review this email, he can fetch the encrypted email from the cloud server and decrypt it. Suppose user ID_1 wants to send the email content F (including the associated attachment) to the users $\{ID_2, ..., ID_n\}$ (where $n \leq N$). Fig. 4(a) shows this phase. The details are as follows.

1) User ID_1 sets $\mathcal{S} = \{ID_1, ..., ID_n\}$, randomly chooses a symmetric key $x \in \mathcal{X}$, chooses a subject α of this email, runs algorithms $C = \mathbf{Enc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, \mathcal{S}, x, \alpha)$ and $C' = SE_x(F)$, finally sends $\alpha||C||C'||\mathcal{S}$ to the cloud server.
2) The cloud server stores the received ciphertext $\alpha||C||C'||\mathcal{S}$.
3) When user $ID_i \in \mathcal{S}$ is online, he retrieves the ciphertext $\alpha||C||C'||\mathcal{S}$ from the cloud sever, and runs algorithms $x = \mathbf{Dec\text{-}1}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID_i, SK_{\text{PRE}}^{ID_i}, C, \mathcal{S})$ and $F = SD_x(C')$ to decrypt out the email content F.
4) When user ID_1 wants to read this email again, he retrieves the ciphertext $\alpha||C||C'||\mathcal{S}$ from the cloud sever, and runs algorithms $x = \mathbf{Dec\text{-}1}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID_1, SK_{\text{PRE}}^{ID_1}, C, \mathcal{S})$ and $F = SD_x(C')$ to decrypt out the email content F.

Security. According to the IND-sID-CPA security of CIBPRE and the security of the symmetric key encryption $(\mathcal{X}, SE_x, SD_x)$, only users $\{ID_1, ..., ID_n\}$ can decrypt out the email content F.

Performance. In above steps, the capability "Identity-based" of CIBPRE avoids user ID_1 to fetch and verify the certificates of users $\{ID_2, ..., ID_n\}$ before encrypting the email. The capability "Broadcast" of CIBPRE makes C having the constant size.

- **Forward A History Encrypted Cloud Email**: In this phase, a user can forward a history encrypted email to new users by generating a re-encryption key for these users and the subject of this email. Suppose user ID_1 wants to forward his history encrypted email $\alpha||C||C'||\mathcal{S}$ to the new users $\{ID'_2, ..., ID'_n\}$ (where $n \leq N+1$). Fig. 4(c) shows this phase. The steps are as follows.
  1) User ID_1 sets $\mathcal{S}' = \{ID'_2, ..., ID'_n\}$, runs algorithm $\mathbf{RKExtract}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID_1, SK_{\text{PRE}}^{ID_1}, \mathcal{S}', \alpha)$ to generate a re-encryption key $d_{ID_1 \to \mathcal{S}'|\alpha}$, and sends $d_{ID_1 \to \mathcal{S}'|\alpha}||\mathcal{S}'$ to the cloud server.
  2) The cloud server runs algorithm $\tilde{C} = \mathbf{ReEnc}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, d_{ID_1 \to \mathcal{S}'|\alpha}, C, \mathcal{S})$ to re-encrypt C, and generate the re-encrypted email $\alpha||\tilde{C}||C'||\mathcal{S}'$.
  3) When user $ID'_i \in \mathcal{S}'$ is online, he retrieves the ciphertext $\alpha||\tilde{C}||C'||\mathcal{S}'$ from the cloud sever, and runs algorithm $x = \mathbf{Dec\text{-}2}_{\text{PRE}}(\mathbf{PK}_{\text{PRE}}, ID_i, SK_{\text{PRE}}^{ID_i}, \tilde{C}, \mathcal{S}')$ and algorithm $F = SD_x(C')$ to decrypt out the email content F.

  Security. According to the IND-sID-CPA security of CIBPRE and the security of the symmetric key encryption $(\mathcal{X}, SE_x, SD_x)$, the re-encrypted email $\alpha||\tilde{C}||C'||\mathcal{S}'$ only can be decrypted by the users in $\mathcal{S}'$. According to the capability "Conditional", the re-encryption key $d_{ID_1 \to \mathcal{S}'|\alpha}$ only can re-encrypt the history email $\alpha||C||C'||\mathcal{S}$. It implies that the cloud server can not forward the other history encrypted emails to any user.

  Performace. In the above steps, the capability "Identity-based" of CIBPRE avoid user ID_1 to fetch and verify the certificates of users $\{ID'_2, ..., ID'_n\}$ before generating a re-encryption key. The capability "Broadcast" of CIBPRE makes the generated re-encryption key having the constant size.

In the CIBPRE-based cloud email system, the enterprise administrator only needs to initialize the system

and generate the private key for the newly joined user. In other words, the enterprise administrator can be offline if no new user joins the system. It is a useful paradigm for the enterprise administrator to resist the outside attacks in practice. The cloud server provides efficient services to send, store and forward users' encrypted emails. Moreover, it is convenient that all users takes email addresses as public keys to encrypt emails. In the aspect of security, all users' emails are confidential even if the cloud sever is compromised.

8 Conclusion

This paper presented a new kind of PRE concept called Conditional Identity-based Broadcast Proxy Re-Encryption (CIBPRE), as well as its IND-sID-CPA security definitions. The CIBPRE is a general concept equipped with the capabilities of Conditional PRE (CPRE), Identity-based PRE (IPRE) and Broadcast PRE (BPRE). The IND-sID-CPA security definition of CIBPRE incorported the security requirements of CPRE, IPRE and BPRE.

CIBPRE inherits the advantages of CPRE, IPRE and BPRE for applications. It allows a user to share their outsourced encrypted data with others in a fine-grained manner. All CIBPRE users takes their identities as public keys to encrypt data. It avoids a user to fetch and verify other users' certificates before encrypting his data. Moreover, it allows a user to generate a broadcast ciphertext for multiple receivers and share his outsourced encrypted data to multiple receivers in a batch manner.

we instantiated the first CIBPRE scheme based on the Identity-Based Broadcast Encryption (IBBE) in [30]. Upon the provable security of the IBBE scheme and the DBDH assumption, the instance of CIBPRE is provably IND-sID-CPA secure in the RO model. It indicates that without the corresponding private key or the right to share a user's outsourced data, one can learn nothing about the user's data.

Finally, we compared the proposed CIBPRE scheme with similar works and the comparison confirms the advantages of our CIBPRE scheme. We built the encrypted cloud email system based our CIBPRE scheme. Compared with the previous techniques such as PGP and IBE, our CIBPRE-based system is much more efficient in the aspect of communication and more practical in user experience.

Acknowledgments

The authors would like to thank the reviewers for their valuable suggestions that helped to improve the paper greatly. The first author is partly supported by the National Natural Science Foundation of China under grant no. 61472156 and the National Program on Key Basic Research Project (973 Program) under grant no. 2014CB340600. The third author is supported by by the Chinese National Key Basic Research Program (973 program) through project 2012CB315905, the Natural Science Foundation of China through projects 61370190, 61173154, 61472429, 61402029, 61272501, 61202465, 61321064 and 61003214, the Beijing Natural Science Foundation through project 4132056, the Fundamental Research Funds for the Central Universities, and the Research Funds (No. 14XNLF02) of Renmin University of China and the Open Research Fund of Beijing Key Laboratory of Trusted Computing.

References

[1] M. Blaze, G. Bleumer and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography", Proc. Advances in Cryptology-EUROCRYPT ' 98, Springer, Heidelberg, 1998, pp. 127-144.
[2] A. Boldyreva, M. Fischlin, A. Palacio and B. Warinschi, "A Closer Look at PKI: Security and Efficiency", Proc. PKC 2007 Springer, Heidelberg, 2007, pp. 458-475.
[3] M. Green and G. Ateniese, "Identity-Based Proxy Re-Encryption", Proc. ACNS 2007, Springer, Heidelberg, 2007, pp. 288-306.
[4] T. Matsuo, "Proxy Re-encryption Systems for Identity-Based Encryption", Proc. PAIRING 2007, Springer, Heidelberg, 2007, pp. 247-267.
[5] C.-K. Chu and W.-G. Tzeng, "Identity-Based Proxy Re-encryption Without Random Oracles", Proc. ISC 2007, Springer, Heidelberg, 2007, pp. 189-202.
[6] L. Ibraimi, Q. Tang, P. Hartel and W. Jonker, "A Type-and-Identity-based Proxy Re-Encryption Scheme and its Application in Healthcare", Proc. SECURE DATA MANAGEMENT 2008, Springer, Heidelberg, 2008, pp. 185-198.
[7] J. Shao, G. Wei, Y. Ling and M. Xie, "Identity-based Conditional Proxy Re-encryption", Proc. IEEE International Conference on Communications (ICC), 2011, pp. 1-5.
[8] K. Liang, Z. Liu, X. Tan, D.S. Wong and C. Tang, "A CCA-Secure identity-based conditional proxy re-encryption without random oracles", Proc. ICISC, 2012, pp. 231-146.
[9] C.-K. Chu, J. Weng, S.S.M. Chow, J. Zhou and R.H. Deng, "Conditional Proxy Broadcast Re-Encryption", Proc. INFORMATION SECURITY AND PRIVACY 2009, Springer, Heidelberg, 2009, pp. 327-342.
[10] Q. Tang, "Type-Based Proxy Re-encryption and Its Construction", proc. INDOCRYPT, 2008, pp. 130-144.
[11] J. Weng, R.H. Deng, X. Ding, C.-K. Chu and J. Lai, "Conditional Proxy Re-Encryption Secure against Chosen-Ciphertext Attack", Proc. ASIACCS '09, ACM, 2009, pp. 322-332.
[12] J. Weng, Y. Yang, Q. Tang, R.H. Deng and F. Bao, "Efficient Conditional Proxy Re-Encryption with Chosen-Ciphertext Security", Proc. Information Security 2009, Springer-Verlag, 2009, pp. 151-166.
[13] L. Fang, W. Susilo and J. Wang, "Anonymous Conditional Proxy Re-encryption without Random Oracle", Proc. ProvSec 2009, Springer, Heidelberg, 2009, pp. 47-60.
[14] K. Liang, Q. Huang, R. Schlegel. D. S. Wong and C. Tang, "A Conditional Proxy Broadcast Re-Encryption Scheme Supporting Timed-Release", Proc. ISPEC 2013, LNCS 7863, Springer, Heidelberg, 2013, pp. 132-146.
[15] Philip R. Zimmermann, "PGP Source Code and Internals", MIT Press, ISBN 0-262-24039-4, 1995.
[16] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing", Proc. Advances in Cryptology-CRYPTO 2001, Springer, Heidelberg, 2001, pp. 213-239.
[17] Radicati Group, "Cloud Business Email Market, 2014-2018", http://www.radicati.com/wp/wp-content/uploads/2014/10/Cloud-Business-Email-Market-2014-2018-Executive-Summary.pdf, 2014.
[18] Proofpoint Group, "Cloud-based Archiving vs. On-Premises Legacy Archiving", http://video.proofpoint.com/id/cloud-based-archiving-vs.-on-premises-legacy-archiving-TCO-white-paper, 2012.
[19] G. Ateniese, K. Fu, M. Green and S. Hohenberger, "Improved Proxy Reencryption Schemes with Applications to Secure Distributed Storage", ACM Transactions on Information and System Security, 2006, pp. 1-30.
[20] R.H. Deng, J. Weng, S. Liu and K. Chen, "Chosen-ciphertext secure proxy re-encryption without pairings", Cryptology and Network Security, vol. 5339, 2008, pp. 1-17.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

[21] V. Kirtane and C.P. Rangan, "RSA-TBOS signcryption with proxy re-encryption", Proceedings of the 8th ACM workshop on Digital rights management (DRM '08), 2008, pp. 59-66.
[22] B. Libert and D. Vergnaud, "Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption", Proc. PKC 2008, Springer, Heidelberg, 2008, pp. 360-379.
[23] J. Shao and Z. Cao, "CCA-Secure Proxy Re-Encryption without pairings", Proc. PKC 2009, Springer-Verlag, 2009, pp. 357-176.
[24] G. Ateniese, K. Benson and S. Hohenberger, "Key-Private Proxy Re-Encryption", Proc. CT-RSA 2009, Springer-Verlag, 2009, pp. 279-294.
[25] J. Shao, P. Liu, G. Wei and Y. Ling, "Anonymous proxy re-encryption", Security and Communication Networks, vol. 5, no. 5, 2012, pp. 439-449.
[26] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy reencryption", Proceedings of the 14th ACM conference on Computer and communications security (CCS'07), 2007, pp. 185-194.
[27] T. Matsuda, R. Nishimaki and K. Tanaka, "CCA Proxy Re-Encryption without Bilinear Maps in the Standard Model", Proc. PKC 2010 Springer, Heidelberg, 2010, pp. 261-278.
[28] K. Liang, M. H. Au, J. K. Liu, X. Qi, W. Susilo, X. P. Tran, D. S. Wong and G. Yang, "A DFA-based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing", IEEE Transactions on Information Forensics and Security 9(10), 2014, pp. 1667-1680.
[29] K. Liang, J. K. Liu, D. S. Wong, W. Susilo, "An Efficient Cloud-based Revocable Identity-based Proxy Re-encryption Scheme for Public Clouds Data Sharing", European Symposium on Research in Computer Security (ESORICS), LNCS 8712, Springer, Heidelberg, 2014, pp. 257-272.
[30] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys", Proc. Advances in Cryptology-ASIACRYPT 2007, Springer, Heidelberg, 2007, pp. 200-215.
[31] D. Boneh and X. Boyen, "Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles", Proc. Advances in Cryptology-EUROCRYPT 2004, Springer, Heidelberg, 2004, pp. 223-238.
[32] D. Boneh and X. Boyen, "Secure Identity Based Encryption Without Random Oracles", Proc. Advances in Cryptology-CRYPTO 2004. Springer, Heidelberg, 2004, pp. 197-206.

Peng Xu received the B.A. degree in computer science from Wuhan university of science and technique, Wuhan, China, in 2003, the Master and Ph.D. degree in computer science from Huazhong university of science and technology, Wuhan, China, respectively in 2006 and 2010. Since 2010, he works as a post-doctor at Huazhong university of science and technology, Wuhan, China. He was PI in three grants respectively from National Natural Science Foundation of China (No. 61472156 and No. 61100222) and China Postdoctoral Science Foundation (No. 20100480900), and a key member in several projects supported by 973 (No. 2014CB340600). He has authored over 20 research papers. He is a member of ACM and IEEE.

Tengfei Jiao received the B.A. degree in computer science from Zhengzhou University, Zhengzhou, China, in 2011. Now, he is studying for a master degree in computer science at Huazhong University of Science and Technology. His research interest is cryptography and cloud security.

Qianhong Wu received his Ph.D. in Cryptography from Xidian University in 2004. Since then, he has been with Wollongong University (Australia) as an associate research fellow, with Wuhan University (China) as an associate professor, with Universitat Rovira i Virgili (Catalonia) as a research director and now with Beihang University (China) as a full professor. His research interests include cryptography, information security and privacy, and *ad hoc* network security. He has been a holder/co-holder of 7 China/Australia/Spain funded projects. He has authored 7 patents and over 100 publications. He has served in the program committee of several international conferences in information security and privacy. He is a member of IACR, ACM and IEEE.

Wei Wang received her PhD degree in Electronic and Communication Engineering from Huazhong university of science and technique, Wuhan, China, in 2011. She is now doing Post-doctor work in Peking University, Beijing, China. Her research interests are cloud security, network coding, multimedia transmission.

Hai Jin received his PhD in computer engineering from HUST in 1994. In 1996, he was awarded a German Academic Exchange Service fellowship to visit the Technical University of Chemnitz in Germany. He worked at The University of Hong Kong between 1998 and 2000, and as a visiting scholar at the University of Southern California between 1999 and 2000. He was awarded Excellent Youth Award from the National Science Foundation of China in 2001. He is the chief scientist of National 973 Basic Research Program Project of Virtualization Technology of Computing System. He has co-authored 15 books and published over 400 research papers. He is a senior member of the IEEE and a member of the ACM.