

## RESEARCH

# LacminCC: Lightweight Anonymous Communication Model In Cloud Computing

Fengyin Li<sup>1\*</sup>, Yanli Wang<sup>1</sup>, Hongwei Ju<sup>2</sup>, Xinying Yu<sup>1</sup>, Zhaojie Wang<sup>1</sup> and Huiyu Zhou<sup>3</sup>

\*Correspondence:  
lfyin318@126.com

<sup>1</sup>School of Information Science and Engineering, Qufu Normal University, Rizhao, China  
Full list of author information is available at the end of the article

## Abstract

With increasing application of cloud computing and big data technologies, a large amount of personal information is stored on the Internet, which raises the issue of privacy leakage. In order to protect people's data privacy, this paper firstly presents a new anonymous Identify-Based Encryption (IBE) scheme and shows the proof of its security under the Bilinear Diffie-Hellman Security Assumption. Then, by introducing the anonymous IBE scheme into an anonymous communication model, this paper introduces a new lightweight anonymous communication model for cloud computing, which guarantees the anonymity of system users and the security of messages during the communication in small groups. Our analysis shows that, the proposed communication model cannot only reduce memory consumption and improve message transmission efficiency, but also effectively resist traffic-analysis attacks, node eavesdropping, and finally achieve secure anonymous communication in cloud computing.

**Keywords:** Identify-Based Encryption; Anonymous communication model; Privacy protection; Bilinear Diffie-Hellman Assumption; Bilinear map

## 1 Introduction

With the widespread application of technologies such as big data [1], cloud computing and the Internet of Things [2], a large amount of personal information has been stored on the Internet, which raises a higher level of requirements for privacy protection. As we have known, privacy protection not only protects the content of the messages, but also secures both parties' identity, communication time and communication paths. However, the existing encryption technologies [3] find it difficult to protect the communication participants' private information such as identity, behavior, and network address. Hackers use traffic-analysis attacks [4] to obtain identity information and communication relationships in the communication process, which leads to the privacy leakage of the users. Therefore, it is extremely important to construct an anonymous communication model and take certain measures to conceal the communication relationship in the communication streams, making it difficult for eavesdroppers to obtain contents and derive the relationship of the parties in the communication.

After the first paper on anonymous communication model was published in 1981 [5], many research efforts have been made in the field of anonymous communication. The existing research on anonymous communication can be divided into three categories. Firstly, Reed [6] proposed an onion routing. The message is encrypted and transmitted through a series of network nodes called onion routers, each of which "peels" away a single layer, uncovering the data's next destination. When the final

layer is decrypted, the message arrives at its destination, so each node cannot know the original and final message at the same time. By this way, onion routing achieves the anonymity of the sender [7], but it cannot resist traffic attacks [8, 9], exiting node vulnerability attacks [10] and other security problems. In order to undertake traffic analysis, Chaum *et al.* [11] proposed an anonymous communication model based on DC-net. The model defines an N-number group, and only one member is allowed to send messages in a given round. Messages are sent via broadcasting without the need for a trust center. However, due to the cooperation of all members, it is vulnerable to internal dishonest members, and it is easy to break the security of the model. The last anonymous communication model based on a flooding algorithm, which uses flooding, epidemic and other algorithms for flooding [12, 13]. When the sender initiates an anonymous transmission, the path of the anonymous transmission is unclear. Therefore, the adversary cannot distinguish where the next hop of the node will be. But the main challenge for anonymous communication models based on the flooding algorithm is that the model will generate a large amount of network transmission traffic during the communication process, and has a great demand for network bandwidth. At the same time, the stability and reliability of system algorithms are not satisfactory.

Based on the above analysis, we find that the existing anonymous communication systems have demanding requirements for network bandwidth and memory, and cannot guarantee stability and reliability. In this case, anonymous communication systems are used in small groups, which are not only inefficient and expensive, but also insecure. Therefore, the demand for lightweight anonymous communication systems for small groups is very immanent. For example, bidders need to hide their identities and whistleblowers need to protect their privacy. On the other hand, blockchain technology has made great progress in ensuring the integrity of data during transmission [14], extracting data [15], and detecting smart contract vulnerabilities [16]. Blockchain, as a distributed database, creates conditions for the development of anonymous communication in the Internet of Things, cloud computing and other technologies. For example: the lightweight anonymous communication system can be applied to information transmission between sensors and servers [17], as well as proprietary security protection in cloud services [18]. Nevertheless, there are few existing research studies on lightweight anonymous communication systems. For this purpose, the main contributions of this paper are as follows.

(1) We propose the anonymous IBE algorithm to encrypt the messages in the communication model, taking the advantage of that the anonymous IBE algorithm has a high degree of ciphertext expansion and does not require certificates management. It can meet the conditions of anonymous communication on the basis of ensuring the security of the messages. In this paper, we also verify the correctness of the proposed algorithm and prove its security under the Bilinear Diffie-Hellman Security Assumption.

(2) We design a lightweight anonymous communication model based on the proposed IBE scheme, simultaneously implementing anonymity, efficiency and security. Analysis shows that the model can resist traffic analysis attacks on the basis of ensuring security and anonymity of the user communications, the model is also able to reduce memory and resource consumption.

The roadmap of this paper is as follows. Section 2 introduces the preliminary work of this project, such as bilinear groups, complexity assumptions, IBE and security model, etc. Section 3 describes our anonymous IBE scheme and proves its correctness and security. In Section 4, a lightweight anonymous communication model in cloud computing is proposed. We elaborate on the communication process of the entire model and how to achieve anonymous communication. Before summarising this paper in Section 6, Section 5 analyses the performance of the proposed model in this paper.

## 2 Preliminary

### 2.1 Bilinear map

Let  $G_1$  and  $G_2$  be multiplicative cyclic groups of prime order  $p$  and  $g$  be a generator of  $G_1$ . The bilinear map  $e : G_1 \times G_1 \rightarrow G_2$  has the following properties [19]:

- (1) Bilinearity:  $\forall P, Q \in G_1$  and  $\forall a, b \in \mathbb{Z}_p$ , we have  $e(P^a, Q^b) = e(P, Q)^{ab}$ .
- (2) Non-degeneracy:  $\forall g \in G_1$ , such that  $e(g, g)$  has order  $p$ , that is,  $e(g, g)$  is a generator of  $G_2$ .
- (3) Computability:  $\forall P, Q \in G_1$ , there is an algorithm that can compute  $e(P, Q)$  efficiently.

### 2.2 Bilinear Diffie-Hellman Assumption

The BDH problem [19, 20] in  $G_1$  is as follows: Given a tuple  $g, g^\alpha, g^b, g^c \in G_1$  as input, output  $e(g, g)^{abc} \in G_2$ . An algorithm  $\mathcal{A}$  has advantage  $\varepsilon$  in solving BDH in  $G_1$  if

$$\Pr \left[ \mathcal{A}(g, g^\alpha, g^b, g^c) = e(g, g)^{abc} \right] \geq \varepsilon \quad (1)$$

where the probability is over the random choice of  $\alpha, b, c$  in  $\mathbb{Z}_p^*$  and the random bits used by  $\mathcal{A}$ . Similarly, an algorithm  $\mathcal{B}$  that outputs  $b \in \{0, 1\}$  has advantage  $\varepsilon$  in solving the decision BDH problem in  $G_1$  if

$$\left| \Pr \left[ \mathcal{B}(g, g^\alpha, g^b, g^c, e(g, g)^{abc}) = 0 \right] - \Pr \left[ \mathcal{B}(g, g^\alpha, g^b, g^c, T) = 0 \right] \right| \geq \varepsilon \quad (2)$$

where the probability is over the random choice of  $\alpha, b, c$  in  $\mathbb{Z}_p^*$ , the random choice of  $T \in G_2^*$ , and the random bits of  $\mathcal{B}$ .

**Definition 1:** The (Decision)  $(t, \varepsilon)$ -BDH assumption holds in  $G_1$  if no  $t$ -time algorithm has advantage  $\varepsilon$  at least in solving the (Decision) BDH problem in  $G_1$ .

Occasionally we drop  $t$  and  $\varepsilon$  and refer to the BDH and Decision BDH assumptions in  $G_1$ .

### 2.3 IBE scheme

In the IBE scheme, participants include users and private key generators (PKG). PKG is a trusted third party, which generates a private key based on the system master key and user identity. Subsequently, PKG distributes the private key to the corresponding users. Furthermore, the identity of the user makes IBE different from the public key of the traditional public key crypto-system. Therefore, IBE is widely used for information security protection. An Identity Based Encryption

(IBE) scheme is a tuple of PPT algorithms defined with respect to a message space  $\mathcal{M}$ , an identity space  $\mathcal{I}$  and a ciphertext space  $\mathcal{C}$  as follows:

*Setup*: On input (in unary) a security parameter  $k$ , generate public parameters  $params$  and a master secret key  $MSK$ . And  $\mathcal{M}, \mathcal{C}, params$  is public.  $MSK$  is kept by PKG.

*Key generation*: On input a master secret key  $MSK$  and an identity  $ID \in \mathcal{I}$ , derive and output a secret key  $d_{ID}$  for identity  $ID$ .

*Encryption*: On input public parameters  $params$ , an identity  $ID \in \mathcal{I}$ , and a message  $m \in \mathcal{M}$ , output a ciphertext  $C \in \mathcal{C}$  that encrypts  $m$  under identity  $ID$ .

*Decryption*: On input a secret key  $d_{ID}$  for identity  $ID \in \mathcal{I}$  and a ciphertext  $C \in \mathcal{C}$ , output  $m'$  if  $C$  is a valid encryption under identity  $ID$ , output a failure symbol  $\perp$  otherwise.

## 2.4 Security model

Boneh and Franklin define chosen ciphertext security for IBE systems under a chosen identity attack [21, 22]. In their model, the adversary is allowed to adaptively choose the public key it wishes to attack (the public key on which it will be challenged). Informally, if the adversary cannot obtain the public key  $ID$  in the ciphertext and has the characteristics of indistinguishability under the chosen ciphertext attack, we believe that the scheme has ANON-IND-ID-CCA (anonymous, indistinguishable and based on  $ID$ 's chosen ciphertext attack) security. More precisely, the security of anonymous IBE scheme is defined using the following game [23].

We define  $\mathcal{A}$  as an adversary and  $\mathcal{B}$  as a challenger.

*Setup*:  $\mathcal{B}$  runs setup, and forwards parameters to  $\mathcal{A}$ .

*Phase 1*: Proceeding adaptively,  $\mathcal{A}$  issues queries  $q_1, \dots, q_m$  where  $q_i$  is one of the following:

Key generation query  $\langle ID_i \rangle$ :  $\mathcal{B}$  runs *Key generation* on  $ID_i$  and forwards the resulting private key to  $\mathcal{A}$ .

Decryption query  $\langle ID_i, C_i \rangle$ :  $\mathcal{B}$  runs *Key generation* on  $ID_i$ , decrypts  $C_i$  with the resulting private key, and sends the result to  $\mathcal{A}$ .

*Challenge*:  $\mathcal{A}$  submits two plaintexts  $m_0, m_1$  and two identities  $ID_0, ID_1$ .  $ID_0, ID_1$  or their prefix cannot appear in any key generation query in Phase 1.  $\mathcal{B}$  selects a random bit  $k, l \in \{0, 1\}$ , sets  $C^* = \text{Encrypt}(params, ID_k, m_l)$ , and sends  $C^*$  to  $\mathcal{A}$  as its challenge ciphertext.

*Phase 2*: This is identical to Phase 1, except that  $\mathcal{A}$  may not request the private key for  $ID_0, ID_1$  or the decryption of  $\langle ID_0, C^* \rangle, \langle ID_1, C^* \rangle$ .

*Guess*:  $\mathcal{A}$  submits a guess  $k', l' \in \{0, 1\}$ .  $\mathcal{A}$  wins if  $k' = k, l' = l$ . We call an adversary  $\mathcal{A}$  in the above game as an ANON-IND-ID-CCA adversary. The advantage  $\varepsilon$  of an adversary  $\mathcal{A}$  in this game is defined as  $|\Pr[k' = k \wedge l' = l] - \frac{1}{4}|$ .

**Definition 2**: An anonymous IBE system is  $(t, q, \varepsilon)$ -ANON-IND-ID-CCA secure if all  $t$ -time ANON-IND-ID-CCA adversaries making at most  $q$  queries have advantage at most  $\varepsilon$  in winning the above game.

## 3 Anonymous IBE scheme

Anonymous IBE can effectively guarantee that it will not disclose any identity information about the recipient in the ciphertexts, and has ANON-IND-ID-CCA security. In this section, we construct an efficient anonymous IBE scheme, and prove its correctness and security.

### 3.1 Construction

Let  $G_1$  and  $G_2$  be multiplicative cyclic groups of prime order  $p$  and  $g$  be a generator of  $G_1$ ,  $e : G_1 \times G_1 \rightarrow G_2$  is the bilinear map.

*Setup:* In order to generate security parameters, we randomly select  $\alpha \in Z_p^*$  and set  $g_1 = g^\alpha, g_2 \in G_1$ . The public parameters  $params$  and the secret master key  $MSK$  are given by

$$params = (g, g_1, g_2), MSK = \alpha. \quad (3)$$

*Key generation:* To generate private key  $d_{ID}$ , we randomly select  $r \in Z_p^*$ , input master secret key  $MSK$  and an identity  $ID \in Z_p^*$  and output

$$d_{ID} = (d_1, d_2) = (g_2^\alpha g_1^{ID \cdot r}, g^{-r}). \quad (4)$$

*Encryption:* To encrypt a message  $m \in G_2$  under public key  $ID$ , pick a random  $t \in Z_p^*$  and we output

$$C = (C_1, C_2, C_3) = (e(g, g_2)^{\alpha t} \cdot m, g^t, g_1^{ID \cdot t}). \quad (5)$$

*Decryption:* To decrypt a ciphertext  $C = (C_1, C_2, C_3)$  using private key  $d_{ID} = (d_1, d_2)$ , output

$$m = C_1 \cdot \frac{1}{e(C_2, d_1) e(d_2, C_3)}. \quad (6)$$

### 3.2 Proof of correctness

If  $C$  is a valid ciphertext encrypted with identity  $ID$  to message  $m$ , then the following expression can be verified:

$$\begin{aligned} & e(C_2, d_1) e(d_2, C_3) \\ &= e(g^t, g_2^\alpha g_1^{ID \cdot r}) e(g^{-r}, g_1^{ID \cdot t}) \\ &= e(g^t, g_2^\alpha) e(g^t, g_1^{ID \cdot r}) e(g^{-r}, g_1^{ID \cdot t}) \\ &= e(g^t, g_2^\alpha) e(g^r, g_1^{ID \cdot t}) e(g^{-r}, g_1^{ID \cdot t}) \\ &= e(g^t, g_2^\alpha) \\ &= e(g, g_2)^{\alpha t} \end{aligned} \quad (7)$$

So, there is  $m = C_1 \cdot \frac{1}{e(C_2, d_1) e(d_2, C_3)}$ .

### 3.3 Proof of security

**Theorem 1:** Assume that the DBDH problem is hard, the proposed anonymous IBE scheme is  $(t, q, \varepsilon)$ -ANON-IND-ID-CCA secure.

**Proof:** Assume  $\mathcal{A}$  is an ANON-IND-ID-CCA adversary,  $\mathcal{B}$  is a challenger. At the beginning of the game,  $\mathcal{B}$  is given a tuple  $(g, g^\alpha, g^b, g^c, T) \in G_1^5$  to decide whether or not  $T = e(g, g)^{\alpha bc}$ .

*Setup:*  $\mathcal{B}$  randomly generates security parameters. Let  $g_1 = g^\alpha, g_2 = g^b$ , the public parameters are  $(g, g_1, g_2)$  which are assigned to  $\mathcal{A}$ .

*Phase 1:*

Key generation query:  $\mathcal{A}$  assigns identity  $ID \in Z_p^*$  to  $\mathcal{B}$ .  $\mathcal{B}$  randomly chooses  $r \in Z_p^*$ , and computes

$$d = (d_1, d_2) = \left( g_1^{rID}, g^{-r} g_2^{\frac{1}{ID}} \right) \quad (8)$$

Let  $r' = r - \frac{b}{ID}$ , which is a valid private key, where

$$d_1 = g_1^{rID} = g_2^\alpha g_1^{-b} g_1^{rID} = g_2^\alpha g_1^{ID-b} = g_2^\alpha g_1^{ID(r - \frac{b}{ID})} = g_2^\alpha g_1^{r'ID} \quad (9)$$

$$d_2 = g^{-r} g_2^{\frac{1}{ID}} = g^{-(r - \frac{b}{ID})} = g^{-r'} \quad (10)$$

Decryption query:  $\mathcal{A}$  assigns  $\langle ID, C \rangle$  to  $\mathcal{B}$ .

$\mathcal{B}$  first executes the key generation query to identity  $ID$ , then decrypts  $C$  with the private key of identity  $ID$ .

*Challenge:*

$\mathcal{A}$  chooses two messages  $m_0, m_1$  of the same length and two identities  $ID_0, ID_1$  to  $\mathcal{B}$ , where  $ID_0, ID_1$  or their prefix have not appeared in any key generation query in Phase 1.

$\mathcal{B}$  randomly selects  $k', l' \in \{0, 1\}$ ,  $c \in Z_p^*$ , and construct  $m_l$  as follows:  
 $C = (C_1, C_2, C_3) = (TM_l, g^c, g_1^{ID_k \cdot c})$ . If  $T = e(g, g)^{\alpha bc}$ , we can obtain:

$$\begin{aligned} C &= (C_1, C_2, C_3) \\ &= \left( ZM_l, g^c, g_1^{ID_k \cdot c} \right) \\ &= \left( e(g, g)^{\alpha bc} M_l, g^c, g_1^{ID_k \cdot c} \right) \\ &= \left( e(g, g_2)^{\alpha c} M_l, g^c, g_1^{ID_k \cdot c} \right) \end{aligned} \quad (11)$$

Therefore,  $C$  is a valid ciphertext.

*Phase 2:*  $\mathcal{A}$  executes key generation queries and decryption queries to  $\mathcal{B}$  as in phase 1, except that the adversary may not request a private key for  $ID_0, ID_1$  or message  $m_0, m_1$ .

*Guess:*  $\mathcal{A}$  submits two guesses  $k', l' \in \{0, 1\}$ . If  $k' = k, l' = l$ , then  $\mathcal{B}$  outputs 1 which means  $T = e(g, g)^{\alpha bc}$ , otherwise it outputs 0 which means  $T \neq e(g, g)^{\alpha bc}$ .

When  $T = e(g, g)^{\alpha bc}$  then  $\mathcal{A}$  must satisfy  $|\Pr(k' = k \wedge l' = l) - \frac{1}{4}| \geq \varepsilon$ . When  $T$  is uniform then  $\Pr(k' = k \wedge l' = l) = \frac{1}{4}$ . Therefore, when  $\alpha, b, c, T$  are uniform, we have

$$\begin{aligned} & \left| \Pr \left( \mathcal{B} \left( g, g^\alpha, g^b, g^c, e(g, g)^{\alpha bc} \right) = 0 \right) \right| - \left| \Pr \left( \mathcal{B} \left( g, g^\alpha, g^b, g^c, T \right) = 0 \right) \right| \\ & \geq \left| \left( \frac{1}{4} + \varepsilon \right) - \frac{1}{4} \right| = \varepsilon \end{aligned} \quad (12)$$

This completes the proof of Theorem 1.

#### 4 Lightweight anonymous communication model in cloud computing

In this section, we construct a lightweight anonymous communication model based on anonymous IBE, which is introduced in Section 3.  $G_1$  and  $G_2$  are multiplicative

cyclic groups of prime order  $p$  and  $g$  is a generator of  $G_1$ . The map  $e$  is a bilinear map which satisfies  $e : G_1 \times G_1 \rightarrow G_2$ .  $\alpha \in Z_p^*$  is the master key of PKG,  $g_2 \in G_1$  is randomly selected, and  $g_1 = g^\alpha$ . Before formally introducing the anonymous communication model, we first give the definition of the symbols used in the model.

**Table 1 Notations.**

Notation	Meaning
$\alpha$	The master key generated by PKG
$ID_{ij}$	User's identity
$d_{ij}$	User $ID_{ij}$ 's private key
$m$	Message to be sent
$C$	Ciphertext
$G_1, G_2$	Multiplicative cyclic group
$g$	A generator of $G_1$
$p$	Prime order of $G_1, G_2$
$g_1$	$g_1 = g^\alpha$
$g_2$	Randomly selected in $G_1$
$r, t$	Randomly selected in $Z_p^*$

## 4.1 Model initialization

### 4.1.1 Entities

(1) The users. Users are very important to the system, and their privacy must be guaranteed. In order to meet the different needs of users, we have designed two encryption methods, which can meet two types of users:

(a) Users who need to send information anonymously and are unwilling to disclose their identity to the recipient. For example, in tip-offs, the whistleblower does not want anyone to know his identity.

(b) Users who need to disclose their identity to the recipient but do not want to inform other users of their identity. For example, in the bidding, the successful bidder needs to inform the bidding company of its identity so that it can continue to communicate after the bid, but it is not allowed to be known by other users in the system to prevent malicious competition.

(2) Bulletin board. The bulletin board is provided for users to upload and download ciphertexts. More precisely, the sender uploads the ciphertext to the bulletin board, and the receiver downloads the ciphertexts from the bulletin board. The bulletin board is an intermediate source for communication, and there is no direct interaction between the users. Because there is no interaction between the users, the adversary cannot directly know the identities of the two communicating parties.

(3) Private key generator (PKG). In this model, PKG generates the system's master secret key, generates the user's private key based on the user's identity, and is also responsible for grouping users. In addition, PKG is credible in this model.

### 4.1.2 Grouping of users

(1) Registration and grouping. When a user enters the system, the system automatically distributes a unique and fixed identity  $ID (ID \in Z_p^*)$  to the user. PKG is responsible for grouping all the users and dividing the users into  $M$  groups, where each group is of  $N$  members. To prevent traffic analysis attacks, the number of  $N$  should be large enough. An  $ID$  corresponds to a unique group number  $i$  and a serial number  $j$  in the group ( $i, j$  are randomly selected, and  $0 < i \leq M, 0 < j \leq N$ ).

We notate the user as  $ID_{ij}$ , and every trusted user knows the identities and group numbers of other users in the system.

(2) Private key generation. Users need to obtain their own private keys before starting communication. PKG generates the system's secret master key and the private key corresponding to each user. More specifically, PKG generates a random number  $r \in Z_p^*$ , a public parameter of the system  $params = (g, g_1, g_2)$ . The private key  $d_{ij}$  corresponding to the user  $ID_{ij}$  is as follows:

$$d_{ij} = (d_1, d_2) = \left( g_2^\alpha g_1^{ID_{ij} \cdot r}, g^{-r} \right) \quad (13)$$

After the private key is generated, PKG distributes the private key to the corresponding users.

#### 4.2 Anonymous communication model

In this section, we introduce how the anonymous communication model implements the communication process. At this stage, users divide time slices to encrypt messages, upload ciphertext, download ciphertext and decrypt ciphertext. During time  $T_1$ , the sender encrypts the message to be sent. During time  $T_2$ , all the users upload the ciphertext to the bulletin board. During time  $T_3$ , users download the ciphertext and decrypt the downloaded ciphertext during time  $T_4$ . The following includes the entire process.

(1) During time  $T_1$ , the sender encrypts message  $m$  using the recipient's identity  $ID_{ij}$  as the public key.

All the users, who want to transfer information in the system, will encrypt messages  $m$  according to the identity of receiver  $ID_{ij}$  at  $T_1$  time. At the same time, the sender also knows the group number of the receiver. In order to save memory costs, we design  $C_1$  as the group number  $i$  where the receiver is located. This is conducive to uploading the ciphertext to the bulletin board, and the receiver can quickly filter out the ciphertext that needs to be downloaded.

If the sender wants the receiver to know his/her identity, he/she can encrypt the message  $m$  as follows:

$$C = (C_1, C_2, C_3, C_4) = \left( i, e(g, g_2)^{\alpha t} \cdot \left( m \parallel \text{Sign}_{\text{send}_{ID_{ij}}} \right), g^t, g_1^{ID_{ij} \cdot t} \right) \quad (14)$$

Where  $t \in Z_p^*$  is randomly selected by the sender,  $ID_{ij}$  is the identity of the recipient,  $\text{Sign}_{\text{send}_{ID_{ij}}}$  is the signature of the sender's identity and  $C_1 = i$ ,  $i$  is the group number of the receiver.

If the sender's identity needs to be kept secret from the receiver, we use the following encryption:

$$C = (C_1, C_2, C_3, C_4) = \left( i, e(g, g_2)^{\alpha t} \cdot m, g^t, g_1^{ID_{ij} \cdot t} \right) \quad (15)$$

(2) During time  $T_2$ , all the users in the system must send ciphertext  $C$  to the bulletin board.

All users, whether they wish to communicate or not, must send the ciphertexts to the bulletin board, and the upload process is completed in time  $T_2$ . For users

who want to send information, upload the ciphertexts within time  $T_2$ . For security reasons, other users who need not communicate also complete the upload of a pseudo-ciphertext within time  $T_2$ .

(3) During time  $T_3$ , the users download the ciphertext  $C$  accordingly from the bulletin board.

After the ciphertexts have been uploaded to the bulletin board, all the users evaluate whether or not the  $C_1$  part of the ciphertexts is equal to their group number  $i$ , to determine whether to download the ciphertext. If  $C_i = i$ , then the recipient must download this ciphertext to avoid missing the messages. The above process is completed during time  $T_3$ .

(4) During time  $T_4$ , the user decrypts the downloaded ciphertext  $C$  with his/her private key  $d_{ij}$ .

All the users use their private keys to decrypt the downloaded ciphertexts one by one. If the decryption is successful, then the real receiver can receive the message sent by the sender. The decryption process is as follows:

$$m \parallel \text{Sign}_{\text{send}_{ID_{ij}}} = C_2 \cdot \frac{1}{e(C_3, d_1) e(d_2, C_4)} \quad (16)$$

$$m = C_2 \cdot \frac{1}{e(C_3, d_1) e(d_2, C_4)} \quad (17)$$

Figure 1 shows the process for the users and bulletin boards to transfer specific ciphertexts. During time  $T_2$ , all the users upload messages to the bulletin board. The red line indicates this process. During time  $T_3$ , the  $C_1$  part of the ciphertexts is equal to a group number in the model. As shown in Figure 1, we assume  $C_1 = 2$ , then all the users in the second group must download the ciphertexts to the local host, other groups will not download this ciphertext. This downloading process is indicated by the green line, and the black line indicates the available communication path in the model.

In consideration of the security of the model, when the number of the rounds of message delivery reaches a certain value, the private key's update and the group's update of the model are triggered. The process is as follows:

(1) Update of private key. When the entire system transmits 1000 rounds of messages, PKG regenerates private keys for all the users to strengthen the security of the system and prevent it from being cracked by the adversary.

(2) Update of group. When the entire system delivers 100 rounds of messages, PKG regroups all the users to strengthen the security of the system and prevent it from being cracked by the adversary.

## 5 Experiments and results

In this section, we evaluate the performance of our model, which has been implemented in Python. All experiments are conducted on a PC with a CPU 2.30 GHz, 8 GB of RAM. We compare the anonymous performance of our lightweight anonymous communication model with several existing anonymous models [6, 24, 25] in Table 2. It can be seen from Table 2 that only our model achieves all the anonymities, whereas the other models cannot.

**Table 2 Comparison of model performance.**

Anonymous communication Model	Sender anonymity	Receiver anonymity	Communication relationship anonymity
Onion Routing	unsatisfied	satisfied	satisfied
DCARPS	satisfied	unsatisfied	unsatisfied
Anonymous Path Routing	unsatisfied	unsatisfied	satisfied
Our model	satisfied	satisfied	satisfied

We evaluate the performance of our lightweight anonymous communication model, including the storage and communication costs. Table 3 shows that DCARPS has the smallest storage cost. However, it has the worst anonymity and security performance.

**Table 3 Performance comparison on storage cost.**

Anonymous communication Model	Storage cost (bits)
Onion Routing	At least two encryption operations and two decryption operations
DCARPS	No extra computation cost with constant IDs
Anonymous Path Routing	At least six hashing operations
Our model	One hashing operation, one encryption operation and one decryption operation

We assume that the communication cost of the whole network for message exchange is  $N$ . In addition, establishing pairwise keys for any two users has extra communication cost  $P$ ,  $\gamma$  is the communication cost of ACK messages ( $\gamma$  is the communication cost to confirm the start of the message delivery).

Our communication model uses the user's  $ID$  as the public key, so there is no need for paired secret key exchange. Similarly, according to our message delivery process, the sender does not need to send a confirmation message to the recipient before sending a message. So the communication cost of lightweight anonymous communication model is  $N$ .

**Table 4 Performance comparison on communication cost.**

Anonymous communication Model	Storage cost (bits)
Onion Routing	$P + N$
DCARPS	No extra communication cost with constant IDs
Anonymous Path Routing	$N + \gamma$
Our model	$N$

Through the above three tables, we find that our model achieves all three anonymities with low storage and computation costs.

## 6 Discuss

### 6.1 Security analysis

(1) Security of messages. The content of the message delivered by the user needs to be protected, which is the basic requirement of the security model. In our model, the information uploaded by users to the bulletin board is encrypted using an anonymous encryption scheme. We have verified its security in Section 3.3, this scheme cannot disclose any content about the user's identity in the ciphertexts, and at the same time, it can also resist any CCA adversary.

(2) Anonymity of messages.

(a) Sender anonymity. In traditional public key cryptography, there is usually a public key infrastructure (PKI), and the sender needs to query the receiver's public key before initiating the communication. In this process, the user performing the

query operation may be the sender who wishes to initiate communication, and the public key to be queried may belong to the receiver.

In our model, the sender no longer needs to query the receiver's public key, because the public key is the identity of the receiver that every user knows. We consider that all the users perform upload operations in time  $T_2$ . The adversary cannot determine which users are the real senders through the traffic analysis attack, which can ensure the sender's anonymity.

(b) Recipient anonymity. The recipient anonymity is to ensure that others cannot evaluate whether or not the message has been received by a certain receiver. In addition, the model also needs to guarantee that during the encryption process, the adversary cannot extract the identity of the receiver.

In our model, the receiver's identity is used as the public key, and the anonymous IBE scheme ensures that the adversary cannot extract the receiver's identity from the ciphertexts. During time  $T_3$ , all the members of the real receiver's group download the ciphertexts. On the other hand, there are relatively many members in the group, and the adversary does not know which member of the group is the real receiver, thus ensuring the receiver's anonymity.

## 6.2 Efficiency analysis

Our scheme has no limit on the number of ciphertexts that need to be sent in each round. Compared with the communication model that can only send one message in each round [11], the more messages we send in each round, the more efficient our model is. Similarly, compared to the anonymous communication model designed by Jiang et al. [17], our model manages users in groups. Before users download the ciphertexts, they need to be screened, which greatly reduces the number of ciphertexts that users download and need to decrypt. When delivering the same amount of messages, our solution saves time and memory on the basis of security.

## 7 Conclusion

In the past, the anonymous communication model had large requirements on network bandwidth and memory, and could not guarantee stability and reliability. It is inefficient, costly, and insecure when an anonymous communication model is used in small groups. In this paper, we design a lightweight anonymous communication model in cloud computing, which is suitable for small and medium-sized groups. In the proposed model, we design an anonymous IBE scheme, modify the ciphertext structure, and simplify the encryption process while ensuring security. Furthermore, all the users are organised in groups and all the ciphertexts are filtered before the downloading practice. The operations reduce the workload of users to download the ciphertexts and the number of the decrypted ciphertexts. Analysis results show that the communication model has better performance while ensuring security and anonymity. The proposed anonymous communication model has good application prospects in cloud computing. For the future work, we will continue to optimize the proposed anonymous communication model and further apply it into cloud computing to solve the problem of privacy leakage.

### Abbreviations

IBE: Identify-Based Encryption; DCARPS: Destination Controlled Anonymous Routing Protocol for Sensor networks.

### Competing interests

The authors declare that they have no competing interests.

### Funding

This study was funded by EU Horizon 2020 DOMINOES Project (Grant Number: 771066).

### Availability of data and materials

Data sharing is not applicable to this article as no datasets are generated or analyzed during the current study.

### Author's contributions

FL, YW, and HJ developed the analytical derivations. FL designed and run the simulations. FL, XY, and ZW wrote the manuscript. FL, YW, and HJ proofread the manuscript. All authors read and approved the final manuscript.

### Acknowledgements

The authors thank the person who provided meticulous and valuable suggestions for improving the paper.

### Author details

<sup>1</sup>School of Information Science and Engineering, Qufu Normal University, Rizhao, China. <sup>2</sup>Experimental Teaching and Equipments Management Center, Qufu Normal University, Rizhao, China. <sup>3</sup>School of Informatics, University of Leicester, Leicester, UK.

### References

1. Liu, H., Kou, H., Yan, C., Qi, L.: Keywords-driven and popularity-aware paper recommendation based on undirected paper citation graph. *Complexity* **2020**, 2085638–1208563815 (2020)
2. Wang, H., Ma, S., Dai, H.-N., Imran, M., Wang, T.: Blockchain-based data privacy management with nudge theory in open banking. *Future Generation Computer Systems* **110**, 812–823 (2020)
3. Abusukhon, A., Bilal, H.: A secure network communication protocol based on text to barcode encryption algorithm. *International Journal of Advanced Computer Science and Applications* **6**(12), 64–70 (2015)
4. Aaron, J., Chris, W., Rob, J., Micah, S., Paul, S.: Users get routed: Traffic correlation on tor by realistic adversaries. In: *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, pp. 337–348 (2013)
5. L., C.D.: Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM* **24**(2), 84–90 (1981)
6. G, R.M., F, S.P., M, G.D.: Anonymous connections and onion routing. *IEEE Journal on Selected areas in Communications* **16**(4), 482–494 (1998)
7. Paul, S., D, G., M, R.: Onion routing for anonymous and private internet connections. *Communications of the ACM* **42**(2), 5 (1999)
8. Kevin, B., Damon, M., Dirk, G., Tadayoshi, K., Douglas, S.: Low-resource routing attacks against tor. In: *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society*, pp. 11–20 (2007)
9. Sambuddho, C., Angelos, S., D, K.A.: Identifying proxy nodes in a tor anonymization circuit. In: *2008 IEEE International Conference on Signal Image Technology and Internet Based Systems*, pp. 633–639 (2008). IEEE
10. Nicholas, H., Y, V.E., Eric, C.-T.: How much anonymity does network latency leak? *ACM Transactions on Information and System Security (TISSEC)* **13**(2), 1–28 (2010)
11. David, C.: The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of cryptology* **1**(1), 65–75 (1988)
12. Fatemeh, S., Milivoj, S., Rizwan, A.M., Michael, B., Claudia, D.: A survey on routing in anonymous communication protocols. *ACM Computing Surveys (CSUR)* **51**(3), 1–39 (2018)
13. Liu, Z., Liu, Y., Winter, P., Mittal, P., Hu, Y.-C.: Torpolice: Towards enforcing service-defined access policies for anonymous communication in the tor network. In: *2017 IEEE 25th International Conference on Network Protocols (ICNP)*, pp. 1–10 (2017). IEEE
14. Xu, X., Zhang, X., Gao, H., Xue, Y., Qi, L., Dou, W.: Become: Blockchain-enabled computation offloading for iot in mobile edge computing. *IEEE Trans. Ind. Informatics* **16**(6), 4187–4195 (2020)
15. Zheng, P., Zheng, Z., Dai, H.: Xblock-eth: Extracting and exploring blockchain data from ethereum. *IEEE Open Journal of the Computer Society* **1**, 95–106 (2020)
16. Wang, W., Song, J., Xu, G., Li, Y., Wang, H., Su, C.: Contractward: Automated vulnerability detection models for ethereum smart contracts. *IEEE Transactions on Network Science and Engineering* (2020)
17. Jiang, L., Li, T., Li, X., Atiquzzaman, M., Ahmad, H., Wang, X.: Anonymous communication via anonymous identity-based encryption and its application in iot. *Wireless Communications and Mobile Computing* **2018** (2018)
18. Antonela, D., Roger, D., Arthur, E., M, F.: Addressing denial of service attacks on free and open communication on the internet. *The Tor Project, Tech. Rep.* (2018)
19. Dan, B., Matt, F.: Identity-based encryption from the weil pairing. In: *Annual International Cryptology Conference*, pp. 213–229 (2001). Springer
20. Antoine, J.: A one round protocol for tripartite diffie–hellman. In: *International Algorithmic Number Theory Symposium*, pp. 385–393 (2000). Springer
21. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: *Annual International Cryptology Conference*, vol. 3621, pp. 258–275 (2005). Springer
22. Dan, B., Xavier, B., Eu-Jin, G.: Hierarchical identity based encryption with constant size ciphertext. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 440–456 (2005). Springer
23. Gentry, C.: Practical identity-based encryption without random oracles, vol. 4004, pp. 445–464 (2006). Springer

24. Sheu, J., Jiang, J., Tu, C.: Anonymous path routing in wireless sensor networks. In: Proceedings of IEEE International Conference on Communications, ICC 2008, Beijing, China, 19-23 May 2008, pp. 2728–2734 (2008). IEEE
25. Nezhad, A.A., Miri, A., Makrakis, D.: Location privacy and anonymity preserving routing for wireless sensor networks. *Comput. Networks* **52**(18), 3433–3452 (2008)

**Figures**

**Figure 1 Lightweight anonymous communication model.** This represents the process of uploading and downloading ciphertexts.