Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 6809796, 8 pages
https://doi.org/10.1155/2018/6809796

Research Article

Anonymous Communication via Anonymous Identity-Based Encryption and Its Application in IoT

Liaoliang Jiang,[1] Tong Li,[1] Xuan Li,[2] Mohammed Atiquzzaman,[3] Haseeb Ahmad,[4] and Xianmin Wang[1]

[1] *School of Computer Science, Guangzhou University, Guangzhou 510000, China*
[2] *College of Mathematics and Informatics, Fujian Normal University, Fujian 350000, China*
[3] *School of Computer Science, The University of Oklahoma, USA*
[4] *Department of Computer Science, National Textile University, Faisalabad, Pakistan*

Correspondence should be addressed to Tong Li; 1120140107@mail.nankai.edu.cn

Received 30 June 2018; Accepted 24 September 2018; Published 21 November 2018

Guest Editor: Karl Andersson

Under the environment of the big data, the correlation between the data makes people have a greater demand for privacy. Moreover, the world has become more diversified and democratic than ever before. Freedom of speech is considered to be very important; thus, anonymity is also a very important security demand. The research of our paper proposes a scheme which can ensure both the privacy and the anonymity of a communication system, that is, the protection of message privacy while ensuring the users' anonymity. It is based on anonymous identity-based encryption (IBE), by which the users' *metadata* are protected. We implement our scheme in JAVA with Java pairing-based cryptography library (JPBC); the experiment shows that our scheme has significant advantage in efficiency compared with other anonymous communication system. Internet-of-Things (IoT) involves many devices, and privacy of devices is very significant. Anonymous communication system provides a secure environment without leaking metadata, which has many application scenarios in IoT.

1. Introduction

In the era of big data, data privacy has become significant as more personal and organizational information is involved. Moreover, the world has become more diversified and democratic than ever before. Following this trend, researchers have unveiled various ways through which adversaries can access private or otherwise sensitive information by network breach such as a called telephone number [1] or the IP address [2]. Therefore, the ultimate objective of privacy is to protect not only the contents of the messages but also the identities of communication parties, the actual time of a communication, and specific user participation during communication. For the above reasons, the research on privacy protection protocols such as anonymous communication system is imperative. In an anonymous communication system, the adversary must not know participant's identity at any time. Further, the adversary should not know the sending and receiving entities and whether a message is valuable. Overall, such pieces of information are called *metadata*. The *metadata* involves crucial private data in the anonymous communication system and it is also a critical parameter of the monitoring for the government and other stakeholders [3]. Anonymous communication system is very practical, and it can be applied to many realistic scenarios. Cloud computing has received more and more attention in recent years, and privacy-preserving and security under cloud environment have become critical issues [4–7], so high-level anonymity is required. In the neural network [8, 9] and secure deduplication [10], the anonymity is also critical.

Some private messaging systems are built on previous work [11–14]. However, such schemes do not provide efficient protocols without leaking *metadata*, which breaches the purpose of anonymous communication systems. There exist two categories of anonymous communication protocols. The first one is called Tor [15], which achieves the anonymity by encrypting the messages in layers under the public key cryptography. Several servers are employed in Tor, and the message is encrypted into a data packet by all servers' public key in turns (the construction of an onion). The encrypted data package is transmitted by the *chain* comprised of all servers. As a server receives a data package, it decrypts the data package through its private key and sends the decrypted data package to the next server; each server carries out the decryption operation until the data package is sent to the recipient. Tor is secure as each server knows only its predecessor and successor rather than other servers' position in the chain; therefore, the servers do not know the specific path of a message's transmission, which guarantees the anonymity of both the sender and recipient. That is how it offers a practical scheme of identity protection. However, some researchers showed that this scheme cannot defend against the traffic analysis attacks [16–18]. Tor's hidden service requires that every server must be honest; for instance, the security will be breached if the "first-server" and the "last-server" make a collusion. The second category is based on the DC-net [19, 20], for instance, verdict [21] and dissent [22]. Those schemes work on an N-member group, who can communicate anonymously, and only one group member is allowed to send a valid message in a given round. Each member shares a value secretly with the other N-1 members, which means that each member has N-1 secret values that are shared with the other N-1 members. Then, each member performs XORs operations with the N-1 shared secret values, but the legitimate sender performs the XORs with the N-1 shared secret values along with an additional message to generate ciphertexts that are later broadcast to the other members. Subsequently, each member receives all the ciphertexts and performs XORs operation on the N ciphertexts together to reveal the message. Because all the shared secret values had been XORed twice, they are cancelled out; thus, the message is extracted but without leaking the identity of the sender. In this way, the DC-net can prevent the traffic attack, as the DC-net is built on *anytrust* model that remains secure until at least one participating server remains honest. However, the recovery of messages must be computed by all the users, which is unrealistic scenario as none of the users could be off-line during underlying process. Hence, the existing methods are vulnerable to the internal dishonest member attacks which can easily break the security. Although, the systems may trace the dishonest member, they cannot exclude the influence of dishonest member during the communication. In summary, these two schemes above are of low-efficiency and the cost of communication is high.

In this paper, we propose an efficient anonymous communication scheme that offers higher security while disposing the aforementioned attack. The proposed scheme incorporates anonymous identity-based encryption (IBE) to achieve anonymous communication. In our scenario, more than one message can be sent simultaneously in each round. Meanwhile, each user uses its ID as the public key; we assume that the ID of each user is unique and it must be well known to other users. We set up a bulletin board from where every user could upload or download the ciphertexts directly at specific time during each round. The recovery of the message is based on the decryption by the recipient rather than the cooperations of all the users, so the system does not need the users to be on-line all the time during the communication, which is a remarkable advantage compared with the verdict and dissent. Since every user has to perform the same operation at the same time, the adversary cannot analyze who is the sender and who is the recipient in a given round. This characteristic ensures strong anonymity of the users.

The primary contributions of the paper are listed as follows:

(1) The user can send and receive the ciphertext during the same round, which means a user can be both a sender and a recipient at the same time. This can improve the efficiency of anonymous communication system.

(2) Our scheme allows the users to send or receive more than one valid "ciphertext" (because the message is extracted after decrypting the ciphertext) in each round. There is no limit to the number of communication ciphertexts. It is a huge advantage compared with other anonymous communication systems which are based on DC-net; this characteristic greatly improves the efficiency of anonymous communication system and reduces the cost of communication.

(3) In the proposed scheme, some dishonest users are tolerable in the communication, because a single user can successfully recover the message by himself instead of through the cooperation of all the other users.

Section 3 introduces the basic concepts of bilinear pairing, IBE and anonymous IBE. Section 4 outlines the system architecture and our security goals, and Section 5 describes the specific scheme and its two protocols. Section 6 presents a security analysis of the proposed system.

2. Related Work

Anonymous communication system has a high-level demand for security; we may consider a mechanism for entering into the anonymous communication system before starting communication. Users can do anonymous authentication before joining the system [23]; only a legal user can be a member of the system. Anonymous authentication can apply to many areas [24–27]. Besides, we can make an improvement of the storage pattern for users' messages. We may combine oblivious RAM [28, 29] with our anonymous communication system; oblivious RAM hides the access patterns of data, and it can prevent adversary from speculating sensitive information through users' access patterns. In the end, we may use other cryptographical techniques [30–33] to enhance the security of our anonymous communication system.

3. Preliminaries

This section outlines the anonymous IBE scheme [34], the difference between ordinary IBE and anonymous IBE. Although the identity-based encryption was firstly proposed by Shamir [35], a practical IBE scheme was constructed by Boneh and Franklin in 2001 [36], and after that, many IBE schemes were proposed [37–40]. The conception of anonymous identity-based encryption was firstly proposed in [41]. This section also introduces the basic knowledge of bilinear pairings, which are used to construct the scheme in the following sections.

3.1. Bilinear Map. Let G_1 be the additive cycle group generated by g and G_2 be multiplicative cyclic group. Prime p is the order of G_1 and G_2. The map $e : G_1 \times G_1 \longrightarrow G_2$ is called bilinear map, if it satisfies the following properties:

(1) Bilinearity: For any $P, Q \in G_1, a, b \in Z$, the following formula holds: $e(P^a, Q^b) = e(P, Q)^{ab}$.

(2) Nondegeneracy: The map e does not map all the pairs in the $G_1 \times G_1$ to the generator in G_2. If P is the generator of G_1, then $e(P, P)$ is the generator of G_2.

(3) Computability: For any P and Q, there is an algorithm that can compute $e(P, Q)$ efficiently.

3.2. IBE. In the IBE scheme, the participating parties include the users and the private key generator (PKG). The identity of the user is considered as the public key that makes IBE different from the traditional public key cryptography. The PKG, which is a trusted third party, generates the private key based on its master key and the user's identity. Subsequently, the private key is distributed to the corresponding user by the PKG. IBE is advantageous and is widely used for information security protection. Firstly, the key management is easy and efficient, because it does not require distributing public key or revoking the key. Secondly, IBE removes the certificate requirement for the public key of user who participates in the communication. For instance, when Alice wants to send a message to Bob, she uses Bob's public key ID_{Bob} that is known to each user. Alice encrypts the message with Bob's identity ID_{Bob} rather than querying Bob's public key from the PKI. This characteristic highlights the purpose of anonymous communication. Suppose that Alice queries Bob's public key from the PKI; the adversary can easily get information about sender/recipient through the operation of querying, so the security goals are breached. After Bob gets the encrypted message, he decrypts the message with his private key that he gets from the PKG. IBE consists of the following four functions [42]:

Setup: inputting security parameter k, returning the public parameter *params* and the master key *msk* of the system. The limited plaintext space M, the limited ciphertext space C, and the *params* are public, and the master key *msk* is secretly kept by the PKG.

Extract: inputting the master key *msk* and a user's identity *id*, generating the corresponding private key sk_{id} for *id*.

Encryption: inputting the message $m \in M$ and *id*, returning the ciphertext $c \in C$.

Decryption: inputting the ciphertext c and the corresponding private key sk_{id} for *id*, returning the plaintext m.

3.3. Anonymous IBE. In traditional IBE, since the recipient's identity is used as the public key, this property may leak the recipient's identity through the adversary's analysis of the ciphertexts. In other words, if the user's identity is leaked, the anonymous communication system is no longer secure. An anonymous IBE scheme must obey two properties:

(1) The adversary cannot get any information about the communication parties.

(2) The user's identity cannot be unveiled by the ciphertexts.

In this paper, we use the anonymous IBE scheme which is based on bilinear map [34]. Let G_1 and G_2 be the group of order p; the map $e : G_1 \times G_1 \longrightarrow G_2$ is the bilinear map, and g is the generator of group G_1. $\sigma \in Z_{p^*}$, $g_2 \in G_1$ are randomly selected, and let $g_1 = g^{\sigma}$. The scheme includes four functions as follows:

Initialization: choose the public parameters g, g_1, g_2 and the master key of PKG denoted as σ.

Private key generation: the PKG randomly selects $r \in Z_{p^*}$ and computes the private key for the corresponding recipient; here ID is the recipient's ID and $ID \in Z_{p^*}$.

$$d = (d_1, d_2, d_3) = \left(g_2^{\sigma} g_1^{ID \cdot r}, g^{r}, g^{ID \cdot r}\right) \tag{1}$$

Encryption: suppose a message $m \in G_2$ needs to be encrypted. The sender randomly selects $t, s \in Z_{p^*}$ and computes the ciphertext.

$$c = (c_1, c_2, c_3, c_4) = \left(e\left(g_1, g_2\right)^{t} \cdot m, g_1^{ID(t+s)}, g_1^{s}, g^{t}\right) \tag{2}$$

Decryption: the recipient uses his own private key $d = (d_1, d_2, d_3)$ to decrypt the ciphertext to obtain the plaintext as follows.

$$m = c_1 \cdot \frac{e\left(d_2, c_2\right)}{e\left(d_1, c_4\right) e\left(d_3, c_3\right)} \tag{3}$$

Suppose that an adversary wants to extract the recipient's identity ID from the ciphertext, it is obvious from the structure of the ciphertext that the ID can only be extracted through $c_2 = g_1^{ID(t+s)}$ by using $c = (c_1, c_2, c_3, c_4)$. Although g_1 is a public parameter, but the t, s are randomly selected from the Z_{p^*} and it is impossible for the adversary to obtain these parameters. Meanwhile, $ID(t + s)$ is the exponent of c_2; the computation is complicated.

4. Architecture of the System

We describe the details of system entities and system architecture in this section; furthermore, we present the security goals of anonymous communication.

4.1. Entities. (i) **The users.** The users are an imperative part of the system whose privacy must be assured, while the users can communicate with any user in the system. The system can satisfy two kinds of users. The first kind is those who just want to disclose some message anonymously; however, the users of this kind do not want to disclose the identity of the sender even to the recipient, for instance, a journalist wants to disclose a scandal about a politician who has participated in the presidential campaign. The second kind of users want to communicate with someone secretly; the users of this kind do not want anyone to know who is communicating with them, or whether he is involved in this communication. For instance, two executives from a tendering company want to negotiate about the final bidding price though geographical differences.

(ii) **Bulletin board.** The bulletin is provided to the users for uploading and downloading ciphertexts. More precisely, the sender uploads the encrypted message to the bulletin board, and the recipient downloads the message from the bulletin board. But as we mentioned above, the bulletin board is an intermediate source for communication, and there is no need for an interaction between users. Because there is no interaction between users, the adversary cannot know the identities of the communicating parties.

(iii) **Private key generator (PKG).** In the system, the role of PKG is to generate private keys of users against their IDs and we assume that PKG is honest.

4.2. Architecture. This section describes the architecture of the system. Each user has a unique identity. The system consist of two components.

(1) The Private Key Protocol. This is a protocol for distributing the private keys among the users according to their identity; this part works between the users and PKG. In order to carry out the decryption operation later, the user should obtain its private key before initiating a communication. The PKG generates the private key through users' identity and its master key for the corresponding users. For instance, Alice's identity is ID_{Alice} and Bob's identity is ID_{Bob}; the PKG generates private key sk_{Alice} for Alice and sk_{Bob} for Bob. Only by obtaining the private key, the later protocol can proceed. All the users should get their private key in specific time t_1.

(2) Communicating Protocol. It is the most important part of the system and it contains four operations. The user uses the recipient's identity as the public key to encrypt the message. For instance, Alice wants to send a message to Bob; Alice uses Bob's identity ID_{Bob} to encrypt the message. The encryption operation should be done in specific time t_2. For consideration of senders' anonymity, every user is required to send at least one message whether the user wants to have a communication or not. After the encryption operation, all the ciphertexts should be uploaded to the bulletin board. The uploading operation should be done in specific time t_3. In specific time t_4, each user downloads all the ciphertexts on the bulletin board. Since the users did not interact before and also the users do not know whether there is any message belonging to them in this round, all the messages in the bulletin board must be downloaded by each user in order not to miss the message.

All the users decrypt all the ciphertexts through its private key in specific time t_5. After time t_5, one round of communication during all the users is finished, and then the next round of communication can start. The subsequent communication rounds are scheduled as shown in Figure 1. In this paper, we have distinct advantage over the previous works. The advantage is that there is no limit to the number of messages sent by the user in each round, which means that one user can communicate with one or more users at a given round.

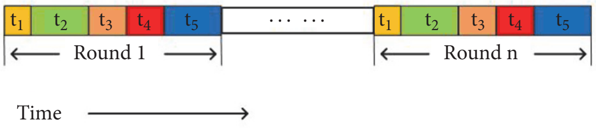


Figure 1: Scheduling of n rounds of communication.

4.3. Security Goal. The system ensures anonymous communication in three aspects.

(1) The message's security: The contents of users' message need to be protected, it is the basic requirement of a secure system.

(2) The sender's anonymity: Unauthorized users could not determine the identity of sender, so the adversary cannot judge which user sent a message in a given round. In other words, the identity of sender should not be leaked.

(3) The recipient's anonymity: The recipient's anonymity is to ensure that others cannot judge whether the message is received by a definite recipient. Furthermore, the system is required to guarantee that the adversary cannot extract the recipient's ID which is used during the process of encryption. Similar to sender's anonymity, the identity of recipient should not be leaked.

The sender's anonymity and the recipient's anonymity are the key security goals which are different from the traditional communication system, as the system should not reveal any *metadata* about users.

5. Anonymous Communication via Anonymous IBE

The scheme consists of two major components: private key generation and anonymous communication. In the presented solution, we construct a general scheme based on anonymous IBE which is provided in Section 3.3. G_1 and G_2 are the groups of order p, and g is the generator of group G_1. The map e is bilinear map which satisfies $G_1 \times G_1 \longrightarrow G_2$. $\sigma \in Z_{p^*}$ is the master key of PKG, $g_2 \in G_1$ are randomly selected, and let $g_1 = g^{\sigma}$. This section describes the construction of these two protocols.

5.1. Private Key Generation Protocol. The private keys are generated through the users' ID by PKG, then PKG distributes those private keys to corresponding users.

The details of private key generation protocol are described in Algorithm 1, where PKG randomly chooses an integer $r \in \mathbb{Z}_p^*$ and uses r to compute the private key k. After the computation, the PKG distributes the private key to the corresponding users.

5.2. Anonymous Communication Protocol. In our scheme, the anonymous communication protocol contains four steps as presented in Figure 2. The steps include encryption,

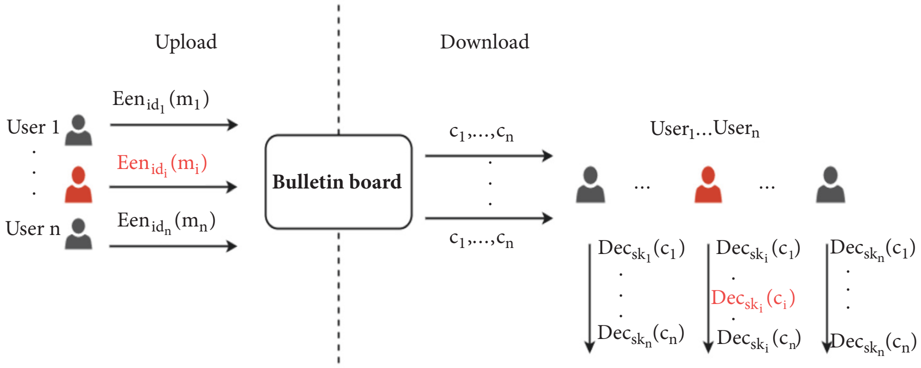

Upload
Download
User 1
User n
$\mathrm{Een}_{id_1}(m_1)$
$\mathrm{Een}_{id_i}(m_i)$
$\mathrm{Een}_{id_n}(m_n)$
Bulletin board
$c_1,\ldots,c_n$
$c_1,\ldots,c_n$
$\mathrm{User}_1\ldots\mathrm{User}_n$
$\mathrm{Dec}_{sk_1}(c_1)$
$\mathrm{Dec}_{sk_n}(c_n)$
$\mathrm{Dec}_{sk_i}(c_1)$
$\mathrm{Dec}_{sk_i}(c_i)$
$\mathrm{Dec}_{sk_i}(c_n)$
$\mathrm{Dec}_{sk_n}(c_1)$
$\mathrm{Dec}_{sk_n}(c_n)$

Figure 2: The four steps of anonymous communication protocol: ① Encryption, ② Upload, ③ Download, ④ Decryption.

```
Input: A user's identity $id$, the public parameters $g, g_1, g_2$, and the master key $\sigma$.
Output: The user's private key $k = (k_1, k_2, k_3)$.
  The PKG performs the followings:
  randomly chooses $r \in \mathbb{Z}_p^*$;
  computes the private key $k = (k_1, k_2, k_3) = (g_2^{\sigma} g_1^{id\cdot r}, g^r, g^{id\cdot r})$;
  sends the private key to the corresponding users at specific time $t_1$;
```

Algorithm 1: Private key protocol.

(1) **Encryption**. If the sender just wants to disclose the message anonymously rather than anyone knows where is message from even the recipient, he computes the ciphertext $c = (c_1, c_2, c_3, c_4) = (e(g_1, g_2)^t \cdot m, g_1^{id(t+s)}, g_1^s, g^t)$; If the sender wants the recipient to know about its identity, the signature $Sign_{Sender_{id}}$ should be attached with the message m, compute the ciphertext $c = (c_1, c_2, c_3, c_4) = (e(g_1, g_2)^t \cdot (m \| Sign_{Sender_{id}}), g_1^{id(t+s)}, g_1^s, g^t)$. The **Encryption** operation should done in specific time t_2.
(2) **Upload**. All the users uploads their ciphertexts c to the bulletin board at the specific time t_3. Each user's ciphertexts c are stored in the bulletin board after this operation.
(3) **Download**. Each involved users are required to download all the ciphertexts which stored in the bulletin board, each user does the **Download** operation at the specific time t_4.
(4) **Decryption**. The user decrypts the ciphertexts c which obtained from the bulletin board in **Download** operation, one by one through the private key k in specific time t_5. The plaintext is computed as $m = c_1 \cdot e(d_2, c_2)/e(d_1, c_4)e(d_3, c_3)$. If there is a signature $Sign_{Sender_{id}}$ attached with the message m, then the user can get $m \| Sign_{Sender_{id}}$.

Algorithm 2: Anonymous communication protocol.

uploading, downloading, and decryption. The protocol is performed collaboratively by the users and the bulletin board.

In the anonymous communication protocol, each user u needs to encrypt his message to generate the ciphertext $c = (c_1, c_2, c_3, c_4)$. He first randomly selects $t, s \in Z_{p^*}$. Here, m is the message which needs to be encrypted, id is the recipient's ID, $Sign_{Sender_{id}}$ is the signature of sender's identity. As we mentioned in Section 4.1, our system can satisfy two kinds of users. If the sender wants the recipient to know where the message is from, the signature can be attached together with the message m. Otherwise, the signature is not necessary to be transmitted. Subsequently, the encrypted message c can be uploaded to the bulletin board. At this step, each user is required to upload at least one encrypted message whether he wants to initiate a communication or not. However, if a user wants to communicate with more than one user, it is permitted to upload more than one ciphertext at the same time. When a user wants to get a message, he needs to download all the ciphertexts from the bulletin board without any interaction with the uploaders. Then, the user just needs to use his private key to decrypt the ciphertexts one by one. If the decryption is successfully performed, it means that the message belongs to the user. It should be noted that each user is required to download all the messages on the bulletin board. Since there are no interactions between the users and the bulletin board before the communication, each user has no idea whether the message belongs to him in the process of a communication. In this way, all the users have to participate in the uploading and downloading operations, while the adversary does not know which parties are really involved in a given round. The details of anonymous communication protocol are shown in Algorithm 2.

6. Security Analysis

As we mentioned in Section 4.3, there are three aspects of security goals needed to be achieved: the message's security, the sender's anonymity, and the recipient's anonymity, and we will analyze the system security as follows.

Every message is encrypted before uploading and the encryption scheme we used can ensure the message's security. The security of encryption scheme we used in our construction had been proved in [34], this encryption scheme can defend against an arbitrary CPA adversary while maintaining anonymity.

In traditional public key cryptography, there is usually a public key infrastructure (PKI), and the sender needs to query the recipient's public key before initiating a communication. In this process, the user who does the operation of querying is likely to be the sender who wants to initiate a communication, and the public key to be queried likely belongs to the recipient. In our scheme, the sender no more needs to query the recipient's public key (because the public key is recipient's identity which is known to each user). On the other hand, although the recipient's identity is used as the public key, the anonymous IBE ensures that the adversary cannot extract the recipient's identity from the ciphertext. Since all the users perform the operation of uploading at time t_3 and download the same amount of ciphertexts at time t_4, the adversary cannot know which user has the intention to participate in a communication through the operations of uploading and downloading. Obviously, our scheme can guarantee the anonymity of both the sender and recipient.

7. Evaluation

In this section, we evaluate the performance of our scheme, which has been implemented in JAVA with Java pairing-based cryptography library (JPBC). All experiments were conducted on a PC with a CPU 2.13 GHz, 6 GB of RAM. In our implementation, a message's length was set as 128 bytes, and the time consumption of uploading and downloading was ignored.

7.1. Computational Consumption. We implemented our scheme in one message and executed 1000 rounds. The computational consumption includes three operations: private key generation, encryption, and decryption. Under the fiber configuration of 100 Mpbs, the cost of uploading and downloading is negligible. We calculate the time cost as in Figure 3. It takes approximately 3.6×10^4 ms to perform the private key generation operation for 1000 rounds, 1.12×10^5 ms to perform the encryption operation for 1000 rounds, and 1.62×10^2 ms to perform the decryption operation for 1000 rounds.

7.2. Communication Consumption. Our scheme has no limit for the number of messages in a round, it is a significant advantage compared with other anonymous communication systems which can send only one message in a round. There are common scenarios; for example, a user wants to communicate with more than one person, or more than one user wants to send message. In the anonymous communication system which limits the number of messages, users have to wait for several rounds. But, in our scheme, all users can send an arbitrary number of messages in a round. This property enhances the efficiency of communication and reduces the cost of communication. Figure 4 shows the communication consumption of our scheme and the anonymous communication system which limits the number of messages.

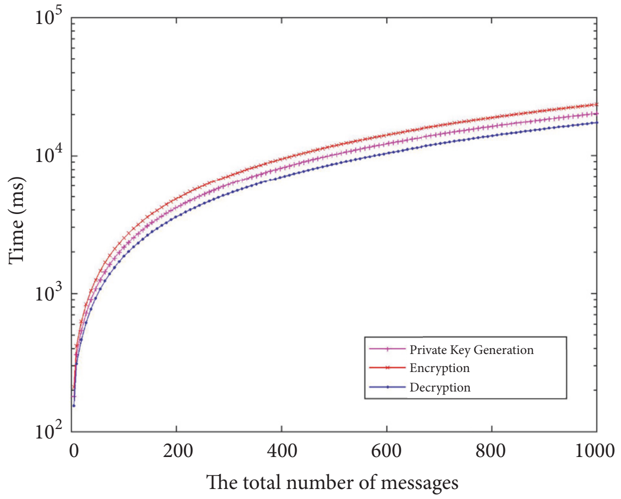


Figure 3: Computational consumption.

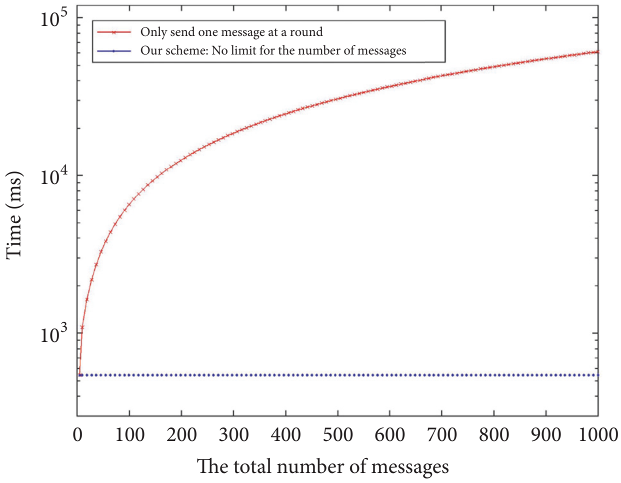


Figure 4: Communication consumption.

8. Conclusions

In this paper, we address a communication system which aims to protect the users' *metadata*. To solve this problem, we propose an anonymous communication system based on anonymous IBE. Our scheme has significant advantage in efficiency compared with previous work and can also offer strong anonymity. In the future, we will consider the user authentication and the application scenario in the smart environment.

Data Availability

The library used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts interests.

Authors' Contributions

The first author conducted the experiments and wrote the first draft of the paper. The other coauthors helped in revising the paper and polished it. All authors read and approved the final manuscript.

Acknowledgments

This work was supported by National Natural Science Foundation of China (No. 61472091), Natural Science Foundation of Guangdong Province for Distinguished Young Scholars (2014A030306020), Guangzhou Scholars Project for Universities of Guangzhou (No. 1201561613), and Science and Technology Planning Project of Guangdong Province, China (2015B010129015).

References

[1] J. Mayer, P. Mutchler, and J. C. Mitchell, "Evaluating the privacy properties of telephone metadata," *Proceedings of the National Acadamy of Sciences of the United States of America*, vol. 113, no. 20, pp. 5536–5541, 2016.

[2] Y.-A. de Montjoye, *Computational PRIvacy: Towards PRIvacy-Conscientious Uses of Metadata*, ProQuest LLC, Ann Arbor, MI, 2015.

[3] A. Rusbridger, "The snowden leaks and the public," *New York Review of Books*, vol. 60, no. 18, 2013.

[4] P. Li, J. Li, Z. Huang et al., "Multi-key privacy-preserving deep learning in cloud computing," *Future Generation Computer Systems*, vol. 74, pp. 76–85, 2017.

[5] C. Gao, Q. Cheng, X. Li, and S. Xia, "Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network," *Cluster Computing*, pp. 1–9, 2018.

[6] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, "Privacy-preserving outsourced classification in cloud computing," *Cluster Computing*, pp. 1–10, 2017.

[7] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, pp. 1–12, 2018.

[8] Y. Li, G. Wang, L. Nie, Q. Wang, and W. Tan, "Distance metric optimization driven convolutional neural network for age invariant face recognition," *Pattern Recognition*, vol. 75, pp. 51–62, 2018.

[9] C. Yuan, LiXinting, J. Q. M. Wu, j. Li, and X. Sun, "Fingerprint liveness detection from different fingerprint materials using convolutional neural network and principal component analysis," *Computers, Materials & Continua*, vol. 53, no. 3, pp. 357–371, 2017.

[10] J. Li, X. Chen, M. Li, J. Li, P. P. C. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp. 1615–1625, 2014.

[11] N. Borisov, G. Danezis, and I. Goldberg, "DP5: A Private Presence Service," *Proceedings on Privacy Enhancing Technologies*, vol. 2015, no. 2, pp. 4–24, 2015.

[12] D. Chaum, D. Das, F. Javani et al., "cMix: Mixing with Minimal Real-Time Asymmetric Cryptographic Operations," in *Applied Cryptography and Network Security*, vol. 10355 of *Lecture Notes in Computer Science*, pp. 557–578, Springer International Publishing, Cham, 2017.

[13] A. Kwon, D. Lazar, S. Devadas, and B. Ford, "Riffle: An efficient communication system with strong anonymity," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 2, pp. 115–134, 2016.

[14] J. Van Den Hooff, D. Lazar, M. Zaharia, and N. Zeldovich, "Vuvuzela: Scalable private messaging resistant to traffic analysis," in *Proceedings of the 25th ACM Symposium on Operating Systems Principles, SOSP 2015*, pp. 137–152, USA, October 2015.

[15] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," Defense Technical Information Center, 2004.

[16] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker, "Low-resource routing attacks against Tor," in *Proceedings of the 6th ACM Workshop on Privacy in the Electronic Society, WPES'07, Held in Association with the 14th ACM Computer and Communications Security Conference*, pp. 11–20, USA, October 2007.

[17] S. Chakravarty, A. Stavrou, and A. D. Keromytis, "Identifying proxy nodes in a tor anonymization circuit," in *Proceedings of the 4th International Conference on Signal Image Technology and Internet Based Systems, SITIS 2008*, pp. 633–639, Indonesia, December 2008.

[18] N. Hopper, E. Y. Vasserman, and E. Chan-Tin, "How much anonymity does network latency leak?" *ACM Transactions on Information and System Security*, vol. 13, no. 2, 2010.

[19] D. Chaum, "The dining cryptographers problem: unconditional sender and recipient untraceability," *Journal of Cryptology. The Journal of the International Association for Cryptologic Research*, vol. 1, no. 1, pp. 65–75, 1988.

[20] P. Golle and A. Juels, "Dining cryptographers revisited," in *Advances in cryptology—EUROCRYPT 2004*, vol. 3027 of *Lecture Notes in Comput. Sci.*, pp. 456–473, Springer, Berlin, 2004.

[21] H. Corrigan-Gibbs, D. I. Wolinsky, and B. Ford, "Proactively accountable anonymous messaging in verdict," in *Proceedings of the USENIX Security Symposium*, pp. 147–162, 2013.

[22] E. Syta, A. Johnson, H. Corrigan-Gibbs, S. Weng, D. Wolinsky, and B. Ford, "Security Analysis of Accountable Anonymous Group Communication in Dissent," Defense Technical Information Center, 2013.

[23] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 912–925, 2018.

[24] J. Shen, C. Wang, T. Li, X. Chen, X. Huang, and Z.-H. Zhan, "Secure data uploading scheme for a smart home system," *Information Sciences*, vol. 453, pp. 186–197, 2018.

[25] J. Xu, L. Wei, Y. Zhang, A. Wang, F. Zhou, and C. Gao, "Dynamic Fully Homomorphic encryption-based Merkle Tree for lightweight streaming authenticated data structures," *Journal of Network and Computer Applications*, vol. 107, pp. 113–124, 2018.

[26] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[27] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5 g smart grid slice," *Journal of Network and Computer Applications*, vol. 122, pp. 50–60, 2018.

[28] B. Li, Y. Huang, Z. Liu, J. Li, Z. Tian, and S.-M. Yiu, "HybridORAM: Practical oblivious cloud storage with constant bandwidth," *Information Sciences*, 2018.

[29] Z. Liu, Y. Huang, J. Li, X. Cheng, and C. Shen, "DivORAM: Towards a practical oblivious RAM with variable block size," *Information Sciences*, vol. 447, pp. 1–11, 2018.

[30] X. Zhang, Y. Tan, C. Liang, Y. Li, and J. Li, "A Covert Channel Over VoLTE via Adjusting Silence Periods," *IEEE Access*, vol. 6, pp. 9292–9302, 2018.

[31] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, 2018.

[32] C. Gao, Q. Cheng, P. He, W. Susilo, and J. Li, "Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack," *Information Sciences*, vol. 444, pp. 72–88, 2018.

[33] Y. Zhang, D. Zheng, and R. H. Deng, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

[34] B. Wang and X. Hong, "An anonymous signature scheme in the standard model," *Journal of Information Science and Engineering*, vol. 30, no. 6, pp. 2003–2017, 2014.

[35] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology: Proceedings of (CRYPTO '84)*, vol. 196 of *Lecture Notes in Computer Science*, pp. 47–53, Springer, Berlin, Germany, 1985.

[36] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[37] B. Waters, "Efficient identity-based encryption without random oracles," *Advances in Cryptology – EUROCRYPT 2005*, vol. 3494, pp. 114–127, 2005.

[38] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in *Advances in cryptology—CRYPTO 2004*, vol. 3152 of *Lecture Notes in Comput. Sci.*, pp. 443–459, Springer, Berlin, 2004.

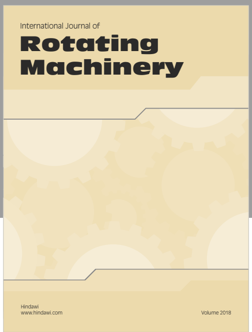
[39] D. Boneh and X. Boyen, "Efficient selective identity-based encryption without random oracles," *Journal of Cryptology. The Journal of the International Association for Cryptologic Research*, vol. 24, no. 4, pp. 659–693, 2011.

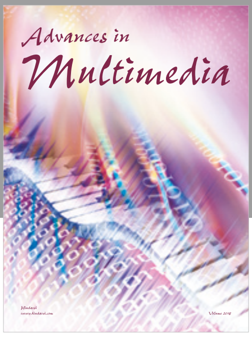
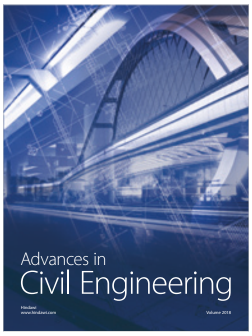
[40] J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," *IEEE Transactions on Computers*, 2013.

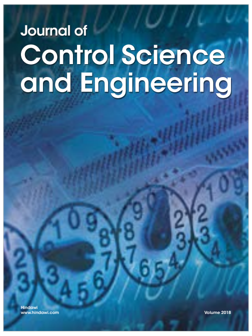
[41] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology—EUROCRYPT 2004*, vol. 3027 of *Lecture Notes in Computer Science*, pp. 506–522, Springer, Berlin, Germany, 2004.

[42] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 3152, pp. 443–459, 2004.

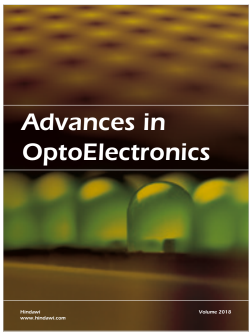
Journal of
Engineering

The Scientific World Journal

International Journal of
Rotating Machinery

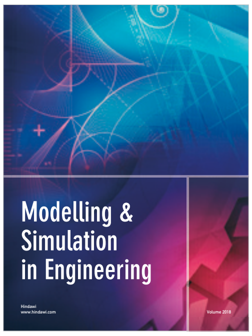
Journal of
Sensors

Advances in
Multimedia

Advances in
Civil Engineering

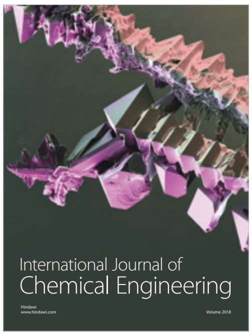
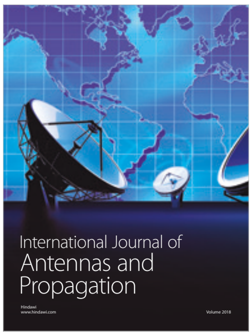

Journal of
Control Science and Engineering

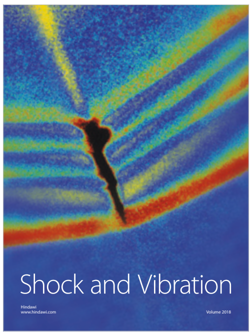
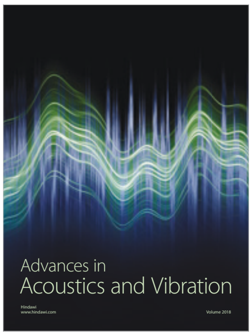
Journal of
Robotics

Journal of
Electrical and Computer Engineering

Advances in
OptoElectronics

VLSI Design

International Journal of
Navigation and Observation

Modelling & Simulation in Engineering

International Journal of
Aerospace Engineering

International Journal of
Chemical Engineering

International Journal of
Antennas and Propagation

Active and Passive Electronic Components

Shock and Vibration

Advances in
Acoustics and Vibration