Lightweight Anonymous Communication Model Based on Anonymous IBE

Yanli Wang, Xinying Yu, and Fengyin Li(✉)

School of Computer Science, Qufu Normal University, Rizhao 276826, China
Lfyin318@126.com

Abstract. With increasing application of big data technology, a large amount of personal information is stored and processed on the Internet, which makes people have a greater demand for privacy. In addition, the development of mobile Internet and cloud computing requires the communication model to be as efficient and low-bandwidth as possible on the basis of security. In order to achieve the goal of protecting users' data privacy, this paper firstly presents a new anonymous Identify-Based Encryption (IBE) scheme, and designs a new lightweight anonymous communication model by introducing the proposed anonymous IBE scheme into an anonymous communication model. This model effectively guarantees the anonymity of system users and the security of messages in the communication process. Performance analysis shows that our communication model can effectively resists node eavesdropping, traffic analysis attacks, and finally achieve communication security and anonymity. Compared with other anonymous communication systems, our scheme has significant advantages in efficiency and relatively low cost. In the future, it has good application prospects.

Keywords: Anonymous communication model · Privacy protection · Identify-based encryption · Bilinear map

1 Introduction

In the era of big data, as more personal information and organizational information are involved, data privacy becomes more and more important. As we all known, our protection of data privacy requires not only the protection of the content of the message, but also the protection of the identity, communication time and communication path of both parties to the communication. However, the existing encryption technologies [2] find it difficult to protect the communication participants' private information such as identity, behavior, and network address. Hackers use traffic-analysis attacks [1] 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.

L. Qi et al. (Eds.): CloudComp 2020, LNICST 363, pp. 103–110, 2021.
https://doi.org/10.1007/978-3-030-69992-5_8

After the first paper on anonymous communication model was published in 1981 [13], 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 [9] proposed an onion routing. People encrypt message and transmit it through a series of network nodes called "onion routers", each node "stripping" a single layer to reveal the next destination of the data. 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 [16], but it cannot resist traffic attacks [12,17], exiting node vulnerability attacks [15] and other security problems. In order to undertake traffic analysis, Chaum et al. [7] 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 [8,14]. 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. In the future, the lightweight anonymous communication system can be applied to information transmission between sensors and servers in the Internet of Things [11], as well as proprietary security protection in cloud services [4]. Nevertheless, there are few existing research studies on lightweight anonymous communication systems. For this purpose, the following are the main contributions of this paper.

(1) An anonymous IBE algorithm is proposed to encrypt messages in the communication model, taking 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 message security.

(2) A lightweight anonymous communication model based on the proposed IBE scheme is proposed, the new model simultaneously implements anonymity, efficiency and security.

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 proposed anonymous IBE scheme and in Sect. 4, a lightweight anonymous communication model based on anonymous IBE is proposed. Before summarising this paper in Sect. 6, Sect. 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, g is a generator of G_1. The bilinear map $e : G_1 \times G_1 \rightarrow G_2$ has the following properties [6]:

(1) Bilinearity: For all $P, Q \in G_1$ and for all $a, b \in Z_p$, we have $e(P^a, Q^b) = e(P, Q)^{ab}$.

(2) Non-degeneracy: $e(g, g) \neq 1$.

(3) Computability: For all $P, Q \in G_1$, there is an algorithm that can compute $e(P, Q)$ efficiently.

2.2 Bilinear Diffie-Hellman Assumption

The BDH problem [3,6] in G_1 is as follows: Input a tuple $g, g^\alpha, g^b, g^c \in G_1$, output $e(g, g)^{\alpha bc} \in G_2$. An algorithm $\mathcal{A}$ has advantage ε in solving BDH in G_1 if

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

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

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

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

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

Occasionally we drop t and ε and refer to the BDH and Decision BDH assumptions in G_1.

2.3 IBE Scheme

In the IBE scheme, participants generally include private key generators (PKG) and users. PKG as a trusted third party, uses the system master key and user ID to generate a private key. Subsequently, the private key is distributed to the corresponding users by PKG. Furthermore, the identity of the user makes IBE different from the public key of the traditional public key crypto-system. Therefore, IBE scheme is widely used in the field of information security protection. An Identity Based Encryption (IBE) scheme is a tuple of PPT algorithms, it is defined in 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 defined the chosen ciphertext security for IBE systems under a chosen identity attack in paper [5]. In the model, the adversary is allowed to adaptively choose the public key it wants 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 [10].

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 $q_1, \cdots, q_m$ 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, two identities ID_0, ID_1. ID_0, ID_1 or their prefix cannot appeare in any key generation query in Phase 1. $\mathcal{B}$ chooses a random bit $k, l \in \{0, 1\}$, sets $C^* = Encrypt(params, ID_k, m_l)$, 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 ε of an adversary A in this game is defined as $\left|\Pr\left[k' = k \wedge l' = l\right] - \frac{1}{4}\right|$.

Definition 2. An anonymous IBE system is (t, q, ε)-ANON-IND-ID-CCA secure if all t-time ANON-IND-ID-CCA adversaries making at most q queries have advantage at most ε 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 design an efficient anonymous IBE scheme, and prove its correctness and security.

Let G_1 and G_2 be multiplicative cyclic groups of prime order p, g is 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

$$params = (g, g_1, g_2), MSK = \alpha. \tag{3}$$

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

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

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

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

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

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

4 Lightweight Anonymous Communication Model Based on Anonymous IBE

In this section, we design a lightweight anonymous communication model based on anonymous IBE, which is proposed in Sect. 3.

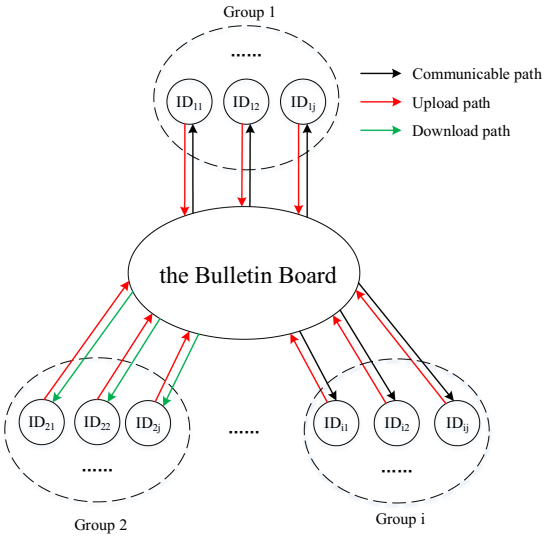

Fig. 1. Lightweight anonymous communication model (Color figure online)

When a user enters the model, the model automatically distributes a unique and fixed identity ID to the user. At the same time, the private key generation (PKG) in the model generates the system's secret master key and the private key corresponding to each user according to the previous IBE encryption mechanism. On the other hand, 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 $0 < i \leq \mathrm{M}, 0 < j \leq \mathrm{N}$). We notate the user as ID_{ij}, and every trusted user knows the identities and group numbers of other users in the system.

In the communication phase, 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 by using the anonymous IBE scheme. It is worth mentioning that in order to reduce memory consumption on the basis of ensuring security, we add the group number of the recipient as a mark. During time T_2, all the users upload the ciphertext to the bulletin board and the bulletin board is provided for users to upload and download ciphertexts. This process is indicated by the red line in Fig. 1. During time T_3, if the mark in the ciphertext is equal to the group number in the model, then all users in the group must download the ciphertext to the local host, other groups will not download the ciphertext. This downloading process is indicated by the green line in Fig. 1, and the black line indicates the available communication path in the model. During time T_4, the user decrypts the downloaded ciphertext with his/her private key.

5 Model Performance Analysis

5.1 Anonymity of Messages

In our model, the public key of the recipient does not need to be queried by the sender, 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. Because the recipient's identity is used as the public key to encrypt the ciphertext, 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.

5.2 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 [7], 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. [11], 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.

6 Conclusion

With the development of mobile Internet and cloud computing, the previous anonymous communication model had large requirements on network bandwidth and memory, which cannot meet its development needs. And using a large-scale anonymous communication model in the group is inefficient, expensive, and insecure. In this paper, we design a lightweight anonymous communication model based on IBE, 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. In the future, we will consider applying this model to user authentication and application scenarios in the Internet of Things.

References

1. 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)
2. Abusukhon, A., Bilal, H.: A secure network communication protocol based on textto barcode encryption algorithm. Int. J. Adv. Comput. Sci. Appl. **6**(12), 64–70 (2015)
3. Joux, A.: A one round protocol for tripartite diffie–hellman. In: Bosma, W. (ed.) ANTS 2000. LNCS, vol. 1838, pp. 385–393. Springer, Heidelberg (2000). https://doi.org/10.1007/10722028_23
4. Antonela, D., Roger, D., Arthur, E., Finkel, M.: Addressing denial of service attacks on free and open communication on the internet. The Tor Project, Technical report (2018)
5. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258–275. Springer, Heidelberg (2005). https://doi.org/10.1007/11535218_16
6. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13
7. David, C.: The dining cryptographers problem: Unconditional sender and recipient untraceability. J. Cryptology **1**(1), 65–75 (1988)
8. Fatemeh, S., Milivoj, S., Rizwan, A.M., Michael, B., Claudia, D.: A survey on routing in anonymous communication protocols. ACM Comput. Surv. (CSUR) **51**(3), 1–39 (2018)
9. Reed, M.G., Syverson, P.F., Goldschlag, D.M.: Anonymous connections and onion routing. IEEE J. Sel. Areas Commun. **16**(4), 482–494 (1998)
10. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006). https://doi.org/10.1007/11761679_27
11. Jiang, L., Li, T., Li, X., Atiquzzaman, M., Ahmad, H., Wang, X.: Anonymous communication via anonymous identity-based encryption and its application iniot. Wireless Commun. Mob. Comput.**2018**, 8 (2018)
12. 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)
13. Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM **24**(2), 84–90 (1981)
14. 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. IEEE (2017)
15. Nicholas, H., Y, V.E., Eric, C.T.: How much anonymity does network latency leak? ACM Trans. Inf. Syst. Secur. (TISSEC) **13**(2), 1–28 (2010)
16. Goldschlag, D., Reedy, M., Syverson, P.: Onion routing for anonymous and private internet connections. Commun. ACM **42**(2), 5 (1999)
17. Sambuddho, C., Angelos, S., Keromytis, A.D.: Identifying proxy nodes in a tor anonymization circuit. In: 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems, pp. 633–639. IEEE (2008)