A New Pairing-Based Scheme for Anonymous Communication System

Meichen Xia(✉) and Zhimin Chen

School of Computer and Software Engineering, Xihua University, Chengdu 610039, China
xiameichen123@gmail.com

Abstract. Anonymous technology is a critical tool to preserve privacy. In some communication systems, users of one communication group want to verify that they are the legal members without exposing their identities. Some identity-based cryptographic solutions have been proposed for anonymous communications. However, these approaches assume that a centralized trust authority is in charge of the private key generation, so the communications are not anonymous to the trust authority. We present a pairing-based anonymous scheme to realize encryption/decryption, digital signature, key exchange, and key revocation solutions for communications system. In our scheme, users can self-choose their private keys and they can also prove that they are the legal members of one group. Our approach is simple and feasible and it can be applied to some anonymous services.

Keywords: Anonymous system · Identity-based cryptographic · Weil paring

1 Introduction

Preserving-privacy communication systems are very important. On the one side, users in the communication need to prove to the peers that they are legal [1,2]. On the other side, they do not want to leak their identities during this conversation. For the anonymous communication, there are always these kinds of ways to follow. (1) Using the pseudonym to hide the actual identity. Zhang et al. [3] proposed the identity-based key management approach [4] for anonymous communications. In their approach, a trust authority (TA) administrates the anonymous communication system in broadcasting wireless environment. TA can also serve as an organizer who generates the publicly known system parameters and distribute the keys for anonymous users. Users use each other's identity (i.e., a pseudonym) as the public key to set up anonymous communication sessions.

Supported by the Sichuan education department research project (no. 16226483), Sichuan Science and Technology Program (2018GZDZX0008), Chengdu Science and Technology Program (2018-YF08-00007-GX), the National Natural Science Foundation of China (61872087).

X. Sun et al. (Eds.): ICAIS 2020, CCIS 1254, pp. 13–20, 2020.
https://doi.org/10.1007/978-981-15-8101-4_2

Based on the identity-based solution, the ciphertext sender just simply uses the receivers' pseudonyms as the public key to encrypt the plaintext. This approach has one drawback, the anonymous communications are not blind to the TA. To resolve the problem in Zhang's scheme, Huang [5] proposed a pseudonym based scheme to achieve the goal that it is blind to TA. (2) Using the ring/group signatures to hide the actual identity of the sender in a set. Zeng et al. [6] proposed a privacy-preserving protocol for VANETs communication based on the ring signature. In their scheme, the actual sender chooses other members to form a ring. The generated signature is verified under these members' public keys. Therefore the sender's identity will not be exposure to the public. (3) Using the deniable authentication to deny the involvement of one conversation. Li et al. [7] proposed an ID-based deniable authentication for ad hoc networks. In their scheme, the sender's output is not verified publicly. Instead, only the conversation peer can verify this authentication. Therefore, the sender can deny as his peer can generate the whole communication transcript by his own. We propose a pairing-based scheme to achieve the anonymous communication. Comparing to traditional identity-based cryptography, our approach does not depend on the TA to generate a user's private key, but TA signs for each user's identity (who are legal). On the one hand, we want to protect users' identities from being exposed; on the other hand, we expect to create a manageable and admissible communication environment for users. Some conclusions in [4,8,9] will be applied in our scheme to realize encryption/decryption, digital signature, key exchange, and revocation solutions for communications system.

2 The Weil Pairing

2.1 The Properties of Weil Pairing

In this section we shall summarize the properties we require of the Weil pairing, much of the details can be found in [4,10]. The major pairing-based construction is the bilinear map. We denote E being an elliptic curve over the field F. Considering two groups G_1 and G_2 of prime order p. G_1 is an additive group and G_2 is a multiplicative group. The bilinear mapping can be denoted by $e : G_1 \times G_1 \rightarrow G_2$ and the mapping has three properties:

1. Bilinear:

$$e(P_1 + P_2, Q) = e(P_1, Q) \bullet e(P_2, Q)$$
$$e(P, Q_1 + Q_2) = e(P, Q_1) \bullet e(P, Q_2)$$
$$e(aP, bQ) = e(P, Q)^{(a+b)}$$

   For$(P, Q, P_1, P_2, Q_1, Q_2) \in G_1$,$(a, b) \in Z_P^*$
2. Non-degenerate: There exists $P \in G_1$ such that $e(P, P) \neq 1$.
3. Computable: One can compute $e(P, Q)$ in polynomial time.

2.2 Some Hard Problems in Elliptic Curve

There are some hard problems in Elliptic Curve Cryptology (ECC), we describe them as follows:

Elliptic Curve Discrete Logarithm Problem (ECDLP Problem): Given P, mP in G_1 with $m \in Z_P^*$, compute m.
Computational Diffie-Hellman Problem (CDH Problem): Give P, aP, bP in G_1 with $a, b \in Z_P^*$ compute abP.
Bilinear Diffie-Hellman Problem (BDH Problem): For a bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$ defined as follows: given$(P, aP, bP, cP) \in G_1$, compute $e(P, P)^{abc} \in G_2$ where $(a, b, c) \in Z_P^*$.
Bilinear Diffie-Hellman Assumption: We assume that the BDH problem is hard, which means there is no polynomial time algorithm to solve BDH problem with non-negligible probability.
Pairing Inversion Problem: Given P and s, find Q such that $e(P, Q) = s$.
The details of the pairing algorithms are out of the scope of our paper. The interested reader may study them from [11]. The remainder of this paper we will use the Weil pairing and take advantage of these hard problems in ECC to ensure our scheme's security.

3 Our Scheme

In our scheme, we propose a pairing-based public key infrastructure. Our scheme includes following steps: Setup, Extract, Encryption/Decryption, Digital Signature, Key Exchange, and Key Revocation.

3.1 Parameters Setup and Key Extract

Similar to the IBC, our scheme also needs TA to setup the system parameters, and some parameters (denoted as *params*) should be publicly known to all users. There are many ways to publish the *params*. For example, it can be published on some trusted web sites, and thus all the users can download it; some publicly well-known trusted party can generate a certificate for the *params*, and thus the certificate can be broadcasted during the anonymous communication and all users can verify the *params*:

The key generate center (KGC and here we denote it as TA) runs BDH *params* generator to generate two groups G_1 and G_2 whose orders are prime p, and a bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$, which are described above. KGC also choose an arbitrary generator $P \in G_1$ and defines three cryptographic hash functions:

$$H : \{0,1\}^n \rightarrow G_1;$$

$$H_1 : \{0,1\}^n \times G_1 \rightarrow Z_p^*;$$

$$H_2 : G_2 \rightarrow \{0,1\}^n;$$

KGC chooses a random number $s \in Z_P^*$ and set $P_{pub} = sP$. Then the KGC publishes system parameters $params = \{G_1, G_2, p, P, P_{pub}, H, H_1, H_2\}$, and keep s as master-key.

A user M_i chooses a random value $a_i \in Z_P^*$ as his private key, and submits his identity ID_i to the KGC. KGC computes $Q_i = s \cdot H(ID_i)$ and returns Q_i to M_i. M_i computes $P_i = a_i Q_i$. a_i is kept as a secret and P_i is public to everyone. $<a_i, P_i>$ is a key pair of M_i.

3.2 Encryption and Decryption

To encrypt the plaintext $M \rightarrow \{0,1\}^n$ for M_i with M_i's public key P_i, M_j performs the following steps:

1. M_j chooses a random value $r_j \in Z_P^*$;
2. M_j computes $g = e(P_i, r_j P)$, the ciphertext

$$C = (M \oplus H_2(g), r_j P_{pub}) = (V, U) \tag{1}$$

3. M_i uses his private key a_i to decrypt:

$$V \oplus H_2(e(a_i H(ID_i), U)) \tag{2}$$

3.3 Digital Signature

Given a message M, M_i needs to sign it for M_j. If M_j computing the following equation comes into existence, M_i will be considered the signer and M_i also will be considered the legal user of one group. Our description is as follows:

Sign: assuming M_i as a signer, M_i chooses a random value $r_i \in Z_P^*$, and computes:

$$U_i = r_i P_i \tag{3}$$
$$h_i = H_1(M, U_i) \tag{4}$$
$$V_i = (r_i + h_i) \cdot a_i \cdot H(ID_i) \tag{5}$$

Sends (U_i, V_i) to receiver M_j.

Verify: M_j computes:

$$h_i = H_1(M, U_i) \tag{6}$$
$$Q_i = U_i + h_i \cdot P_i \tag{7}$$

and performs the following test:

$$e(V_i, P_{pub}) = e(Q_i, P) \tag{8}$$

3.4 Key Exchange

Suppose two users M_i and M_j wish to agree a key. We denote the private keys of the two users as a_i and a_j, their public keys are P_i and P_j, and both of them choose random$(r_i, r_j) \in Z_P^*$, they broadcast: $r_i P_{pub}$ and $r_j P_{pub}$.

M_i computes:

$$\begin{aligned} k_{ij} &= e(r_i P_j, P) e(a_i H(ID_i), r_j P_{pub}) \\ &= e(H(ID_j), P_{pub})^{a_j r_i} e(H(ID_i), P_{pub})^{a_i r_j} \end{aligned} \tag{9}$$

M_j computes:

$$\begin{aligned} k_{ji} &= e(r_j P_i, P) e(a_j H(ID_j), r_i P_{pub}) \\ &= e(H(ID_i), P_{pub})^{a_i r_j} e(H(ID_j), P_{pub})^{a_j r_i} \end{aligned} \tag{10}$$

Obviously that $k_{ij} = k_{ji}$.

3.5 Key Revocation

Our scheme is simple for TA to revoke the key of users when users leave the group. If a user M_i leaves the group, the TA takes charge of the revocation event. TA adds the public key P_i corresponding to M_i into the public key revocation list, and TA maintains the list. Thus, before encrypting a message or manipulating the other events, M_i should check the revocation list in order to validate the corresponding public key.

If a user whose public key has already added into the revocation list, and he will want to join the group again, it only needs to choose a new a_i to construct $a_i \cdot Q_i$ as his public key. The proposed IBC schemes have difficulty in key renewal. After revocation, new ID-based keys are difficult in issuing for the same identity. This scheme which we propose introduces a new format for public keys such new public key can be used for the same identity after the previous key has been revoked. M_i only needs to choose a new a_i to construct his new public key after being revoked.

4 Analysis of Our Scheme

4.1 Comparison Between Our Scheme and IBC

Our scheme is similar to IBC scheme, however, they are fundamentally different. We describe their difference as follows.

Firstly, the duty of KGC is different. In IBC scheme, the KGC (TA) takes charge of generating the user's private key. But in our scheme, KGC signs for user's identity to make user legal.

Secondly, the ways of key generation are different. In IBC scheme, users' pairwise of keys is generated by KGC. It means that KGC knows all the keys of users so that KGC can decrypt all ciphertexts which users deliver and KGC can

sign messages by imitating legal users. In other words, the way of key generation in IBC scheme is not blind to KGC. But in our scheme, the private key of user is generated by user himself, nobody except himself knows the private key. User's public key is based on signature of KGC and the user's private key so that he can verify his legality. Our scheme is suit for anonymous communication system.

Thirdly, in IBC scheme, the users can use the identities of others as their public key, in other words, the identities of users are not anonymous in communications. In our scheme, the identities of users are blind to anyone, and the public key of M_i is masked by the corresponding private key $a_i \in Z_P^*$. Both the public key and the private key cannot be derived by other users.

Finally, in IBC scheme, there is no simple way to renew the identity of M_i if his public key has been revoked. But in our scheme, we present a new form that the KGC signs for ID_i, if M_i wants to join the group again after his public key being revoked, he only needs to choose a new value a_i to construct the public key. Notice, KGC should maintain a revocation list which all the users can avail it.

4.2 Security Analysis of Our Scheme

In our scheme, private key a_i is chosen by M_i himself, and the public key of M_i is $a_i sH(ID_i)$. It is a one-way function from private key to public key under ECDLP problem, which is presented in Sect. 2.2.

Theorem 1. *Our Encryption\Decryption scheme is secure.*

Here, we analyze our scheme presented in Sect. 3.2. To see how it works, we demonstrate the correctness in the Encryption\Decryption algorithm. When decrypts the ciphertext, he performs as follow:

$$\begin{aligned} V \oplus H_2(e(a_i H(ID_i)), U) &= V \oplus H_2(e(a_i H(ID_i)), r_i P_{pub}) \\ &= V \oplus H_2(e(a_i sH(ID_i)), r_i P) \\ &= V \oplus H_2(e(P_i, r_i P)) \\ &= M \oplus H_2(g) \oplus H_2(g) \\ &= M \end{aligned}$$

Proof. We assume that the IBE scheme is secure due to the proof presented by Boneh et al. [4,12]. To prove our scheme is secure, we should prove the modification introduced by our scheme will not affect the security of the original IBE scheme. In our scheme, everyone including KGC cannot derive $a_j H(ID_j)$ from $P_j = a_j sH(ID_j)$, though he knows $sH(ID_j)$. Because it is at least as hard as to solve ECDLP problem. In encryption, M_j can compute $g = e(P_i, r_j P) = e(a_i H(ID_i), r_j P_{pub})$. To find $a_i H(ID_i)$ and satisfy $g = e(a_i H(ID_i), r_j P_{pub})$ is believed to be a pairing inversion problem (see Sect. 2.2).

IBE scheme is proved in choosing ciphertext attack secure under ***Random Oracle*** model by Boneh et al. [4,12]. There is no polynomial bounded algorithm having a non-negligible advantage in solving the BDH problem. Based on the above analysis, we claim that our scheme is also secure.

Theorem 2. *Our signature scheme is secure.*

Firstly, we also present the correctness of our signature scheme.

$$\begin{aligned} e(V_j, P_{pub}) &= e((r_i + h_i)a_i H(ID_i), P_{pub}) \\ &= e((r_i + h_i)a_i sH(ID_i), P) \\ &= e(U_i + h_i P_i, P) \\ &= e(Q_i, P) \end{aligned}$$

Proof. M_i uses private key a_i to sign the message M. The adversary cannot solve $a_i H(ID_i)$ from $U_i = r_i s a_i H(ID_i)$, which is equivalent to solving ECDLP problem as presented above. Thus the adversary cannot forge the signature $V_i = (r_i + h_i)a_i H(ID_i)$. So adversary cannot modify the (U_i, V_i) to satisfy the equation $e(V_i, P_{pub}) = e(Q_i, P)$.

The correctness of key exchange has been presented in Sect. 3.4, and here we present the secure properties in our key exchange scheme.

(1) **Known Key Security:** The key exchange of every times, M_i would choose a different random value, and the adversary cannot deduce the future session keys from the past session keys.
(2) **Forward Secrecy:** If a long term secret key, such as a_i has disclosed, at some point in the future does not lead to the compromise of communications in the past, as though the private key of KGC is compromised.
(3) **Key Control:** Neither party can control the outcome of the session keys, everyone should contribute the equal share to the key exchange.

4.3 Anonymity Analysis of Our Scheme

In our scheme, the private key a_i of M_i is chosen by M_i himself, and identity of M_i is masked by private key a_i. Both of pairwise keys cannot be derived by other users. And the adversary needs to know the private information a_i. Given a point $sH(ID_i)$ and $P_i = a_i sH(ID_i)$, the adversary cannot derive the value a_i which is equivalent to solving ECDLP problem. The KGC only knows users' identities when he verifies the users' legality. This kind of hidden identity just suits for anonymous communication system.

5 Conclusion

We propose a paring-based scheme for anonymous communication system. In our scheme, pairs of keys are generated by users themselves. KGC takes charge of signing the identities of users. If a user is legal, (it means he is signed by KGC) they can communicate with others including encryption/decryption, digital signature, key exchange and so on. In our scheme, key revocation is simple because the key renewal is easy to realize. We present the correctness and the security analysis of our algorithm. Our scheme is simple and feasible and it is suitable for anonymous communication system.

References

1. Kou, L., Shi, Y., Zhang, L., et al.: A lightweight three-factor user authentication protocol for the information perception of IoT. CMC-Comput. Mater. Continua **58**(2), 545–565 (2019)
2. Jiang, X., Liu, M., Yang, C., et al.: A blockchain-based authentication protocol for WLAN mesh security access. CMC-Comput. Mater. Continua **58**(1), 45–59 (2019)
3. Zhang, Y., Liu, W., Lou, W.: Anonymous communications in mobile ad hoc networks. In: 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings of IEEE **3**, 1940–1951 (2005)
4. 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
5. Huang, D.: Pseudonym-based cryptography for anonymous communications in mobile ad-hoc networks. Int. J. Secur. Netw. **2**, 272–283 (2007)
6. Zeng, S., Huang, Y., Liu, X.: Privacy-preserving communication for VANETs with conditionally anonymous ring signature. Int. J. Netw. Secur. **17**(2), 135–141 (2015)
7. Li, F., Xiong, P., Jin, C.: Identity-based deniable authentication for ad hoc network. Computing **96**, 843–853 (2014)
8. Choon, J.C., Hee Cheon, J.: An identity-based signature from gap Diffie-Hellman groups. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 18–30. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36288-6_2
9. Smart, N.P.: Identity-based authenticated key agreement protocol based on weil pairing. Electron. Lett. **38**(13), 630–632 (2002)
10. Menezes, A.J., Okamoto, T., Vanstone, S.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Info. Th. **39**, 1639–1646 (1993)
11. Bao, F., Deng, R.H., Zhu, H.F.: Variations of Diffie-Hellman problem. In: Qing, S., Gollmann, D., Zhou, J. (eds.) ICICS 2003. LNCS, vol. 2836, pp. 301–312. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-39927-8_28
12. Li, D., Luo, M., Zhao, B., Che, X.: Provably secure APK redevelopment authorization scheme in the standard model. CMC-Comput. Mater. Continua **56**(3), 447–465 (2018)