A Novel Message Authentication Scheme With Absolute Privacy for the Internet of Things Networks

JIAN LI\textsuperscript{1}, ZHENJIANG ZHANG\textsuperscript{1}, LIN HUI\textsuperscript{2}, AND ZHANGBING ZHOU\textsuperscript{3,4}

\textsuperscript{1}School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China
\textsuperscript{2}Department of Innovative Information and Technology, Tamkang University, New Taipei City 25137, Taiwan
\textsuperscript{3}School of Information Engineering, China University of Geosciences, Beijing 100083, China
\textsuperscript{4}Computer Science Department, TELECOM SudParis, 91011 Évry, France

Corresponding author: Jian Li (lijian@bjtu.edu.cn)

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant KWJB519026536, and in part by the National Natural Science Foundation of China under Grant 61701019.

ABSTRACT With the rapid development and massive deployment of the Internet of things (IoT) networks, security related issues in the IoT networks have been paid more and more attention to. Among all the security concerns, message authentication is critical in preventing the unauthorized messages from being transmitted in the IoT networks. Many message authentication schemes have been proposed based on the public-key cryptosystem, where the key management is simple and scalable. Identity based cryptosystem is a special type of public-key cryptosystem and can further ease the process of the key management since the public keys can be obtained easily. In this paper, we devise an efficient message authentication with enhanced privacy (IMAEP) scheme using the identity based signature. Our proposed scheme can provide both unconditional privacy as well as the enhanced privacy under full key exposure attack. Our proposed scheme can also provide existential unforgeability under the adaptive chosen-message-and-identity attack. Compared with the scheme that has the same level of anonymity and security, our proposed scheme has much lower computational overhead, and can provide extra unconditional privacy. Next we propose an extended IMAEP (EIMAEP) scheme for the general access structures where the message is signed by a group of users instead of one user. We also conduct comprehensive analysis and demonstrate that the EIMAEP scheme can achieve the same level of privacy and unforgeability as the IMAEP scheme.

INDEX TERMS Message authentication, privacy, Internet of Things networks, identity-based cryptography.

I. INTRODUCTION

Compared to the early stages of Internet of things that utilized computation-limited devices and simple sensor networks [2], today’s next generation of Internet of Things (IoT) networks such as in [3] have equipped with advanced communication and computation technologies, and have become more and more intelligent. These systems can automatically sense the physical data and react to the physical world accordingly without any human intervention. Thus correct message exchange within the IoT networks is critical for the system to function properly [4]. Unauthorized messages must be filtered out to recognize the harmful “fake” critical messages, or to save the precious energy of sensor nodes and so on. Message authentication plays a key role in thwarting unauthorized messages from being forwarded in the IoT networks. Many authentication schemes have been proposed to provide message authenticity and integrity verification for the IoT networks. These schemes can largely be divided into two categories: symmetric-key based approaches and public-key based approaches.

For the symmetric-key based approaches [5], [6], the sender uses a shared secret key to generate a message authentication code (MAC) for the transmitted message. The verifier can examine the authenticity of the message using the same shared key. However, the key management is very complex. Since each pair of the senders and receivers have to share a distinct secret key, the scalability for the
The major contributions of this paper are:

achieving both unconditional privacy and enhanced privacy.

the identity based ring signature scheme in [17], aiming at application scenarios such as witness protection. In this the true message sender. It is a desirable feature in some approaches. In unconditional privacy, nobody can identify privacy through pseudonyms-based or group signature-based approaches. Many literatures such as [13]–[16] study the conditional privacy, the true message sender can be identified by group managers or some trusted third party. In identity based cryptosystem [11], [12], the public key for any receiver can be generated by the sender locally without contacting the trusted agent. The key management and distribution is further simplified in this kind of cryptosystem. Thus in [1], [13]–[17] several authentication schemes built upon the identity based cryptosystem are proposed.

During authenticating of messages transmitted in the IoT networks, source privacy should be preserved as well. Take the remote metering system of the smart grid as an example, where meter readings are transmitted through wireless sensor networks, the household that generates specific power statistic messages should not be identified through these transmitted messages. There are two types of privacy in message authentication: conditional and unconditional. In conditional privacy, the true message sender can be identified by group managers or some trusted third party. Many literatures such as [13]–[16] study the conditional privacy through pseudonyms-based or group signature-based approaches. In unconditional privacy, nobody can identify the true message sender. It is a desirable feature in some application scenarios such as witness protection. In this paper, we study the ID-based ring signature problem through the identity based ring signature scheme in [17], aiming at achieving both unconditional privacy and enhanced privacy. The major contributions of this paper are:

1) We propose an efficient message authentication with enhanced privacy (IMAEAP) scheme. The scheme can provide unconditional privacy as well as the enhanced privacy defined in [18] under the full key exposure attack.

2) We formally prove that the proposed IMAEP scheme can achieve the claimed privacy and unforgeability against the adaptive chosen-message-and-identity attack.

3) Compared with the scheme in [1] that has the same level of anonymity and security, our proposed scheme has much lower computational overhead, and can provide extra unconditional privacy.

4) We propose an EIMAEP scheme for the general access structures where the message is signed by a group of users instead of one user. We demonstrate that the EIMAEP scheme can achieve the same level of privacy and unforgeability as the IMAEP scheme through comprehensive analysis.

The rest of this paper is organized as follows: Section II discusses the related work. Section III presents the system settings, design goals and cryptographic tools we used. The proposed IMAEP scheme and the security/performance analysis are presented in Section IV and V respectively. In Section VI and VII we propose the EIMAEP scheme for the general access structures and analyze its security and applications. We conclude in Section VIII.

II. RELATED WORK

According to the cryptosystem used, message authentication schemes can be classified into symmetric-key based approaches and public-key based approaches. In the former category, symmetric cryptography is used. The authors in [5] study the message authentication in wireless sensor networks, where the MAC’s correctness is calculated probabilistically on each sensor node. Messages with invalid MAC’s are dropped. In [6], the authors propose to only perform the symmetric MAC operation in the vehicular privacy-preserving communications in vehicular ad-hoc networks of the Internet of Things. The advantage of the symmetric key based schemes is low computational overhead. However, when the scale of the network becomes large, the key management involving a huge amount of keys would be infeasible.

For the later category, the public key infrastructure (PKI) based authentication is adopted. In [7], the authors propose a secure framework with privacy-preserving based on group signature in vehicular communication. In [8], the authors propose to apply the ring signatures on elliptic curve in an anonymous authentication scheme in wireless sensor networks, which can achieve an unconditional source privacy with low computational overheads. In [9], the authors combine the pseudonyms with group signature and propose an efficient privacy-preserving authentication scheme for the Internet of Things. In [19], the authors propose an improved lightweight authentication protocol for the Internet of Vehicles. In [20], the authors propose a four party authentication protocol for smart vehicular communication. In [21], the authors make use of the El-Gamal cryptosystem and construct a privacy-preserving RFID authentication protocol.

Among all the public-key based approaches, identity based cryptosystem has distinct advantages that can further simplify the key management, and has been studied a lot recently. In [13], the authors propose an identity based group signature scheme to provide privacy protection for users in cloud computing. In [15], the authors propose an authentication scheme for vehicular sensor networks which can preserve privacy, based on an identity based signature scheme where no pairing is needed. In [16], the authors propose an efficient anonymous authentication scheme in the Internet of Things.
of Things by leveraging both the pseudonyms and identity-based signature. In [22], the authors study the privacy-aware authentication problem in the mobile cloud computing environments. In [23], the authors propose an identity-based data sharing scheme, which can check the data integrity while preserving privacy. In the scheme, they introduce an extra data sanitizer to perform sanitizing tasks to user’s files. In [24], the authors propose a secure file storage and sharing scheme based on identity-based authentication. In [17], the authors propose an efficient ring signature scheme using the identity-based cryptography. They conclude that their scheme has the property of unconditional source anonymity. However, for the full key exposure attack [18] and other similar advanced attacks, the privacy of their scheme is no longer preserved. The authors in [1] improve the work of [17] and propose a scheme that can still preserve the privacy under such advanced attacks. However, unconditional privacy is not longer preserved. The authors propose IMAEP and EIMAEP schemes in this paper. Our proposed schemes have the same level of enhanced privacy in [1]. Moreover, we demonstrate that our schemes can achieve the unconditional privacy and the computational overhead is much lower.

III. PRELIMINARIES
A. SYSTEM MODEL AND ASSUMPTIONS
We assume that the wireless ad-hoc network consists of a number of users, each with a unique identity that can be used in the ID-based cryptographic operations. The network is fully connected and any two users can communicate directly or through relays of intermediate users. There is a trusted key generation center (KGC) in charge of security parameter and private key generation.

In the paper, we consider the following types of attacks against the proposed schemes:
- Adversaries, who cannot get access to the private keys of the users involved in the ring signature, try to identify the true signer or signer group.
- Adversaries, who know all the private keys of the users involved in the ring signature, try to identify the true signer or signer group.
- Adversaries, who can make a polynomial number of queries to the algorithms in the proposed schemes, try to forge a valid signature which has not been queried before.

B. DESIGN GOALS
Our proposed authentication schemes aim at achieving the following goals:
- **Message authentication**: When receiving a message, the receiver should be able to check whether the message is sent by some user in a particular group or by a group of users. In other words, the adversaries cannot forge valid signatures, with which the fake message injected into the network will be detected.
- **Message integrity**: When receiving a message, the receiver should be able to check whether the message has been modified in the intermediate relay nodes by the adversaries. If the message content is modified, it will be detected.
- **Hop-by-hop message authentication**: When receiving a message, every intermediate relay node on the routing path should be able to check the message’s authenticity and integrity.
- **Identity privacy**: When obtaining a message, the adversaries cannot determine the ID of the true message sender, even in the case where all the users’ private keys involved in the ring signature are known by the adversaries.
- **Efficiency**: The authentication scheme should be efficient: it should have low computational overhead and communication overhead.

C. BILINEAR MAP
Let \( q \) be a large prime number, \( G_1 \) be an additive cyclic group of order \( q \) and \( G_2 \) be a multiplicative group of order \( q \).

A bilinear map [12] can be written as \( \hat{e} : G_1 \times G_1 \rightarrow G_2 \) and has the following properties:

1) **Bilinear**: for \( P, Q, R \in G_1 \), \( \hat{e}(P + Q, R) = \hat{e}(P, R) \hat{e}(Q, R) \) and \( \hat{e}(P, Q + R) = \hat{e}(P, Q) \hat{e}(P, R) \); for \( P, Q \in G_1 \) and \( a, b \in \mathbb{Z}_q^* \), \( \hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab} \).
2) **Non-degenerate**: There exist \( P, Q \in G_1 \) such that \( \hat{e}(P, Q) \neq 1 \). The map does not project all possible combinations of \( G_1 \times G_1 \) to the identity in \( G_2 \).
3) **Computable**: For \( P, Q \in G_1 \), it is computationally feasible to compute \( \hat{e}(P, Q) \).

The following Computational Diffie-Hellman Problem is defined for the group \( G_1 \):

**Definition 1 (Computational Diffie-Hellman Problem)**: Assume \( P \) is a generator of \( G_1 \). For two points \( aP, bP \) generated from \( P \) where \( a, b \in \mathbb{Z}_q^* \), calculate \( abP \).

Based on the following assumption, the proposed IMAEP/EIMAEP schemes are secure:

**Definition 2 (Computational Diffie-Hellman Assumption)**: We assume that the Computational Diffie-Hellman problem cannot be solved by any polynomial time algorithm \( B \) with non-negligible probability.

D. NOTATIONS
The notations used in this paper are listed in Table 1.

IV. EFFICIENT MESSAGE AUTHENTICATION WITH ENHANCED PRIVACY (IMAEP) SCHEME
A. SCHEME FRAMEWORK
Similar to the framework defined in [1], the proposed IMAEP scheme has a framework consisting of four algorithms:

1) **Setup**: Given a security parameter \( k \) as input, the trusted key generation center (KGC) generates a set of system parameters \( \text{params} \) and a master secret key \( x \). The system parameters \( \text{params} \) define a finite message space and a finite signature space. These parameters are made publicly available. The master secret key \( x \) is stored privately by the KGC.
TABLE 1. Notations.

| m     | message to be signed |
|-------|----------------------|
| n     | number of identities or identity subsets in the ring signature |
| k     | security parameter of the schemes |
| σ(·)  | bilinear map |
| P     | generator of the additive cyclic group $G_1$ |
| z     | master secret of the KGC |
| $P_{pub}$ | public key of the KGC |
| $H(·)$ | cryptographic hash function to generate the public key of an ID |
| L     | set of identities for which the signature is produced |
| $ID_1$ | identity of the $i^{th}$ user in L |
| $S_{ID_1}$ | private key of $ID_1$ |
| $Q_{ID_1}$ | public key of $ID_1$ |
| $L_i$ | a subset of members who collaborate to sign a message in the IMAEP scheme |
| $d_i$ | number of identities in $L_i$ |
| $L$   | general access structure with $n$ subsets |
| $ID_{i,j}$ | identity of the $j^{th}$ user in $L_i$ |
| $S_{ID_{i,j}}$ | private key of $ID_{i,j}$ |
| $Q_{ID_{i,j}}$ | public key of $ID_{i,j}$ |
| $PK_i$ | summation of public keys in $L_i$ |

2) **KeyGen:** Given the master secret key $x$ and a signer’s identity $ID \in \{0, 1\}^*$, the KGC computes the signer’s secret signing key $S_{ID}$. For the identity based signature, the participating members can compute the public key $Q_{ID}$ efficiently.

3) **Sign:** Let $\{ID_1, ID_2, \ldots, ID_n\}$ be the identities of $n$ users in a group. To sign a message $m$, a user can use its secret signing key $S_{ID}$, $1 \leq s \leq n$ and the group identities $\{ID_1, ID_2, \ldots, ID_n\}$ to compute the corresponding ring signature $\sigma$.

4) **Verify:** Given a message $m$, the identities of the signer’s group $\{ID_1, ID_2, \ldots, ID_n\}$ and aiding information $f(x, \sigma)$ computed by the KGC, a verifier can check the validity of a ring signature $\sigma$ on the message. The verifier will accept the signature if it is valid. In other cases, the verifier will decline the signature.

We can achieve the message authentication for the signer through the IMAEP scheme. Moreover, the true signer will not be identified in a group of users. The only way to find out the message sender is by randomly selecting one from the group.

**B. SCHEME SECURITY DEFINITION**

There are two aspects to define the security of the IMAEP scheme: anonymity and unforgeability. For anonymity, we study the privacy property of the scheme. For unforgeability, we study the signature’s authenticity.

1) **ANONYMITY**

We define anonymity using the following statement:

**Definition 3 (Unconditional source anonymity):** Given a message $m$ and a group of identities $\{ID_1, ID_2, \ldots, ID_n\}$, for an adversary who does not belong to the group, if the adversary cannot identify the true signer $s$ with probability larger than $1/n$ based on a valid signature $\sigma$, the signature scheme has the property of unconditional source anonymity.

In this paper, we also study the enhanced privacy which has stronger definitions for security [18] other than the unconditional source anonymity. The enhanced privacy consists of two extensions: anonymity with regard to adversarially-chosen keys and anonymity against the full key exposure.

For the first extension, the adversary can inject “fake” $ID$’s into the signer group, which will decrease the number of legitimate signers in the group. These “fake” $ID$’s will not be used to sign messages. Then the adversary can increase the probability of finding out the true signer of messages. To prevent from the anonymity with regard to adversarially-chosen keys attack, the validity of the identities in the group can be verified first to detect the “fake” $ID$’s. We can devise verification algorithms to achieve this, but it is another research area independent from the message authentication studied in this paper. We mainly focus on the second security extension. Under the anonymity against the full key exposure attack, adversaries can reveal all the private keys in the signing group $L$ and analyze the keys to isolate the real signer. In this attack, the adversaries obtain almost all the sensitive information and can manipulate the private keys to break the privacy.

2) **UNFORGEABILITY**

Similar to [17], we will first define the EUF-IDRS-CMIA2 game then the existential unforgeability under the adaptive chosen-message-and-identity attack, which is modeled by the EUF-IDRS-CMIA2 game.

**Definition 4 (The EUF-IDRS-CMIA2 game [17]):** There are three phases in the game:

- **Setup:** A challenger $C$ will first run the Setup algorithm in section IV-A. Then it will send the public parameters params to an adversary $A$ which is a polynomial time adversary. The hash functions used in the scheme will not be sent.

- **Attack:** For the following algorithms, the adversary $A$ can query as many times as it wants to:
  - Hash functions: the adversary $A$ can use any input to query any hash function in the authentication scheme.
  - **KeyGen:** the adversary $A$ can get the signing key $S_{ID}$ of any identity $ID$. For the $ID$ provided by $A$, $C$ will generate the secret key using the KeyGen algorithm in section IV-A and return $S_{ID}$.
  - **Sign:** the adversary $A$ can get the signature $\sigma$ of any message $m$. For $m$, $S_{ID}$ and an identity set $\{ID_1, ID_2, \ldots, ID_n\}$, $C$ will generate the signature using the Sign algorithm in section IV-A and return $\sigma$.

- **Forgery:** given a message $m$ and an identity set $\{ID_1, ID_2, \ldots, ID_n\}$, the following conditions are met: 1) $A$ did not make queries for any private keys corresponding to the identities in $\{ID_1, ID_2, \ldots, ID_n\}$ during the Attack phase. 2) $A$ did not make queries for the signatures relating to $m$ or any identities in...
During the Attack phase, then the adversary $A$ outputs a signature $\sigma$ for $m$ and $\{ID_1, ID_2, \ldots, ID_n\}$. If $\sigma$ can pass the verification in the Verify algorithm of section IV-A, we say that $A$ wins the game. We also define the probability with which $A$ wins the game as the advantage of $A$. 

**Definition 5 (Existential Unforgeability Against the Adaptive Chosen-Message-and-Identity Attack [17]):** In the EUF-IDRS-CMIA2 game for an identity based message authentication scheme, if there does not exist any adversary that has a non-negligible advantage, we say that the scheme is existentially unforgeable against the adaptive chosen-message-and-identity attack.

**C. SCHEME CONSTRUCTION**

In this section, we will show the construction of our proposed IMAEP scheme based on the simple signature scheme [17]. There are four algorithms:

**Setup:** The KGC will generate the system parameters for a given security parameter $k$:

1) Generate $q = \Omega(2^k)$ which is a large prime number, and $\Omega(\cdot)$ means “asymptotic lower bound”. Generate $G_1$ which is an additive cyclic group of order $q$. Generate $G_2$ which is a multiplicative cyclic group of order $q$. Then generate $\hat{\epsilon} : G_1 \times G_1 \to G_2$, which is a bilinear map.

2) Let $P$ be a generator of $G_1$. Generate the master secret key: a random number $x \in Z_q^*$. Then compute $P_{pub} = xP$, which is the public key of the KGC.

3) Choose two cryptographic hash functions $H(\cdot)$ and $H_0(\cdot)$ which maps the set $\{0, 1\}^*$ to $G_1$, $H_0(\cdot)$ maps the set $\{0, 1\}^*$ to $Z_q^*$.

After the parameter generation and computation, the KGC will make $\text{param} = \{q, G_1, G_2, \hat{\epsilon}(\cdot, \cdot), P, P_{pub}, H(\cdot), H_0(\cdot)\}$ publicly available as the system parameters.

**KeyGen:** For a user with an ID $\in \{0, 1\}^*$, the KGC will compute the corresponding private key $S_{ID}$ using $S_{ID} = xH(ID) \in G_1$. Then through a secret channel, the KGC will send the private key to the user. Other users can efficiently retrieve a user’s public key by computing $Q_{ID} = H(ID) \in G_1$.

**Sign:** To sign a message $m$, a user $s$ will execute the following steps with its private key $S_{ID}$, and the public parameters $\text{params}$:

1) Form a signing group by choosing a set of $n$ identities $L = \{ID_1, ID_2, \ldots, ID_n\}$, including the user $s$.

2) Compute the public keys of all the users in the group according to $Q_{ID_i} = H(ID_i) \in G_1$, $i = 1, \ldots, n$.

3) Generate random points $U_i \in G_1$ and compute $h_i = H_0(m||L||U_i)$, where $||$ denotes the operation of concatenation and $i = 1, \ldots, n$, $i \neq s$.

4) Compute

$$U_s = r'_sQ_{ID_s} + \alpha P_{pub} - \sum_{i=1, i \neq s}^n (U_i + h_iQ_{ID_i}),$$

$$W = \alpha P,$$

5) Calculate $h_x = H_0(m||L||U_s)$ and

$$V = (r'_s + h_x)S_{ID_s} + \alpha P_{pub}.\quad (3)$$

6) Export the signature for $m$ $\sigma = \{U_1, \ldots, U_n, V, W, L\}$.\quad (4)

**Verify:** To check the validity of a signature $\sigma = \{U_1, \ldots, U_n, V, W, L\}$ on $m$, a verifier will take the following steps:

1) Request $T_1, T_2 \in G_2$ from the KGC, which will be used in the verification. $T_1, T_2$ are computed in the KGC by

$$T_1 = \hat{\epsilon}(P, W)^2,\quad (5)$$

$$T_2 = \hat{\epsilon}(P, V)^2.\quad (6)$$

2) Compute $Q_{ID_i} = H(ID_i), h_i = H_0(m||L||U_i)$ for $i = 1, \ldots, n$.

3) Check whether equation (7) holds:

$$\hat{\epsilon} \left( P_{pub}, \sum_{i=1}^n (U_i + h_iQ_{ID_i}) \right) T_1^{-1} = \hat{\epsilon}(P, V) T_2^{-1}.\quad (7)$$

4) The signature $\sigma$ is determined as valid if equation (7) holds. In all other cases, the signature is viewed as invalid and will be rejected.

To show that the IMAEP scheme is correct, we have the following theorem:

**Theorem 1:** The IMAEP scheme is correct if a signature $\sigma$ is valid.

**Proof:** If a signature $\sigma$ is valid, the left hand side of equation (7) can be written as

$$\hat{\epsilon} \left( P_{pub}, \sum_{i=1}^n (U_i + h_iQ_{ID_i}) \right) T_1^{-1} = \hat{\epsilon}(P, V) T_2^{-1}.$$

$$= \hat{\epsilon} \left( P_{pub}, U_s + h_sQ_{ID_s} + \sum_{i=1, i \neq s}^n (U_i + h_iQ_{ID_i}) \right) T_1^{-1} = \hat{\epsilon}(P, V) T_2^{-1}.$$

$$= \hat{\epsilon} \left( P_{pub}, r'_sQ_{ID_s} + \alpha P_{pub} + h_sQ_{ID_s} \right) T_1^{-1} = \hat{\epsilon}(P, r'_sS_{ID_s} + \alpha P_{pub} + h_sS_{ID_s}) T_1^{-1} = \hat{\epsilon}(P, r'_sS_{ID_s} + \alpha P_{pub}) T_1^{-1} = \hat{\epsilon}(P, \alpha P) T_1^{-1}.$$

$$= \hat{\epsilon}(P, r'_sS_{ID_s} + h_sS_{ID_s}) T_1^{-1} = \hat{\epsilon}(P, \alpha P) T_1^{-1}.$$

$$= \hat{\epsilon}(P, \alpha P) T_1^{-1}.$$
V. SECURITY AND PERFORMANCE ANALYSIS FOR IMAEP SCHEME

A. SECURITY ANALYSIS

In this section, we will analyze the security of the proposed IMAEP scheme, including unconditional source anonymity, anonymity under the full key exposure attack, and existential unforgeability under the adaptive chosen-message-and-identity attack.

1) UNCONDITIONAL SOURCE ANONYMITY

Theorem 2: The proposed IMAEP scheme can provide unconditional source anonymity.

Proof: (Sketch) An adversary can obtain information through

\[ U_j + \sum_{i=1, i \neq j}^n (U_i + h_iQ_{ID_j}) = (r_j + h_j)Q_{ID_j} - h_jQ_{ID_j} + \alpha P_{pub} \quad (9) \]

for each \( j \in \{1, \ldots, n\} \) at best if the adversary is not inside the signing group \( L \).

Since the adversary cannot get the values of \( r_j, h_j, Q_{ID_j}, \alpha \), \( U_j + \sum_{i=1, i \neq j}^n (U_i + h_iQ_{ID_j}) \) is indistinguishable from \( U_j + \sum_{i=1, i \neq j}^n (U_i + h_iQ_{ID_j}) \), \( j \neq s \) for the adversary. The only way to infer the real signer is to simply guess. The probability of a successful guessing is \( 1/n \). \( \square \)

2) ANONYMITY AGAINST THE FULL KEY EXPOSURE ATTACK

Theorem 3: The proposed IMAEP scheme can provide anonymity against the full key exposure attack.

Proof: (Sketch) An adversary can obtain all the private keys \( S_{id} \) \( (1 \leq j \leq n) \) of the signing group \( L \), where the real signer’s private key \( S_{id} \) is also included. In addition to the information obtained in (9), the adversary could get more information through

\[ V - h_jS_{ID_j} = (r_j + h_j)S_{ID_j} - h_jS_{ID_j} + \alpha P_{pub} \quad (10) \]

for each \( j \in \{1, \ldots, n\} \). Then the following bilinear pairings can be computed:

\[ \hat{e}(S_{ID_j}, U_j + \sum_{i=1, i \neq j}^n (U_i + h_iQ_{ID_j})) = \hat{e}(S_{ID_j}, (r_j + h_j)Q_{ID_j} - h_jQ_{ID_j} + \alpha P_{pub}) \]

\[ = \hat{e}(S_{ID_j}, (r_j + h_j)Q_{ID_j} - h_jQ_{ID_j})\hat{e}(S_{ID_j}, \alpha P_{pub}), \quad (11) \]

\[ \hat{e}(V - h_jS_{ID_j}, Q_{ID_j}) = \hat{e}(r_j + h_j)S_{ID_j} - h_jS_{ID_j} + \alpha P_{pub}, Q_{ID_j}) \]

\[ = \hat{e}(r_j + h_j)S_{ID_j} - h_jS_{ID_j})\hat{e}(\alpha P_{pub}, Q_{ID_j}). \quad (12) \]

The only way for the adversary to find out the real signer is by comparing (11) and (12):

- It is obvious that (11) and (12) are not equal for \( j \neq s \).
- For the case that \( j \) equals to \( s \), equation (11) can be written as \( \hat{e}(S_{ID_s}, r_jQ_{ID_j})\hat{e}(S_{ID_s}, \alpha P_{pub}) \) and equation (12) can be written as \( \hat{e}(r_jS_{ID_s}, Q_{ID_j})\hat{e}(\alpha P_{pub}, Q_{ID_j}) \).

These two equations are not equal because of the fact \( \hat{e}(S_{ID_s}, \alpha P_{pub}) \neq \hat{e}(\alpha P_{pub}, Q_{ID_j}) \).

No matter whether for the case \( j \neq s \) or the case \( j = s \), equations (11) and (12) are not equal. The adversary cannot spot the true signer. \( \square \)

It should be noted that, the adversary could successfully identify the real signer using the approaches in the proof of Theorem 3, if \( \hat{e}(S_{ID_j}, \alpha P_{pub}) \) does not appear in equation (11) and \( \hat{e}(\alpha P_{pub}, Q_{ID_j}) \) does not appear in equation (12):

- It is obvious that (11) and (12) are not equal for \( j \neq s \).
- For the case that \( j \) equals \( s \), equation (11) can be written as \( \hat{e}(S_{ID_j}, r_jQ_{ID_j}) \) and equation (12) can be written as \( \hat{e}(r_jS_{ID_s}, Q_{ID_j}) \). Thus they are equal.

This is the case for the scheme in [17] where \( \alpha P_{pub} \) does not appear in \( U_s \) or \( V \). The introducing of \( \alpha P_{pub} \) in the signing algorithm ensures that the adversary cannot identify the real signer even if it can access all the private keys in the signing group.

3) EXISTENTIAL UNFORGEABILITY AGAINST THE ADAPTIVE CHOSEN-MESSAGE-AND-IDENTITY ATTACK

Lemma 1 (The Forking Lemma): Assume \( A \) is a Probabilistic Polynomial Time (PPT) Turing machine. If the two conditions are met: 1) \( A \) can only access the public data and use the public data as input; 2) With non-negligible probability and a bounded polynomial time \( T \), for message \( m \), \( A \) can output a valid IMAEP signature \( \sigma = (U_1, \ldots, U_n, h_1, \ldots, h_n, V, W, L) \), then a replay of this machine can output another valid IMAEP signature \( \sigma' = (U_1, \ldots, U_n, h_1', \ldots, h_n', V', W, L) \) with non-negligible probability, where \( A \) and a different oracle are involved. In the signatures \( \sigma \) and \( \sigma' \), not all the \( h_i \) and corresponding \( h_i' \) are equal for \( 1 \leq i \leq n \).

Theorem 4: For the IMAEP scheme, if an adversary has a non-negligible advantage in the EUF-IDRS-CMIA2 game, the probability of solving the Computational Diffie-Hellman problem will be non-negligible.

Proof: To prove the theorem, we will construct a challenger \( C \) to solve the Computational Diffie-Hellman problem with non-negligible probability, employing an adversary that has a non-negligible advantage in the EUF-IDRS-CMIA2 game (assume the probability is \( \varepsilon_{eA} \)). The proof is completed in four steps.

Step 1. challenger \( C \) setup:
Let \( P \) be a generator of \( G_1 \) and \( (P, aP, bP) \) be the Computational Diffie-Hellman problem to be solved, where \( a, b \in \mathbb{Z}_q^* \) are randomly selected and not known by \( C \). Assume there is an adversary \( A \) that has a non-negligible advantage in the EUF-IDRS-CMIA2 game. \( C \) will answer \( A \) all the queries in the game. Similar to the setup in [25], the KGC public key of the ring signature is defined to be \( P_{pub} = aP \) and will be sent to \( A \). \( C \) will maintain two lists \( LIST \) and \( LIST_0 \) to save the inputs and outputs of previously queried hash functions \( H(\cdot) \) and \( H_0(\cdot) \).
Step 2. $A$ attacks the KGC and the signer of the IMAEP scheme emulated by challenger $C$:  

C answers the hash function $H(\cdot)$ queries as follows:  

1) For an $ID_i$ submitted by $A$, $C$ first checks LIST. If $ID_i$ exists in LIST, $C$ will return the corresponding value $H(ID_i)$ already saved in LIST.
2) If $ID_i$ does not exist in LIST, which means it is queried for the first time, $C$ will generate a random number $x_i$ which does not exist in LIST. Next $C$ will toss a random coin $\beta_i$ with the probability $Pr(\beta_i = 0) = \mu$ and $Pr(\beta_i = 1) = 1 - \mu$, where $\mu$ will be determined later. If the outcome $\beta_i = 0$, $C$ will calculate $H(ID_i) = x_iP$. If the outcome $\beta_i = 1$, $C$ will calculate $H(ID_i) = x_ibP$. Then $C$ will save the tuple $(ID_i, x_i, \beta_i, H(ID_i))$ in LIST.

In this way, $C$ can emulate the random oracle $H(\cdot)$ and keep the hash function consistent.

C answers the hash function $H_0(\cdot)$ queries as follows:  

1) Similar to the queries of $H(\cdot)$, for the query $Y_i$ submitted by $A$, $C$ first checks LIST. If $Y_i$ exists in LIST, $C$ will return the corresponding value $H_0(Y_i)$ already saved in LIST.  
2) If $Y_i$ does not exist in LIST, $C$ will generate a random number $y_i$ which does not exist in LIST and return $y_i$ as the result. Then $C$ will save the pair $(Y_i, y_i)$ in LIST.

C answers the Sign queries as follows:  

1) $C$ randomly chooses an index $s$, $1 \leq s \leq n$, to be the index of the signer. Different from the standard Sign algorithm where $\alpha \in \mathbb{Z}_p^*$ is chosen randomly, here $\alpha$ will be fixed to a constant and will be the same for any Sign queries.
2) Look up $ID_s \in L$, $1 \leq s \leq n$, submitted by $A$ in LIST. If $ID_s$ has not been queried before, $C$ will run the $H(\cdot)$ query first to get $H(ID_s)$. If $\beta_s = 1$ for $ID_s$, $C$ will halt and the solving process of the Computational Diffie-Hellman problem will fail for this time.
3) For the users in $L$, compute the corresponding public keys following $Q_{ID_i} = H(ID_i)$, $1 \leq i \leq n$, where $H(ID_i)$ is looked up from LIST.
4) Randomly generate points $U_i \in \mathbb{G}_1$, where $1 \leq i \leq n$ and $i \neq s$. If $m||L||U_i$ does not exist in LIST (where $\| \cdot \|$ is the concatenation operation), $C$ will run the $H_0(\cdot)$ query first. Next $C$ will calculate $h_i = H_0(m||L||U_i)$ which $H_0(m||L||U_i)$ is looked up from LIST.
5) Choose a random number $r'_j \in \mathbb{Z}_p^*$, calculate $U_j$, $W$, and $V$ using step 4) and step 5) in the Sign algorithm of the IMAEP scheme in section IV-C.
6) Return the signature $\sigma = \{U_1, \ldots, U_n, V, W, L\}$.

Step 3. $A$ forges a valid signature:  

Since we assume that $A$ has non-negligible probability in winning the EUF-DRS-CMIA2 game, $A$ can produce a valid signature $\sigma = \{U_1, \ldots, U_n, V, W, L\}$ with non-negligible probability.  

Step 4. $C$ solves the Computational Diffie-Hellman problem:  

Assume in the EUF-DRS-CMIA2 game, $A$ issues $Q_K$ times KeyGen query and $Q_s$ times Sign query. If $C$ does not halt during the KeyGen queries or Sign queries, $C$ can produce a valid signature $\{U_1, \ldots, U_n, h_1, \ldots, h_n, V, W, L\}$ on message $m$ with non-negligible probability greater than $\mu Q_K + Q_s \varepsilon_{AEF}^\mu$.

If for each of the $ID_i$ in $L$ the corresponding $\beta_i$ in LIST equals to 1, which means $C$ does not know the private key of any $ID_i \in L$, the probability would be $1 - \mu^n$. In this case, according to the Forking Lemma 1, a replay of $C$ could produce another valid signature $\{U_1, \ldots, U_n, h'_1, \ldots, h'_n, V', W, L\}$ on message $m$ with non-negligible probability $\varepsilon_F$, such that $h_j \neq h'_j$ for some $j \in \{1, \ldots, n\}$ and $h_i = h'_i$ for $1 \leq i \leq n$, $i \neq j$. Thus the conditional probability $Pr(C)$ can produce two valid signatures | $C$ can produce a valid signature | to $(1 - \mu)^n \varepsilon_F$.

Then we have the following equations:

$$\hat{\varepsilon} \left( P_{pub}, \sum_{i=1}^{n} (U_i + h_iQ_{ID_i}) \right) T_1^{-1} = \hat{\varepsilon} \left( P, V \right) T_2^{-1},$$

$$\hat{\varepsilon} \left( P_{pub}, \sum_{i=1}^{n} (U_i + h'_iQ_{ID_i}) \right) T_1^{-1} = \hat{\varepsilon} \left( P, V' \right) T_2^{-1}.$$  

If we divide these two equations, we can get

$$\hat{\varepsilon} \left( P_{pub}, (h_j - h'_j)Q_{ID_j} \right) = \hat{\varepsilon} \left( aP, (h_j - h'_j)x_jbP \right) = \hat{\varepsilon} \left( P, (h_j - h'_j)x_jabP \right) = \hat{\varepsilon} \left( P, V - V' \right).$$

Since $\hat{\varepsilon}$ is non-degenerate, $C$ can solve the Computational Diffie-Hellman problem through

$$abP = (h_j - h'_j)^{-1}(V - V'),$$

with the probability

$$Pr(C \text{ solves the problem}) = \mu Q_K + Q_s (1 - \mu)^n \varepsilon_{AEF}^\mu.$$  

When $\mu = (Q_K + Q_s)/(Q_K + Q_s + n)$, the first half of equation (18) will be maximized with the value

$$\left( \frac{Q_K + Q_s}{Q_K + Q_s + n} \right)^q \left( \frac{n}{Q_K + Q_s + n} \right)^n,$$

which can be further reduced to $(n/e(Q_K + Q_s))^n$ for large $Q_K + Q_s$, where $e$ is the base of the natural logarithm. Thus equation (18) can be written as:

$$Pr(C \text{ solves the problem}) = \left( \frac{n}{e(Q_K + Q_s)} \right)^n \varepsilon_{AEF}^\mu.$$  

Theorem 5: The IMAEP scheme is existential unforgeable against the adaptive chosen-message-and-identity attack.
Based on Definition 5 and Theorem 4, Theorem 5 can be derived directly. We can also prove the unforgeability following the direction below: according to the Forking Lemma, a polynomial time adversary can output two valid IMAEP signatures \( \{U_1, \ldots, U_n, h_1, \ldots, h_n, V, W, L\} \) and \( \{U_1, \ldots, U_n, h'_1, \ldots, h'_n, V', W, L\} \), such that \( h_i = h'_i \) for \( 1 \leq i \leq n, i \neq j, h_j \neq h'_j \), if it is capable of generating a valid IMAEP signature with some probability that is non-negligible. According to equation (8), we have
\[
\hat{\epsilon}(P_{pub}, \sum_{i=1}^{n}(U_i + h_iQ_{ID}))T_1^{-1} = \hat{\epsilon}(P, V)T_2^{-1},
\]
\[
\hat{\epsilon}(P_{pub}, \sum_{i=1}^{n}(U_i + h'_iQ_{ID}))T_1^{-1} = \hat{\epsilon}(P, V')T_2^{-1}.
\]
If we divide these two equations, we can get
\[
\hat{\epsilon}(P_{pub}, (h_j - h'_j)Q_{ID}) = \hat{\epsilon}(P, V - V'),
\]
which equals to
\[
\hat{\epsilon}(P, (h_j - h'_j)S_{IDj}) = \hat{\epsilon}(P, V - V').
\]
Thus the adversary can get the private key
\[S_{IDj} = (h_j - h'_j)^{-1}(V - V')\]
since the bilinear map \( \hat{\epsilon} \) is non-degenerate. This contradicts to the setting in the KeyGen algorithm in the IMAEP scheme, where the KGC will send the private key to the user using a secret channel and the user will keep the private key as a secret. Moreover, obtaining the private key \( S_{IDj} \) makes the forgery of a valid signature trivial.

### TABLE 2. Computational overhead comparison.

|                | \( G_1 \) Mul | \( H_0 \) | Pairing | \( G_2 \) Mul |
|----------------|---------------|-----------|---------|---------------|
| IMAEP scheme in [1] | \( n + 3 \)   | \( n \)   | 0       | –             |
| Verify         | \( n + 2 \)   | \( n \)   | 1       | –             |
| IMAEP scheme in [1] | \( n \)       | \( n \)   | 2       | 2             |
| Verify         | \( 3n/2 \)    | \( 3n/2 \)| \( n + 3 \)| –             |

### B. PERFORMANCE ANALYSIS

In this section, the computational overhead and communication overhead of the IMAEP scheme will be evaluated. The performance of the scheme in [1] is also analyzed for comparison since it can provide the same anonymity against the full key exposure attack and defines the enhanced privacy. In Table 2 we show the computational overhead in terms of major mathematical operations for signature generating and verification. The number of major operations are counted according to the specific steps in the algorithms. As an example, for the IMAEP scheme, in step 4) of the signing phase, \( n + 1 \) multiplications between elements from \( \mathbb{Z}_p^* \) and \( G_1 \) are performed in equation (1) and one more such multiplication is carried out in equation (2). In step 5) one new multiplication is performed in equation (3). In total, there are \( n + 3 \) multiplications in \( G_1 \) during the signing in the IMAEP scheme. The calculation for the numbers of other operations are similar. For the signature verification in [1], a verifier will have to check \( n \) identities of the signing group \( L \) in the worst case. To make the comparison fair, we assume during the verification phase, a verifier will check an average number of ID’s, which is \( \lfloor n/2 \rfloor \). Here \( \lfloor x \rfloor \) means outputting the largest integer that is smaller than or equal to \( x \).

During the signing phase, the IMAEP does not need the pairing operation which is computational intensive while the scheme in [1] involves pairing. During the verification phase, the operations needed in the IMAEP scheme is much less. It is worth noting that the IMAEP scheme only needs a constant number of pairing operations, while in the scheme [1] the number of pairing operations goes up linearly with the increasing of the group size.

Although during the verification phase, the verifier has to receive some aiding information from the KGC in the IMAEP scheme, considering its low computational cost, the small communication overhead is negligible. Moreover, the KGC and the verifier can be placed in the same node in practical implementations. In this case, there is no need to transfer the aiding information.

For the scheme proposed in [1], during the message signing, the calculation of \( h_i \) is different from the calculation of \( h_j \). Thus for the verification of a valid signature, the verifier has to assume \( ID_i \) to be the signer first and verify the signatures for every \( i \) from 1 to \( n \) until the verification equation holds for some \( i = s \). While the signature is accepted, the identity \( ID_s \) of the true signer can be obtained by the verifier. This scheme loses the property of unconditional privacy. Moreover, the authenticity of a message can only be verified by the designated verifier for the scheme in [1]. In networks where packets are forwarded by intermediate relay nodes, fake messages will be forwarded to the destination without being detected, which will lead to a waste of precious energy and bandwidth in the Internet of Things.

### VI. EIMAEPS SCHEME FOR GENERAL AD-HOC ACCESS STRUCTURES

In previous section, we study the ring signature scheme for a group of \( ID_s \): \( L = \{ID_1, ID_2, \ldots, ID_n\} \) with one group member \( ID_s \) as the signer of the message to be authenticated. In this section, we will extend the discussion to general ad-hoc access structures as in [25] and propose an extended IMAEP (EIMAEPS) scheme with the same level of anonymity as the IMAEP scheme.

#### A. RING SIGNATURE IN GENERAL AD-HOC ACCESS STRUCTURES

In general ad-hoc access structures, a single member with identity \( ID_s \) is extended to a subset \( L_i \) of \( d_i \) members with identities \( ID_{ij}, 1 \leq j \leq d_i \). The general access structure is defined as \( \mathcal{L} = \{L_1, L_2, \ldots, L_n\} \) with \( n \) subsets. To sign a message, all the members in a subset \( L_s \) will collaborate to calculate a valid signature. A verifier can check whether the signature is produced by some subset in \( \mathcal{L} \). However, anyone outside the subset \( L_s \) will not be able to tell which subset in \( \mathcal{L} \) is the actual signer.

#### B. EIMAEPS SCHEME

For the EIMAEPS scheme, the KGC will run the same Setup and KeyGen algorithms as the IMAEP scheme described in section IV-C.
Sign: To sign a message $m$, users with the identities $ID_{s,j}$, $1 \leq j \leq d_r$, that belong to subset $\mathcal{L}_s$ can collaborate and execute the following steps, with their private keys $S_{s,j}$ and the public parameters $\text{params}$:

1) Choose one user in $\mathcal{L}_s$ as the agent user to collect partial signatures from other users in $\mathcal{L}_s$ and complete the rest of the signing process. Without loss of generality, we assume the ID of the agent user to be $ID_{s,1}$.

2) The agent user selects a set of $n$ subsets $\mathcal{L} = \{\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_n\}$ with $\mathcal{L}_i$ as one of the subsets.

3) For $i = 1, \ldots, n$, the agent user computes the public keys of all the users in $\mathcal{L}_i$ according to $Q_{i,j} = H(ID_{s,j}) \in \mathcal{G}_1$, $1 \leq j \leq d_i$. Then for each $i = 1, \ldots, n$, calculate $PK_i = \sum_{j=1}^{d_i} Q_{i,j}$, which can be thought as the public key of the subset $\mathcal{L}_i$.

4) For each subset $\mathcal{L}_i$, $i = 1, \ldots, n$, the agent user generates random points $U_i \in \mathcal{G}_1$ and calculate $h_i = H_0(m||\mathcal{L}_i||U_i)$ where $||$ is the concatenation operation.

5) Each user of $\mathcal{L}_s$ chooses a random number $r'_{s,j} \in \mathbb{Z}_q^*$, calculates $U_{s,j} = r'_{s,j} Q_{s,j}$. $U_{s,j}$, $2 \leq j \leq d_s$, will be sent to the agent user.

6) The agent user chooses a random number $\alpha \in \mathbb{Z}_q^*$ and calculates

$$U_s = \sum_{j=1}^{d_s} U_{s,j} + \alpha P_{pub} - \sum_{i=1, i \neq s}^n (U_i + h_i PK_i), \quad (21)$$

$$W = \alpha P, \quad (22)$$

$$h_s = H_0(m||\mathcal{L}||U_s). \quad (23)$$

Then the agent user will send $h_s$ to all the other users in $\mathcal{L}_s$.

7) Each user of $\mathcal{L}_s$ calculates $V_{s,j} = (r'_{s,j} + h_s) S_{s,j}$. $V_{s,j}$, $2 \leq j \leq d_s$, will be sent to the agent user.

8) The agent user calculates

$$V = \sum_{j=1}^{d_s} V_{s,j} + \alpha P_{pub}. \quad (24)$$

9) Output the signature on message $m$ as

$$\sigma = \{U_1, \ldots, U_n, V, W, \mathcal{L}\}. \quad (25)$$

Verify: To check the validity of a signature $\sigma = \{U_1, \ldots, U_n, V, W, \mathcal{L}\}$ on $m$, a verifier will take the following steps:

1) Request $T_1, T_2 \in \mathcal{G}_2$ from the KGC the same way as the Verify algorithm of IMAEP scheme in section IV-C.

2) For $i = 1, \ldots, n$, calculate $h_i = H_0(m||\mathcal{L}||U_i)$ and $PK_i = \sum_{j=1}^{d_i} Q_{i,j}$ where $Q_{i,j} = H(ID_{s,j}), 1 \leq j \leq d_i$.

3) Check whether equation (26) holds:

$$\hat{e}(P_{pub}, \sum_{i=1, i \neq j}^n (U_i + h_i PK_i)) T_1^{-1} = \hat{e}(P, V) T_2^{-1}. \quad (26)$$

4) The signature $\sigma$ is determined as valid if equation (26) holds. In all other cases, the signature is viewed as invalid and will be rejected.

Similar to the IMAEP scheme, we have the following theorem to show that the EIMAEP scheme is correct:

**Theorem 6**: The EIMAEP scheme is correct if a signature $\sigma$ is valid.

**Proof**: If a signature $\sigma$ is valid, the left hand side of equation (26) can be written as

$$\hat{e}(P_{pub}, \sum_{i=1}^n (U_i + h_i PK_i)) T_1^{-1} = $$

$$= \hat{e}(xP, \sum_{j=1}^{d_s} U_{s,j} + h_s PK_s)$$

$$= \hat{e}(xP, \sum_{j=1}^{d_s} (r'_{s,j} + h_s) Q_{s,j})$$

$$= \hat{e}(P, \sum_{j=1}^{d_s} (r'_{s,j} + h_s) S_{s,j} + \alpha P_{pub}) T_2^{-1}$$

$$= \hat{e}(P, V) T_2^{-1}. \quad (27)$$

Since EIMAEP scheme is an extension of the IMAEP scheme, the analysis of the performance of the EIMAEP scheme is similar to that of the IMAEP scheme: EIMAEP scheme is computationally efficient considering the major mathematical operations needed in the corresponding algorithms.

**VII. SECURITY AND APPLICATION ANALYSIS FOR EIMAEP SCHEME**

**A. SECURITY ANALYSIS**

1) **UNCONDITIONAL SOURCE ANONYMITY**

**Theorem 7**: The EIMAEP scheme can provide unconditional source anonymity.

Similar to the proof of Theorem 2, for the adversary outside the access structure $\mathcal{L}$, the only way to infer the real signer is to simply guess. The probability of a successful guessing is $1/n$.

2) **ANONYMITY AGAINST THE FULL KEY EXPOSURE ATTACK**

For the EIMAEP scheme, the adversary can obtain all the private keys in the access structure $\mathcal{L}$ and try to identify the true signing subset $\mathcal{L}_s$.

**Theorem 8**: The EIMAEP scheme can provide anonymity against the full key exposure attack.

Similar to the proof of Theorem 3, the adversary can compute the following bilinear parings:

$$\hat{e}(SK_j, U_j + \sum_{i=1, i \neq j}^n (U_i + h_i PK_i))$$

$$= \hat{e}(SK_j, \sum_{k=1}^{d_s} (r'_{s,k} + h_s) Q_{s,k} - h_j PK_j + \alpha P_{pub})$$

$$= \hat{e}(SK_j, \sum_{k=1}^{d_s} (r'_{s,k} + h_s) Q_{s,k} - h_j PK_j) \hat{e}(SK_j, \alpha P_{pub}), \quad (28)$$
\[ \hat{e}(V - h_j \hat{SK}_j, PK_j) = \hat{e}\left(\sum_{k=1}^{d_i} (r_{j,k} + h_k)S_{s,k} - h_j \hat{SK}_j + \alpha P_{pub}, PK_j\right) \]
\[ = \hat{e}\left(\sum_{k=1}^{d_i} (r_{j,k} + h_k)S_{s,k} - h_j \hat{SK}_j, PK_j\right) \hat{e}(\alpha P_{pub}, PK_j). \]

(29)

where \( SK_j = \sum_{k=1}^{d_i} S_{j,k} \).

The only way for the adversary to find out the real signer is by comparing (28) and (29):

- It is obvious that (28) and (29) are not equal for \( j \neq s \).
- For the case that \( j \) equals to \( s \), equation (28) can be written as \( \hat{e}(SK_s, \sum_{k=1}^{d_i} r_{s,k}Q_{s,k}) \hat{e}(\alpha P_{pub}) \) and equation (29) can be written as \( \hat{e}(\sum_{k=1}^{d_i} r_{s,k}S_{s,k}, PK_s) \times \hat{e}(\alpha P_{pub}, PK_s) \). These two equations are not equal because of the fact \( \hat{e}(SK_s, \alpha P_{pub}) \neq \hat{e}(\alpha P_{pub}, PK_s) \).

No matter whether for the case \( j \neq s \) or the case \( j = s \), equations (28) and (29) are not equal. The adversary cannot spot the true signer.

It should be noted that, the adversary could successfully identify the real signer using the above approaches, if \( \hat{e}(SK_j, \alpha P_{pub}) \) does not appear in equation (28) and \( \hat{e}(\alpha P_{pub}, PK_j) \) does not appear in equation (29). This is the case for the scheme in [17] where \( \alpha P_{pub} \) does not appear in \( U_s \) or \( V \). The introducing of \( \alpha P_{pub} \) ensures the EIMAEP scheme’s anonymity for general access structures.

3) EXISTENTIAL UNFORGEABILITY AGAINST THE ADAPTIVE CHOSEN-MESSAGE-AND-IDENTITY ATTACK

Theorem 9: The EIMAEP scheme is existential unforgeable against the adaptive chosen-message-and-identity attack.

The theorem can be formally proved the similar way as in the proof of unforgeability of the IMAEP scheme. The corresponding EUF-IDRS-CMIA2 game should be modified as follows: 1) Change the Sign queries for identity sets \( L = \{ID_1, ID_2, \ldots, ID_n\} \) to queries for general access structures \( L = \{L_1, L_2, \ldots, L_n\} \). 2) The adversary \( A \) will forge a signature for \( L \) with the restriction that \( A \) did not make queries for all of the private keys in any subset \( L_i, 1 \leq i \leq n \).

Similarly, we can also prove the unforgeability another way through the application of the Forking Lemma: a polynomial adversary can output two valid EIMAEP signatures \( \{U_1, \ldots, U_{n_1}, h_1, \ldots, h_n, V, W, \emptyset\} \) and \( \{U_1, \ldots, U_{n_1}, h_1', \ldots, h_n', V', W, \emptyset\} \), such that \( h_i = h_i' \) for \( 1 \leq i \leq n, i \neq j, h_j \neq h_j' \). According to equation (27), we have
\[ \hat{e}(P_{pub}, \sum_{i=1}^{n} (U_i + h_iPK_i)) T_1^{-1} = \hat{e}(P, V) T_2^{-1}, \]
\[ \hat{e}(P_{pub}, \sum_{i=1}^{n} (U_i + h'_iPK_i)) T_1^{-1} = \hat{e}(P, V') T_2^{-1}. \]

Then we can get
\[ \hat{e}(P, (h_j - h'_j)PK_j) = \hat{e}(P, V - V'), \]
which equals to
\[ \hat{e}(V - h_j \hat{SK}_j, PK_j) = \hat{e}(V - h_j \hat{SK}_j, PK_j). \]

Thus the adversary can get
\[ SK_j = \sum_{k=1}^{d_i} S_{j,k} = (h_j - h'_j)^{-1}(V - V'). \]

(31)

In the KeyGen algorithm, the KGC will send the private key to the user using a secret channel and the user will keep the private key as a secret. The adversary cannot get the summation of the private keys of any subset either. Even we loose the condition and let the adversary get access to at most \( d_i - 1 \) private keys in subset \( L_i \), it still cannot forge a valid signature.

B. A POSSIBLE APPLICATION IN THRESHOLD SIGNATURES

The EIMAEP scheme for general access structures can also be used in threshold signatures, where \( t \) users in a group of \( N \) users collaborate to produce a signature on message \( m \) and a verifier can be convinced that at least \( t \) users have signed \( m \). As an example, assume that there are \( N \) members in an application in the Internet of Things and the application requires that a valid announcement has to be signed by at least \( t \) members. Then a group of members \( L_1, d_i \geq t \) can publish an announcement as follows:

1) Randomly choose members of the application and form another \( n - 1 \) groups \( L_2, \ldots, L_n \) with the number of members in each group to be at least \( t \). In practice, the group of the true signers \( L_1 \) can switch their index with another subset \( L_i \) to hide the group in \( L \).

2) Generate the ring signature for the general access structure \( L = \{L_1, L_2, \ldots, L_n\} \) using the EIMAEP scheme and publish the announcement.

In this way, the authenticity of the announcement can be verified and the group of the true signers will not be identified. We can achieve the anonymous threshold ring signature with enhanced privacy using the EIMAEP scheme.

VIII. CONCLUSION

In this paper, we propose an efficient message authentication with enhanced privacy (IMAEP) scheme using the identity based cryptography for the IoT networks. The IMAEP scheme can provide unconditional privacy as well as the enhanced privacy defined in [18] under the full key exposure attack. The proposed scheme can also achieve unforgeability under the adaptive chosen-message-and-identity attack. For all the statements and theorems, we conduct detailed analysis and provide formal proofs. Compared with the scheme in [1] that has the same level of anonymity and security, our proposed scheme has much lower computational overhead, and can provide extra unconditional privacy. For the general access structure \( L \) consisting of \( n \) subsets, we propose the EIMAEP scheme to support a group of users \( L_s \) in \( L \) to anonymously sign a message. Comprehensive analysis shows that the EIMAEP scheme can achieve the same level of privacy and unforgeability as the IMAEP scheme.
REFERENCES

[1] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, “An identity-based ring signature scheme with enhanced privacy,” in Proc. SecureComm Workshops, Aug. 2006, pp. 1–5.

[2] G. Pujolle, “An autonomic-oriented architecture for the Internet of Things,” in Proc. IEEE John Vincent Atanasoff Int. Symp. Mod. Comput. (JVA), Oct. 2006, pp. 163–168.

[3] X. Yu and Y. Xue, “Smart grids: A cyber-physical systems perspective,” Proc. IEEE, vol. 104, no. 5, pp. 1058–1070, May 2016.

[4] A. Burg, A. Chattopadhyay, and K.-Y. Lam, “Wireless communication and security issues for cyber-physical systems and the Internet-of-Things,” Proc. IEEE, vol. 106, no. 1, pp. 38–60, Jan. 2018.

[5] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks,” IEEE J. Sel. Areas Commun., vol. 23, no. 4, pp. 839–850, Apr. 2005.

[6] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, “TSVC: Timed efficient and secure vehicular communications with privacy preserving,” IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4987–4998, Dec. 2008.

[7] J. Guo, J. P. Baugh, and S. Wang, “A group signature based secure and privacy-preserving vehicular communication framework,” in Proc. Mobile Netw. Veh. Environ., May 2007, pp. 103–108.

[8] J. Li, Y. Li, J. Ren, and J. Wu, “Hop-by-hop message authentication and source privacy in WirelessSensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 5, pp. 1223–1232, May 2014.

[9] U. Rajput, F. Abbas, H. Eun, and H. Oh, “A hybrid approach for efficient privacy-preserving authentication in VANET,” IEEE Access, vol. 5, pp. 12014–12030, 2017.

[10] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 26, no. 1, pp. 96–99, Jan. 1983.

[11] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. CRYPTO, 1985, pp. 47–53.

[12] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” SIAM J. Comput., vol. 32, no. 3, pp. 586–615, Jan. 2003.

[13] S. Kuzhalvaimozhi and G. R. Rao, “Privacy protection in cloud using identity based group signature,” in Proc. 5th Int. Conf. Appl. Digit. Inf. Web Technol. (ICADITW), Feb. 2014, pp. 75–80.

[14] D. He, S. Zeadally, B. Xu, and X. Huang, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” IEEE Trans. Inf. Forensics Secur., vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[15] N.-W. Lo and J.-L. Tsai, “An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings,” IEEE Trans. Intell. Transp. Syst., vol. 17, no. 5, pp. 1319–1328, May 2016.

[16] S.-F. Zheng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, “Enhancing security and privacy for identity-based batch verification schemes in VANETs,” IEEE Trans. Veh. Technol., vol. 66, no. 4, pp. 3235–3248, Apr. 2017.

[17] S. S. M. Chow, S. M. Yiu, and L. C. K. Hui, “Efficient identity-based ring signature,” in Proc. 3rd Int. Conf. Appl. Cryptogr. Netw. Secur. (ACNS), 2005, pp. 499–512.

[18] A. Bender, J. Katz, and R. Morris, “Ring signatures: Stronger definitions, and constructions without random oracles,” in Theory of Cryptog- raphy, Berlin, Germany: Springer, 2006, pp. 60–79.

[19] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, “A secure authentication protocol for Internet of vehicles,” IEEE Access, vol. 7, pp. 12047–12057, 2019.

[20] V. Sureshkumar, S. Anandhi, R. Madhumathi, and N. Selvarajan, “Light weight authentication and key establishment protocol for smart vehicles communication in smart city,” in Smart City and Informatication, Singapore: Springer, 2019, pp. 349–362.

[21] F. M. Salem and R. Amin, “A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS,” Inf. Sci., to be published.

[22] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, “Privacy-aware authentication scheme for mobile cloud computing services,” IEEE Syst. J., vol. 12, no. 2, pp. 1621–1631, Jun. 2018.

[23] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, “Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage,” IEEE Trans. Inf. Forensics Secur., vol. 14, no. 2, pp. 331–346, Feb. 2019.

[24] A. Karati, R. Amin, S. K. H. Islam, and K.-K.-R. Choo, “Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment,” IEEE Trans. Cloud Comput., to be published.

[25] J. Herranz and G. Sáez, “New identity-based ring signature schemes,” in Proc. 6th Int. Conf. Inf. Commun. Secur. (ICICS), 2004, pp. 27–39.

JIAN LI received the B.S. and M.S. degrees in electrical engineering from Tsinghua University, China, in 2005 and 2008, respectively, and the Ph.D. degree in electrical engineering from Michigan State University, East Lansing, in 2015. He is currently an Assistant Professor with the School of Electronic and Information Engineering, Beijing Jiaotong University, China. His current research interests include network security, cloud storage, wireless sensor networks in the Internet of Things, privacy-preserving communications, and cognitive networks.

ZHENGJING ZHANG received the Ph.D. degree in communication and information systems from Beijing Jiaotong University, Beijing, China, in 2008. Since 2014, he has been a Professor with the Department of Electronic and Information Engineering, Beijing Jiaotong University. He is currently an Assistant Dean of the School of Software Engineering, Beijing Jiaotong University. He has published about 160 professional research articles. His research interests include wireless sensor network techniques and wearable sensor network techniques, including multisource data fusion, security and privacy, routing, and energy management. He is also a Guest Editor of the Journal of Electrical and Computer Engineering.

LIN HUI received the B.S. degree in mathematics from Tunghai University, the M.S. degree in mathematics from Fu Jen Catholic University, Taiwan, and the Ph.D. degree in computer science and information engineering from Tamkang University, Taiwan, in 2006. She got the support from the Chungshang Institute of Science and Technology to be a Special Student with the Department of Computer Science, University of Wisconsin–Madison, USA, in 1993. She is currently an Associate Professor with the Department of Innovation Information and Technology, Tamkang University. Her current research interests include operation research, data mining, and multimedia applications. She has published more than 80 journal articles, book chapters, and conference papers related to these fields.

ZHANGBING ZHOU is currently a Professor with the China University of Geosciences, Beijing, China, and an Adjunct Associate Professor with Telecom SudParis, France. His research interests include wireless sensor networks, services computing, and business process management. * * *